Chapter 1: Introduction to OTCnet

OTCnet Participant User Guide

Table of Contents

List of Figures

List of Tables

Glossary

Click this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Introduction to OTCnet Overview and OTCnet Course Content*. In this chapter:

- You will be introduced to OTCnet
- You will learn about OTCnet User Roles

Topics

The topics in this chapter include the following:

1. OTCnet Elements, Process Flows and End Users
2. OTCnet User Roles

Audience

The intended audience for *Introduction to OTCnet* includes:

- Administration Users
- Deposit Processing and Reporting Users
- Check Capture, Check Processing and Reporting Users
- Card Processing Users
- Viewers

Topic 1. Introduction to OTCnet

Overview

The Bureau of the Fiscal Service (BFS) Over the Counter Division (OTCD) provides the Over-the-Counter Channel Application (OTCnet) to facilitate electronic processing, reporting of deposits, and transaction activities. OTCnet financial services include retail transactions made at agency offices, face-to-face collection points, and point of sale (POS) locations throughout the US and abroad.

OTCD oversees the systems, networks and program infrastructure that enable world-class OTCnet financial services, including the collection of checks, cash, coins and credit, debit, and gift card transactions at agency POS locations around the globe. The OTCD is responsible for implementing a coordinated government-wide strategy for the collection of over-the-counter transactions and deposit activities (cash, card, check, foreign checks/currency, seized currency), and the transition from paper checks to electronic mechanisms.

OTCnet is a secure web-based system that enables federal agencies to integrate check conversion, deposit reporting, and card processing, so that all check, cash, coin, and card deposits to the Treasury General Account (TGA) are handled by one web-based application.

OTCnet offers agencies superior customer service and high-quality e-commerce solutions for collections and reporting needs.

OTCnet financial services includes the following:

- Electronic processing of US checks presented for cashing, payment, or deposit
- Processing of US currency, foreign currency cash and foreign check deposits
- Acceptance of credit, debit, and gift cards (Visa, MasterCard, American Express, Discover)
- Support of the Self-Service Kiosk
- Automation of the collection and settlement process
- Support of online reporting and research capabilities for reconciliation and inquiries
- Improvements of deposit history record-keeping
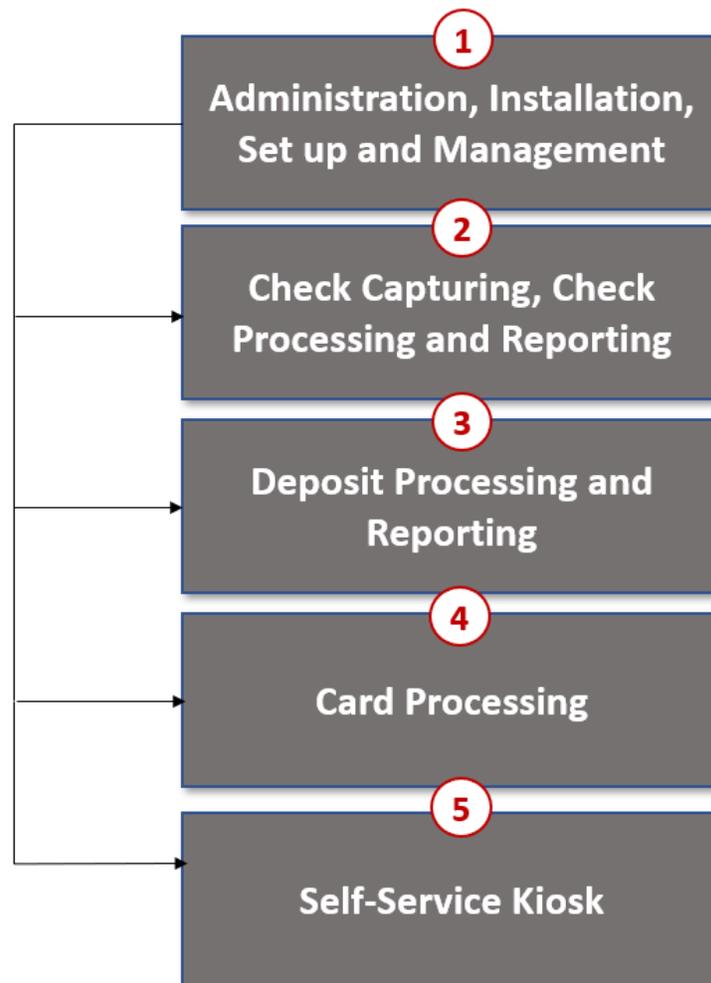
OTCnet Elements

OTCnet comprises five elements:

1. *Administration
2. Check Capture, Check Processing and Reporting
3. Deposit Processing and Reporting
4. Card Processing
5. Self-Service Kiosk: Web Service

*Administration functions support Check Capture, Check Processing and Reporting, Deposit Processing and Reporting, Card Processing, and Self-Service Kiosk as shown in Figure 1.

Figure 1. OTCnet Elements

The functions of the five elements are:

- **Administration, Installation Set Up and Management** allows for those with administrative permissions to install and manage OTCnet and set up users.

- **Check Capturing, Check Processing** converts personal and business checks into electronic fund transfers. Transactions include consumer, consumer accounts receivable, and business transactions

- **Deposit Processing** permits federal agencies to create and submit deposits for confirmation. This platform also allows financial institutions (FIs) to confirm those deposits and create adjustments electronically. Deposits are created for US currency, foreign cash, and foreign checks

- **Card Processing** allows agencies to provide their customers with an option to make payments via credit/debit cards and gift cards

- **Self-Service Kiosk** is a third-party vendor standalone kiosk supported by OTCnet

OTCnet Process Flow: Check Capture, Check Processing and Reporting

Check Capture and Check Processing involve converting paper checks received over the counter or through the mail into electronic debits to the check writer's account. The process is highly automated and greatly improves the collection, reconciliation, research, and reporting processes associated with federal agencies check collections.

In OTCnet, your agency scans a check, and the scanner captures an image of the front and back of each check. In OTCnet Online, the image is available immediately. You can also access the Collections Information Repository (CIR) to retrieve deposit information.

The captured image of the check is stored for seven years in OTCnet. You can search the check images as well as the check capture and transaction date through the Check Image and Research Archive (CIRA) Query feature within OTCnet.

OTCnet sends summary as well as detailed information to CIR for those agencies that are not processing tax transactions.

CIR sends accounting entries with Treasury Account Symbol/Business Event Type Code (TAS/BETC) or Classification Keys (C-Keys) to Central Accounting Reporting System/ Government Wide Accounting (CARS). CARS invokes Shared Account Module (SAM) to either validate, translate, or default the TAS/BETC based on the accounting information received on the transaction.

OTCnet sends the captured check data to the Debit Gateway at the Federal Reserve Bank Cleveland (FRB-C). FRB-C/Debit Gateway sends the data and settles to the financial institution (FI) either through FedACH (Automated Clearing House) personal check or Check 21 (non-personal check) where the check was written.

The FI where the check was written shows the account was debited (Complete Check Capture and Check Processing and Reporting Process flow as shown in Figure 2).

If your agency uses the Master Verification Database (MVD) (which provides downloads of prior negative check information and blocked items), the information is passed to the agency's Local Verification Database (LVD) when each batch is closed. The LVD is then used to determine the check writer's status and implement your agency's bad check policy, if applicable.

Figure 2. Check Capture, Check Processing, and Reporting Process Flow
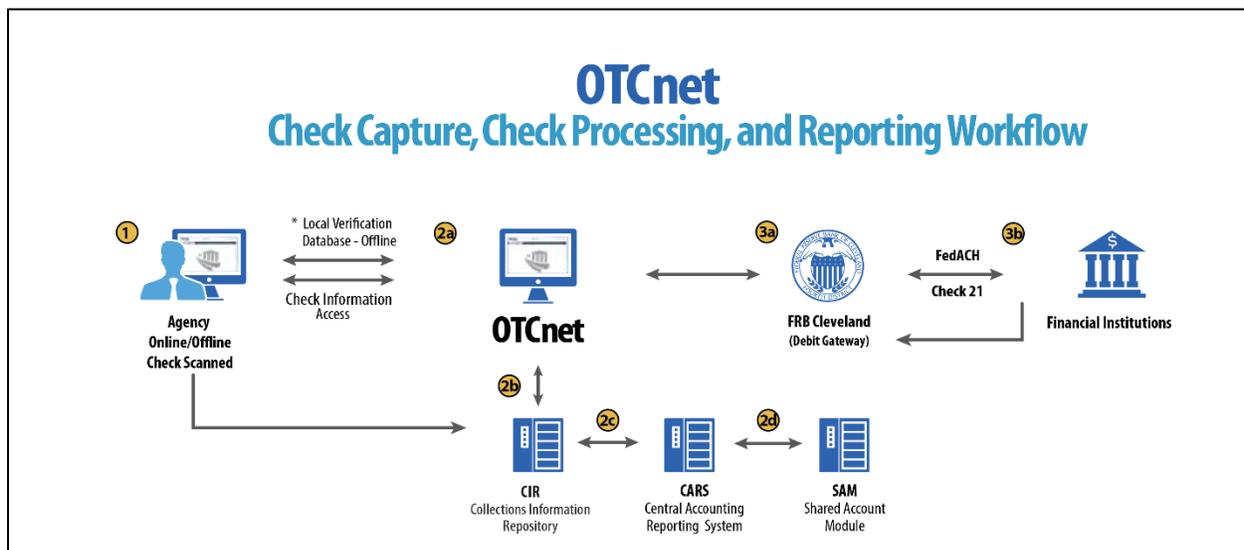
What is ACH?

The ACH Network is a nationwide batch-oriented electronic funds transfer system governed by the NACHA (National Automated Clearing House Association) operating rules, which provide for the interbank clearing of electronic payments for participating depository financial institutions. The Federal Reserve and Electronic Payments Network act as ACH operators, central clearing facilities through which financial institutions transmit or receive ACH entries. ACH payments include:

- Direct deposit of payroll, Social Security and other government benefits, and tax refunds
- Direct payment of consumer bills such as mortgages, loans, utility bills and insurance premiums
- Business-to-business payments
- E-checks
- E-commerce payments
- Federal, state, and local tax payments

What is Check 21?

Check 21, also known as the Check Clearing for the 21st Century Act, was signed into law on October 28, 2003. Provisions of the law took effect on October 28, 2004. It is important to understand the effects of Check 21 on OTCnet. Check 21 provides the legal framework for the creation of substitute checks, which can be used in place of the original paper document without an agreement in place with other financial institutions. A substitute check is a paper reproduction of the original check.

To meet legal requirements, a substitute check must:

- Contain an image of the front and back of the original check.

- Bear a legend that states, "This is a legal copy of your check. It can be used the same way you would use the original check."

- Display a magnetic Ink character recognition (MICR) line containing information appearing on the MICR line of the original check.

- Conform in paper stock, dimension, and otherwise, with generally applicable industry standards for substitute checks.

- Be suitable for automated processing in the same manner as the original check.

Overall, this legislation has modernized the nation's check payments system. Check 21 is designed to foster innovation in the payments system and to enhance its efficiency by reducing some of the legal impediments to check truncation.

ALL payment instruments are eligible for processing under OTCnet, including business checks, money orders, Treasury checks, credit card checks, traveler's checks, cashier's checks, official checks, third-party checks, payroll checks and checks drawn on state or local government accounts.

Check 21 requires financial institutions to accept a substitute check from a presenting institute and grant it equivalent status to the original check if the substitute check meets prescribed requirements. It also requires a reconverting bank to meet the warranties and indemnities enacted through legislation and subsequent regulations. Check 21 requires financial institutions to provide education to individual consumers on substitute checks and consumer re-credit rights.

For more information on Check 21, visit: https://www.frbservices.org/education/products-services-education/check21-act.html

Acceptable forms of FedACH and Check 21 payment types are shown in Table 1.

Table 1. FedACH and Check 21 Payment Types

FedACH	Check 21
- Direct Deposit of payroll, Social Security and other government benefits, and tax refunds - Direct Payment of consumer bills such as mortgages, loans, utility bills and insurance premiums - Business-to-business payments - E checks - E commerce payments - Federal, state, and local tax payments	- Business Checks - Money Orders - Treasury Checks - Credit Card Checks - Traveler's Checks - Cashier's Checks - Official Checks - Third-party Checks - Payroll Checks - Checks drawn on state or local government - Personal Check (No Notice) - Personal Check (Opt Out)

## OTCnet Process Flow: Deposit Reporting

Deposit Processing electronically collects US and foreign funds, which facilitates the daily classification of Treasury collections.

As shown in Figure 3, the Deposit Preparer, or Agency, electronically reports the deposit to Treasury using OTCnet and prints out the OTCnet deposit ticket. The bank deposit ticket, OTCnet deposit ticket, cash and checks (US and foreign) are taken to your Treasury General Account (TGA) bank. At the TGA bank, the Deposit Confirmer confirms the deposit, rejects the deposit, or creates an adjustment to the deposit using OTCnet.

OTCnet sends commercial deposit voucher information to CIR. CIR receives commercial deposit information from OTCnet for reconciliation and transmits it to the Treasury Cash Management System (TCMS) for cash concentration purposes. TCMS receives the commercial deposit data from CIR and initiates the cash concentration activity.

The Deposit Preparer and Deposit Viewer can access OTCnet to view their deposit ticket information, as well as access reports, receive rejections, and view adjustments.

Figure 3. Deposit Processing Workflow
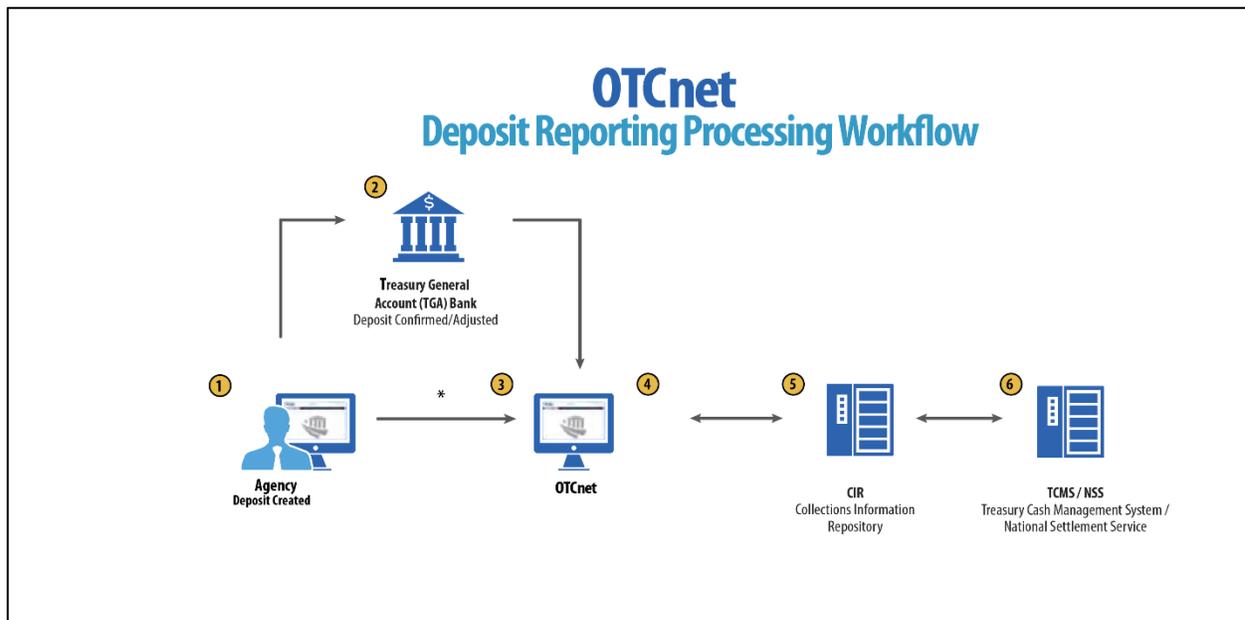
OTCnet Process Flow: Card Processing

Card processing is a web-based functionality that provides agency customers with an option to make payments with a credit, debit, or gift card. Card transactions are sent directly to WorldPay.

As shown in Figure 4, the Agency initiates the Card Processing payment. Currently, OTCnet does not store any card transaction details. The Agency can access the Collections Information Repository (CIR) to retrieve deposit and card payment information.

The customer pays with a credit/debit card or gift card at an agency terminal station. The customer authorizes the amount to be charged to their account. The Verifone/OTCnet terminal sends the transaction data to Worldpay for authorization.

Worldpay processes the payment in four steps:

Step 1 – Authorization (Real Time)
Worldpay sends the transaction data to the card issuer through the card network (e.g., Visa, Discover, Amex, and Mastercard). The card issuer determines whether funding is available and returns authorization through the card networks to Worldpay.

Step 2 – Clearing
Funds in the daily transaction batch are cleared from Worldpay to Comerica Bank. The processing cutoff for credit card payments is 4:30 AM; for debit card payments the cutoff is 2:00 AM.

Step 3 – Settlement
The card issuer sends the settlement money back to Worldpay via the card networks once the payments have been authorized and cleared. The timing for this transaction varies by credit/debit network.

Step 4 – Deposit Reporting
If the payment is approved, Worldpay sends deposit voucher transaction data to CIR via the Worldpay flat file the following morning between 4:00 and 6:00 AM.

CIR sends the voucher information to the Treasury Cash Management System (TCMS). TCMS uses the National Settlement Service (NSS) to draw funds. NSS transfers funds to the TGA Bank NY/FRB and reconciles them with Worldpay/Comerica Bank.

Figure 4. Card Processing Workflow
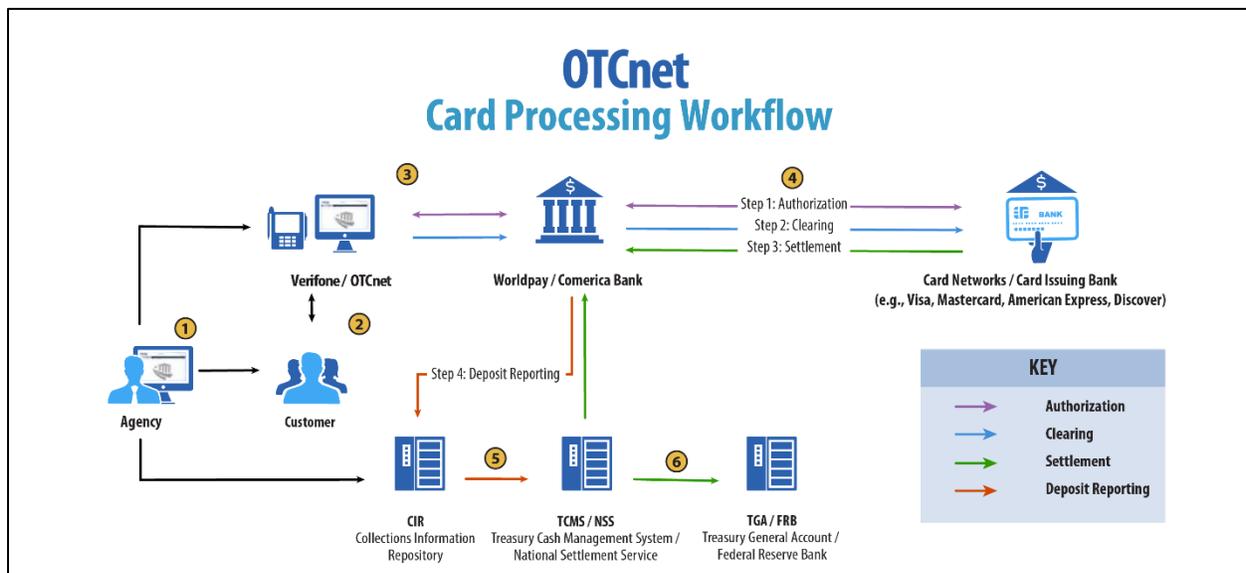
OTCnet Process Flow: Self-Service Kiosk: Check Payment

Self-Service Kiosk: Check Processing is a web-based functionality that provides agency customers with an option to make payments with a check at a kiosk. The Kiosk Operator sets up the workstation and Kiosk Tablet daily by logging in to and locking down the Kiosk Tablet.

As shown in Figure 5, the kiosk captures the image of the front and back of each check and stores these images on the kiosk server. The captured images are uploaded to the OTCnet server on a scheduled basis and are stored in OTCnet for seven years.

OTCnet sends the captured check data to Debit Gateway at the Federal Reserve Bank Cleveland (FRB-C). FRB-C/Debit Gateway forwards the data to the Financial Institution (FI) where the check was written, either through FedACH (for personal checks) or Check 21 (for non-personal checks). The FI receives the data and shows the account as debited.

OTCnet also sends summary as well as detailed information to the Collections Information Repository (CIR). CIR sends accounting entries with Treasury Account Symbol/Business Event Type Code (TAS/BETC) or Classification Keys (C-Keys) to the Central Accounting Reporting System (CARS). CARS invokes the Shared Account Module (SAM) to either validate, translate, or default the TAS/BETC based on the accounting information received on the transaction.

Agencies access OTCnet for Check Processing reports and use OTCnet's Check Image and Research Archive (CIRA) Query feature to search for check images, check capture dates and transaction dates. Agencies retrieve deposit information from the Collections Information Repository (CIR).

Figure 5. Self-Service Kiosk: Check Payment
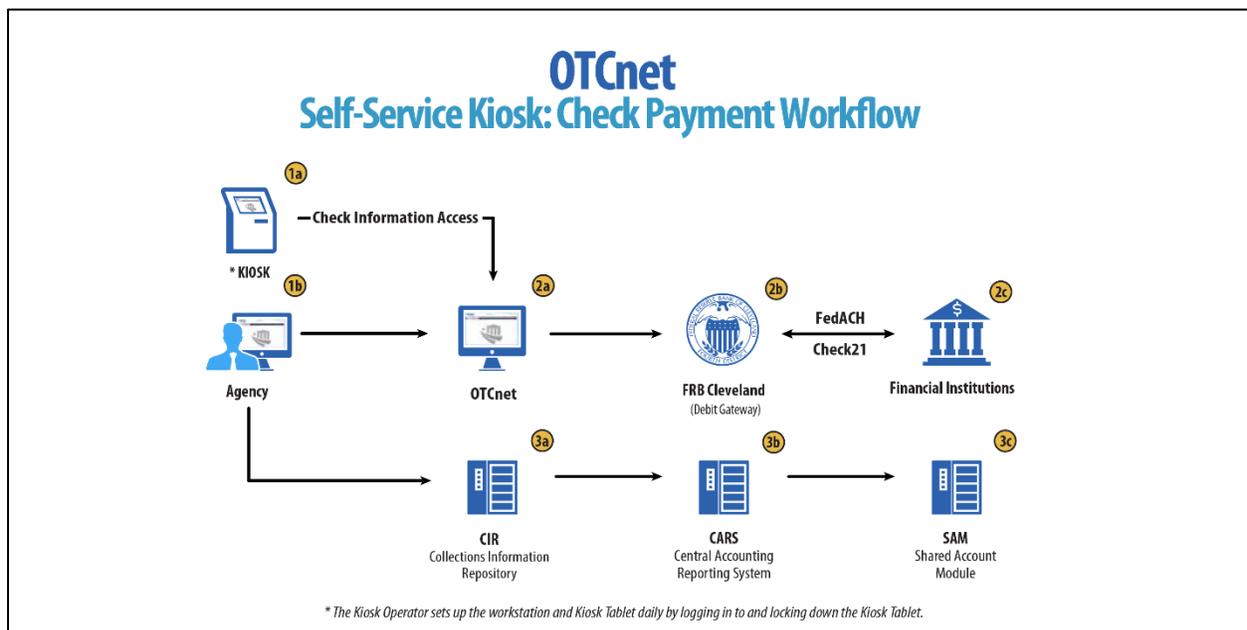
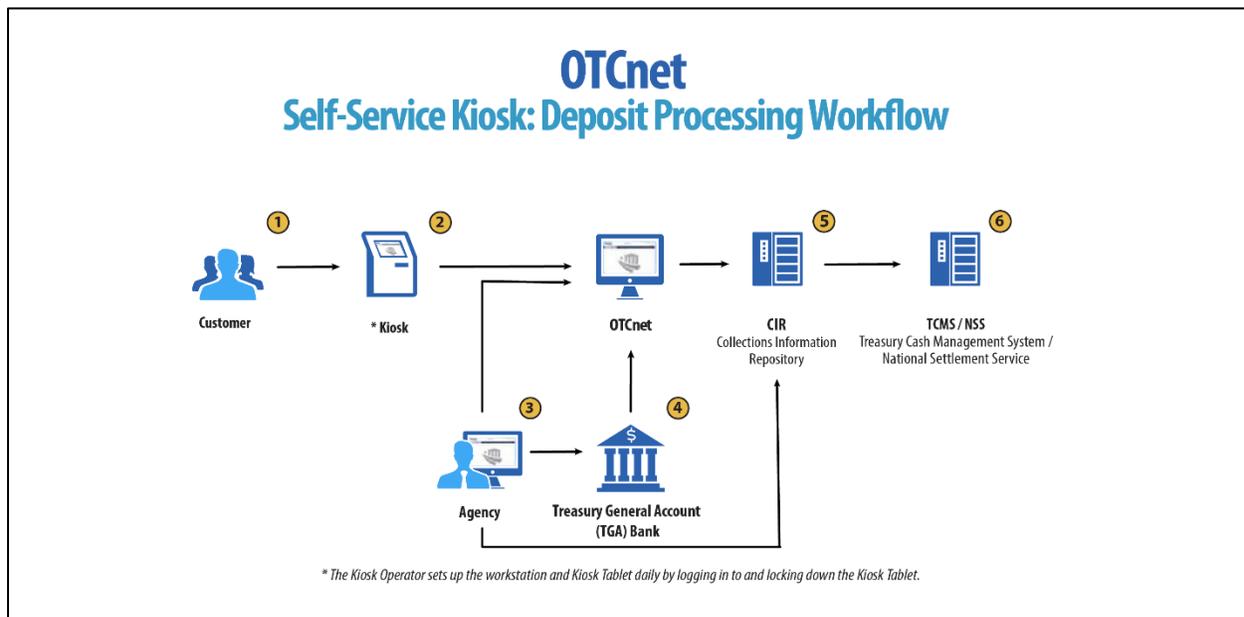## OTCnet Process Flow: Self-Service Kiosk: Deposit Processing

Self-Service Kiosk: Deposit Processing is a web-based functionality that provides agency customers with an option to make US cash payments at a kiosk. The Kiosk Operator sets up the workstation and Kiosk Tablet daily by logging in to and locking down the Kiosk Tablet.

As shown in Figure 6, the customer (kiosk user) makes US cash payments using the kiosk. The kiosk sends the deposit information to OTCnet with draft status. OTCnet creates a deposit voucher for the kiosk's cash payment transactions with accounting code information. The agency logs in to OTCnet to classify, approve and submit the voucher to the agency's FI and

can view the Deposit Process report. The FI verifies and confirms the deposit in OTCnet; the cash goes to the bank.

Once the FI has confirmed the deposit, OTCnet sends voucher information to the Collections Information Repository (CIR). CIR sends the voucher information to the Treasury Cash Management System (TCMS) and TCMS uses the National Settlement Service (NSS) to draw funds. Agencies can access CIR to retrieve deposit information.

Figure 6. Self-Service Kiosk: Deposit Processing Workflow

OTCnet Process Flow: Self-Service Kiosk: Card Processing

Self-Service Kiosk: Card Processing is a web-based functionality that provides agency customers with an option to make payments with a credit, debit, or Visa/Mastercard gift card at an agency terminal station. Card transactions are sent directly to WorldPay.

The Kiosk Operator sets up the workstation and Kiosk Tablet daily by logging in to and locking down the Kiosk Tablet.

As shown in Figure 7, payments can be made with a credit/debit card or Visa/Mastercard gift card at the kiosk. The customer authorizes the amount to be charged to their account. The kiosk sends transaction data to Worldpay for authorization.

Worldpay processes the payment in four steps:

Step 1 - Authorization (Real Time)
Worldpay sends the transaction data over to the card issuer through the card networks (e.g., Visa, Discover, Amex and Mastercard). The card issuer determines if funding is available and returns authorization back through the card networks to Worldpay.

Step 2 – Clearing
Funds in the daily transaction batch are cleared from Worldpay to Comerica Bank. The processing cutoff is 2:00 AM for debit card payments and 4:30 AM for credit card payments.

Step 3 – Settlement
Once the payments have been authorized and cleared, the card issuer sends the settlement money back to Worldpay via the card networks. The timing of the transfer varies by credit/debit network.

Step 4 - Deposit Reporting
If the payment is approved, Worldpay sends deposit voucher transaction data to the Collections Information Repository (CIR) via the Worldpay flat file the following morning between 4:00 AM and 6:00 AM.

CIR sends the voucher information to the Treasury Cash Management System (TCMS). TCMS uses the National Settlement Service (NSS) to draw funds. The kiosk sends the card transaction data to OTCnet via the card web service. NSS transfers funds to the TGA Bank NY/FRB and reconciles with Worldpay/Comerica Bank. The agency accesses OTCnet for Card Processing reporting; the agency can also access CIR to retrieve deposit information.

Figure 7. Self-Service Kiosk: Card Processing Workflow
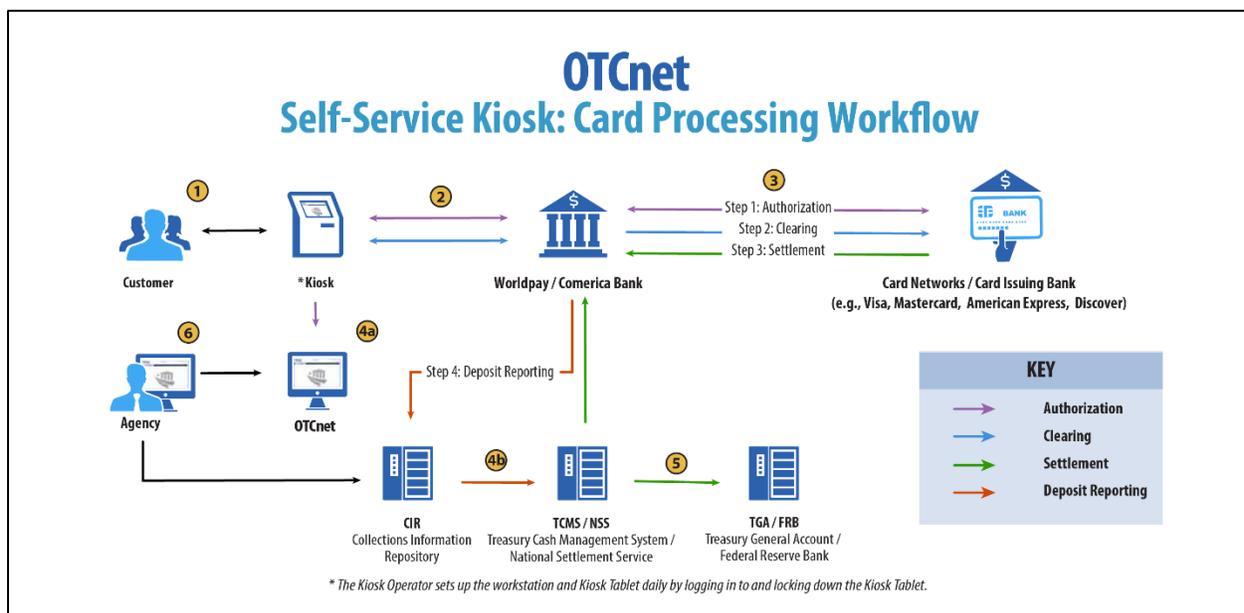
OTCnet End Users

There are four functional areas of the OTCnet application:

1. Administration
2. Check Capture, Processing and Reporting
3. Deposit Processing and Reporting
4. Card Processing

The user role you hold is based on the types of tasks you will perform.

- Administration user roles, with varying degrees of permission, perform administrative duties such as user management and system installation.

- Check Capture/Check Processing and Reporting user roles perform functions to capture checks, process checks, access reports and edit or view the Master Verification Database (MVD).

- Deposit Processing and Reporting user roles create or approve deposits, confirm (reject or adjust) deposits, or view deposit information, as shown in Table 2.

- Card Processing user roles perform functions to process card transactions.

Table 2. End User Roles

Administration	Check Capture/ Check Processing and Reporting	Deposit Processing and Reporting	Card Processing
Agency • Check Capture Supervisor • Check Capture Administrator • Accounting Specialist/ Local • Accounting Specialist • Card Administrator **Financial Institution/ Federal Reserve** • Primary Security Administrator • Local Security Administrator	**Agency** • Check Capture Operator • Check Capture Lead Operator • Check Capture Supervisor • Batch Approver* • Master Verification Database (MVD) Editor • Master Verification Database (MVD) Viewer	**Agency** • Deposit Preparer • Deposit Approver • Viewer **Financial Institution/ Federal Reserve** • Deposit Confirmer • Viewer	**Agency** • Card Operator

*Batch Approver is a sub-role assigned to users with existing roles.

Topic 2. OTCnet User Roles

Individuals are granted user access based on their job roles. Agency and Financial Institution/Federal Reserve Bank (FI/FRB) user roles are listed in Table 3 below with corresponding descriptions of job roles, the user roles that may assign the access, and whether the user can access Check Capture, Deposit Processing, or Card Processing functions.

