Do Not Pay
User Enrollment Guide
for PKI Token Users

August 2019

Table of Contents

About This Enrollment Guide

This guide is intended for new users of the Do Not Pay Portal (the Portal) that use a Public Key Infrastructure (PKI) Token. This guide illustrates the steps necessary to gain access to the Portal. The information in this reference guide has been divided into nine sections. Each section provides a brief description of each topic to provide the user guidance on each step of the enrollment process.

I. DNP OVERVIEW

The Do Not Pay Business Center provides services and support activities related to the identification, detection, and prevention of improper payments under the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) and the Federal Improper Payments Coordination Act of 2015 (FIPCA).

- The Office of Management and Budget (OMB) designated the Department of the Treasury to host the working system to assist agencies in detecting and preventing improper payments.

- The Bureau of the Fiscal Service (Fiscal Service) operates the DNP Business Center.

The mission of DNP is to protect the integrity of the federal government's payment processes by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals.

DNP provides multiple data sources so that agencies can verify eligibility of a vendor, grantee, loan recipient, or beneficiary. Agencies can make payment eligibility decisions at any time during the payment lifecycle for example, during pre-award and pre-payment eligibility verification.

- DNP is a **no cost** resource for federal agencies and federally funded state administered programs
- DNP is **not** a list of entities or people that should not be paid
- DNP offers customized data analysis to help agencies detect fraud, waste, and abuse as well as strengthen internal controls
- DNP meets existing federal data security and privacy standards
- DNP is committed to providing:
    - quality data
    - more data sources
    - continuous system development
    - cutting edge data analytics
    - customized agency outreach

DNP Business Center Components:

Web-based Portal

The DNP Portal provides the capability of multiple data source searches simultaneously. You can search for a single person or entity; you can batch your searches; and you can set up regular monitoring in the Portal.

The Portal has four ways to deliver match information to an agency. The delivery method is based upon approved data sources and where in the payment lifecycle the match is reviewed.

- Online Search
- Batch Matching
- Continuous Monitoring
- Payment Integration

Data Analytics

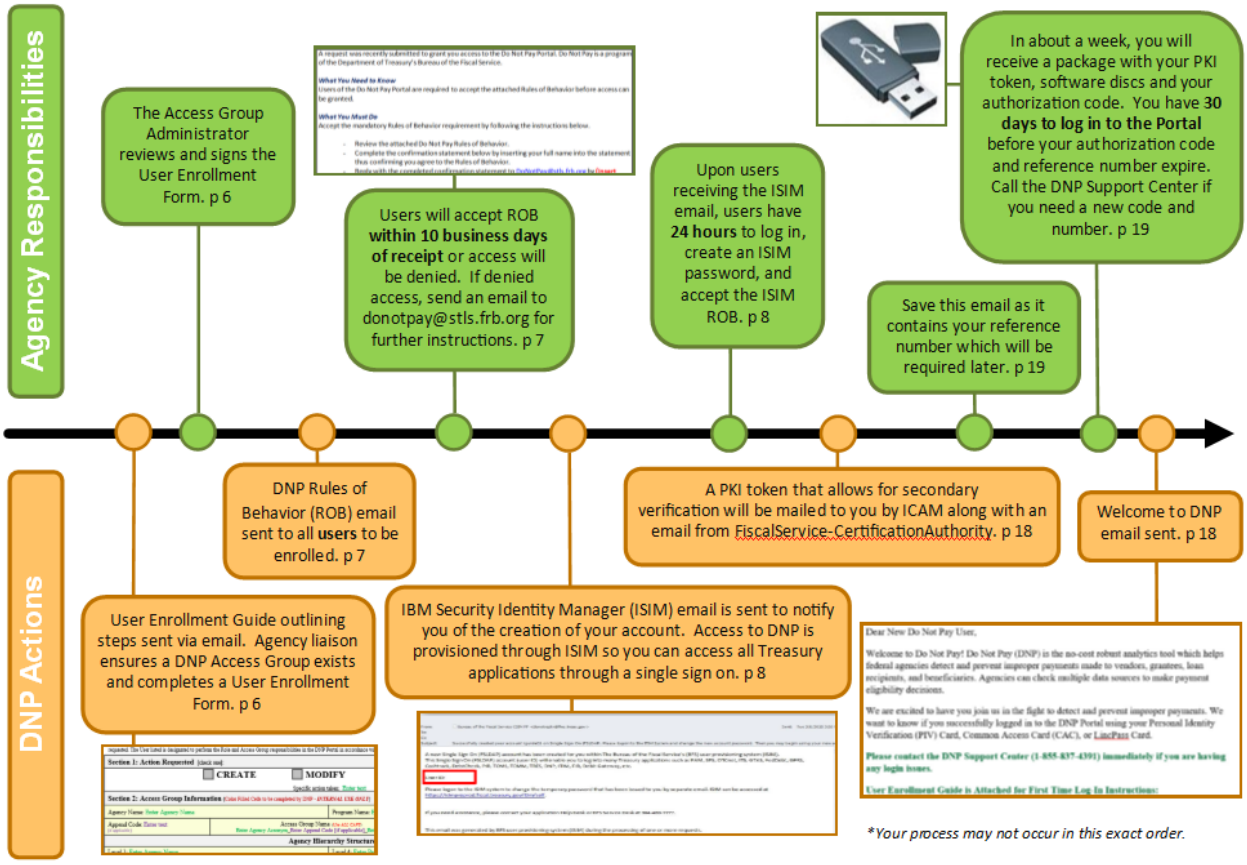
Data Analytics provides advanced payment analysis to federal agencies. In partnership with the agencies, a variety of data analysis and visualizations can be conducted to help combat improper payments.

- Analyzes payment data for indicators that a payment is being made in error or is vulnerable to abuse
- Develops risk scoring to help agencies prioritize and manage reviewing and investigating cross-matches
- Screens payees for eligibility such as identifying deceased beneficiaries

Agency Support

Agency Support is made up of onboarding specialists, outreach liaisons, and a help desk. Agency Support works with agencies to meet program needs, determine and target the best DNP processes and data sources, and provide training, Portal demonstrations, and share knowledge. Agency Support hosts community of events to share best practices for addressing improper payments, as well as assist with business processes by helping agencies map DNP into existing business processes.

PKI Token Onboarding Process Overview



This is a high-level flowchart of the DNP PKI Token onboarding process. These steps are detailed within this document.

II. COMPLETING FORMS

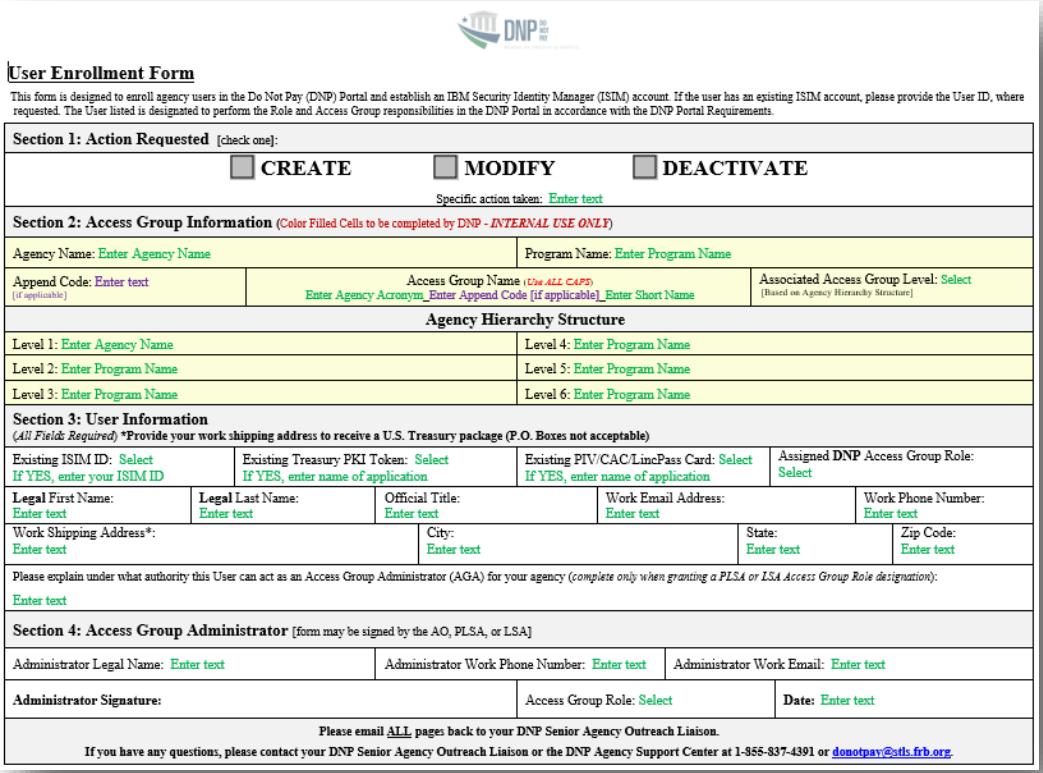
Senior Agency Outreach Liaison Sends User Enrollment Form

Your agency's Point of Contact (PoC) will receive an email from your Senior Agency Outreach Liaison after the access group has been created. This email will contain a User Enrollment Form that must be reviewed and completed for each anticipated Portal user. If an anticipated Portal user has an existing U.S. Treasury issued Public Key Infrastructure (PKI) Token for another U.S. Treasury application (e.g., SPS, JFICS, etc.), this must be indicated on the User Enrollment Form.

Access Group Administrator (AGA) Completes and Signs the User Enrollment Form

Your Senior Agency Outreach Liaison will populate all the "Internal Use Only" fields within your User Enrollment Form before sending to your agency. The remaining fields will need to be completed and the form must be signed by your agency's designated AGA. Your agency's Authorizing Official (AO), Primary Local Security Administrator (PLSA), or Local Security Administrator (LSA) can act as an AGA; AGAs designate which access group a user is permitted to view. The DNP Program requires that each page of your User Enrollment Form be returned to your Senior Agency Outreach Liaison. If there are questions regarding specific fields within your form, your Senior Agency Outreach Liaison can assist you.

Example of the User Enrollment Form:



User Enrollment Form

This form is designed to enroll agency users in the Do Not Pay (DNP) Portal and establish an IBM Security Identity Manager (ISIM) account. If the user has an existing ISIM account, please provide the User ID, where requested. The User listed is designated to perform the Role and Access Group responsibilities in the DNP Portal in accordance with the DNP Portal Requirements.

Section 1: Action Requested [check one]:			
☐ **CREATE**	☐ **MODIFY**	☐ **DEACTIVATE**	
Specific action taken: Enter text			
Section 2: Access Group Information (Color Filled Cells to be completed by DNP - *INTERNAL USE ONLY*)			
Agency Name: Enter Agency Name		Program Name: Enter Program Name	
Append Code: Enter text [if applicable]	Access Group Name (*Use ALL CAPS*) Enter Agency Acronym_Enter Append Code [if applicable]_Enter Short Name	Associated Access Group Level: Select [Based on Agency Hierarchy Structure]	
Agency Hierarchy Structure			
Level 1: Enter Agency Name		Level 4: Enter Program Name	
Level 2: Enter Program Name		Level 5: Enter Program Name	
Level 3: Enter Program Name		Level 6: Enter Program Name	
Section 3: User Information (*All Fields Required*) ***Provide your work shipping address to receive a U.S. Treasury package (P.O. Boxes not acceptable)**			
Existing ISIM ID: Select If YES, enter your ISIM ID	Existing Treasury PKI Token: Select If YES, enter name of application	Existing PIV/CAC/LincPass Card: Select If YES, enter name of application	Assigned **DNP** Access Group Role: Select
Legal First Name: Enter text	**Legal** Last Name: Enter text	Official Title: Enter text	Work Email Address: Enter text	Work Phone Number: Enter text
Work Shipping Address*: Enter text	City: Enter text	State: Enter text	Zip Code: Enter text
Please explain under what authority this User can act as an Access Group Administrator (AGA) for your agency (*complete only when granting a PLSA or LSA Access Group Role designation*): Enter text			
Section 4: Access Group Administrator [form may be signed by the AO, PLSA, or LSA]			
Administrator Legal Name: Enter text	Administrator Work Phone Number: Enter text	Administrator Work Email: Enter text	
Administrator Signature:	Access Group Role: Select	**Date:** Enter text	
Please email ALL pages back to your DNP Senior Agency Outreach Liaison. **If you have any questions, please contact your DNP Senior Agency Outreach Liaison or the DNP Agency Support Center at 1-855-837-4391 or donotpay@stls.frb.org.**			

Senior Agency Outreach Liaison Completes PKI Form and Requests a New PKI Token on Your Behalf

If your completed User Enrollment Form indicates that you do not have a U.S. Treasury issued PKI Token, your Senior Agency Outreach Liaison will complete the DNP PKI form, using information from your User Enrollment Form, which will be used to request a new PKI Token on your behalf. Once your PKI form has been processed, you should receive a U.S. Treasury package, along with your new PKI Token via UPS Overnight from the U.S. Treasury.

