Santander Commercial Banking

May 2025

Santander Commercial Card

Smart Data Account Manager Guide

For Program Administrators

Contents

1 Introduction 3

2 Where to go for What 4

3 Program Terminology 6

4 Company Program Administrator...7

4.1 Role of a Company Program Administrator 7

4.2 Granting Smart Data Account Manager Administration Permissions 7

5 Getting Started with Smart Data Account Manager – Company Program Administrators..........9

6 RSA SecureID Token for Two Factor Authentication.. 11

6.1 Initial Set Up - Phone.. 11

6.2 Initial Set Up - Desktop... 13

6.3 Resetting users' Multifactor Authentication.. 16

6.4 Common Issues with Tokens.. 17

7 Company Registration Code.. 18

8 User Administration 19

8.1 Reset User's Password / Unlock User 19

8.2 Update a User's Contact Details 21

8.3 Adding a New User / Access and Security Profiles.. 22

9 Account Management.. 25

9.1 Searching for an Account 25

9.2 Activate cards.. 26

9.3 Making Edits to a Card Account 26

9.4 Ordering a Replacement Card.. 28

9.5 Temporary Credit Limit 29

9.6 Creating a New Card Account 30

10 Statement and Transactions... 35

10.1 Downloading a Statement 35

10.2 Viewing and Downloading Transactions and Authorizations 36

11 Billing and Payments 38

11.1 Program Billing.. 38

11.2 Program Payment 38
11.3 38
11.4 Making a Payment 38
12 Disputing a Transaction 40
13 Cardholder Self Service 41
13.1 Fraud Alerts 41
13.2 Card holder Self Registration on Smart Data 42
13.3 Cardholder Card Activation and PIN Setting 44
13.4 Resetting Verification ID 44
13.5 Lost or Stolen Cards 45
14 Fraud Best Practice Controls 46
15 Reports 47

1 Introduction

This guide explains how to perform key tasks as a Santander Commercial Card Program Administrator (PA). There are many self-service tasks on the Smart Data Realtime Account Manager (SDRAM) application and there are other times when you will need to contact us for assistance.

This guide explains:

- Who to contact for each eventuality you may come across as a Program Administrator.
- Step-by-step instructions on various Program Administrator tasks for SDRAM
- Guidance for cardholder self-service tasks.
- Information on Billing, Payments, and Disputes
- Best Practice for reducing declined transactions and managing fraud.

Separate Guides are available for our Expense Management, Virtual Card, and Travel programs. You can request these from Client Service:

Santander Client Service is open for Program Administrators:

Monday – Friday 7:30 AM – 5:00 PM ET

For Program Administrator service after hours: 877-598-7799

Email: clientservice@santander.us

2 Where to go for What

Common Tasks	Smart Data Account Manager	Automated Voice System	Program Admin Phone Support	Program Admin Email support	Relationship Management
	www.smartdata.santanderbank.com	877-598-7799 24/7	844-726-0095 For service after hours: 877-598-7799	clientservice@santander.us Mon-Fri, business hours	RM / Cash Management Sales Officer
Card Activation		✓			
Select or Change Card PIN		✓			
Onetime payment		✓(No fee)	✓ (Fee)		
Account Balance	✓	✓	✓		
Account Available Credit	✓	✓	✓		
Declined Transactions	✓		✓		
User Password Reset / Login Assistance	✓		✓		
Cardholder Address / Phone Change	✓		✓		
Adding or Removing Company Program Administrator	✓		✓		
Change of Bulk Shipment Address for Cards			✓		
Security Profile Administration	✓		✓		
Transaction Inquiry	✓		✓	✓	
Account Status	✓		✓	✓	
Temporary Blocks on Cards	✓		✓	✓	
Statements	✓		✓	✓	
Merchant Code Blocks	✓		✓	✓	
Cardholder Name Change	✓		✓	✓	
Technical Help Assistance with Self-Service Tasks	✓		✓	✓	
File Delivery Issues e.g., Missing Files, Data Transmission Issues			✓	✓	
New Corporate Account			✓	✓	
Reallocate Corporate Account Credit Limits			✓	✓	
Change Deposit Account for Payments and/or Rebates			✓	✓	

Common Tasks	Smart Data Account Manager	Automated Voice System	Program Admin Phone Support	Program Admin Email support	Relationship Management
Change of Company Details			✓	✓	
Billing Cycle Changes			✓	✓	
Bulk Cardholder Applications			✓	✓	
Bulk Cardholder Maintenance			✓	✓	
Virtual Card Supplier Maintenance			✓	✓	
Rebate Queries					✓
Issue Virtual Cards					✓
Company Credit Line Increases					✓
Supplier enablement program					✓
Not Sufficient Funds for Payment					✓
Integrated Payable Platform – Enterprise Payment Link					✓
Program Closure					✓

For all questions relating to MasterCard Liability Waiver and MasterCard Benefits, to request MasterCard Assist Services or to file a claim, call 1-800-MasterCard (1-800-627-8372).

3 Program Terminology

Units and Hierarchy

A unit is a single node on your company's hierarchy. In the example below, the company, New England Equipment Inc, has three units reporting into the top 'SuperCorporate' unit in the hierarchy.

	Type	Level	Examples
Unit	SuperCorporate	Level 1: 010	New England Equipment Inc
Unit	Corporate	Level 2: 020	North Sales Team
Unit	Corporate	Level 2: 020	South Sales Team
Unit	Corporate	Level 2: 020	Virtual Card Purchasing
Unit	Individual	Level 3: 030	Sally Smith

- Statements and billing are made a Level 2 for all corporate bill programs.
- Hierarchies can be as simple or as complex as your company needs. We will work with your Program Administrator at onboarding to define and create your company's hierarchy.

A Corporate account can only have cards with one product type, i.e., one of:

- OneCard – general purpose card
- T&E – Travel and Entertainment
- Purchase
- Virtual Purchase
- Virtual Travel

If you need more than one product type, you need to have more than one corporate account.

Account Holders and Program Administrator

Account Holders and Program Administrators are SDRAM 'Users' and are not included in the hierarchy.

- An Account Holder is associated with one or more accounts and can view statements for the account. If the program is Individual Bill, the cardholder may make payments on the account.
- A Program Administrator is associated with one or more units on the hierarchy and has administrative access to that unit and lower units. The Program Administrator may or may not also be an Account Holder.

4 Company Program Administrator

4.1 Role of a Company Program Administrator

A Company Program Administrator:

- Can manage all the card accounts for the units they have been permissioned for.
- Is responsible for managing administrative rights for the units they have access to.
- Can designate other Company Program Administrators by giving them the Company Program Administrator role in Smart Data Account Manager.
- Can contact Client Service on behalf of any company for the units they have been permissioned for (except for fraud claims which need to be made by the cardholder).
- Is the company representative and contact point for Santander and will receive all Commercial Card program communications.

4.2 Granting Smart Data Account Manager Administration Permissions

Each company must have at least one Company Program Administrator who has full access to the company's accounts in Smart Data Account Manager and can assign administrative privileges to other users. Company Program Administrators can create other Company Program Administrator roles in Smart Data, as well as other users with other security profiles. Users can be assigned to all or just some points in the company's hierarchy. See Section 8.4 for step-by-step instructions on setting up Smart Data users.

These are the standard security profiles Company Program Administrators can choose from when setting up new Smart Data Account Manager users.

Security Access Role	Permissions
Company Program Administrator	Full Company Program Administrator rights for all units they have been given access to.
Level Manager	A user who has access to certain Org Points rather than the whole company hierarchy.

Security Access Role	Permissions
Account Holder	Standard account holder.

A Company Program Administrator can be given permissions to setup bespoke profiles. To have this feature enabled for you or to discuss options call the number on the back of your cards or Client Service on 877-598-7799 or email a request to clientservice@santander.us.

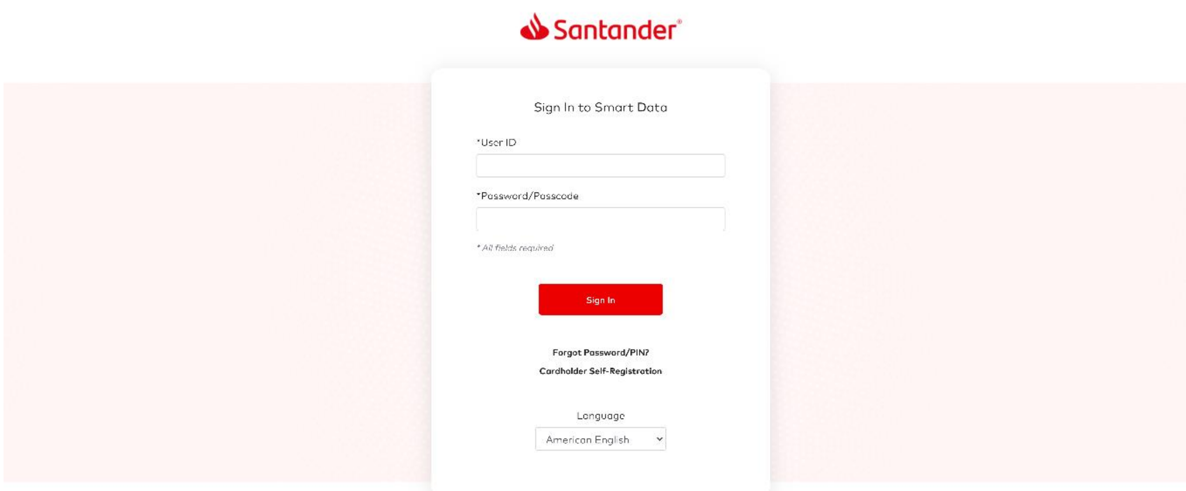
NOTE: If you request this capability and alter a Company Program Administrator profile, be aware that Client Service will service all callers with a Company Program Administrator profile, irrespective of what permissions you have added or taken away. If you do not want the users to call Client Service, you must give them profiles with different names.

If a company doesn't have a Program Administrator and needs to set one up, the company will need to complete the Santander Commercial Card Program Administrator Request Form. The form can be requested from Client service on 877-598-7799 or email clientservice.santander.us

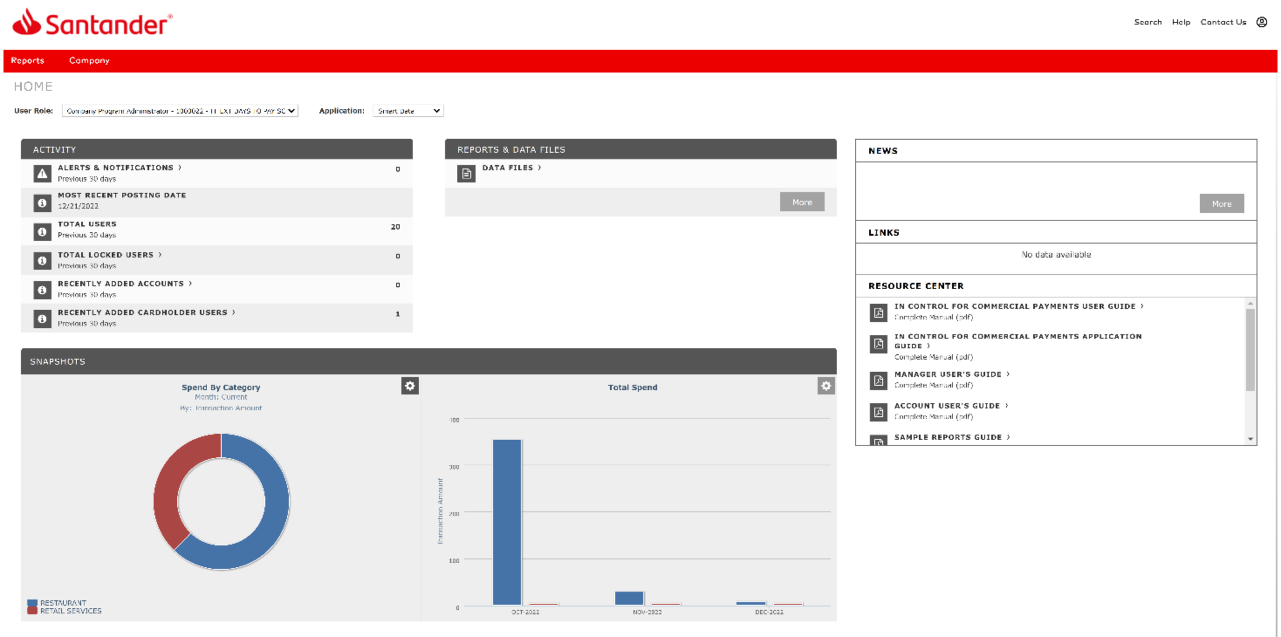
5 Getting Started with Smart Data Account Manager – Company Program Administrators

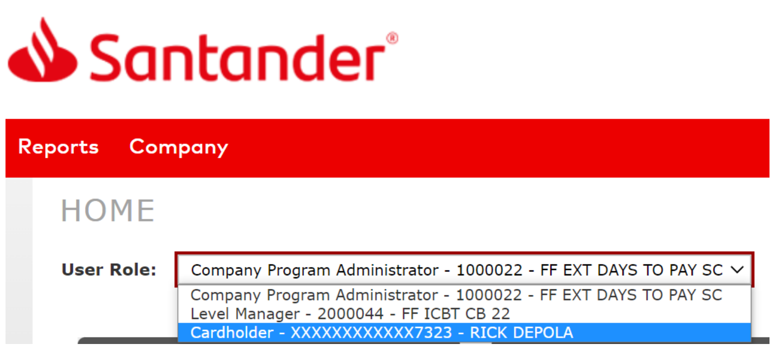
As a Company Program Administrator, you will be sent two emails, one with your username and one with your password for Smart Data (cardholders are able to self-register).

After receiving your credentials: smartdata@santanderbank.com

	Action/Information
1	Enter the username and password and then set up a new password and security question. 

