JACKHENRY University

NetTeller®

Release 2020

Secure Tokens Training Guide

SilverLake, CIF 20/20®, Core Director®, Episys®

December 11, 2020

jack henry & ASSOCIATES INC.®

© 1999-2020 Jack Henry & Associates, Inc.

All rights reserved. Information in this document is subject to change without notice. Dates contained in this document are provided as estimates only and can be changed at any time at the sole discretion of Jack Henry & Associates, Inc.

Printed in the United States of America.

No part of this document may be copied, reproduced, stored in a retrieval system, displayed, distributed or transmitted in any form or any means whatsoever (electronic, mechanical or otherwise), including by photocopying or recording for any purpose, without the prior written permission of Jack Henry & Associates, Inc. Making unauthorized copies of this document for any purpose other than your own personal use is a violation of United States copyright laws.

Any unauthorized use of Jack Henry & Associates, Inc.'s, trademarks and service marks is strictly prohibited. A list of registered and unregistered marks owned or licensed by Jack Henry & Associates, Inc. is located at:
https://www.jackhenry.com/more-from-jha/pages/trademark-notice.aspx

Various other trademarks and service marks used or referenced in this document are the property of their respective owners.

Secure Tokens 4
Secure Token Devices 4
Registering a Token in Online Banking 5
NetTeller Back Office 6
Manage Secure Token Users 6
Secure Tokens Menu 7
Registering a User for Secure Tokens 10
Viewing Activated Users 11
Symantec Verisign Identity Protection Manager (VIP Manager) 13
Accessing VIP Manager 13
VIP Manager Dashboard 14
VIP Manager Credentials 15
Search for a Credential 16
Creating VIP Administrators 21
Reports 23
Help 24
Registering a Customer Support Representative's Token 24
Reset a Customer Support Representative's Token 25
Generating Temporary Token Codes for Misplaced Tokens 25
Assisting Users with Lost Tokens 27
Registering a New Token 29
Troubleshooting an Invalid Token 31
Resetting a Blocked User 33

© 1999-2020 Jack Henry & Associates, Inc.

Secure Tokens

As an extra level of security, secure tokens provide an additional layer of authentication for your end users. During logon, users are prompted to enter a six-digit code from their token device. Additionally, collected secure tokens users can now use their token to authenticate their activity when a Security Manager rule is triggered. If the user enters the wrong credential code or does not have their token, they are not able to log on to NetTeller or complete their online banking activity. While used primarily for Cash Management users, you can enable any NetTeller ID with this feature.

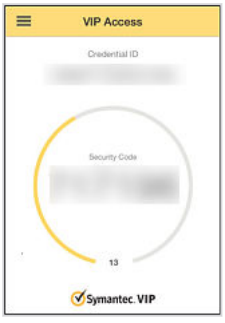
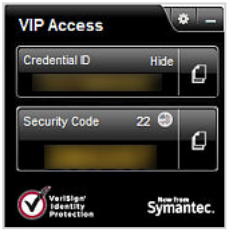
Secure Token Devices

Three types of tokens are available for users to choose from:

- Hard Tokens
- Mobile Soft Tokens
- Desktop Soft Tokens

The financial institution purchases hard tokens, and soft tokens are a free download.

Tokens

Hard Token	Mobile Device Access	Desktop Access
Physical token that is given to the end user. Contact your JHA Inside Sales Representative to order physical tokens. If you are unsure of your contact, email TellMeMore@jackhenry.com. 	Virtual token that is downloaded to a mobile device. Search for *VIP Access* in your device's app store. 	Virtual token that is downloaded to a computer desktop. Go to *https://idprotect.vip.symantec.com/* for instructions on how to download the desktop token. 

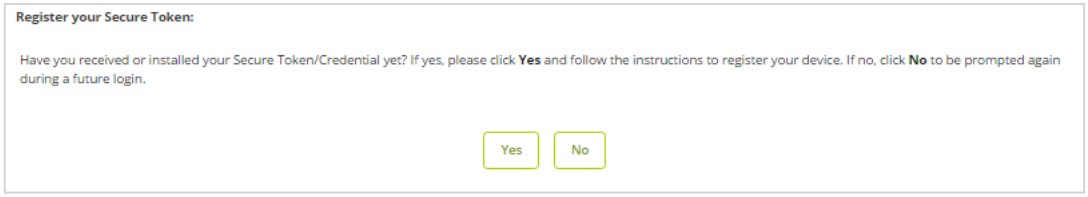
© 1999-2020 Jack Henry & Associates, Inc.

Registering a Token in Online Banking

1. Log on with your NetTeller user name and password.

> **TIP**
> Single sign-on (SSO) is required for Cash Management users.

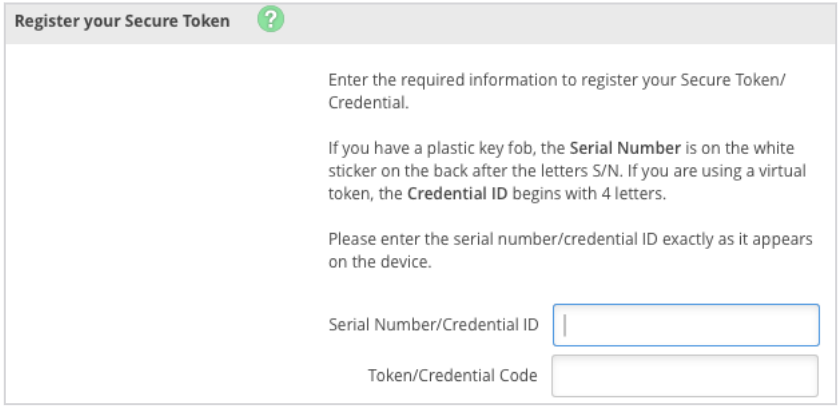
2. Indicate if you have received your physical token or downloaded your virtual token.



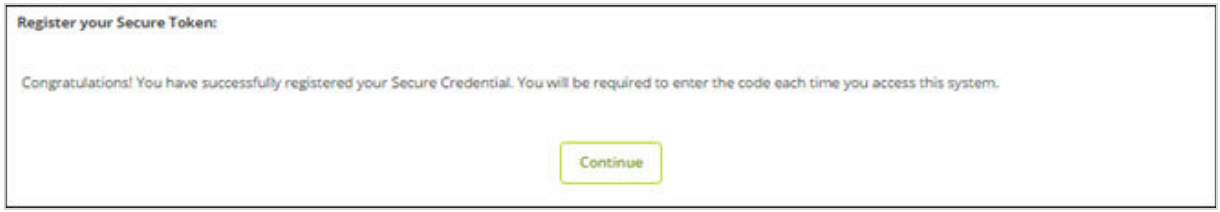
A message appears with how many days are left before your registration period ends if you have not received your token.

3. Enter the token **Serial Number/Credential ID** and six-digit **Token/Credential Code**.

> **NOTE**
> For hard tokens, the serial number is on the back of the token.

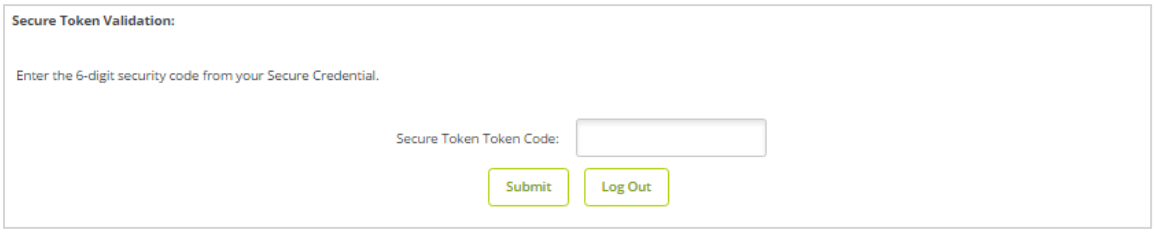


4. Select **Submit**.
   A success message appears.



© 1999-2020 Jack Henry & Associates, Inc.

Once registered, the token must be used during each NetTeller logon after entering your credentials.



NetTeller Back Office

NetTeller Back Office is the management module for NetTeller Online Banking and its ancillary products.