III. EMAILS

DNP Rules of Behavior Email

After your user enrollment form has been returned to your Senior Agency Outreach Liaison, you will receive an email from the DNP email box (DoNotPay@fiscal.treasury.org), asking you to review and accept our Rules of Behavior (RoB). Please ensure that you thoroughly review the requirements and accept the terms. Acceptance is as easy as filling in your name and replying to the original email sent from DNP.

Example of the RoB Email:

A request was recently submitted to grant you access to the Do Not Pay Portal. Do Not Pay is a program of the Department of Treasury's Bureau of the Fiscal Service.

What You Need to Know
Users of the Do Not Pay Portal are required to accept the attached Rules of Behavior before access can be granted.

What You Must Do
Accept the mandatory Rules of Behavior requirement by following the instructions below.

- Review the attached Do Not Pay Rules of Behavior.
- Complete the confirmation statement below by inserting your full name into the statement thus confirming you agree to the Rules of Behavior.
- Reply with the completed confirmation statement to DoNotPay@fiscal.treasury.org by **(insert date).**

****Note: Once you receive access you must login within 30 days or your access will be automatically deleted. ****

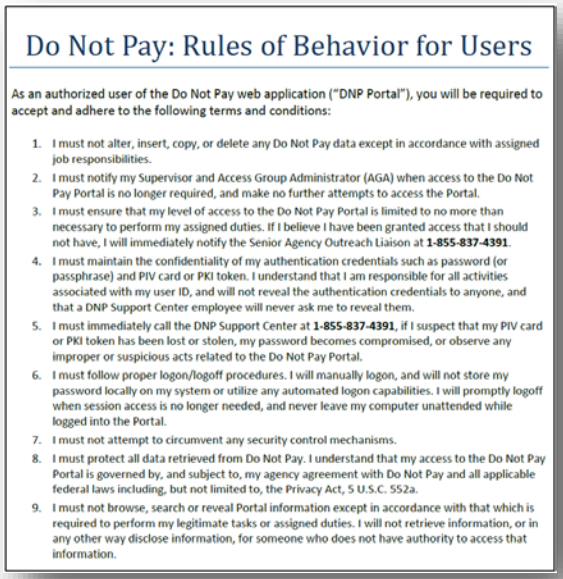
You must reply by (insert date) to avoid having your access to Do Not Pay denied.

Confirmation Statement:

I, **(insert full name here)**, have read and agree to the attached document in accordance with the Do Not Pay Rules of Behavior requirement.

*****Note: By replying to this email with a confirmation statement, you are stating that you agree to the Rules of Behavior for Do Not Pay.*****

Example of the attached RoB Document:



Do Not Pay: Rules of Behavior for Users

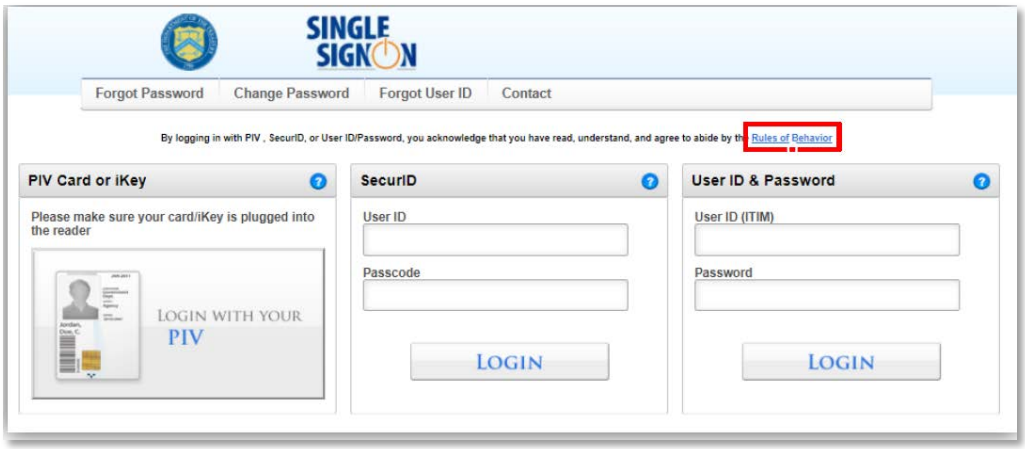
As an authorized user of the Do Not Pay web application ("DNP Portal"), you will be required to accept and adhere to the following terms and conditions:

1. I must not alter, insert, copy, or delete any Do Not Pay data except in accordance with assigned job responsibilities.
2. I must notify my Supervisor and Access Group Administrator (AGA) when access to the Do Not Pay Portal is no longer required, and make no further attempts to access the Portal.
3. I must ensure that my level of access to the Do Not Pay Portal is limited to no more than necessary to perform my assigned duties. If I believe I have been granted access that I should not have, I will immediately notify the Senior Agency Outreach Liaison at **1-855-837-4391**.
4. I must maintain the confidentiality of my authentication credentials such as password (or passphrase) and PIV card or PKI token. I understand that I am responsible for all activities associated with my user ID, and will not reveal the authentication credentials to anyone, and that a DNP Support Center employee will never ask me to reveal them.
5. I must immediately call the DNP Support Center at **1-855-837-4391**, if I suspect that my PIV card or PKI token has been lost or stolen, my password becomes compromised, or observe any improper or suspicious acts related to the Do Not Pay Portal.
6. I must follow proper logon/logoff procedures. I will manually logon, and will not store my password locally on my system or utilize any automated logon capabilities. I will promptly logoff when session access is no longer needed, and never leave my computer unattended while logged into the Portal.
7. I must not attempt to circumvent any security control mechanisms.
8. I must protect all data retrieved from Do Not Pay. I understand that my access to the Do Not Pay Portal is governed by, and subject to, my agency agreement with Do Not Pay and all applicable federal laws including, but not limited to, the Privacy Act, 5 U.S.C. 552a.
9. I must not browse, search or reveal Portal information except in accordance with that which is required to perform my legitimate tasks or assigned duties. I will not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.

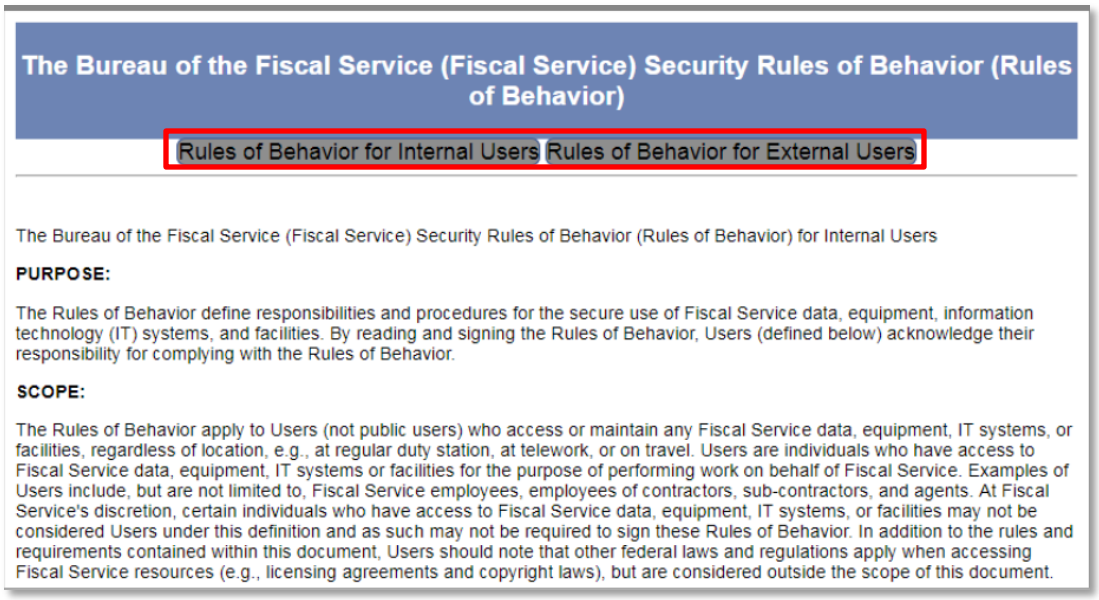
IBM Security Identity Manager (ISIM) Email

After you have accepted DNP's RoB, your User Enrollment Form will move to the user provisioning phase. Before granting access to the Portal, you must have an ISIM account. After your account has been provisioned, you will receive two automated emails; one with your ISIM User ID and one with a temporary ISIM password. You must login to create your ISIM password. **You have 24 hours to create an ISIM password; if not, the temporary password must be reset.**

In ISIM, you will be reminded on the Single Sign On page that by logging in, you agree to abide by the Rules of Behavior. A link will also be available that will direct you to review the Rules of Behavior. There is a set of Rules for both Internal and External Users.



You can either scroll or click the appropriate box to review the Rules of Behavior that apply to you.



The Bureau of the Fiscal Service (Fiscal Service) Security Rules of Behavior (Rules of Behavior)

Rules of Behavior for Internal Users | Rules of Behavior for External Users

The Bureau of the Fiscal Service (Fiscal Service) Security Rules of Behavior (Rules of Behavior) for Internal Users

PURPOSE:

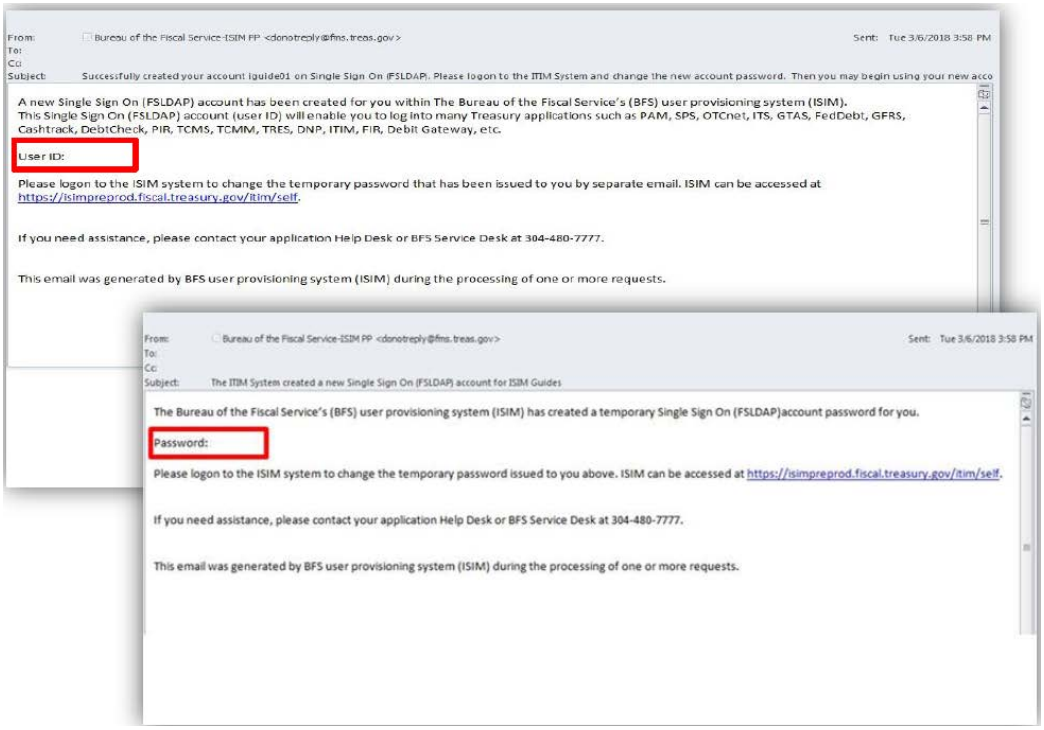
The Rules of Behavior define responsibilities and procedures for the secure use of Fiscal Service data, equipment, information technology (IT) systems, and facilities. By reading and signing the Rules of Behavior, Users (defined below) acknowledge their responsibility for complying with the Rules of Behavior.

SCOPE:

The Rules of Behavior apply to Users (not public users) who access or maintain any Fiscal Service data, equipment, IT systems, or facilities, regardless of location, e.g., at regular duty station, at telework, or on travel. Users are individuals who have access to Fiscal Service data, equipment, IT systems or facilities for the purpose of performing work on behalf of Fiscal Service. Examples of Users include, but are not limited to, Fiscal Service employees, employees of contractors, sub-contractors, and agents. At Fiscal Service's discretion, certain individuals who have access to Fiscal Service data, equipment, IT systems, or facilities may not be considered Users under this definition and as such may not be required to sign these Rules of Behavior. In addition to the rules and requirements contained within this document, Users should note that other federal laws and regulations apply when accessing Fiscal Service resources (e.g., licensing agreements and copyright laws), but are considered outside the scope of this document.

You will receive the following two emails. The first email includes your ISIM User ID while the second includes your temporary ISIM password. For security purposes, they are sent separately.

Example of ISIM Emails:



From: Bureau of the Fiscal Service-ISIM PP <donotreply@fms.treas.gov> Sent: Tue 3/6/2018 3:58 PM
To:
Cc:
Subject: Successfully created your account iguide01 on Single Sign On (FSLDAP). Please logon to the ITIM System and change the new account password. Then you may begin using your new acco

A new Single Sign On (FSLDAP) account has been created for you within The Bureau of the Fiscal Service's (BFS) user provisioning system (ISIM).
This Single Sign On (FSLDAP) account (user ID) will enable you to log into many Treasury applications such as PAM, SPS, OTCnet, ITS, GTAS, FedDebt, GFRS, Cashtrack, DebtCheck, PIR, TCMS, TCMM, TRES, DNP, ITIM, FIR, Debit Gateway, etc.