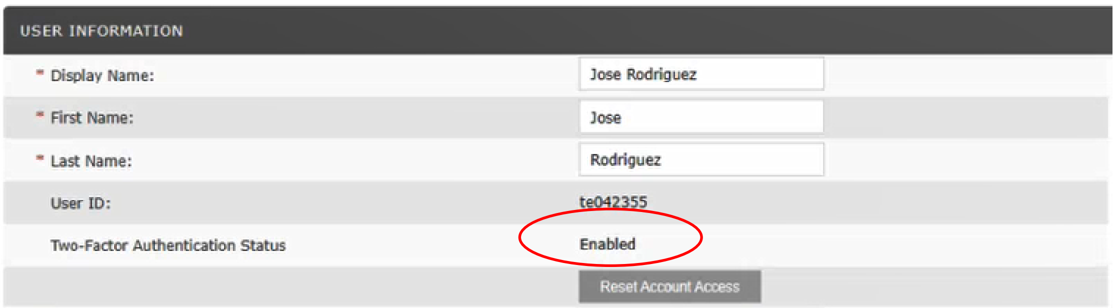
<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>2</td><td>You will then arrive at the landing page.


</td></tr>
<tr><td>3</td><td>If you have more than one security role you can toggle between them from the dropdown box. To return to the home screen click on the Santander logo from any page.


</td></tr>
</table>

6 RSA SecureID Token for Two Factor Authentication

Users who can either create Virtual Cards or order new physical cards must have Two Factor Authentication enabled. You will see whether this has been applied in a user's profile under **Two-Factor Authentication Status**.



USER INFORMATION	
* Display Name:	Jose Rodriguez
* First Name:	Jose
* Last Name:	Rodriguez
User ID:	te042355
Two-Factor Authentication Status	Enabled
	Reset Account Access

Smart Data uses a token for Two-Factor Authentication. This token can either be download to your phone or desktop.

6.1 Initial Set Up - Phone

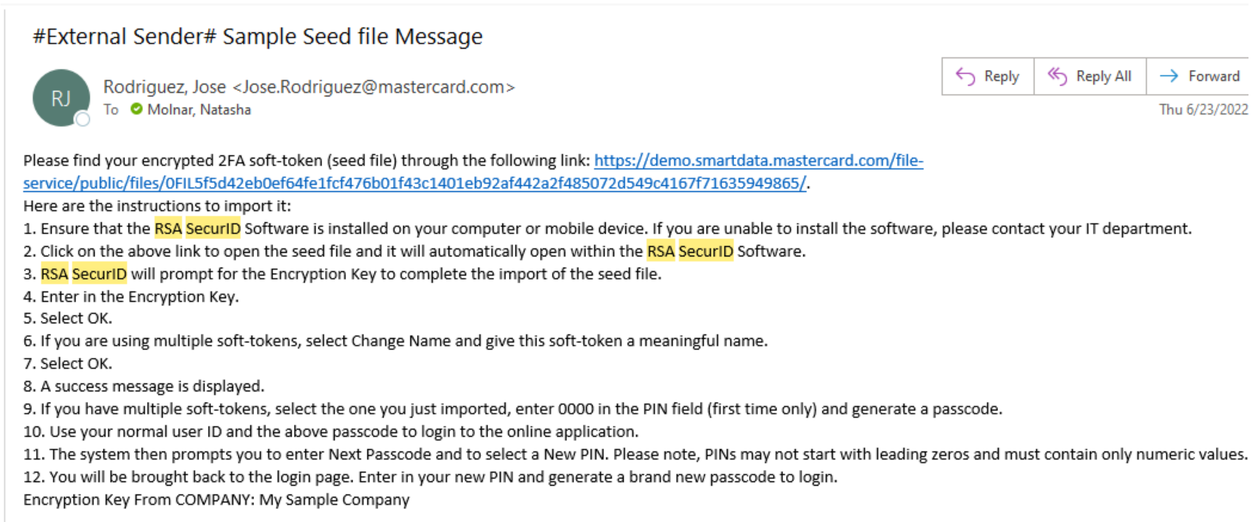
The token can be loaded on a phone or desktop, but it is ONE OR THE OTHER, you cannot use a desktop and your phone.

To have the token on your phone, download the SecurID app to your Android or Apple Device. The icon in the Apple or Google Play Store is:

Smart Data must be open on your desktop to enable the soft token on your phone

- https://www.smartdata.santanderbank.com

A seed file will be emailed from the following address smartdatahelp@mastercard.com. It will look like this:



#External Sender# Sample Seed file Message

Rodriguez, Jose <Jose.Rodriguez@mastercard.com>
To Molnar, Natasha

Reply | Reply All | Forward
Thu 6/23/2022

Please find your encrypted 2FA soft-token (seed file) through the following link: https://demo.smartdata.mastercard.com/file-service/public/files/0FIL5f5d42eb0ef64fe1fcf476b01f43c1401eb92af442a2f485072d549c4167f71635949865/.
Here are the instructions to import it:
1. Ensure that the RSA SecurID Software is installed on your computer or mobile device. If you are unable to install the software, please contact your IT department.
2. Click on the above link to open the seed file and it will automatically open within the RSA SecurID Software.
3. RSA SecurID will prompt for the Encryption Key to complete the import of the seed file.
4. Enter in the Encryption Key.
5. Select OK.
6. If you are using multiple soft-tokens, select Change Name and give this soft-token a meaningful name.
7. Select OK.
8. A success message is displayed.
9. If you have multiple soft-tokens, select the one you just imported, enter 0000 in the PIN field (first time only) and generate a passcode.
10. Use your normal user ID and the above passcode to login to the online application.
11. The system then prompts you to enter Next Passcode and to select a New PIN. Please note, PINs may not start with leading zeros and must contain only numeric values.
12. You will be brought back to the login page. Enter in your new PIN and generate a brand new passcode to login.
Encryption Key From COMPANY: My Sample Company

Preparation:

Make sure you have completed all these steps before you begin to set/reset your RSA soft token:

1) Have Smart Data open on your computer: https://smartdata.santanderbank.com.

2) Make sure you know your Smart Data User ID. If you do not know your User ID, contact our client service team on 844 726 0095, Mon-Fri 07:30AM – 5:00 PM EST

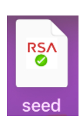
3) Have the email referenced above open on your phone (or computer if not using phone app).

4) Have the **RSA Authenticator** app downloaded to your phone (or desktop). The application icon in the App Store or Google Play, will look like this:

5) Have your company's Encryption Key available.

- Look out for a secure email with "SecureThisMessage" in the subject line which will contain your Encryption Key.

- Delete any previous seed files downloaded for the RSA app from your downloads on your phone or computer. If you are on a phone, open the **Files** app, go to the **Downloads** folder, and delete any **RSA seed** files. They will look like this:



Steps to set soft token:

1) If using the RSA app for the first time, open the RSA app and click **Get Started.**
2) In your mail app: Click on the 2FA soft-token (seed file) link in the email you received.
   - Usually, this will automatically open the RSA app on your phone (or RSA SecurID on your computer)
   - If not, follow the prompts to download the seed file. Go to the saved seed file (you will find this in your downloads folder) and click on the seed file icon. This will open the
3) In the RSA app: When prompted for a password, enter the Encryption Key provided by Santander. Select OK
4) In the RSA app: Enter **0000** in the PIN field and an 8-digit passcode will appear.
5) In Smart Data: Enter your User ID and the above 8-digit passcode to login.
6) In Smart Data: Follow the prompts to create a New PIN and enter the *next* 8-digit passcode from the RSA app.
   - *Wait* for the first passcode on the screen to expire and use the second one that appears.
   - PINs may not start with leading zeros and must contain only numeric values.
7) Close the RSA app and reopen it.
8) In the RSA app: Enter the New PIN you just created.
9) In Smart Data: Login using your User ID, and the *next* 8-digit passcode generated in the RSA app.
   - *Wait* for the first passcode on the screen to expire and use the second one that appears.
   - If you receive the Smart Data error, Invalid Login, please attempt to login up to 3 times.

9. If you are unable to access Smart Data after following these steps, please call us on 844 726 0095, Mon-Fri 07:30AM – 5:00 PM EST.

6.2 Initial RSA Set Up - Desktop

The token can be loaded on a phone or desktop, but it is ONE OR THE OTHER, you cannot use a desktop *and* your phone.

To have the token on your desktop, install the application from the RSA website:

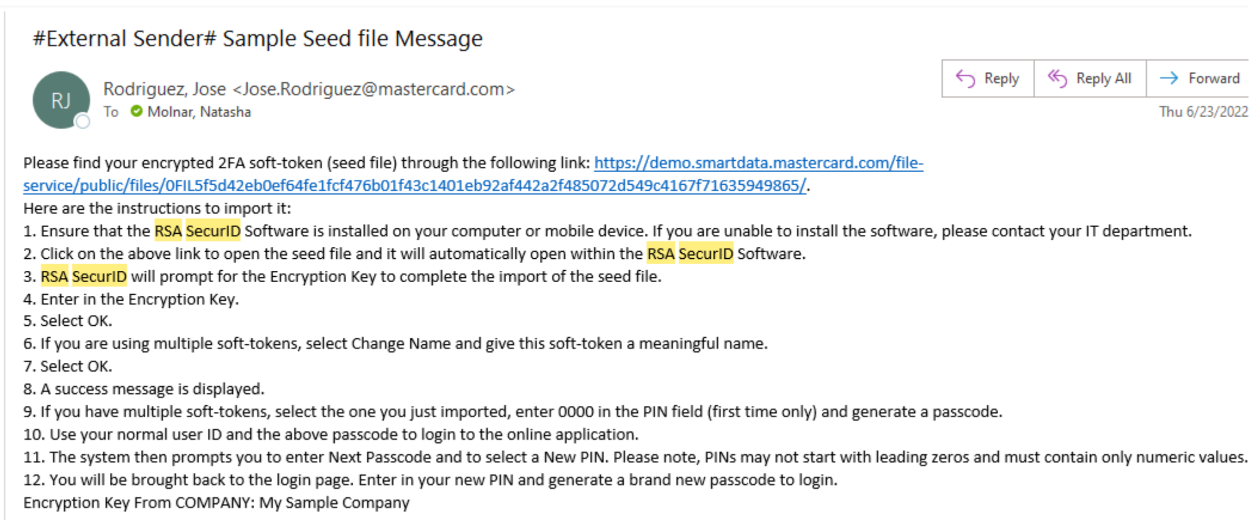
https://community.rsa.com/t5/securid-software-tokens/ct-p/securid-software-tokens

You may need to consult your IT Department if your company usually blocks downloads from websites.

Smart Data must be open on your desktop to enable the soft token

- https://www.smartdata.santanderbank.com

You will have received an email with a link for a Seed File from smartdatahelp@mastercard.com. Click on the link within the email to download the Seed file and follow the steps in the email



#External Sender# Sample Seed file Message

RJ Rodriguez, Jose <Jose.Rodriguez@mastercard.com>

To Molnar, Natasha

Reply | Reply All | Forward

Thu 6/23/2022

Please find your encrypted 2FA soft-token (seed file) through the following link: https://demo.smartdata.mastercard.com/file-service/public/files/0FIL5f5d42eb0ef64fe1fcf476b01f43c1401eb92af442a2f485072d549c4167f71635949865/.

Here are the instructions to import it:

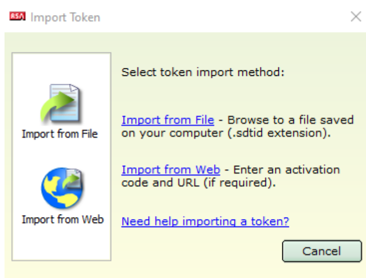
1. Ensure that the RSA SecurID Software is installed on your computer or mobile device. If you are unable to install the software, please contact your IT department.
2. Click on the above link to open the seed file and it will automatically open within the RSA SecurID Software.
3. RSA SecurID will prompt for the Encryption Key to complete the import of the seed file.
4. Enter in the Encryption Key.
5. Select OK.
6. If you are using multiple soft-tokens, select Change Name and give this soft-token a meaningful name.
7. Select OK.
8. A success message is displayed.
9. If you have multiple soft-tokens, select the one you just imported, enter 0000 in the PIN field (first time only) and generate a passcode.
10. Use your normal user ID and the above passcode to login to the online application.
11. The system then prompts you to enter Next Passcode and to select a New PIN. Please note, PINs may not start with leading zeros and must contain only numeric values.
12. You will be brought back to the login page. Enter in your new PIN and generate a brand new passcode to login.

Encryption Key From COMPANY: My Sample Company

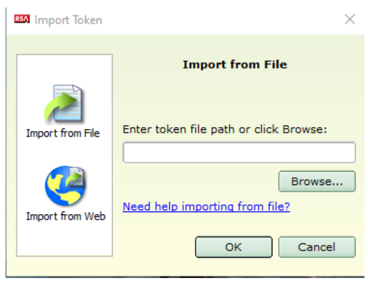
You must have the RSA software already installed for these steps to work.

Once you have the seed file downloaded, open the token, and go to **Options** and **Import Token.**

Choose the **Import from File** option.



Browse to find the Seed File – typically it will be in the Downloads folder.



Select the Seed File and click **Open**, and the system will take you through a process to name the token.

The same RSA SecureID tool can have multiple tokens, if required:

To enable the SecureID token:

- Enter **0000** when SecurID asks for a PIN number
- An eight-digit value will appear on the SecurID screen
- Enter your username and the eight-digit value from the SecurID as the passcode on the Smart Data login screen.
- You will be prompted to select a SecureID PIN number (cannot begin with a zero) and enter the next SecurID eight-digit passcode into Smart Data. Either wait for the next eight-digit passcode to appear on SecureID or click on **Options** and **Next Code**.