NetTeller Back Office is used to manage products and users.

> **TIP**
> Use the *Site* tab in the top-right corner to search for specific menu options.

Manage Secure Token Users

To access user maintenance, go to **NetTeller Back Office** > **Manage Users** > **Manage Secure Token Users**.

Token user maintenance is located in the **Manage Secure Token User** menu. This menu allows customer service representatives (CSR) to perform the following actions on a per NetTeller ID basis.

- Activate
- Deactivate
- Reset
- Suspend
- View Details

> **NOTE**
> The number of *Registered* tokens may be different than the number of *Users* because *Registered* tokens represent both current and previous token users. Deleted Cash Management users' tokens do not appear.

CSR rights must be established to perform desired secure token actions within this menu. The necessary CSR rights are established through custom CSR roles that have available entitlements in the **Manage Users** > **Manage CSR Roles** menu.

© 1999-2020 Jack Henry & Associates, Inc.

> **TIP**
> More information on granting entitlements is found in the *NetTeller Back Office Training Guide*.

Secure Tokens Menu

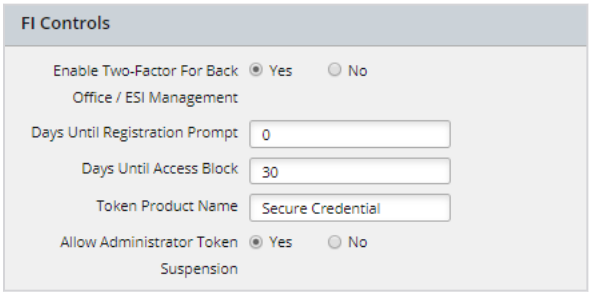
To access secure token parameters, go to **NetTeller Back Office** > **Manage Products** > **Secure Tokens**.

The **Secure Tokens** menu allows customer service representatives (CSR) to work with Secure Token parameters. CSR rights to work with this menu are established through custom CSR roles that have available entitlements in the **Manage Products** > **Manage Secure Tokens** menu.

> **TIP**
> More information on granting entitlements is found in the *NetTeller Back Office Training Guide*.

Financial Institution (FI) Controls

FI Controls allows you to configure credential parameters and establish system message verbiage.



Enable Two-Factor for Back Office/ESI Management

Enable this field if you want to require two-factor authentication for all CSRs logging on to NetTeller Back Office. Two-factor authentication requires either a physical or virtual token to be registered to CSRs. After CSRs enter their NetTeller Back Office credentials, they are prompted for authentication so that they can continue their activity. For CSRs that access **ESI Management** through NetTeller Back Office's **Home** > **External Admin Sites**, the same token authenticates them into an ESI Management session. If you do not enable this field and keep the default setting of *No*, CSRs can access NetTeller Back Office without using two-factor authentication.

> **TIP**
> Recommended: Set this field to *Yes*.

Days Until Registration Prompt

© 1999-2020 Jack Henry & Associates, Inc.

Enter the number of calendar days before a user is prompted to register a token after activation. The recommended setting is *0*.

> **NOTE**
> This field only applies to NetTeller users, not CSRs.

Days Until Access Block

Enter the number of days before being blocked because of failure to register credentials. Once a financial institution marks a user as activated, the user is prompted to register the token based on the **Days Until Registration Prompt**. The registration prompt continues at each logon until the user successfully registers the token. If the user fails to register the token within the **Days Until Access Block**, the user is blocked after logging on.

> **NOTE**
> This field only applies to NetTeller users, not CSRs.

Token Product Name

Enter the product name that appears on screens related to secure tokens.

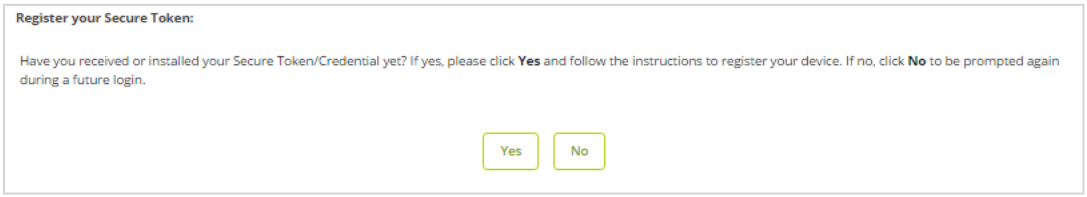
Allow Administrator Token Suspension

Select one of the following options to determine whether Cash Management administrators can suspend token authentication for themselves or other cash users:

- Select *Yes* to allow full administrators to turn tokens on or off for cash users.
- Select *No* to make full administrators call the financial institution to have tokens suspended for cash users.

Registration Prompt Message

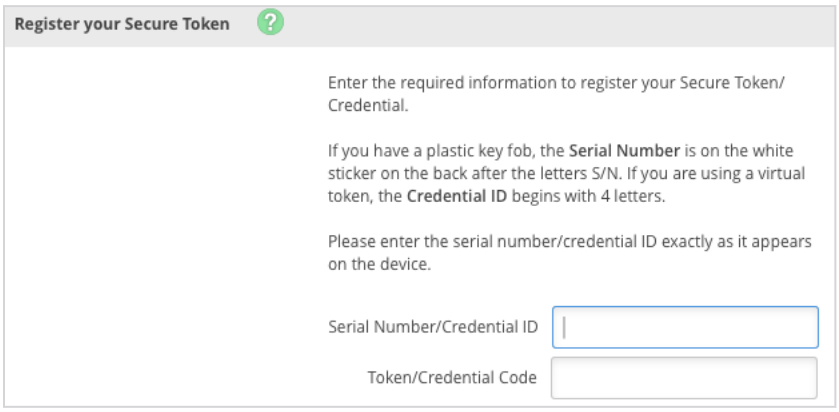
Enter the message that appears to users asking if the secure token has been received.



Registration Input Message

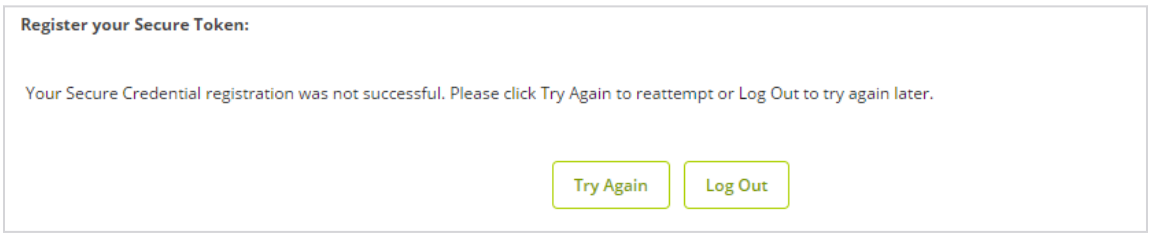
Enter the message that appears when the device registration information is entered.

© 1999-2020 Jack Henry & Associates, Inc.



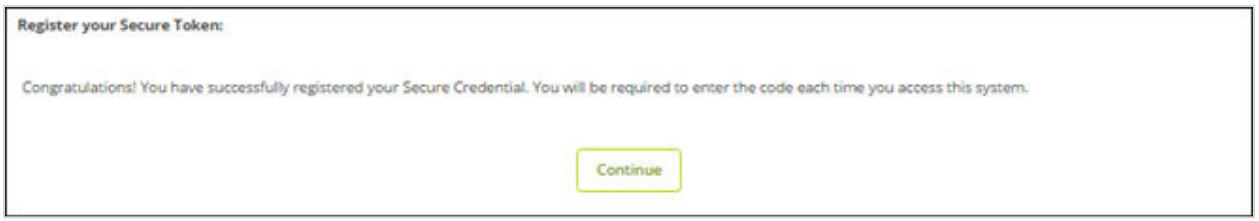
Registration Error Message

Enter the message that appears if a device is not successfully registered.



