



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

3.42.8

AUGUST 28, 2025

## EFFECTIVE DATE

(10-01-2025)

## PURPOSE

- (1) This transmits revised IRM 3.42.8, E-Services Procedures for Electronic Products and Services Support (EPSS).

## MATERIAL CHANGES

- (1) IRM 3.42.8.1.1, Background - Updated to include Taxpayer Identification Number (TIN) Matching.
- (2) IRM 3.42.8.1.3, Roles and Responsibilities - Updated IRM reference to Servicewide Policy Statements.
- (3) IRM 3.42.8.1.7, Related Resources - Removed Publication 2108-A, added Publication 2108.
- (4) IRM 3.42.8.3.1, Authorizes Users - Added Form 941 (sp) and Form 943 (sp).
- (5) IRM 3.42.8.3.1.2, Compromised Secure Access Digital Identity (SADI) Account - IPU 24U1036 issued 10-11-2024 - In (2) revised reset password information.
- (6) IRM 3.42.8.4.1, Restricting an Account - IPU 25U0223 issued 02-14-2025 - In (4) Revised to update instructions.
- (7) IRM 3.42.8.5, Business Tax Accounts - IPU 24U1036 issued 10-11-2024 - Added new Business Tax Account (BTA) information section.
- (8) IRM 3.42.8.5.1, Authenticated CP311/CP311A Inquiries - IPU 25U0337 issued 03-11-2025 - Updated to include EIN Information.
- (9) IRM 3.42.8.5.2, Other CP311/CP311A Restriction Inquiries - IPU 25U0337 issued 03-11-2025 - Updated to include EIN Information.
- (10) IRM 3.42.8.5.3, Unrestricting (Enabling) an Account - IPU 24U1036 issued 10-11-2024 - Revised escalation description.
- (11) IRM 3.42.8.5.3, Unrestricting (Enabling) an Account - Updated IRM reference.
- (12) IRM 3.42.8.7, Taxpayer Identification Number (TIN) Matching - Revised Publication 2108A to Publication 2108 Federal Agency TIN Matching program.
- (13) IRM 3.42.8.8.1, Access to Client Information- Added Form 2848.
- (14) IRM 3.42.8.8.2, Rejected TDS - Added column I under AUTHS.
- (15) Exhibit 3.42.8-1, Acronyms - Revised to remove irrelevant entries and add POA and TIA.
- (16) Editorial changes made throughout the IRM section including:
  - Incorporation of Plain Language Standards
  - Corrections to typographical errors
  - Updated terminology

## **EFFECT ON OTHER DOCUMENTS**

IRM 3.42.8 dated 08/21/2024 is superseded. This IRM incorporates the following IRM Procedural Updates: 24U1036 issued 10/11/2024, 25U0223 issued 02/14/2025 and 25U0337 issued 03/11/2025.

## **AUDIENCE**

EPSS e-help desk assistors, Technical Services Operation (TSO) employees, and managers, analysts, business owners, and others who provide support to users of IRS electronic products and services.

Jason Romero-Stephens  
Director, Electronic Products and Services Support  
Taxpayer Services Division

3.42.8

E-Services Procedures for Electronic Products and Services Support (EPSS)

## Table of Contents

3.42.8.1 Program Scope and Objectives

3.42.8.1.1 Background

3.42.8.1.2 Authority

3.42.8.1.3 Roles and Responsibilities

3.42.8.1.4 Program Management and Review

3.42.8.1.5 Program Controls

3.42.8.1.6 Terms and Acronyms

3.42.8.1.7 Related Resources

3.42.8.2 Taxpayer Advocate Service

3.42.8.3 Disclosure

3.42.8.3.1 Authorized Users

3.42.8.3.1.1 Caller Authentication

3.42.8.3.1.2 Compromised Secure Access Digital Identity (SADI) Account

3.42.8.4 Secure Access Digital Identity (SADI)

3.42.8.4.1 Restricting an Account

3.42.8.4.2 Un-Restricting (Enabling) an Account

3.42.8.5 Business Tax Account (BTA)

3.42.8.5.1 Authenticated CP311 Restriction Inquiries

3.42.8.5.2 Other CP311/CP311A Restriction Inquiries

3.42.8.5.3 Unrestricting (Enabling) an Account

3.42.8.6 E-Services

3.42.8.6.1 Accessing E-Services

3.42.8.6.1.1 Employee User Portal (EUP)

3.42.8.6.1.2 Integrated Enterprise Portal (IEP)

3.42.8.6.1.3 Clear Cache

3.42.8.6.2 Short ID

3.42.8.7 Taxpayer Identification Number (TIN) Matching

3.42.8.7.1 TIN Matching Access Inquiries

3.42.8.7.2 Delete/Revoke/Restore a TIN Matching Application

3.42.8.7.3 Replace a Principal

3.42.8.7.4 Bulk TIN - Valid Response

3.42.8.7.5 Bulk TIN - No Response

3.42.8.7.6 TIN Matching Suspended and/or Locked Out

3.42.8.7.7 TIN Matching Error Messages

3.42.8.8 Transcript Delivery System (TDS)

- 
- 3.42.8.8.1 Access to Client Information
    - 3.42.8.8.1.1 Centralized Authorization File (CAF)
  - 3.42.8.8.2 Rejected TDS
  - 3.42.8.8.3 Married Taxpayers
  - 3.42.8.8.4 IRS Employees
  - 3.42.8.8.5 State Users
  - 3.42.8.8.6 Common TDS Problems
    - 3.42.8.8.6.1 Bulk Request Upload Error Message
    - 3.42.8.8.6.2 Unable to Receive Business Master File (BMF) Return Transcripts
    - 3.42.8.8.6.3 TDS Letters Cut Off or Cannot Print
  - 3.42.8.8.7 Income Verification Express Service (IVES) Users
  - 3.42.8.9 Miscellaneous E-Services
    - 3.42.8.9.1 PIN Rules/Inquiries
    - 3.42.8.9.2 Secure Mailbox
    - 3.42.8.9.3 Missing Links