User ID:

Please logon to the ISIM system to change the temporary password that has been issued to you by separate email. ISIM can be accessed at https://isimpreprod.fiscal.treasury.gov/itim/self.

If you need assistance, please contact your application Help Desk or BFS Service Desk at 304-480-7777.

This email was generated by BFS user provisioning system (ISIM) during the processing of one or more requests.

From: Bureau of the Fiscal Service-ISIM PP <donotreply@fms.treas.gov> Sent: Tue 3/6/2018 3:58 PM
To:
Cc:
Subject: The ITIM System created a new Single Sign On (FSLDAP) account for ISIM Guides

The Bureau of the Fiscal Service's (BFS) user provisioning system (ISIM) has created a temporary Single Sign On (FSLDAP)account password for you.

Password:

Please logon to the ISIM system to change the temporary password issued to you above. ISIM can be accessed at https://isimpreprod.fiscal.treasury.gov/itim/self.

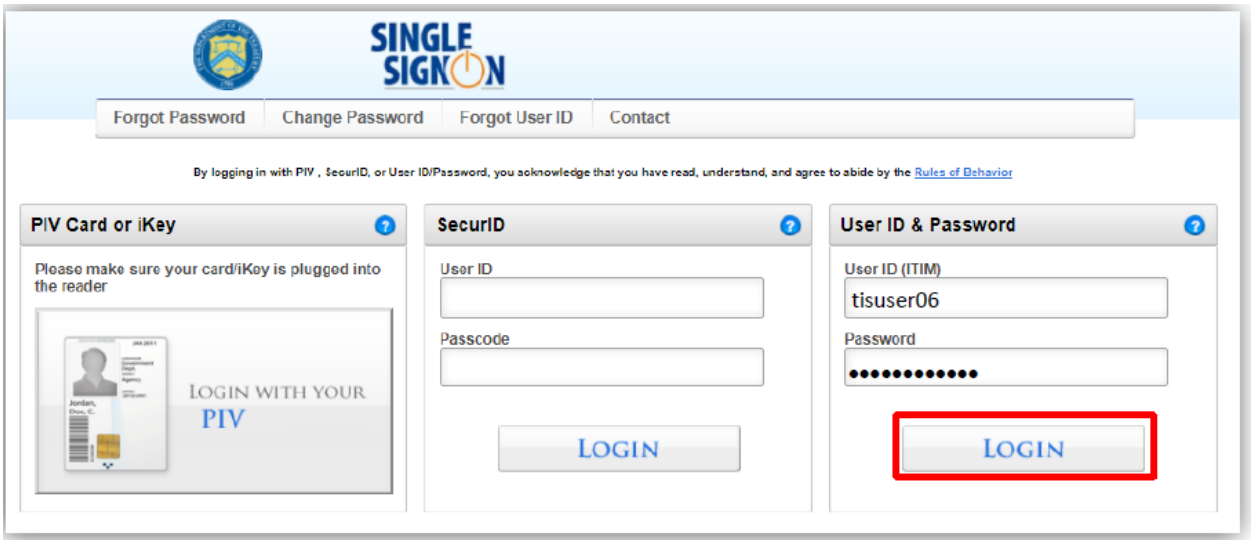
If you need assistance, please contact your application Help Desk or BFS Service Desk at 304-480-7777.

This email was generated by BFS user provisioning system (ISIM) during the processing of one or more requests.

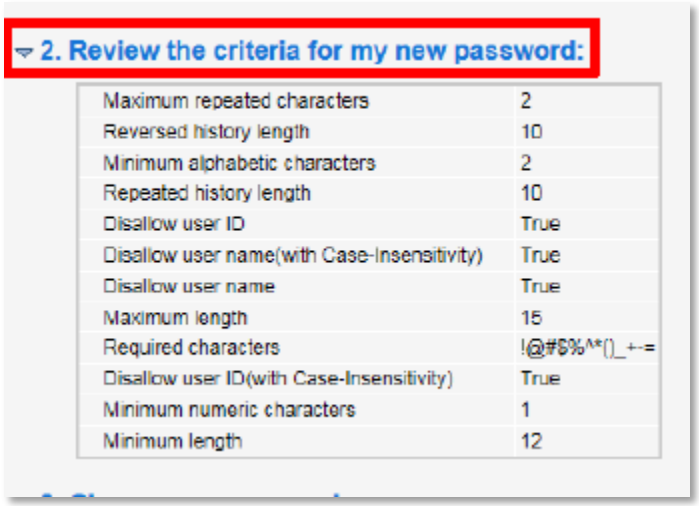
How to Create Your ISIM Single Sign On ("SSO") Password

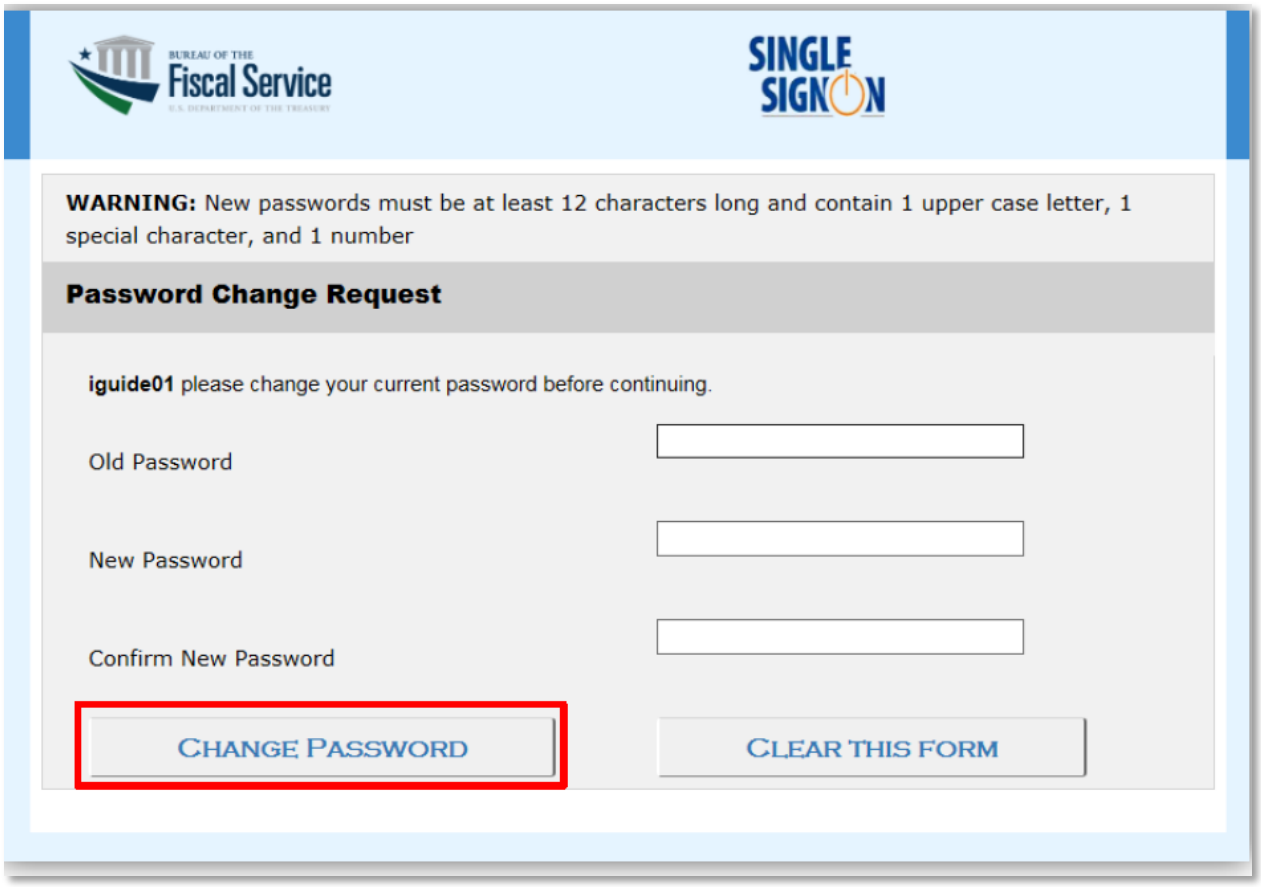
The following instructions will assist you in creating your ISIM SSO password.

1. By clicking the link on the second email, it will take you to the Single Sign On page where you will enter your User ID and temporary password received in the email and click **[Login]**.

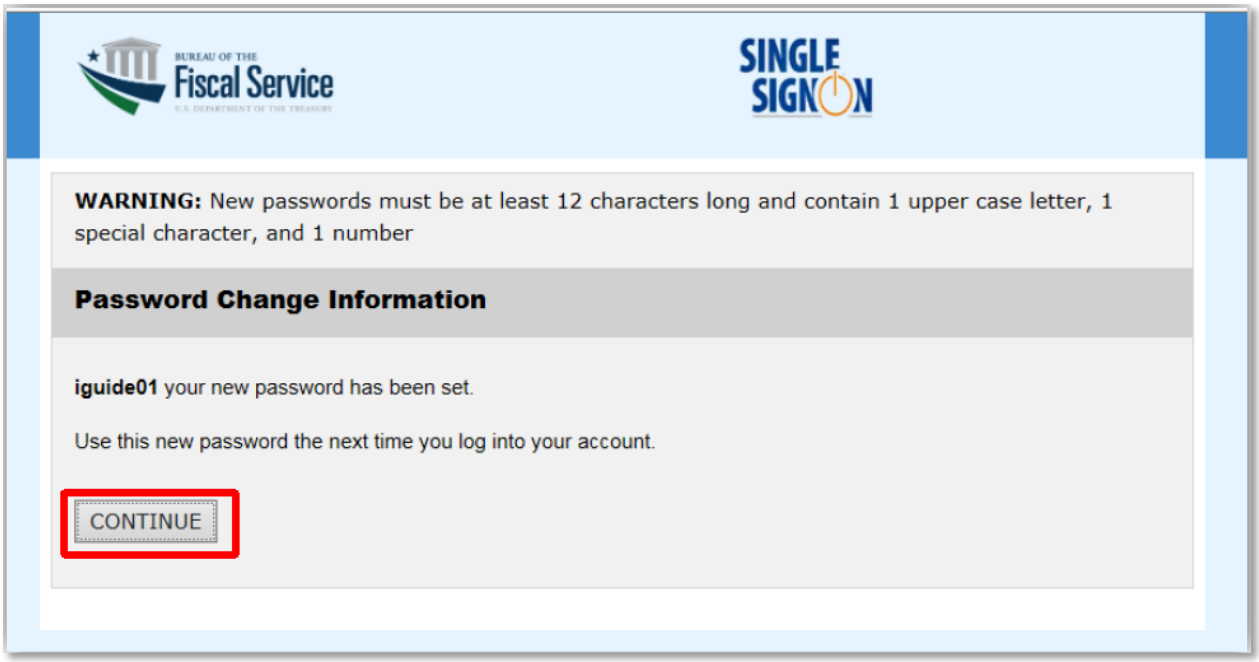


2. You will then be directed to change your password by entering the temporary password again and then your new password following the rules listed. After changing your password click **[Change Password]**.