Registration Confirmation Message

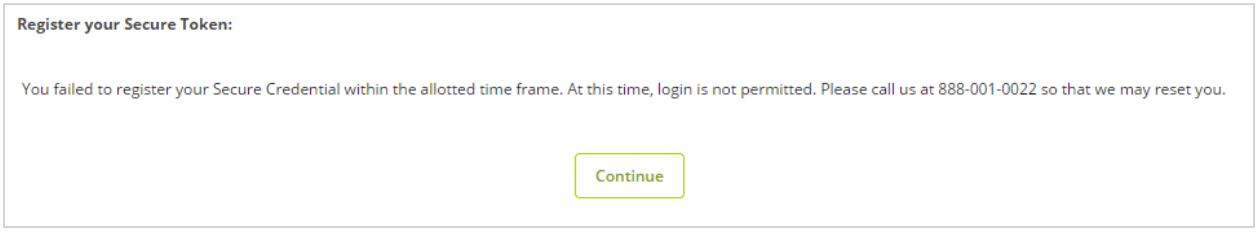
Enter the message that appears when registration of the secure token is successfully completed.



Block Message

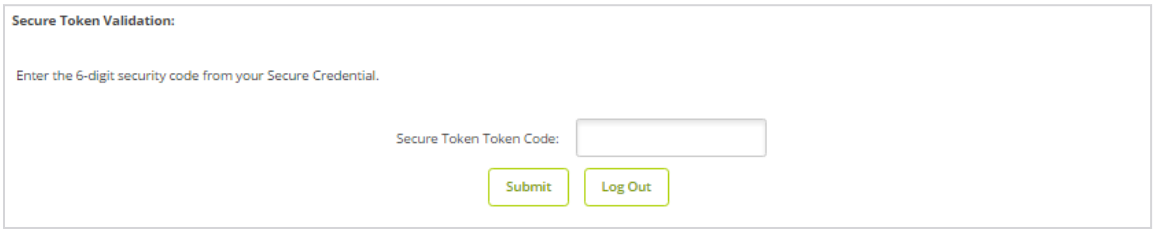
Enter the message that appears when a token is not registered in the allotted time frame.

© 1999-2020 Jack Henry & Associates, Inc.



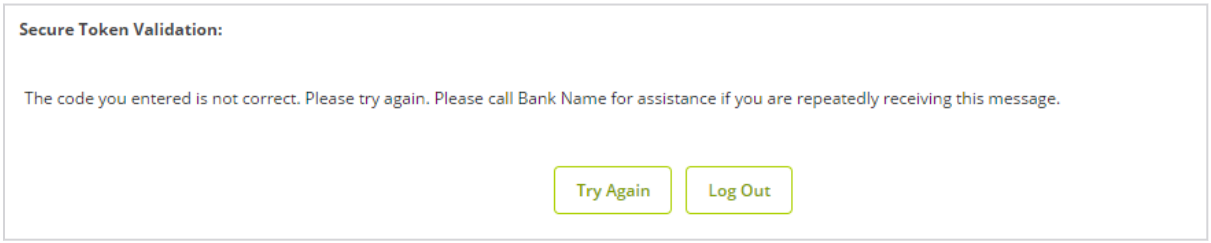
Authentication Prompt Message

Enter the message that prompts users to enter their token credentials during logon or during NetTeller Security Manager authentication.



Validation Error Message

Enter the message that appears when you enter an invalid code.



Registering a User for Secure Tokens

1. Go to **Manage Users** > **Manage Secure Token Users**.
   The following columns appear.

NetTeller ID

The NetTeller ID of the user matching the search criteria.

Alias

The established NetTeller alias.

Name

© 1999-2020 Jack Henry & Associates, Inc.

The full name of the cash user established during user setup. For retail users, this is the name tied to the NetTeller ID.

Active

The status of the NetTeller ID's secure token settings.

Users

The number of users tied to the NetTeller ID.

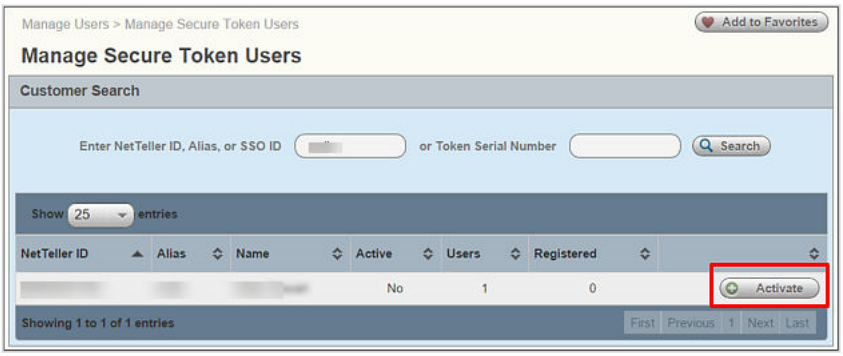
Registered

The number of users who have completed registration.

2. Search by the **NetTeller ID**, **Alias**, **SSO ID**, or **Token Serial Number**.
3. Next to the desired ID, select **Activate**.

Activate

Select to activate a user for secure tokens.



Viewing Activated Users

Use this procedure to view and maintain NetTeller IDs that are currently activated for token authentication.

1. Go to **Manage Users** > **Manage Secure Token Users**.
   The following columns appear.

NetTeller ID

The NetTeller ID of the user matching the search criteria.

Alias

The established NetTeller alias.

Name

The full name of the cash user established during user setup. For retail users, this is the name tied to the NetTeller ID.

Active

© 1999-2020 Jack Henry & Associates, Inc.

The status of the NetTeller ID's secure token settings.

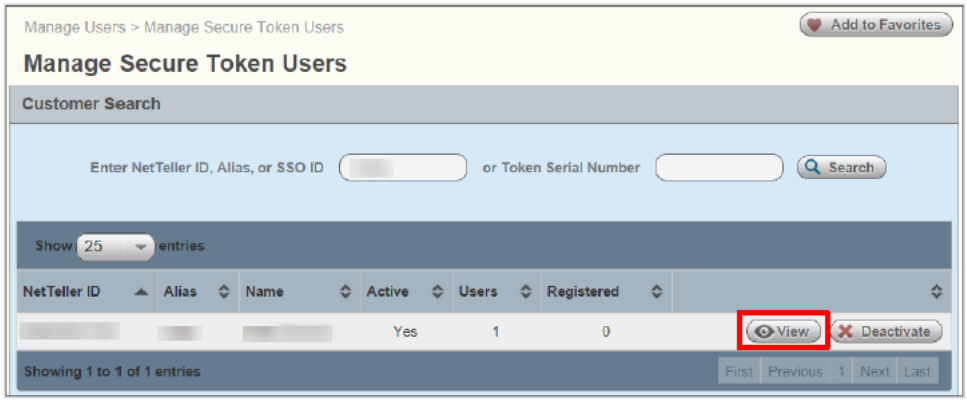
Users

The number of users tied to the NetTeller ID.

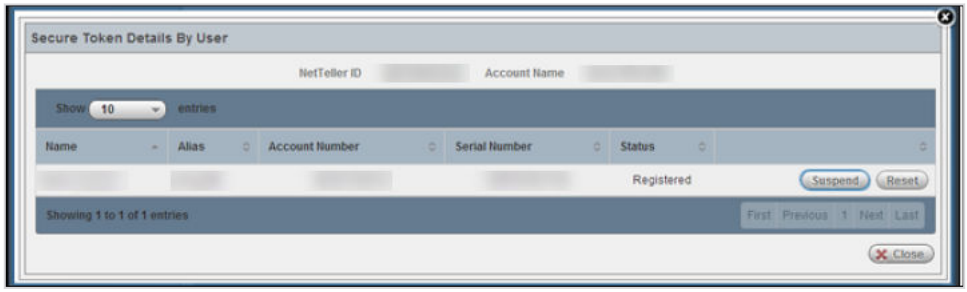
Registered

The number of users who have completed registration.

2. Search for the user by the **NetTeller ID**, **Alias**, **SSO ID**, or **Token Serial Number** to filter your results.
3. Next to the desired user, select **View** to view the individual user and token details.



Details for the secure token user appear.



Selected details are defined in the following list.

Account Number

The account number generated during registration. This number can be used to look up a user in the VIP Manager Back Office module. Users cannot see this number.

Serial Number

The serial number related to the secure token. The serial number only appears if you have registered the device. Each user can only have one serial number.

© 1999-2020 Jack Henry & Associates, Inc.