Table 3. OTCnet Agency and FI/FRB User Roles

User Role	Role Description	Assignable By	Check Capture	Deposit Processing	Card Processing
Accounting Specialist	The agency user in this role is an expert on the organizational structure, reporting needs and accounting rules for their agency. This role will establish and maintain the organizational foundation, accounting data and accounting relationships at the highest level of the agency in OTCnet. This role can also establish, maintain, and view processing options that one or more lower-level endpoints will use in OTCnet.	Agency PLSA Agency LSA		•	
Agency Local Security Administrator (LSA)	The agency user in this role will maintain user access to an organization, including assigning/removing user roles and assigning/removing organization hierarchy access. LSAs can also view security reports.	Agency PLSA	•	•	
Agency Primary Local Security Administrator (PLSA)	The agency user in this role has the same capabilities as an LSA with the additional capability of creating and modifying LSAs for their organization. There can only be one PLSA per agency.	OTCnet Customer Support Team	•	•	
Agency Manager	The agency user in this role can view and download CIRA CSV (Comma-Separated Values) reports and ACR (Accessibility Conformance Report) Activity reports, run CIRA queries and view other general reports such as the SF215 Deposit Ticket and 5515 Debit Voucher reports. The agency user can view if an endpoint is designated for summary-level classification, and the agency comments associated with an endpoint.	Agency PLSA Agency LSA	•		
Card Administrator	The agency user in this role has the capability to manage endpoints for card processing. The user can view and modify terminal configuration. The user can also modify, delete, view, and search organization hierarchy. Lastly, this user has the capability to download releases and read/view audit card modules.	Agency PLSA Agency LSA			•

User Role	Role Description	Assignable By	Check Capture	Deposit Processing	Card Processing
Card Operator	This user views organizational hierarchy and searches within the organization. This user can process credit card payments, query card transactions, and view terminal configuration. Finally, this user can read/view the audit log and has partial access to the user's own activities.	Agency PLSA Agency LSA			•
Check Capture Administrator	The agency user in this role has the capability to define and modify the check capture sites as well as manage accounting codes and modify endpoint mappings. For example, this user can set up the location policy and location group. Additionally, this user can view, modify, and import accounting codes and modify endpoint mappings. This user can also configure the Check Capture functions and perform upgrades to the application, as well as download user profiles for the site. Furthermore, this user can view checks at the item level or a batch at the summary level classified with multiple accounting codes, view/download CIRA CSV reports and ACR Activity reports, run CIRA queries and view other general reports such as the SF215 Deposit Ticket and 5515 Debit Voucher reports. The agency user can view if an endpoint is designated for summary-level classification, and the agency comments associated with an endpoint. This user has permission to download software or firmware to the terminal using the Download Check Capture application permission. Lastly, this user is authorized to download the OTCnet Local Bridge (OLB) application, install the OLB certificate, install the OLB application, create the OLB profile, and start and stop the OLB application.	Agency PLSA Agency LSA	•		

User Role	Role Description	Assignable By	Check Capture	Deposit Processing	Card Processing
Check Capture Lead Operator	The agency user in this role will have the ability to scan checks into a batch, view and classify checks at the item level or a batch at the summary level with multiple accounting codes, close a batch, edit a batch, balance check amounts, and enter batch control values during batch closing. This user is authorized to install the OTCnet Local Bridge (OLB) certificate, install the OLB application, create the OLB profile, and start and stop the OLB application. Additionally, this user is authorized to accept checks with poor quality, make MICR line corrections, and accept duplicates. This user is not authorized to use out-of-date LVD. This role can establish, maintain, and view processing options for an endpoint pertaining to summary-level classification and agency comments.	Agency PLSA Agency LSA	•		
Check Capture Operator	This agency user has the authorization to scan checks into a batch, view and classify checks at the item level or a batch at the summary level with multiple accounting codes, close a batch, balance check amounts, and enter batch control values during batch closing. This agency user can also view if an endpoint is designated for summary-level classification, and the agency comments associated with an endpoint. This user is authorized to install the OTCnet Local Bridge (OLB) certificate, install the OLB application, create the OLB profile, and start and stop the OLB application. Additionally, the user can enter/apply the Accounting Code at the time of scanning checks. However, the user does not have authorization to accept duplicates, make MICR corrections, authorize the use of out-of-date LVD, or accept checks with poor quality.	Agency PLSA Agency LSA	•		

User Role	Role Description	Assignable By	Check Capture	Deposit Processing	Card Processing
Check Capture Supervisor	The agency user in this role is the most powerful user on the Check Capture site. The user can perform almost all the functions in Check Capture, including view and classify checks at the item level or a batch at the summary level, accept duplicates, make MICR corrections, authorize the use of out-of-date LVD, accept checks with poor quality, as well as view, modify, and import accounting codes, and modify endpoint mappings. However, this user does not have any permissions associated with scanning checks. To ensure "checks and balances," scanning checks is reserved for a Check Capture Operator or Lead Operator only. This role can also establish, maintain, and view processing options that one or more lower-level endpoints will use in OTCnet. This user is authorized to install the OTCnet Local Bridge (OLB) certificate, install the OLB application, create the OLB profile, and start and stop the OLB application.	Agency PLSA Agency LSA	•		
CIRA Viewer	The agency user in this role can only view organization endpoints and CIRA records. This is the check processing role with the lowest level of access. The agency user can view if an endpoint is designated for summary level classification, and the agency comments associated with an endpoint.	Agency PLSA Agency LSA	•		
Deposit Approver	The agency user in this role will approve the deposit report and submit the information to the TGA financial institution.	Agency PLSA Agency LSA		•	
Deposit Preparer	The agency user in this role prepares the deposit ticket and supporting information for transmission to the TGA financial institution.	Agency PLSA Agency LSA		•	
FPA Viewer	The agency user in this role can only search/view deposits and adjustments and produce reports.	Agency PLSA Agency LSA		•	
Local Accounting Specialist	The agency user in this role is an expert on the organizational structure, reporting needs and accounting rules for its depositing and lower-level endpoints. This role will establish, maintain, and view the organizational structure, accounting code mappings to individual endpoints, and the processing options that one or more lower-level endpoints will use in OTCnet.	Agency PLSA Agency LSA		•	

User Role	Role Description	Assignable By	Check Capture	Deposit Processing	Card Processing
MVD Editor	The agency user in this role can create, update, and read verification records. This role can also download CSV formatted reports, view other general reports such as the 215 Deposit Ticket, 5515 Debit Voucher reports and the ACR Activity report. The agency user can view if an endpoint is designated for summary-level classification and the agency comments associated with an endpoint.	Agency PLSA Agency LSA	•		
MVD Viewer	The agency user in this role can read CIRA records, verification records, and block records containing only AB permissions. This role also has permission to download CSV formatted reports and view other general reports such as the 215 Deposit Ticket, 5515 Debit Voucher reports and the ACR Activity report. The agency user can view if an endpoint is designated for summary-level classification, and the agency comments associated with an endpoint.	Agency PLSA Agency LSA	•		
View Report	The agency user in this role will have access to agency reports except for the CIRA CSV report.	Agency PLSA Agency LSA	•	•	
Deposit Confirmer	The financial institution user in this role will verify the submitted deposit ticket, reject the deposit ticket, if necessary, forward the information to the Treasury, and create adjustments as necessary.	FI PLSA FI LSA		•	
FI Viewer	The financial institution user in this role can only search and view deposits and adjustments, view Financial Institution information and produce reports from it.	FI PLSA FI LSA		•	
FI/FRB Local Security Administrator (LSA)	The financial institution/federal reserve bank user in this role will maintain user access to an organization, including assigning/removing user roles and assigning/removing organization hierarchy access.	FI PLSA		•	
FI/FRB Primary Local Security Administrator (PLSA)	The financial institution/federal reserve bank user in this role has the same capabilities as an LSA, with the additional capability of creating and modifying LSAs for their organization. There can only be one PLSA per financial institution.	OTCnet Customer Support Team		•	
FI/FRB Confirmer	The FI/FRB user in this role will verify the submitted deposit ticket, reject the deposit ticket, if necessary, forward the information to the Treasury, and create adjustments as necessary.	FI PLSA FI LSA		•	
FRB Viewer	The FRB user in this role can only search and view deposits and adjustments, view FRB information and produce reports from it.	FI PLSA FI LSA		•	

Agency User Role Combinations

As shown in Table 4 and Table 5, Agency Deposit Processing, Check Capture and Card Processing user roles can be combined and assigned to an individual user. "•" indicates that the role in the column heading can be combined with the role to the far left of it.

Table 4. Combinable Agency Deposit Processing, Check Capture and Card Processing User Roles

Agency User Roles	Agency PLSA	Agency LSA	Accounting Specialist	Local Accounting Specialist	Deposit Preparer	Deposit Approver	FPA Viewer
Agency PLSA							•
Agency LSA							•
Accounting Specialist				•	•	•	•
Local Accounting Specialist			•		•	•	•
Deposit Preparer			•	•		•	•
Deposit Approver			•	•	•		•
FPA Viewer	•	•	•	•	•	•	•
CIRA Viewer			•	•	•	•	•
View Report			•	•	•	•	•
MVD Editor			•	•	•	•	•
MVD Viewer	•	•	•	•	•	•	•
Card Administrator			•	•	•	•	
Card Operator			•	•	•	•	
Check Capture Operator			•	•	•	•	•
Check Capture Lead Operator			•	•	•	•	•
Check Capture Administrator		•	•	•	•	•	•
Check Capture Supervisor			•	•	•	•	•

Administration

Table 5. Combinable Agency Check Capture and Card Processing User Roles

Deposit Reporting, Check Capture and Card Processing User Roles	Agency Manager	CIRA Viewer	View Report	MVD Editor	MVD Viewer	Check Capture Operator	Check Capture Lead Operator	Check Capture Admin.	Check Capture Supvr.	Batch Approver
Agency PLSA					•					
Agency LSA					•			•		
Accounting Specialist		•	•	•	•	•	•	•	•	
Local Accounting Specialist		•	•	•	•	•	•	•	•	
Deposit Preparer		•	•	•	•	•	•	•	•	
Deposit Approver		•	•	•	•	•	•	•	•	
Agency Manager				•				•	•	
CIRA Viewer			•	•	•	•	•	•	•	
View Report		•		•	•	•	•	•	•	
MVD Editor	•	•	•		•	•	•	•	•	
MVD Viewer		•	•	•		•	•	•	•	
Card Administrator							•	•	•	
Card Operator						•	•	•	•	
Check Capture Operator		•	•	•	•					•
Check Capture Lead Operator		•	•	•	•			•	•	•
Check Capture Administrator	•	•	•	•	•		•		•	
Check Capture Supervisor	•	•	•	•	•		•	•		
Batch Approver						•	•			

Financial Institution (FI) User Role Combinations

Financial institution user roles that can be combined and assigned to an individual user are shown in Table 6. "•" indicates that the role in the column heading can be combined with the role to the far left of it.

Table 6. Combinable Financial Institution User Roles

Financial Institution (FI) User Roles	FI PLSA	FI LSA	FI Confirmer	FI Viewer
FI PLSA				•
FI LSA				•
FI Confirmer				•
FI Viewer	•	•	•	

System Tasks by Agency and Financial Institution (FI) Roles

The following two tables show the system tasks that can be performed by agency and Financial Institution/Federal Reserve Bank (FI/FRB) user roles. "•" indicates that the user role shown in the column heading can perform the task listed to the far left of it.

Table 7. Deposit Processing and Reporting Roles

Deposit Processing & Reporting Task	Agency PLSA	Agency LSA	Agency Acc Spec	Agency Local Acc Spec	Agency Dep. Prep.	Agency Dep. Appr.	FI/ FRB Viewer	FI/ FRB PLSA	FI/ FRB LSA	FI/ FRB Dep. Confirmer	FI/ FRB Viewer
Add/Update/Delete a User	•	•						•	•		
Reset Password	•	•						•	•		
Manage Own Account	•	•	•	•	•	•	•	•	•	•	•
OTCnet Logon and Homepage	•	•	•	•	•	•	•	•	•	•	•
Create/Modify Deposit					•						
Submit Deposit						•					
Confirm/Reject Deposit										•	
View Deposit/Adjustment Detail					•	•	•			•	•
Search Deposit/ Adjustment					•	•	•			•	•
Create Deposit/ Adjustment										•	
Create Return Item Adjustment										•	
Modify Organization Hierarchy			•	•							
Delete Organization Hierarchy			•	•							
View Organization Hierarchy			•	•							
Search Organization Hierarchy			•	•							
Modify Accounting Codes*			•								
Import Accounting Codes*			•								
View Accounting Codes*			•	•							
Modify Endpoint Mappings*			•	•							
Modify Custom Labels			•								
View Custom Labels			•	•							
Modify Processing Options			•	•							
View Processing Options			•	•							
Modify User Defined Fields			•								
View User Defined Fields			•	•							
View Financial Institutions										•	•
View Business Reports			•	•	•	•	•			•	•
View Security Reports	•	•						•	•		

Deposit Processing & Reporting Task	Agency PLSA	Agency LSA	Agency Acc Spec	Agency Local Acc Spec	Agency Dep. Prep.	Agency Dep. Appr.	FI/ FRB Viewer	FI/ FRB PLSA	FI/ FRB LSA	FI/ FRB Dep. Confirmer	FI/ FRB Viewer
View Administrative Reports					•	•	•			•	•
Read/View Audit Log	•	•									
View Reporters Flag			•	•							

The following table specifies OTCnet Check Capture roles and corresponding permissions at the agency level.

Table 8. Check Capture Roles

Check Capture Task	Check Capture Operator	Check Capture Lead Operator	Check Capture Admin.	Check Capture Supervisor	Batch Approver*	Online
Authorize Duplicates		•		•		Online
Authorize MICR Correction		•		•		Online
Authorize Poor Image Quality		•				Online
Balance Check Amounts		•		•		Online
Change Batch Control Values	•	•		•		Online
Change Batch Status				•		Online
Close Batch	•	•		•		Online
Edit Batch		•		•		Online
Change Mode	•	•				Online
Configure Check Capture System (settings)			•	•		Online
View Check Capture System Configuration	•	•	•	•		Online
Configure Batch Manager	•	•	•	•		Online
Override Verification				•		Online
Process Transactions (Scan Checks)	•	•				Online
Approve/Submit Batch				•	•	Online
View Batch List	•	•	•	•		Online
Void Item During Balancing				•	•	Online
Void Transaction				•	•	Online
Check Capture System Maintenance (Upgrade Scanner Firmware)			•	•		Online

Check Capture Task	Check Capture Operator	Check Capture Lead Operator	Check Capture Admin.	Check Capture Supervisor	Batch Approver*	Online
Create and Download Local Bridge Credential File	•	•	•	•		Online
Startup of OTCnet Local Bridge (OLB) Application	•	•	•	•		
Modify Classify Batch	•	•		•		Online
View Classify Batch	•	•	•	•		Online
Modify Classify Item	•	•		•		Online
View Classify Item	•	•	•	•		Online

The OTCnet Agency Check Processing user roles and their associated permissions are shown in Table 9.

Table 9. Check Processing

Check Processing Task	Agency Manager	Check Capture Operator	Check Capture Lead Operator	Check Capture Admin.	Check Capture Supervisor	CIRA Viewer*	View Reports*	MVD Editor	MVD Viewer	Batch Approver*
Manage Own Account	•	•	•	•	•	•		•	•	
OTCnet Logon and Homepage	•	•	•	•	•	•		•	•	
Modify Organization Hierarchy			•	•	•					
Delete Organization Hierarchy				•	•					
View organization Hierarchy	•	•	•	•	•	•		•	•	
Search Organization	•	•	•	•	•	•		•	•	
Create/Modify Verification Records								•		
View Verification Records								•	•	
Read Block Record Containing Only an ABA								•	•	
Create/Modify Check Capture Site				•						
Download Release**				•						

Check Processing Task	Agency Manager	Check Capture Operator	Check Capture Lead Operator	Check Capture Admin.	Check Capture Supervisor	CIRA Viewer*	View Reports*	MVD Editor	MVD Viewer	Batch Approver*
View CIRA	•					•	•	•	•	
Read/View Audit Admin (Partial)				•						
Read/View Audit Check Capture (All)				•						
Read/View Audit Check Capture Module (Partial)					•					
Read/View Audit Check Capture Module (Partial – User's Own Activity)		•	•							
Read/View Audit Check Processing (All)									•	
Read CIRA Check Image Report	•			•			•	•	•	
Read CIRA CSV Report	•			•				•	•	
Download CIRA CSV Historical Report	•			•			•	•	•	
Read Deposit Ticket Report	•			•			•	•	•	
Read Debit Voucher Report	•			•			•	•	•	
Modify Accounting Codes				•	•					
Import Accounting Codes				•	•					
View Accounting Codes				•	•		•			
Modify Endpoint Mappings				•	•					
Modify Summary-level Classification Flag			•		•					
View Summary-level Classification Flag	•	•	•	•	•	•		•	•	

Check Processing Task	Agency Manager	Check Capture Operator	Check Capture Lead Operator	Check Capture Admin.	Check Capture Supervisor	CIRA Viewer*	View Reports*	MVD Editor	MVD Viewer	Batch Approver*
Edit Agency Comments			•		•					
View Agency Comments	•	•	•	•	•	•		•	•	
Modify Processing Options			•		•					
View Processing Options			•		•					
ACR Activity Report	•			•			•	•	•	

*CIRA Viewer, View Reports, and Batch Approver are sub-roles assigned to users with existing roles.

**Download Release – includes downloading firmware, the OTCnet Local Bridge (OLB) application, and Security Updates.

Table 10. Card Processing

Card Processing Task	Card Operator	Card Administrator	Card Uploader*
Manage Own Account	•	•	
OTCnet Logon and Homepage	•	•	
Modify Organization Hierarchy		•	
Delete Organization Hierarchy		•	
View Organization Hierarchy	•	•	
Search Organization	•	•	
Process Card Payments	•		
Print Receipts	•		
Card Transaction Query	•		
Modify User-defined Fields (UDF)		•	
View User-defined Fields (UDF)		•	
Manage Card Process – Modify Terminal Configuration		•	
Manage Card Process – View Terminal Configuration	•	•	
Download OTCnet Local Bridge		•	
Create OTCnet Local Bridge OLB Credentials	•	•	
Import OTCnet Local Bridge OLB Credentials	•	•	
Read/View Audit Admin – (Partial)		•	
Read/View Audit Card Module – (All)		•	
Read/View Audit Card Module – (Partial – Access User's Own Activities Only)	•		
Card Web Service			•

*The Card Uploader is a Self-Service kiosk-server system role that is authorized to transmit card data from an external kiosk system to OTCnet. This role requests acknowledgement of the data transmitted; the system account with this role has no other permissions.

Summary

In this chapter, you learned:

- OTCnet Background and Organization
- OTCnet User Roles

Chapter 2: Accessing and Navigating OTCnet

OTCnet Participant User Guide

Table of Contents

List of Figures

List of Tables

Glossary

Select this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Accessing and Navigating OTCnet*. In this chapter, you will learn how to:

- Start and stop the OTCnet Local Bridge (OLB) application
- Request access for yourself in SailPoint IIQ
- Log in to OTCnet Online
- Navigate the OTCnet Online home page

Topics

The topics in this chapter include the following:

1. Starting and Stopping the OTCnet Local Bridge (OLB) Application
2. Requesting Access for Yourself in SailPoint IIQ
3. Logging in to OTCnet Online
4. Navigating the OTCnet Online Home Page

Audience

The intended audience for the *Accessing and Navigating OTCnet* Participant User Guide includes:

- All OTCnet users

Topic 1 Starting and Stopping the OTCnet Local Bridge (OLB) Application

The OTCnet Local Bridge (OLB) application is required for terminal detection and performing check capture, check processing and card processing tasks. If a user logs in to perform one of these operations and the OLB application is not started, the user receives the following message: *Terminal detection failed. Please ensure that the OLB application is running*. The OLB application is also required if you are using the Deployable Disbursing System (DDS) interface (Department of Defense [DoD] only).

If you are a **Check Capture Administrator**, **Check Capture Supervisor**, **Check Capture Lead Operator**, **Check Capture Operator, Card Operator** or **Card Administrator**, the OLB application must be started on the terminal to perform terminal configuration, check capture, check processing, and card processing tasks.

Before starting the OLB application, ensure the following steps are completed in this order:

1. The **Check Capture Administrator** and **Card Administrator** downloaded the OLB application.
2. The OLB application is installed on the terminal.
3. Each user has created an OLB profile, ensuring that the OLB credential file was not renamed (the file name remained the same as it was generated).
4. Each user has imported his/her OLB credentials to the terminal.

There is no "timeout" with the OLB application (i.e., a suspension or break in OTCnet activity). Therefore, the OLB application stays connected unless one of the following occurs:

- The user logs out of the terminal (Windows session).
- The terminal is restarted or rebooted.
- The user stops the OLB application on the terminal.

When using Microsoft Edge or Google Chrome:

- Ensure the latest version of the OLB is installed.

Start and Stop the OTCnet Local Bridge (OLB) Application

All users are authorized to start and stop the OTCnet Local Bridge (OLB) application.

To start the OLB application, either double-click the **Start OTCnet Local Bridge** icon on your terminal desktop or select **Start>Programs>Start OTCnet Local Bridge**.

If the **Start OTCnet Local Bridge** icon does not reside in either location, contact your **Card Administrator** or **Check Capture Administrator.** They will support your completion of the following steps:

- Ensure the latest version of the OLB is installed.
- Create your OLB profile.

- Import your OLB credentials.

If the OLB application is started on the terminal, you will receive an *OTCnet Local Bridge Application is already running* message.

When the *OTCnet Local Bridge Startup* page appears, enter your **OTCnet User ID** and **Password** in the appropriate text boxes. (Users will continue to use their User IDs to log in to OLB. They will not use their PIV/CAC or ID.me accounts).

Password Criteria includes the following. Your password must meet the following criteria:

- Be at least 12 characters long

- Not have more than two repeating characters

- Not repeat any of your last ten passwords

- Not have been your password during the last ten days

- Not be a word in a language, slang, dialect, or jargon

- Not be related to personal identity, history, environment, or other personal associations

To stop the OLB, double-click the **Stop OTCnet Local Bridge** icon located on the terminal desktop or select **Start**>**Programs**>**Stop OTCnet Local Bridge**.

Start and Stop the OTCnet Local Bridge (OLB) Application

To start the OTCnet Local Bridge (OLB) application, complete the following steps:

1. Double-click the **Start OTCnet Local Bridge** icon located on the terminal desktop.

    Or

    Select **Start**>**Programs**>**Start OTCnet Local Bridge**

2. The *OTCnet Local Bridge Startup* page appears. Enter your **OTCnet User ID** and **Password** in the appropriate text boxes.

3. Select **Log In**. A *Login Successful. OTCnet Local Bridge Application Started* message appears.

- Select **Cancel** and the *Are you sure you want to exit* message appears.
- Select **Yes** to cancel the OLB startup.
- Select **No** to return to the OTCnet Local Bridge Startup page.

4. Select **OK**.

Application Tip

Once you start the OLB application, proceed to log in to OTCnet Online.

5. To stop the OLB application, double-click the **Stop OTCnet Local Bridge** icon located on the terminal desktop as shown in Figure 1.

Figure 1. Stop OTCnet Local Bridge Icon

    Or

    Select **Start**>**Programs**>**Stop OTCnet Local Bridge**.

6. When the **Stop OTCnet Local Bridge** window and the *Are you sure you want to stop the OTCnet Local Bridge Application?* message appears, select **Yes**.

Application Tips

- If you select **No**, the *Are you sure you want to stop the OTCnet Local Bridge Application?* message closes, and the OLB application remains running.
- Stopping the OLB application ensures the application is completely closed and that your OTCnet session is securely terminated.
- Before uninstalling the OLB application, you must first stop the OLB application. If the OLB application has been started on the terminal, ensure that it is stopped before uninstalling the application.

Administration

Topic 2 Requesting Access for Yourself in SailPoint IIQ

Following the transition to Common Approach to Identity Assurance (CAIA), the SailPoint IdentityIQ (IIQ) environment will be used to manage the identities and provisioning of new users.

CAIA is a solution consisting of a common federation platform by which users seeking access to Fiscal Service programs will be able to register, proof, and authenticate their identity via one or more selected credential service providers.

Prospective OTCnet users can create identities through **Personal Identity Verification Cards (PIV)**, **Common Access Cards (CAC)**, or **ID.me**.

As a prospective OTCnet user, you can select your desired role(s) and high-level organization(s) based on instructions from your security administrator(s).

Self-Register/Create an Account in SailPoint IIQ

You can self-register in SailPoint IIQ and create an account using **PIV/CAC** or **ID.me**.

This functionality is available to all users but is not the preferred method for registering through SailPoint IIQ. The preferred option is for Primary Local Security Administrators or Local Security Administrators (PLSAs/LSAs) to assist with creating an identity for a user and/or requesting an HLO or role access for them in SailPoint IIQ.

Follow the on-screen instructions to sign in with an existing account or create an account. If prompted, follow the on-screen instructions to verify your identity. After completing all steps, you should see the SailPoint IIQ home page.

Self-Register/Create an Account in SailPoint IIQ

To self-register in SailPoint IIQ, navigate to the SailPoint IIQ environment at: *https://iiq.fiscal.treasury.gov/* and complete the following steps:

1. Log in using **PIV/CAC** or **ID.me** credentials as shown in Figure 2.

Figure 2. SailPoint IIQ Login Page
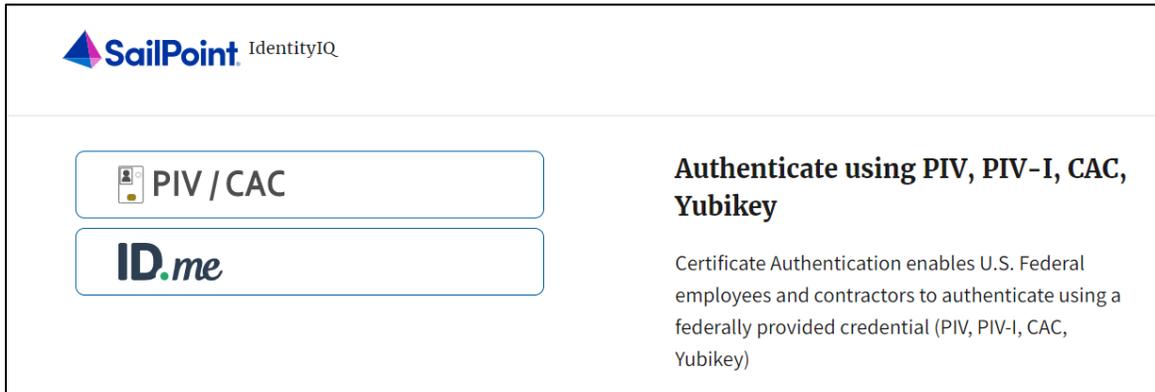
2. Follow the on-screen instructions to sign in with an existing account or create an account.

3. If prompted, follow the on-screen instructions to verify your identity.

4. After completing all steps, you should see the SailPoint IIQ home page.

Application Tip

New OTCnet users including those with **PIV/CAC** access can go through SailPoint IIQ to do the self-registration to create an account and request role(s) and high-level organization(s) before logging in to OTCnet. Once their high-level access is approved in SailPoint IIQ, they can proceed to log in to OTCnet.

Request Access for Yourself in SailPoint IIQ

If you need application entitlement, you can sign in to SailPoint IIQ and request the specific access you need (self-request).

To request access for yourself, log in to SailPoint IIQ and navigate to **Manage My Access.** Make sure **Add Access** is selected. In the search field, enter part or all of the **HLO/role** name you want to request. Select the **HLO/role** by selecting the **checkmark** to the left of the **HLO/role** name. Then select **Next**. On the **Review and Submit** screen, verify the requested **HLO/role(s)** are correct and select the **Submit** button.

A confirmation message will appear. SailPoint IIQ will automatically notify the necessary approvers to review the request. Once approved, your PLSA/LSA can create your identity in OTCnet and assign endpoints and roles for you. You will receive an autogenerated email when your user account is created in OTCnet.

Request Access for Yourself in SailPoint IIQ

To request access for yourself in SailPoint IIQ, complete the following steps:

1. From the **Home** screen of SailPoint, navigate to **Manage My Access** through the **Manage MyAccess** button as shown in Figure 3.

Figure 3. SailPoint Home Page with Manage My Access Button
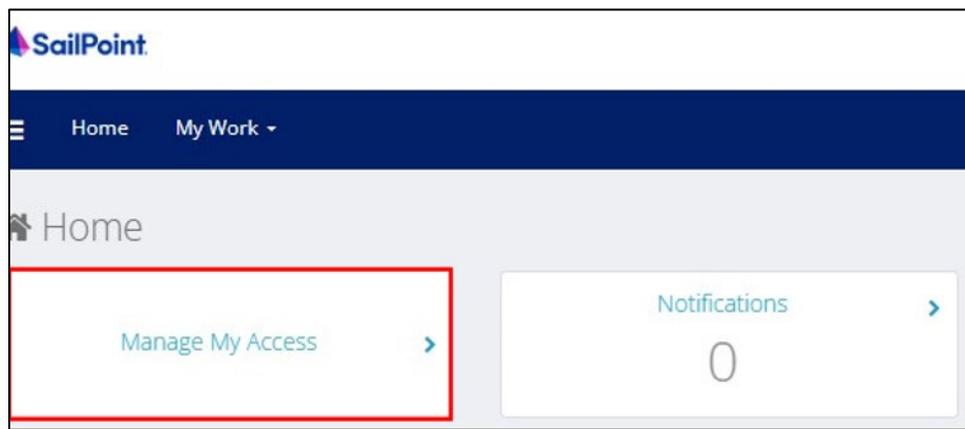
2. On the **Manage My Access** screen, ensure that the **Add Access** tab is selected as shown in Figure 4.

Application Tips

Search for the specific **HLO** name (e.g., Alaska USA Federal Credit Union) and user **role** (e.g., Check Capture Operator). If the HLO or user role's name is not known, type **HLO**/**Role** in the search field.

3. Search for an **HLO**. Select an **HLO** by selecting the **checkmark** to the left of the **HLO's** name.

4. Continue on the same screen to search for a user role. Select a **role** by selecting the **checkmark** to the left of the **role's** name. Then select **Next.**

Application Tips

- Multiple **HLOs** and **roles** can be selected.
- All roles selected in SailPoint IIQ will be validated (and edited as needed) in OTCnet by the designated **PLSA/LSA**.

Figure 4. Add Access Screen
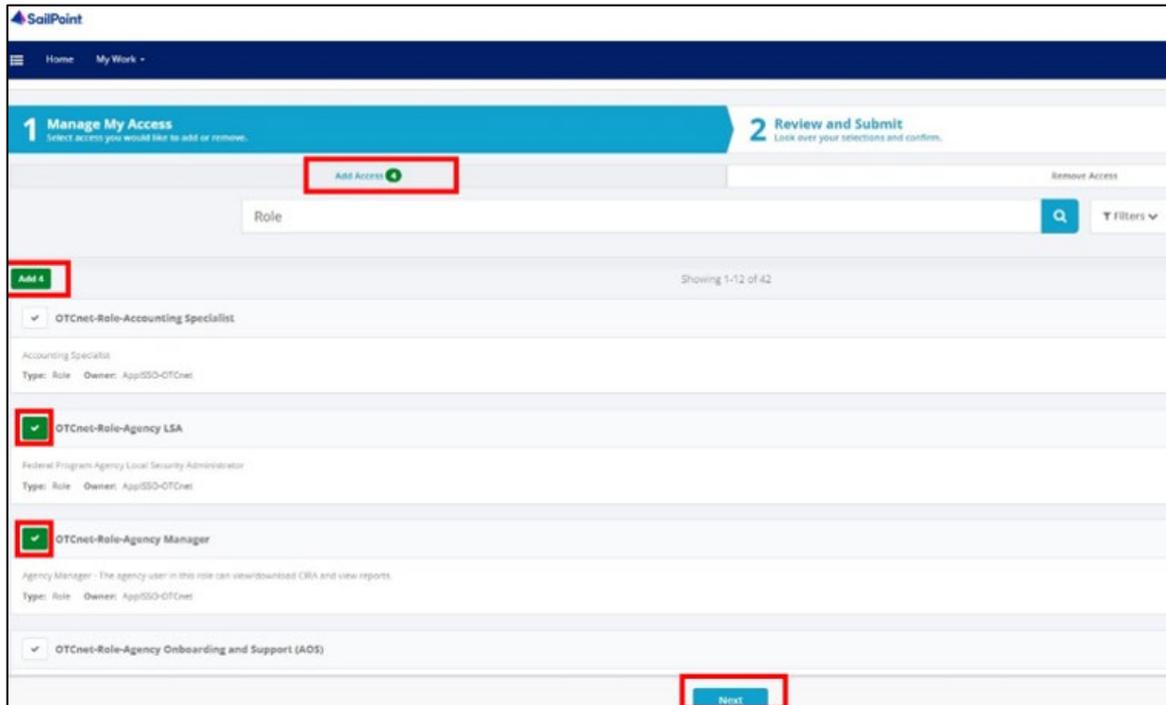
5. On the **Review and Submit** screen, verify the requested **HLOs** and **role(s)** are correct. Select the **voice bubble** to the right of the **HLO** or **role** to add any comments.

6. Select the **Submit** button at the bottom of the screen when finished, as shown in Figure 5.

Figure 5. Review and Submit Screen
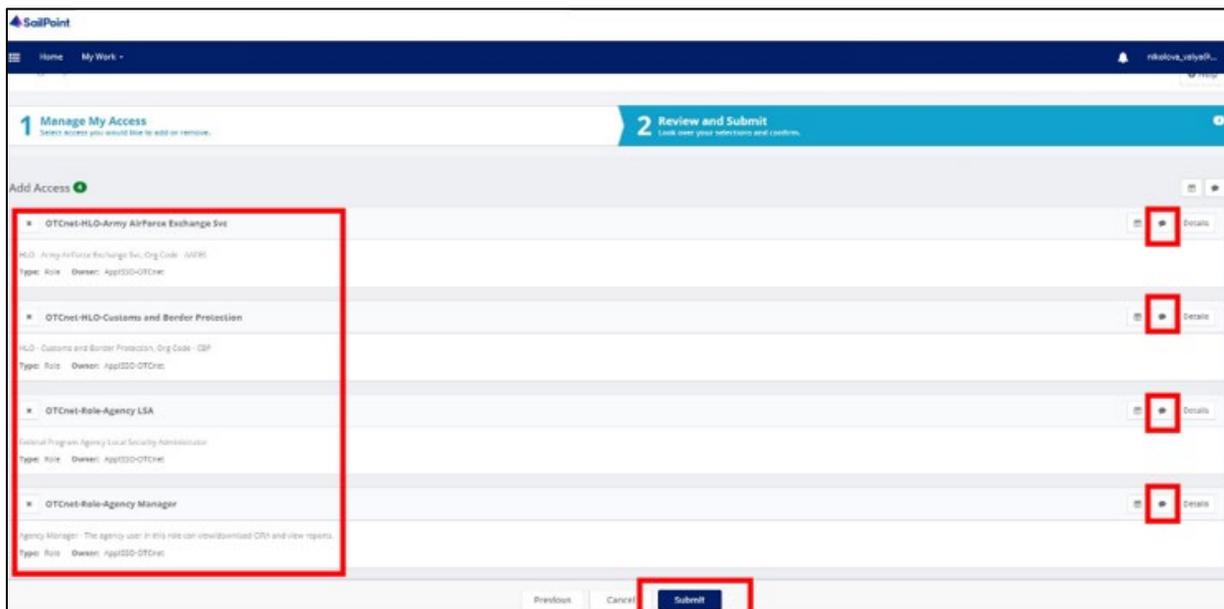
7. A confirmation message will appear. SailPoint IIQ will automatically notify the necessary approvers to review the request. Once approved, your PLSA/LSA can create your identity in OTCnet and assign endpoints and roles for you.