To sign into Smart Data:

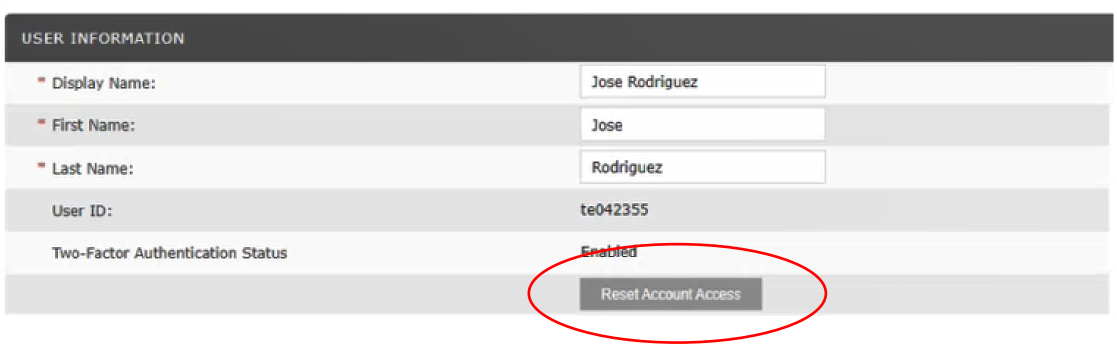
- Enter the new PIN into the SecurID App to retrieve an eight-digit passcode
- Enter your username and the eight-digit passcode into Smart Data

6.3 Resetting users' Multifactor Authentication

From time-to-time users will need to have a reset their multifactor authentication due to:

- Forgotten PIN
- New Computer
- New Phone

To reset a user, click on **Reset Account Access** from the **User Information** screen.



The user will receive the email with the link to the Seed File and should follow the steps outlined above for initial setup.

6.4 Common Issues with Tokens

It can take a few minutes for the email with the seed file to reach the user. If you click the **Reset Account Access** button a second time, the original seed file sent will be canceled and will not work. The user must wait for the email associated with the last time the **Reset Account Access** button was clicked.

When users use the token for the first time, they must enter a PIN of **0000** into the token and put the resultant code into Smart Data. They are then asked to set their own PIN, and it asks them to *wait for the next code*. Often, users do not wait for the next code but enter the code they can see on the screen. They should be told to wait for the code or choose **Next Code** from **Options**.

Our Client Service team are available to help with RSA SecureID token issues:

Santander Client Service is open for Program Administrators:

Monday – Friday 7:30 AM – 5:00 PM ET

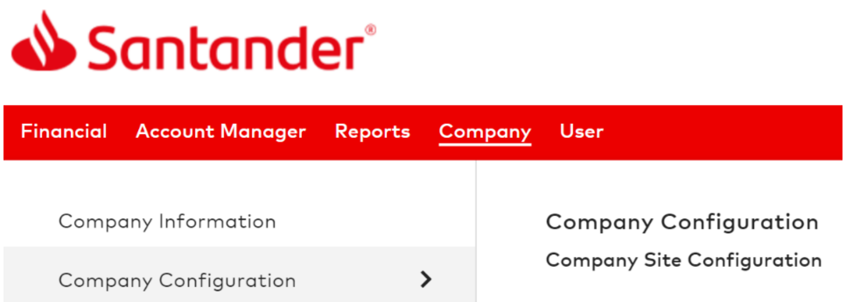
For Program Administrator service after hours: 877-598-7799

Email: clientservice@santander.us

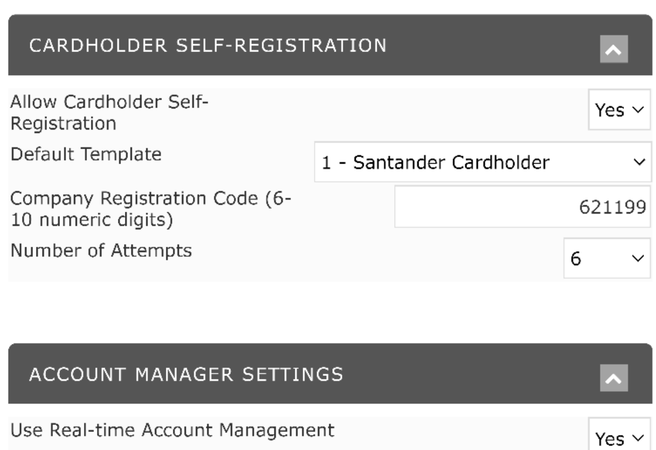
7 Company Registration Code

When cardholders self-register on Smart Data they need to enter a Company Registration Code.

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>To find your Company Registration Code, go to the Company menu, choose Company Configuration and Company Site Configuration



</td></tr>
<tr><td>2</td><td>Scroll down to the Cardholder Self-Registration panel to find your Company Resigration Code. Your cardholders will need this code to self-register on CenterSuite.

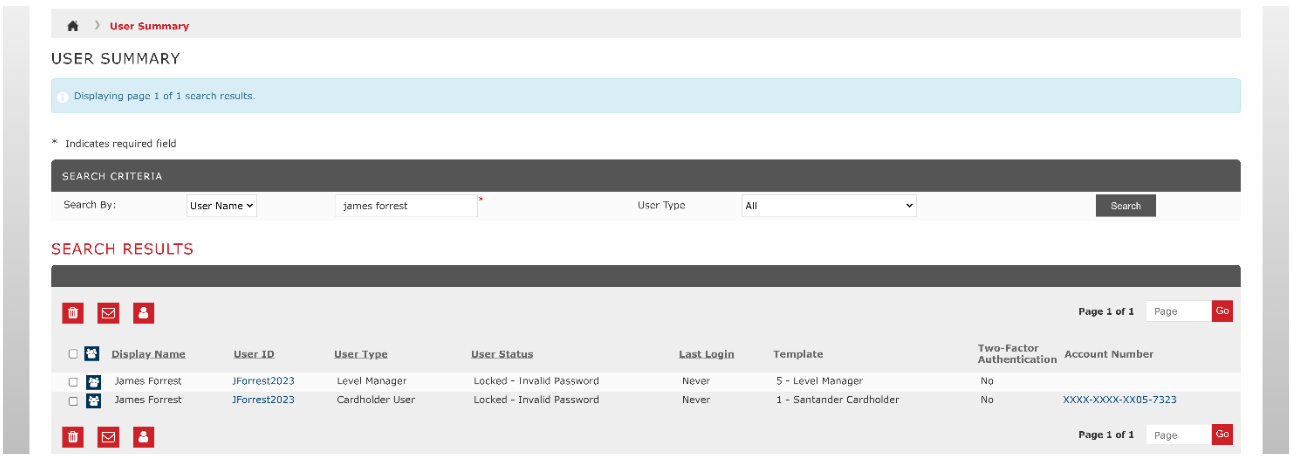


</td></tr>
</table>

8 User Administration

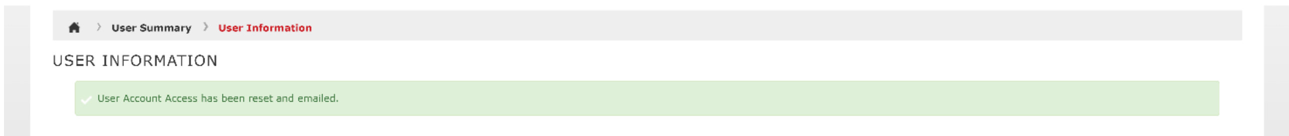
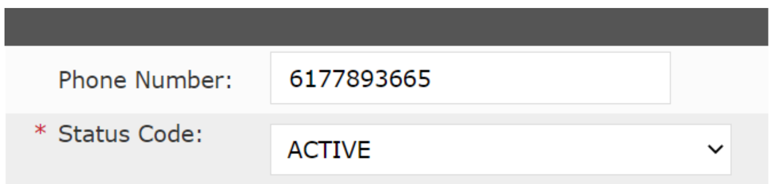
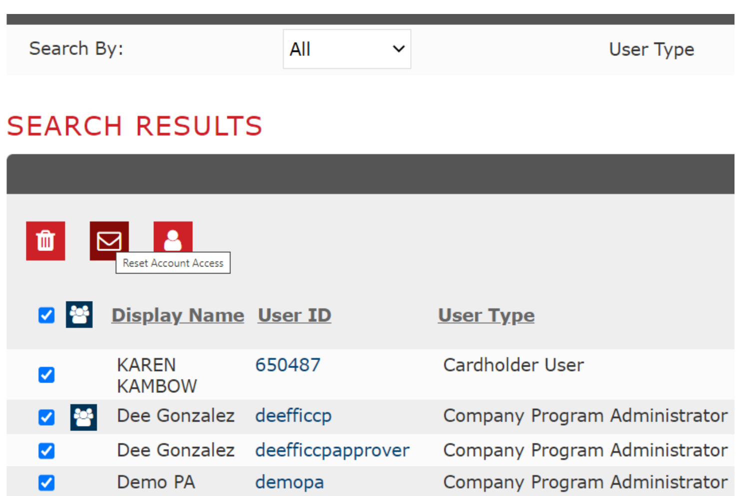
8.1 Reset User's Password / Unlock User

From the **User** menu, choose **User Summary** and search for the user who needs resetting.

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>Users cannot login if they are Inactive (not logged in for 90 days) or Locked (they have entered their password incorrectly multiple times). You can see this for the user under the User Status field.

</td></tr>
<tr><td>2</td><td>Note: The user cannot reset their password if they are Inactive or Locked. The user reset password function on the login screen only works if they are Active.

You can reset account access by clicking on their User ID to open their profile, and then click on the Reset Account Access

</td></tr>
</table>

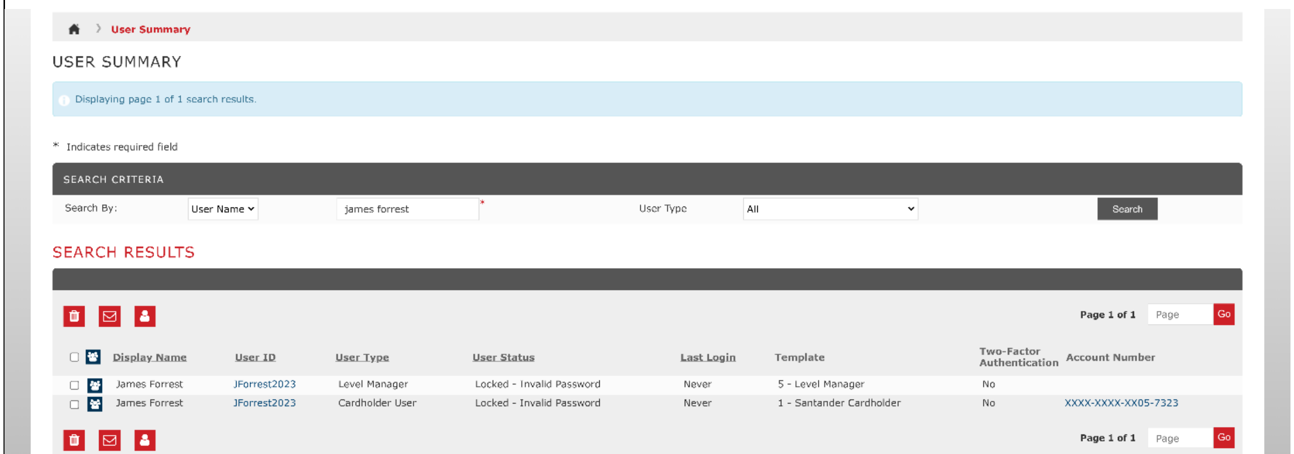
<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>3</td><td>You will see the confirmation message that account access has been reset and emailed. If they have multi-factor authentication, the email they receive will explain the reset process for RSA tokens (see Section 6 on RSA tokens).

</td></tr>
<tr><td>4</td><td>You must also change the status code to ACTIVE, or they will not be able to use the password reset email.

</td></tr>
<tr><td>5</td><td>The password reset link is valid for one week, HOWEVER, if the user was unable to login because they were Inactive (not logged in for 90 days) they need to login in the SAME DAY as you reset them to Active, or they will flip back to Inactive overnight.</td></tr>
<tr><td>6</td><td>There is the option to reset passwords for multiple users at once, say if you want all your user passwords reset. Check the top check box to select all, and then click on the Reset Account Access icon.

</td></tr>
</table>

8.2 Update a User's Contact Details

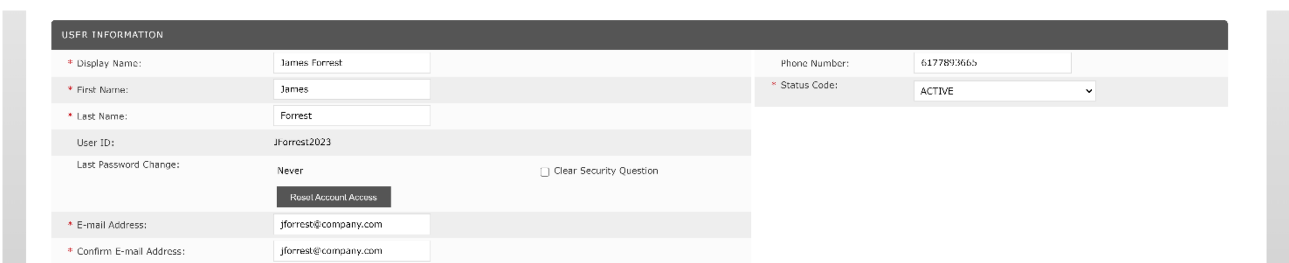
Please note, these steps will only change their Smart Data user profile and will not update any details associated with their card account. Search for the user from the **User** menu and **User Summary** option.