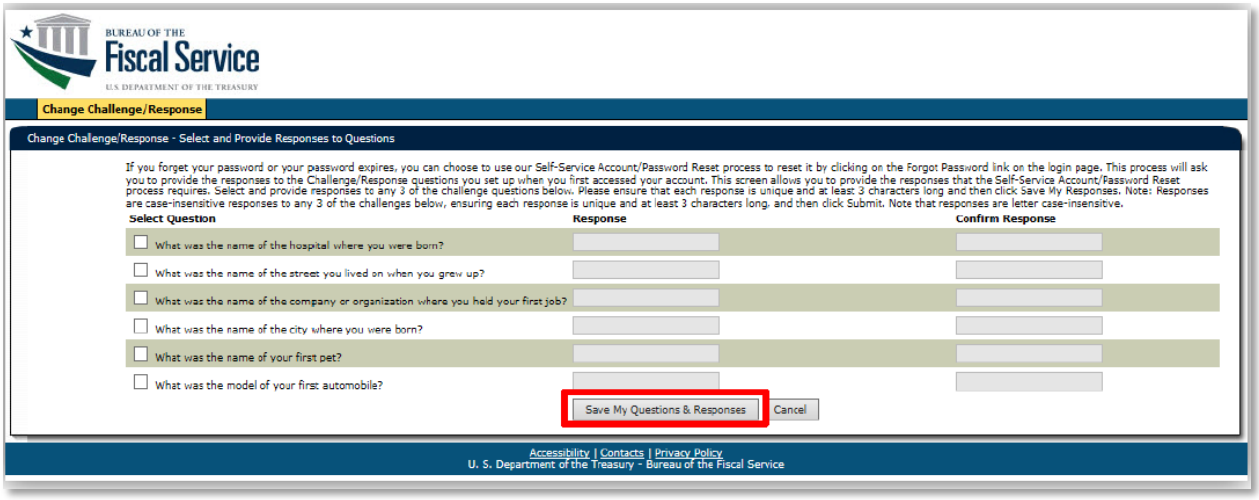




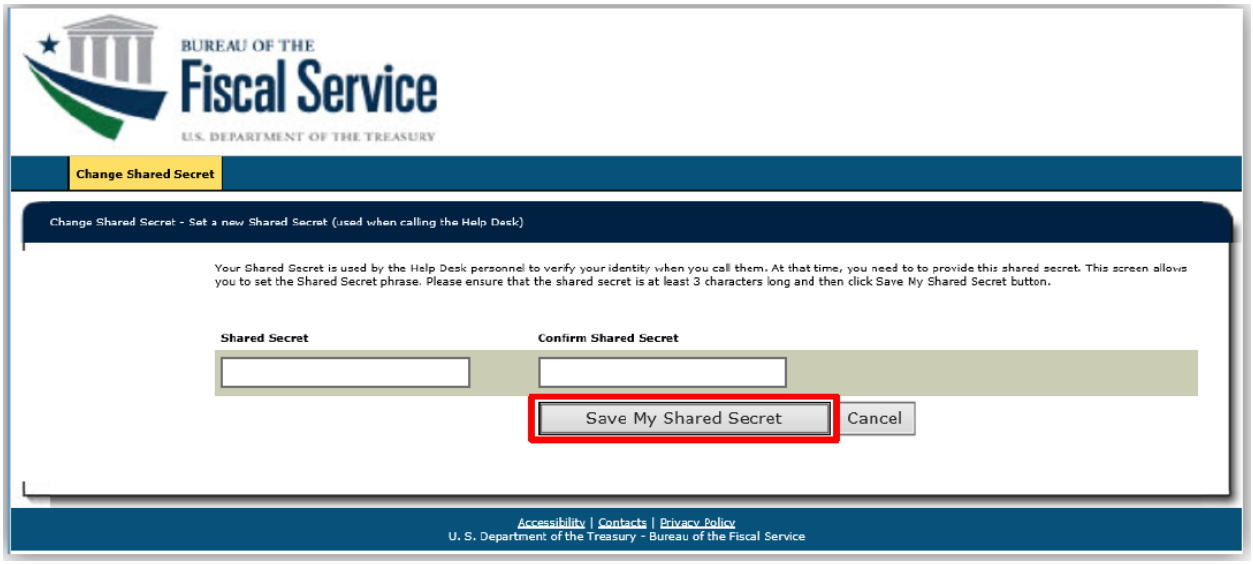
3. You will receive confirmation that this will be the password to use the next time you log in. Click **[Continue]** to complete the Challenge/Response steps.



4. Next you will need to complete the Challenge/Response information. The responses to these questions will help validate your identity for future password resets. Select the check box next to the three questions you want to answer and type your answer in the Response field as well as the Confirm Response field. After responding to three of the six questions, click **[Save My Questions & Responses]**.

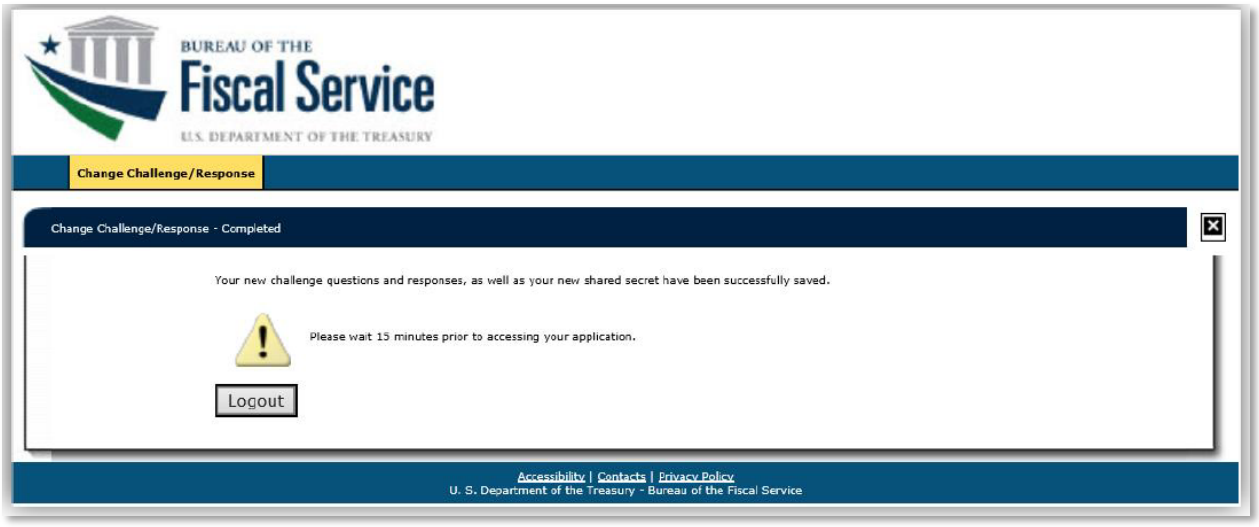


5. You will now need to enter your Shared Secret. The Shared Secret is used to assist the help desk validate your identity if you need your password reset but have forgotten your Challenge/Response information. Your Shared Secret is required to be at least 3 characters long and should be a word or phrase that is easy for you to remember. After populating and confirming your Shared Secret, click **[Save my Shared Secret]**.

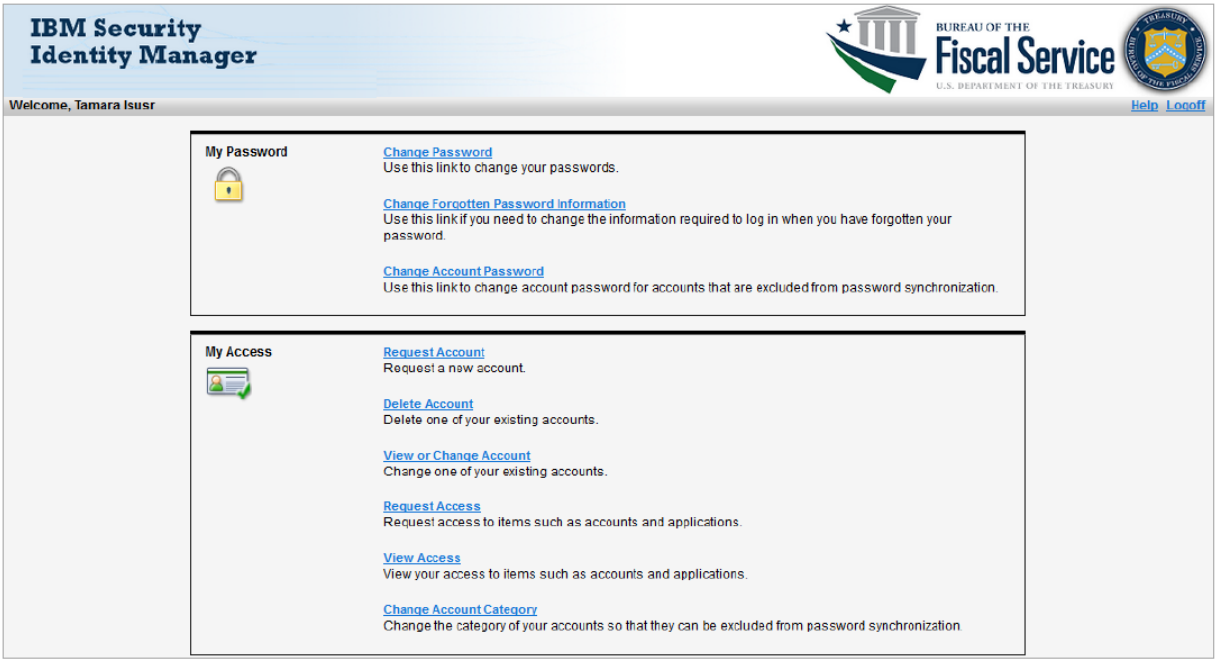


6. The system confirms that your Challenge/Response and Shared Secret have been saved. You will be required to wait 15 minutes before you are able to log into ISIM again or your application for the first time.

7. Click the **[Logout]**.



8. View of the ISIM Self-Service screen once the ISIM password has been successfully created.



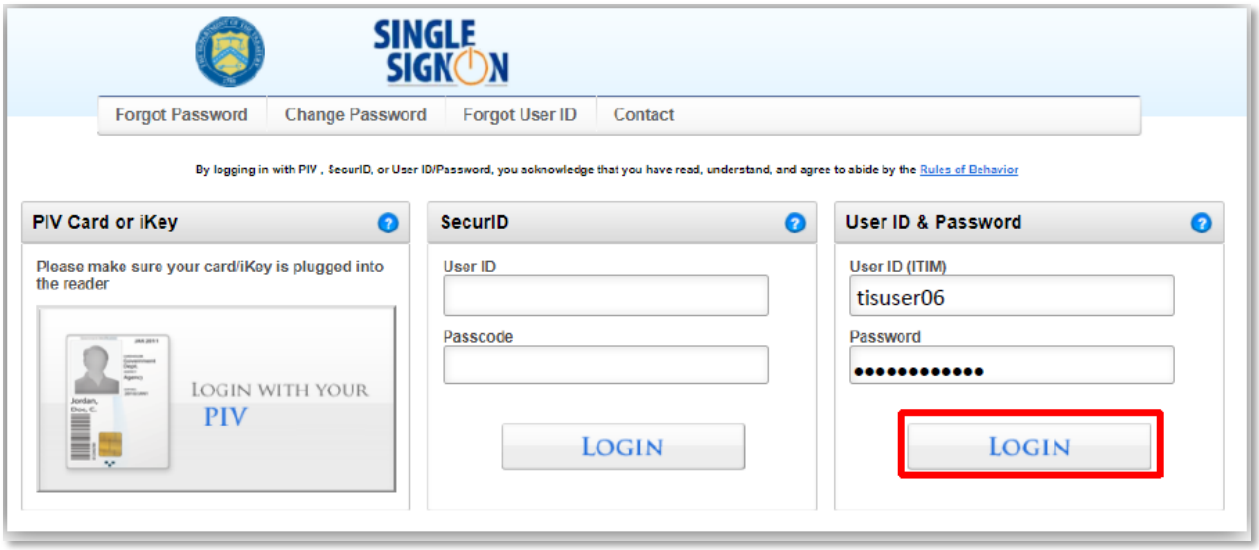
How to Reset Your ISIM Single Sign On ("SSO") Password

The following instructions will assist you in resetting your ISIM SSO password.

1. Access the ISIM Self-Service website.

   URL – https://isim.fiscal.treasury.gov/itim/self

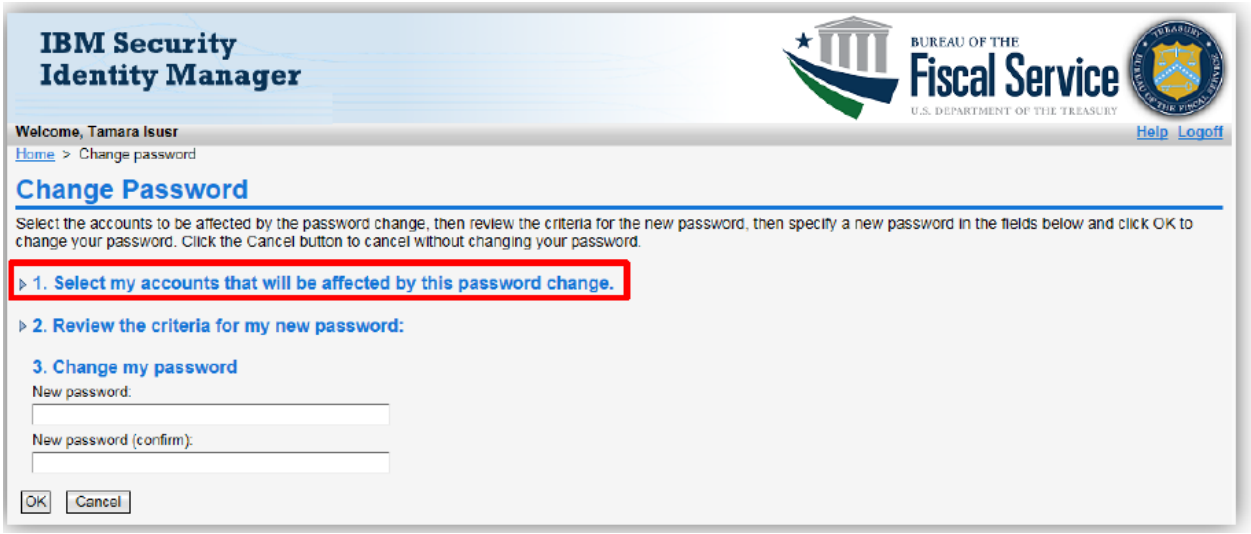
2. Enter your User ID and Password, and then click **[Log In]**.