Status

The status of the secure token user:

- *SSO Required* - The cash user has not yet established the single sign-on ID for Cash Management. Single sign-on is required to use secure tokens.
- *Not Registered* - The user has not registered the token.
- *Registered* - The user has successfully registered the device.

Suspend

Select to turn off token prompt at logon. Suspended users are able to log on to NetTeller using only a correct user name and password.

Unsuspend

Select to turn on token authentication prompt for suspended users.

Reset

Select to require re-registration of the secure token. Use this option if the credentials were not registered in the original allotted time frame set up in **Days Before Access Block**. You can also use this option to register new credentials.

Symantec Verisign Identity Protection Manager (VIP Manager)

VIP stands for Verisign Identity Protection. JHA partners with Symantec/Verisign to provide secure tokens to users. The VIP Manager is a self-service site. All administrators that log on to the VIP Manager must have a secure token device.

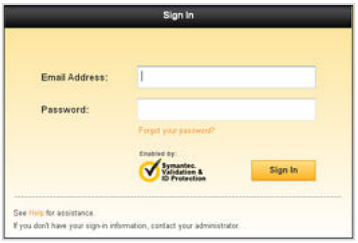
The VIP Manager is used for the following reasons:

- Resetting a token that does not sync up
- Deactivating a token to stop the billing
- Generating a temporary security code to keep the level of protection in place, even if the user forgot their token
- Viewing reports

Accessing VIP Manager

1. Access VIP Manager through one of the following options:
   - In NetTeller Back Office, go to **Home** > **External Admin Sites** > **Symantec Verisign VIP Manager**.
   - Go to *https://manager.vip.symantec.com/vipmgr/signin.v*.
2. Log on with your VIP Manager email address and password.

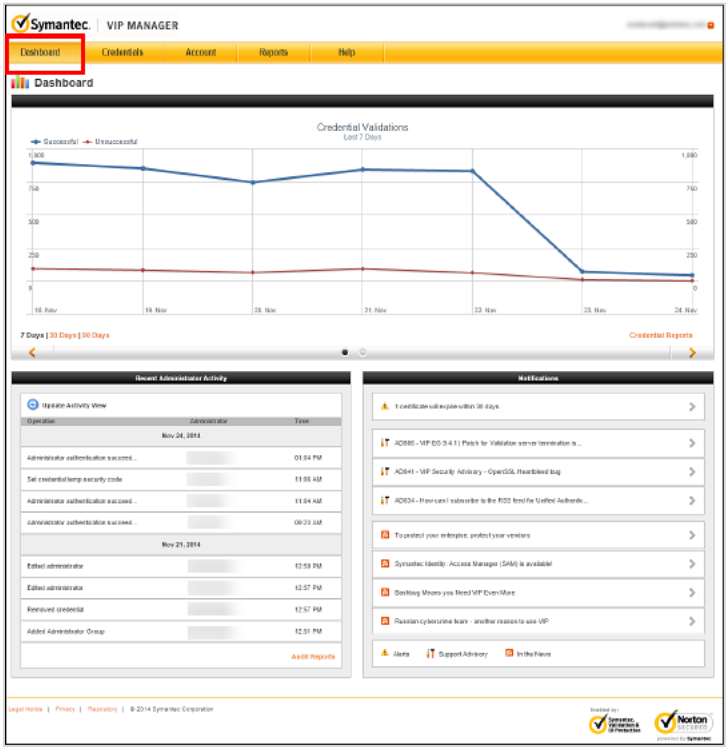
© 1999-2020 Jack Henry & Associates, Inc.



3. Enter the six-digit security code from the credential.

VIP Manager Dashboard

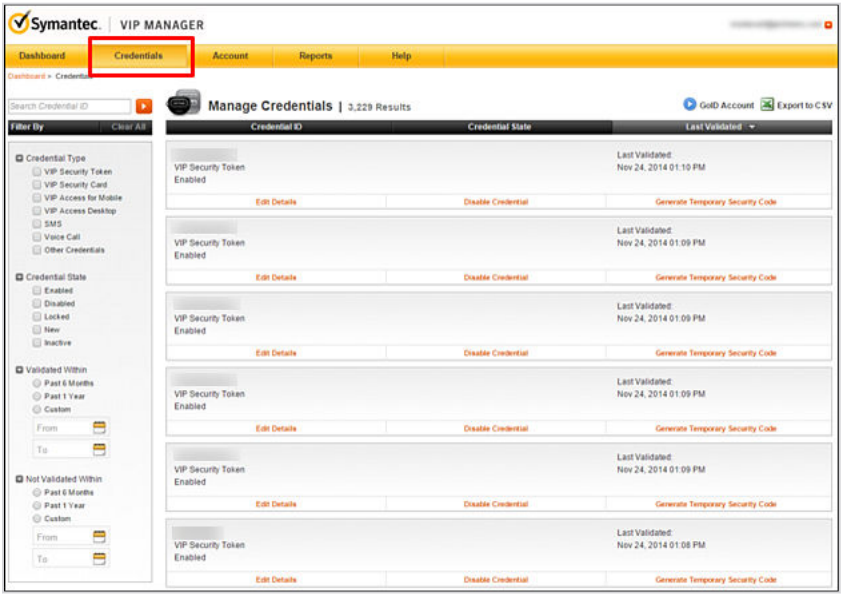
The *Dashboard* tab gives an overview of various activities that are related to credentials and back-office functions.



VIP Manager Credentials

From the *Credentials* tab, you can perform various actions on a credential ID. Some of those actions include:

- Generating a temporary security code.
- Disabling a credential.
- Resetting a credential.



The following is a list of credential states.

Disabled

The credential is in use with an associated account, but is not currently available. This state is set voluntarily, such as when a credential is lost or stolen. Temporary security codes are allowed.

New

The credential is not registered.

Enabled

The credential is in use. Financial institutions are billed for the number of enabled credentials.

Inactive

The credential is in use with an associated account but is not currently available. This state does not permit the use of temporary security codes. This state also stops billing.

© 1999-2020 Jack Henry & Associates, Inc.

Locked

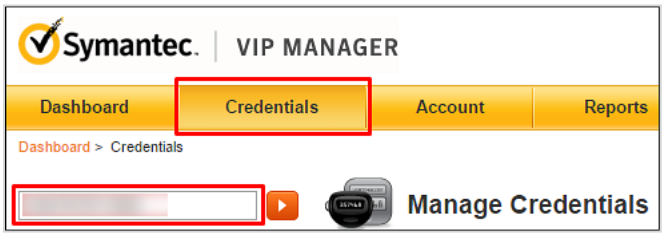
The system locks a token after entering 10 consecutive incorrect security codes.

Search for a Credential

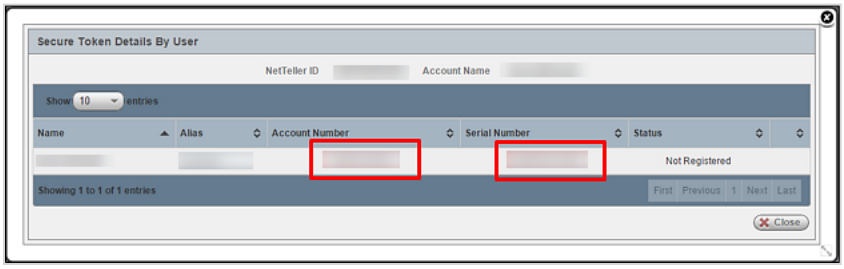
There are two options that your institution can use to search for a credential.

Option One

Search by the credential ID.



The GoID account number and credential ID (serial number) are found by going to **NetTeller Back Office** > **Manag Users** > **Manage Secure Token Users** > **View**.

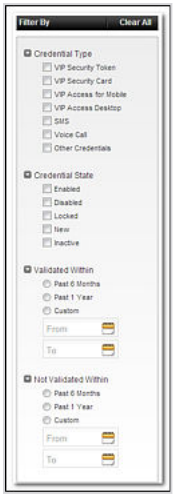


Option Two

This option consists of searching using the following methods:

- **Credential Type**
- **Credential State**
- **Validation Within Date**

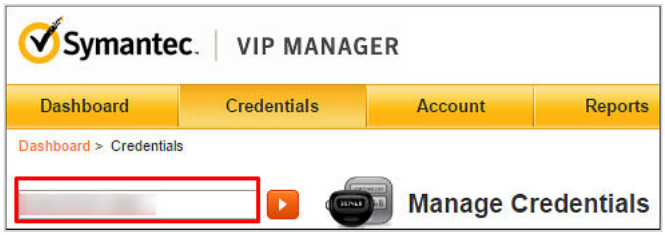
© 1999-2020 Jack Henry & Associates, Inc.