Action/Information

1 Click on the user ID to open the **User Information** screen.



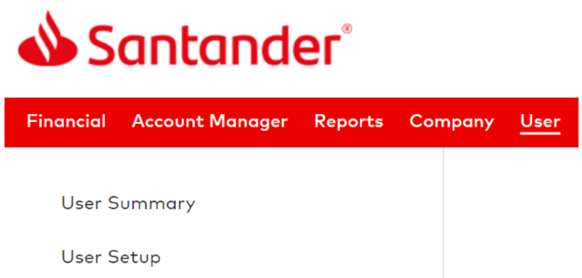
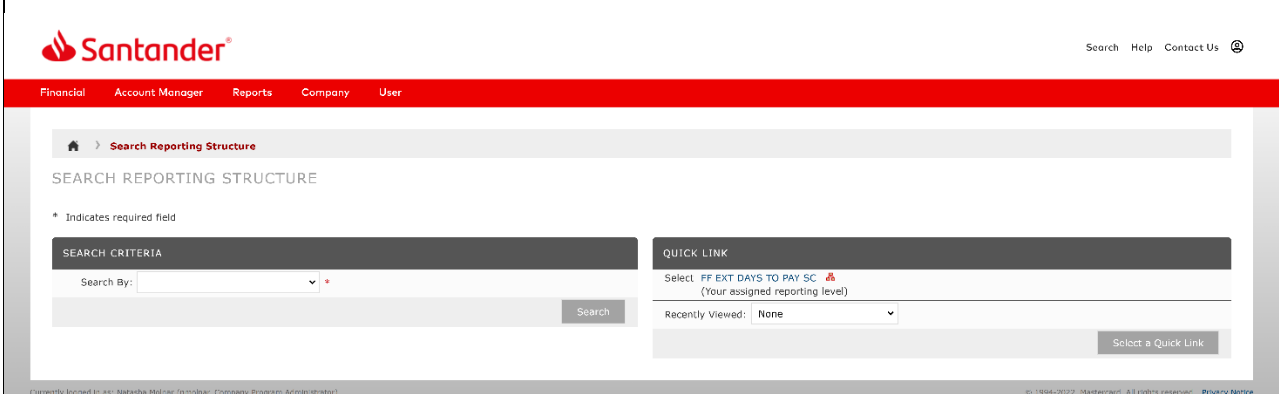
2 Update the user's email address or phone number and click **Save**

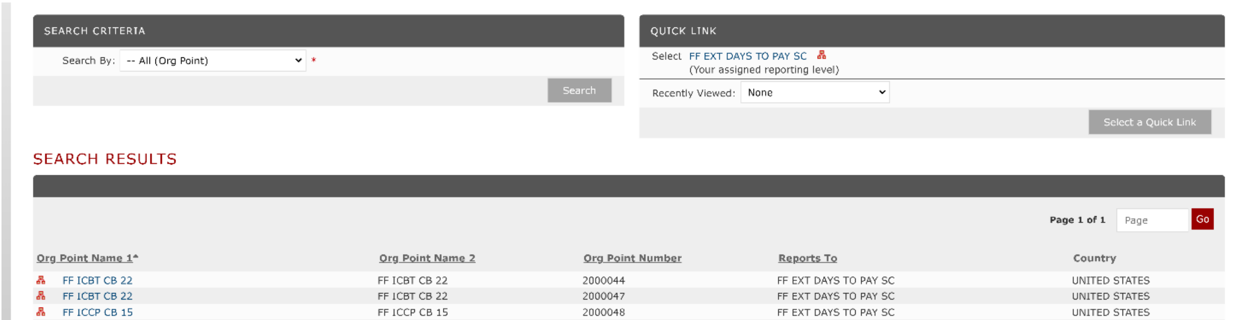


8.3 Adding a New User / Access and Security Profiles

Users can be **Account Holders** and administrators such as **Company Program Administrator** or **Level Manager**. Typically, **Account Holders** will self-register when they first receive a new card (see Section 16.2).

You will need to create users with administration roles, as follows:

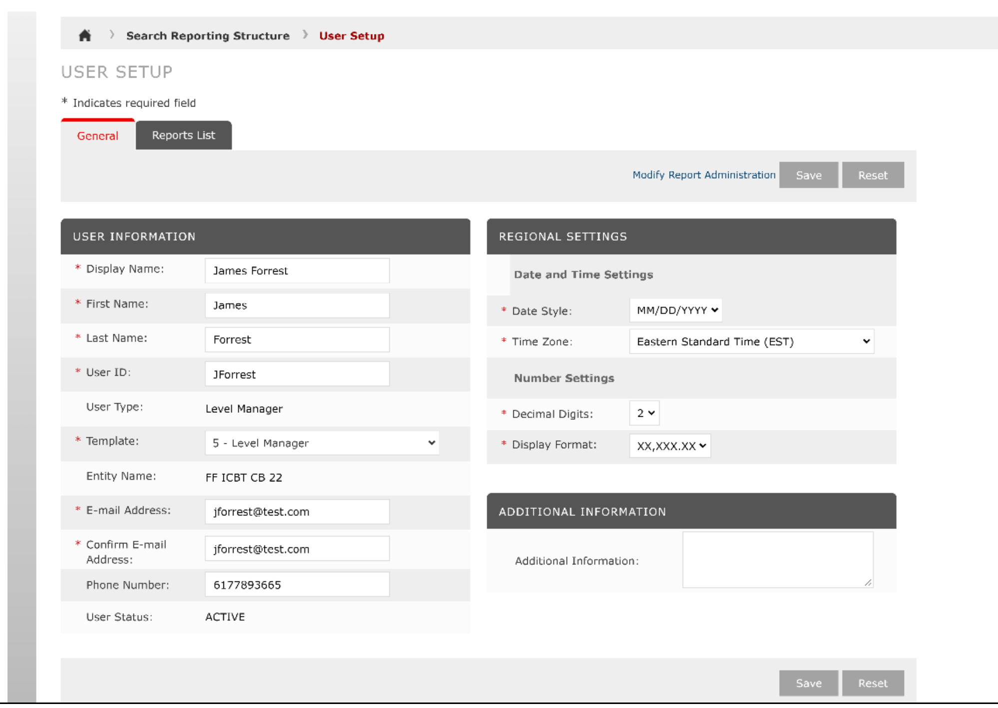
<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>From the User menu, choose User Set Up

</td></tr>
<tr><td>2</td><td>If the User is to be a Company Program Administrator for the whole company, click on the company name under Quick Link. If the user is just going to be associated with certain Org Points or Accounts, find the appropriate Org Point or Account using the Search By filter.

</td></tr>
</table>

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>3</td><td>If the user is just going to be associated with certain Org Points or Accounts, select the appropriate Org Point or Account (you can only add one at a time). See Section 3 for more information about Org Points and Accounts.

</td></tr>
<tr><td>4</td><td>Complete the user details on the next page and click Save.

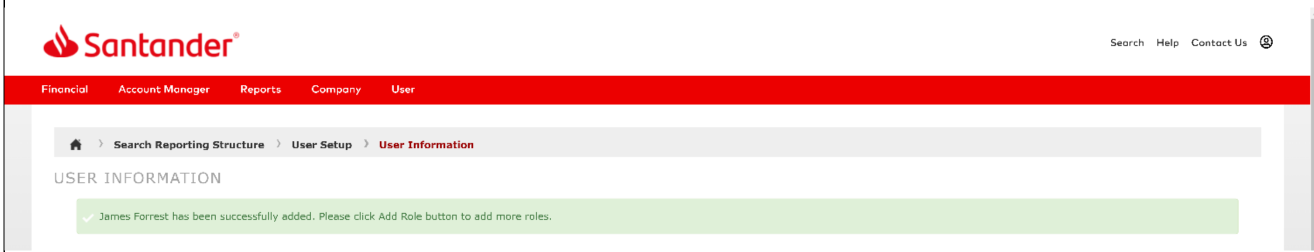
If you choose if you selected access for the whole company, the User Type will automically be set at Company Program Administrator.

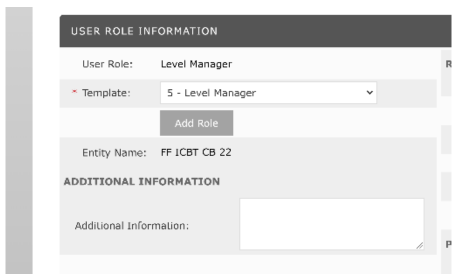
If you choose access to an Org Point, the User Type will automatically be set at Level Manger, as they do not have full company access.

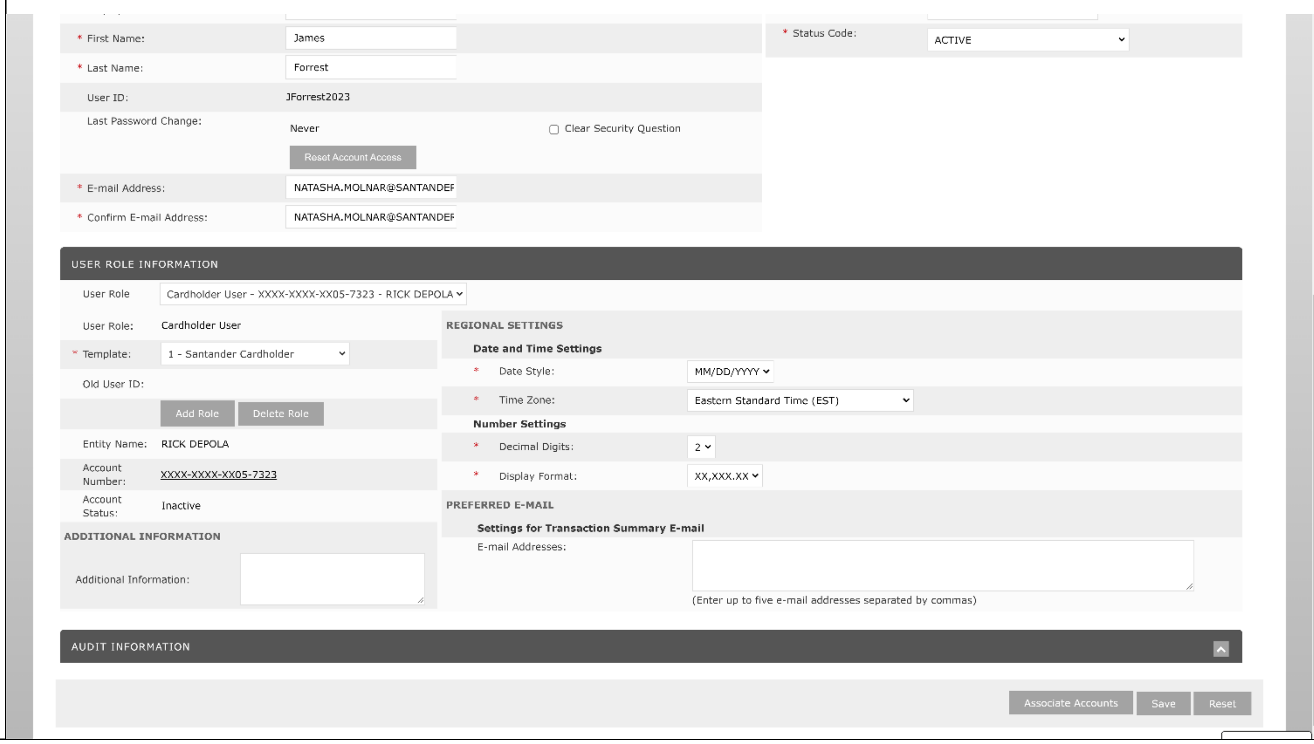
If you choose a card account, the User Type will automatically be set at Cardholder User.

<u>Make sure you choose a template for the User Type</u> (eg Reporting Only if you do not want to give them full access to this Org Point).

</td></tr>
</table>

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>5</td><td>You will get a confirmation message and advice to click on **Add Role** to add more roles.


</td></tr>
<tr><td>6</td><td>If you want to add another role, click on **Add Role** to give the new user access to another Org Point (or account if they are also a card holder).


</td></tr>
<tr><td>7</td><td>Repeat steps 2-6 until you have built up all the roles for the new user, then click **Save** at the bottom of the screen.

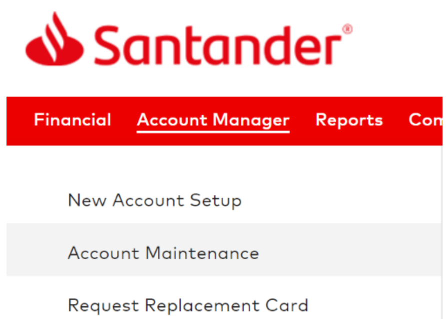

</td></tr>
</table>

9 Account Management

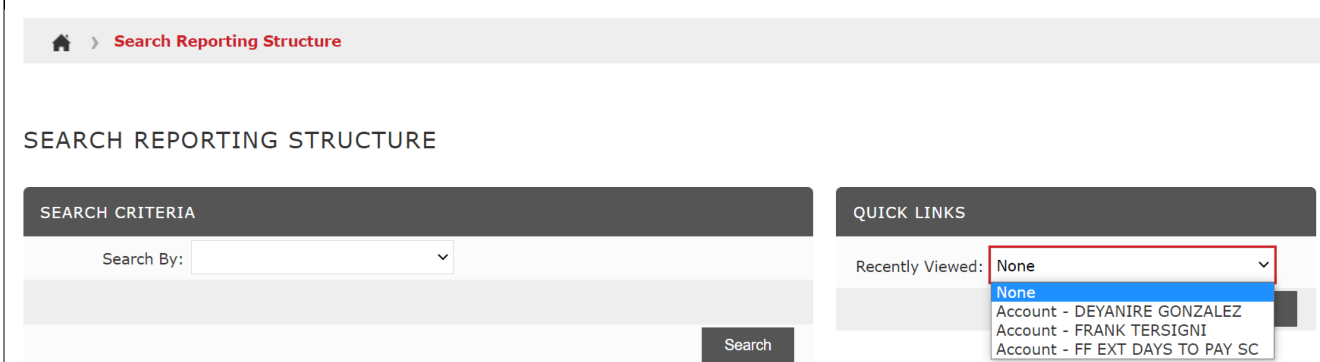
As a Company Program Administrator, you can view all accounts, corporate and cardholder, and make edits to your cardholder accounts.