Application Tips

- You will receive an autogenerated email when your user account is created in OTCnet.

- Then you can access the OTCnet application.

Topic 3 Logging in to OTCnet Online

To log in to Fiscal Service Single Sign On (OTCnet Online) from the OTCnet Online login screen, use your **PIV/CAC** credentials if you are a government user or contractor, or **ID.me** if you are a non-government user.

If you are a non-government user who creates an account through **ID.me,** you will specify your email address associated with OTCnet. ID.me is a private single sign-on provider that meets the government's online identity proofing and authentication requirements.

Accounts registered by users for CAIA authentication are not application-specific, the same account credentials can be used on other sites or applications that are linked to CAIA. For example, Social Security Administration, Internal Revenue Service, Department of Veterans Affairs, and other government agencies accept **ID.me** credentials for logging in.

Log in to OTCnet Online

To log in to OTCnet Online, visit *https://otcnet.for.fiscal.treasury.gov* and log in with the following options: **PIV/CAC** or **ID.me.** Select the option that suits you best and follow the on-screen instructions to verify your identity or create an account in SailPoint IIQ.

Once you log in to OTCnet, you will be able to access functionality for one or more of the following:

- Administration
- Deposit Processing and Reporting
- Check Capture
- Check Processing
- Card Processing

The OTCnet Local Bridge (OLB) application is required for performing check processing, check capture, card processing and terminal configuration operations. If you are a **Check Capture Administrator**, **Check Capture Supervisor**, **Check Capture Lead Operator**, **Check Capture Operator, Card Operator** or **Card Administrator**, the **OLB** application must be started on the terminal to perform these operations.

Once a **new, first-time OTCnet agency end-user** has been fully provisioned with roles and endpoints, the first time they log in to OTCnet, they will receive an autogenerated email *'Welcome to OTCnet!'* that includes a list of resources to learn how to use OTCnet as well as important contact information to get acclimated to everything that OTCnet has to offer.

Log in to OTCnet Online

To log in to Fiscal Service Single Sign-On (OTCnet Online), complete the following steps:

1. Access *https://otcnet.for.fiscal.treasury.gov*. A page is presented which displays the following login options: **PIV/CAC** and **ID.me**, as shown in Figure 6.

Figure 6. OTCnet Login Screen
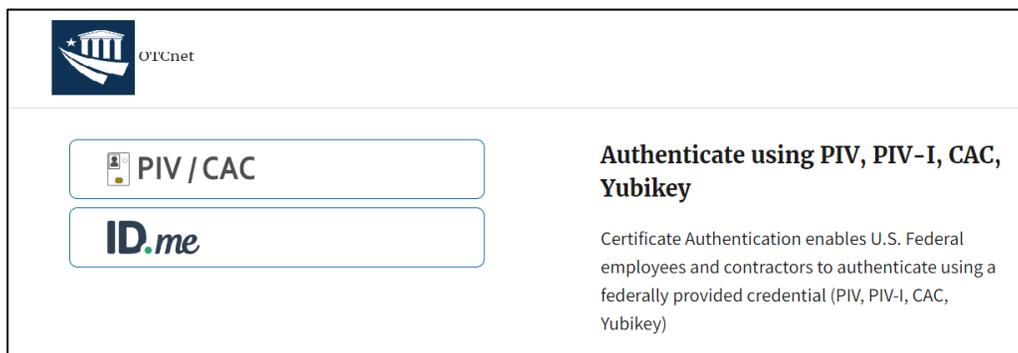
2. Select the option that best represents your status and follow the on-screen instructions.

Application Tips

PIV/CAC (Government Users/Contractors)

- Select the **PIV/CAC** button.

- If prompted, select your certificate and enter your PIN. If prompted, follow the on-screen instructions to verify your email address.

The first time a **PIV/CAC** certificate is used to authenticate, the email verification process is initiated.

- A web page is displayed prompting you to submit the **email address** that will be associated with your certificate. A **verification code** is sent to the email address specified.

- A web page is displayed to allow you to input the verification code from the email.

ID.me for Non-Government Users

- Select the **ID.me** button.

- Follow the on-screen instructions to sign in with an existing account or create an account. If prompted, follow the on-screen instructions to verify your identity.

- Use your **work email address** to create initially your **ID.me** identity. It is still recommended to add your personal email to your **ID.me** identity.

3. When you log in to OTCnet Online for first time you may be alerted that you are not permitted to access the application until your agency's security administrator completes your user provisioning in OTCnet, as shown in Figure 7.

4. Once your agency's security administrator has imported your user identity to OTCnet and assigned endpoints and roles for you, you will be able to access the application.

Figure 7. First Time Log In Screen
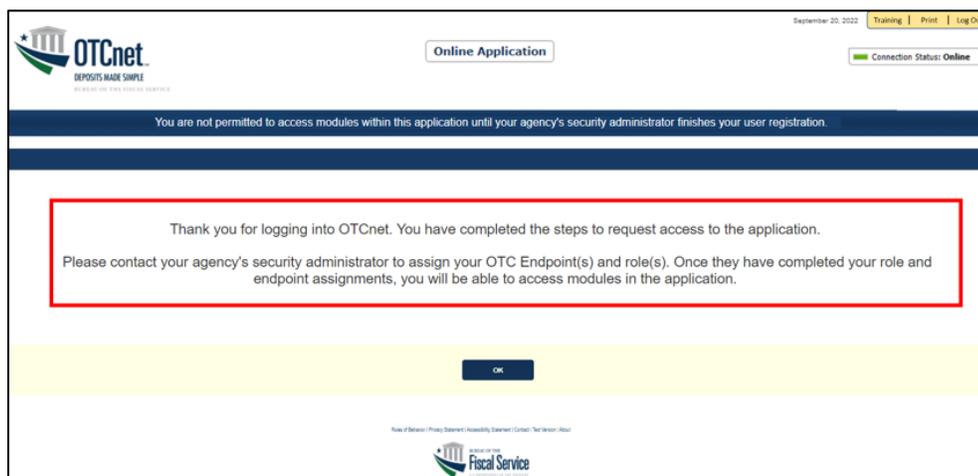
5. To completely log out, close your browser. You will need to reauthenticate the next time you log in to OTCnet.

💡 **Application Tip**

Ensure that you log in to OTCnet **at least once every 120 days** (or four months). Your user account will be disabled after 120 consecutive days of inactivity. To restore your account, contact the **Customer Support Team** to begin the process.

💡 **Application Tip**

If you are a **Check Capture Administrator**, **Check Capture Supervisor**, **Check Capture Lead Operator**, **Check Capture Operator**, **Card Operator** or **Card Administrator**, and use Microsoft Edge or Google Chrome when logging in to OTCnet Online, you will not see the OTCnet splash screen. Instead, the system automatically displays the OTCnet Homepage Message Overlay.

Topic 4 Navigating the OTCnet Online Home Page

The *OTCnet Online* home page allows **Check Capture Supervisors**, **Check Capture Lead Operators**, **Check Capture Operators** and **Card Operators** to process deposits, capture checks, process checks, process card transactions, view reports, and perform administrative and security functions. Additionally, a user can access information for training, help and to update a user profile. The OTCnet Online home page is accessible for users to either view or perform any of these functionalities.

OTCnet Online Main Menu

To access the OTCnet Main Menu, log in with your **PIV/CAC** or **ID.me** credentials at the following URL: *https://otcnet.for.fiscal.treasury.gov*. Table 1 provides a list of the Main Menu options available to you. They are accessible on the upper right corner of the OTCnet application.

Table 1. Main Menu Link Descriptions

Link	Description
Home	Allows a user to return to the OTCnet home page.
Training	Allows a user to access Web-Based Training (WBT) and other corresponding training materials.
Print	Allows a user to print the page.
Help	Allows a user to access help for the page they are on.
Log Out	Allows a user to log out of OTCnet.

The Main Menu is shown in Figure 8. The links are accessible on the upper right side of the OTCnet home page.

Figure 8: OTCnet Main Menu Page

15

OTCnet Homepage Message Overlay

All user roles have access to the OTCnet Homepage Message Overlay in OTCnet Online. For all Microsoft Edge and Google Chrome users, the message overlay automatically presents when you first log in to OTCnet.

The message overlay is a messaging platform presenting important news and information on the OTCnet system as shown in Figure 9. It is recommended that you read the messages, close the message overlay, and continue viewing the OTCnet homepage.

Figure 9. OTCnet Homepage Message Overlay
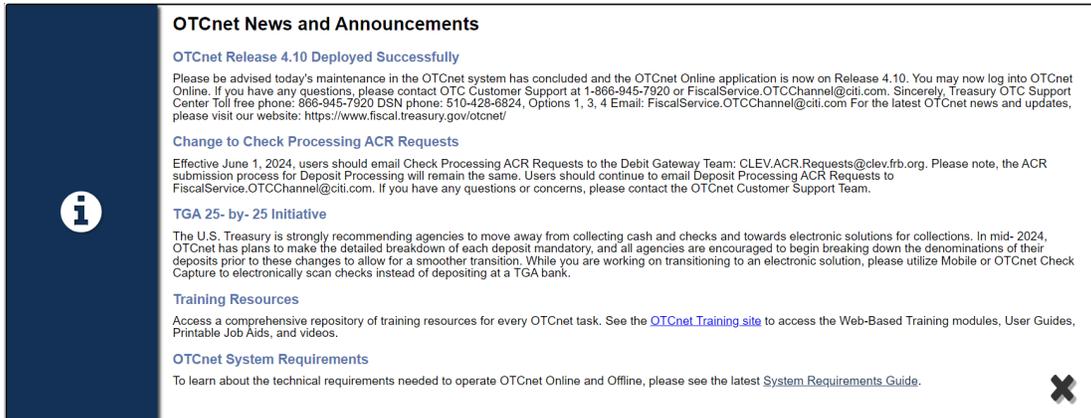
OTCnet Support Contact Overlay

Users can contact the OTCnet Customer Service team by submitting a form through the **Customer Support** button on the OTCnet homepage. This feature helps to standardize and streamline the inquiries and requests made to Customer Service. Select the **Customer Support** button on the bottom of the OTCnet homepage. The **Treasury OTC Support Contact** overlay appears over the homepage as shown in Figure 10.

Figure 10: Treasury OTC Support Contact Form
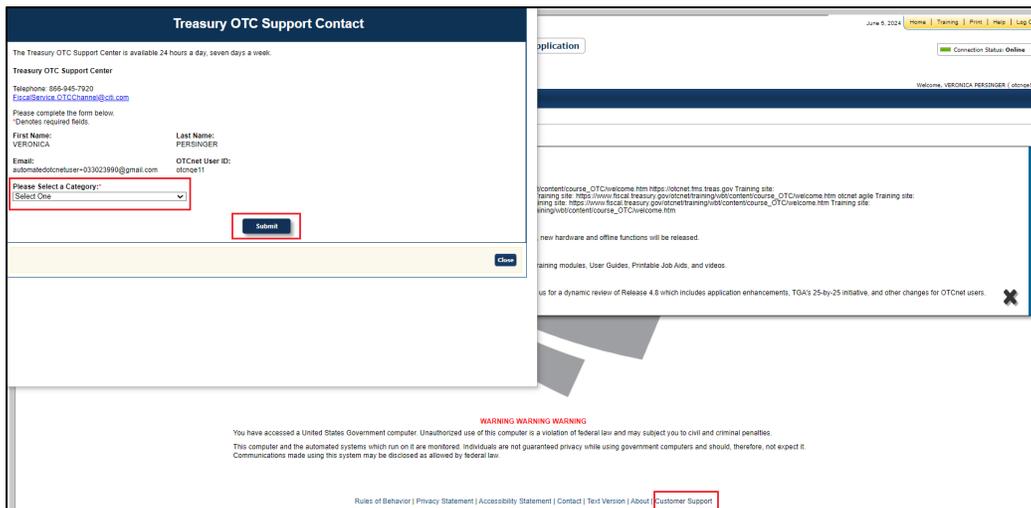
Select the **Please Select a Category** dropdown. The following options appear:

- Batch Management
- Check Scan
- Deposit Processing
- OTCnet Local Bridge (OLB)
- User Management
- Other

After you make the selections, select the **Submit** button to submit the request.

OTCnet Online Deposit Processing Tab Functionality

To access the OTCnet Deposit Processing functionality, log in with your **PIV/CAC** or **ID.me** credentials. Table 2 provides a list of the Deposit Processing functions that are available to you.

Table 2. Deposit Processing Tab Descriptions

Function	Description
Create Deposit	Allows a user to create deposits for US Currency, Foreign Check Items, and/or Foreign Currency Cash.
Search Deposits	Allows a user to search for deposits.
Search Adjustments	Allows a user to search for adjustments.
Create Returned Item Adjustment	Allows a user to create a returned item adjustment.

The Deposit Processing tab, as shown in Figure 11, allows you to access Deposit Processing functionality, although depending on your user role, you may not see all functionality.

Figure 11. Deposit Processing Tab
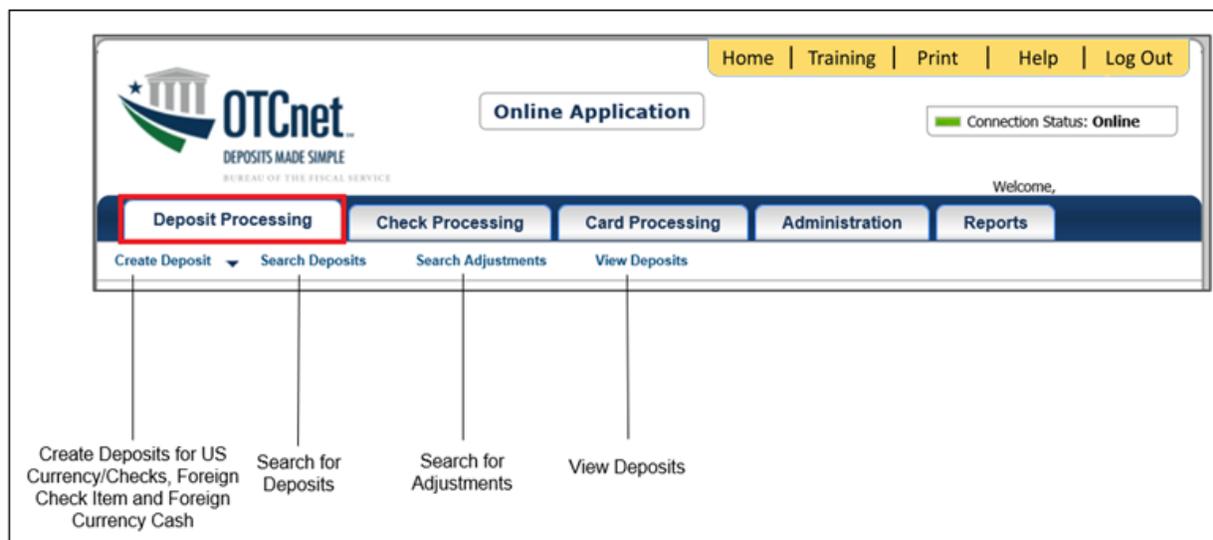
OTCnet Online Check Processing Tab Functionality

To access the OTCnet Check Processing functionality, log in with your **PIV/CAC** or **ID.me** credentials. Table 3 provides a list of the Check Processing functions that are available to you.

Table 3. Check Processing Tab Descriptions

Function	Description
Manage Verification	Allows a user to search and/or create an MVD record.
CIRA Query	Allows a user to view and/or modify a CIRA record.
Batch Management	Allows a user to search, view, close, approve and submit a batch. A user may edit and void an item within a batch with the proper permission.
Check Scan	Allows a user to scan checks.

The Check Processing tab is shown in Figure 12. Depending on your user role, you may not see all functionality shown in the image.

Figure 12. Check Processing Tab
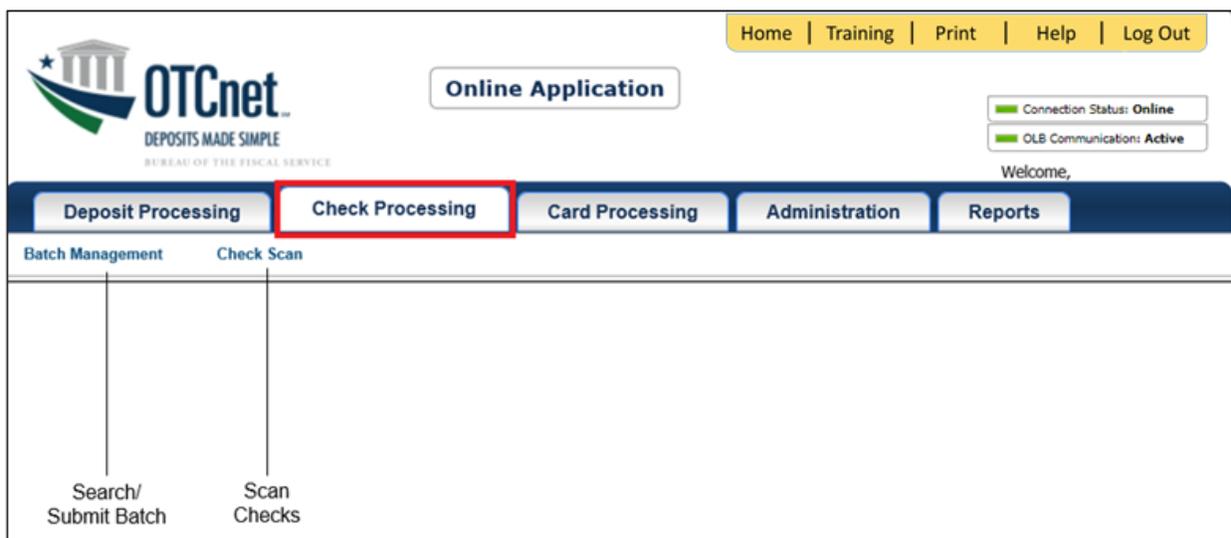
OTCnet Online Card Processing Tab Functionality

To access the OTCnet card processing functionality, log in with your **PIV/CAC** or **ID.me** credentials. Table 4 provides a list of the card processing functions that are available to you.

Table 4. Card Processing Tab Descriptions

Function	Description
Card Transaction Query	Allows a user to query a card transaction.
Process Card Payment	Allows a user to process a card payment.

The Card Processing tab is shown in Figure 13. Depending on your user role, you may not see all functionality shown in the image.

Figure 13. Card Processing Tab
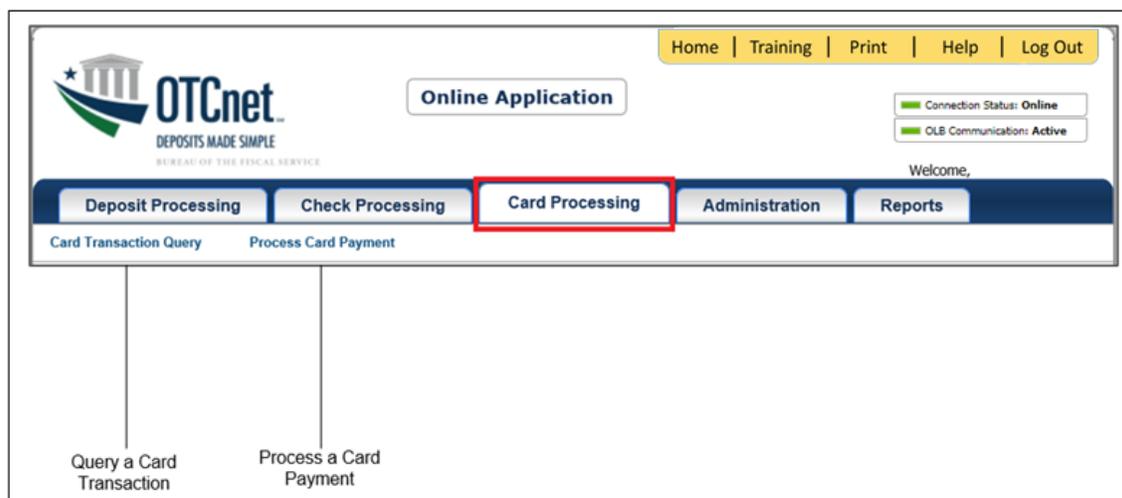
OTCnet Online Administration Tab Functionality

To access the OTCnet Administration functionality, log in with your **PIV/CAC** or **ID.me** credentials. Table 5 provides a list of the Administration functions that are available to you.

Table 5. Administration Tab Descriptions

Function	Description
Manage Organizations	Allows a user to manage Organization Hierarchy, Accounting Codes, Custom Labels, Processing Options, and User Defined Fields.
Manage FI	Allows a user to create and/or modify a Financial Institution, transfer FI RTN Numbers, transfer CA$HLINK accounts, and maintain FRB CA$HLINK accounts.
Manage Users	Allows a user to manage OTCnet user accounts and profiles.
Management	Allows a user to manage OTCnet processes.
Manage Check Processing	Allows a user to manage terminal configuration and forms.
Manage Card Processing	Allows a user to manage terminal configuration.
Manage Centralized Deployment	Allows users access to the following: Release Configuration, Edit Release and Download Release.
Audit	Allows a user to review the audit log history.
Utilities	Allows a user to review batch utilities, including Batch Recreate and Batch Repair.

The Administration tab is shown in Figure 14. Depending on your user role, you may not see all functionality shown in the image.

Figure 14. Administration Tab

OTCnet Online Reports Tab Functionality

To access the OTCnet Reports functionality, log in with your **PIV/CAC** or **ID.me** credentials. Table 6 provides a list of the Reports functions that are available to you. Depending on your user role, you are only authorized to view and download certain reports.

Table 6. Reports Tab Descriptions

Function	Description
Deposit Processing Reports	Allows a user to view and download Business, Security and Administration reports.
Check Processing Reports	Allows a user to access Check Processing reports.
Scheduled Reports	Allows a user to query and download scheduled reports.

The Reports tab is shown in Figure 15. Depending on your user role, you may not see all functionality shown in the image.

Figure 15. Manage Reports

Administration

Summary

In this chapter, you learned how to:

- Start and stop the OTCnet Local Bridge (OLB) application

- Request access for yourself in SailPoint IIQ

- Log in to OTCnet Online

- Navigate the OTCnet Online home page

Chapter 3. Managing User Accounts

OTCnet Participant User Guide

Table of Contents

List of Figures

Glossary

Select this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Managing User Accounts*. In this chapter, you will learn how to:

- Manage user accounts
- Create an identity for a user in SailPoint IIQ
- Add or remove user access in SailPoint IIQ
- Approve or deny user access requests in SailPoint IIQ
- Import a user identity to OTCnet
- Add or remove an endpoint/role for an OTCnet user
- Approve or reject an endpoint/role (or the removal of an endpoint/role) in OTCnet

Topics

The topics in this chapter include the following:

1. The Purpose of Managing User Accounts
2. Creating an Identity for a User in SailPoint IIQ
3. Adding or Removing User Access in SailPoint IIQ
4. Approving or Denying User Access Requests in SailPoint IIQ
5. Importing a User Identity to OTCnet
6. Adding or Removing an Endpoint/Role for an OTCnet User
7. Approving or Rejecting an Endpoint/Role (or the Removal of an Endpoint/Role) in OTCnet

Audience

The intended audience for the Managing User Accounts Participant User Guide includes:

- Primary Local Security Administrator (PLSA)
- Local Security Administrator (LSA)

Topic 1 The Purpose of Managing User Accounts

As the **Primary Local Security Administrator (PLSA)** or **Local Security Administrator (LSA)** for your organization, you are authorized to manage the users who have access to OTCnet. Before a user can access OTCnet, they must have an identity and account created in SailPoint IIQ.

The **PLSAs**/**LSAs** assist with creating an identity for a user and/or requesting a High-Level Organization (HLO) or role access for them in SailPoint IIQ. This is the preferred method of registration for users in SailPoint IIQ, while the self-registration functionality is available to users as needed.

Managing a user's account involves (in order):

- Registering users by creating an identity for a user in SailPoint IIQ

- Adding or removing user access in SailPoint IIQ

- Approving or denying user access requests in SailPoint IIQ

- Importing a user identity to OTCnet

- Adding or removing an endpoint/role for a user in OTCnet

- Approving or rejecting an endpoint/role (or the removal of an endpoint/role) for a user in OTCnet

The **User Provisioning** workflow includes the following high-level action steps:

1. The **PLSA** or **LSA** receives an authorized/approved request to add a new user (from their organization) to OTCnet.

2. The **PLSA** or **LSA** logs in to SailPoint IIQ, selects **Manage User Access**, and searches for the **email address** of the new user from the request in step 1.

   a. If the email address is <u>not found</u>, the **PLSA** or **LSA** selects **Manage Identity** and **Create Identity** from the menu options. They enter the authorized user's email address and select **Submit**.

   b. If the email address <u>is found</u>, the **PLSA** or **LSA** continues with step 3.

3. The **PLSA** or **LSA** adds the authorized **role**/**HLO** or **role**/**Financial Institution** (**FI**) combinations to the identity.

4. Another **PLSA** or **LSA** approves (or denies) the request in SailPoint.

5. The **PLSA** or **LSA** imports the **email address** of a new user to OTCnet so that the user can be added to the OTCnet database. Then the **PLSA** or **LSA** assigns the authorized **endpoint(s)** and **role(s)** to the user.

6. Another **PLSA** or **LSA** approves (or rejects) the request in OTCnet. Then the user is informed that their OTCnet provisioning is complete.

Topic 2 Creating a User Identity in SailPoint IIQ

SailPoint IIQ is an identity management solution utilized by the Department of the Treasury. It is being phased in through the Common Approach to Identity Assurance project, commonly referred to as CAIA.

Create a User Identity in SailPoint IIQ

The **PLSAs** and **LSAs** assist with creating an identity for a user and/or requesting an **HLO** or **role** access for them in SailPoint IIQ. **This is the preferred method for registering users and requesting HLO and role access for users in SailPoint IIQ**.

To create a user identity, select **Create Identity** from the menu at the top left of the SailPoint IIQ application under **Manage Identity.** Then enter their **email address** and select the **Submit** button.

Two notification emails will be sent out once an identity is created:

- One to the new identity holder, and

- One to the person who created the identity.

New users, not registered in SailPoint IIQ, will not be able to access OTCnet. Their identity will not be recognized. They may get a message that the email and/or password they entered is incorrect.

Create a User Identity in SailPoint IIQ

To create a user identity, complete the following steps:

1. At the top left of the SailPoint IIQ application, select the **Hamburger Menu** to display the available menu options.

2. Select the **Manage Identity** option, then select **Create Identity** as shown in Figure 1.

Figure 1: Creating Identity in SailPoint IIQ
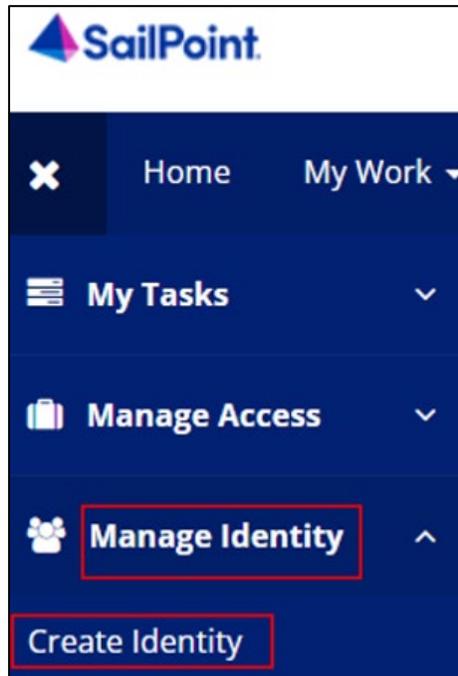
3. SailPoint IIQ will route to the **Create Identity** screen as shown in Figure 2.

💡 **Application Tip**

- There will be two fields available to fill out, **Identity Name** and **Email**.

- The **Identity Name** will be prepopulated as it is a unique identifier required by SailPoint IIQ.

4. Enter an **email address** for the identity you want to create and select **Submit** at the bottom of the page.

Figure 2: Create Identity Screen

Create Identity
If you would like to request that a new identity be created, please fill in the fields below. Fields marked with an asterisk are required.

CAIA Create Identity

Identity Name *

d83c99f2-146d-4a09-989b-2c0d7c93b1a0

Email *

lastname123@gmail.com

Cancel   Submit

💡 **Application Tip**

SailPoint IIQ will notify you if an identity with the email you provided already exists.

5. Once submitted, SailPoint IIQ will display the home page with a success message as shown in Figure 3.

Figure 3: Create Identity Request Submitted

SailPoint

Home   My Work ▾

Create identity request submitted
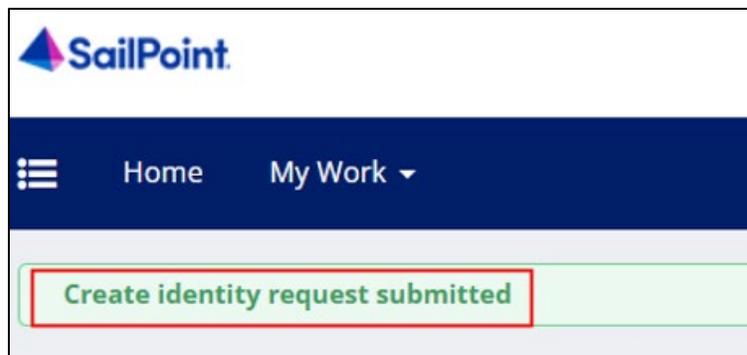
Application Tip

- Due to system design, it may take up to a minute for the identity to be processed in SailPoint IIQ.

- Two notification emails will be sent out once an identity is created, one to the new identity holder and one to the person who created the identity.

Administration

Topic 3 Adding or Removing User Access in SailPoint IIQ

There are two system administrator groups inside SailPoint IIQ, requestors and approvers.

- Requestors can request (or add access) on behalf of someone else. They can also remove user access.

- Approvers can approve or deny those requests. The application approvers will receive notification that there is an access request available to review.

After a **PLSA** or **LSA** requests access for a user, the application looks for other approvers for the organizational **HLO or role** selection and notifies them of the pending request.

In SailPoint IIQ, approvers are determined based on the HLO selections (approvers are security administrators with the same HLO assignments).

Add User Access in SailPoint IIQ

To request/add OTCnet user access, select **Manage Access** from the main menu, then select **Manage User Access.** Search for the user by typing their **email address** and selecting the **Search** button. Then select the **checkmark** to the left of the user's email address in the returned search result and select **Next.**

Make sure that **Add Access** is selected. In the search field, enter the **HLO or role** name to be assigned to the user. To select the **HLO or role** in the search results, select the **checkmark** to the left of the **HLO or role** name, then select **Next.** Review the requested role(s) and select the **Submit** button.

Add User Access in SailPoint IIQ

To request/add OTCnet user access, complete the following steps:

1. At the top left of left of the application, select the **Hamburger Menu** to display the options.
2. Select the **Manage Access** option, then select **Manage User Access** as shown in Figure 4.

Figure 4: Manage Access/Manage User Access
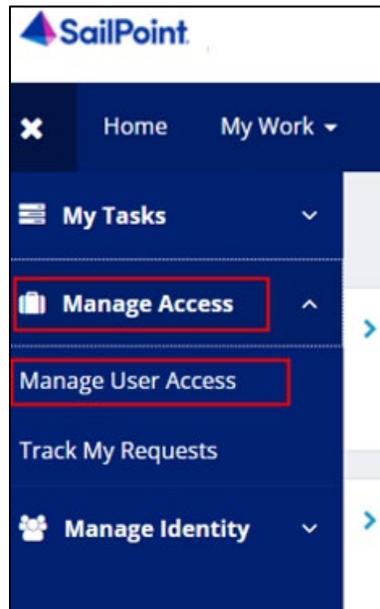
3. Search for the user (recipient of the access) by typing their **email address** and selecting the **Search** button (blue magnifying glass) as shown in Figure 5.
4. Select the **checkmark** to the left of the user's **email address** in the returned search result, then select **Next** at the bottom of the page.

Figure 5: Select Users Screen
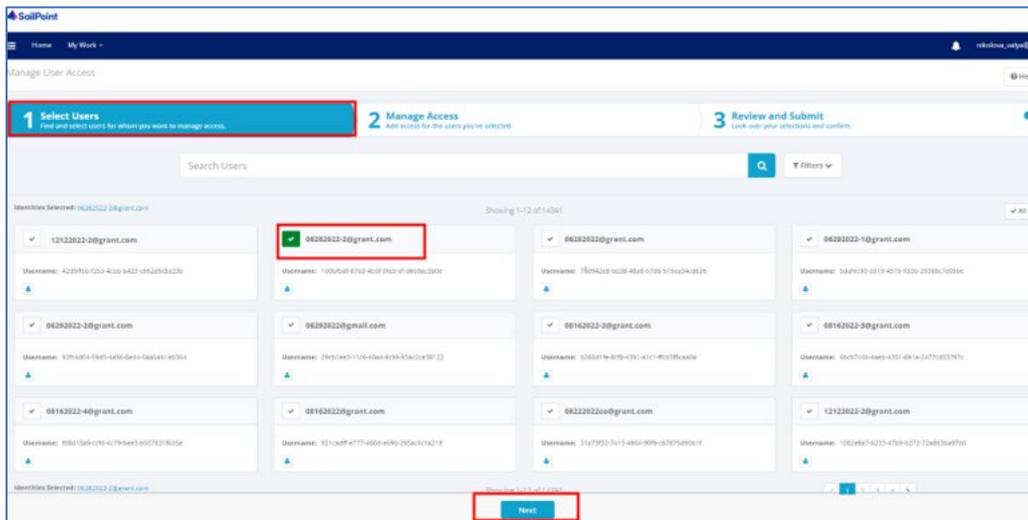
5. Select **Add Access** as shown in Figure 6. In the search field, enter part or all of the **HLO or role** name to be assigned to the user. For example, enter "customer."

🔆 **Application Tip**

If you are unsure of the **HLO or role** name, simply select the **Magnifying Glass** button to return all roles that you as a requestor are authorized to provision to users.

---

6. Select an **HLO or role** by selecting the **checkmark** to the left of the **HLO or role** name. Select **Next** at the bottom of the page.