Generating a Temporary Security Code

If a user does not have their token, you can generate a temporary code, and the user can log on to NetTeller using the temporary code.

1. Search for the credential.



2. Select **Generate Temporary Security Code**.

3. Select if the temporary code is for a one-time use or multiple uses.

> **NOTE**
> If one-time use is selected, the code expires after one logon. If multiple uses is selected, you must enter an expiration date.

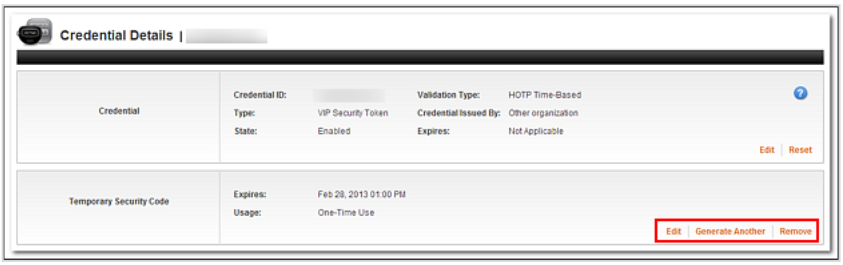
© 1999-2020 Jack Henry & Associates, Inc.

4. If you want to delete a multiple use security code before the expiration date, use the following steps.

   a) Select **Edit Details**.

   b) Select **Remove**.

5. If you want to update the expiration date, use the following steps.



   a) Select **Edit Details**.

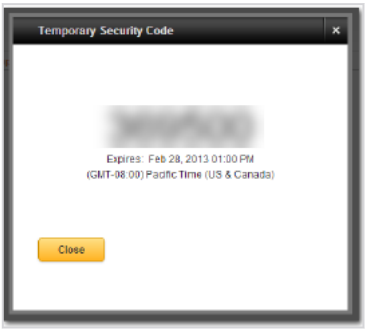
   b) Select **Generate Another**.

      This step creates a new temporary security code.

6. Select **Generate**.

   A temporary code appears. Once you navigate away from this page, you cannot view this temporary code.

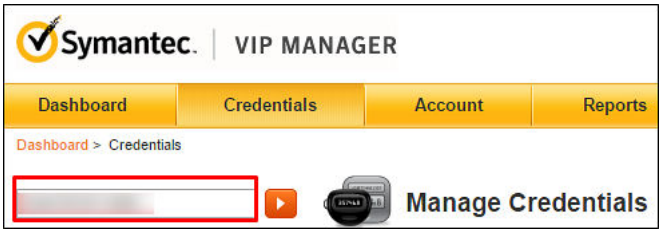
© 1999-2020 Jack Henry & Associates, Inc.



Deactivating a Credential

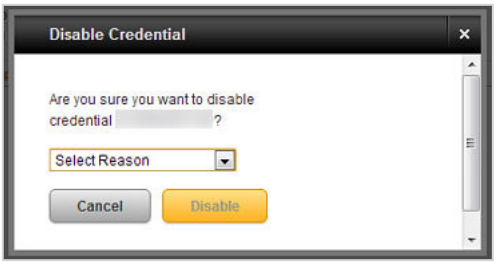
You can deactivate a credential if it is lost or stolen. Deactivating the token also stops billing.

1. Search for the credential.



2. Select **Disable Credential**.

3. Select the reason that you are disabling this credential, and then select **Disable**.



Select **Enable Credential** to enable this credential in the future. This option resumes billing.

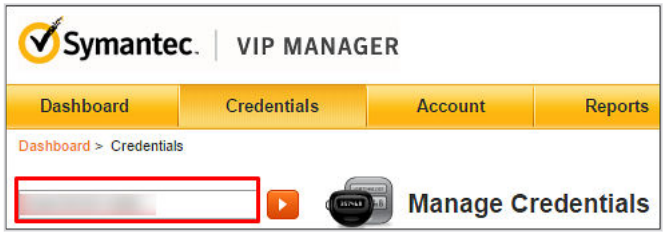
© 1999-2020 Jack Henry & Associates, Inc.

Resetting a Credential

In order to reset a credential, you must have access to the credential in real-time.

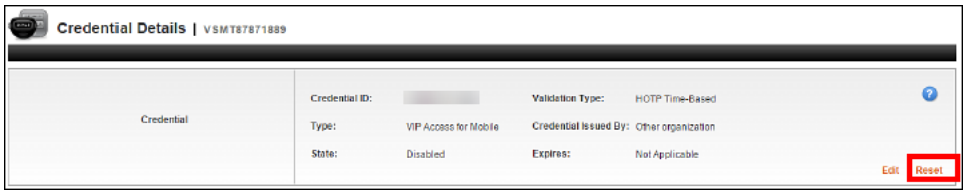
Sometimes Secure Tokens users report that their security code is not accepted. If this error occurs, it is necessary to check the credential to find out if there is a data mismatch.

1. Search for the credential.



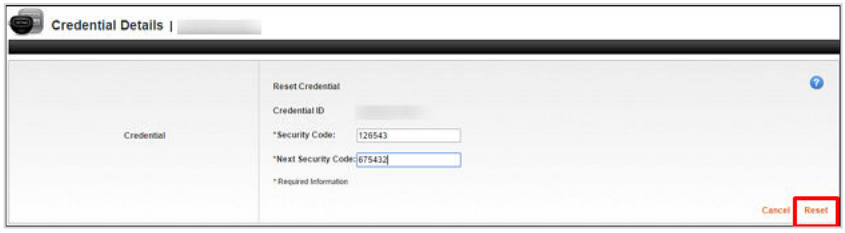
2. Select **Edit Details**.

3. Select **Reset**.



4. Enter two consecutive security codes from the credential, and then select **Reset**.

© 1999-2020 Jack Henry & Associates, Inc.

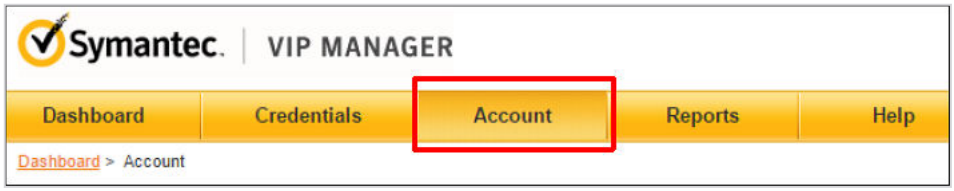


A confirmation message appears at the top of the screen.

Creating VIP Administrators

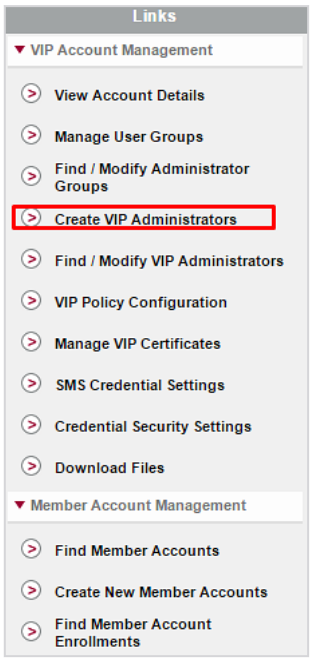
Use this option to create new VIP administrators that have access to the VIP Manager back office.