9.1 Searching for an Account

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>From the Account Manager menu, choose Account Maintenance



</td></tr>
<tr><td>2</td><td>You can search for an individual account, a corporate account or supercorporate account (your overall client account). Accounts you have viewed recently will appear in the Recently Viewed drop down under Quick Links



</td></tr>
</table>

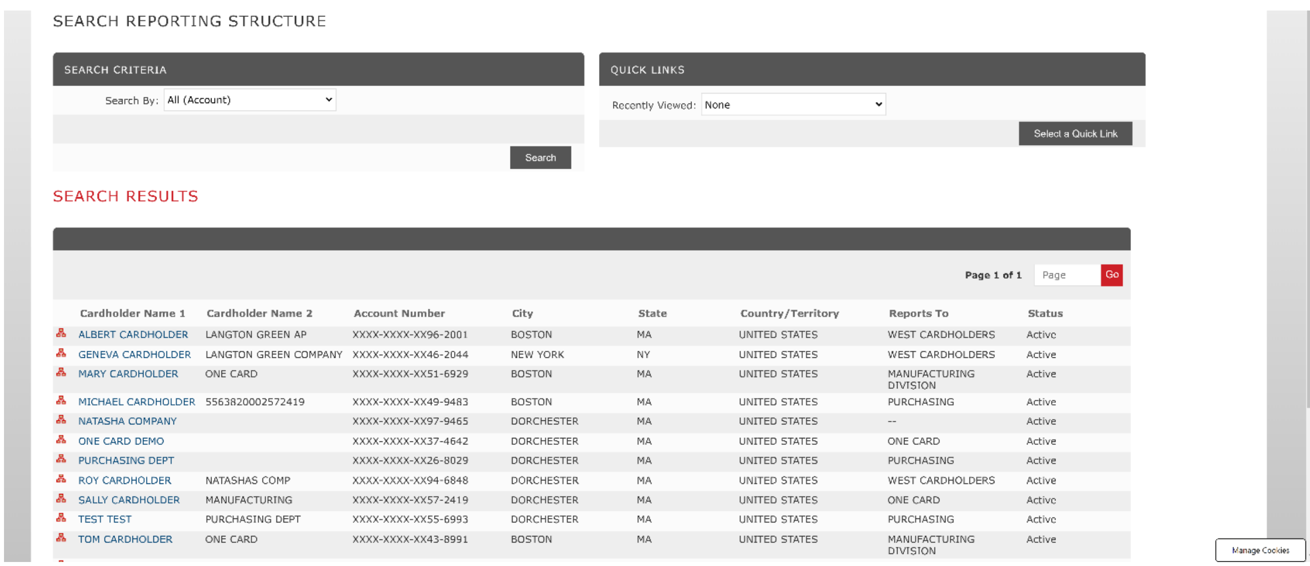
9.2 Activate cards

Cardholders can activate their cards by calling the number on the sticker on their new cards, 855-805-4337. They will need their Verification ID when calling in. See Section 9.3.3 for where the Verification ID can be found.

9.3 Making Edits to a Card Account

Search for the cardholder from the **Account Manager** menu and choose **Account Maintenance**.

	Action/Information
1	You cannot make edits to your SuperCorporate and Corporate accounts, but you can manage your Individual accounts from this screen. Search for the account and click on the **Cardholder Name 1** link



SEARCH REPORTING STRUCTURE

SEARCH CRITERIA

Search By: All (Account)

Search

QUICK LINKS

Recently Viewed: None

Select a Quick Link

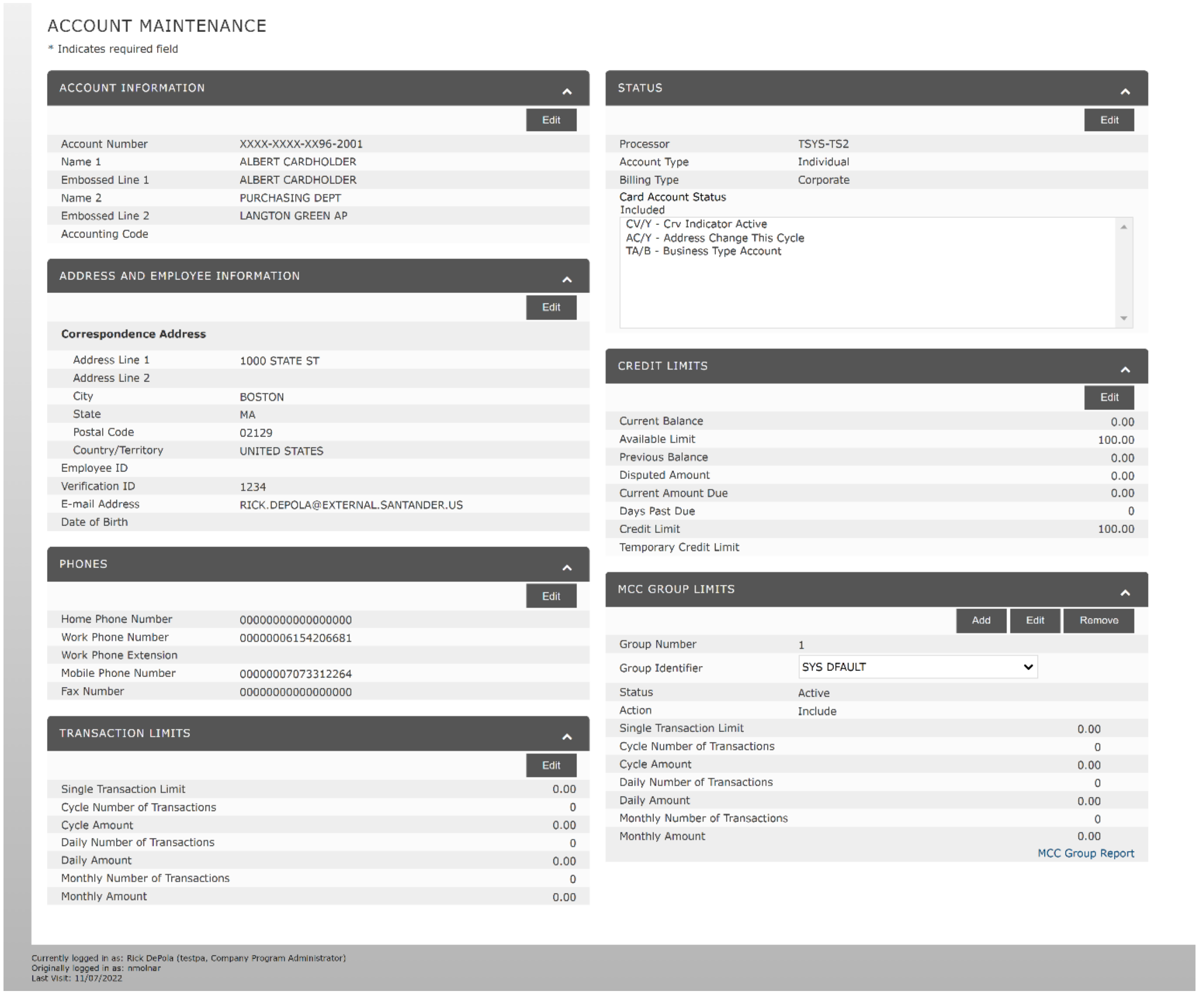
SEARCH RESULTS

Page 1 of 1 Page Go

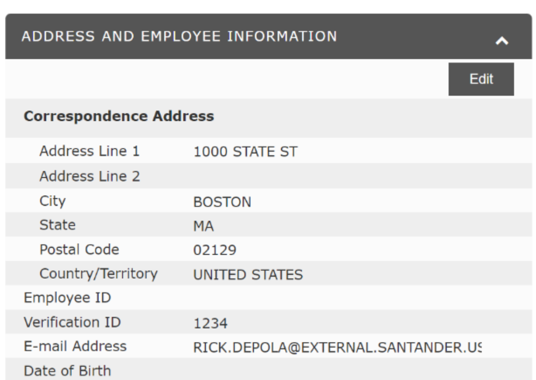
Cardholder Name 1	Cardholder Name 2	Account Number	City	State	Country/Territory	Reports To	Status
ALBERT CARDHOLDER	LANGTON GREEN AP	XXXX-XXXX-XX96-2001	BOSTON	MA	UNITED STATES	WEST CARDHOLDERS	Active
GENEVA CARDHOLDER	LANGTON GREEN COMPANY	XXXX-XXXX-XX46-2044	NEW YORK	NY	UNITED STATES	WEST CARDHOLDERS	Active
MARY CARDHOLDER	ONE CARD	XXXX-XXXX-XX51-6929	BOSTON	MA	UNITED STATES	MANUFACTURING DIVISION	Active
MICHAEL CARDHOLDER	5563820002572419	XXXX-XXXX-XX49-9483	BOSTON	MA	UNITED STATES	PURCHASING	Active
NATASHA COMPANY		XXXX-XXXX-XX97-9465	DORCHESTER	MA	UNITED STATES	--	Active
ONE CARD DEMO		XXXX-XXXX-XX37-4642	DORCHESTER	MA	UNITED STATES	ONE CARD	Active
PURCHASING DEPT		XXXX-XXXX-XX26-8029	DORCHESTER	MA	UNITED STATES	PURCHASING	Active
ROY CARDHOLDER	NATASHAS COMP	XXXX-XXXX-XX94-6848	DORCHESTER	MA	UNITED STATES	WEST CARDHOLDERS	Active
SALLY CARDHOLDER	MANUFACTURING	XXXX-XXXX-XX57-2419	DORCHESTER	MA	UNITED STATES	ONE CARD	Active
TEST TEST	PURCHASING DEPT	XXXX-XXXX-XX55-6993	DORCHESTER	MA	UNITED STATES	PURCHASING	Active
TOM CARDHOLDER	ONE CARD	XXXX-XXXX-XX43-8991	BOSTON	MA	UNITED STATES	MANUFACTURING DIVISION	Active

Manage Cookies

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>2</td><td>You can update Account Information, Card Status, Address and Employee Information, Credit Limits, Phone Numbers, MCC Group Limits and Transaction Limits



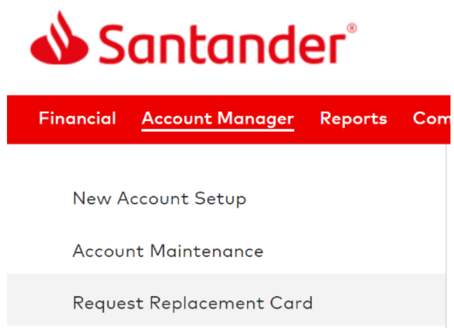
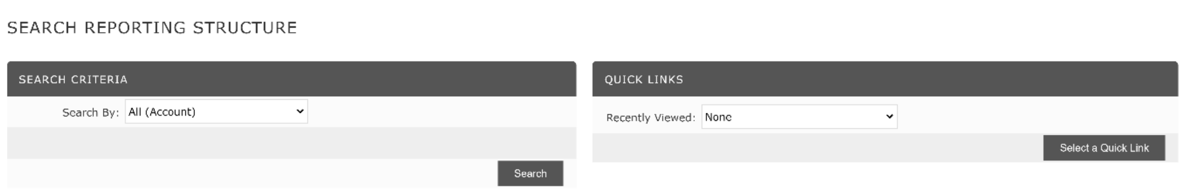
</td></tr>
<tr><td>3</td><td>The Verification ID is 4-digit number is used for authentication when calling Client Service to activate a card or for any other enquiry. If cardholders provide a correct Verification ID in the voice automated system or when speaking to an agent, they will not need to answer the usual security questions. To edit



</td></tr>
</table>

9.4 Ordering a Replacement Card

The feature should only be used if a cardholder's card is damaged, e.g., the chip is not working. It should **NOT be used if the card has been lost or stolen**. All lost or stolen cards should be reported by calling Client Service on 877-598-7799.

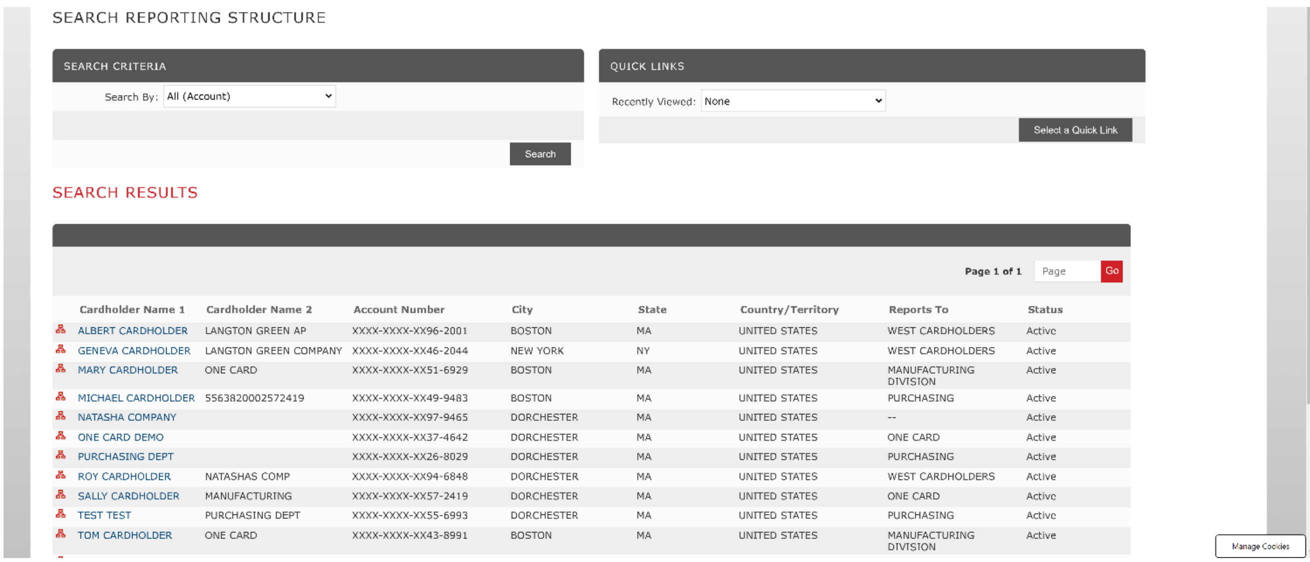
	Action/Information
1	To order a replacement card, select the **Request Replacement Card** from the **Account Manager** menu 
2	Search for the account you need a replacement card for. Accounts you have viewed recently will appear in the **Recently Viewed** drop down under **Quick Links.** 

9.5 Temporary Credit Limit

Search for the cardholder from the **Account Manager** menu and choose **Account Maintenance**.