3. The ISIM Self-Service website will display.

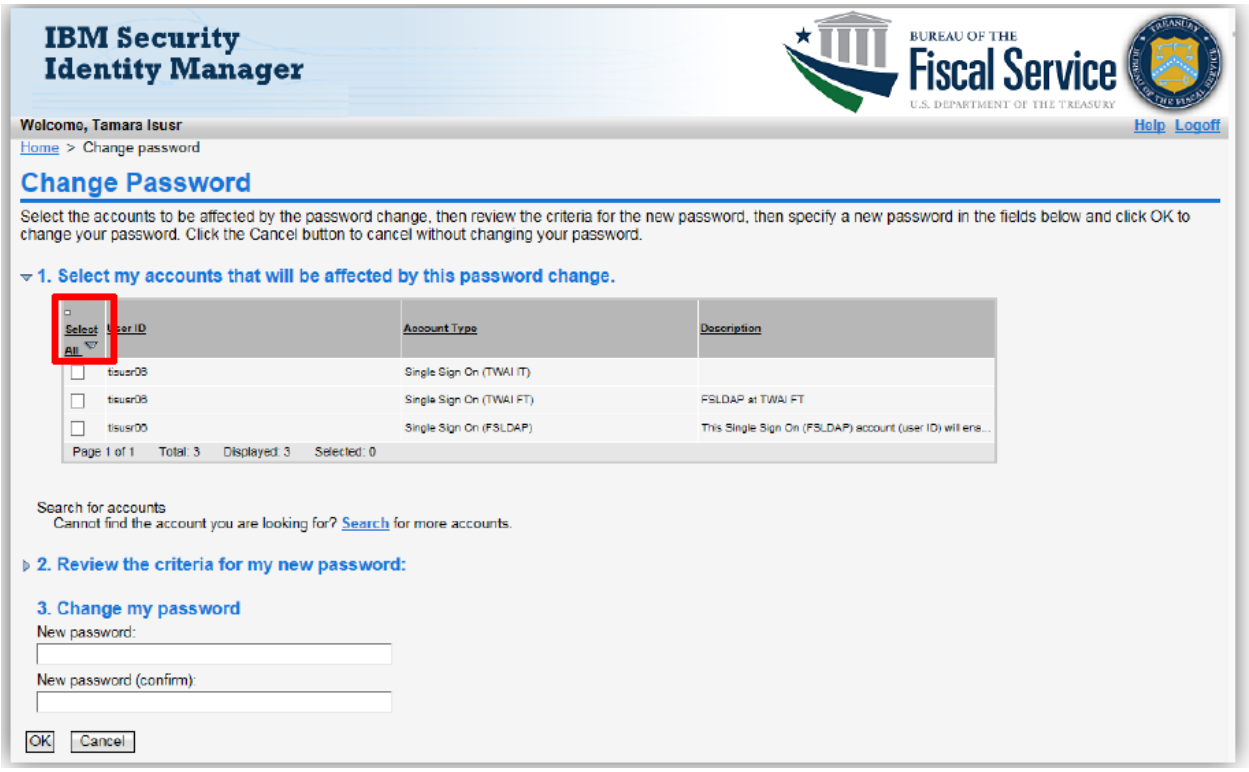
4. Click **[Change Password]**.

5. On the Change Password page, you will first need to select the accounts for which you would like to change the password. Click (1) **[Select my accounts that will be affected by this password change]**.



6. All the accounts associated with your profile will appear. You can change the password for all your accounts or just select accounts. To synchronize the password on all your accounts in ISIM, click the Select All check box. If you only want to change your password for particular accounts only select the check box to the left of the account type.

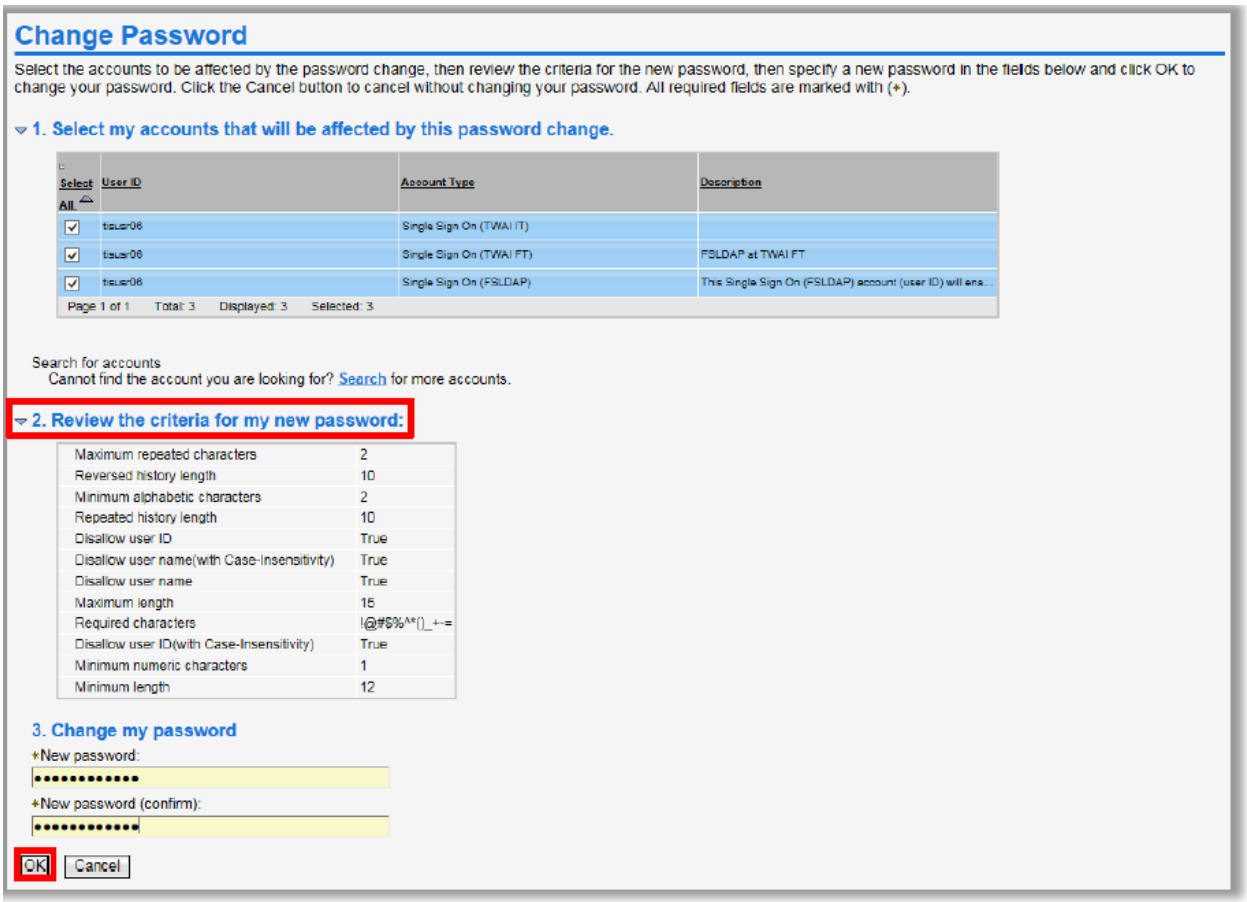
7. Check the box next to **[Single Sign On (FSLDAP)]** in the Account Type column.



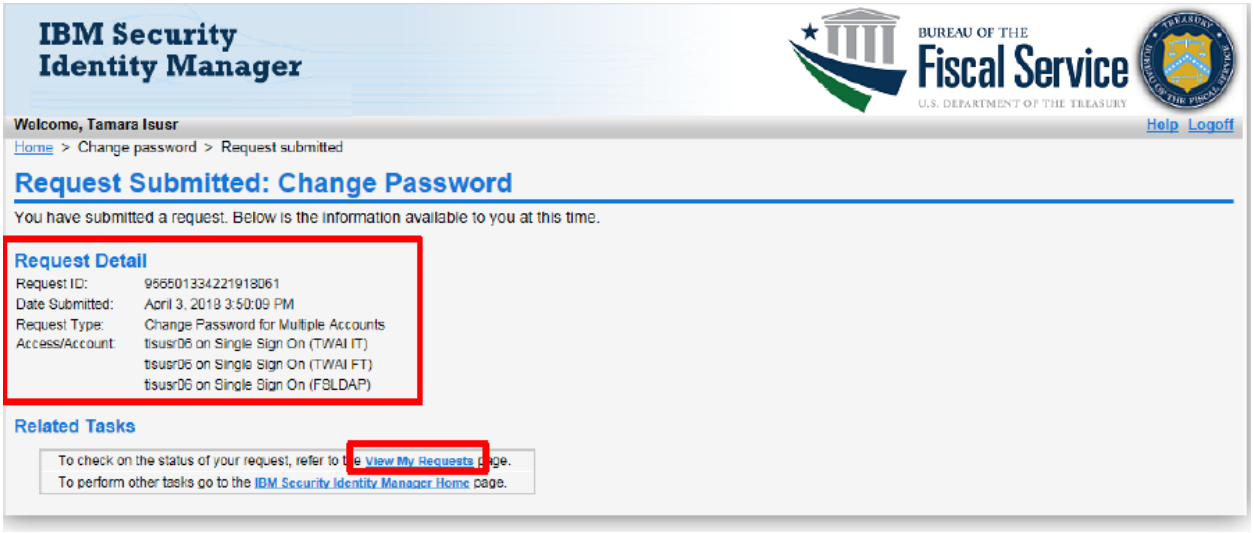
8. Click **[Review the criteria for my new password]** to display the criteria for creating your new password. You must now enter your new password using the criteria outlined and then confirm the password by re-entering it. Click **[OK]** to change your password. If you do not want to change your password, click **[Cancel]** and you will be directed back to the Self-Service home page.

   Note: If the Single Sign On account is not selected, the criteria for the password will not show when Option 2 is expanded.

9. Enter the new password in the New password field, confirm the password in the New password (confirm) field, and then click **[OK]**.

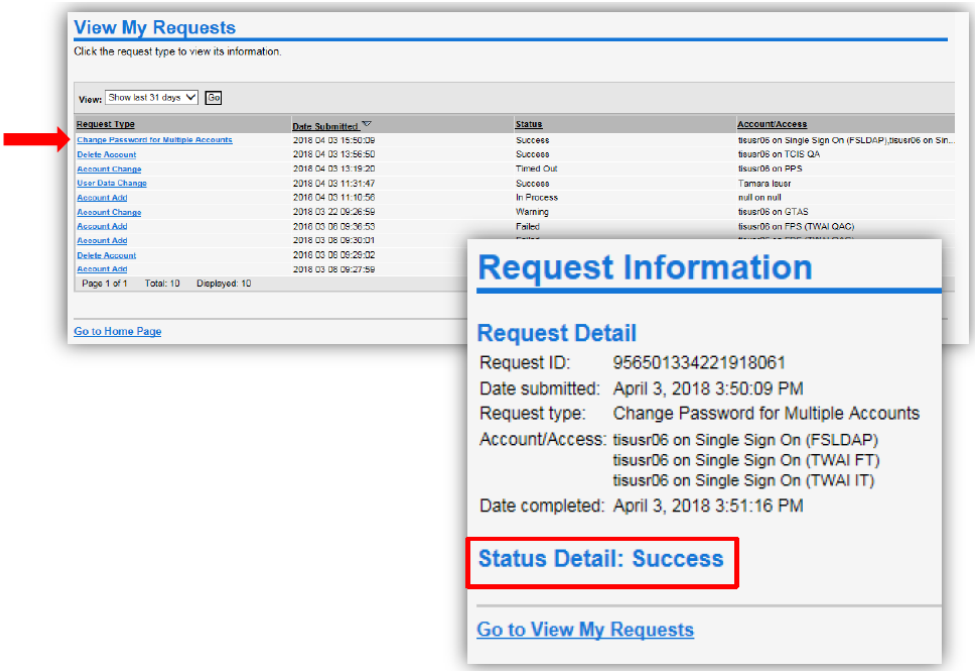


10. The Request Submitted page shows the request detail of the action you just performed. To check the status of your request, click **[View My Requests].**



11. To verify your password was changed successfully click on the appropriate link in the **Request Type** column.

    The Status Detail shows the password change was successful. If you receive a Status Detail showing a failed request, you need to contact the Fiscal Service Help Desk at (304) 480-7777 for assistance to change your password.



12. Log off and log back in to test your new password.

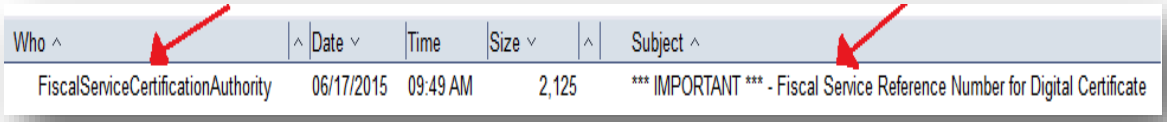
FiscalServiceCertificationAuthority Email

After your ISIM account has been provisioned, your PKI form will be sent to the U.S. Treasury for processing. After your PKI form has been processed, you will receive an email from FiscalServiceCertificationAuthority@fiscal.treasury.gov with your reference number. **Save this email**. Your reference will be needed during the setup of your PKI Token password.