Figure 6: Manage Access/Add Access Screen

9
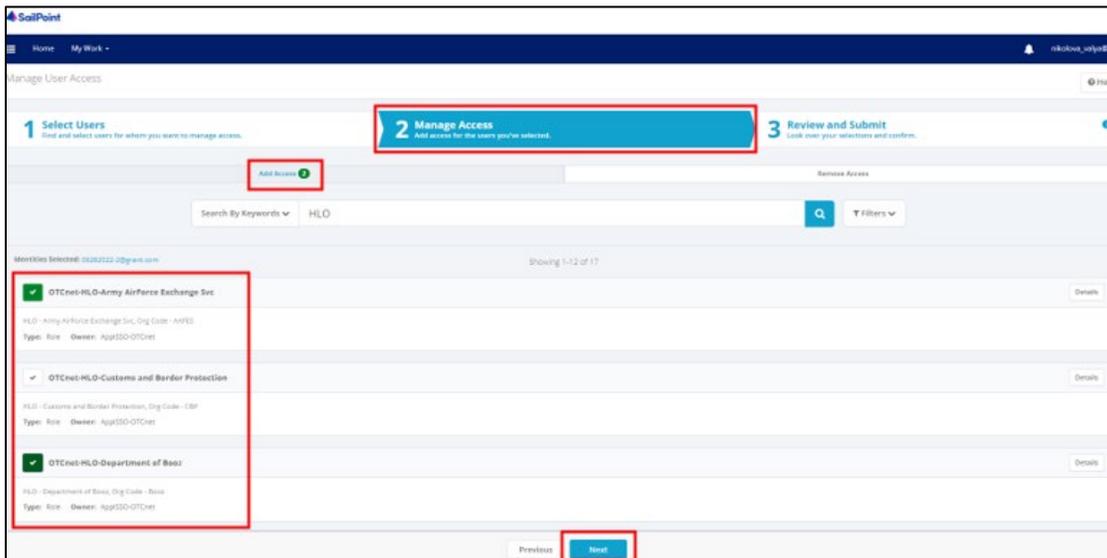
> **Application Tip**
>
> Multiple **HLOs or roles** can be selected.

7. Review the requested **HLOs or role(s)** as shown in Figure 7. Select the **voice bubble** on the right side to add any comments on the **HLO or role**, as needed. Then select the **Submit** button when finished.

Figure 7: Review and Submit Add Access Screen

8. A confirmation message will appear. You will also receive an **email** confirmation. The request is now pending approval.

Remove User Access in SailPoint IIQ

To remove user's access, select **Manage Access** from the main menu, then select **Manage User Access.** Search for the user by typing their **email address** and selecting the **Search** button. Then select the **checkmark** to the left of the user's **email address** in the returned search result and select **Next.**

Make sure **Remove Access** is selected and then select the **Magnifying Glass** Icon to the right of the text box to return all currently assigned **HLOs or roles** for the selected user. If everything is correct, select the **Submit** button to confirm the changes. If the information is incorrect, select the **Previous** button to modify the removal.

Remove User Access in SailPoint IIQ

To remove OTCnet user access, complete the following steps:

1. At the top left of the application, select the **Hamburger Menu** to display the options.

2. Select the **Manage Access** option, then select **Manage User Access.**

3. Search for the user by typing their **email address** and selecting the **Search** button (blue magnifying glass) as shown in Figure 8.

4. Select the **checkmark** to the left of the user's **email address** in the returned search result, then select **Next** at the bottom of the page.

Figure 8: Search Users Screen
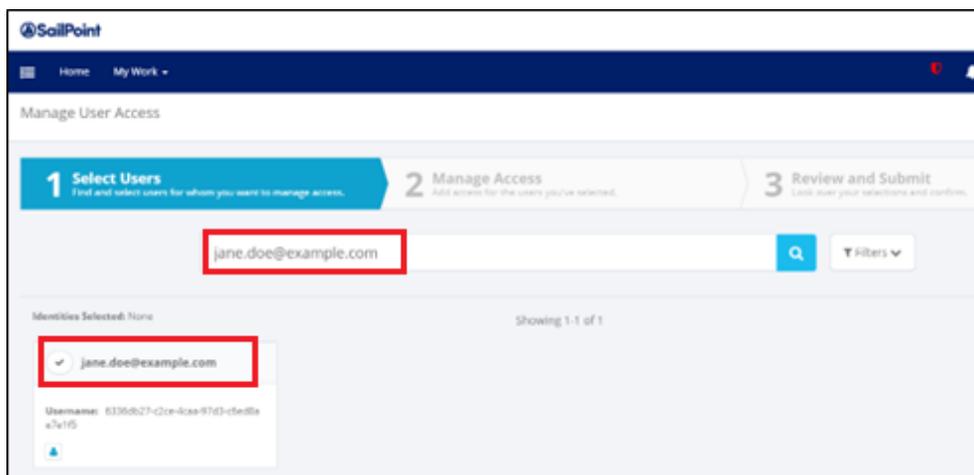
5. Select **Remove Access** as shown in Figure 9. Then select the **Magnifying Glass** icon to the right of the text box to return all currently assigned **HLOs or roles** for the selected user. Select **Next**.

Figure 9: Remove User Access Screen
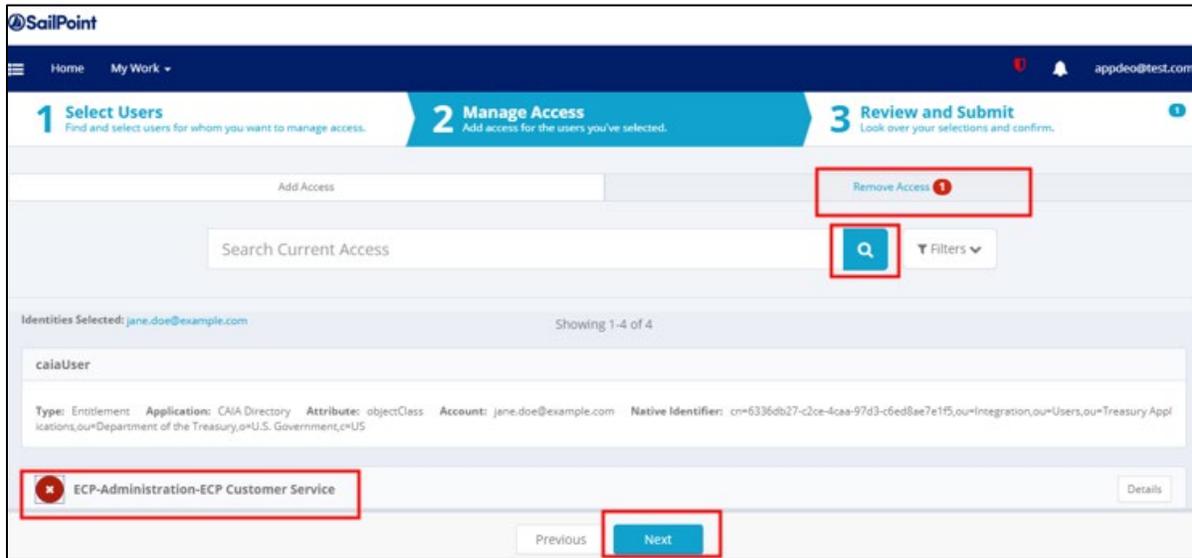
💡 **Application Tip**

The requestor will only be able to remove **HLOs or roles** that they are authorized to manage.

6. Review the information to confirm the removal as shown in Figure 10. You may add any comments using the **voice bubble** on the right side. Then select the **Submit** button to confirm the changes.

Figure 10: Review and Submit Remove Access Screen

13
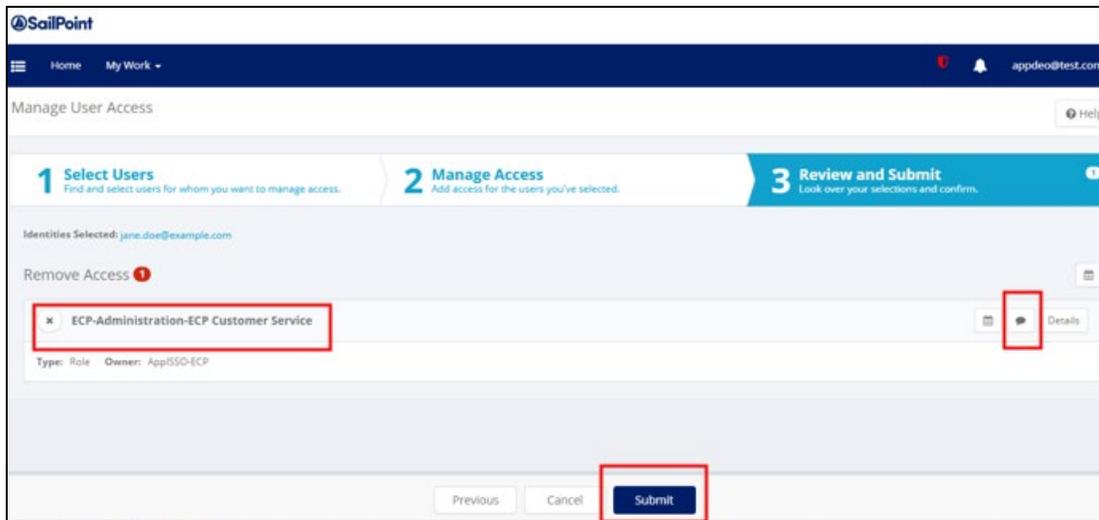
Application Tip

If the information is incorrect, select the **Previous** button to modify the removal.

Topic 4 Approving or Denying User Access Requests in SailPoint IIQ

A **PLSA** or **LSA** assigns **HLOs or roles** to a user; approvers of these requests are determined based on the **HLO** org selections. They are security administrators with the same HLO assignments. An approver logs in to SailPoint IIQ and approves (or denies) the request(s).

Most actions within SailPoint IIQ will require at least one level of approval.

Approve or Deny User Access Requests in SailPoint IIQ

To approve or deny user access requests, first notice a **red number notification** next to the **Bell** icon in the upper right-hand corner of the main SailPoint IIQ dashboard. Select the **Approvals** (or **Notifications**) box or the **Approvals** option under the **Bell** icon.

On the right side of the screen containing the details about the request, you will have the option to approve or deny the request. Select **Approve** or **Deny** and you will see a confirmation pop-up window.

Approve or Deny User Access Requests in SailPoint IIQ

To approve or deny user access requests, complete the following steps:

1. Notice a **red number notification** next to the **Bell** icon in the upper right-hand corner of the main SailPoint IIQ dashboard as shown in Figure 11.

   Application Tip

   You may also receive an email notification about the approval request.

2. Select the **Approvals** (or **Notifications**) box, or the **Approvals** option under the **Bell** icon on the home page.

Figure 11: Approval Awaiting the Approver's Action Screen
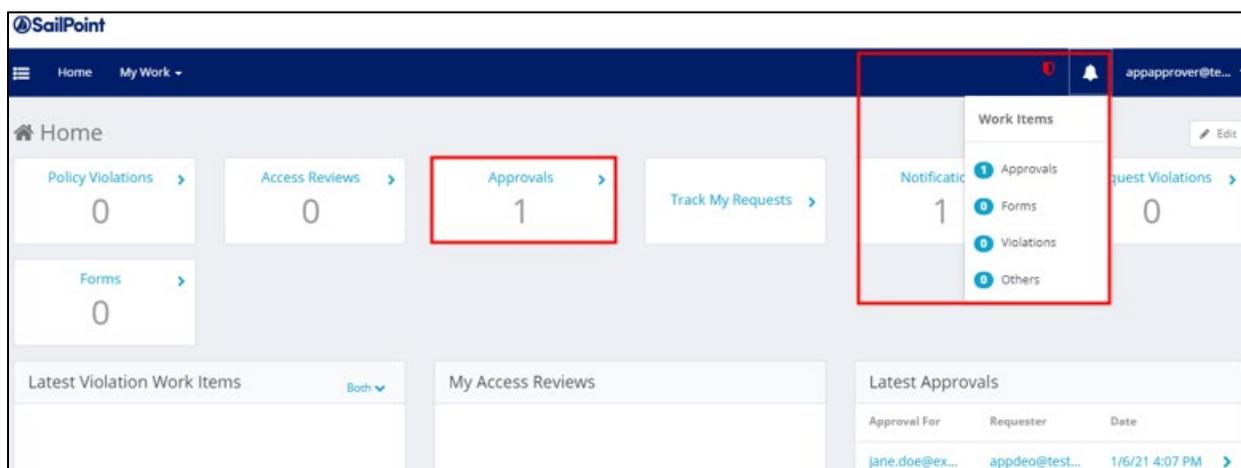
3. You will be redirected to a screen containing the details about the request as shown in Figure 12.

4. Add any comments using the **voice bubble** on the right side of the screen. Then select the **Approve** or **Deny** button. A confirmation pop-up window will appear.

Figure 12: Approve or Deny Screen
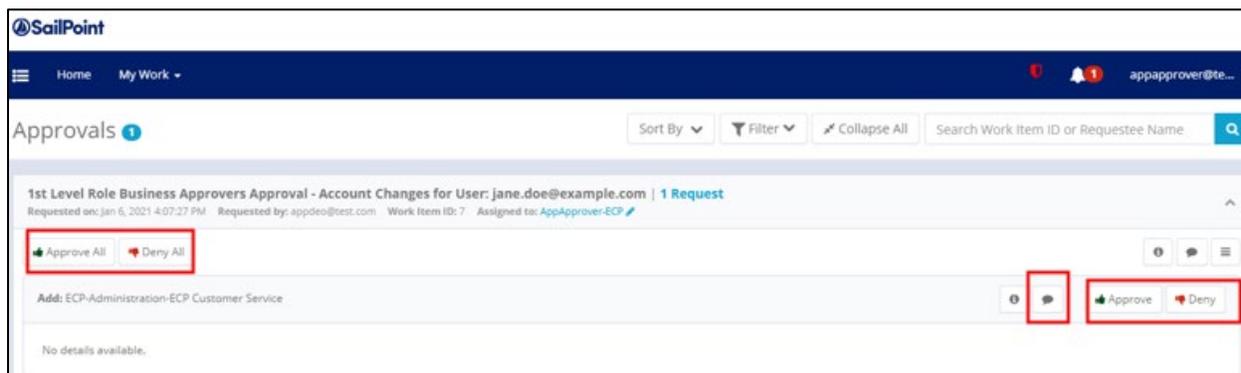
Application Tip

You may select the **Approve All** or **Deny All** button on the left if you want to approve or deny multiple requests.

Application Tip

If the first-level approver denies the request, any additional levels of approval will not occur.

Administration

Topic 5 Importing User Identity to OTCnet

Security administrators (PLSAs and LSAs) will import the **email address** of a new user to OTCnet so that the user can be added to the OTCnet database without having to wait for the user to log in.

Import User Identity to OTCnet

PLSAs/LSAs can import the user identity to OTCnet:

- After creating an identity for a user and requesting user access for them in SailPoint, and

- After the user access request is approved by another PLSA/LSA.

Then the PLSA or LSA will add the authorized endpoint(s) and role(s) to the user in OTCnet.

To import a user identity to OTCnet: from the **OTCnet Home page**>**Administration**>**Manage Users,** select the **Import OTCnet User Identity** tab. On the **Import OTCnet User Identity** page, enter one or more **email addresses** (separated by a space, comma, semicolon, or a new line) of the user whose identity will be imported. Select the **Import User** button.

A confirmation page displays, alerting you that the user identity has been imported and/or if there are errors. Select the **OK** button on the confirmation page to return to the OTCnet home page or the **Fix Errors and Reimport** button to navigate back to the Import OTCnet User Identity page to fix the errors.

Import User Identity to OTCnet

To import an OTCnet user identity to OTCnet, complete the following steps:

1. From the **OTCnet Home page**>**Administration**>**Manage Users,** select the **Import OTCnet User Identity** tab as shown in Figure 13.

Figure 13: Import OTCnet User Identity
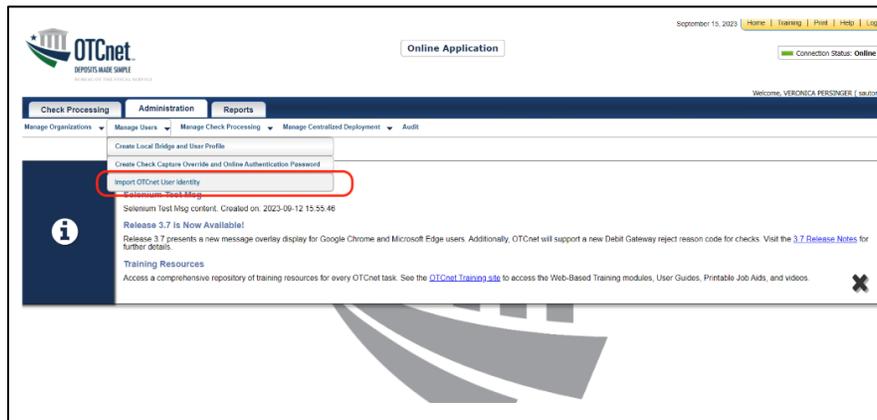
2. On the **Import OTCnet User Identity** page, enter one or more **email addresses** (separated by a space, comma, semicolon, or a new line) of the user whose identity will be imported.
3. Select the **Import User** button as shown in Figure 14.

Figure 14: Enter User's Email Address to Import User

Application Tips

- Please only use this module for importing emails for **NEW** users. **Do NOT** use this screen to update an email for an existing user.

- If you select the **Import User** button without entering an email address, an error message will display, notifying you that at least one email address should be entered.

- When you select the **Cancel** button, you will be returned to the home page.

4. A confirmation page displays, alerting you that the user identity has been imported and/or if there are errors as shown in Figure 15.

5. Select the **OK** button on the confirmation page to return to the OTCnet home page or the **Fix Errors and Reimport** button to navigate back to the Import OTCnet User Identity page to fix the errors.

Figure 15: Import User Identity Confirmation Screen

Application Tips

Error messages may include:

- The email address already exists in the OTCnet database.

- The email address has an invalid format. Ensure all email addresses are properly formatted and separated by a space, comma, semicolon, or a new line.

- The email address is greater than 128 characters and cannot be imported.

Ensure that you enter the **correct email address** for the user. If you import an incorrect email address, another entry in the database will be created and the user will not be able to access the application.

Application Tip

- OTCnet automatically recognizes when an existing user logs in with a **new email address**. The database is updated to reflect the user's new email address, preventing them from receiving a blank screen upon login.

- As a reminder, PLSAs and LSAs are responsible for **updating the user email** associated with the user's identity in **SailPoint** and verifying that the user is assigned the correct roles and endpoints associated with their **new email address** in SailPoint.

Topic 6 Adding or Removing an Endpoint/Role for an OTCnet User

There are two types of user provisioning access requests in OTCnet:

- Adding an endpoint/role

- Removing an endpoint/role

In OTCnet, **PLSA/LSA** users log in to select specific **endpoint(s)/role(s)** for fine-grained access under the HLO(s) and role(s) selected and approved in SailPoint IIQ for a user.

Add an Endpoint/Role for an OTCnet User

To add an **endpoint/role** for an OTCnet user, select the **Search User Directory** button from the **OTCnet Home page>Administration>Manage Users>Manage OTCnet Users** screen. In the search field, type the user **email address.** Then under **Manage User Account**, select **View Account**.

From the **Manage User Account** screen, select the **Add Endpoint/Role** button. From the **Add Endpoint/Role** screen, select a **role** from the **Choose a Role** dropdown. Then select the associated **level(s)** from the dropdown options. There can be many levels to select depending on the HLO/endpoint hierarchy. Finally, select the **Submit** button to submit your request. Review the confirmation page that appears and select the **OK** button to return to the **Manage OTCnet Users** home screen.

Add an Endpoint/Role for an OTCnet User

To add an **endpoint/role** for an OTCnet user, complete the following steps:

1. From the **OTCnet Home page**>**Administration**>**Manage Users**>**Manage OTCnet Users** screen, select the **Search User Directory** button.

2. In the search field, type the user's **email address.**

3. Under **Manage User Account**, select **View Account** for the desired user as shown in Figure 16.

Figure 16: Search User Directory Screen

4. The **Manage User Account** screen displays as shown in Figure 17.

5. Review the read-only information, including the current endpoint/role assignments listed for the user. Select the **Add Endpoint/Role** button.

Figure 17: Manage User Account Screen

6. The **Add Endpoint/Role** screen displays as show in Figure 18.

7. Select a **role** from the **Choose a Role** dropdown, choosing from the options provisioned for the specific OTCnet user.

8. Then select the associated **level(s)** from the dropdown options (each one is based on the previous selection and may be prepopulated). There can be many levels to select depending on the HLO/endpoint hierarchy.

9. As needed, use the **Add Role** button to select additional roles. Once you select a role, it will be added to the *Selected Role at Endpoint* field as illustrated in Figure 18.

Application Tips

- You can select up to **10 roles** per request. After 10 role additions, the **Add Role** button is disabled. To add additional roles, you must repeat the process by submitting a new request.

- If a user changes their **email address**, security administrators should verify that the user is assigned the correct roles and endpoints associated with their **new email address** through the **Manage OTCnet Users** module.

Figure 18: Add Endpoint/Role Screen

10. Once you have selected all necessary roles, select the **Submit** button to submit your request.

11. The confirmation page appears as shown in Figure 19.

12. Select the **OK** button to return to the **Manage OTCnet Users** screen.

Figure 19: Confirmation Screen on Adding Endpoint/Role Request Submitted

---

Application Tip

You will be notified via email when the request is approved or rejected by another PLSA/LSA.

Application Tip

- Ensure that users log in to OTCnet **at least once every 120 days** (or four months). After the four-month period of inactivity, the user's OTCnet entitlements will be systematically removed from their **SailPoint** identity.

   o To restore their account, users must contact the **Customer Support Team** to begin the process.

   o Customer Support will reach out to **PLSAs** and **LSAs** and require permission to restore the user's account.

   o **PLSA/LSAs** must confirm all the previously assigned roles that were associated with the user's identity before they can be added back.

Remove an Endpoint/Role for an OTCnet User

To remove an endpoint/role for an OTCnet user, select the **Search User Directory** button from the **OTCnet Home page>Administration>Manage Users>Manage OTCnet Users** screen. In the search field, type the user's **email address.** Then under **Manage User Account**, select **View Account**.

From the **Manage User Account** screen, select the **Remove Endpoint/Role** button. From the **Select an Endpoint and Role to Remove** screen, select the **Delete** checkbox next to the specific **Assigned Endpoint** or **Assigned Role at Endpoint** item. Then select the **Submit** button to submit your request. Review the confirmation page that appears and select the **OK** button to return to the **Manage OTCnet Users** home screen.

Remove an Endpoint/Role for an OTCnet User

To remove an endpoint/role for an OTCnet user, complete the following steps:

1. From the **OTCnet Home page**>**Administration**>**Manage Users**>**Manage OTCnet Users** screen, select the **Search User Directory** button.

2. From the **Search User Directory** screen, type the user's **email address** in the search field.

3. Under **Manage User Account**, select **View Account**.

4. The **Manage User Account** screen displays as shown in Figure 20. Review the read-only information, including the current endpoint/role assignments listed for the user.

5. Select the **Remove Endpoint/Role** button.

Figure 20: Manage User Account Screen

6. The **Select an Endpoint and Role to Remove** screen displays as show in Figure 21.

7. Select the **Delete** checkbox next to the specific **Assigned Endpoint** or **Assigned Role at Endpoint** item.

> 💡 **Application Tip**
>
> You can select multiple **checkboxes** to remove multiple assigned endpoints/roles.

8. Then select the **Submit** button to submit your request.

Figure 21: Select an Endpoint and Role to Remove Screen

9. The confirmation page appears as shown in Figure 22.

10. Select the **OK** button to return to the **Manage OTCnet Users** screen.

Figure 22: Confirmation Screen on Removing Endpoint/Role Request Submitted

 Application Tips

- You will be notified via email when the request is approved or rejected by another PLSA/LSA.

- When a role is successfully removed it is logged in the **Audit log**.

Topic 7 Approving or Rejecting an Endpoint/Role (or the Removal of an Endpoint/Role)

In OTCnet, approvers are determined based on the **endpoint** selections.

- An access request is sent to all **PLSAs** and **LSAs** at the same level or above the selected endpoints within the same hierarchy.

- An approver logs in and approves (or rejects) the submitted request.

As a **PLSA** or **LSA** you are authorized to approve or reject an endpoint/role (or to remove an endpoint/role) for an OTCnet user. You can approve or reject a request *after* another **PLSA** or **LSA** within the same OTC endpoint or hierarchy generates the request (adds or removes an endpoint/role for a user in OTCnet).

After the request is approved, the user to whom the OTCnet request applies receives an email notification containing information about the approval of the request. If you reject the request, the **PLSA** or **LSA** who created the request receives a notification of the rejection.

For **new users** who have not logged in to OTCnet yet, both the **User Name** and **User ID** values will be empty in the database and displayed as blank values on the screen.

Approve or Reject an Endpoint/Role (or the Removal of an Endpoint/Role)

To approve or reject an endpoint/role, log in to OTCnet and select **Administration>Manage Users>Manage OTCnet Users** from the home page**.** You will notice your **Pending Requests** list. Select the **View Details** link to view a specific request. Review the read-only information and enter any approval or rejection comments in the **Approver Comments** field. Select the **Approve** or **Reject** button. Review the read-only information on the confirmation page and select **OK** to return to the **Manage OTCnet Users** page.

To approve or reject a **removal** of an endpoint/role, follow the same process and steps as for approving or rejecting an endpoint/role request, starting with selecting the **View Details** link from the **Manage OTCnet Users** page for a **Remove Endpoint/Role** type of request.

Approve or Reject an Endpoint/Role (or the Removal of an Endpoint/Role)

To approve an endpoint/role for an OTCnet user, complete the following steps:

1. Log in to OTCnet and from the **Administration** tab**,** select **Manage Users,** and then **Manage OTCnet Users**.

2. From the **Manage OTCnet Users** screen, notice the **Pending Requests** list (**Your To-Do list**) as shown in Figure 23.

Application Tips

- You will receive an email notification regarding a new user provisioning request awaiting review when a provisioning request is made and added to your **pending requests list**, to alert you when a user needs your verification.

- For each request, notice the **Request Type**, **Time Due**, and **Requestee.**

- Notice two request types, for **Access Approval** and **Remove Endpoint/Role**. Each selection will take you to the appropriate workflow for access approval or access removal, respectively.

3. Select the **View Details** link for a specific **access approval** request.

Figure 23: Manage OTCnet Users Screen

4. The **Access Approval Request** screen displays as shown in Figure 24.

5. Review the read-only information and enter any approval or rejection comments in the **Approver Comments** field.

 Application Tips

- If you reject the request, you **must** provide comments in the specified field. Otherwise, you will get an error message and will not be able to continue until you provide comments.

- You can enter a **maximum** amount of 4000 characters.

6. Select the **Approve** or **Reject** button.

Figure 24: Access Approval Request Screen

 Application Tip

- Selecting **Cancel** will cancel the approval process.

- If you select **Reject**, you will get a notification: "Are you sure if you want to reject this request?" Select **Reject** or **Cancel**.

7. A confirmation page about the approval/rejection of the access request will display as shown in Figure 25.

8. Review the read-only information and select **OK** to return to the **Manage OTCnet Users** page.

Figure 25: Confirmation Screen on Approval/Rejection of the Access Request

Application Tip

Requestors will be notified via email when a request is approved or rejected.

Application Tip

- To approve or reject a **removal** of an endpoint/role, follow the same process and steps as for approving or rejecting an endpoint/role request.

- Start with selecting the **View Details** link from the **Manage OTCnet Users** page for a **Remove Endpoint/Role** request.

Summary

In this chapter, you learned how to:

- Manage user accounts

- Create an identity for a user in SailPoint IIQ

- Add or remove user access in SailPoint IIQ

- Approve or deny user access requests in SailPoint IIQ

- Import a user identity to OTCnet

- Add or remove an endpoint/role for an OTCnet user

- Approve or reject an endpoint/role (or the removal of an endpoint/role) in OTCnet

Chapter 4. Managing Your Agency's Hierarchy, Accounting Codes and Processing Options

OTCnet Participant User Guide

Table of Contents

List of Figures

Glossary

Select this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Managing Your Agency's Hierarchy*. In this chapter, you will learn:

- The purpose of organizational hierarchy
- How to add lower-level endpoints to the highest level of an organization hierarchy
- How to add additional lower-level endpoints or a financial institution relationship to a hierarchy that was previously defined
- How to make changes to OTC endpoints
- How to delete or neutralize OTC endpoints
- How to view OTC endpoints
- How to modify accounting codes
- How to modify endpoint mappings
- How to modify processing options

Topics

The topics in this chapter include the following:

1. The Purpose of the Organizational Hierarchy
2. Creating an Organizational Hierarchy
3. Managing the Organizational Hierarchy
4. Managing Accounting Codes
5. Managing Processing Options

Audience

The intended audience for the *Managing Your Agency's Hierarchy Participant User Guide* varies by system:

Deposit Processing

- Accounting Specialist
- Local Accounting Specialist
- Viewer (Views the organization's hierarchy endpoint only)

Check Capture and Check Processing

- Check Capture Administrator
- Check Capture Supervisor

- Check Capture Lead Operator

Card Processing

- Card Administrator
- Card Operator (Views the organization's hierarchy endpoint only)

Topic 1 The Purpose of the Organizational Hierarchy

As your Agency's **Accounting Specialist** (**AS**), **Local Accounting Specialist** (**LAS**), **Check Capture Administrator** (**CCA**), **Check Capture Supervisor (CCS)** and **Card Administrator (CA)** you are responsible for identifying and maintaining the organizational structure for your Agency's deposits, check capture, and card processing settings. This organizational structure is called a hierarchy.

Creating a hierarchy accomplishes the following:

- Describes the relationships and reporting structures between **OTC Endpoints** (i.e., locations) within your organization that process check transactions, create deposits, submit deposits or process card transactions, in OTCnet.

- Defines the content of the reports that individuals may run based on their **OTC Endpoints** within the hierarchy.

- Enables staff to process check transactions, create deposits, submit deposits, process card transactions and pull reports on all appropriate **OTC Endpoints** within the organization.

Work with your management to determine your desired hierarchy. Use the OTCnet tools provided in this document to define your OTCnet hierarchy. The organizational hierarchy you create allows for the following:

- **Deposit Preparers** may create deposits from specific **OTC Endpoints**
- **Check Capture Operators** may scan checks
- **Card Operators** may process credit card, debit card and gift card payments

You are responsible for indicating which hierarchy locations are **OTC Endpoints**, and how deposits at **OTC Endpoints** should be handled. The following describes the label that appears next to the endpoint and the endpoint types in OTCnet.

- **TGA** – denotes a **Deposit Processing** endpoint
- **CHK** – denotes a **Check Capture** endpoint
- **CDC** – denotes a **Card Processing** endpoint
- **M** – denotes a **Mapped Accounting Code**

Topic 2 Creating an Organizational Hierarchy

Once your **High-Level Agency Support (HLAS)** has entered your organization into OTCnet, you are responsible for entering your organizational hierarchy. As part of your setup process, the **HLAS** creates the highest level of your hierarchy for you; you add to that hierarchy according to your organization's needs.

The highest level of your organization cannot be a depositing endpoint. You may create multiple lower levels in your hierarchy, as needed, with multiple **OTC Endpoints** in each level.

You may edit your hierarchy as desired by updating the information for each **OTC Endpoint** you create. You may delete an **OTC Endpoint** from which no deposit, check transaction or card transaction has been made. You may not delete an **OTC Endpoint** once a deposit, check or card transaction has been made from that **OTC Endpoint**.

OTC Endpoints may not be deleted after a deposit, check or card transaction has been made because historical information about that deposit or check transaction would also be deleted, creating inaccurate reporting. However, you may neutralize an OTC Endpoint, if deposits or check transactions have been created. Card Processing Endpoints can also be neutralized.

Your organization's hierarchy is accessible by selecting **Administration** and the **Manage Organization** menu option.

Create an OTC Endpoint

The **Accounting Specialist**, **Local Accounting Specialist**, **Check Capture Administrator**, **Check Capture Supervisor** and **Card Administrators** can add endpoints.

To add an OTC Endpoint from the highest level of an organizational hierarchy, select your organization's OTC Endpoint and check the **Add lower levels to this OTC Endpoint** checkbox.

Information on **Short Name** and **Description** includes:

- The **Short Name** and **Description** fields provide an abbreviation and a full description, respectively, of the **OTC Endpoint** you are adding.

- **Short names** are user-defined text describing an organization. Short names must be unique within an organization hierarchy (e.g., Short Name: IRS; Description: Internal Revenue Service).

- Special characters are accepted in **Short Name** and **Description** fields; however, only use standard American Standard Code for Information Interchange (ASCII) characters. The standard ASCII range is 32-126. If non-standard ASCII characters (0-31, 127-255) are entered in the **Short Name** and **Description** fields, you cannot manage OTC Endpoints (select endpoints) in OTCnet Online. Instead, an error message appears suggesting you contact Customer Support.

Create an OTC Endpoint

To add an OTC Endpoint from the highest organization hierarchy, complete the following steps:

1. From the **Administration** tab, select **Manage Organization**>**Organization Hierarchy**>**Modify**. The *Step 1 of 3: Select an OTC Endpoint* page appears.

2. Select your OTC Endpoint from the list. The *Step 2 of 3: Update OTC Endpoint Information* page appears. View details for **Add lower levels to this OTC Endpoint** checkbox as shown in Figure 1.

3. Check the **Add lower levels to this OTC Endpoint** checkbox.

4. Enter the lower-level OTC Endpoint's **Short Name** and **Description** and select **Next**.

Application Tip

- In the table that appears, add new **OTC Endpoints** that fall in the level under the current **OTC Endpoint**.
- **Short names** are user-defined text describing an organization. Short names must be unique within an organization hierarchy (e.g., Short Name: IRS; Description: Internal Revenue Service).

Figure 1. Step 2 of 3: Update OTC Endpoint Information

5. In the *Step 3 of 3: Review OTC Endpoint(s)* page, review and verify the OTC Endpoint details and select **Submit**. A *Confirmation* page appears presenting the modified OTC Endpoint (and verifies the added lower-level OTC Endpoint).

Additional Buttons

- Select **Add More Lines** to add additional lower levels to this endpoint.
- Select **Cancel** to return to the OTCnet Home Page. No data is saved.
- Select **Previous** to return to the previous page.
- Select **Return Home** to return to the OTCnet Home Page.