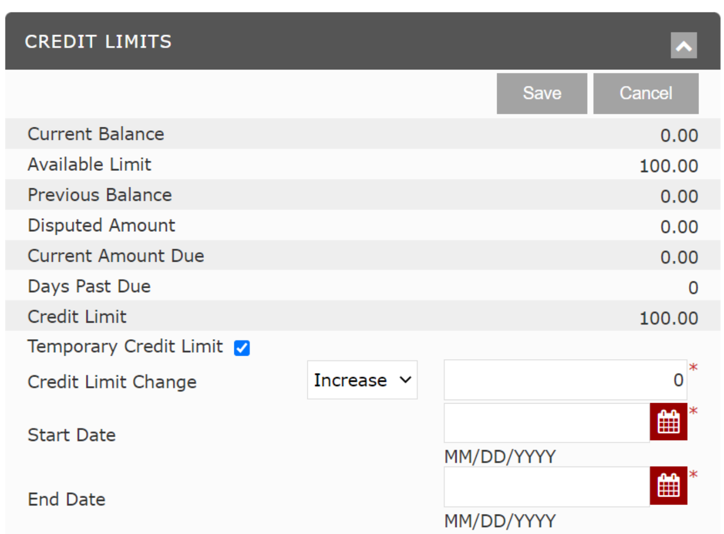
<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>

Search for the account and click on the **Cardholder Name 1** link



</td></tr>
<tr><td>6</td><td>

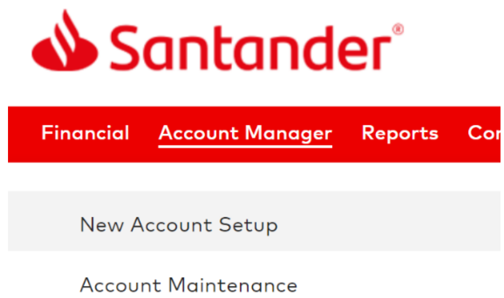
The option to make a temporary credit limit increase displays when you click the **Edit** button on the **Credit Limit** section. Check the **Temporary Credit Limit** box. Enter the parameters and click **Save**.



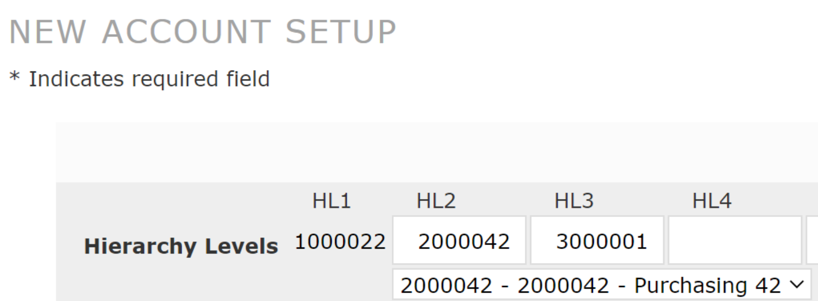
</td></tr>
</table>

9.6 Creating a New Card Account

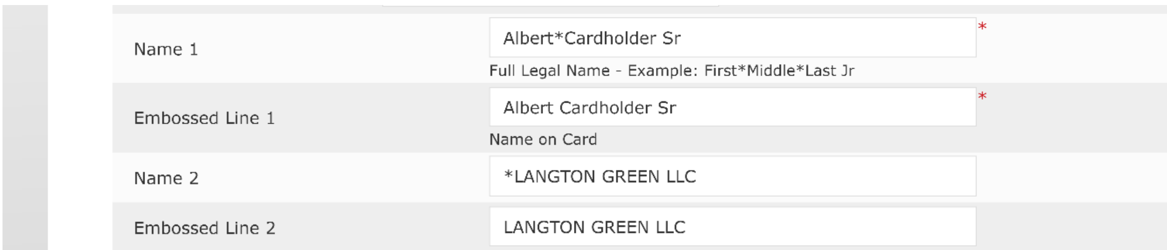
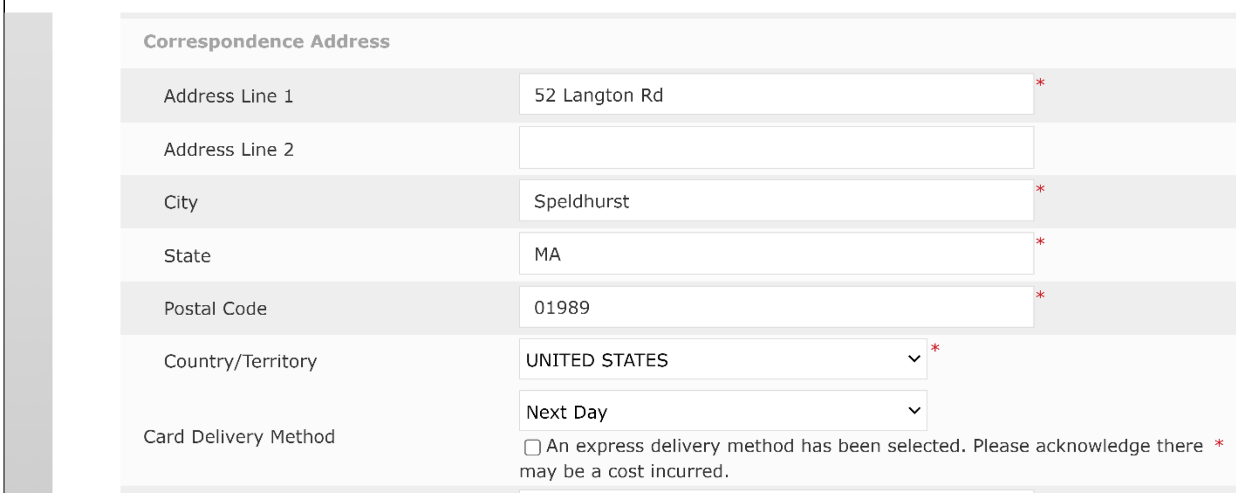
<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>From the Account Manager menu, choose New Account Setup.



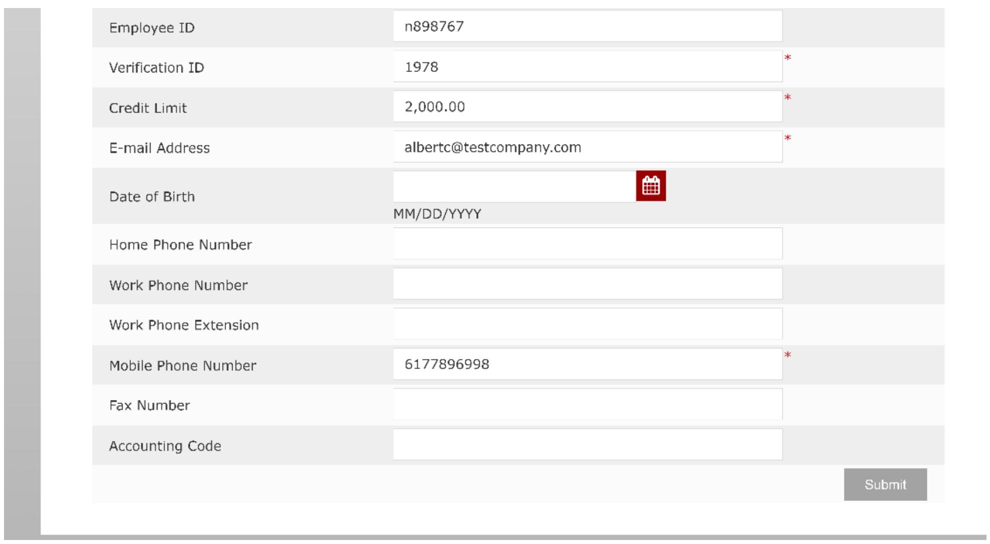
</td></tr>
<tr><td>2</td><td>The first thing you will need to do is choose where in your company hierarchy (or which Org Point) you want the new card to go. The first level of your hierarchy, the supercorporate, has already been chosen for you (in the example below it is 10000022). You will then chose which corporate billing account for the card (in the example below the card is is Purchasing 2000042). Finally you should enter 3000001 at the third hierarchy level (unless you company has been set up with a more complex hirarchy structure).



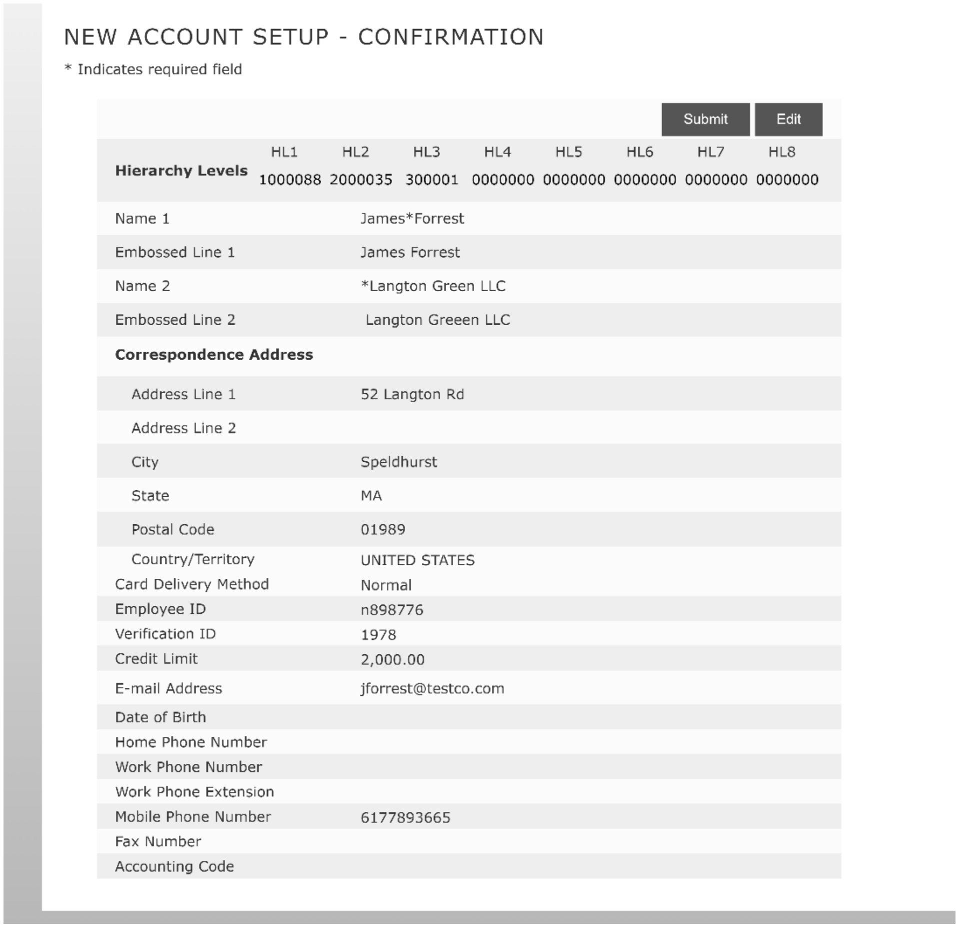
</td></tr>
</table>

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>3</td><td>Now enter the card account details.
When you enter the cardholder name put an asterisk between the names as shown. The Embossed Line 1 field will show how the name will be printed on the card.
The company name (embossed line 2) will be pre-filled with your company name. If you wish to overwrite this you can.

</td></tr>
<tr><td>4</td><td>Enter the address you want the card to be sent to.
Note that if you choose Next Day, rather than Normal for Card Delivery Method, a fee will be applied.

</td></tr>
</table>

	Action/Information
5	Employee ID is optional, but is useful if you use or plan to use an expense management service. The Verification ID is 4-digit number which is used to for authentication when calling Client Service to activate the card or for any other enquiry. If cardholders provide a correct Verification ID in the voice automated system or when speaking to an agent, they will not need to answer the usual security questions. To edit the Verification ID the account holder will need to call Client Service. An email address and mobile phone number are required. When completed, click **Submit**



	Action/Information
6	You will get a confirmation screen. Check the details and click **Submit**



NEW ACCOUNT SETUP - CONFIRMATION

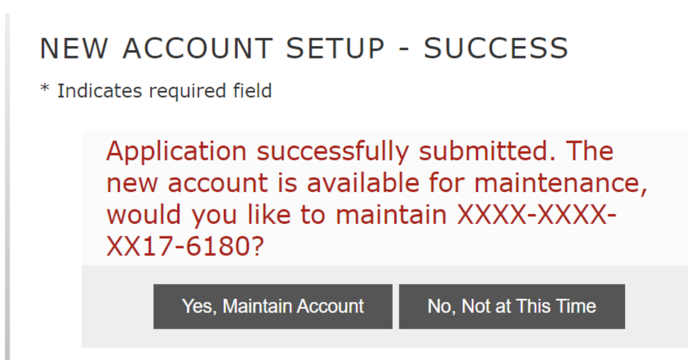
* Indicates required field

Submit Edit

Hierarchy Levels	HL1	HL2	HL3	HL4	HL5	HL6	HL7	HL8
	1000088	2000035	300001	0000000	0000000	0000000	0000000	0000000

Name 1	James*Forrest
Embossed Line 1	James Forrest
Name 2	*Langton Green LLC
Embossed Line 2	Langton Greeen LLC
Correspondence Address	
Address Line 1	52 Langton Rd
Address Line 2	
City	Speldhurst
State	MA
Postal Code	01989
Country/Territory	UNITED STATES
Card Delivery Method	Normal
Employee ID	n898776
Verification ID	1978
Credit Limit	2,000.00
E-mail Address	jforrest@testco.com
Date of Birth	
Home Phone Number	
Work Phone Number	
Work Phone Extension	
Mobile Phone Number	6177893665
Fax Number	
Accounting Code	

7	You will get a success message and be asked if you want to make any maintenance changes to the account. Given that you have just created the account you are unlikely to have changes at this step. If you click **No, Not at This Time**, you will only be able to make edits after 1-3 days, when the card has been created and appears in Smart Data.



NEW ACCOUNT SETUP - SUCCESS

* Indicates required field

Application successfully submitted. The new account is available for maintenance, would you like to maintain XXXX-XXXX-XX17-6180?

Yes, Maintain Account No, Not at This Time

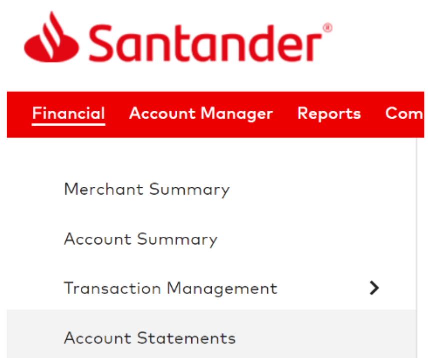
	Action/Information
8	When the card has been created, you will be able to see it and maintain it from the Account Maintenance menu option (see Section 9.3).