Example of the FiscalServiceCertificationAuthority Email:

SUBJECT: *** IMPORTANT *** - Fiscal Service Reference Number for Digital Certificate

Below is a screen capture of how it should appear in your mail box:

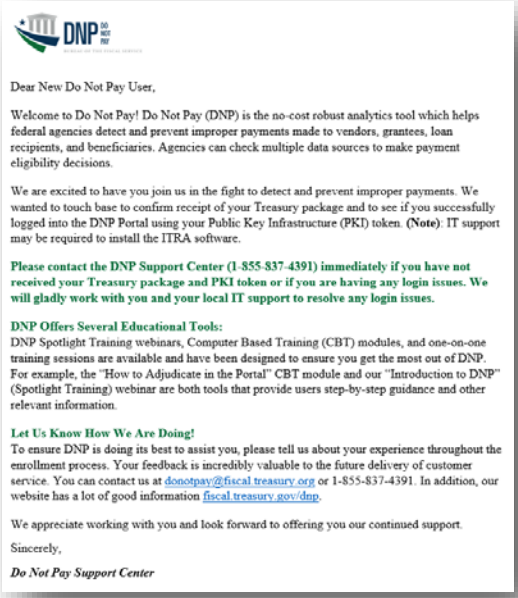


Who	Date	Time	Size	Subject
FiscalServiceCertificationAuthority	06/17/2015	09:49 AM	2,125	*** IMPORTANT *** - Fiscal Service Reference Number for Digital Certificate

Welcome to DNP Email

After the U.S. Treasury processes your PKI form, you will receive the Welcome to DNP Email from the DNP email box (DoNotPay@fiscal.treasury.org). This email contains potential tools to ensure that you get the most out of the DNP Program and the Portal, and contact information for the DNP Support Center, if you should encounter issues attempting to log into the Portal (855) 837-4391.

Example of the Welcome to DNP Email:



Dear New Do Not Pay User,

Welcome to Do Not Pay! Do Not Pay (DNP) is the no-cost robust analytics tool which helps federal agencies detect and prevent improper payments made to vendors, grantees, loan recipients, and beneficiaries. Agencies can check multiple data sources to make payment eligibility decisions.

We are excited to have you join us in the fight to detect and prevent improper payments. We wanted to touch base to confirm receipt of your Treasury package and to see if you successfully logged into the DNP Portal using your Public Key Infrastructure (PKI) token. **(Note)**: IT support may be required to install the ITRA software.

Please contact the DNP Support Center (1-855-837-4391) immediately if you have not received your Treasury package and PKI token or if you are having any login issues. We will gladly work with you and your local IT support to resolve any login issues.

DNP Offers Several Educational Tools:
DNP Spotlight Training webinars, Computer Based Training (CBT) modules, and one-on-one training sessions are available and have been designed to ensure you get the most out of DNP. For example, the "How to Adjudicate in the Portal" CBT module and our "Introduction to DNP" (Spotlight Training) webinar are both tools that provide users step-by-step guidance and other relevant information.

Let Us Know How We Are Doing!
To ensure DNP is doing its best to assist you, please tell us about your experience throughout the enrollment process. Your feedback is incredibly valuable to the future delivery of customer service. You can contact us at donotpay@fiscal.treasury.org or 1-855-837-4391. In addition, our website has a lot of good information fiscal.treasury.gov/dnp.

We appreciate working with you and look forward to offering you our continued support.

Sincerely,

Do Not Pay Support Center

IV. GAINING ACCESS TO THE PORTAL USING A PKI TOKEN

PKI Token:

- If you have been issued a new U.S. Treasury PKI Token, click *here* to move to the "Setting up your PKI Token" section in this Guide to set up your PKI Token before accessing the Portal.
- If you have an existing U.S. Treasury PKI Token, click *here* to move to the "Logging into the DNP Portal" section in this Guide to assist you in logging into the Portal.

Example of a PKI Token:

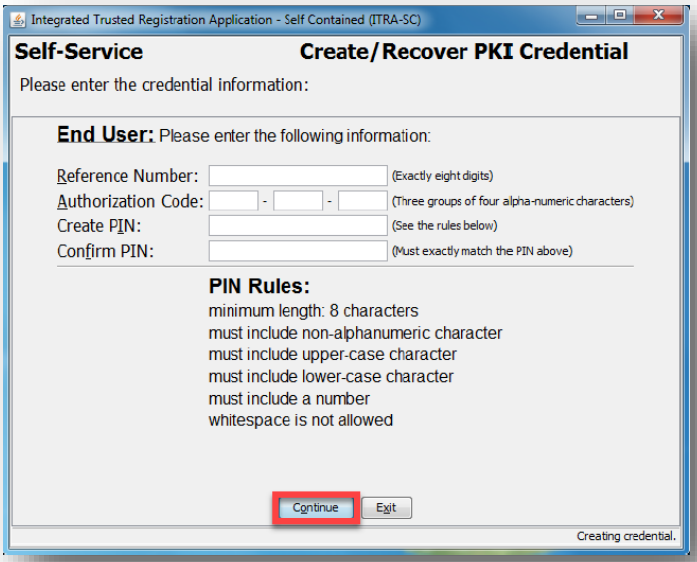
Setting Up Your PKI Token

If your Senior Agency Outreach Liaison requested a PKI Token on your behalf, you will receive a package from the U.S. Treasury via UPS Overnight. Your package will include: a welcome letter, a key ring, two software discs, your authorization code, and a PKI Token.

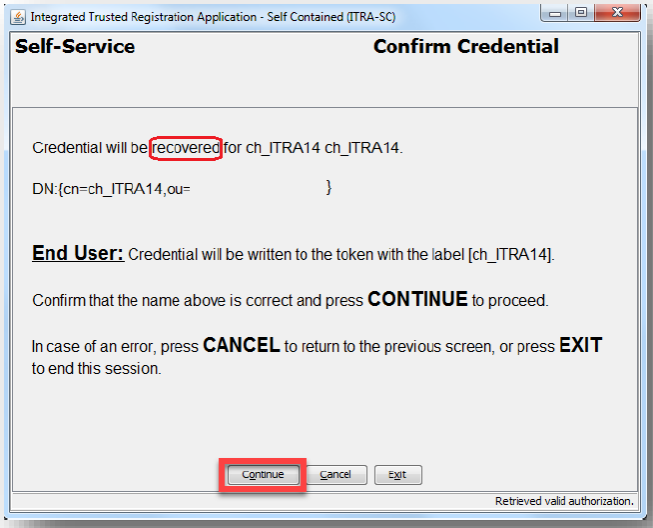
If you do not set up your PKI Token within 30 days of the initial authorization code and reference number issuance, the authorization code and reference number that were sent will expire. If they expire, you will need to contact the DNP Support Center at (855) 837-4391 to request a new authorization code and a reference number.

To set up your PKI Token for use in the Portal, follow the steps below:

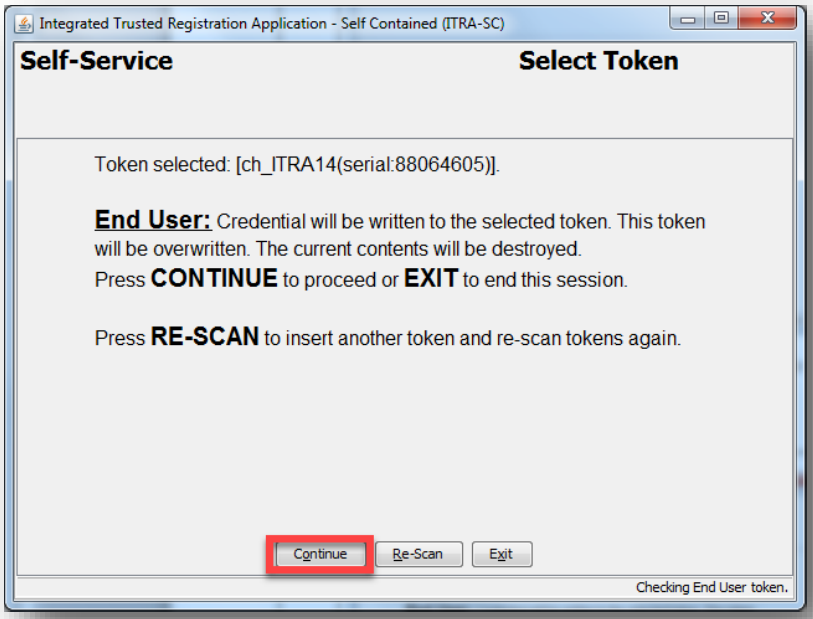
1. Read over the materials within your U.S. Treasury package.
2. Contact your local help desk or local IT support if you do not have administrative rights to install the ITRA-SC software, included in your U.S. Treasury package onto your computer.
3. Once the ITRA-SC software has been installed, click on the desktop icon that was created and titled "Launch ITRA Self-Contained".
4. Click on the second button "Self Service Create/Recovery"
5. Insert your PKI Token into an active USB port located on your workstation
6. Enter your reference number located in the email from FiscalServiceCertificationAuthority@fiscal.treasury.gov (refer to the Fiscal Service email on page 19 for further details) and the authorization code located on the folded sheet of paper included in your U.S. Treasury package sent to you via UPS. Create a PIN that you will use with your PKI Token to log into the Portal.



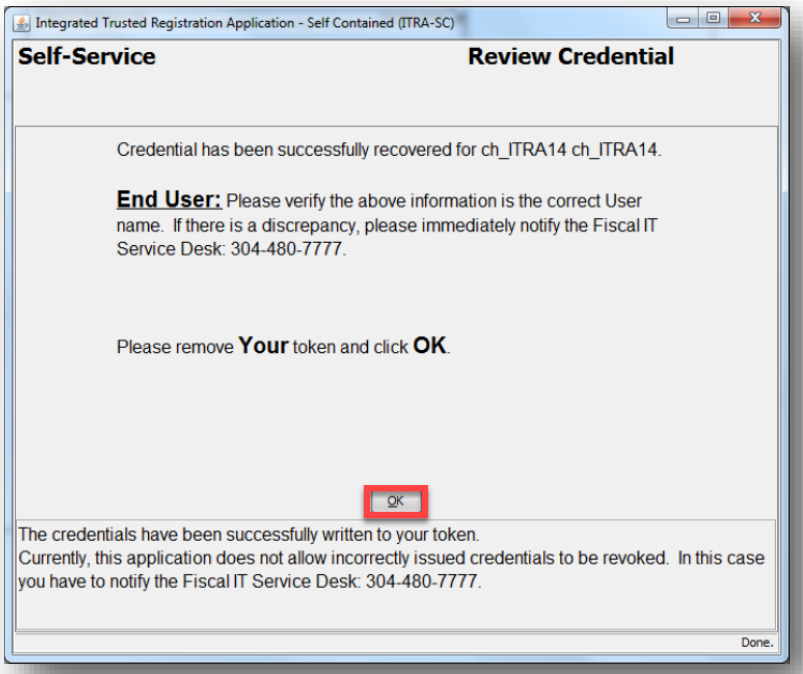
7. After you click **[Continue]**, your credential will be written to your PKI Token.



8. Read the information in the prompting window to confirm your name and User ID appear and if correct, click **[Continue]**. If incorrect, contact the DNP Support Center at (855) 837-4391 and they will contact U.S. Treasury PKI Support.
   Note: If you are a new user creating a PIN, the circled word would display as **created"** if you are recovering your PIN the circled word would display as **"recovered"**.



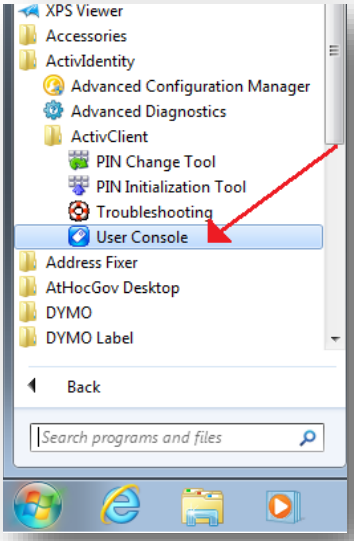
9. Please do not remove the PKI Token while the system writes your credential on it.
10. Once your credential has been written onto your PKI Token, click **[OK]**.
11. Now you can log into the Portal at https://fiscal.treasury.gov/DNP/ with your PKI Token inserted into your active USB port, with the PIN you created.



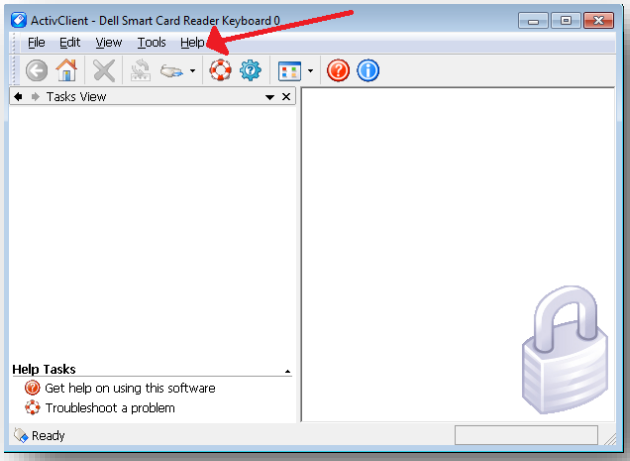
Checking ActivClient Version for DNP PKI Users

Note: For users using ActivClient version 6.2 or 7.0, this will require a registry edit. Contact the DNP Support Center at (855) 837-4391 for assistance. You will also need to contact your local IT Support for administrative rights.