Topic 3. Managing the Organizational Hierarchy

Once **Accounting Specialists**, **Local Accounting Specialists**, **Check Capture Administrators**, **Check Capture Supervisors** and **Card Administrators** have performed the initial setup of your organizational hierarchy, you can add to it and adjust it to suit your needs by performing the following tasks:

- Adding a lower level to an existing OTC Endpoint

- Modifying OTC Endpoint information

- Deleting an OTC Endpoint

- Viewing an OTC Endpoint

Before a user is provisioned to a deposit-processing OTC Endpoint (**TGA**), ensure the **Allow OTC Endpoint to create deposits for over-the-counter collections** checkbox is checked. Before a user is provisioned to a check capture OTC Endpoint (**CHK**), ensure the **Enable Check Capture** checkbox is checked. Before a user is provisioned to a card-processing OTC Endpoint (**CDC**), ensure the **Enable Card Processing** checkbox is checked.

Required fields for **Enable Card Processing** include **Chain Code**, **Division**, **ALC**, **Merchant ID**, **Address**, **Signature Capture** and **Return Policy**.

If the **Allow OTC Endpoint to create deposits for over-the-counter collections** checkbox, the **Enable Check Capture** checkbox and **Enable Card Processing** checkboxes are not checked when modifying OTC Endpoint information, you cannot provision the user to the appropriate OTCnet Endpoint.

Add a Lower Level to an Existing OTC Endpoint

Accounting Specialists, **Local Accounting Specialists**, **Check Capture Administrators**, **Check Capture Supervisors** and **Card Administrators** can add as many levels to your Agency hierarchy as needed, each with as many required OTC Endpoints.

To add a lower level to an existing OTC Endpoint, select your OTC Endpoint. Check the **Add lower levels to this OTC Endpoint** checkbox to add lower levels to the existing endpoint. Enter **Short Name** and **Description** fields for all **OTC Endpoints** in the next lower level. Verify the OTC Endpoint details are correct. Select **Submit**. A *Confirmation* page appears presenting the OTC Endpoint that has been modified (added). Verify that the OTC Endpoint details are correct.

Add a Lower Level to an OTC Endpoint

To add a lower level to an OTC Endpoint, complete the following steps:

1. From the **Administration** tab, select **Manage Organization**>**Organization Hierarchy**>**Modify**. The *Step 1 of 3: Select an OTC Endpoint* page appears.

2. Select an OTC Endpoint from the list that appears. The *Step 2 of 3: Update OTC Endpoint Information* page appears.

3. Check the **Add lower levels to this OTC Endpoint** checkbox to add lower levels to the existing endpoint as shown in Figure 2. **Short Name** and **Description** text boxes appear.

4. Enter a short name and description in the **Short Name** and **Description** fields for all the **OTC Endpoints** in the next lower level. When you have finished, select **Next**.

Figure 2. Step 2 of 3: Short Name and Description for OTC Endpoint Information

5. Verify that the OTC Endpoint details are correct and select **Submit**. A *Confirmation* page appears presenting the modified OTC Endpoint.

Additional Buttons

- Select **Add More Lines** to add additional lower levels to this endpoint.
- Select **Cancel** to return to the OTCnet Home Page. No data is saved.
- Select **Previous** to return to the previous page.
- Select **Return Home** to return to the OTCnet Home Page.

Modify OTC Endpoint Information

Accounting Specialists, **Local Accounting Specialists**, **Check Capture Administrators**, **Check Capture Supervisors** and **Card Administrators** are authorized to modify the **Short Name** or **Description** of an existing OTC Endpoint, enable the OTC Endpoint to create deposits (indicated with **TGA**), capture checks (indicated with **CHK**), process card transactions (indicated with Card Debit Card or **CDC**), or add a lower level to the OTC Endpoint.

Similarly, any **CDC** endpoint that is also a **TGA** and/or **CHK** endpoint, requires a card processing role with permission to modify an organization (e.g., **Card Administrator**).

To modify endpoint information settings for an OTC Endpoint with **TGA**, **CHK** and **CDC**, the user must have **Accounting Specialist**, **Check Capture Administrator**, **Check Capture Supervisor** and **Card Administrator** privileges.

Additional Information for modifying the OTC Endpoint information includes:

- Special characters are accepted in **Short Name** and **Description** fields; however, only use standard American Standard Code for Information Interchange (ASCII) characters. The standard ASCII range is 32-126. If non-standard ASCII characters (0-31, 127-255) are entered in the **Short Name** and **Description** fields, you cannot manage OTC Endpoints (select endpoints) in OTCnet Online. Instead, an error message appears suggesting that you contact Customer Support.

- The **Agency Assigned Suspensions - Days** allows you to specify the number of calendar days an individual is unable to cash a check or pay by check. It is calculated from the date the system is aware of the return file. The **Agency Assigned Suspensions - Occurrence** allows you to specify the suspension level.

- **Include Represented and Retired Check** or **Include Retired Check Only** allows you to specify whether the verification record is generated on Represented or Retired items. **Include Retired Check Only** allows you to specify whether the verification record is generated on only Retired items.

- **Include Expired** indicates whether previous suspensions that have since expired are counted when accessing the suspension level to assign when the individual writes a check. **Agency Verification Policies—Delete** allows you to remove the check cashing policy for your OTC Endpoint. Once the check cashing policy is removed for the OTC Endpoint, the higher-level organization's check cashing policy is automatically assigned to your OTC Endpoint.

- **Data Privacy** defines the extent to which users from other locations are able to view verification records. By default, **Account**, **User Defined Field 1**, **Bank Routing Number**, **Note** and **Mask PII** are checked as **Blocked**. If a checkbox is checked, it indicates that the OTC Endpoint information has been defined. For maximum data privacy, all fields would be marked as blocked, except for **Short Name**. However, there may be situations where it is acceptable for outside users to view certain fields in verification records.

- **Enable Card Processing** options are defined as the following:
    - A **Chain Code** is an alphanumeric designator (e.g., 0F123B) assigned by WorldPay to reflect unique channel of card processing. A Chain Code is required for initial setup with lower-level endpoints. Once the Chain Code is saved, it cannot be changed. An agency can have multiple Chain Codes, but no two agencies will have the same Chain Code.

- A **Division** is a three-digit value assigned at lower-level endpoints under the chain code to designate unique lines of accounting. The Division code for all OTC Endpoints is any value from 001 to 999.

- The **Agency Location Code (ALC)** is required for initial setup. Once the ALC is saved, it cannot be changed. If an endpoint adds card processing functionality to an existing TGA or CHK endpoint, the ALC will already be populated.

- The **Merchant ID** is a unique alphanumeric designator, received from CAS, that reflects the card processing location. An ALC is associated with multiple merchant IDs; however, each merchant ID must be unique for each lower-level endpoint. The Merchant ID field may contain up to 13 characters.

  Once the **Chain Code**, **Division**, **ALC**, and **Merchant ID** are saved, they will grey out and cannot be changed. If any of these details need to be changed, a new endpoint must be created, and the information will need to be added again.

- If the **Signature Capture** checkbox is checked, the customer's signature and the message "*I agree to pay the above total amount in accordance with the card issuer's agreement*" will appear on your agency's sales receipts. For refunds, the customer's signature and the message "*I agree that I have received a refund for the amount stated above*" will appear on your agency's refund receipts. By default, the **Signature Capture** checkbox is unchecked.

- **Return Policy** indicates the agency's return policy for card transactions. It is stored in the system and generated on receipts as mandated by the Treasury Financial Manual. The default return policy choice is **None**. Selecting **Return Policy** is optional and does not apply to all endpoints (e.g., a return policy is not required when the card user is not purchasing an item but only paying a fee or making a payment).

  Return Policy choices include:

  - NO REFUND, ALL SALES FINAL – For any agency that does not accept merchandise in return or exchange and does not issue refunds to cardholders.

  - EXCHANGE ONLY – For any agency that only accepts merchandise in immediate exchange for similar merchandise of a price equal to the amount of the original transaction.

  - IN-STORE CREDIT ONLY – For any agency that accepts returned merchandise and delivers to the cardholder an in-store credit equal to the value of the merchandise returned that may be used only in the agency's place(s) of business.

  - REFUNDS ONLY AVAILABLE WITHIN 30 DAYS OF SERVICE OR PURCHASE – For any agency that issues refunds to the original credit or debit card within 30 days of purchase or service.

  - Other – The agency is prompted to enter some descriptive text outlining their agency's return policy.

  - None – Select if a return policy does not apply to an agency.

- Prior to specifying Debit Gateway, confirmation must be received from the OTCnet Deployment Team to set up each applicable OTCnet Endpoint.

  - **No** indicates that the Debit Gateway setup is not complete, and the OTC Endpoint is not ready to perform check capturing activities.

- **Yes** indicates that the Debit Gateway setup is complete, and the OTC Endpoint is now ready to perform check capture activities. A notification message appears as a reminder to submit your Agency Site Profile (ASP) for all check capture endpoints. If the ASP is not submitted to the OTCnet Deployment Team, this can prevent transactions from processing. Select **OK**.

- By default, all agencies will have the **Close Batch** checkbox checked. To close the batch, the user must print the PDF report or export the batch list report.

  - If the **Close Batch** checkbox is unchecked, the user can close the batch without having to print the PDF report or export the batch list report.

- By default, all agencies will have the **Approve Batch** checkbox checked. In order to approve the batch, the user must print the PDF report or export the batch list report.

  - If the **Approve Batch** checkbox is unchecked, the user can approve the batch without having to print the PDF report or export the batch list report.

- If the user is closing or approving multiple batches online and the **Close Batch** or **Approve Batch** checkboxes are checked for any OTCnet endpoint, then the user must print the PDF reports or export the list reports. The batch is not closed or approved until **Confirm** is selected, which is enabled when the **Print PDF Report** or **Export** is selected.

  - If the user is closing and/or approving multiple batches online and the **Close Batch** or **Approve Batch** checkboxes are not checked for any OTCnet endpoint, then the user can close and/or approve multiple batches without printing the PDF reports or exporting the list reports. **Confirm** is enabled and the user can select to close and/or approve the multiple batches.

- If **Special Designation** is selected, a user is able to view which ALCs are CARS Reporters.

  - The CARS Reporter special designation information is read-only and displays for TGA and CHK endpoints. Only an HLAS can specify the **Special Designation** information.

  - **Yes** indicates that the OTC Endpoint is associated with an ALC that has been designated as a CARS Reporter. **No** indicates that the OTC Endpoint is not associated with an ALC that has been designated as a CARS Reporter. If an ALC is identified as a CARS Reporter, entering the Accounting Code information is mandatory. This will apply to all ALC+2 within the hierarchy of the ALC.

Modify OTC Endpoint Information

To modify an OTC Endpoint, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Organization Hierarchy**>**Modify**. The *Step 1 of 3: Select an OTC Endpoint* page appears.

> **Application Tip**
>
> To modify endpoint information settings for an OTC Endpoint with **TGA**, **CHK** and **CDC**, the user must have **Accounting Specialist**, **Check Capture Administrator** and **Card Administrator** privileges.

2. Select your OTC Endpoint from the list that appears. The *Step 2 of 3: Update OTC Endpoint Information* page appears as shown in Figure 3.

3. Update the OTC Endpoint Information.

   To update the **General** details of an OTC Endpoint, complete the following:

   • Enter the **Short Name** and **Description** for the OTC Endpoint.

Figure 3. Step 2 of 3: Update OTC Endpoint Information - Collapsed

13

Application Tip

A short name must be entered to identify the OTC Endpoint that is being updated. If an OTC Endpoint exists, the data displayed in the text is available for update.

To allow the OTC Endpoint to create deposits, complete the following:

- Select the **Allow OTC Endpoint to create deposits for over-the-counter collections** checkbox as shown in Figure 4.

Application Tip

Before a user is provisioned to a deposit-processing OTC Endpoint (**TGA**), ensure the **Allow OTC Endpoint to create deposits for over-the-counter collections** checkbox is checked.

- Update **Agency Location Code** by completing the following step:
  - Entering the **ALC**
- Update **Address** by completing the following step:
  - Entering the **address** details
- Update **Financial Institution Relationship(s)** by completing the following steps:
  - Selecting both the **Financial Institution** and the associated **Routing Transit Number (RTN)**
  - Entering the **Demand Deposit Account (DDA),** retyping the **DDA** and selecting **Add**.

Application Tip

To delete the Financial Institution relationship, select the **Delete** checkbox(es) under the **Delete** column.

14

Figure 4. Allow OTC Endpoint to create deposits for over-the-counter collections

To specify the check cashing policies of the OTC Endpoint, complete the following:

- Select the **Check Cashing Policies** checkbox as shown in Figure 5.

> 💡 **Application Tip**
>
> The **Default Reason Codes** allows you to specify the return reason codes relevant to your agency's program. These codes represent the numeric codes used in ACH and paper return processing, which specify the reason for the return of the transaction and Check 21 codes.

> 💡 **Application Tip**
>
> If checkbox is checked and grayed out, it indicates that this OTC Endpoint is either inheriting the policies from the parent organization or its own information has already been defined, and the user does not have the privilege to make modifications. Only a **CCA** has privileges to modify the check cashing policies.

- Add **Default Reason Codes** by completing the following steps:
    - Selecting a default reason code and selecting **Add**, optional. Repeat steps as necessary.
- Delete **Assigned Return Reason Code Filters** by completing the following steps:
    - Checking **Delete** box(es) under the **Delete** column, optional

> 💡 **Application Tip**
>
> The **Default Reason Codes** allow you to specify the return reason codes relevant to your agency's program. These codes represent the numeric codes used in ACH and paper return processing, which specify the reason for the return of the transaction and Check 21 codes.

Figure 5. Default Reason Codes
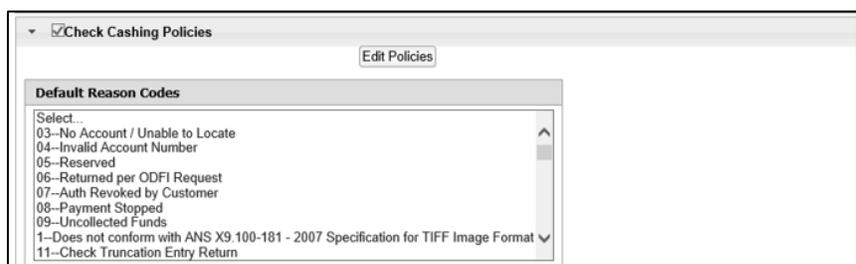
- Update **Agency Assigned Suspensions** by completing the following steps, *optional:*

    - Entering the number of **Days**

    - Entering the **Occurrence** number

    - Selecting the **Agency Assigned Suspensions** you want to **Delete** by checking the boxes under the **Delete** column, *if applicable*

Application Tip

- To update the **Agency Assigned Suspensions**, select the applicable **Default Reason Code** in the box provided.
- The **Agency Assigned Suspensions - Days** allows you to specify the number of calendar days than an individual is unable to cash a check or pay by check and is calculated from the date the system is aware of the return file. The **Agency Assigned Suspensions - Occurrence** allows you to specify the suspension level.

- Update **Agency Verification Policy** by completing the following steps, *optional:*

    - Selecting **Include Represented and Retired Check or Include Retired Check Only**

    - Checking **Include Expired**

    - Entering the number of **Expired Days**

    - Checking **Agency Verification Policies**—**Delete**

Application Tip

- **Include Represented and Retired Check** or **Include Retired Check Only** allows you to specify whether the verification record is generated on Represented or Retired items. **Include Retired Check Only** allows you to specify whether the verification record is generated on only Retired items.
- **Include Expired** indicates whether previous suspensions that have since expired are counted when accessing the suspension level to assign when the individual writes a check. **Agency Verification Policies—Delete** allows you to remove the check cashing policy for your OTC Endpoint. Once the check cashing policy is removed for the OTC Endpoint, the higher-level organization's check cashing policy is automatically assigned to your OTC Endpoint.

To specify the data privacy of the OTC Endpoint, complete the following:

- Select the **Data Privacy** checkbox.
- Update **Data Privacy**:
  - Select the **Data Privacy – Agency Available Attributes** you want to block or unblock by checking the boxes under the **Blocked** column.

Application Tip

By default, **Account**, **User Defined Field 1**, **Bank Routing Number**, **Note** and **Mask PII** are checked as **Blocked.**

To enable the OTC Endpoint to capture checks, complete the following:

- Select the **Enable Check Capture** checkbox.
- Update **Enable Check Capture** by entering the **Agency Location Code (ALC+2)**.

Application Tip

- Before a user is provisioned to a check capture OTC Endpoint (CHK), ensure the **Enable Check Capture** checkbox is checked.
- If checkbox is checked, it indicates that the OTC Endpoint information has been defined.
- The ALC+2 is required for initial setup. Once the ALC+2 is entered it cannot be updated.

- Update **OTC Verification Group** by completing the following steps as shown in Figure 6:
  - Entering the **Short Name** (Starting With) and selecting **Search**
  - Selecting **Yes** or **No** for **Queue Interface**

▪ Selecting the **OTC Endpoint** you want to add by checking the box under the **Assign** column and selecting **Add Agency Group**

Figure 6. Enable Check Capture

> **Application Tips**
>
> - By default, the OTC Endpoint **Short Name** displays. Add additional OTC Endpoints to the OTC Verification Group by selecting the **Clear** button to clear the **Short Name** and entering a Short Name, selecting **Search** and selecting **Add Agency Group**.
> - Designating an **OTC Verification Group** allows for verification data to be shared among non-related OTC Endpoints. For example, **Lower Level 1** and **Lower Level 2** are siblings under the high-level organization, Training Team Top Level. Since there is no parent-child relationship between these two OTC Endpoints, users from one OTC Endpoint are isolated from the other's verification data. By adding both unrelated locations to an **OTC Verification Group**, they are able to share information.
> - The **Queue Interface** is used by military agencies that utilize the Deployable Disbursing System (DDS) database bridge.

- Under **OTC Verification Group, Current Agency Site**,

  - Select the **OTC Endpoint** you want to delete by checking the box under the **Delete** column.

To enable the **OTC Endpoint** to process card payments, complete the following steps:

- Select the **Enable Card Processing** checkbox

> **Application Tip**
>
> Before a user is provisioned to a card processing OTC Endpoint (**CDC**), ensure the **Enable Card Processing** checkbox is checked.

- Update **Enable Card Processing** by completing the following steps as show in Figure 7:

  - Entering the **Chain Code**
  - Entering the **Division**
  - Entering the **ALC**
  - Entering the **Merchant ID**

- Update the **Address** by entering the address details

- Designate the Signature Capture by completing the following steps:

  - Checking the **Signature Capture** check box, *optional*

- Select a **Return Policy** by completing the following steps:

  - Selecting the appropriate card transaction policy radio button for your organization, *optional*

Figure 7. Enable Card Processing Address, Signature Capture and Return Policy

To add lower-level endpoints, complete the following:

- Select the Add lower levels to this OTC Endpoint checkbox.

- Update **Add lower levels to this OTC Endpoint** by completing the following steps:
    - Entering the **Short Name** and **Description**.
    - Selecting **Add More Lines** to add additional lower levels to this OTC Endpoint.

Application Tip

A short name must be entered to identify the OTC Endpoint that is being updated. If an OTC Endpoint exists, the data displayed in the text is available for update.

To specify the advanced administration, complete the following:

- Select **Advanced Administration**

- Specify **Advanced Administration** by completing the following:
    - Selecting **Yes** or **No** for **Debit Gateway**
    - Viewing or specifying the **Forms Rendered Solution**
    - Viewing the **Report Only Summary Level Data to CIR**
    - Viewing the **Summary Level Classification**

Application Tip

By default, all forms are set to be rendered and viewed in HTML. Under general circumstances, the ActiveX option does not need to be specified. The **Forms Rendered Solution** is read-only and only an HLAS can specify the option to switch between viewing and accessing forms in HTML or ActiveX.

Application Tips

- The **Report Only Summary Level Data to CIR** Information is read-only and only an HLAS can specify the information.
- A checked box indicates that detailed-level data will not be transmitted to Collections Information Repository (CIR) and only summary data is reported to CIR for all the check transactions that are processed under this OTC Endpoint (CHK) or ALC+2. This is mainly for the OTC Endpoints that are used to process tax data. An unchecked box indicates that detailed-level data is transmitted to CIR.
- The **Summary Level Classification** is read-only and only a **High-Level Agency Support (HLAS)**, **Check Capture Supervisor**, and **Check Lead Operator** can specify the information.
- A checked box indicates that Check Capture Lead Operators and Check Capture Operators cannot classify individual checks. Instead, the classification of the batch will occur after all the checks have been scanned. An unchecked box indicates the Check Capture Operator will have to classify checks at the item level.

- Specify **Batch List Print/Export Required During** options by completing the following:
  - Checking or unchecking the **Close Batch** checkbox
  - Checking or unchecking the **Approve Batch** checkbox
- View or **Specify Agency Comments**

Administration

Figure 8. Advanced Administration

Application Tips

- A Check Capture Lead Operator, Check Capture Supervisor, and HLAS can add, edit, or remove **Agency Comments**. A Check Capture Administrator, Check Capture Operator, Agency Manager, and CIRA Viewer can view **Agency Comments**.
- The **Specify Agency Comments** field allows agencies to add, edit, or remove Agency comments that are sent to CIR as part of the check transmission.

To view the special designation, complete the following:

- Select **Special Designation** as shown in Figure 9.

Figure 9. Special Designation

Application Tips

- The CARS Reporter special designation information is read-only and displays for **TGA** and **CHK** endpoints. Only an HLAS can specify the **Special Designation** information.
- **Yes** indicates that the OTC Endpoint *is* associated with an ALC that has been designated as a CARS Reporter. **No** indicates that the OTC Endpoint *is not* associated with an ALC that has been designated as a CARS Reporter.

---

4. Select **Next**. The *Step 3 of 3: Review OTC Endpoint* page appears.

5. Verify the information is correct and select **Submit**. Select **Edit**, to modify the information entered and return to Step 4.

> **Additional Buttons**

- Select **Previous** to return to the previous page.
- Select **Cancel** to return to the OTCnet Home Page. No data is saved.
- Select **Return Home** to return to the OTCnet Home Page.

Delete or Neutralize an OTC Endpoint

Accounting Specialists, Local Accounting Specialists, Check Capture Administrators, **Check Capture Supervisors** and **Card Administrators** are authorized to neutralize an **OTC Endpoint** or delete an **OTC Endpoint.**

Consider the following information on *deleting* an OTC Endpoint:

- You can delete an **OTC Endpoint** if no deposits or check transactions have been made to that endpoint.

- Deleting the **OTC Endpoint** deletes all information associated with the **OTC Endpoint**. This includes deleting deposit information that impacts the reports you run in OTCnet.

- Before deleting an **OTC Endpoint**, all user accounts must be removed from the OTCnet Deposit Processing Endpoint and OTCnet Check Processing Endpoint.

- The Agency Form Data must be removed. To remove the Agency Form Data, contact Customer Support at fiscalservice.otcchannel@citi.com.

Consider the following information on *neutralizing* an OTC Endpoint:

- You can neutralize an **OTC Endpoint** when deposits or check transactions have been created for that endpoint.

- Once the OTCnet Endpoint is neutralized, deposits or check transactions can no longer be created from that endpoint. The information from previously created deposits or check transactions can be accessed from OTCnet reporting.

- All user accounts must be removed from the OTCnet Deposit Processing Endpoint and OTCnet Check Processing Endpoint.

- The Agency Form Data must be removed. To remove the Agency Form Data, contact Customer Support at fiscalservice.otcchannel@citi.com.

Delete or Neutralize an OTC Endpoint

To delete or neutralize an OTC Endpoint, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Organization Hierarchy**>**Delete**. The *Step 1 of 2: Select the OTC Endpoint(s)* page appears.

2. Select the OTC Endpoints you would like to **Delete** and select **Next** as shown in Figure 10**.**

    Or

    Select the OTC Endpoints you would like to **Neutralize** and select **Next**.

Figure 10. Step 1 of 2: Select the OTC Endpoint(s)

3. The *Step 2 of 2: Review OTC Endpoint(s)* page appears. Verify that the correct endpoint is marked for deletion or neutralization and select **Submit**.

4. A *Confirmation* page appears confirming the deletion or neutralization.

Additional Button

Select **Return Home** to return to the OTCnet Home Page.

View an OTC Endpoint

Accounting Specialists, **Local Accounting Specialists**, **Check Capture Administrators**, **Check Capture Supervisors**, **Check Capture Lead Operators**, **Card Administrators** and **Card Operators** are authorized to view an OTC Endpoint.

When the *View OTC Endpoint* page appears, you can verify the following information for the OTC Endpoint:

- **General** information including **Short Name**, **Description**, **ALC** and whether the endpoint is for **check capture**, **deposit processing** or **card processing**

- **Address** including **Address** details

- **Financial Institution Relationships and Active Financial Institution Relationships** including **Financial Institution** and **RTN**

- **Check Cashing Policies** including **Assigned Return Reason Code Filters**

- **Agency Assigned Suspensions** including **Days** and **Occurrence**

- **Agency Verification Policies** including **Include Retired Check Only**, **Include Expired, Expired Days** and **Agency Verification Policies**—**Delete**

- **Data Privacy**—**Agency Available Attributes** including **Attribute Name (Short Name, Account, Mask PII, Bank Routing Number, User Defined Field 1 and Note)** and whether it is **Blocked**

- **Check Capture** including the **ALC+2** and **Queue Interface**

- **OTC Verification Current Agency Site Lower Level I** including the **Short Name, Description** and **ALC+2** and whether it should be **Deleted**

- **Card Processing** including the **Chain Code, Division** and **Merchant ID**

- **Lower Levels** including the **Short Name** and **Description**

- **Advanced Administration** including **Debit Gateway**, **Forms Rendered Solution**, **Report Only Summary Data to CIR**, **Summary Level Classification**, **Batch List Report Print/Export Required at Close Batch, Batch List Report Print/Export Required at Approve Batch** and **Specify Agency Comments**

- **Special Designation** including **GWA Reporter ALC** and **Non-appropriated Funds ALC**

View an OTC Endpoint

To view an OTC Endpoint, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Organization Hierarchy**>**View**. The *View Organization* page appears.

2. Select the OTC Endpoint you would like to view. The *View OTC Endpoint* page appears as shown in Figure 11.

Figure 11. View OTC Endpoint

Additional Buttons

- Select **Previous** to return to the previous page.
- Select **Return Home** to return to the OTCnet Home Page.

Search for an OTC Endpoint

Accounting Specialists, **Local Accounting Specialists**, **Check Capture Administrators**, Check **Capture Supervisors**, **Check Capture Lead Operators**, **Card Administrators** and **Card Operators** can search for an OTC Endpoint.

When the *View OTC Endpoint* page appears, you can verify the following information for the OTC Endpoint:

- **General** information including **Short Name**, **Description**, **ALC** and whether the endpoint is for **check capture**, **deposit processing** or **card processing**

- **Address**

- **Financial Institution Relationships and Active Financial Institution Relationships** including **Financial Institution** and **RTN**

- **Check Cashing Policies** including **Assigned Return Reason Code Filters**

- **Agency Assigned Suspensions** including **Days** and **Occurrence**

- **Agency Verification Policies** including **Include Retired Check Only**, **Include Expired, Expired Days** and **Agency Verification Policies**—**Delete**

- **Data Privacy**—**Agency Available Attributes** including **Attribute Name (Short Name, Account, Mask PII, Bank Routing Number, User Defined Field 1 and Note)** and whether it is **Blocked**

- **Check Capture** including the **ALC+2** and **Queue Interface**

- **OTC Verification Current Agency Site Lower Level I** including the **Short Name, Description** and **ALC+2** and whether it should be **Deleted**

- **Card Processing** including the **Chain Code, Division** and **Merchant ID**

- **Lower Levels** including the **Short Name** and **Description**

- **Advanced Administration** including **Debit Gateway**, **Forms Rendered Solution**, **Report Only Summary Data to CIR**, **Summary Level Classification**, **Batch List Report Print/Export Required at Close Batch, Batch List Report Print/Export Required at Approve Batch** and **Specify Agency Comments**

- **Special Designation** including **GWA Reporter ALC** and **Non-appropriated Funds ALC**

Search for an OTC Endpoint

To search for an OTC Endpoint, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Organization Hierarchy**>**Search**. The *View Organization* page appears.

2. Select the OTC Endpoint you would like to view. The *View OTC Endpoint* page appears as shown in Figure 12.

Figure 12. Step 2 of 2: View OTC Endpoint

Topic 4. Managing Accounting Codes

OTCnet provides enhanced check capture and deposit reporting functionalities to support the Central Accounting Reporting System (CARS). The CARS objectives include capturing classification information at the earliest possible time, streamlining central accounting and reporting, eliminating burdensome reconciliation, and providing timely Fund Balance with Treasury (FBWT) information to agencies.

OTCnet captures classification information for transactions (over-the-counter deposits) processed through the Deposit Reporting function and the Check Capture function to support the CARS requirement that all transactions capture standard classification information.

For OTCnet, standard classification information is accepted in the form of a Treasury Account Symbol (TAS) string or a Classification Key (C-Key), which is an internal Agency Accounting Code that is translated into a valid TAS.

OTCnet sends this C-Key information to CARS through the Collections Information Repository (CIR). CARS then communicates with the Shared Accounting Module (SAM) application to translate the C-Key into a valid TAS/BETC through the Cash Flow and Default Profiles that have been set up in SAM. Initially, classification of check transactions for non-CARS reporting agencies is optional.

To learn more about CARS, visit http://fms.treas.gov/CARS/index.html.

Modify Accounting Codes

The **Check Capture Administrator**, **Check Capture Supervisor** and **Accounting Specialist** are authorized to modify an accounting code. They can modify the classification code and description for an accounting code, indicate whether it's a Treasury Account Symbol (TAS) and add and delete accounting codes.

If an **Agency Accounting Code** label is customized, it is displayed as the label above the imported codes, according to the custom label that was defined for the highest-level organization. This applies to OTC Endpoints that use the deposit processing and/or check processing functionalities. The default accounting code label is **Agency Accounting Code**.

Modify Accounting Codes

To modify an existing accounting code, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Accounting Codes**>**Modify**. The *Step 1 of 3: Select OTC Endpoint* page appears.

2. Select the organization endpoint for the accounting codes you wish to modify. The *Step 2 of 3: Update Accounting Codes* page appears.

3. Under the **New Accounting Codes to be Added** table, enter the accounting code details, and select **Next**.

Application Tip

If an **Agency Accounting Code** label is customized, it is displayed as the label above the imported or modified codes within the Maintain Accounting Codes module, according to the custom label that was defined for the highest-level organization. Within the rest of the application, custom labels apply to deposit processing functionalities, but are not extended to check processing functionalities. The default accounting code label is **Agency Accounting Code**.

Update the details by completing the following:
  - Selecting the **TAS** checkbox to indicate that the accounting code is a Treasury Account Symbol (TAS), *if applicable*
  - Entering details in both the **Agency Accounting Code** and **Description** text boxes as shown in Figure 13
  - Checking the **Skip Selected** box to skip saving any of the imported accounting codes

Figure 13. Step 2 of 3: Update Accounting Codes

4. The *Step 3 of 3: Review Accounting Codes* page appears. Verify the information is correct and select **Submit**.

5. A *Confirmation* page appears presenting the imported accounting codes. Simultaneously, accounting codes flagged as TAS must be transmitted to the Shared Accounting Module (SAM) to confirm they are valid TAS strings.

Additional Button

Select **Return Home** to return to the OTCnet Home Page.

Import Accounting Codes

The **Check Capture Administrator (CCA)**, **Check Capture Supervisor (CCS)** and **Accounting Specialist (Acc Spec)** are authorized to import accounting codes.

To import an accounting code, the **CCA**, **CCS**, or **Acc Spec** has several options. From the *Import From File* page, they can select the type of accounting code (e.g., CSV File, Fixed File, XML File) they want to import into the system, browse to its location and Import. Next, they can review the accounting codes to be imported into the system and update as needed. Another option is to remove accounting codes before submitting them, by marking them for removal and updating the list of codes.

Details are updated by selecting the **TAS** checkbox to indicate the accounting code is a Treasury Account Symbol (TAS), *if applicable*, entering the details in both the **Agency Accounting Code** and **Description** text boxes and/or checking the **Skip Selected** box to skip saving the imported accounting codes.

Once the accounting codes are successfully imported and the *Confirmation* page appears, simultaneously, the accounting codes flagged as TAS must be transmitted to SAM to confirm that they are valid TAS strings.

Import Accounting Codes

To import an accounting code, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Accounting Codes**>**Import**. The *Step 1 of 4: Select OTC Endpoint* page appears.
2. Select the top-level organization endpoint for which you want to import accounting codes. The *Step 2 of 4: Import from File* page appears.
3. Select the type of accounting code to import into the system and browse to its location and select **Import**. The *Step 3 of 4: Select Accounting Codes* page appears.
4. Update the list of accounting codes that are imported into the system and select **Next** as shown in Figure 14.

Figure 14. Step 3 of 4: Select Accounting Codes

Update the details by completing the following steps:

- Selecting the **TAS** checkbox to indicate that the accounting code is a Treasury Account Symbol (TAS), *if applicable*

Application Tip

Download Treasury Account Symbols (TAS), for import from the Shared Account Module (SAM) site at: https://www.sam.fms.treas.gov/sampublic/tasbetc.htm.

- Entering the details in both the **Agency Accounting Code** and **Description** text boxes
- Checking the **Skip Selected** box to skip saving any of the imported accounting codes

5. The *Step 4 of 4: Review* page appears. Verify the information is correct and select **Submit**.
6. A *Confirmation* page appears showing that the accounting codes have been imported. Simultaneously, accounting codes flagged as TAS will need to be transmitted to the Shared Accounting Module (SAM) to confirm that they are valid TAS strings.

Additional Button

Select **Return Home** to return to the OTCnet Home Page.

Administration

View Accounting Codes

The **Accounting Specialist (Acc Spec)**, **Local Accounting Specialist (LAS)**, **Check Capture Administrator (CCA)**, and **Check Capture Supervisor (CCS)** are authorized to view the active accounting codes available for the organization hierarchy.

To view an accounting code, the **Acc Spec**, **LAS**, **CCA** or **CCS** selects the highest-level organization endpoint accounting code available to view.

If an Agency Accounting Code label is customized, it is displayed as the label above the imported codes, according to the custom label that was defined for the highest-level organization. This applies to OTC Endpoints that use the deposit processing and/or check processing functionalities. The default accounting code label is **Agency Accounting Code**.

View Accounting Codes

To view an accounting code, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Accounting Codes**>**View**. The *View Accounting Codes* page appears.
2. Select the highest-level organization endpoint accounting codes available to view. The *View Accounting Codes* page appears as shown in Figure 15.