Exhibits

- 3.42.8-1 Acronyms

3.42.8.1  
(09-20-2021)  
**Program Scope and Objectives**

- (1) **Purpose:** This **IRM** section provides instructions for Electronic Products and Services Support (EPSS) phone assistants working in Andover MA, Atlanta GA, Austin TX, Cincinnati OH, Martinsburg WV and Ogden UT who respond to external customers needing assistance or information when using e-Services web-based products.
- (2) **Audience:** EPSS tax examining technicians and information technology specialists who respond to secure access and e-Services inquiries.
- (3) **Policy Owner:** Director, EPSS
- (4) **Program Owner:** EPSS, Operations Support, Program Management
- (5) **Primary Stakeholders:** All IRS users of electronic products and services.
- (6) **Program Goals:** To support customer-valued e-solutions for Servicewide electronic products and services.

3.42.8.1.1  
(10-01-2025)  
**Background**

- (1) In 2007, Electronic Products and Services Support (EPSS) was created. One of the primary programs in EPSS is e-Services, which is a suite of web-based products that provides customers with electronic options for interacting with the IRS. Customers include tax professionals, financial institutions, state agencies, IRS employees, and other qualified business partners.
- (2) EPSS provides electronic products and services support to individuals, businesses and e-file providers.
- (3) EPSS support includes:
  - Electronic Filing (e-file)
  - Electronic Federal Tax Payment System (EFTPS)
  - Electronic Services (E-Services)
  - Filing Information Returns Electronically (FIRE) System
  - Foreign Account Taxpayer Compliance Act (FATCA) online registration and International Compliance Management Module (ICMM) Error Notifications
  - Affordable Care Act (ACA) Information Returns
  - Transcript Delivery Service (TDS)
  - Taxpayer Identification Number (TIN) Matching

3.42.8.1.2  
(10-01-2023)  
**Authority**

- (1) EPSS is guided by the following legal and regulatory authorities:
  - IRC Section 7803(a)(3), Taxpayer Bill of Rights
  - IRC Section 6103, Confidentiality and Disclosure of Returns and Return Information
  - Treasury regulation section 301.6011-2(c)(1)
  - Protecting Americans from Tax Hikes (PATH) Act
  - Restructuring and Reform Act of 1998 (RRA 98)
  - Taxpayer First Act Section 2301

3.42.8.1.3  
(10-01-2025)

**Roles and  
Responsibilities**

- (1) The Taxpayer Bill of Rights (TBOR) lists rights that already existed in the tax code, putting them in simple language and grouping them into 10 fundamental rights. Employees are responsible for being familiar with and acting in accord with taxpayer rights. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For additional information about the TBOR, see *Taxpayer Bill of Rights*.
- (2) The Director of Electronic Products and Services Support (EPSS) is responsible for the development and delivery of policy and guidance that impacts assistors.
- (3) The e-help Operations Chief offers technical assistance to the users of IRS electronic products and services: such as Electronic Return Originators (EROs), Software Developers, Transmitters, etc.
- (4) The TSO Chief serves as a focal point for electronic processing of Form 1099 series, Form 1098, Form 5498, Form 1042-S, and all other information returns.
- (5) The Operations Support (OS) Chief offers program management oversight to ensure the effectiveness of all programs under the jurisdiction of the EPSS Director.
- (6) All employees complete duties following IRM 1.2.1.2.36, Policy Statement 1-236, Fairness and Integrity in Enforcement Selection.

3.42.8.1.4  
(09-09-2021)

**Program Management  
and Review**

- (1) EPSS oversees and maintains programs by performing reviews and certification as described below:
  - Continual E-help Support System (EHSS) Knowledge Article Certification
  - EPSS Program Letter - documents expectations for telephone and paper inventory programs including quality review guidelines, goals and employee certification
  - Quality Measures - goals based on five quality attributes: Customer Accuracy, Procedural, Regulatory, Professionalism, and Timeliness. Quality review goals include frequency, method of sampling and performance targets. Reviews performed with the use of Contact Recording (CR) and Embedded Quality Review System (CQRS)

3.42.8.1.5  
(09-09-2021)

**Program Controls**

- (1) CR and CQRS reviews of completed calls ensure compliance with IRM guidelines.
- (2) Senior managers and program and policy analysts perform annual program reviews on a rotating basis to ensure adherence to policies and procedures.

3.42.8.1.6  
(09-09-2021)

**Terms and Acronyms**

- (1) For a list of acronyms used in EPSS, see Exhibit 3.42.8-1.

- (2) The table below lists only the approved IRS business partners that are eligible to participate in e-Services:

Customer	E-Services Product
Tax professionals who request transcripts through Secure Object Repository (SOR) as an e-Services Product.	Online e-file application
Electronic Return Originators (ERO) who have e-filed 5 or more accepted returns	Transcript Delivery System (TDS)
Low Income Tax Clinics	TDS
Circular 230 Practitioners who qualify as Attorneys, CPAs or EAs	TDS
Reporting Agents	TDS
State Taxing Authorities	TDS
Payers of income subject to back-up withholding	TIN Matching Application, Interactive TIN Matching, Bulk TIN Matching

**Figure 3.42.8-1 IRS Business Partners who Participate in e-Services**

For more information, visit the *E-Services* page on [irs.gov](https://irs.gov).