1. Select **Account**.

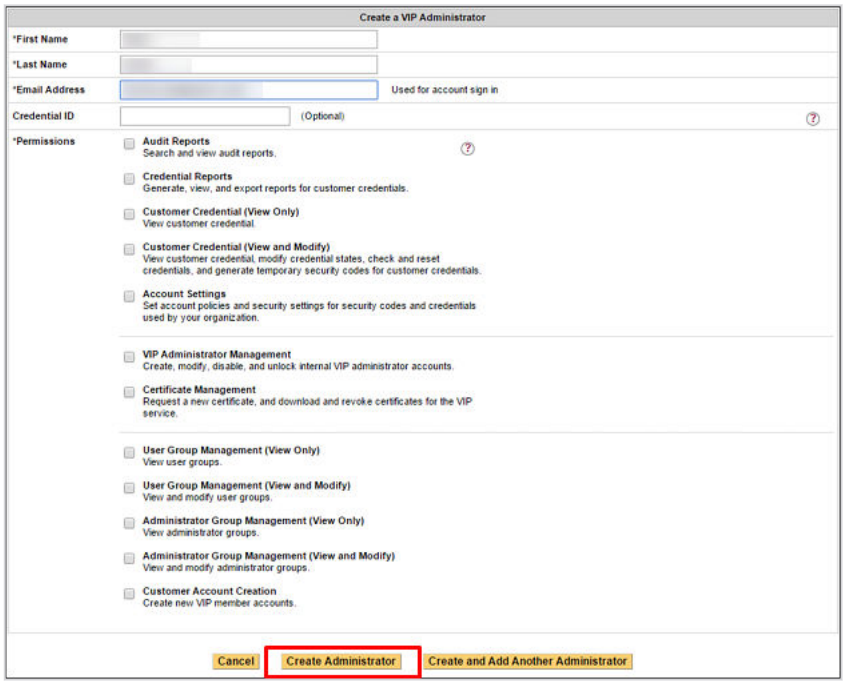


2. Select **Create VIP Administrators**.

© 1999-2020 Jack Henry & Associates, Inc.



3. Complete the required fields and user permissions, and then select **Create Administrator**.

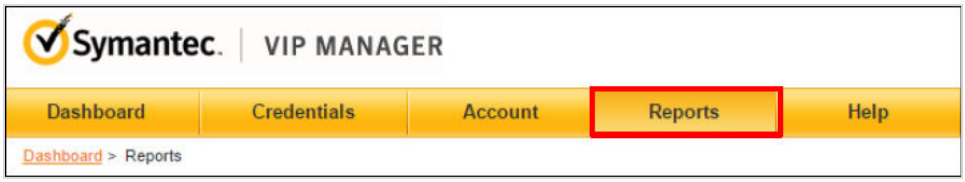


> **NOTE**
> An asterisk indicates a required field.

The user receives an email with instructions to log on.

Reports

Select **Reports** to view credential and internal audit reports.



The following is a list of credential reports.

Current Report

Number of tokens currently in use, sorted by credential state.

Historical Report

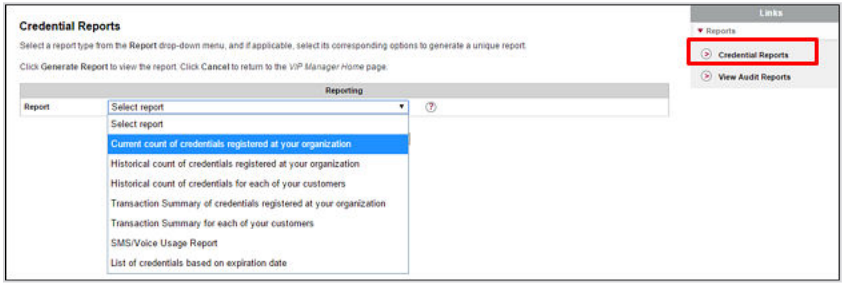
Search for a date range.

Transaction Report

A count of user activity.

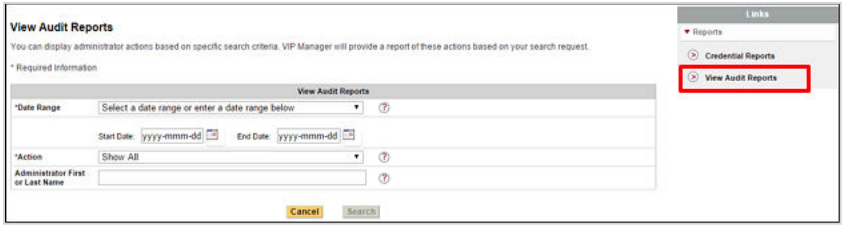
Expiration Date Report

Search by the date that the tokens are set to expire.



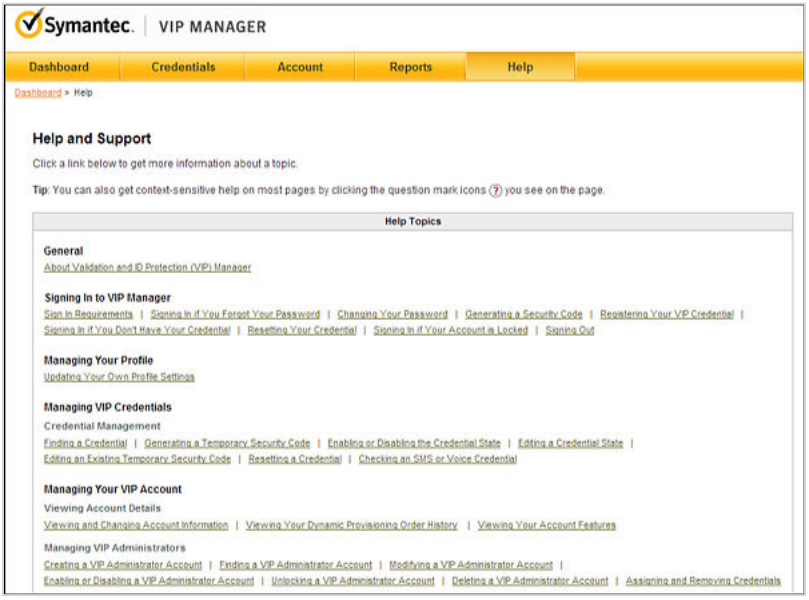
Audit Reports

Search by date range, action, or administrator. This report is for back-office audits.



Help

VIP Manager has a strong online help section. Use it to learn more about available features.



Registering a Customer Support Representative's Token

Secure tokens provide your employees an additional layer of authentication.

If your financial institution has enabled both secure tokens and **Enable Two-Factor for Back Office/ESI Management** in **NetTeller Back Office** > **Manage Products** > **Secure Tokens**, you are prompted to register your token upon your first NetTeller Back Office logon.

Complete the following steps to register your token during your initial logon.

1. Log on to NetTeller Back Office using your **Financial Institution Number**, **User Name**, and **Password**.
2. Complete the **Serial Number/Credential ID** and **Token/Credential Code** fields to register your token, and then select **Continue**.
   A *Registration Successful* screen appears.

   > **TIP**
   > If you entered incorrect information, the *Registration Error* screen appears instead. You can select **Try Again** to attempt registering the token again.
3. Select **Continue**.

© 1999-2020 Jack Henry & Associates, Inc.

Once you have registered your token and after every time you log on, a validation screen appears.

4. Enter your **Secure Credential Code**, and then select **Submit** to access the site.

> **TIP**
> If you enter an incorrect token code, enter the same code used during registration, leave the field blank, or if the token is in a state other than *Registered*, you see the *Validation Error* screen where you can **Try Again**.

You have successfully registered your token.

For subsequent logons, enter your token's code to log on to NetTeller Back Office. If you use ESI Management, the token authentication established in the NetTeller Back Office session applies to ESI Management.

Reset a Customer Support Representative's Token

You can reset a token so that the Customer Support Representative (CSR) can re-register their token.

To reset a CSR's token, go to **NetTeller Back Office** > **Manage Users** > **Manage CSR List** > **Edit User**. Next to the **Token Status** field, select **Reset**. The CSR is then prompted upon their next NetTeller Back Office logon to re-register their token.