Figure 15. View Accounting Codes

Application Tips

- Only active accounting codes available for deposit processing and check processing (if applicable) appear.
- Under the **Active Accounting Code** table, both **Treasury Account Symbols** (**TAS**) and accounting codes not identified as **TAS** display.
- If an accounting code is a **TAS**, a check mark displays under the **TAS** column, and the SAM validation status (**Valid**, **Invalid** or **In Process**) displays under the **Validation Status** column.

Additional Buttons

Select **Return Home** to return to the OTCnet Home Page.

Modify Endpoint Mappings

An endpoint mapping is the assignment of accounting codes to an agency's OTC Endpoint, to which a deposit amount is allocated.

The accounting codes that display on the page are the codes that:

- Meet your search criteria.

- Are not assigned to your OTC Endpoint.

If you do not enter search criteria, all the accounting codes defined for the highest-level organization appear.

Additional information for modifying Endpoint Mapping includes the following:

- If an agency has identified accounting codes as **TAS**, only **TAS** identified as **Valid** by **SAM** will be available for mapping to an OTC Endpoint.

- To remove mappings for an accounting code, check the **Remove** box(es) and select **Update**.

- A mapped accounting code is not eligible for removal if a batch is associated with a transaction within an active batch that is **Open**, **Closed**, or **Approved** or a deposit that is in **Draft** or **Awaiting Approval (AWAP)** status. An error message is displayed to a user if this scenario occurs.

Modify Endpoint Mappings

To map accounting codes to OTC Endpoints, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Accounting Codes**>**Modify OTC Endpoint Mappings**. The *Step 1 of 4: Select OTC Endpoint* page appears.

2. Select the OTC Endpoint for the accounting code endpoint mapping you would like to assign or remove. *The Step 2 of 4: View Assigned Accounting Codes page* appears.

Application Tip

If an Agency Accounting Code label is customized, it is displayed as the label above the imported or modified codes within the Maintain Accounting Codes module, according to the custom label that was defined for the highest-level organization. Within the rest of the application, custom labels apply to deposit processing functionalities but are not extended to check processing functionalities. The default accounting code label is **Agency Accounting Code**.

3. Select **Assign Mappings** to assign an accounting code to an OTCnet Endpoint. The *Step 2 of 4 Continued: Search and Assign Accounting Codes* page appears.

> Or

Select **Remove Mappings** to remove an accounting code from an OTCnet Endpoint. The *Step 3 of 4: Remove Accounting Codes* page appears.

4. Assign or remove an accounting code to or from an OTCnet Endpoint as shown in Figure 16.

> To **Assign Mappings** to an OTCnet Endpoint, complete the following:

> - Enter the **Accounting Code (Starting With)** search criteria, *optional*
> - Enter the **Description (Contains)** search criteria, *optional*
> - Select **Search**, *optional*
> - Check the **Assign** box(es) for the accounting codes you must assign
> - Select **Next** (Proceed to *Step 3 of 4: Assign Accounting Codes*)

> Or

> To **Remove Mappings** from an OTCnet Endpoint, complete the following:

> - Check the **Remove** box(es) for the accounting codes that you must remove
> - Select **Next** (Proceed to *Step 4 of 4: Review Accounting Codes from Endpoint*)

Figure 16. Step 2 of 4 Continued: Search and Assign Accounting Codes

Application Tip

If an Agency has identified accounting codes as a **Treasury Account Symbol** (**TAS**), only a TAS identified as **Valid** by **Shared Accounting Module** (**SAM**) is available for mapping to an OTC Endpoint.

5. The *Step 3 of 4: Assign Accounting Codes* page appears. Review and verify the accounting code(s) you would like to assign and select **Next**. (Proceed to *Step 4 of 4: Review Accounting Codes to Endpoint*)

Application Tips

- Check the **Remove** box(es) and select the **Update** button to delete the OTC Endpoint mapping for an accounting code.
- A mapped accounting code is not eligible for removal if a batch is associated with a transaction within an active batch that is **Open**, **Closed** or **Approved,** or a deposit that is in **Draft** or **Awaiting Approval** (**AWAP**) status. An error message is displayed to a user if this scenario occurs.

6. The *Step 4 of 4: Review Accounting Codes to Endpoint* page appears. Confirm the information is correct and select **Submit** to assign the accounting code(s) to the OTC Endpoint.

42

OR

The *Step 4 of 4: Review Accounting Codes to Endpoint* page appears. Confirm the information is correct and select **Submit** to remove the accounting code(s) to the OTC Endpoint.

7. A *Confirmation* page appears showing that the accounting codes have been assigned to or removed from the OTC Endpoint.

Additional Buttons

- Select Return Home to return to the OTCnet Home Page.
- Select Manage Additional to manage another accounting code.

Topic 5. Managing Processing Options

As part of managing your organization hierarchy, you need to define your deposit processing options. **Processing options** are parameters for the deposit and adjustments process. You must first define processing options at the highest level of the organization before defining lower-level options. For lower-level organizations, if you do not define these options, then the lower-level organizations will take on the options set for the next higher-level organization that does have the options set.

If you do not define processing options, your organization cannot create deposits or classify a batch at the summary level. You can define processing options at any level within your organization. You can also view the processing options by **OTC Endpoint** report to manage processing options in your organization.

As an **Accounting Specialist**, you are authorized to modify the following processing options for your organization's hierarchy:

- ***Accounting Classifications for Adjustments, Corrections, and Returned Items***: Identifies the default accounting codes to which you want adjusted amounts credited and debited. This also applies to credit and debit voucher ALC Account Switch Corrections, returned items, and batches classified at the summary level containing a failed item.

- ***Correspondence***: Provides the financial institution with address information for any correspondence, including returned item information

- ***Deposit Preparation***: Sets default settings for deposit preparation to save time for Deposit Preparers

- ***Transaction History***: Sets default settings for historical data about transactions

Modify Processing Options

The **Accounting Specialist** and **Local Accounting Specialist** are authorized to modify Deposit Processing options. The **Check Capture Supervisor** and **Check Capture Lead Operator** are authorized to modify Check Processing options.

The page displays accounting codes:

- That are not applied as a debit or credit adjustment to your OTC Endpoint

- That meet your search criteria

If you do not enter search criteria, all accounting codes defined for the highest-level organization appear.

Modify Processing Options

To modify a processing option, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Processing Options**>**Modify**. The *Step 1 of 3: Select Organization Endpoint* page appears.

💡 **Application Tips**

- Processing options must first be defined for the highest-level organization before any lower-level organization's processing options are defined.
- If the processing options are not defined for the highest-level organization, all lower-level organization links are disabled.

2. Select the OTC Endpoint for which you want to modify a processing option. The *Step 2 of 3: Define Processing Options* page appears.

3. Modify the processing option(s) and select **Next**.

   To modify **Accounting Classifications for Adjustments, Corrections, and Returned Items**, complete the following:

💡 **Application Tips**

- An accounting code is assigned to both a debit adjustment and credit adjustment.
- Accounting classifications for adjustments apply to **Accounting Specialists**, **Check Capture Supervisors** and **Check Capture Lead Operators**. Accounting classifications for corrections and returned items apply to **Check Capture Supervisors** and **Check Capture Lead Operators**.

   Update Default Accounting Codes by completing the following:
- Selecting either **Use parent's values** or **Use my values**
- Entering the search criteria for the accounting code you would like to view and select **Search** (magnifying glass)

💡 **Application Tip**

To narrow an accounting code search, enter a partial or full accounting code.

   Or

- Selecting **Search** (magnifying glass) to view accounting codes

Application Tip

- All accounting codes that meet your search criteria and are not applied as a debit or credit adjustment, correction or returned item to your OTC Endpoint are displayed on the page. If you do not enter search criteria, all the accounting codes defined for the highest-level organization appear.
- By default, the first ten accounting codes display, first by ascending special character order, then by numerical order and finally by ascending alphabetical order by accounting code.
- If the organization has more than ten accounting codes, select the pagination menu above the section containing the existing accounting codes to view additional pages of results. The system will only allow a user to view and apply active accounting codes not designated as TAS or those designated as TAS that have been validated by SAM.

- Selecting the accounting code to apply a credit and/or debit type and selecting **Assign to Debit** and/or **Assign to Credit**

Application Tip

- An accounting code is assigned to debit and credit adjustment, correction, and returned item types.
- After an accounting code is assigned to debit or credit adjustment, it appears in the Adjustment Type/Default Accounting Code table.

- Selecting **Yes** or **No** to allow changes by an organization lower in the hierarchy

Update **Default Accounting Code Usage** by completing the following steps:
- Selecting either **Use parent's values** or **Use my values**
- Selecting either **Always Use the Default for Deposit Adjustments** or **Default based upon Deposit Subtotals for Deposit Adjustments**
- Selecting **Yes** or **No** to allow changes by an organization lower in the hierarchy

To modify **Correspondence**, complete the following steps:
Update **Returned Items** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Entering the corresponding address information that you would like to be displayed to a financial institution when a return item adjustment is created
- Selecting **Yes** or **No** to allow changes by an organization lower in the hierarchy

Update **Deposit Adjustment** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Entering the corresponding address information that you would like to be displayed to a financial institution when a deposit adjustment is created
- Selecting **Yes** or **No** to allow changes by an organization lower in the hierarchy

To modify **Deposit Preparation**, complete the following steps:
Update **ITGA Deposit Creation** by:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** to allow an endpoint to create foreign deposits
  - If the endpoint accepts foreign deposits, enter the **Default foreign currency when creating deposits** details
- Selecting **Yes** or **No** to allow changes by an organization lower in the hierarchy

Update **Subtotals and Cash Count** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** for each of the following options:
  - Include subtotals for Checks/Money Orders and Cash
  - Include Currency count and subtotals by denomination
  - Include Coin count and subtotals by denomination
  - Allow changes by an organization lower in the hierarchy

Update **Accounting Code Subtotals** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** for each of the following options:
  - Allow negative accounting code subtotals
  - Allow changes by an organization lower in the hierarchy

Update **Separation of Duties** as shown in Figure 17 by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** for each of the following options:
  - Deposits must be prepared and approved by different employees
  - Allow changes by an organization lower in the hierarchy

Figure 17. Update Deposit Processing Options with Deposit Preparation expanded

To modify **Transaction History**, complete the following steps:
- Select **Use parent's values** or **Use my values**
- Enter the **Number of days displayed** in the text box, *if applicable*
- Select **Yes** or **No** to allow changes by an organization lower in the hierarchy

4. The *Step 3 of 3: Review the following processing options* page appears. Verify the information is correct and select **Submit**.

5. A *Confirmation* page appears, showing which processing options were applied to the organization.

Additional Buttons

- Select **Cancel** to return to the OTCnet Home Page. No data is saved.
- Select **Edit** to return to the previous page.
- Select **Next** to advance to the next page.
- Select **Previous** to return to the previous page.
- Select **Submit** to complete the process and display the Confirmation page.
- Select **Return Home** to return to the OTCnet Home Page.

View Processing Options

The **Accounting Specialist** and **Local Accounting Specialist** are authorized to view deposit processing options. The **Check Capture Supervisor** and **Check Capture Lead Operator** are authorized to view check processing options.

When the *View Processing Options* page appears, it presents the custom labels in effect for the organization hierarchy, including the following:

- **Accounting Classifications for Adjustments, Corrections, and Returned Items**
- **Correspondence**
- **Deposit Preparation**
- **Transaction History**

View Processing Options

To view a processing option, complete the following steps:

1. From the **Administration** tab, select **Manage Organizations**>**Processing Options**>**View**. The *Select Organization Endpoint* page appears.

2. Select the highest-level organization or any lower-level OTC Endpoint to view the processing options.

3. A *View Processing Options* page appears, presenting the custom labels in effect for the organization hierarchy as shown in Figure 18.

Figure 18. View Processing Options

Additional Button

Select **Return Home** to return to the OTCnet Home Page.

Summary

In this chapter, you learned:

- The purpose of organizational hierarchy

- How to add lower-level endpoints to the highest level of an organization hierarchy

- How to add additional lower-level endpoints or a financial institution relationship to a hierarchy that was previously defined

- How to make changes to OTC Endpoints

- How to delete OTC Endpoints

- How to view OTC Endpoints

- How to modify accounting codes

Chapter 5. Configuring Administration and Card Processing Settings

OTCnet Participant User Guide

Table of Contents

List of Figures

Glossary

Click this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Configuring Administration and Card Processing Settings*. In this chapter, you will learn:

- How to create, edit and delete custom labels
- How to set your options for processing and deposits
- How to create, edit and delete user defined fields (UDFs) specific to your agency

Topics

The topics in this chapter include the following:

1. Managing Custom Labels
2. Managing Processing Options
3. Creating and Editing User Defined Fields (UDFs)

Audience

The intended audience for the *Configuring Administration and Card Processing Settings* Participant User Guide includes:

- Accounting Specialist
- Local Accounting Specialist
- Card Administrator

Topic 1 Managing Custom Labels

As an **Accounting Specialist**, you are authorized to define (create), modify and/or view a custom label. As part of your responsibility in managing your organization hierarchy, which includes entering the appropriate accounting codes, you can also customize the field labels in the deposit preparation page. These fields are called custom labels.

Customizing the labels for your organization's **Deposit Preparers** and **Deposit Approvers** is useful when these roles are preparing and submitting deposits and/or reports. A custom label allows you to define a level in the organization hierarchy, the internal control number, or an agency accounting code. Performing this customization is *optional*.

Agency Accounting Code is the default name for the label; when you define the label, you are actually modifying its name. When referring to a custom label, the terms *define* and *create* are used interchangeably.

As an example, if your agency refers to *Accounting Codes* as *Financial Numbers,* you can modify the custom label to be *Financial Number*.

Once a custom label is defined, you may modify it. You can also view your custom labels from **Manage Organizations**, **Custom Labels**.

Define a Custom Label

To define (create) a custom label, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**Custom Labels**>**Modify**. The *Select OTC Endpoint* page appears.

2. Select the highest-level OTC Endpoint for which you want to modify custom labels. The *Step 1 of 2: Update Custom Labels* page appears.

3. Update the custom label(s) for the organization hierarchy by completing the following steps as shown in Figure 1:

    a. Enter a title for your **Organization Hierarchy Labels**.

    b. Enter an agency accounting code title for the **Accounting Code Definition Label**.

    c. Click **Next**.

Figure 1. Step 1 of 2: Update Custom Labels

4. The *Step 2 of 2: Review Custom Labels* page appears.

Application Tips

The **Accounting Specialist** is authorized to complete the following steps:

- Define a new **Organization Hierarchy Label**
- Update the existing label(s)
- Modify the label of the accounting code definition

5. Verify the information is correct and click **Submit**. A *Confirmation* page appears presenting the custom labels modified for the organization hierarchy.

Additional Buttons

- Click **Cancel** to return to the OTCnet Home Page. No data is saved.
- Click **Edit** to make additional changes.
- Click **Previous** to return to the previous page.
- Click **Submit** to complete the process and display the Confirmation page.

Modify a Custom Label

To modify a custom field label, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**Custom Labels**>**Modify**. The *Select OTC Endpoint page* appears.

2. Select the organization endpoint for which you want to modify custom labels. *The Step 1 of 2: Update Custom Labels* page appears.

3. Update the custom labels for the organization hierarchy and click **Next**. The *Step 2 of 2: Review Custom Labels* page appears as shown in Figure 2.

Figure 2. Step 2 of 2: Review Custom Labels

Application Tips

- If an Agency Accounting Code label is customized, it is displayed as the label above the imported or modified codes within the Maintain Accounting Codes module, according to the custom label that was defined for the highest-level organization.
- Within the rest of the application, custom labels apply to deposit processing functionalities, but are not extended to check processing functionalities.
- The default accounting code label is **Agency Accounting Code**.

4. Verify the information is correct and click **Submit**.

A *Confirmation* page appears presenting the custom labels modified for the organization hierarchy.

View a Custom Label

To view a custom label, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**Custom Labels**>**View**. The *Select OTC Endpoint* page appears.

2. Select the highest-level organization for which you would like to view the custom labels. The *View Custom Labels* page appears showing the custom labels that are in effect for the organization hierarchy as shown in Figure 3

Figure 3. View Custom Labels

Additional Buttons

- Click **Cancel** to return to the OTCnet Home Page. No data is saved.
- Click **Return Home** to return to the OTCnet Home Page.

Topic 2 Managing Processing Options

Managing your organization hierarchy includes defining your deposit processing options. **Processing options** are parameters for the deposit and adjustments process. For processing options, you must define the following:

- First, define processing options at the highest level of the organization, before defining lower-level options.

- For lower-level organizations, you must define these options, or the lower-level organizations will take on the options set for the next higher-level organization that does have the options set.

You must define processing options or your organization cannot create deposits. Define processing options at any level within your organization. View the processing options by **OTC Endpoint** report to manage processing options in your organization.

As an **Accounting Specialist**, you are authorized to modify the following processing options for your organization's hierarchy:

- **Accounting Classifications for Adjustments**: Identifies the default accounting codes to which you want adjusted amounts credited and debited

- **Correspondence**: Provides the financial institution with address information for any correspondence, including returned item information

- **Deposit Preparation**: Sets default settings for deposit preparation to save time for Deposit Preparers

- **Transaction History**: Sets default settings for historical data about transactions

Modifying Processing Options

Accounting Specialists are authorized to modify processing options for the following:

- **Accounting Classifications for Adjustments, Corrections, and Returned Items**

- **Correspondence**

- **Deposit Preparation**

- **Transaction History**

When defining processing options, keep the following information in mind:

- To narrow an accounting code search, enter a partial or full accounting code.

- All accounting codes that meet your search criteria and that are not applied as a debit or credit adjustment to your OTC Endpoint are displayed on the page. You must enter search criteria, or all the accounting codes defined for the highest-level organization appear.

- By default, the first ten accounting codes display in the following order, by:

    - Ascending special character order

    - Numerical order

- Ascending alphabetical order by accounting code

- If an organization has more than ten accounting codes, click the pagination menu above the section containing the existing accounting codes to view additional page results. The system only allows a user to view and apply active accounting codes not designated as Treasury Account Symbol (TAS), or those designated as TAS and that have been validated by Share Accounting Module (SAM).

- After an accounting code is assigned to debit or credit adjustment, it appears in the Adjustment Type table.

Modify a Processing Option

To modify a processing option, complete the following steps:

1. From **Administration**, click **Manage Organizations**>**Processing Options**>**Modify**. The *Step 1 of 3: Select Organization Endpoint* page appears.

Application Tips

- Processing options must first be defined for the highest-level organization before any lower-level organization's processing options can be defined.
- If the processing options are not defined for the highest-level organization, all lower-level organization links are disabled.

2. Select the OTC Endpoint for which you want to modify a processing option. The *Step 2 of 3: Define Processing Options* page appears.

3. Modify the processing option(s) and click **Next**.

   To modify **Accounting Classifications for Adjustments**, **Corrections**, and **Returned Items** as shown in Figure 4, complete the following steps:

   Update **Default Accounting Codes** by:

   - Selecting either **Use parent's values** or **Use my values**

       Or

   - Clicking **Search** (magnifying glass) to view accounting codes

Application Tip

- If selecting **Use my values**, enter the search criteria for the accounting code you would like to view and click **Search** (magnifying glass)
- To narrow an accounting code search, enter a partial or full accounting code

   - Selecting the accounting code to apply a credit and/or debit adjustment type and clicking **Assign to Debit** and/or **Assign to Credit**
   - Selecting **Yes** or **No** to allow changes by an organization lower in hierarchy

Application Tip

- An accounting code can be assigned to both a debit adjustment and credit adjustment
- After an accounting code is assigned to a debit or credit adjustment, it appears in the Adjustment Type table

Figure 4. Step 2 of 3: Define Processing Options page with Accounting Classifications for Adjustments, Corrections and Returned Items expanded

Update **Default Accounting Code Usage** by completing the following steps:
- Selecting either **Use parent's values** or **Use my values**
- Selecting either **Always Use the Default for Deposit Adjustments** or **Default based upon Deposit Subtotals for Deposit Adjustments**
- Selecting **Yes** or **No** to allow changes by an organization lower in hierarchy

To modify **Correspondence**, complete the following steps as shown in Figure 5:
Update **Returned Items** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Entering the corresponding address information that you would like to be displayed to a financial institution when a return item adjustment is created
- Selecting **Yes** or **No** to allow changes by an organization lower in hierarchy

Update **Deposit Adjustment** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Entering the corresponding address information that you would like to be displayed to a financial institution when a deposit adjustment is created
- Selecting **Yes** or **No** to allow changes by an organization lower in hierarchy

Figure 5. Define Processing Options page with Correspondence expanded

To modify **Deposit Preparation**, complete the following:

Update **ITGA Deposit Creation** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** to allow the endpoint to create foreign deposits:
    - If the endpoint accepts foreign deposits, enter the **Default foreign currency when creating deposits** details
- Selecting **Yes** or **No** to allow changes by an organization lower in hierarchy

Update **Subtotals and Cash Count** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** for each of the following options:
    - Include subtotals for checks/money orders and cash
    - Include currency count and subtotals by denomination
    - Include coin count and subtotals by denomination
    - Allow changes by an organization lower in hierarchy

Update **Accounting Code Subtotals** by completing the following steps:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** for each of the following options:
    - Allow negative accounting code subtotals
    - Allow changes by an organization lower in hierarchy

Update **Separation of Duties** by completing the following steps as shown in Figure 6:
- Selecting **Use parent's values** or **Use my values**
- Selecting **Yes** or **No** for each of the following options
    - Deposits must be prepared and approved by different employees
    - Allow changes by an organization lower in hierarchy

13

Figure 6. Update Deposit Processing Options with Deposit Preparation expanded

To modify **Transaction History**, complete the following steps as shown in Figure 7:

- Selecting **Use parent's values** or **Use my values**
- Entering the **Number of days** displayed in the text box, if applicable
- Selecting **Yes** or **No** to allow changes by an organization lower in hierarchy

Figure 7. Deposit Procession Options with Transaction History expanded

4. The *Step 3 of 3: Review the following processing options* page appears. Verify the information is correct and click **Submit**.

5. A *Confirmation* page appears showing which processing options were applied to the organization.

15

Viewing Processing Options

Accounting Specialists are authorized to view the following processing option details:

- **Accounting Classifications for Adjustments, Corrections, and Returned Items**
- **Correspondence**
- **Deposit Preparation**
- **Transaction History**

From the **Viewing Processing Options** page, you can view the custom labels that are in effect for your organization hierarchy.

View Processing Options

To view a processing option, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**Processing Options**>**View**. The *Select Organization Endpoint* page appears.
2. Select the highest-level organization or any lower-level OTC Endpoint for which you would like to view the processing options. A *View Processing Options* page appears, showing which custom labels are in effect for the organization hierarchy as shown in Figure 8.

Additional Button

Click **Return Home** to return to the OTCnet Home Page.

Figure 8. View Processing Options

Topic 3. Creating and Editing User Defined Fields (UDFs)

As an **Accounting Specialist** and **Card Administrator**, you are authorized to create, modify and delete a UDF for your organization hierarchy. A UDF is an optional field for the **Deposit Preparer** and **Card Operator** to complete that describes a deposit activity or deposit accounting activity (e.g., a vendor number) or a card transaction, specific to your organization. **Deposit Preparers** use UDFs when entering deposit activity and accounting activity information during the deposit preparation process. **Card Operators** use UDFs when entering card payment details during card transaction processing.

Your organization may elect to use UDFs. If so, communicate this to each of your OTC Endpoints and identify the information to be included.

Accounting Specialists and **Card Administrators** perform the following tasks in working with UDFs:

- Create a UDF

- Modify a UDF

- Delete a UDF

- View a UDF

Deposit processing activities are disabled to read-only if an **Accounting Specialist** or **Card Administrator** has selected an endpoint that is both a Deposit Processing and a Card Processing Endpoint, and this endpoint has a deposit that is currently in progress. You cannot modify or delete any deposit processing UDFs at this endpoint. You can select the **Create Card Processing** activity.

Creating a User Defined Field

Accounting Specialists and **Card Administrators** are authorized to create up to four UDFs for deposit activity and three UDFs for card processing for your agency. Up to three UDFs for a **Create Deposit** UDF and up to two UDFs for the **Create Deposit Subtotals** UDF can be created.

To create a UDF, from the *Select User Defined Field to Maintain* page, click **Create UDF.** When the *Step 2 of 3: Modify the User Defined Field* page appears, add your UDF fields (i.e., **Activity**, **Label**, **Description**, **Date Type**, **Maximum Input Length**, **Minimum Input length**, **Display Order Number**, and **Activity User Entry**).

Create a User Defined Field

To create a UDF, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**User Defined Fields**> **Modify**. The *Select OTC Endpoint* screen appears.
2. Select the highest-level organization for which you want to modify UDFs. The *Step 1 of 3: Select User Defined Field to Maintain* page appears.
3. Click **Create UDF** as shown in Figure 9. The *Step 2 of 3: Modify the User Defined Field* page appears.

Figure 9. Select 1 of 3: Select User Defined Field to Maintain

Application Tip

A message is displayed discouraging users from creating UDFs that request PII data.

4. Add the UDF and click **Done**.

    Add a UDF by:

    *   Selecting the **Activity** type for the UDF

Application Tips

*   There are two types of deposit processing activities (**Create Deposit** and **Create Deposit Subtotal**) and one activity for card processing (**Create Card Processing**).
*   For TGA/CDC Endpoints with active deposits, in the drop-down **Activity** menu, the deposit activities are disabled. In this case, **Accounting Specialists** and **Card Administrators** can only select the **Create Card Processing** activity

    *   Entering the **Label** and **Description**
    *   Selecting a **Data Type**

19

- ▪ If the **Drop Down List of Alphanumeric Values** Data Type is selected, proceed to step 6.

  - ▪ If another **Data Type** is selected, continue entering in information for the fields below. Proceed to step 7.

- • Entering the

  - ▪ **Maximum Input Length (Maximum length is 255)**

  - ▪ **Minimum Input Length**

  - ▪ **Display Order Number**

- • Selecting **Mandatory** or **Optional** for Activity User Entry

Application Tips

- ● When a deposit is in progress at a TGA or CDC endpoint, a UDF cannot be modified or deleted if the deposit is in **Draft** or **Awaiting Approval (AWAP)** status.
- ● If the **Accounting Specialist** or **Card Administrator** selected an endpoint that is both a TGA and a CDC Endpoint, and this endpoint has a deposit that is currently in progress, the deposit processing activities are disabled to read-only.
- ● Only the **Card Processing** activity is active.
- ● The **Card Administrator** continues card processing activities when a deposit is in progress.

Application Tips

- ● If the **Drop-Down List of Alphanumeric** values data type is selected, a **Permitted Values** section appears.
- ● Click **List Values**. A *Step 2 of 3 (Continued): Define Permitted Values* page appears.
- ● Enter details for both the **Value** and **Description.**
- ● Click **Done** to return to the *Step 2 of 3: Modify the User Defined Field* page.

5. The *Step 1 of 3: Select User Defined Field to Maintain* page appears again. Select **Next**.

6. The *Step 3 of 3: Review* page appears. Verify the UDF information is correct. Select the plus sign next to the UDF to expand it.

7. The *Step 3 of 3: Review page* appears. Verify the UDF information is correct and click **Submit** as shown in Figure 10.

Figure 10. Review User Defined Fields page

8.   A confirmation page appears presenting the UDF data that is saved to the database.

Additional Buttons

- Click **Cancel** to return to the OTCnet Home Page. No data is saved.
- Click **Edit** to make additional changes.
- Click **Next** to advance to the next page.
- Click **Previous** to return to the previous page.
- Click **Return Home** to return to the OTCnet Home Page

Modifying a User Defined Field

Accounting Specialists and **Card Administrators** are authorized to modify UDFs, as needed, to accommodate your organization's changing needs.

For deposit processing, you cannot modify a UDF that is associated with a deposit that is still in **Draft** or **awaiting approval (AWAP)** status. **Draft** or **AWAP** deposits must be submitted to the Financial Institution before you modify any UDFs associated with them. **Draft** or **AWAP** status does not impact card processing.

When modifying a UDF, you can modify the following UDF fields:

- **Activity**
- **Label**
- **Description**
- **Date Type**
- **Maximum Input Length**
- **Minimum Input length**
- **Display Order Number**
- **Activity User Entry**

Modify a User Defined Field

To modify an existing UDF, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**User Defined Fields**>**Modify**. The *Select OTC Endpoint* screen appears.

2. Select the highest-level organization for which you want to modify a UDF. The *Step 1 of 3: Select User Defined Field to Maintain* page appears.

3. Click the **UDF Label hyperlink**. The *Step 2 of 3: Modify User Defined Field* page appears.

Application Tip

A message is displayed discouraging users from creating UDFs that request personally identifiable information (DII) data.

4. Make the changes to the UDF and click **Done**. The *Step 1 of 3: Select User Defined Field to Maintain* page appears as shown in Figure 11.

Figure 11. Select User Defined Field to Maintain

5. Click **Next**. The *Step 3 of 3: Review* page appears.

6. Verify the UDF information is correct and click **Submit**. A confirmation page appears presenting the UDF data that has been saved to the database.

Additional Buttons

- Click **Cancel** to return to the OTCnet Home Page. No data is saved.
- Click **Create UDF** to create a new UDF.
- Click **Next** to advance to the next page.
- Click **Previous** to return to the previous page.
- Click **Edit** to make additional changes to a UDF.
- Click **Submit** to complete the process and display the **Confirmation** page.
- Click **Return Home** to return to the OTCnet Home Page.

Deleting a User Defined Field

Accounting Specialists and **Card Administrators** are authorized to delete a user defined field (UDF). If a UDF isn't needed, delete it to save labor for your **Deposit Preparers** and **Card Administrators**.

For deposit processing, you cannot modify a UDF that is associated with a deposit that is still in **Draft** or **awaiting approval (AWAP)** status. **Draft** or **AWAP** deposits must be submitted to the financial institution before you modify any UDFs associated with them. **Draft** or **AWAP** status does not impact card processing.

Delete a User Defined Field

To delete a UDF, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**User Defined Fields**>**Modify**. The *Select OTC Endpoint* screen appears.

2. Select the highest-level organization for which you want to delete the UDF. The *Step 1 of 3: Select User Defined Field to Maintain* page appears as shown in Figure 12.

3. Click the **Delete** checkbox next to the appropriate field and click **Next**. *The Step 3 of 3: Review* page appears. Select the plus sign next to the UDF to expand it.

Figure 12. Select 1 of 3: Select User Defined Field to Maintain

Application Tip

A UDF, during deposit processing, cannot be deleted if it is associated with a deposit that is in **Draft** or **awaiting approval (AWAP)** status. Only the **Card Processing** activity is active.

4. Verify the correct information is marked for deletion and click **Submit**. A *Confirmation* page appears showing the UDF data is saved to the database.

Additional Buttons

- Click **Cancel** to return to the OTCnet Home Page. No data is saved.
- Click **Create UDF** to create a new UDF.
- Click **Next** to advance to the next page.
- Click **Previous** to return to the previous page.
- Click **Edit** to make additional changes to a UDF.
- Click **Submit** to complete the process and display the Confirmation page.
- Click **Return Home** to return to the OTCnet Home Page.

Viewing a User Defined Field

As an **Accounting Specialist**, **Local Accounting Specialist**, **Viewer** and **Card Administrator,** you are authorized to view the UDFs that exist for your organization.

To view a UDF, choose it in the *View User Defined Field* page. You can view the following characteristics:

- **Activity Type**
- **Label**
- **Description**
- **Data Type**
- **Display Order Number**
- **Activity User Entry**
- **Minimum Input Length**
- **Maximum Input Length**

View a User Defined Field

To view a UDF, complete the following steps:

1. From the **Administration** tab, click **Manage Organizations**>**User Defined Fields** >**View**. The *Select OTC Endpoint* screen appears.

2. Select the highest-level organization for which you would like to view a UDF. *A View User Defined Field* page appears.

3. Click on any of the UDFs to view its characteristics (e.g., activity type, label, description, etc.). The characteristics appear as shown in Figure 13.

Figure 13. View User Defined Field

Summary

This chapter provided information on:

- How to create, edit and delete custom labels

- How to set your options for processing deposits

- How to create, edit and delete UDFs specific to your agency

Chapter 6. Viewing Financial Institutions

OTCnet Participant User Guide

Table of Contents

List of Figures

Glossary

Click this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Viewing Financial Institutions.* In this chapter, you will learn:

- How to view a financial instruction

Topics

The topic in this chapter is: Viewing Financial Institutions.

Audience

The intended audience for the *Viewing Financial Institutions* Participant User Guide includes:

- Financial Institution (FI) Confirmer
- Federal Reserve Bank (FRB) Confirmer
- FI Viewer
- FRB Viewer

Topic 1 Viewing a Financial Institution

Financial Institution (**FI) Confirmers**, **Federal Reserve Bank (FRB) Confirmers**, **FI Viewers** and **FRB Viewers** are authorized to locate and view financial institution details. You can only view a financial institution with an **Active** status.

Viewing a financial institution allows you to see related details, including the following:

- Institute Information
- Routing Transit Numbers (RTN) and Status
- CA$HLINK II Account Number (CAN)/Account Key Relationships

View a Financial Institution

To view a Financial Institution (FI), complete the following steps:

1. From **Administration**, select **Manage FI>Financial Institution>View**.
2. The *View the Financial Institution* page appears. View details for financial institutions as shown in Figure 1 and Figure 2.

Figure 1. View FRB Detail

Figure 2. View Financial Institution Detail

Application Tip

FI Confirmers, Federal Reserve Bank (**FRB) Confirmers**, **FI Viewers**, and **FRB Viewers** are authorized to view Institution Information, Routing Transit Numbers (RTN) and Status and CAN/Acct Key Relationships.

Additional Button

Click **Return Home** to return to the OTCnet Home Page.

Summary

In this chapter, you learned how to view a financial institution.

Administration

Chapter 7. OTCnet Local Bridge (OLB) Setup Guide

OTCnet Participant User Guide

Table of Contents

List of Figures

Glossary

Select this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to the *OTCnet Local Bridge (OLB) Setup Guide.* In this chapter, you will learn:

- How to download and install the OTCnet Local Bridge (OLB) application
- How to create your OLB profile
- How to import your OLB credentials

Topics

The topics in this chapter include the following:

1. Downloading and Installing the OLB Application
2. Creating the OLB Profile
3. Importing the OLB Credentials

Audience

The intended audience for the *OTCnet Local Bridge (OLB) Setup* Participant User Guide includes:

Downloading and Installing the OLB Application

- Check Capture Administrator
- Card Administrator

Creating the OLB Profile

- Check Capture Administrator
- Card Administrator
- Check Capture Supervisor
- Check Capture Lead Operator
- Check Capture Operator
- Card Operator

Importing the OLB Credentials

- Check Capture Administrator
- Card Administrator
- Check Capture Supervisor
- Check Capture Lead Operator

- Check Capture Operator
- Card Operator

Administration

Topic 1 Downloading and Installing the OTCnet Local Bridge (OLB) Application

Downloading the OTCnet Local Bridge (OLB) Application

The **Check Capture Administrator (CCA)** and **Card Administrator (CA)** are authorized to download the OTCnet Local Bridge (OLB). The OLB is a stand-alone application that must be installed on all user workstations performing card processing, check capture, check processing and terminal configuration operations.