## 3.42.8.1.7 (10-01-2025) Related Resources

- (1) Resources available to help assistors in the performance of their duties include: Training, publications, Internal Revenue Manuals, EPSS communications and EPSS SERP Portal. Assistors must report their time under the right Organization, Function, and Program (OFF) codes for tracking purposes. See Exhibit 3.42.7-1, Organization, Function and Program (OFF) Codes (Phones and email), and Exhibit 3.42.7-2, e-help Organization, Function and Program (OFF) Codes (Paper), for programs to use when working telephones, email, and paper.
- (2) Use the publications, IRMs, and websites below to resolve issues related to this IRM section:
- Publication 1281, Backup Withholding on Missing and Incorrect Name/ TIN(s)
  - Publication 2108, Federal Agency TIN Matching Program
  - Publication 3112, IRS e-file Application and Participation
  - Rev. Proc. 2007-40, Requirements of Participants in the IRS e-file Program
  - Rev. Proc. 2003-9, E-Services Online TIN Matching Program
  - Rev. Proc. 97-22, Guidance on Electronic Records
  - IRM 3.42.7, EPSS Help Desk Support
  - IRM 3.42.10, Authorized IRS e-file Providers

- The Servicewide Electronic Research Portal (SERP) is designed to give all IRS employees intranet access to IRMs and other reference materials, and to retrieve frequently-referenced documents required to perform their jobs. Use the IRMs posted on SERP for the most up-to-date procedures.

### 3.42.8.2 (10-01-2024)

#### **Taxpayer Advocate Service**

- (1) The Taxpayer Advocate Service (TAS) is an independent organization within the Internal Revenue Service (IRS), led by the National Taxpayer Advocate, that helps taxpayers and protects taxpayer rights. TAS offers free help to taxpayers when a tax problem is causing a financial difficulty, when they've tried and been unable to resolve their issue with the IRS, or when they believe an IRS system, process, or procedure just isn't working as it should. TAS strives to ensure that every taxpayer is treated fairly and knows and understands their rights under the Taxpayer Bill of Rights. TAS has at least one taxpayer advocate office located in every state, the District of Columbia, and Puerto Rico.
- (2) In general, the e-help Desk does not answer account-specific questions (e.g., calls received regarding individual tax accounts). If the e-help Desk assistor cannot resolve an inquiry, referring the issue to TAS may be appropriate. Refer taxpayers to TAS (see IRM Part 13, Taxpayer Advocate Service) when the contact meets TAS criteria (see IRM 13.1.7, Taxpayer Advocate Service (TAS) Case Criteria) and you cannot resolve the taxpayers issue the same day. The definition of "same day" is within 24 hours. "Same day" cases include cases you can completely resolve in 24 hours, as well as cases in which you have taken steps within 24 hours to begin resolving the taxpayer's issue. Do not refer these cases to TAS unless they meet TAS criteria and the taxpayer asks to be transferred to TAS. Refer to IRM 13.1.7.5, Same Day Resolution by Operations. When referring cases to TAS, use Form 911, Request for Taxpayer Advocate Service Assistance (And Application for Taxpayer Assistance Order), and forward to TAS in accordance with your local procedures.
- (3) There is a Service Level Agreement (SLA) between TAS and the Taxpayer Services (TS) Division, as well as SLAs between TAS and the other Operating Divisions. These agreements outline the procedures and responsibilities for the processing of TAS casework when either the statutory or Delegated authority to complete the case transactions rests outside of TAS. The TS SLA is available at *TAS Site Pages SLA*.
- (4) TAS emphasizes the polite and respectful treatment of taxpayers and practitioners by IRS employees. See IRM 3.42.7.14.2, Telephone Etiquette, for e-help Desk policies.
- (5) Congressional inquiries are referred to TAS.

### 3.42.8.3 (10-01-2024)

#### **Disclosure**

- (1) The Office of Disclosure administers the provisions of IRC 6103, "Confidentiality and disclosure of returns and return information." All IRS employees are responsible for ensuring taxpayer confidentiality is protected, and tax records are properly safeguarded and disclosed only as provided by law.
- (2) E-help Desk assistants must prevent unauthorized disclosure of prohibited information when providing support to e-Services users. Before providing information, confirm the identity of the person you're speaking to on the telephone. Verify that the caller is authorized to receive the information. Disclose only what is necessary when giving information to third parties.



- (3) See IRM 3.42.7.3.1, Office of Disclosure, for additional information on e-help Desk disclosure procedures. In addition, see IRM 3.42.7.15, Authentication and Authorization Guidelines and IRM 10.5, Privacy and Information Protection. This section and the subsections that follow provide specific guidance for authenticating customers calling the e-help Desk including e-Services users.
- (4) Complete information on disclosure, the Freedom of Information Act (FOIA), and the Privacy Act, may be found in IRM 11.3, Disclosure of Official Information. For questions or additional information visit the *Contact Disclosure* page. The Disclosure Help Desk number and e-mail address are for internal use only.