Generating Temporary Token Codes for Misplaced Tokens

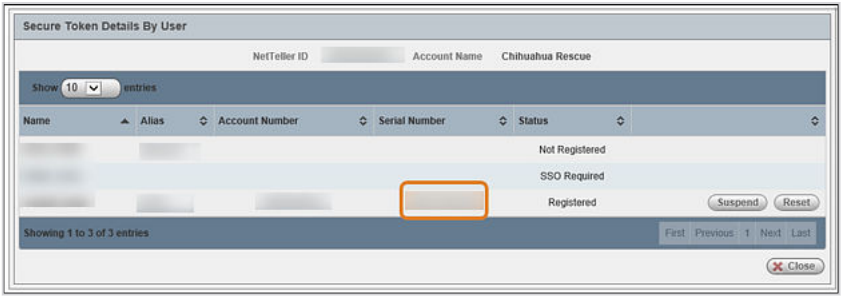
If a user must access NetTeller but does not have their token with them or has misplaced their token, you can generate a temporary token code for them to use.

> **TIP**
> If you are a CSR and you know your token serial number but you cannot generate a token code, you can generate a temporary token code. Log on to Symantec™ VIP Manager and complete the following steps beginning at step 3.

1. View user information.
   a) Go to NetTeller Back Office.
   b) Select **Manage Users**.
   c) Select **Manage Secure Token Users**.

© 1999-2020 Jack Henry & Associates, Inc.

2. Copy the user's serial number.



3. Search using the serial number to locate credential in the Symantec™ VIP Manager.
4. Select **Generate Temporary Security Code**.

5. Establish the usage and expiration and select **Generate**.

© 1999-2020 Jack Henry & Associates, Inc.

Assisting Users with Lost Tokens

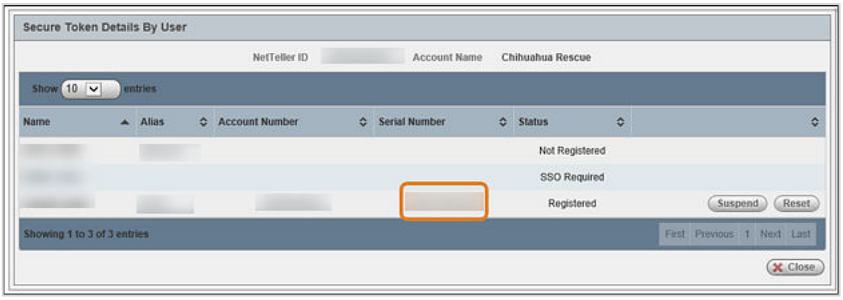
If a user loses their token, you can do any of the following actions:

- Deactivate the lost token.
- Provide the user with a new token.
- Prompt for the registration of a new token.

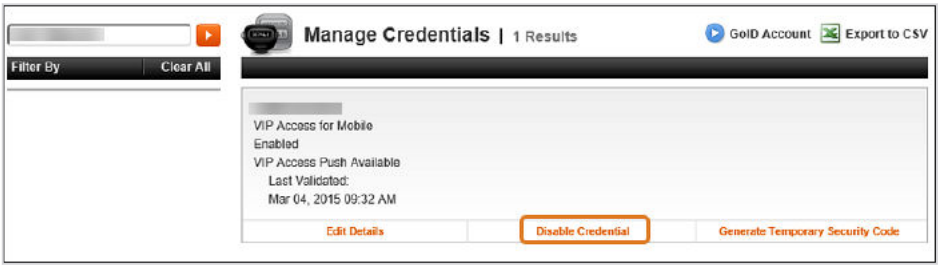
1. View user information.
   a) Go to NetTeller Back Office.
   b) Select **Manage Users**.
   c) Select **Manage Secure Token Users**.

2. Copy the user's **Serial Number**.

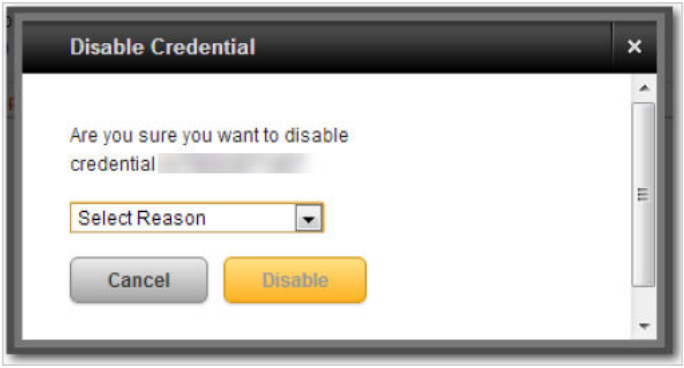
© 1999-2020 Jack Henry & Associates, Inc.



3. Search using the serial number to locate the credential in the Symantec Back Office.
4. Select **Disable Credential**.

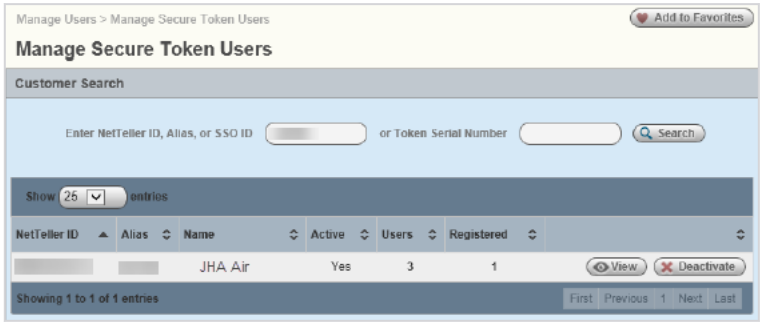


5. Select the reason for disabling the token.

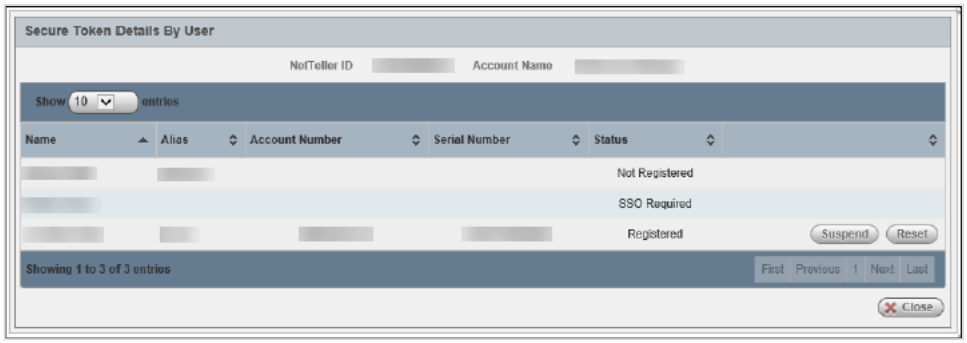


6. Provide user with a new token or assist them with downloading a new one.
7. To view user information, go to NetTeller Back Office.
8. Select **Manage Users**.
9. Select **Manage Secure Token Users**.

© 1999-2020 Jack Henry & Associates, Inc.



10. Select **Reset** for user.

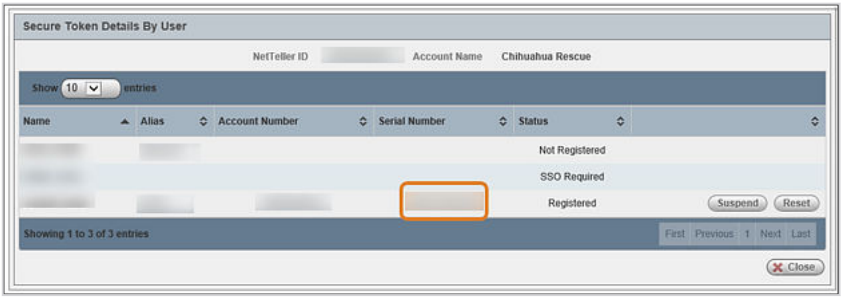


Registering a New Token

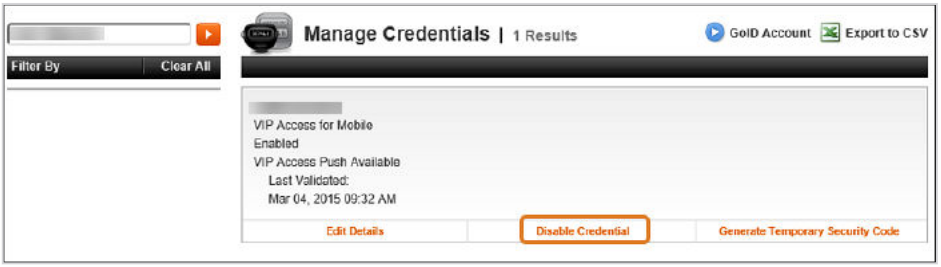
Users with a new token must go through the registration process again.