10 Statement and Transactions

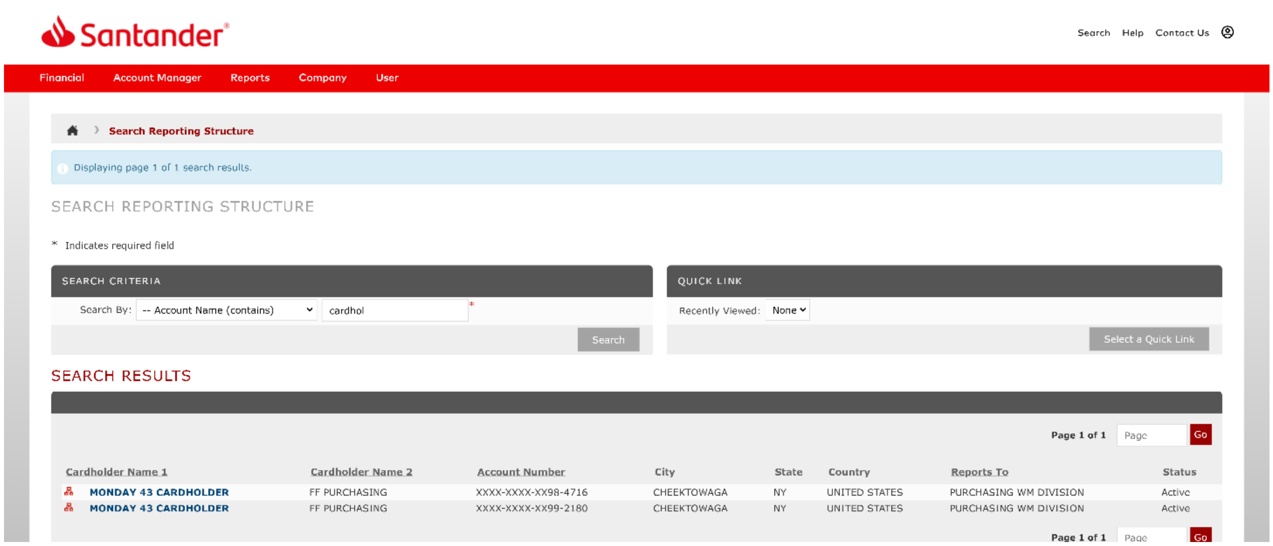
10.1 Downloading a Statement

Smart Data Account Manager makes it easy to access statements.

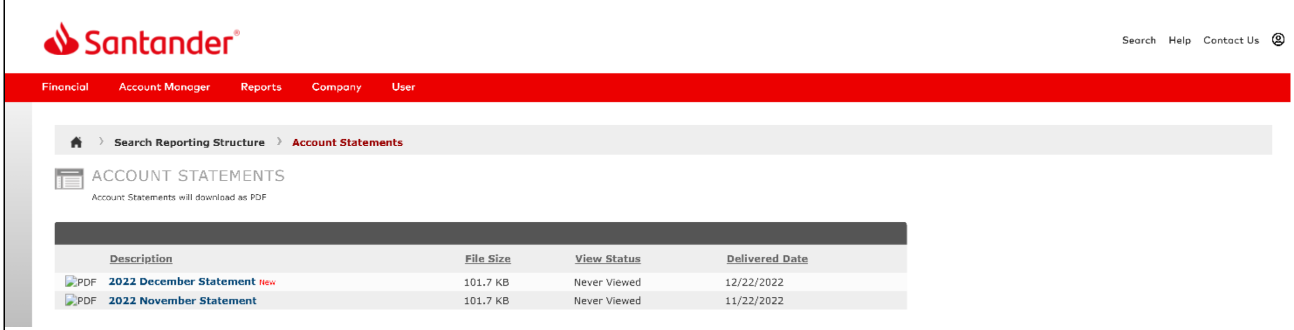
<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>Choose the Account Statements under Financial menu.



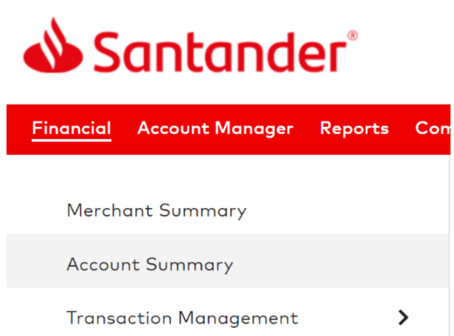
</td></tr>
<tr><td>2</td><td>Search for the account. You can view statements at the company (supercorporate), billing (corporate) or individual level. Click on the Cardholder Name 1 field

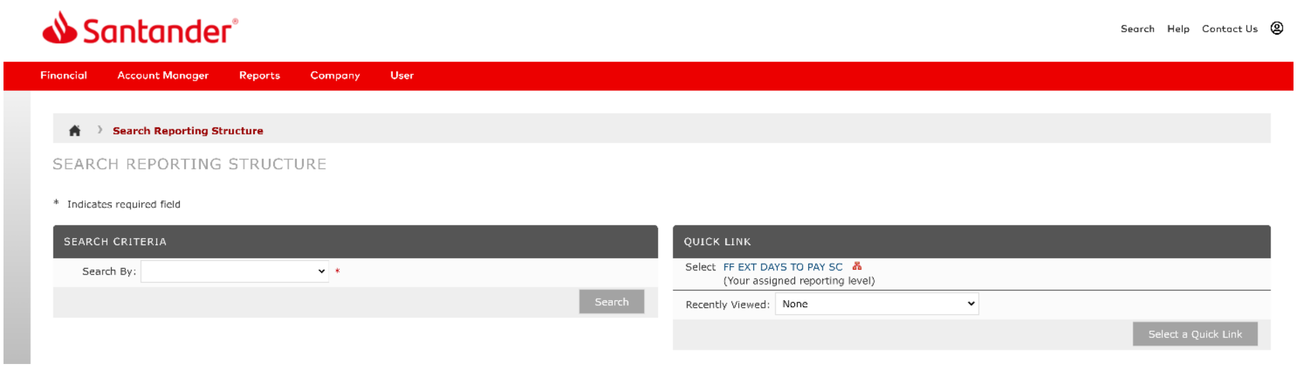


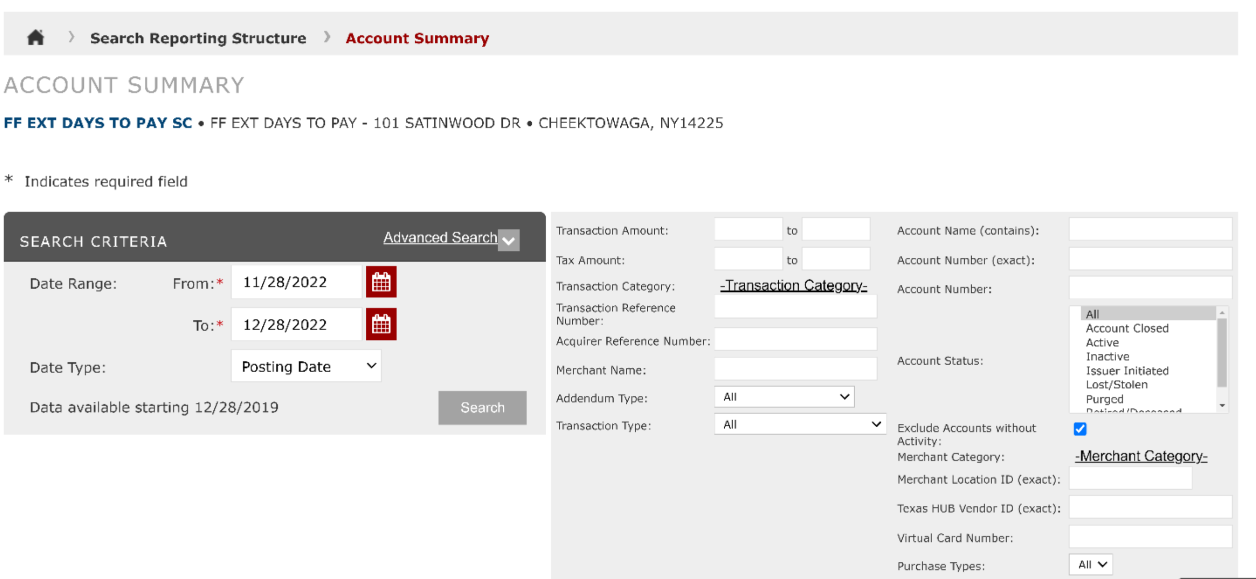
</td></tr>
</table>

	Action/Information
3	Statements for the chosen account will be displayed. 
6	Smart Data Account Manager has statements for the last 13 months. If you require an older statement, call or email Client Service. **NOTE:** A fee for each statement will be applied to the account.

10.2 Viewing and Downloading Transactions and Authorizations

	Action/Information
1	Choose the **Account Summary** option under the **Financial** menu 

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>3</td><td>Search for the Account or Org Point you want transactions for. If you want transactions for the whole supercorporate, click on the link under Quick Links.


</td></tr>
<tr><td>4</td><td>Choose the date range for the transactions. If you click on the Advanced Search option, you can specify other filters for your search. All the transactions for the range you have selected will be displayed.


</td></tr>
</table>

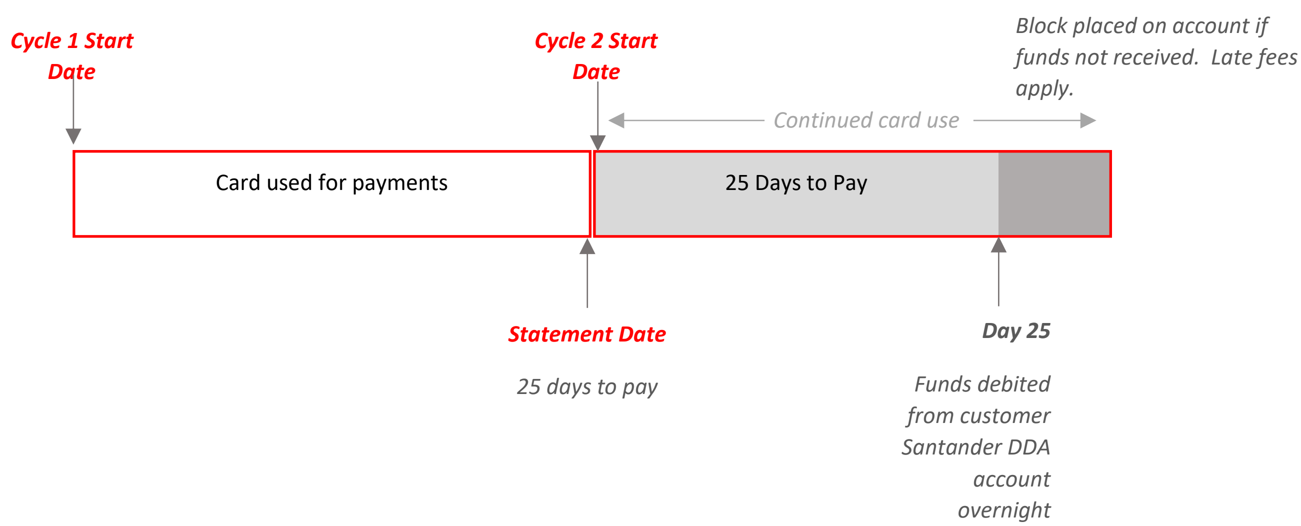
11 Billing and Payments

11.1 Program Billing

When there is transaction activity on any card, the Company Program Administrator or designated recipient will receive an account statement notification at the end of their billing cycle via email. The statement will be available on Smart Data Account Manager.

11.2 Program Payment

If you are on a corporate bill or monthly payment cycle, your monthly statement balance is typically due 15 or 25 days after your statement date. Your DDA account with Santander will be auto debited overnight and you will see this deducted from your account on the morning of Day 16 or 26 of the payment cycle.



If you are on a cycle other than monthly, your due date is agreed during the on-boarding process.

11.3 Making a Payment

Customers on **Corporate Bill** will have payments automatically deducted each cycle. However, there may be times when a Company Program Administrator may need to make an intra-cycle, one-time payment. Cardholders under **Individual Bill** programs may need to make payment for unauthorized transactions.

Payments cannot be made at the supercorp level, as transactions are only posted to corporate or individual accounts.

A one-time payment will reset the available funds for the corporate account, meaning that individual cardholders who have not reached their credit limits will be able to transact again. Individual cardholders who have reached their credit limit will not be able to transact until the next billing cycle, even if there is capacity at the corporate account level.

For example: New England Equipment LLC has one corporate account and two cardholders, Tom, and Sara. The credit limit for the corporate account is $5000, which has been reached mid-cycle meaning that both cards are unable to transact.

- Sara has a credit limit of $4000 and has spent $4000 already this month
- Tom has a credit limit of $2000 and has spent $1000 already this month

The Company Program Administrator makes a one-time payment of $2000:

- Sara will still not be able to use her card unless the Company Program Administrator goes into Smart Data Account Manager and increases her credit limit.
- Tom can spend up to $1000 during the rest of the month.

To make a payment you will need to call the number of the back of your cards, 877-598-7799. You should have the account verification ID for the corporate account you are making the payment for. See Section 7.3.3 for where to find the Verification ID. **Using the voice automated system for making a payment is free; however, there is a charge if you have an agent set up the payment for you.**

12 Disputing a Transaction

If the cardholder wishes to dispute a transaction, they should first contact the merchant and raise it with them. If the merchant does not resolve the issue, the cardholder must contact Client Service to begin a dispute. Call 855-465-8107 to initiate a billing dispute.

Procedure

- First contact the merchant and raise it with them.
  - Keep notes and copies of all correspondence.
- If the claim cannot be resolved with the merchant contact Cardholder Support at 877-598-7799 to initiate a billing dispute.
- Cardholder Support will gather the necessary information to begin the procedure and pass the case to the Dispute Department.
- Santander will send the cardholder a letter acknowledging the dispute (using address on file in CentreSuite).
- Cardholders may receive requests for additional information during the dispute resolution process.
  - Please respond to any questions or requests for information as soon as possible or the dispute may be closed.
- Santander will submit the required documentation and the investigation begins.
  - The merchant is allowed 45 days to respond. If a response is not received within 45 days, disputes are automatically resolved in favor of the cardholder.
- The Dispute Department will inform the cardholder of the outcome.