## 3.42.8.3.1 (10-01-2025) Authorized Users

- (1) Five categories of authorized users can access e-Services products:
  - **Principal** - a sole proprietor, a partner who has a 5 percent or more interest in a partnership, or a corporate officer (e.g., a President, Vice President, Secretary, Treasurer). A Principal for an entity that is not a sole proprietorship, partnership or corporation is an individual authorized to act for the entity in legal and/or tax matters.
  - **Responsible Official** - an individual designated by a Principal to perform specific duties of a Principal. In TIN Matching, this includes modifying an existing TIN Matching Application.
  - **Delegated User** - an individual authorized by a Principal or Responsible Official to perform duties for which they have been granted authority.
  - **Authorized Agent** - an individual that, with a payer's written authorization, matches name and TIN combinations on behalf of a payer.
  - **Reporting Agent** - an accounting service, franchiser, bank, service bureau or other entity that complies with Rev. Proc. 2012-32 and is authorized to prepare electronically Form 940, Employer's Annual Federal Unemployment (FUTA) Tax Return; Form 940-PR, Planilla para la Declaracion Anual del Patrono de la Contribucion Federal para el Desempleo (FUTA)(Historical); Form 941, Employer's QUARTERLY Federal Tax Return; Form 941-PR, Planilla para la Declaracion Federal TRIMESTRAL del Patrono; Form 941(sp), (Spanish Version) Employer's QUARTERLY Federal Tax Return; Form 941-SS, Employer's QUARTERLY Federal Tax Return - American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, and the U.S. Virgin Islands (Historical); Form 943, Employer's Annual Federal Tax Return for Agricultural Employees; Form 943-PR, Planilla para la Declaracion Anual de la Contribucion Federal del Patrono de Empleados Agricolas; Form 943(sp), (Spanish Version) Employer's Annual Federal Tax Return for Agricultural Employees; Form 944, Employer's Annual Federal Tax Return; and Form 945, Annual Return of Withheld Federal Income Tax, for a taxpayer. Reporting Agents sign all the electronic returns that they file with a single Personal Identification Number (PIN) signature. When adding the Reporting Agent provider option the system will validate the EIN on the application if it has Form 8655, Reporting Agent Authorization on file.
  - **Authorized Delegate** - an Authorized Delegate (AD) is an individual that is given the responsibility by the Responsible Officials to maintain and sign a revised application. An AD may not create, sign or submit an initial application and may not add, edit or delete an RO.

3.42.8.3.1.1  
(10-01-2024)

**Caller Authentication**

- (1) IRM 3.42.7.15, Authentication and Authorization Guidelines, gives procedures for authentication and authorization for different types of e-Services customers.

3.42.8.3.1.2  
(10-11-2024)

**Compromised Secure Access Digital Identity (SADI) Account**

- (1) Users cannot log in to an e-Services application (i.e., IRS e-file application, TIN Matching, TDS, etc.) using another person's username and password. If it is determined the caller has accessed the system using another user's login credentials, do the following:

- Advise the caller that this is a security violation and violation of the e-Services terms of agreement and that login credentials are personal login, not a company login.
- Ask to speak to the person who owns the login credentials. Advise owner of the security violation and advise them to change their password. Only after properly authenticating the caller, and determining this person is authorized to the specific information, may you proceed with the call.
- If the owner of the credentials does not come to the phone, advise caller that the call must be terminated. Request that the owner of the login credentials call the help desk to enable the account. Determine what application the caller has accessed and document in the description. Escalate to an incident and assign to e-Services Technical Level 2 provider group.

**Note:** If the owner of the credentials calls in later to enable an account disabled by level 2 due to a security violation, complete High-Risk Authentication (HRA) and enable the account. To enable an account, follow the instructions in IRM 3.42.8.4.2, Un-Restricting (Enabling) an Account. Advise the caller that this is a security violation and that the login ID is a personal login, not a company login. After the account is enabled, resolve any other account issues such as activating any inactive applications.

- (2) If the caller believes, or the assistor discovers through discussion and/or research that their account was compromised, advise the owner to reset their password. If the caller would like their account restricted follow steps in IRM 3.42.8.4.1, Restricting an Account.

3.42.8.4  
(05-16-2023)

**Secure Access Digital Identity (SADI)**

- (1) Secure Access Digital Identity (SADI) is the modernized identity proofing and authentication solution for public facing Internal Revenue Service (IRS) applications.
- (2) With SADI, the IRS will no longer provide ID proofing and authentication services. This process is handled by Credential Service Providers (CSPs). CSPs are third parties that will provide the ID proofing/authentication services and the login credentials for the SADI process.
- (3) When a user creates an account through the CSP, the system will generate a CP 303, Your Secure Access Acknowledgement Notice.
- (4) EPSS provides limited support for the following Secure Access Digital Identity related issues for inquiries received after the initial account creation:
- Customer believes they did not create account
  - Customer needs account restricted/un-restricted (enabled)

**Note:** All other taxpayer related SADI issues are unsupported. See IRM 21.2.1.58 , Secure Access Digital Identity (SADI).

- (5) The taxpayer can designate a representative to act for them in unrestricting (enabling) or restricting the taxpayers' SADI Account by submitting a Form 2848, Power of Attorney and Declaration of Representative. On the form, the taxpayer must indicate specific-use and indicate "Restrict SADI Account" or "Un-Restrict/Enable SADI Account" in the "Matter" column (tax form/years would be marked as "N/A").
- (6) Follow all EPSS procedures for interaction/incident creation, solutions and authentication found in IRM 3.42.7 , EPSS Help Desk Support.

## 3.42.8.4.1 (02-14-2025) Restricting an Account

- (1) Differences in security requirements for the online applications will result in different customer experiences. The customer will receive a CP 303 indicating an account has been created to login to the various online systems.
- (2) Explain the letter they received is related to requesting an IRS online account. Ask the customer if they recall creating an online account. If the customer recalls creating an online account, close interaction.
- (3) If the customer does not recall registering or requests their account be disabled, **advise the customer you will restrict their account.**
  - If asked about how this account could have been used, explain we do not have the capability to research historical records associated with an online product.
  - If the caller is concerned they may be a victim of identity theft (IDT) they can consider filing an Identity Theft Affidavit with the IRS (Form 14039, Identity Theft Affidavit/Form 14039 (sp),(Spanish Version) Identify Theft Affidavit) which is available online at irs.gov (keyword: identity theft). If the customer requests assistance in completing Form 14039, you can help the customer navigate to the form. If asked about the mailing address or fax number, advise the caller to follow the guidance in Form 14039 instructions. Advise the customer to wait 90 days before contacting the Identity Protection Specialized Unit (IPSU).
- (4) Access the Secure Access Digital Identity (SADI) Admin Console and restrict the account using the steps in Figure 3.42.8-2 below:

### Steps to Restrict an IRS Online Account using the SADI ADMIN Console

1. On the SADI Admin Screen, access the drop-down menu to select the search criteria then enter the identifying information:

- TIN XXXXXXXXXX or XXX-XX-XXXX,
- Universally Unique Identifier (UUID)
- Email Address
- IRS ShortID

2. To view the user's account, select "View Details"

**Steps to Restrict an IRS Online Account using the SADI ADMIN Console**

3. Once in the user's account, expand the "Restrictions" section and click on "Apply a Restriction"

4. Complete the required fields:

**Note:** The TIN field will be pre-populated and grayed out.

- Reason: Drop down list of all available restrictions. Select the restriction that applies to the customer's needs.
- Admin Comments:
  - Date of Contact
  - Interaction number

5. Click Submit. The system will show a message at the top of the Account Details page confirming the restriction has been added. "Account Status" will then change to "Restricted".

**Figure 3.42.8-2 Steps to Restrict an IRS Online Account using the SADI ADMIN Console**

- (5) Enter TC 971 AC 522 using IDRS Command Code (CC) REQ77 in customer's individual account when restricting an online account due to possible Identity Theft or customer stating they did not request an online account. Include the following reason codes in the Miscellaneous field when entering TC 971 or TC 972:

- **WI EPSS Disable** – Use when entering TC 971 AC 522.
- **PPDS OPIP IRSERR** – Use when entering a TC 972 to reverse a TC 971 in error.
- **PPDS OPIP NOIDT** – Use when entering a TC 972 to reverse a TC 971 previously input by EPSS and caller is now stating they were not a victim of identity theft.

**Note:** Use the date of the CP 303 for the secondary date if known or use the previous day of the account disable.

**Note:** If the response screen when using IDRS Command Code REQ77 states "NO DATA AVAILABLE", A TC971 AC522 is not required. Include the following comment in the interaction in EHSS: "Unable to enter TC971 AC522 - REQ77 response screen stated NO DATA AVAILABLE".

- (6) Before closing the interaction, you **must** select the appropriate restriction reason code problem type.

3.42.8.4.2  
(10-01-2024)  
**Un-Restricting  
(Enabling) an Account**

- (1) A customer may contact the IRS to have their account enabled. If the customer would like their account enabled, complete High-Risk Authentication. Follow Guidance in IRM 3.42.7.15.9, Secure Access Digital Identity (SADI) Authentication/Authorization.
- (2) Access the Secure Access Digital Identity (SADI) Admin Console and enable the account using the steps in Figure 3.42.8-3 below:

Steps to Un-Restrict (Enable) an IRS Online Account using the SADI ADMIN Console
<p>1. On the SADI Admin Screen, access the drop-down menu to select the search criteria then enter the identifying information:</p> <ul style="list-style-type: none"> <li>• TIN XXXXXXXXXX or XXX-XX-XXXX,</li> <li>• Last Name, First Name (Smith, John),</li> <li>• Unique Identifier (UUID)</li> <li>• Email Address</li> </ul>
<p>2. To view the user's account, select "View Details"</p>
<p>3. Once in the user's account, expand the "Restrictions" section and click on "Remove Restriction" if the option is available.</p> <p><b>Note:</b> If the option to "Remove Restriction" is not next to the restriction, it cannot be removed by a Level 1 assistor.</p>
<p>4. Complete the required fields:</p> <ul style="list-style-type: none"> <li>• Admin Comments: <ul style="list-style-type: none"> <li>• Date of Contact</li> <li>• Interaction number</li> <li>• Notate the caller's phone number. If the caller will not provide one, notate phone number not provided.</li> </ul> </li> </ul>
<p>5. Click Submit. The system will show a message at the top of the Account Details page confirming the restriction has been removed. "Account Status" will then change to "Active".</p>

**Figure 3.42.8-3 Steps to Un-restrict (Enable) an IRS Online Account using the SADI ADMIN Console**

3.42.8.5  
(10-11-2024)  
**Business Tax Account (BTA)**

- (1) Business Tax Account (BTA) provides online self-service capabilities for business taxpayers to interact with the IRS efficiently and effectively while reducing the burden of paper and phone interactions.
- (2) For entities other than Sole Proprietors, a Designated Official (DO) will need to request access to see an entity's information.
- (3) A CP311 will be mailed to the DO. The DO must return to BTA and enter the PIN to complete the registration process by accepting a final self-assertion and electronically sign.
- (4) A CP311A notifies the business that someone requested to be a DO on behalf of the business.
- (5) Both letters are mailed to the last known entity address.
- (6) EPSS only supports calls where an individual and/or business did not request or authorize BTA access:
  - Customer believes they did not create account.
  - Customer needs account restricted/un-restricted (enabled)

**Note:** All other taxpayer related BTA issues are unsupported.

#### 3.42.8.5.1 (03-11-2025)

##### Authenticated CP311 Restriction Inquiries

- (7) Follow all EPSS procedures for interaction/incident creation, solution and authentication found in IRM 3.42.7 , EPSS Help Desk Support.
- (1) If the caller receives a CP311, explain that the letter they received is related to online request to Business Tax Account (BTA).
- (2) Ask the caller if they recall creating an online account. If the caller does recall creating an online BTA account, advise the caller to follow the instructions on the notice, and close the interaction.
- (3) If the caller does not recall creating an account, or requests their account be restricted, **advise the caller of the following:**
- Your request is being referred to another area for review and determination.
  - The PIN request will be blocked.
- Note:** This restriction only impacts online access to BTA and **does not** impact the ability for a business/entity to e-file returns, make federal tax payments via EFTPS or an individuals' SADI access.
- The caller can continue to use the non-digital channels (telephone, in-person, correspondence) to interact with the IRS regarding their business/entity.
  - If the caller is concerned they may be a victim of **tax related** identity theft, they can consider filing a Form 14309-B, Business Identity Theft Affidavit which is available online at irs.gov.
- (4) Document the following in the description and escalate the interaction to an incident and assign to BTA Analysts Provider Group:
- Name of caller
  - Title of caller
  - Phone number of caller
  - Name of entity (as it appears on the notice)
  - EIN of entity
  - Individual listed as the DO requesting access. For the CP311, this individual is listed in the Attn. section of the address.
  - U.S. State where entity filed for articles of incorporation or similar registration.