1. View user information.
   a) Go to NetTeller Back Office.
   b) Select **Manage Users**.
   c) Select **Manage Secure Token Users**.

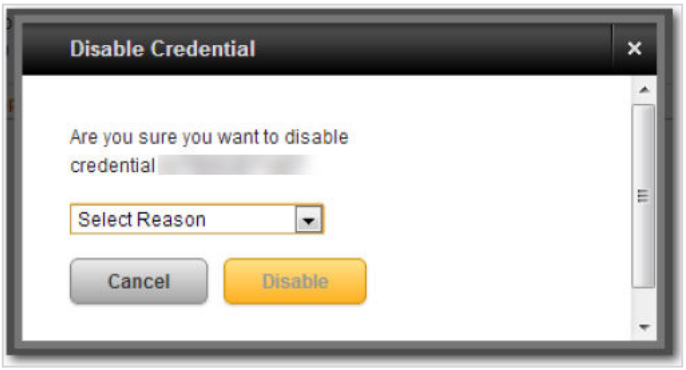
2. Copy the user's serial number.



3. Search using the serial number to locate the credential in the Symantec Back Office.
4. Select **Disable Credential**.

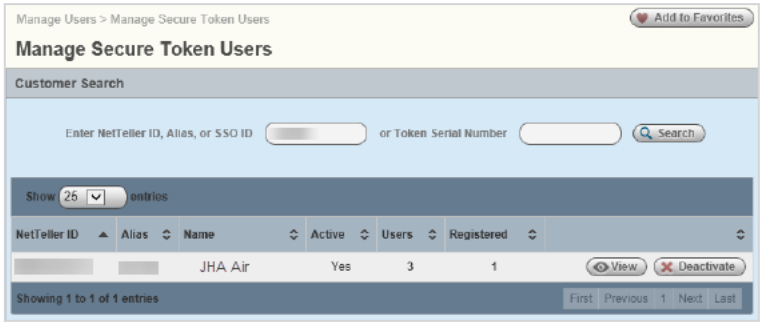


5. Select the reason for disabling the token.

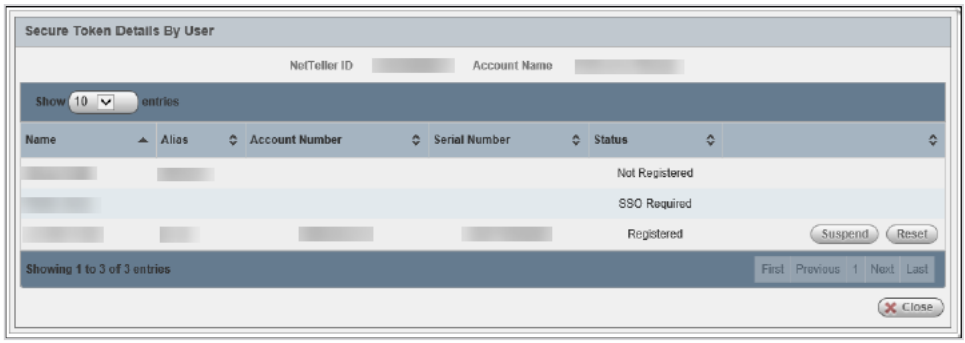


6. Provide user with a new token or assist them with downloading a new one.
7. To view user information, go to NetTeller Back Office.
8. Select **Manage Users**.
9. Select **Manage Secure Token Users**.

© 1999-2020 Jack Henry & Associates, Inc.



10. Select **Reset** for user.

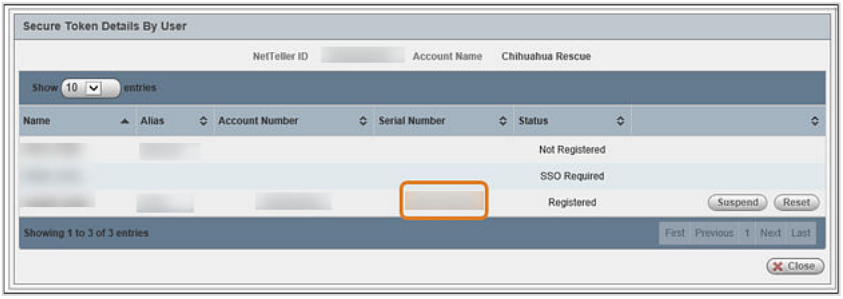


Troubleshooting an Invalid Token

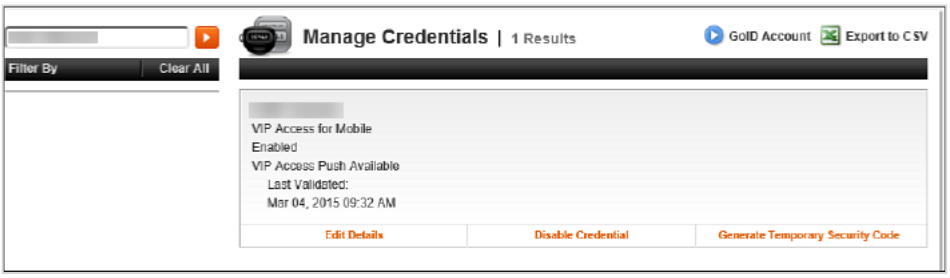
At times, a miscommunication occurs between NetTeller and Symantec. If a user receives an invalid code error, resetting the token corrects the error.

1. View user information.
   a) Go to NetTeller Back Office.
   b) Select **Manage Users**.
   c) Select **Manage Secure Token Users**.

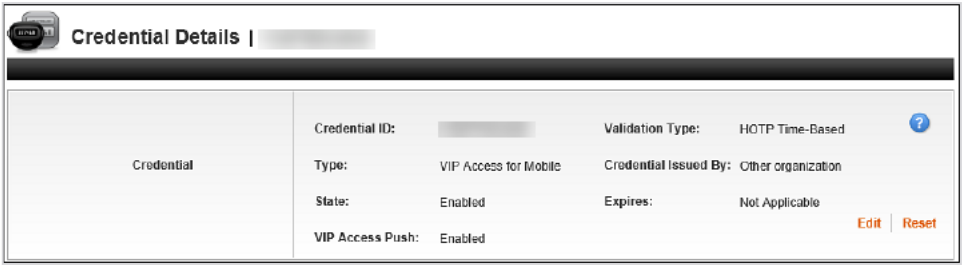
2. Copy the user's serial number.



3. Search using the serial number to locate the credential in the Symantec Back Office.
4. Select **Edit Details**.



5. Select **Reset**.



6. While speaking with the user, enter two consecutive security codes.

© 1999-2020 Jack Henry & Associates, Inc.

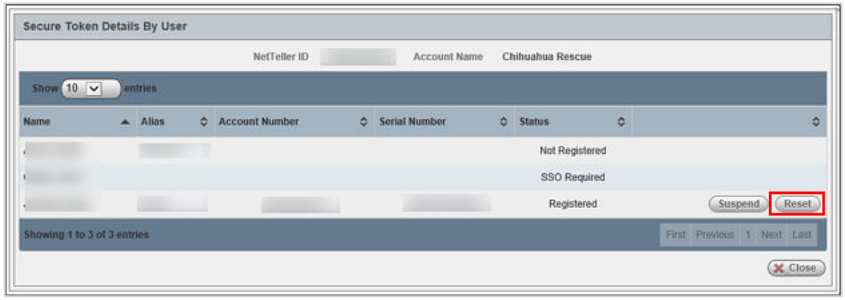
7. Select **Reset**.
   The user can now enter their credential information.

Resetting a Blocked User

Financial institutions assign a user a specific number of days to register their token. If the token is not registered in that time frame, the user is blocked from logging on to NetTeller. After this occurs, the registration time period must be reset.

1. View user information.
   a) Go to NetTeller Back Office.
   b) Select **Manage Users**.
   c) Select **Manage Secure Token Users**.

2. Select **Reset** for the desired user.



© 1999-2020 Jack Henry & Associates, Inc.