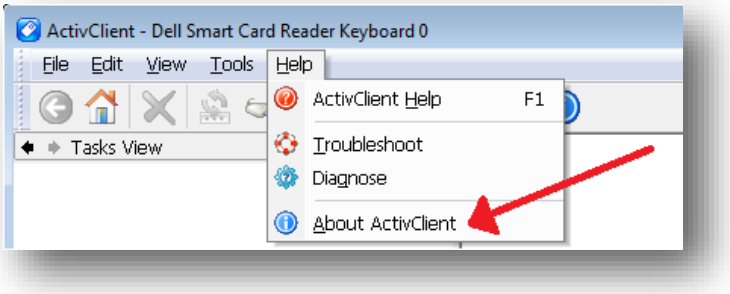
Select **Start – All Programs – ActivIdentity – ActivClient – User Console**.



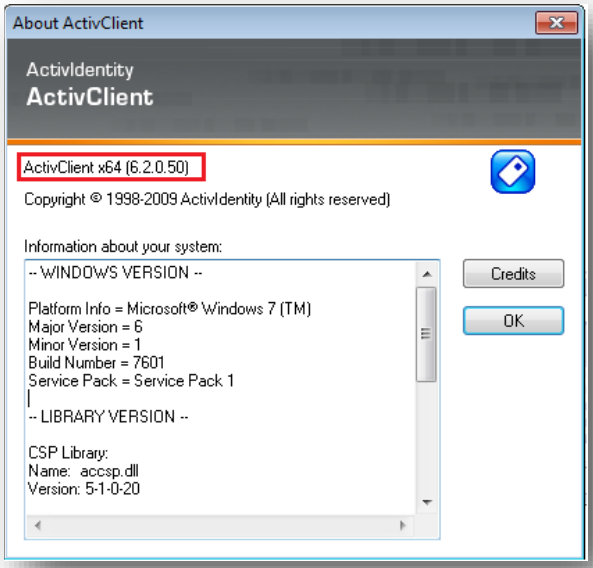
1. In the "User Console" and on the menu bar, select **Help**.



2. Next, to display ActivClient program information and version number, select **About ActivClient**.



Check to see if either ActivClient version 6.2 or 7.0 are installed, as appears in the area of the screen capture has in the area of the red box below:

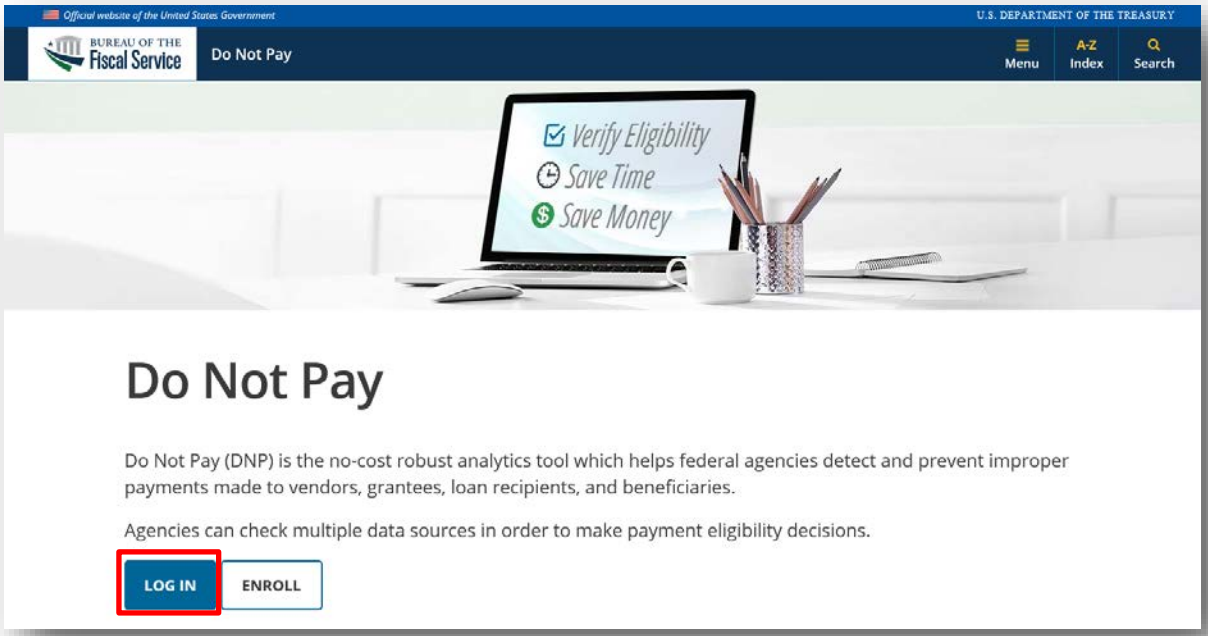


3. You may report that you have ActivClient and its version to the DNP Support Center at (855) 837-4391 for further assistance.

V. LOGGING INTO THE DNP PORTAL

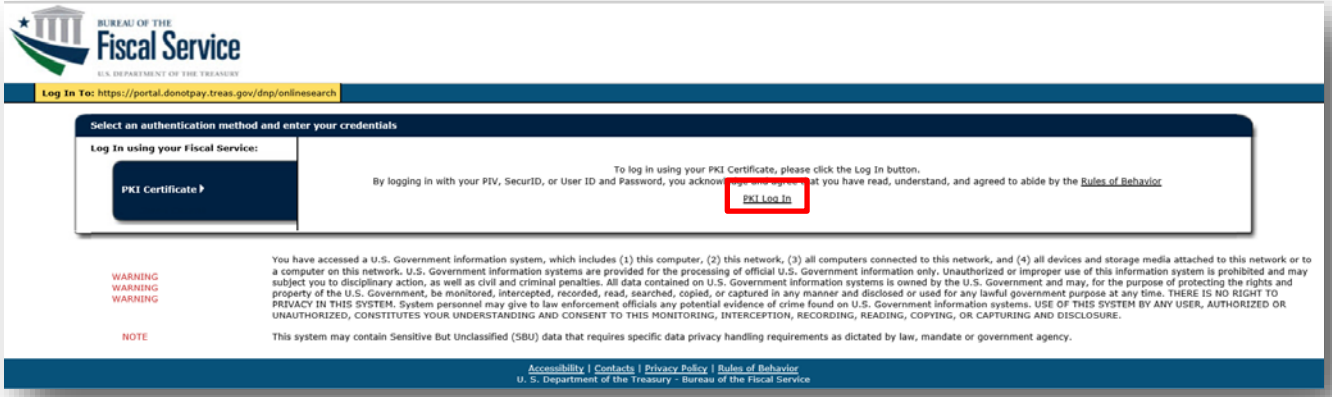
Open Your Internet Browser

1. Type https://fiscal.treasury.gov/DNP/ in the address bar and select **[Enter]**.
2. Insert your Treasury issued PKI Token.
3. Click **[Log In]**

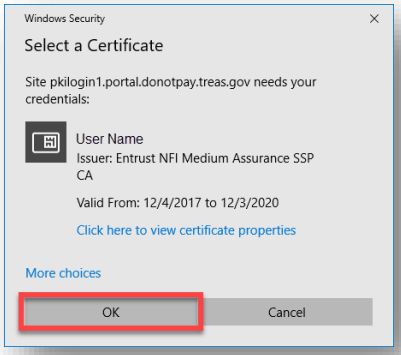


Fiscal Service Enterprise Single Sign On

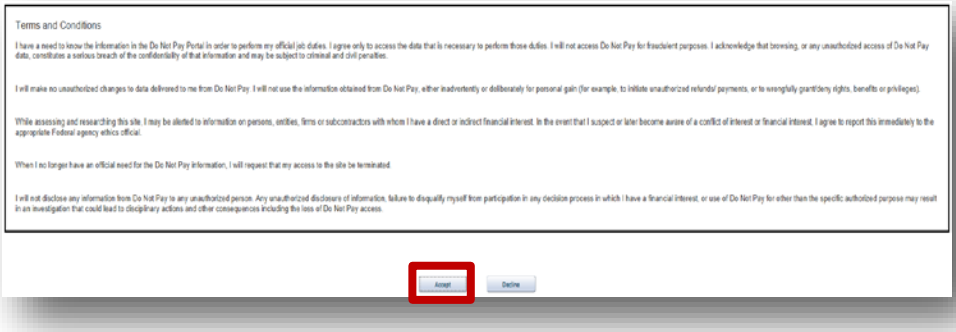
1) A new browser window will open.
   - Click **[PKI Log In]**.



2) Another browser window will open with your User ID populated.
   - Click **[OK]** and then enter your password associated with your PKI Token.



3) Another browser window will open with DNP's Terms and Conditions.
   - Please review the document and then click **[Accept]** to gain access to the application. This window will open each time you login.



DNP Portal: Homepage

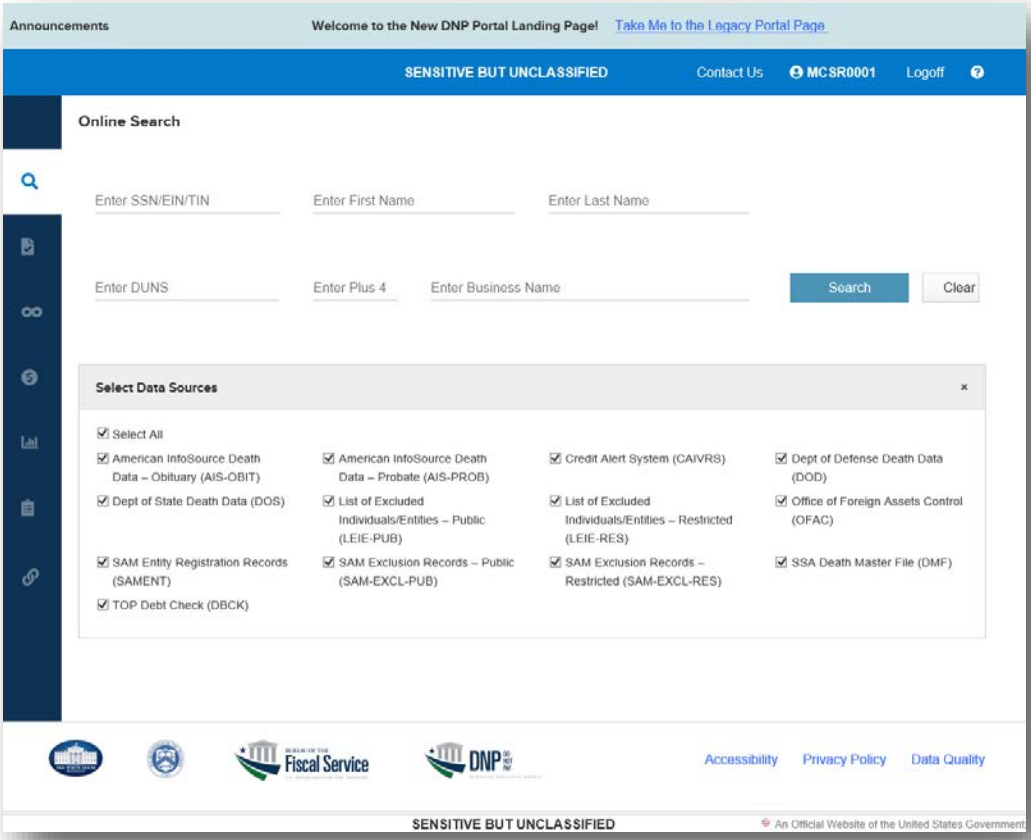
In order to retain your access to the Portal you must follow the ISIM Aging Rules:

- **Suspended:** All user accounts that have not logged into the Portal in the last 120 days will have an account status change to "suspended".
    - Suspended users must call the Treasury Support Center Help Desk at 1-855-837-4391 to have their account restored for access to the Portal.

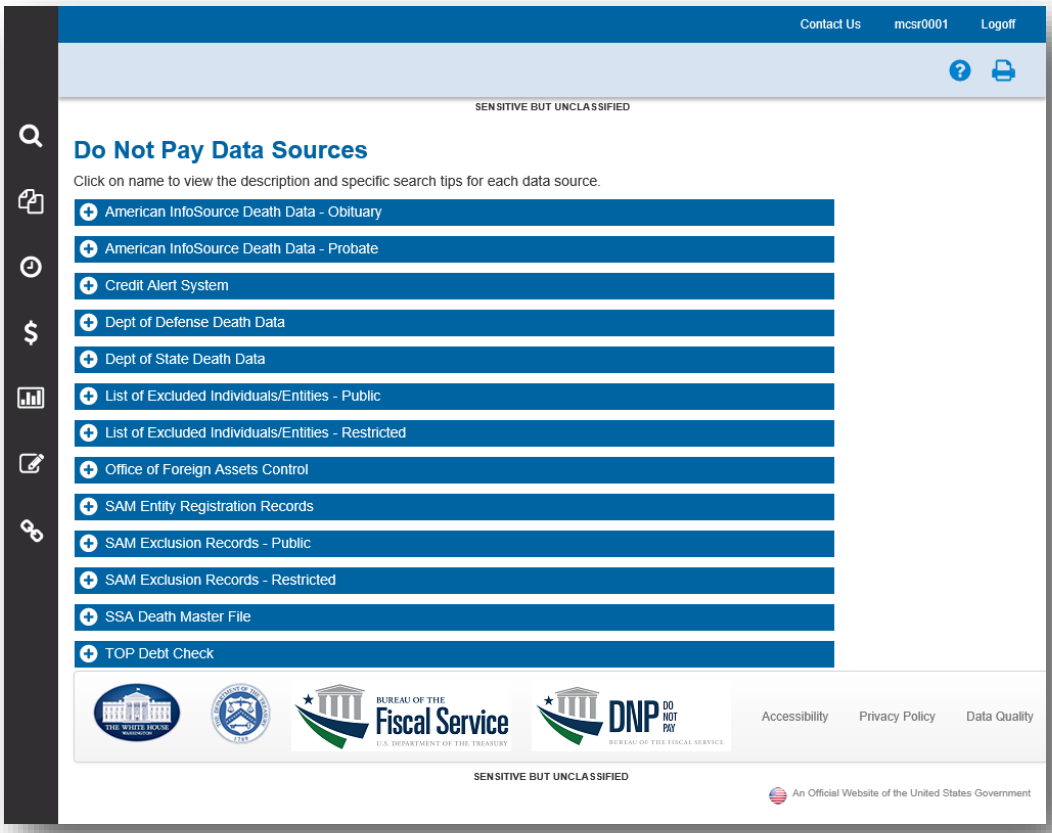
- **Deleted:** All user accounts that have not logged into the Portal in the last 13 months will be "deleted".
    - To regain access to the Portal, deleted users must complete the DNP enrollment process.