**Note:** If the caller is unaware of where/what articles of incorporation were filed, state "unknown" in the description.

#### 3.42.8.5.2 (03-11-2025)

##### Other CP311/CP311A Restriction Inquiries

- (1) If the caller received a CP311/CP311A, explain that the letter they received is related to requesting a Business Tax Account.
- (2) Ask the caller if they recall creating an online account or having the individual request the access to the system. If the caller recalls creating an online account or having the individual request access, advise the caller to follow the instructions on the notice, and close the interaction.
- (3) If the caller did not authorize the individual listed on the CP311/CP311A to have access or the caller requests the EIN/Entity be blocked, advise the caller of the following:



- Your request is being referred to another area for review and determination.
- The PIN request will be blocked.

**Note:** This restriction only impacts online access to BTA and **does not** impact the ability for a business/entity to e-file returns, make federal tax payments via EFTPS or an individuals' SADI access.

- The caller can continue to use the non-digital channels (telephone, in-person, correspondence) to interact with the IRS regarding their business/entity.
- If the caller is concerned they may be a victim of **tax related** identity theft, they can consider filing a Form 14039-B, Business Identity Theft Affidavit, which is available online at [irs.gov](https://www.irs.gov).
- Other individuals who can legally bind the entity (Designated Officials) can still register for access. Unless the caller requests the EIN/Entity be blocked, other DOs will be unable to access BTA on behalf of the business.

- (4) Document the following in the description, escalate the interaction to an incident and assign to BTA Analysts Provider Group:

- Name of caller
- Title of caller
- Phone number of caller
- Name of entity (as it appears on the notice)
- EIN of entity
- Individual listed as the DO requesting access
- U.S. State where entity filed for articles of incorporation or similar registration

**Note:** If the caller is unaware of where/what articles of incorporation were filed, state "unknown" in the description.

## 3.42.8.5.3 (10-01-2025) Unrestricting (Enabling) an Account

- (1) Advise the caller of the following:

- Your request is being referred to another area for review and determination.
- Please allow up to 10 business days before accessing the system.

**Note:** See IRM 3.42.7.15.8 , SAM, EFTPS, BTA and Business Online e-file (e.g., Large Taxpayers) Authentication/Authorization.

- (2) Document the following in the description, escalate the interaction to an incident and assign to BTA Analysts Provider Group:

- Name of caller
- Title of caller
- Phone number of caller
- Name of entity (as it appears on the notice)
- EIN of entity
- Individual listed as the DO requesting access
- U.S. State where entity filed for articles of incorporation or similar registration

**Note:** If the caller is unaware of where/what articles of incorporation were filed, state “unknown” in the description.

3.42.8.6  
(09-09-2021)  
**E-Services**

- (1) E-Services is available 24 hours a day, 7 days a week from any computer with an Internet connection. The e-help Desk assistants must provide quality service to external customers who encounter problems or need information about e-Services.
- (2) The e-help Desk assistants provide support for the following e-Services products:
  - **IRS e-file Application** - permits users to submit a new or revised IRS e-file Application to become an Authorized IRS *e-file* Provider and to update their application as needed. See IRM 3.42.10, Authorized IRS e-file Providers, for information on adding a new location, closing an office, etc.
  - **Taxpayer Identification Number (TIN) Matching Application** - allows payers of income subject to backup withholding to apply for the TIN Matching Program.
  - **TIN Matching Program** - allows authorized users to match TINs and names directly against IRS records.
  - **Transcript Delivery System (TDS)** - allows users to electronically request and receive transcripts, wage and income documents for a taxpayer's account, and verification of non-filing. Tax preparers using TDS must have an unmodified Power of Attorney (POA) on file.
- (3) Products and Services Support (PSS) is responsible for the e-Services Technical Level 2 Provider Group and works e-Services issues that the e-help Desk cannot resolve on first contact.

**Reminder:** Document the Interaction per IRM 3.42.7.6.8.1, Writing Descriptions for Level 2, when escalating to e-Services Technical Level 2. Escalate the interaction to obtain an Incident Management (IM) case number and provide the IM case number to the customer.

3.42.8.6.1  
(10-01-2024)  
**Accessing E-Services**

- (1) The e-Services system supports all common internet browsers (i.e., Edge, Safari, Firefox, Chrome, etc.).
- (2) Employees access e-Services via the Employee User Portal (EUP).
- (3) Customers access e-Services via the Integrated Enterprise Portal (IEP). Access e-Services applications by one of the following:
  - irs.gov > “Tax Pros” > “Access e-Services” button > select application
  - irs.gov > Keyword search “e-Services” > “e-Services” > select application
- (4) E-Services Error Codes
  - If e-Services User is receiving an error code 114, assign incident to e-Services Technical Level 2 Provider Group.
  - If e-Services User is trying to complete the Terms of Service (TOS) and the page is not appearing, the page is looping or the page takes the



user straight back to the e-Services page on irs.gov without offering the user a chance to sign the TOS, assign incident to e-Services Technical Level 2 Provider Group.