NOTE:

- Cardholders must notify the issuer of dispute within 60 days from statement date on which transaction appears or 90 days from the date of the transaction.
- Cardholders should retain all receipts and other transaction documentation.
- Cardholders may not dispute if previously disputed.
- Only posted transactions can be disputed.
- Cardholders cannot dispute fees.
- The account may continue to be billed for the amount in question. The customer does not have to pay any questioned amount while it is being investigated, but the customer is still obligated to pay the parts of the bill that are not in question.

13 Cardholder Self Service

13.1 Fraud Alerts

If Santander suspects a transaction on your account may be fraudulent the cardholder will get an email and text from us (providing we have a mobile phone number listed for the account in Smart Data Account Manager). The cardholder may text a response back:

- If they text back that the transactions listed in text were NOT fraudulent, then they need take no further action. The card will remain unblocked.
- If they do not recognize the transactions listed in the text as theirs and text back that the transactions ARE fraudulent, we will block the card and immediately arrange to send out a new card.

Cardholders may call the number in the email if they did not receive the text or prefer to call.

Failure to respond to our alerts will result in cards being blocked until the cardholder makes contact.

If you suspect fraud on your account **DO NOT WAIT** for a notification. Call Cardholder Support immediately on 877-598-7799, available 24 hours a day, 7 days a week.

Company Program Administrators may call in on behalf of customers to notify us of fraud on an account, but this will just result in a block going on the card. A claims process will not begin, and a new card will not be ordered until the Cardholder calls in.

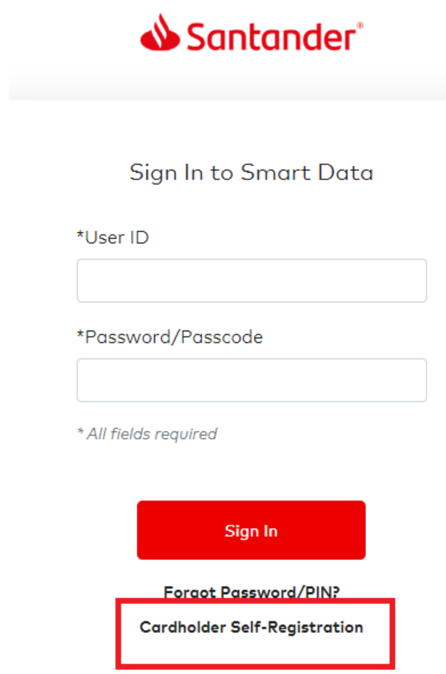
13.2 Card holder Self Registration on Smart Data

Cardholders need to register for access to Smart Data Account Manager as follows:

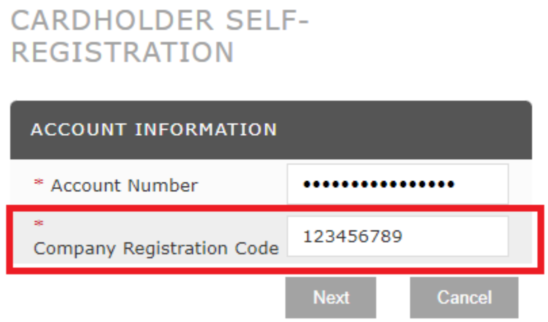
Click this link, or copy it into your browser: smartdata.santanderbank.com

Cardholders will need the following to register:

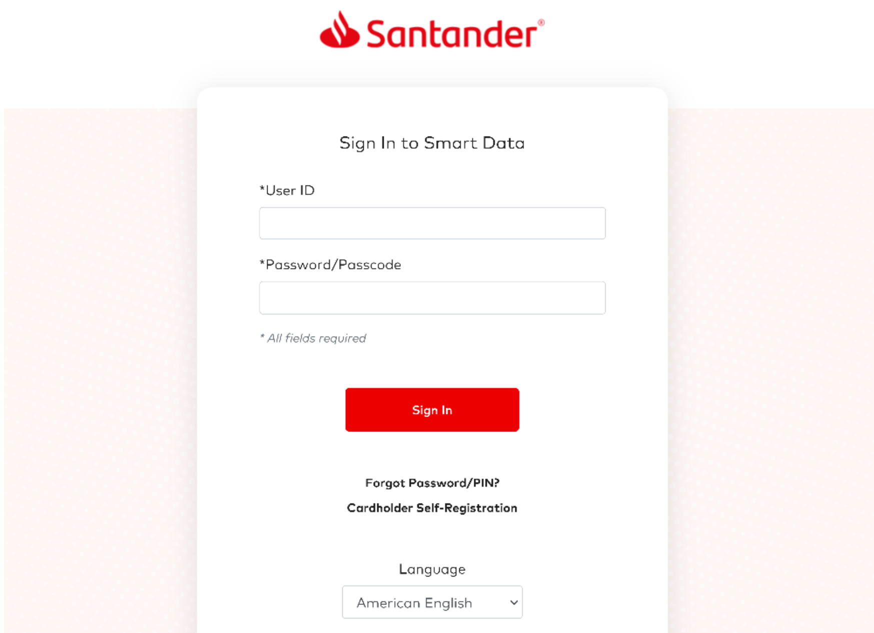
- 16-digit card number
- Your Company Registration Code (see Section 7 for where to find this)

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>1</td><td>Click Cardholder Self-Registration, underneath the Forgot Password/PIN link on the home page.


</td></tr>
</table>

<table>
<tr><th></th><th>Action/Information</th></tr>
<tr><td>2</td><td>Enter your 16-digit card number and Company Registration Code (provided by the program administrator). Click Next

</td></tr>
<tr><td>3</td><td>Complete the User Information fields and Click Register Account to save your credentials

</td></tr>
</table>

	Action/Information
4	5. Click **Return** to Login Screen, enter your user ID and password, and click **Sign In** 

13.3 Cardholder Card Activation and PIN Setting

Cardholders will need to activate their cards by the number on the sticker on their cards, 1 855-805-4337 and following the IVR prompts. As part of the activation process, they will be prompted to set their card PIN. They MUST complete this process. ***They will need a PIN for transactions where cards are inserted or swiped.***

They will need their 16-digit card number and Verification ID (see Section 9.3.3 for where to find a Verification ID).

13.4 Resetting Verification ID

A Verification ID is 4-digit number which customers will use to authenticate themselves when calling Customer Service to activate a card or ask a question. If customers provide a correct Verification ID, they will not need to answer the usual security questions. Cardholders and Company Program Administrators may view their Verification ID in the account details listed under **Account Maintenance** (see Section 9.3.3). Cardholders, Level Managers and Company Program Administrators may reset their Verification IDs by calling Client Service on 877-598-7799.

13.5 Lost or Stolen Cards

All lost or stolen cards must be reported as soon as possible by calling 877-598-7799, open 24/7/365. Smart Data Account Manager **cannot** be used to report or administer lost or stolen cards, a call *must* be made.

14 Fraud Best Practice Controls

Set and Communicate Company Policy

Determine and implement a company card use policy, e.g., Set rules for your employees for use of cards.

Monitor and Take Quick Action

- Analyze cardholder spend for suspicious activities.
- Ensure cardholders review their statements for unauthorized activity.
- Report suspicious transactions.
- Ensure every cardholder has a mobile phone number listed, to enable Santander to verify the validity of transactions by text.

Set Card and Transaction Limits

Each card can be assigned a monthly card limit as a control to avoid unnecessary exposure to fraud. Review these limits periodically to ensure they are still appropriate. See section 5.4.6 for instructions on how to edit cardholder limits.

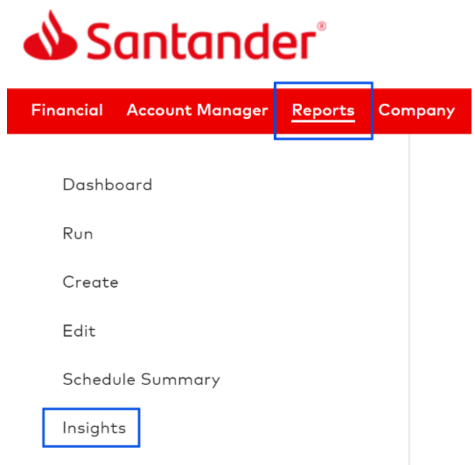
Set Merchant Category Code (MCC) Blocks

Restricting the types of merchants where your company's cards can be used is a prudent control measure. Setting Merchant Category Code (MCC) strategies for your cards restricts possible miss-use of cards by employees and can reduce the risk of fraud should the card details get into the wrong hands.

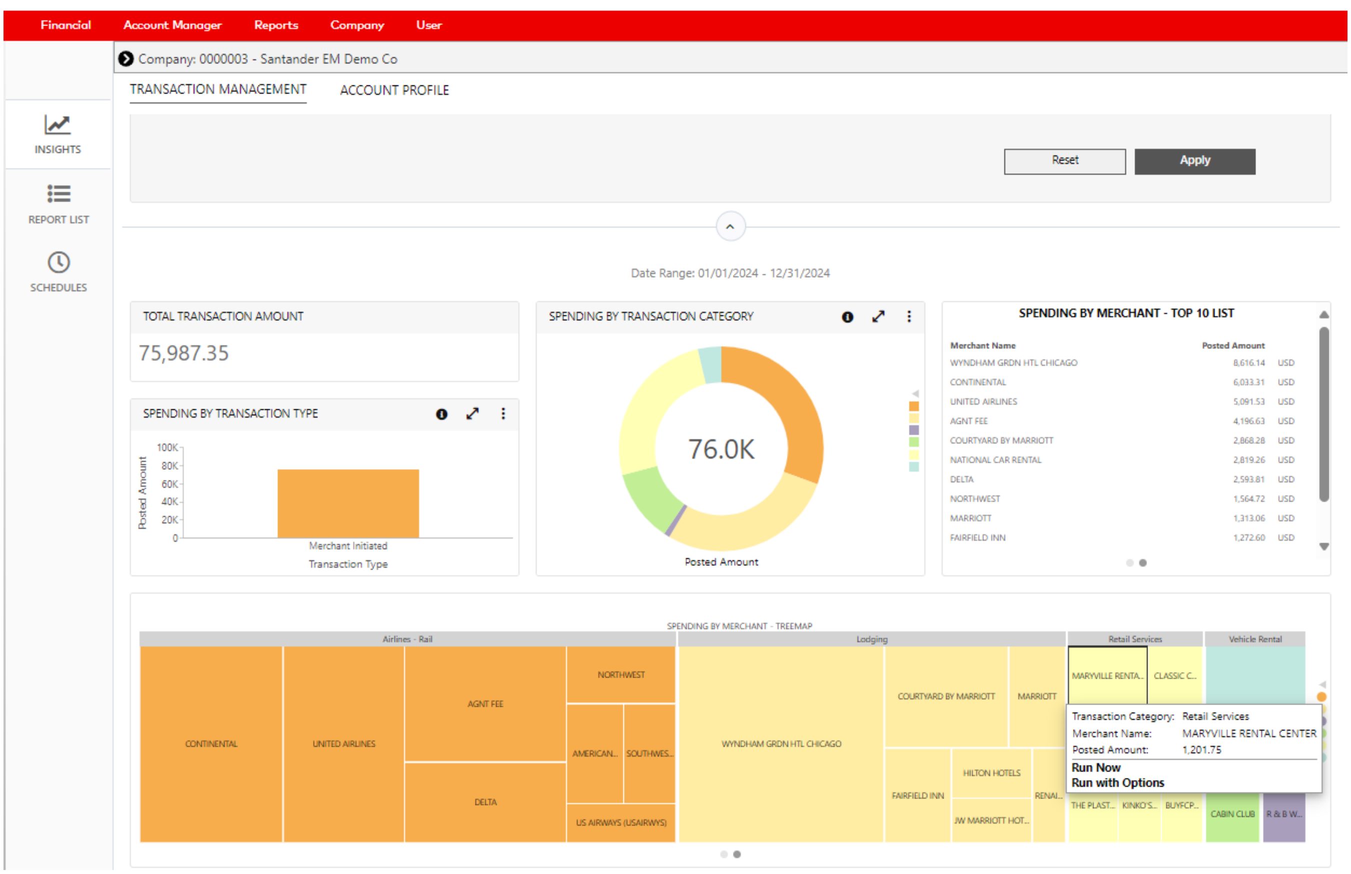
Santander has a set of recommended MCC Groups for different product types, e.g., Travel and Entertainment, or Purchasing. We recommend you choose appropriate MCC groups for your program or even at the cardholder level. Strategies are usually set up when you are onboarded but can be requested at any time by calling Client Service, 877-598-7799.

15 Reports

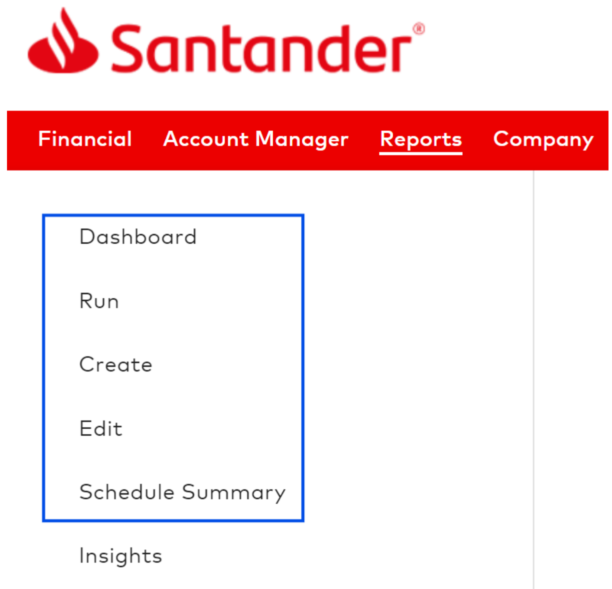
All reports are accessed via the **Reports** menu at the top of the screen. Most reports are accessed via the **Insights** tab.



Reports can be viewed, run, and scheduled within the **Insights** tab:



The other menu options, **Dashboard**, **Run**, **Create**, **Edit** and **Schedule Summary** relate to User Defined Exports.



Smart Data does not have QuickBooks integration, however, an export that is compatible with QuickBooks can be created. A user guide is available from Client Services.

For more information on reporting, see our full Reports Guides:

- Smart Data Reports Guide
- Virtual Card Reporting Guide

These are available by contacting Client Service, phone: 844 726 0095 or email clientservice@santander.us