Windows Administrator privileges are required to install the OLB application on a workstation. Users may contact the **CCA** or the Agency's IT team to complete this step. The OLB must be installed before proceeding to the steps below. The download release process was streamlined for ease and efficiency—as a result, we recommend you download the newest version of the OLB.

OTCnet Firmware:

- For **check processing workstations**, the OLB application is installed before or after the OTCnet Firmware is installed.

- Both the OLB application and Firmware must be installed on the workstation.

  - The OLB application is required if you are using the Deployable Disbursing System (DDS) Interface (DoD only).

- For **card processing workstations**, Firmware is not required.

- Depending on your user role, you may not have access to both **Manage Check Processing** and **Manage Card Processing** functions.

OTCnet supports Microsoft Edge and Google Chrome browsers.

When using Microsoft Edge and Google Chrome:

- Ensure the latest version of the OLB is installed.

After the **CCA** or **CA** downloads the OLB application, users (**CCA, Check Capture Supervisor [CCS]**, **Check Capture Lead Operator [CCLO]**, **Check Capture Operator [CCO], CA** and **Card Operator [CO]**) complete the following steps in setting up the OLB application:

- Install the OLB application
- Create the OLB profile
- Start the OLB application

Download the OTCnet Local Bridge (OLB) Application

To download the OTCnet Local Bridge (OLB) application, complete the following steps:

1. From **Administration**, select **Manage Centralized Deployment**>**Download Release**.

2. The *Download Release* page appears. From the **Application** drop-down menu, select **OTCnet Local Bridge**. Select **Next** as shown in Figure 1.

Figure 1. Download Release, OLB

Application Tips

- By default, the **Application** drop-down menu is set to **Firmware**. Select **OTCnet Local Bridge**.
- The OLB application can be installed before or after Firmware is installed.
- However, both the OLB application and Firmware must be installed for workstation configuration.

3. The *Select OTCnet Local Bridge for Download* page appears. Select the **OTCnet Local Bridge** hyperlink, for the newest version of the OLB, to download the OLB Zip file.

4. The *Review OTCnet Local Bridge Download* page appears. Select **Download**. The zip file downloads to your workstation.

Application Tip

- Before you install the new OLB version, you must uninstall any older OLB version(s).
- Select **Previous** to return to the previous page.
- Select **Return Home** to return to the OTCnet Home page.

Installing the OTCnet Local Bridge (OLB) Application

After the **CA** or **CCA** downloads the OLB application, the next step is for the **CA**, **CCA, CCS**, **CCLO**, **CCO, CA** and **CO** to install the OLB application. To install the OLB application, you must have Windows Administrator privileges on each workstation.

Multiple versions of the OLB are available for download. Depending on your agency, you may choose to install the newest version, or an older version—the newest version is recommended.

Version information includes the following:

- **OLB Installer**
  For OLB version 2.5.0.0 and newer, the bundled Java Runtime Environment (JRE) was removed from the OLB installer. The OLB installer now verifies whether Java is installed on the workstation, and if the Java version is one that OTCnet supports. If Java is not installed on the workstation, Windows Administrator privileges are required to install Java.

  For additional information, and to verify that you meet system and configuration requirements, review the system requirements document: https://fiscal.treasury.gov/files/otcnet/otcnet-sys-req.pdf

Before you install the OLB application, and prior to each upgrade, the currently installed OLB application version must be uninstalled.

> **To uninstall a previous version of the OLB For Windows 10:**
>
> - If running, stop the OLB application
> - Access your Control Panel under **Star**t>**Windows Settings**>**Control Panel**
> - Double-click **Add or Remove Programs**
> - Select **OTCnet OLB** in the **Currently installed programs** box
> - Select **Remove**
> - Select **Yes** and wait while the OLB application uninstalls

Install the OTCnet Local Bridge (OLB) Application

To install the OLB application, complete the following steps:

5. Locate the folder on the workstation where the OLB zip file resides, e.g., your Downloads folder. Double-click the zip file. Double-click the EXE file as shown in Figure 2 to start the installation.

Application Tip

The EXE must be launched and executed by a Windows Administrator.

Figure 2. OTCnet Local Bridge

1. The *Welcome to the OTCnet OLB Setup program* dialog box appears. Select **Next**.

Application Tip

- Select **Cancel** to cancel and exit the setup.

2. The *Destination Location* dialog box appears. Select **Next**.

Application Tip

- It is recommended that you install the OLB application into the default destination folder (i.e., C:\Program Files\OTCnet_ olb).
- Select **Cancel** to cancel and exit the setup.
- Select **Back** to return to the previous dialog box.

3. The *Start Installation* dialog box appears. Select **Next**.

4. The *Server Port Settings* dialog box appears. Select **Next**. Wait a moment while the files install.

💡 **Application Tips**

- It is recommended that you install the OLB application with the default list of fixed ports.
- If your agency has different server port settings or needs, contact Customer Support.

5. Once the *OTCnet Local Bridge has been successfully installed* message appears, select **Finish**.

💡 **Application Tips**

- The OLB Installer verifies that Java is installed on the workstation.
- If Java is not installed, you will receive a "*Java X must be installed for the OLB to function. The JAVA_HOME environment variable must also be set pointing to the main Java installation folder*" message as shown in Figure 3. A Windows Administrator must install Java.

Figure 3. Java message
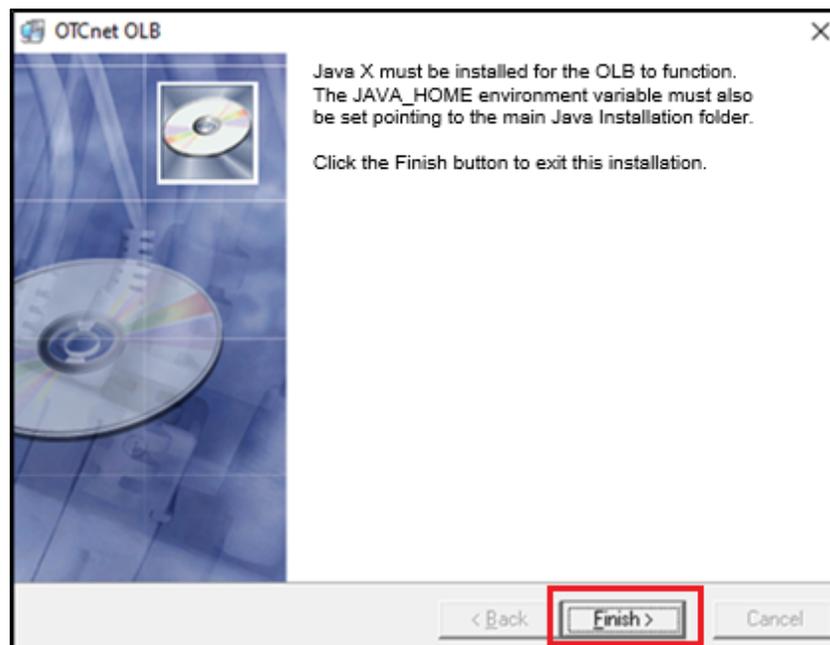
6. The OTCnet OLB start and stop icons appear on the workstation desktop as shown in Figure 4.

Figure 4. Start and Stop OTCnet Local Bridge icons

Upgrading the OTCnet Local Bridge (OLB) Application

The **CCA** and **CA** are authorized to upgrade the OLB.

As newer versions of the OTCnet OLB application become available, your Agency may choose to upgrade its workstations. *Upgrade* refers to installing an updated version of OTCnet OLB on a workstation that has a previous version of the OTCnet OLB installed.

Prior to initiating an OTCnet OLB application upgrade, consider the following information:

- Before uninstalling the OLB application, you must first stop the OLB application.

- If the OLB application is started on the workstation, ensure that it is stopped before uninstalling the application, or you will not be able to install the new OLB version.

- You must have Windows Administrator privileges to upgrade each computer.

- When upgrading to a newer OLB version, uninstall the previous OLB version and perform a new installation.

- If you previously created and imported your OLB credentials, you will not need to recreate and reimport your OLB credentials after upgrading to a newer OLB version.

- The OLB application is required for workstation detection and performing check capture and check processing operations.

Upgrade the OTCnet Local Bridge (OLB) Application

To upgrade the OTCnet Local Bridge (OLB) application, complete the following steps:

1. Stop the OTCnet OLB application. From the desktop, double-click **Stop OTCnet Local Bridge**.
2. Locate the folder where the OTCnet OLB application is installed and uninstall it.
3. After downloading the latest version of the OTCnet OLB application, locate the folder on the workstation where the OLB zip file resides, e.g., your Downloads folder. Double-click the zip file. Double-click the .EXE file to start the installation.
4. The *Welcome to the OTCnet OLB Setup program* dialog box appears as shown in Figure 5. Select **Next**.

Figure 5. Welcome to the OTCnet OLB Setup Dialog Box
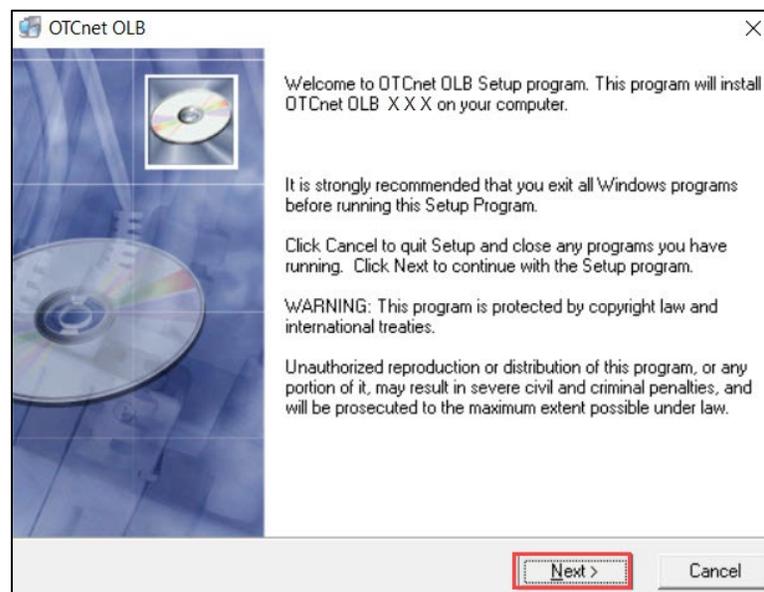
Application Tip

- Select **Cancel** to cancel and exit the setup.

5. The *Destination Location* dialog box appears. Select **Next**.

Application Tip

As a best practice, it is recommended that the OLB application be installed in the default destination folder (i.e., C:\Program Files\OTCnet_olbC).

Additional Buttons

- Select **Cancel** to exit the setup.
- Select **Back** to return to the previous dialog box.

6. The *Start Installation* dialog box appears. Select **Next**.

7. The *Server Port Settings* dialog box appears. Select **Next**. Wait a moment while the files install.

Application Tip

- It is recommended that you install the OLB application with the default list of fixed ports.
- If your agency has different server port settings or needs, contact Customer Support.

8. Once the *OTCnet OLB has been successfully installed* message appears, select **Finish**.

Application Tip

- The OLB Installer verifies that Java is installed on the workstation.
- If Java is not installed, you will receive a "*Java X must be installed for the OLB to function. The JAVA_HOME environment variable must also be set pointing to the main Java installation folder*" message as shown in Figure 6. A Windows Administrator must install Java.
- To upgrade your OLB version, you do not need to recreate or import your OLB credentials.

Figure 6. Java message
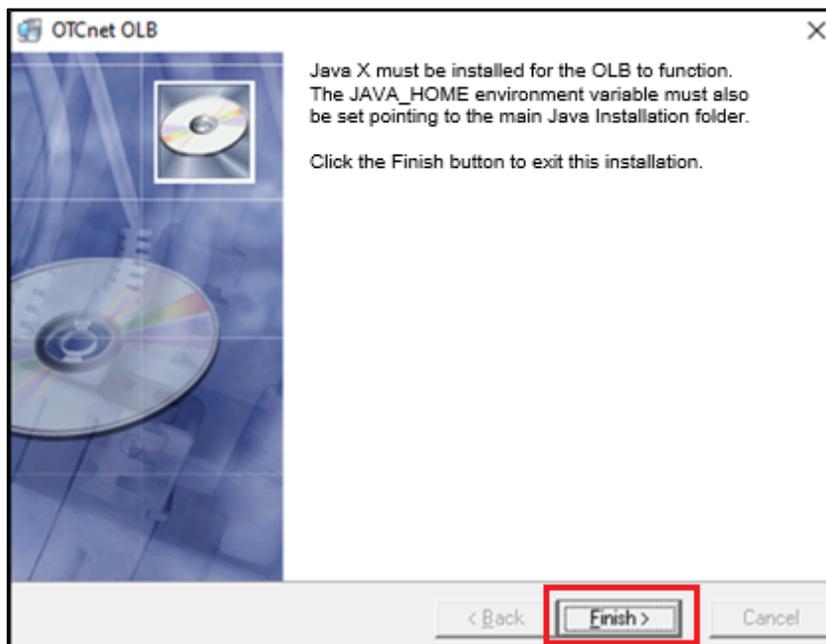
9. The OTCnet OLB start and stop icons appear on the desktop of the workstation as shown in Figure 7.

Figure 7. Start and Stop OTCnet Local Bridge icons

Topic 2 Creating the OTCnet Local Bridge (OLB) Profile

After the **CCA** or **CA** downloads the OTCnet Local Bridge (OLB) application, the next step is to create the OLB profile.

If you are assigned the role of **CCA**, **CCS**, **CCLO**, **CCO**, **CA** or **CO**, you are authorized to create the OLB profile. The OLB profile is unique to each user role. Therefore, each of these user roles must create an OLB profile.

Before creating an OLB profile, consider the following information:

- Creating an OLB profile applies to all card processing and check processing users, including **CCA**, **CCS**, **CCLO**, **CCO, CA** and **CO**.

- The OLB application is required for the following:

    - Check capture workstation detection

    - The Deployable Disbursing System (DDS) Interface (DoD and Check Processing only)

    - Performing check processing and check capture operations and performing card processing operations and card workstation detection.

When creating a Local Bridge password, keep the following password criteria in mind. The password must contain:

- At least 12 characters

- No more than two repeating characters

The password must not be:

- A word in a language, slang, dialect, or jargon

- Related to personal identity, history, environment, or other personal associations

- Shared or displayed in plain view

The password criteria are displayed on the page when you enter and confirm your Local Bridge password.

Create the OTCnet Local Bridge (OLB) Profile

To create an OLB profile, complete the following steps:

1. From **Administration**, select **Manage Users**>**Create Local Bridge and User Profile**.

2. Select the relevant radio button for your version of the OLB.

Application Tips

Before you create your new profile, and if you downloaded and installed the newest version of the OLB, you must import the new OLB credentials file, required.

3. Enter your **Local Bridge Password** and confirm your **Local Bridge Password** as shown in Figure 8. Select **Submit**.

Figure 8. Create Local Bridge and User Profile Radio Buttons and Password

Application Tip

Select **Submit** and the system generates the credential file based on the application version selected.

Additional Buttons

- Select **Clear** to reset the password fields.
- Select **Cancel** to return to the OTCnet Home Page.

4. A *Do you want to open or save [file name].ini?* dialog box appears. Select the **Save** drop-down arrow and select **Save as**.

Application Tips

- When saving the OLB credential file, ***do not*** rename the file as the file name must remain the same as it was when it was generated.
- If the file name is changed, the OLB application will not run.

Additional Buttons

- Select **Open** and the file opens in the Microsoft Notepad application.
- Select **Cancel** and the *Do you want to open or save* dialog box closes; you remain on the *Create Local Bridge and User Profile* page.

5. The *Save* dialog box appears. Select **Save** as shown in Figure 9 or **Cancel**.

Figure 9. Create Local Bridge and User Profile Save
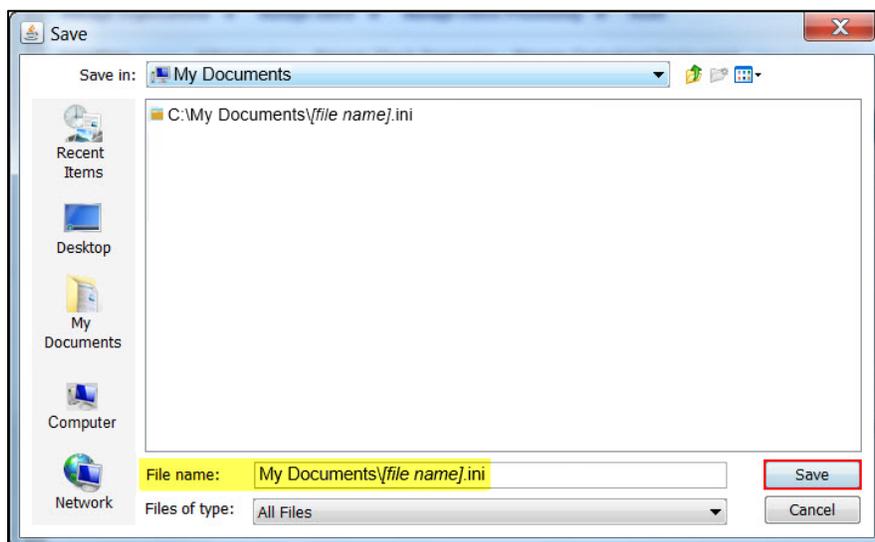
Application Tips

- Choose the location where you want to save the OLB credential file. Save the OLB credential file to any folder where you can save a file (e.g., My Documents folder, Desktop folder).
- The default location on the *Save* dialog box is the user's **My Documents** folder.
- For a forgotten OLB password, or if you attempt to enter an incorrect password three times (or more), you must recreate an OLB credential file through the *Create Local Bridge and User Profile* page and save it again.
- You must also import your OLB credentials again, which is the next step in the OLB startup process.

Additional Button

Select **Cancel** to return to the *Create Local Bridge and User Profile* page without saving the file.

Topic 3 Importing OTCnet Local Bridge (OLB) Credentials

The OTCnet Local Bridge (OLB) application is required for OTCnet Online users performing workstation configuration, check processing, card processing and check capture operations. As a **CCA**, **CCS**, **CCLO**, **CCO**, **CA** or **CO**, you are required to import your OLB credentials to the workstation.

Additional version information includes the following:

- If upgrading your OLB version, in general, you do not need to recreate or re-import your OLB credentials.

- If upgrading your OLB version from a version older than 2.2.0.0, you must recreate and re-import your OLB credentials.

The only time you need to recreate an OLB password is if you forget your OLB password. After recreating your OLB password, OTCnet users must re-import OLB credentials.

Importing OLB credentials is unique to each user. Therefore, if there are multiple users on a workstation, each user must import their own OLB credentials.

Users are only required to import their OLB credentials *once*. After importing OLB credentials, users can successfully start the OLB application.

Before importing your OLB credentials, ensure the following steps have been completed in this order:

1. The **CCA** or **CA** downloaded the OLB application.

2. The OLB application is installed on the workstation.

3. Each user has created an OLB profile, ensuring that the OLB credential file was *not* renamed (the file name remained the same as it was when generated).

Import OTCnet Local Bridge (OLB) Credentials

To import OTCnet Local Bridge (OLB) credentials, complete the following steps:

1. Double-click the **Start OTCnet Local Bridge** icon located on the workstation desktop.

   Or

   Select **Start**>P**rograms**>**Start OTCnet Local Bridge**.

Application Tips

If the icon does not reside in either location, contact your **CCA** or **CA**. They can help with:

- Completing the steps required to install the OLB application on the workstation
- Creating your OLB profile
- Importing your OLB credentials

2. The *OTCnet Local Bridge Startup* window appears. Select the **File** menu.
3. Select **Import User Profile** as shown in Figure 10.

Figure 10. Start OTCnet Local Bridge Startup

4. The *Select User Profile File* window appears. Navigate to the location on the workstation where the OLB credential file was saved. Select the file and select **Import**.

Application Tip

The default location on the *Select User Profile File* window is the user's **My Documents** folder.

5. A *Successfully imported user profile* message appears. Select **OK**. Once you have successfully imported your OLB credentials, proceed with starting the OLB application on the workstation.

Summary

In this chapter, you learned:

- How to download and install the OTCnet Local Bridge (OLB) application
- How to create the OTCnet Local Bridge (OLB) profile
- How to import the OTCnet Local Bridge (OLB) credentials

Chapter 8. Configuring Card Terminal Processing Settings

OTCnet Participant User Guide

Table of Contents

List of Figures

List of Tables

Glossary

Select this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Configuring Card Processing Settings*. In this chapter, you will learn:

- The purpose of configuring card processing settings
- How to set up or modify a card terminal configuration
- How to view a card terminal configuration
- How to search an audit log online
- How to select an 80mm Card Receipt Printer

Topics

This chapter is organized by the following topics:

1. Purpose of Configuring Card Processing Settings
2. Setting Up or Modifying a Card Terminal Configuration
3. Searching an Audit Log
4. Selecting the 80mm Card Receipt Printer

Audience

The intended audience for the *Configuring Card Terminal Processing Settings* Participant User Guide includes:

View / Modify Configuration Functions

- Card Administrator
- Check Capture Administrator
- Check Capture Supervisor

View Configuration Only

- Card Operator
- Check Capture Lead Operator
- Check Capture Operator

Topic 1 Purpose of Configuring Card Processing Settings

As a **Card Administrator (CA),** you are authorized to configure the card processing settings for your Agency's card terminal. Additionally, as a **CA**, you are authorized to manually download or upgrade application software (e.g., the OTCnet Local Bridge Application [OLB]) which is used to communicate between OTCnet and a card terminal. You must register your card terminal.

For check processing, a **Check Capture Administrator (CCA)** can also download or upgrade the OLB.

To meet your agency's card transaction needs, each card terminal must have configuration settings individually applied. The card terminal must be paired with OTCnet **before** the card terminal can be used for processing payments in OTCnet Online. The following is a list of data elements needed to pair the card terminal to OTCnet:

- **Card Terminal Internet Protocol (IP) Address**—an Internet Protocol address is a unique number or address that computing devices, (e.g., computers, laptops, tablets, etc.) connected to a computer network, use to identify themselves and communicate with other devices in an IP-based network (e.g., the Internet).

- **OTC Endpoint Credit-Debit Card (CDC)**—The endpoint (location) setup in OTCnet for CDC processing

- **OTCnet-Generated Eight-Character Pairing Pin**—A pairing pin is a unique eight-character OTCnet-generated number used to pair OTCnet and the card terminal. During card terminal setup, the card terminal prompts the user for the pairing pin.

Topic 2 Setting Up or Modifying a Card Terminal Configuration

As a **Card Administrator (CA)** you are authorized to register/configure a card terminal. To register a card terminal, you must select your OTC Endpoint and enter your Card Terminal Internet Protocol (IP) Address. You can also unregister a card terminal. For this you must begin the steps to re-register a card terminal. And you are authorized to view a card terminal. To configure a card terminal, start the OLB. If the OLB is not started, you cannot pair the card terminal with OTCnet.

Once the OLB is started, ensure the following:

- The card terminal must be ethernet connected to the Internet/network and ready for pairing with the OTCnet server

- The **CA** must use either a Static (Fixed Internet Protocol Address [IP]) or Dynamic Host Configuration Protocol (DHCP) when configuring the card terminal. A static IP address is recommended as it will not change.

Registering a Card Terminal

To register a card terminal, modify your Card Terminal Configuration, by selecting your OTC Endpoint and entering your Card Terminal IP Address. The system searches for and displays a pairing pin, which you will enter into the card terminal. The system compares Merchant IDs and communicates when the connection is successful.

Register a Card Terminal

To register/configure a card terminal, complete the following steps:

1. From the **Administration** tab, select **Manage Card Processing**>**Card Terminal Configuration**>**Modify**. The *Step 1 of 3: Select OTC Endpoint and Card Terminal Type* page appears.

💡 Application Tip

When configuring a card terminal, if you have not started the OLB application, you will receive the following message: "*Card terminal detection failed. Ensure that the OLB application is running.*"

2. Select the OTC Endpoint. Select **Add**. The Endpoint appears under **Configured OTC Endpoint**.

3. Select the **Card Terminal Type** from the dropdown at the bottom of the page. Then select **Next** as shown in Figure 1.

Figure 1: Step 1 of 3 Select OTC Endpoint and Card Terminal Type Page

Application Tips

- You need to **upgrade the OLB** to a new version to avoid receiving an error when registering your device to OTCnet and using your **M440** card terminal.
- If you are an existing **MX925** user, you will also need to upgrade to the latest OLB to keep using the existing card terminals.

4. The *Step 2 of 3: Terminal Registration* page appears, as shown in Figure 2. Enter the **Card Terminal Internet Protocol (IP) Address** and select **Register**.

Figure 2: Terminal Registration, Enter Card Terminal IP Address

Application Tip

Internet Protocol (IP) Address is a unique number or address that computing devices (e.g., laptops, tablets, mobile phones, etc.) connected to a computer network, use to identify themselves and communicate with other devices in an IP-based network (e.g., the Internet). Please contact your deployment specialist to help you retrieve your IP address at: fiscalservice.otcdeployment@citi.com.

5. The system searches for the pairing pin. A pairing pin displays.

6. Enter the **Pairing Pin** on the card terminal, as shown in Figure 3. Press the **green button**. The green button indicates "**OK**" on the card terminal. The system compares Merchant IDs.

Figure 3: Step 2 of 3: Card Terminal Registration and Entering the Pairing Pin in the Card Terminal
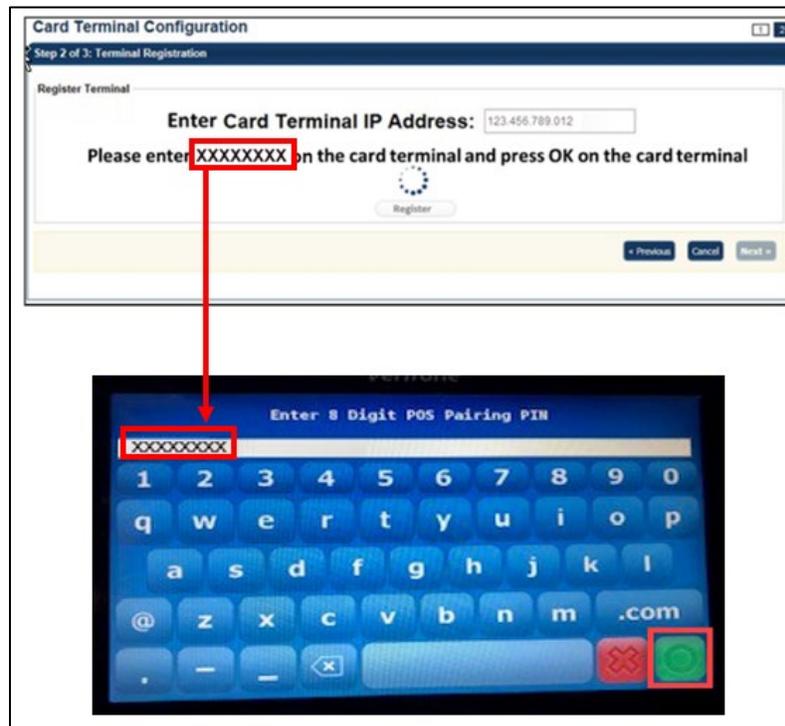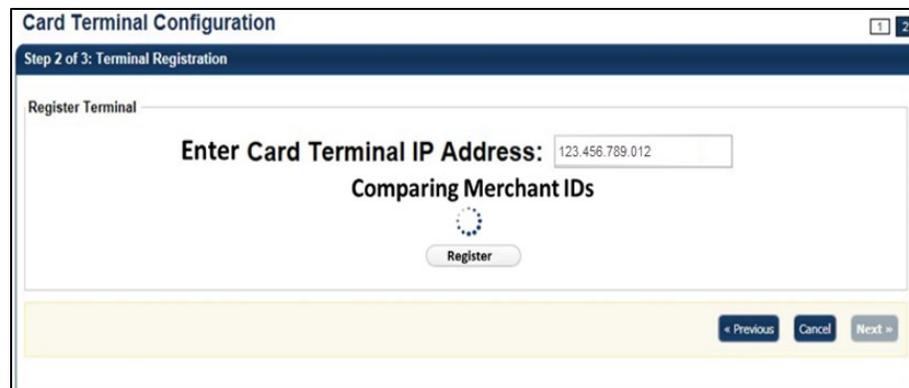

💡 **Application Tips**

- A pairing pin is a unique eight-character OTCnet-generated number used to pair OTCnet and the card terminal.
- It may take 15-20 seconds to receive a pairing pin.
- The pairing pin number is entered on the card terminal.

7. The system compares **Merchant IDs** as shown in Figure 4.

Figure 4. Step 2 of 3: Terminal Registration, Comparing Merchant IDs message

> 💡 **Application Tips**
>
> - A **Merchant ID** is a unique designator assigned by Worldpay to reflect the processing location.
> - Each agency has several Merchant IDs under a single **Chain Code**, to distinguish which agency location processed card transactions.
> - The **Merchant ID** is entered at the lower-level endpoint in OTCnet.

8. The "*Registration Successful!*" message appears. Select **Next**.

9. The "*Connection successful!*" message appears. Select **Next**.

10. *The Step 3 of 3: Review the Terminal Configuration* page appears. Select **Submit** as shown in Figure 5.

Figure 5. Step 3 of 3: Review the Card Terminal Configuration

> 💡 **Application Tips**
>
> - Select the **Edit** hyperlink to modify the information entered.
> - Select the **Unregister** hyperlink to unregister the terminal.

11. The *Confirmation* page appears. View the card terminal configurations, they are automatically populated.

Additional Button

Select **Return Home** to return to the OTCnet Home Page.

Application Tips

- When you try to refund a transaction on the **Card Transaction History Details** page with a different card terminal than the configured card terminal, the following error displays at the top of the screen: *"Registration was not found/valid, or the terminal is offline/busy."*

- When you try to perform a card transaction on the **Process Payment** page with a different card terminal than the configured card terminal, the following error displays at the top of the screen: *"Registration was not found/valid, or the terminal is offline/busy."*

- If you have a terminal model saved in **Card Terminal Configuration** but have a different physical card terminal connected when going through Step 2 of 3 Terminal Registration, the registration will fail with the following error displayed at the top of the screen: *"Card terminal Merchant ID does not match the Merchant ID of the configured endpoint or terminal type does not match the selected type. Please select Previous to restart Terminal Configuration."*

Unregistering a Card Terminal

As a **CA** you are authorized to unregister a card terminal after it has been paired with OTCnet, as needed. At times, you may need to unregister a terminal (i.e., you may want to add a different card terminal to an OTCnet terminal, or you may mistakenly register a terminal and wish to unregister it). First, you must begin the steps to re-register a card terminal before you can unregister it.

To unregister a card terminal, after it's been paired with OTCnet, there are two options:

Option 1: Unregister from the *Registration Successful!* page.

Option 2: Unregister from the Review (*Step 3 of 3: Review the Terminal Configuration*) page.

For Option 1, you will modify your Card Terminal Configuration by selecting an OTC Endpoint and entering the card terminal **IP Address** for the card terminal you wish to register. You will enter the pairing pin in the card terminal. Once the "*Registration Successful!*" message appears, you can unregister the card terminal.

For Option 2, you will modify your Card Terminal Configuration by selecting an OTC Endpoint and entering the card terminal **IP Address** for the card terminal you wish to register. You will enter the pairing pin in the card terminal. Once the "*Registration Successful!*" message appears, and the *Step 3 of 3: Review the Terminal Configuration* page appears, you can unregister the card terminal.

Unregister a Card Terminal

To unregister a card terminal after it's been paired with OTCnet, there are two options:

- **Option 1:** Unregister from the *Registration Successful!* page.
- **Option 2:** Unregister from the Review (*Step 3 of 3: Review the Terminal Configuration*) page.

For Option 1, complete the following steps:

1. From the **Administration** tab, select **Manage Card Processing**>**Card Terminal Configuration**>**Modify**. The *Step 1 of 3: Select OTC Endpoint and Card Terminal Type* page appears.

2. Select an OTC Endpoint. Select **Add**.

3. Select the **Card Terminal Type** and then select **Next**. The *Step 2 of 3: Terminal Registration* page appears.

4. Enter the card terminal **IP Address** in the **Enter Card Terminal IP Address** text box for the card terminal you wish to register, as shown in Figure 6. Select **Register**.

Figure 6: Card Terminal Registration, Enter IP Address

5. OTCnet searches for the pairing pin. Once the pairing pin appears in OTCnet, enter it into the card terminal and press the **green button.** The green button indicates "**OK**" on the card terminal.
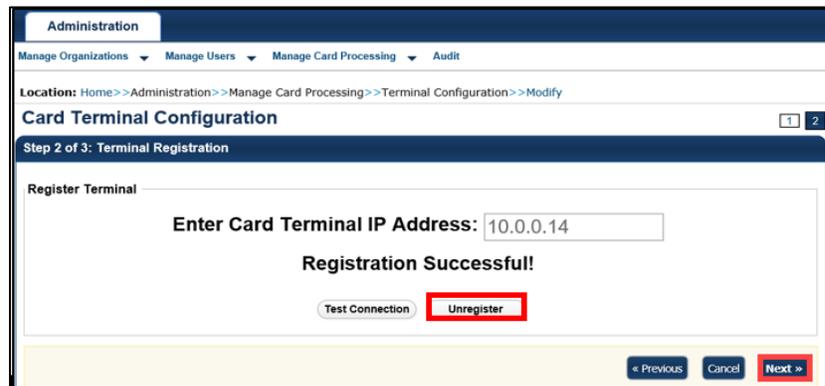
💡 **Application Tip**

It may take 15-20 seconds to receive a pairing pin.