3.42.8.6.1.1  
(09-17-2020)  
**Employee User Portal (EUP)**

- (1) The Employee User Portal (EUP) is a Web hosting infrastructure. It supports an Intranet portal that allows IRS employees to access business applications and data (e.g., e-Services and Modernized e-file (MeF)). The EUP communicates with MeF via Application Message and Data Access Service (AMDAS). The EUP infrastructure is located on the IRS Intranet.
- (2) Employee registration and authentication is required for the EUP. A Business Entitlement Access Request System (BEARS) request is not required for EUP access but is required for access to individual applications within EUP. To access the EUP, you will need the following information:
  - Standard Employee Identifier (SEID). If you do not know your SEID, locate it using the *Discovery Directory*.
  - Appropriate e-Services roles. Obtain these from your manager. Request the roles through *BEARS*.

3.42.8.6.1.2  
(09-17-2020)  
**Integrated Enterprise Portal (IEP)**

- (1) The IRS Integrated Enterprise Portal (IEP) (previously referred to as “Registered User Portal (RUP)”) allows registered individuals, third-party users and self-authenticated individual taxpayers access to selected specific tax information and other sensitive applications and data. User interactions are encrypted from the user’s workstation or system to the portal. The IEP also supports the exchange of bulk files of information with the IRS. The IEP communicates with the back-end modernization application system.

3.42.8.6.1.3  
(10-01-2024)  
**Clear Cache**

- (1) Customers may receive an error such as “URL not found”, “Target not found” or “Response empty” when accessing and using e-Services because they need to clear their cache. Recommend the customer do the following:
  - Completely close their web browser, clear the cache, and sign in again.
  - Set irs.gov as their only shortcut/favorite.
  - Get to the login page by clicking on Tax Professionals then e-Services for Tax Pros or search by using “e-Services” to get to the e-Services for Tax Pros link.

**Note:** Examples of browsers currently supported are Edge, Safari, Firefox, Chrome (this list is not all inclusive). Internet Explorer is being phased out as an acceptable browser.

- (2) If the customer does not know how to clear the cache, request they complete a search on steps to clear cache for their browser.

**Note:** Additional clearing cache information for common internet browsers is available in the Knowledge Management document KM000661, System Related Problems.

3.42.8.6.2  
(10-01-2022)  
**Short ID**

- (1) A Short ID is an 8-10 character alphanumeric code that each e-Services user will need if they want information delivered to their Secure Object Repository (SOR) or if they use the Application Program Interface (API).

- If the individual was an e-Services user **before** the SADI transition, the Short ID is their existing e-Services Username.
- If the individual was an e-Services user **after** the SADI transition, the Short ID is an alphanumeric system generated ID.

(2) A user's Short ID is found on their e-Services **Select Your Organization** page.

#### 3.42.8.7

(10-01-2025)

#### Taxpayer Identification Number (TIN) Matching

- (1) The e-Services TIN Matching Program is intended to assist those members of the third party payer community, and their authorized agents, with meeting their obligation for filing accurate and complete annual information return documents. In addition to financial institutions, other eligible entities are credit card companies, state agencies, third-party settlement organizations, and third-party network transaction companies. The system allows authorized users to match TINs and names directly against IRS records. The TIN Matching system allows for a proximal match for SSN's, meaning the first letter of the name control must match, the second and third letters can be swapped, the third and fourth letters can be swapped, and any valid character in the second, third, or fourth position will create a proximal match (i.e., AXCD, ABXD, and ABCX would all be valid proximal matches for name control ABCD).
- (2) TIN Matching does not divulge a taxpayer's TIN or a business's EIN. It only verifies whether the TIN and name combination which the user submitted matches IRS records. To participate in this program, authorized users must complete a TIN Matching Application through e-Services and meet the following eligibility requirements:
  - Applicant must be a payer of income subject to backup withholding submitted on Form 1099-B, Form 1099-DIV, Form 1099-G, Form 1099-INT, Form 1099-K, Form 1099-MISC, Form 1099-NEC, Form 1099-OID or Form 1099-PATR.
  - Payer must have filed Form 1096, Annual Summary and Transmittal of U.S. Information Returns, reporting income paid on Form 1099, or submit information returns electronically, in one of the last two years.
- (3) Use IDRS CC PMFOL to research Payer Master File and verify payer is eligible to participate in TIN Matching.
- (4) TIN Matching Roles:
  - a. **Principal** - a partner or an individual who owns at least five percent of the firm that is applying to participate in the TIN Matching Program. The "Principal" may also be a corporate officer of a publicly traded firm, such as President, Vice President, Secretary, or Treasurer. The "Principal" must be the person who can legally bind the firm in matters before the IRS and must complete the original application to TIN Match on behalf of the firm. Principals may modify any section of the application. They may add and/or remove locations and authorized users and change the firm/organization information.
  - b. **Responsible Official** - an individual who holds a supervisory position within the firm. A "Responsible Official" has the authority to update an application on behalf of their listed firm and firm "Principal". The "Responsible Official" may change the firm/organization information, assign/disable "authorized agent" and "Delegated user" roles, add and/or

remove locations and perform TIN Matching. Responsible Officials may modify any section of the application.

**Note:** Only a Principal or Responsible Official can add another Principal or Responsible Official. It is a good practice to list a second person. The Responsible Official can be a different individual from the Principal. More than one Principal and/or Responsible Official can be listed.

- c. **Authorized Agent** - a person or firm that, with the payer's authorization, transmits specific information return documents to the IRS on behalf of the firm and may match name/TIN combinations on behalf of the payer.
- d. **Delegated User** - an individual who will utilize the TIN Matching session options on behalf of the firm. A "Delegated User" may not assign or disable users or update applications on behalf of their assigned firm. A "Delegated User" may only perform TIN Matching on behalf of their assigned firm.