Note: If you no longer need access to the Portal, please contact your Authorizing Official, Primary Local Security Administrator, or your Local Security Administrator.

Redesigned Portal (Online Search is the only functionality that is currently available)



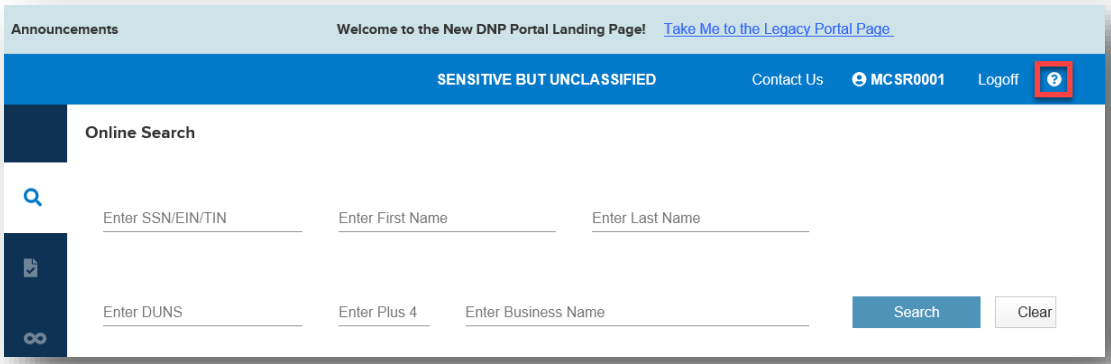
Legacy Portal (All other functionalities remain in the Legacy Portal until the redesign is completed by September 2020)

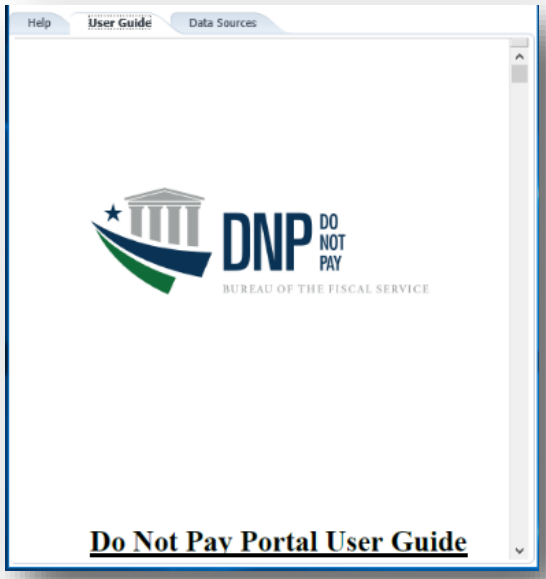


VI. USER GUIDE

For assistance navigating the Portal, you may refer to the User Guide within the Portal.

1. Log into the Portal
2. Click on the (upper right corner)
3. A new window will open. Click **[User Guide]**.





VII. TROUBLESHOOTING

Unable to Log into the Portal

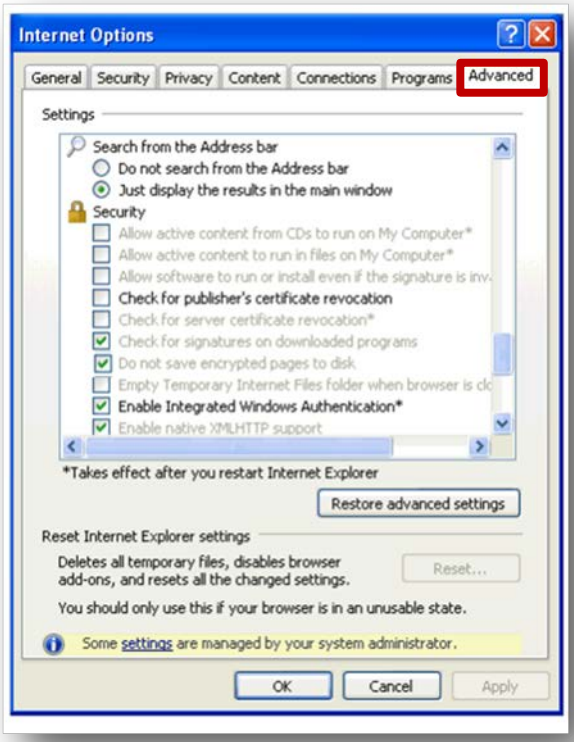
A. Verify the URL is correct. (https://fiscal.treasury.gov/DNP/)
B. Verify your version of Internet Explorer (Under Help > About Internet Explorer) – Internet Explorer (IE) 8, 9, and 11, Google Chrome, or Mozilla Firefox are supported.
C. Delete Temporary Internet Files (TIFs) and Cookies from Internet Explorer and restart Internet Explorer. (Tools > Internet Options > Browsing History – Delete > Delete Cookies, Delete Temporary Internet Files)
D. After re-opening Internet Explorer, please type https://fiscal.treasury.gov/DNP/ manually into your address bar.
E. If you are getting prompted for a PKI certificate, make sure you are choosing your user ID from the certificate box.
F. Verify you are inputting the password that you had set up for your PKI Token in the Password screen.

If you are still receiving an error, record the error message (a screenshot is best), and forward your name, ISIM User ID, phone number, email address, and a brief description of the problem in a secured email to the Do Not Pay email box or call the DNP Support Center at (855) 837-4391 for assistance.

Issues on Downloading Text or Excel File with Existing Browser

If the existing browser that is being used is preventing you from downloading a Text or Excel file, ensure that the browser settings under the Security section that reads "Do not save encrypted pages to disk" is checked. It depends on the browser version in use where this setting is located.

- Please see example below for Microsoft Internet Explorer (IE).
  - Specific for IE7, IE8, and IE9; it's under Tools-> Internet Options -> Advanced Tab -> Security



VIII. DO NOT PAY REQUIREMENTS

This section details the system and configuration requirements necessary to utilize the Portal.

Requirement Type	Details
System	• Web Browser: Internet Explorer 11 and Google Chrome **Note:** Please do not use the back button on your browser. DNP does not support the use of the browser back button. The navigation pane on the left side of the DNP Portal may be used to return to a previous screen. • Adobe Reader X and XI • Entrust Root Certificate: The Entrust (2048) Root Certificate must be installed in the "Trusted Root Certification Authorities" certificate store on the "local machine" (all user profiles) for the workstation. This certificate is normally installed by default with Internet Explorer. If it has been removed, you will need to have your agency reinstall the certificate. • Microsoft Excel versions 2003-2019 **Note:** Excel downloads from DNP are in the Excel 2003 format but can be opened in later versions of Excel. Downloads are subject to Excel 2003 limit of 65,000 rows, so files larger than that may be truncated. • Internet Options Security Settings • Active USB Port • Windows Resolution: 1280 x 1024 or higher
PKI Token	• Login requires PKI • Users must install the ITRA-SC software that will facilitate the use of their PKI credential **Note:** The ITRA software installation requires that you have administrative rights to install software on their computer. This may require the involvement of your local IT Support Services. The PKI installation software contains: o Token/Smart card middleware o JRE (Java runtime environment) version o JCE (Java cryptographic extensions) and certificate trust lists to be installed on agency workstation • Pentium II 500MHZ or Higher • 256 MB RAM • 100MB Free Hard Disk Space • 1 Free Active USB Port • 2X CD ROM Drive

Requirement Type	Details
Hardware	• If your agency currently has SafeNet installed to use and maintain a USB token, you will not need to install the software required to use your PKI Token. • The iKey specifications can be found on the following web site: https://safenet.gemalto.com/uploadedFiles/Products/Enterprise_Data_Protection/Multi-Factor_Authentication/Certificate-based_(PKI)_USB_Authenticators/SafeNet_product_brief_iKey4000.pdf The iKey 4000 USB token has the following characteristics: o The iKey 4000 is a FIPS 140-2 Level 3 rated cryptographic module. o The iKey 4000 is not recognized as a USB storage module. It does not appear as a drive in Windows explorer. This means that the iKey is not prevented from being used if an agency defines its Windows Group Policy to write-protect or disable USB ports.
Software	Software is provided on a CD labeled ITRA-SC. The ITRA-SC CD should be provided to all end users during the Fiscal Service PKI enrollment process and will install the components listed below. This setup will install and configure all needed components on the desktop to ensure successful operation of all Fiscal Service PKI applications. After successful installation of the ITRA-SC program, agency end users will have the ability to access the following: • ITRA – Credential creation and maintenance • Any Fiscal Service PKI-enabled application the agency user is authorized to use **Note:** The PKI Token acts as a secondary authentication device and is *incapable* of storing or acting as a storage media device for the DNP Portal user. Please contact your local IT support for any agency-specific requirements (firewall/network configurations, etc.).

IX. FREQUENTLY ASKED QUESTIONS (FAQs)

Q. Why is gaining access to the DNP Portal such a time intensive process?

A. The primary reason it takes time to gain access to the Portal is due to the security measures DNP takes to ensure that data sent and received in our system is secure. As we review your enrollment request, there are several time intensive steps that may delay the process, some of which include: observing The Privacy Act of 1974 with regard to an enrollment request, or reconciling your agency's specific technology practices against others in our system, a process that can sometimes lend itself to unpredictable interfacing problems. Ultimately, DNP makes every effort to ensure that privacy and security risks are mitigated, a process that takes time and may attribute to a lengthy enrollment process.

Q. What does it mean that I've been selected to be a user in the DNP Portal?

A. Your position plays a vital role in the payment cycle at your agency. As part of your agency's ongoing efforts to reduce improper payments, your agency is verifying their payments through the DNP Portal. Contact your Authorizing Official to obtain additional details. If you are unsure who you are Authorizing Official is at your agency, call DNP (855) 837-4391 and we can help point you to the correct person at your agency.

Q. What are Rules of Behavior and why are they needed?

A. Rules of Behavior (RoB) are required and provide good information security and raise security awareness. RoB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

Q. What should I do if I did not accept the Rules of Behavior within 10 days?

A. Access will be denied if acceptance is not received within 10 days. Send an email to donotpay@fiscal.treasury.org requesting further instructions to accept the Rules of Behavior.

Q. Why do I need a Treasury issued PKI Token?

A. Your PKI Token is used to verify and certify that you are allowed access to the DNP Portal. Your PKI Token is a secondary layer of authentication, to protect your information and your agency's data within the DNP Portal.

Q. My initial log on did not occur within 30 days of being granted access to DNP. What will happen to my access?

A. You have 24 hours to create an ISIM password; if not, the temporary password must be reset. To retain access to the DNP Portal, you must login in at least every 120 days or your access will be suspended. If you do not login to the DNP Portal in 13 months, your access to the DNP Portal will be deleted.

Q. How do I learn how to use the Portal?

A. Go to the DNP website at www.fiscal.treasury.gov/DNP/ to utilize resources. There, you can sign up specifically for Spotlight training. These webinars give instructions on various DNP Portal functions and services offered. As a user, you should receive an email invitation for the training at the beginning of each month. Also, your liaison is always available for one-on-one training to fit your specific needs.

Q. What if I have a question about my match results in the Portal?

A. Contact the DNP Support Center or send an email requesting contact at the DNP mailbox, donotpay@fiscal.treasury.gov. **Do not send Personally Identifiable Information (PII) or screen shots with PII via email.**

Q. What should I do with my PKI Token if I no longer require Portal access (e.g., retiring or leaving)?

A. Return your PKI token to:

Bureau of the Fiscal Service
257 Bosley Industrial Park Drive
Parkersburg Warehouse & OP Center Dock 1
Attn: ICAM
Mail Stop T2-A
Parkersburg WV 26101

X. GETTING HELP

There are several ways you can obtain help when using the DNP Portal.

You may contact your Senior Agency Outreach Liaison or the DNP Support Center:
☎ (855) 837-4391
✉ donotpay@fiscal.treasury.gov.