6. The "*Registration Successful!*" message appears. Select **Unregister**, as shown in Figure 7. Then select **Next**.

10

Figure 7: Step 2 of 3: Terminal Registration

7. The "*Terminal unregistered*" message appears.

Additional Buttons

-   Select **Test Connection** to test the pairing connection between the card terminal and OTCnet.
-   Select **Unregister** to unregister the card terminal.
-   Select **Cancel** to terminal registration. A "Registration cancelled" message appears and the terminal registration stops.
-   Select **Previous** to return to the previous page.
-   Select **Return Home** to return to the OTCnet Home Page*.*

For Option 2, complete the following steps:

1. From the **Administration** tab, select **Manage Card Processing**>**Terminal Configuration**>**Modify**. The *Step 1 of 3: Select OTC Endpoint and Card Terminal Type* page appears.

2. Select an OTC Endpoint. Select **Add.**

3. Select **Card Terminal Type**.

4. Select **Next**. The *Step 2 of 3: Terminal Registration* page appears.

5. Enter the **Card Terminal IP Address** for the card terminal you wish to register. Select **Register**. OTCnet searches for the pairing pin.

6. Enter the pairing pin number that appears in OTCnet into the card terminal. Press the **green button.** The green button indicates "**OK**" on the card terminal.

Application Tip

It may take 15-20 seconds to receive a pairing pin.

7. The "*Registration Successful!"* message appears. Select **Next.**

8. The *Step 3 of 3: Review the Terminal Configuration* page appears, as shown in Figure 8. Select **Unregister**.

Figure 8: Step 3 of 3: Review the Terminal Configuration

9. The "*Registration Successful!*" page appears. Select **Unregister**.

10. Select **Next**. The "*Terminal unregistered*" message appears.

Additional Buttons

- Select **Edit** to navigate to the *Step 1 of 3: Select OTC Endpoint* page *and Card Terminal Type* to remove an OTC endpoint or add another available OTC endpoint.
- Select **Unregister** to unregister the card terminal.
- Select **Cancel** to stop terminal registration. A "*Registration cancelled*" message appears and the terminal registration ends.
- Select **Previous** to return to the previous page.
- Select **Return Home** to return to the OTCnet Home Page.

Viewing a Card Terminal Configuration

As a **CA** or **CO,** you are authorized to view a card terminal configuration.

From the *View Card Terminal Configuration* page, the following actions occur:

- OTCnet verifies your OLB connection and the card terminal configuration.
    - This typically takes about 10-15 seconds.
- The card terminal that has been configured appears.

View a Card Terminal Configuration

To view a card terminal configuration, complete the following steps:

1. From the **Administration** tab, select **Manage Card Processing**>**Terminal Configuration**>**View**.

2. The *Card Terminal Configuration View* page appears, as shown in Figure 9.

3. Select **Return Home** to return to the home page.

Figure 9: Card Terminal Configuration View

Topic 3 Searching an Audit Log

The audit log records are interactions between the user and OTCnet. They allow users to search and view audit log entries for the completed audit trail within OTCnet. The audit log is available for download to a *Comma Separated Value* (CSV) report. It opens in a spreadsheet program or can be printed in a formatted audit log report.

If the audit log records contain Personally Identifiable Information (PII), the data is masked in the Transaction Description.

The **CA** and **Card Operator (CO)** are authorized to search audit logs related to card processing activities. The **CCA, Check Card Operator (CCO)**, **Check Card Lead Operator (CCLO)** and **Check Card Supervisor (CCS)** can search audit logs related to check processing activities. Depending on your role, you can search for and view only specific audit logs. See Table 1 for details.

Table 1: Audit Log User Permissions

User Role	Audit Log Access
Check Capture Administrator (CCA)	Partial administration-related activities and all check capture-related activities
Check Capture Operator (CCO)	Own check capture-related activities
Check Capture Lead Operator (CCLO)	Own check capture-related activities
Check Capture Supervisor (CCS)	Partial check capture-related activities pertaining to own actions or actions taken by their CCO or CCLO
FS Viewer or Security Viewer	Administration-related, check capture-related, check processing-related, and deposit processing-related activities
Card Administrator (CA)	Partial administration-related activities and all card-related activities
Card Operator (CO)	Partial access to user's own card-related activities

You can search audit logs by module, user, OTC Endpoint and other search criteria. When running a search without specifying any criteria, by default, the search results include all activities in the system that you have access to view. When running additional searches, the *Search Results* table repopulates with the results of the new search.

Search an Audit Log Online

To search an audit log, complete the following steps:

1. From the **Administration** tab, select **Audit**. The *Search Audit Logs* page appears.
2. Enter your search criteria.

> Under **Search Criteria**, *optional*
>
> - Select a **Module** type
> - Enter a **User**
> - Select an **OTC Endpoint**
> - Enter the **From** and **To** date and time ranges, *required*
> - Select a **Keyword**, *required*
> - Select a **Category Name**, *required*
> - Enter the **Terminal ID**
> - Enter the **Batch ID**
> - Select an **Event Type**
> - Select an **Operation Mode**

Application Tips

- Module drop-down options vary by user role. **Module** options include **Administration**, **Check Capture**, **Check Processing**, **Card Processing**, and **Deposit Processing**.
- The **From** and **To Created On Date** must be entered in **MM/DD/YYYY** format and cannot exceed 30 days.
- The **Keyword** and **Category Name** drop-down options vary by user role. **Operation Mode** options include **All**, **Online**, or **Offline**.

💡 **Application Tip**

Event Types are categories of events that are recorded by the audit log.

Table 2. Event Types

Event Type	Description
All	Includes all event types in the audit log
Error	Error entries are created when the system is unable to complete an action.
Informational	Information entries are general records of the activity that has happened while using OTCnet.
Warning	Warning entries are created to inform the user when events of note have taken place. This includes cancelling an action, deleting information from the system and inactive users.

---

3. Select **Search**. The *Search Results* table appears as shown in Figure 10.

Figure 10. Audit Log Output

💡 **Application Tips**

- Run a search (select a **module type**, **FROM** and **TO** dates, and a **keyword**).
  - The search results include all activities in the system that you have access to view.
  - Run additional searches. The Search Results table repopulates with the results of the new search.
- Select **Download** to download the search results.
- Select **Print Audit Log Records** to print a formatted audit log record.
- If the audit log records contain Personally Identifiable Information (PII), the data is masked.
- An entry in the **audit log** will appear each time a user submits a request to generate a **CIR file status report** asynchronously, when the **scheduled report** is successfully generated, and when the user successfully **downloads** the generated report.

---

4. Select the **Audit Log ID** hyperlink to view additional details for an individual audit log entry. The *View Audit Log Details* page appears as shown in Figure 11.

17

Figure 11: Sample View Audit Log Details Page

Additional Buttons

- Select **Previous** to return to the previous page.
- Select **Return Home** to the OTCnet Home Page.

Topic 4 Selecting an 80mm Card Receipt Printer

As a **Card Operator (CO**), you have the option to choose **Select 80mm Card Receipt Printer.** OTCnet offers the option to select an 80mm Card Receipt Printer for card processing receipts. Receipts are printed on 80mm (3.125 inch) paper.

Before selecting your 80mm printer, ensure that you verify the following:

- Your printer must be installed on your workstation or network. If you do not install the 80mm printer, card receipts are sent to your default Windows printer.

- The OLB is not started. If it is started, you will receive a message that the OLB is running and you cannot access the OLB menu until you stop the OLB.

- You must have the latest OLB version to select the 80mm printer.

If your agency uses check processing and/or deposit processing, check or deposit items print to the Windows default printer, not the 80mm printer.

For additional information about the 80mm printer driver installation process, review the system requirements document (https://www.fiscal.treasury.gov/files/otcnet/OTCnet-SysReq.pdf).

Select an 80mm Card Receipt Printer

To select the 80mm Card Receipt Printer, complete the following steps:
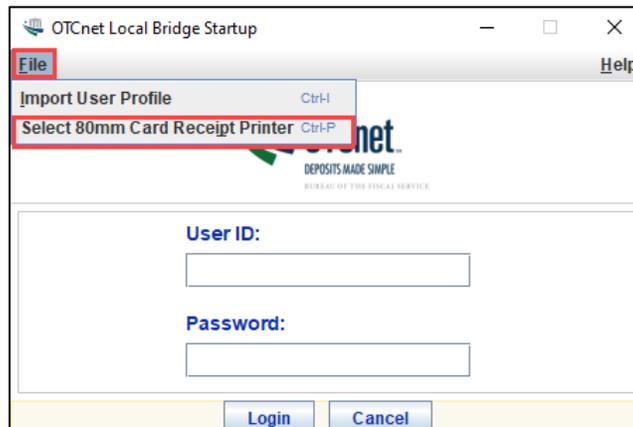
1. Double-select the **Start OTCnet Local Bridge** icon located on the terminal's desktop.

     Or

   Select **Start**>**Programs**>**Start OTCnet Local Bridge**.

2. The *OTCnet Local Bridge Startup* window appears. Select the **File** menu, and select **Select 80mm Card Receipt Printer**, as shown in Figure 12.

Figure 12. Start OTCnet Local Bridge Startup

3. The *Select 80mm Card Receipt Printer* window appears. Select a printer and select **Confirm**, as shown in Figure 13.

Figure 13: Confirm the 80mm Printer
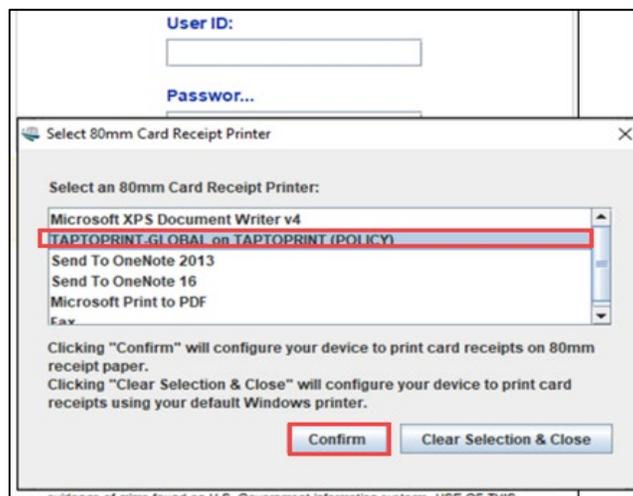
Application Tips

- To cancel your selection (**Select 80mm Card Receipt Printer**), select **Clear Selection & Close** to cancel and close the window.
- A "*The Windows default printer, 'Microsoft Print to PDF,' is used as your card receipt printer*" message appears.

4. The "*You have successfully chosen XXX Printer as your 80mm card receipt printer*" message appears. Select **OK** to return to the OLB Login page.

Application Tips

- In the event that your 80mm printer is no longer available (if your printer drivers are removed from the Window's list of managed printers), the "*Your previously selected 80mm card receipt printer, 'XXX Printer', is no longer available. Card Receipt printing reverts back to using the Windows default printer. Please select an 80mm printer again to enable 80mm card receipt printing*" message appears on the OLB login page.
- Select **Ok**.

Summary

In this chapter, you learned:

- The purpose of configuring card processing settings

- How to set up or modify a card terminal configuration

- How to unregister a card terminal

- How to view a card terminal configuration

- How to search an audit log online

- How to select the 80mm Card Receipt Printer

Chapter 9. Configuring Check Processing Settings

OTCnet Participant User Guide

Table of Contents

List of Figures

List of Tables

Glossary

Select this link to access the full OTCnet Glossary.

Overview, Topics, and Audience

Overview

Welcome to *Configuring Check Processing Settings*. In this chapter, you will learn:

- The purpose of configuring check capture settings
- How to set up or modify a terminal configuration
- How to view a terminal configuration
- How to search an audit log
- How to download and install firmware
- How to create check capture override and online authentication password

Topics

This chapter is organized by the following topics:

1. Purpose of Configuring Check Processing Settings
2. Set Up or Modify a Terminal Configuration
3. Search an Audit Log
4. Download and Install Firmware
5. Create Check Capture Override and Online Authentication Password

Audience

The intended audience for *the Configuring Check Processing Settings* Participant User Guide includes:

View/Modify Configuration Functions

- Check Capture Administrator
- Check Capture Supervisor

View Configuration Only

- Check Capture Lead Operator
- Check Capture Operator

Topic 1 Purpose of Configuring Check Processing Settings Online

Only **Check Capture Administrators (CCA)** and **Check Capture Supervisors (CCS)** are authorized to configure the check processing settings for your Agency terminals. Depending on your user role, you may see all, or only specific check capture activities within your Agency.

Additionally, as a **CCA**, you can manually download or upgrade application software for a terminal (e.g., the OTCnet Local Bridge [OLB] Application) used to communicate between OTCnet and the check capture terminal.

To meet your check capturing for your location, each OTCnet terminal must have configuration settings individually applied. You can add or update the following:

- **System Configuration:** Used to define receipt printing

- **Application Configuration:** Used to define a Terminal ID and processing mode, specify a cashflow method, and to specify batch control and batch control prompts

- **Devices Configuration:** Used to specify the scanner type and communication channel, as well as enable franking

- **Available OTC Endpoints:** Used to add available OTC Endpoints for data entry

- **Configured OTC Endpoints:** Used to set a default OTC Endpoint, review already-configured OTC Endpoints or remove unused OTC Endpoints from the terminal

Topic 2 Setting Up or Modifying a Terminal Configuration

The **CCA** and **CCS** are authorized to configure a check capture terminal. To configure a check capture terminal online, enter your system configuration, add or update your OTC endpoints and verify the terminal configuration. The **Card Administrator (CA)** is authorized to configure a card terminal.

If you are configuring a check capture terminal, you must first start the OTCnet Local Bridge (OLB) application.

The **Scanner Types** table presents a list of the scanners supported by OTCnet. They can be configured to a check capture terminal.

Table 1. Scanner Types

RDM EC7000i	This scanner will automatically scan both sides of a check and can scan in single or batch mode (one or more checks in a batch)
RDM EC9100i	This scanner will automatically scan both sides of a check and can scan in single or batch mode (one or more checks in a batch)
RDM EC9600i	This scanner will automatically scan both sides of a check and can scan in single or batch mode (one or more checks in a batch)
RDM EC9700i	This scanner will automatically scan both sides of a check and can scan in single or batch mode (one or more checks in a batch)
Panini MyVision X	This scanner will automatically scan both sides of a check and can scan in single or batch mode (one or more checks in a batch)
Panini Vision X	This scanner will automatically scan both sides of a check and can scan in single or batch mode (one or more checks at a time)
Panini I: Deal	This scanner will automatically scan both sides of a check and can scan in single or batch mode (one or more checks at a time)

Configuring a Check Capture Terminal Online

To configure a check capture terminal online, enter your system configuration, including **LVD Usage**, **Receipt Printing**, **Application Configuration** and **Devices Configuration** and add or update your OTC endpoints, as needed. Verify the terminal configuration, including **Configured OTC Endpoints**, **System Configuration**, **Application Configuration** and **Devices Configuration**. You can also edit the information.

Configure a Check Capture Terminal Online

To configure a check capture terminal online, complete the following steps:

1. From the **Administration** tab, select **Manage Check Processing**>**Terminal Configuration**>**Modify**. The *Step 1 of 4: Gathering Terminal Information* page may appear briefly. The *Step 2 of 4: Update the Terminal Configuration* page appears.

2. Enter the system configuration and select **Next**. The *Step 3 of 4: Update the Configured OTC Endpoints* page appears.

Under **System Configuration:**
Set **LVD Usage** by, *optional*
- Checking or unchecking **Personal Check** and/or **Non- Personal** for **Customer Present**
- Checking or unchecking **Personal Check** and/or **Non- Personal** for **Customer Not Present**

Application Tip

If you are configuring a check capture terminal and have not started the OTCnet Local Bridge (OLB) application, you will receive the following message: *Terminal detection failed. Please ensure that the OLB application is running*.

Set **Receipt Printing** by, *optional*
- Checking **Customer Present**, *optional*
  - Selecting the **Manual** or **Automatic** radio button
    - Checking **with preview**
- Checking **Customer Not Present**, *optional*
  - Selecting the **Manual** or **Automatic** radio button
    - Checking **with preview**

Application Tips

- Leaving both the **Customer Present** and **Customer Not Present** fields unchecked results in the disabling of this option. If receipts are desired, select the appropriate box(es). When the **Customer Present** and/or **Customer Not Present** fields are selected, the default setting is **Manual**.
  - Select **Manual** to require the operator to take additional steps to print the receipt.
  - Select **Automatic** to print a receipt each time a transaction is entered.
  - Select **with preview** to allow the operator to see the receipt on the screen prior to the generation of the printout.
- When printing receipts, the system prints to the Windows default printer. All receipts print to the Windows default printer.

Under **Application Configuration:**

- Enter the **Terminal ID**

- Select **Single** or **Batch** for Processing mode

- Select **Settle Best Method** or **Truncate All Items** for Cashflow

- Check **Back Office Processing Only**

- Select **Optional** or **Mandatory** for Batch Control

- Select **Prompt on Batch Create** and/or **Prompt on Batch Close** for Batch Control Prompts

Application Tips

- The **Terminal ID** field is available for data entry during initial setup. After the **Terminal ID** is assigned, it is protected and cannot be changed.
- The **Host Name** field is automatically generated based on your computer's registry and cannot be changed.
- The **Single** processing mode allows the user to scan only one check at a time. The **Batch** processing mode allows groups of checks to be scanned all at once, prior to the data entry for the items. The **Batch** processing mode is available for RDM EC7000i, EC9100i, EC9600i, EC9700i and Panini MyVision X, VisionX and I:Deal.
- The **Settle Best Method** is the default selection, and when selected exclusively on the configuration screen, all processing methods (**Customer Present**, **Customer Not Present**, and **Back Office**) are allowed for either personal or non-personal items on the Entry Screen. The **Back Office** processing method must be used by agencies that receive payments in person, then scan the checks at a later time in a controlled, back-office environment. If **Truncate All Items** is selected, only non-personal items are allowed (for all processing methods) on the entry screen.
- If the **Batch Control** is set to **Optional**, OTCnet prompts the user to use the batch control. If the **Batch Control** is set to **Mandatory**, OTCnet prompts for batch control totals.

Under **Devices Configuration:**

- Select the **Scanner** model, *required*
- Select **USB Port** or **Serial Port**, *required*
- Select the Serial Port type
- Check **Franking Enabled**, *optional*

Application Tips

- **USB Port:** RDM EC7000i, EC9100i, EC9600i, EC9700i, Panini MyVision, Panini VisionX, and Panini I: Deal scanners require a USB port communication channel. RDM EC7000i scanners support USB and Serial communication channels.
- **Serial Port and COM dropdown:** The user selects the serial port (i.e., COM port) where they have connected a serial scanner.
- **USB-to-Serial adapters:** USB-to-serial adapters are not supported. RDM EC7000i scanners support USB and Serial communication channels.
- A "*No Serial Ports are available for configuration*" message displays if a Serial Port is not available for the terminal. A "*No Serial Ports are available for configuration*" message does not display if the terminal has a COM port enabled or if there is a COM port enabled, and there is no physical Serial Port.
- The **Franking Enabled** option allows the scanner to automatically stamp the front of checks. Franking is available for RDM EC7000i, EC9100i, EC9600i, EC9700i, and Panini I: Deal scanners.

3. Add or remove the OTCnet endpoint(s) that perform check scan, designate a default OTC Endpoint, and select **Next** as shown in Figure 1. The *Step 4 of 4: Review the Terminal Configuration* page appears.

   Under **Available OTC Endpoints:**
   - Select the **OTC Endpoint(s)** you want to **Add** by checking the box(es) under the **Add** column, and selecting **Add**

   Under **Configure OTC Endpoint:**
   - Select a **Default OTC Endpoint**, *required*

   - Select the OTC Endpoint(s) you want to **Delete** by checking the box(es) under the **Remove** column, and selecting **Remove**, *if applicable*

Figure 1. Step 3 of 4: Update the Configured OTC Endpoints

Application Tips

- The OTC Endpoints are permission-based and are only visible to users with the appropriate permissions. At least one **Default OTC Endpoint** is required per terminal. While a default is chosen, it does not prevent you from scanning against another configured **OTC Endpoint**.
- Selecting a **Default OTC Endpoint** determines which OTC Endpoint to use when performing Check Scan actions.
- Multiple OTC Endpoints can be selected, but only one can be set as a **Default OTC Endpoint**.

4. Verify the Terminal Configuration is correct and select **Submit**. Select **Edit** to modify the information entered. A *Confirmation* page appears stating that the Terminal Configuration record has been updated.

Additional Buttons

- Select **Cancel** to return to the OTCnet Home Page. No data is saved.
- Select **Previous** to return to the previous page.
- Select **Return Home** to return to the OTCnet Home Page.

Viewing Terminal Configuration

The **CCA**, **CCS**, **Check Capture Lead Operator (CCLO)** and **Check Capture Operator (CCO)** are authorized to view check terminal configuration details for each terminal configured.

Terminal configuration details include the following:

- **OTC Endpoint Configuration:** OTC Endpoints and default OTC Endpoint
- **System Configuration:** Receipt printing
- **Application Configuration:** Terminal ID, host name, processing mode, cashflow method, batch control and batch control prompts
- **Devices Configuration:** Scanner type, communication channel, and franking

You can view the terminal configuration from the *View Terminal Configuration* page.

View Terminal Configuration

To view the terminal configuration, complete the following steps:

1. From the **Administration** tab, select **Manage Check Processing**>**Terminal Configuration**> **View**.

2. The *View* page appears as shown in Figure 2.

Figure 2. View Terminal Configuration Page

Additional Button

Select **Return Home** to go to the OTCnet Home page.

Topic 3 Searching an Audit Log

The audit log records are interactions between the user and OTCnet. They allow users to search and view audit log entries for the completed audit trail within OTCnet. The audit log is available for download to a *Comma Separated Value* (CSV) report and opened in a spreadsheet program or available to print in a formatted audit log report.

If the audit log records contain Personally Identifiable Information (PII), the data is masked in the Transaction Description. To view more details about a specific batch, including PII, access **Batch Management**.

The **CCA**, **CCO**, **CCLO**, and **CCS** are authorized to search audit logs related to check processing activities. The **CA** and **Card Operator (CO)** are authorized to search audit logs related to card processing activities. Depending on your role, you can search for and view only specific audit logs. See Table 2 for more details.

Table 2. Audit Log User Permissions

User Role	Audit Log Access
Check Capture Administrator (CCA)	Partial administration-related activities and all check capture-related activities
Check Capture Operator (CCO)	Own check capture-related activities
Check Capture Lead Operator (CCLO)	Own check capture-related activities
Check Capture Supervisor (CCS)	Partial check capture-related activities pertaining to own actions or actions taken by their CCO or CCLO
FS Viewer or Security Viewer	Administration-related, check capture-related, check processing-related, and deposit processing-related activities
Card Administrator (CA)	Partial administration-related activities and all card-related activities
Card Operator (CO)	Partial access to user's own card-related activities

You can search audit logs by module, user, **OTC Endpoint**, and other search criteria (created on date, batch ID, event type, etc.). If you run a search without specifying any criteria, by default the search results include all activities in the system that you have access to view. If you run additional searches, the *Search Results* table repopulates with the results of the new search.

Searching an Audit Log Online

To search an audit log, enter your search criteria—including module options (**Administration Check Capture** and **Check Processing), User, OTC Endpoint, From** and **To** dates, **Keyword (All** or make your selection from the list, i.e., **Application Exception, Batch Management**, etc.) and **Category Name (All** or make your selection from the list, i.e., **Accept Duplicate, Access**, etc.), **Terminal ID, Batch ID** and **Event Type (Error, Information** and **Warning)**, and **Operation Mode (All**, **Online**, or **Offline).**

Select your Audit Log ID hyperlink to view additional details for an individual audit log entry. Download and print your formatted audit log record, including the **Audit Log Record Summary**; **Audit Log ID**, **Created On**, **Context**, **User Email Address, OTC Endpoint**, **Terminal ID**, **Batch ID**, **Transaction Description**, **Module** and **Event Type**, **Audit Log Attribute Info**, **User Name** and **Audit Log Field Info**. You can also view your audit log details.

Search an Audit Log Online

To search an audit log, complete the following steps:

1. From the **Administration** tab, select **Audit**. The *Search Audit Logs* page appears.
2. Enter your search criteria.

Under **Search Criteria**, *optional*

- Select a **Module** type
- Enter a **User**
- Select an **OTC Endpoint**
- Enter the **From** and **To** date and time ranges, *required*
- Select a **Keyword**, *required*
- Select a **Category Name**, *required*
- Enter the **Terminal ID**
- Enter the **Batch ID**
- Select an **Event Type**
- Select an **Operation Mode**

Application Tips

- Module drop-down options vary by user role. **Module** options include **Administration**, **Check Capture**, **Check Processing, Card Processing,** and **Deposit Processing.**
- The **From** and **To Created On Date** must be entered in MM/DD/YYYY format and cannot exceed 30 days.
- The **Keyword** and **Category Name** drop-down options vary by user role.
- **Operation Mode** options include **All**, **Online**, or **Offline**.

💡 **Application Tip**

Event Types are categories of events that are recorded by the audit log.

Table 3. Event Types

Event Type	Description
All	Includes all event types in the audit log
Error	Error entries are created when the system is unable to complete an action.
Informational	Information entries are general records of the activity that has happened while using OTCnet.
Warning	Warning entries are created to inform the user when events of note have taken place. This includes cancelling an action, deleting information from the system and inactive users.

3. Select **Search**. The *Search Results* table appears as shown in Figure 3.

Figure 3. Audit Log Output

💡 **Application Tips**

- Run a search (select a **module type**, **FROM** and **TO** dates, and a **keyword**).
  - o The search results include all activities in the system that you have access to view.
  - o Run additional searches. The Search Results table repopulates with the results of the new search.
- Select **Download** to download the search results.
- Select **Print Audit Log Records** to print a formatted audit log record.
- If the audit log records contain Personally Identifiable Information (PII), the data is masked.
- An entry in the **audit log** will appear each time a user submits a request to generate a **CIR file status report** asynchronously, when the **scheduled report** is successfully generated, and when the user successfully **downloads** the generated report.

4. Select the **Audit Log ID** hyperlink to view additional details for an individual audit log entry. The *View Audit Log Details* page appears as shown in Figure 4.

Figure 4: Sample View Audit Log Details Page

- Select **Previous** to return to the previous page.
- Select **Return Home** to the OTCnet Home Page.

Topic 4 Downloading and Installing Firmware

Downloading Firmware

If you are assigned the role of **CCA**, you are authorized to manually download check capture application firmware. The firmware "release" allows for the initial download or upgrades to the scanner software that enables a scanner to be used on a terminal. The firmware version you install also contains a series of other back-end installation files that must be used on a terminal to enable it to be used for Check Capture in OTCnet.

Prior to each firmware upgrade, the currently installed firmware must be uninstalled.

Additionally, firmware upgrades are operating system- (Windows 11 or Windows 10) and scanner- (e.g., RDM EC7000i, EC9100i, EC9600i, EC9700i, Panini I;Deal, Panini MyVision, or Panini Vision X) specific. Note: Firmware versions 4.3.0 and 4.4.0 are only compatible with OLB versions 2.3.0 and above. Firmware version 4.4.0 or higher is required for the RDM EC9600i and EC9700i scanner models.

Therefore, downloading and executing the correct firmware upgrades ensures that a terminal and scanner are functioning properly. To determine firmware upgrades by firmware version, scanner, and operating system, refer to the *OTCnet System Requirements and Reference Guide* at: https://fiscal.treasury.gov/files/otcnet/otcnet-sys-req.pdf.

If an agency (OTC Endpoint) has multiple terminals and requires more than one firmware due to varying workstation requirements, download and execute the firmware for each terminal.

You must download firmware using **Download Release**, selecting **Firmware** and saving the file to your chosen location.

Download Firmware

To download firmware, complete the following steps:

1. From the **Administration** tab, select **Manage Centralized Deployment** >**Download Release**.

2. From the **Application** drop-down menu, select **Firmware**.

3. Select **Next**. The *Select Firmware for Download* page appears.

Application Tips

- Prior to each firmware upgrade, the currently installed firmware version must be uninstalled.
- Firmware upgrades are operating system- (e.g., Windows 11 or Windows 10) and scanner- (e.g., EC7000i, EC9100i, EC9600i, EC9700i, Panini MyVision X) specific.
- Each firmware version has a corresponding terminal configuration that it supports (by scanner and by operating system). Determine the appropriate firmware upgrade by firmware version, scanner, and operating system before downloading.

4. Select the **Firmware** hyperlink to download the firmware. The *Review Firmware Download* page appears.

5. Select **Download** as shown in Figure 5. The *Save Program* dialog box appears.

Figure 5. Review Firmware Download

6. Select **Save** or **Cancel**.

Application Tips

- Select **Save** to choose the location where you want to save the file.
- Select **Cancel** to return to the *OTCnet Check Capture Application Download* page without saving the file.

Additional Buttons

- Select **Previous** to return to the previous page.
- Select **Return Home** to return to the OTCnet Home page.

Installing Firmware

After the **CCA** downloads the firmware, the next step is to install the firmware (this must be done for each terminal). This can be completed by the **CCA**, **CCS**, **CCLO**, and **CCO**. However, before you install the firmware, consider the following information:

- You must have Windows Administrator privileges to install the firmware.

- Ensure the scanner is not connected to the terminal as it may cause scanner connectivity issues.

- If a previous version of firmware is installed, uninstall it before installing the new firmware version. See the *Install OTCnet Firmware* printable job aid for specific directions.

- Firmware version 4.3.0 supports the RDM EC7000i, RDM EC9100i, Panini MyVisionX, Panini Vision X, and Panini I: Deal scanners. Firmware version 4.4.0 supports the RDM EC9600i and RDM EC9700i scanners.

For Windows 11 and Windows 10:

1. Access your Control Panel under **Start** > **Window Systems** > **Control Panel**
2. Select **Programs** > **Uninstall Programs**
3. In the **Currently installed programs** box, select **OTCnetFirmware**
4. Select **Remove**
5. Select **Yes** and wait while the Firmware uninstalls

Verify the **OTCnetFirmware** and **Panini** X.X.X **Universal Installer** automatically uninstalled.

For more information about the firmware version that matches the terminal settings, refer to the *OTCnet System Requirements and Reference Guide* at: https://fiscal.treasury.gov/files/otcnet/otcnet-sys-req.pdf.
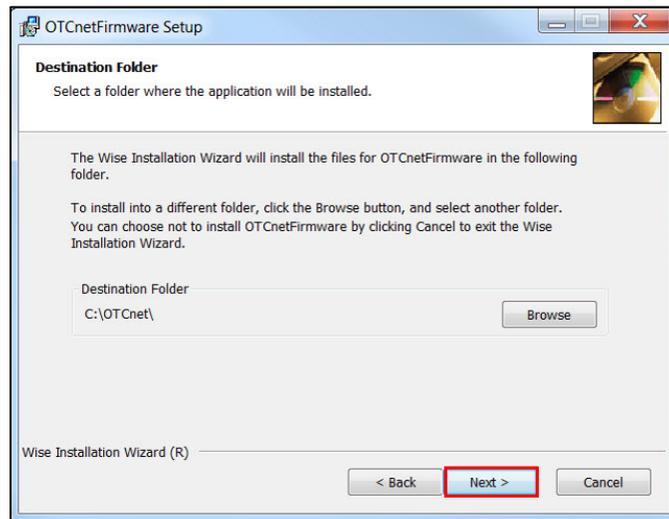
To install firmware, install the firmware file (MSI file).

18

Install Firmware

To install OTCnet firmware, complete the following steps:

1. Locate the folder where the firmware file (MSI file) resides and double-select the file to start the installation. The *Welcome to the OTCnet Firmware Installation Wizard* dialog box appears.

2. Select **Next**. The *User Information* dialog box appears.

3. Select **Next**. The *Destination Folder* dialog box appears as shown in Figure 6.

Figure 6. Destination Folder Dialog Box

Application Tip

To install the firmware to another folder destination, select **Browse** to select a different folder. Select **Cancel** to exit the setup.

4. Select **Next**. The *Ready to Install the Application* dialog box appears.

5. Select **Next**. Wait a moment while the files install.

Application Tip

During the installation process for OTCnet Firmware, you can continue to use their workstations. However, OTCnet and all related activities are unavailable until the installation of the Firmware is complete.

The installation time can vary from workstation to workstation. Users can expect a duration of up to 30 minutes to complete full installation. Do not close the installation window until the installation is complete.

6. The *OTCnet Firmware has been successfully installed* message appears. Select **Finish**.

Topic 5 Creating Check Capture Override and Online Authentication

In OTCnet, the following user roles can create check capture override and online authentication password:

- Check Capture Administrator (CCA)

- Check Capture Lead Operator (CCLO)

- Check Capture Supervisor (CCS)

The Primary/Local Security Administrator (P/LSA) must create the OTCnet online user identity.

Additionally, this user identity must also be successfully provisioned and approved, and a password must be provided.

Creating Check Capture Override and Online Authentication Password

From the **Administration** tab, select **Manage Users**>**Create Check Capture Override and Online Authentication Password**. Enter and confirm your **password**, then select the **Submit** button. A **Confirmation** page displays stating that you have successfully created your **Check Capture Override and Online Authentication password**. Select **OK** to return to the *OTCnet homepage.*

Create Check Capture Override and Online Authentication Password

To create check capture override and online authentication password, complete the following steps:

1. From the **Administration** tab, select **Manage Users**>**Create Check Capture Override and Online Authentication Password**. The **Create Password** screen displays as shown in Figure 7.

2. Enter and confirm your **password**.

💡 **Application Tip**

The **Check Capture Administrator, Check Capture Supervisor, and Check Capture Lead Operator** can create an online authentication password. The password must satisfy the following requirements:

- Must be at least 12 characters long.
- Must not be longer than 64 characters.
- Must not have more than two repeating characters.
- Must not be a word in a language, slang, dialect, or jargon.
- Must not be related to personal identity, history, environment, or other personal associations.
- Must not be shared or displayed in plain view.

3. Select the **Submit** button to process the data.

Figure 7: Create Check Capture Override and Online Authentication Password

> 🖱️ **Additional Buttons**
>
> If your **password** does not comply with the Fiscal Service password policy requirements, you will get an error message to try again. The password requirements will be displayed on the screen.

4. A **Confirmation** page displays, as show in Figure 8, stating that you have successfully created your **Check Capture Override and Online Authentication Password**.

5. Select **OK** to return to the *OTCnet Homepage*.

Figure 8: Confirmation Page (Check Capture Override/Online Authentication)

Summary

This chapter provided information on:

- The purpose of configuring check processing settings
- How to set up or modify a terminal configuration
- How to view a terminal configuration
- How to search an audit log
- How to download and install firmware
- How to create check capture override and online authentication password