- (5) Publication 2108 , Federal Agency TIN Matching Program, provides guidelines for the TIN Matching Program.

## 3.42.8.7.1 (05-16-2023) **TIN Matching Access Inquiries**

- (1) When the customer (payer) indicates that they cannot access TIN Matching even though their employer has named them as an authorized user, take the following steps:
  - a. Verify the user has created a Secure Access Digital Identity Account.
  - b. Verify the caller is using the correct link on irs.gov.
  - c. Verify the caller is listed on the TIN Matching Application.

**Note:** If they aren't listed on the application, explain they need the Principal to add them. If the application is not in Completed status, explain the principal must submit the application before they can see their links.

  - d. Many users forget to resubmit the application after making additions or changes. Unlike an IRS e-file Application, the TIN Matching Application requires a PIN entry only at the initiation of the application, not after each subsequent change. If the authorized user fails to submit the application, the assistor will submit the application in the interest of good customer service. Remind the caller, they must resubmit the application after any changes to avoid future problems.
  - e. If the caller is still receiving the error after trying all the above, escalate the incident to e-Services Technical Level 2 Provider Group.

## 3.42.8.7.2 (10-01-2016) **Delete/Revoke/Restore a TIN Matching Application**

- (1) If the customer inquires about the ability to remove a firm's TIN Matching Application from the system or requests restoration of a previously deleted application, determine their role on the application. If they are not the Principal, advise the caller that only Principals can make such a request.
- (2) If the caller is the Principal and still needs assistance with revoking, deleting, or would like to restore a previously deleted TIN Matching Application, advise the customer that you will refer their request to the e-Services technical staff for resolution. Escalate interaction to e-Services Technical Level 2 Provider Group. Document interaction with the following information:

- Name of Principal
- IRS Short ID of Principal
- Telephone number (with time zone) of Principal
- Position in the company (president, vice president, owner, etc.)
- Company name as shown on the TIN Matching Application
- Company TIN as shown on the TIN Matching Application
- Reason for revoking, deleting or restoring the application

3.42.8.7.3  
(10-01-2024)

**Replace a Principal**

- (1) If there is only one Principal or Responsible Official on the application and they are no longer with the company or the application was started without a Principal or Responsible Official, advise the caller that only an owner, officer, or partner of the company can replace/add the new Principal. If an existing Principal is listed on the application, the individual becoming the new Principal must know who the existing Principal is and give you the individual's name. If the caller qualifies as a principal, after authenticating using the SAM, EFTPS, BTA, and Business On-line Filer section of the EPSS Authentication and Authorization (AA) Job Aid, make the necessary changes. Advise the new principal to submit the application.

3.42.8.7.4  
(04-01-2014)

**Bulk TIN - Valid Response**

- (1) When submitting a Bulk TIN Request (up to 100,000 TIN and name combinations), as well as an Interactive TIN Request (up to 25 TIN and name combinations), there are nine possible result codes. If the customer calls in for an explanation of these codes, offer the following definitions:
  - a. 0 - Name/TIN combination matches IRS records
  - b. 1 - Missing TIN or TIN not a nine-digit number
  - c. 2 - TIN not currently issued
  - d. 3 - Name/TIN combination does NOT match IRS records
  - e. 4 - Invalid request (e.g., contains alphas, special characters). Must have TIN Type, TIN, Name (Name field is limited to 50 characters)
  - f. 5 - Duplicate request
  - g. 6 - Matched on SSN, when the TIN type is (3), Unknown
  - h. 7 - Matched on EIN, when the TIN type is (3), Unknown
  - i. 8 - Matched on SSN and EIN, when the TIN type is (3), Unknown
- (2) If the customer does not see the result code they were expecting, and asks for the correct TIN, explain we are not authorized to disclose that information and they will need to verify with their client.

3.42.8.7.5  
(04-01-2014)

**Bulk TIN - No Response**

- (1) When a customer submits a Bulk TIN request, they will receive an acknowledgement page with tracking number. The customer will receive a response within 24 hours. If a customer calls because a response has not been received, or the results are illegible, ask the customer to resubmit their Bulk TIN request. Have them record the tracking number and the date/time stamp of their submission. If they still have not received a response after an additional 24 hours have passed, they should call the e-help Desk again.
- (2) When the customer calls back because they still have not received a response, escalate interaction to e-Services Technical Level 2 Provider Group. Include tracking number and date/time stamp provided by customer, Short ID, and company EIN in interaction documentation.

3.42.8.7.6  
(10-01-2014)  
**TIN Matching  
Suspended and/or  
Locked Out**

- (1) When the customer is suspended and/or locked out while performing Interactive TIN matching, they will receive a pop-up message indicating they are locked and the reason (e.g., Results Code 5 - Duplicate). Inform the customer:
  - a. The TIN Matching program contains a built-in security feature that detects when a customer's EIN, SSN or ITIN is being researched using different names.
  - b. Account access is blocked for four days (96 hours).
  - c. They will have to wait for the system to unlock them.
- (2) When the customer is locked out while performing Bulk TIN Matching, the system will generate a tracking number for the submission and a message referencing this tracking number is sent immediately to their Secure Mailbox. The bulk lockout does not return result codes.
- (3) General Services Administration (GSA) is the organization responsible for the System for Award Management (SAM) website. If a GSA customer is locked out:
  - a. Verify customer information (customer name, telephone number, firm name and EIN) in EHSS. If not correct, document correct information in interaction description along with the Short ID and EIN.
  - b. Escalate interaction to e-Services Technical Level 2 Provider Group.

3.42.8.7.7  
(10-01-2014)  
**TIN Matching Error  
Messages**

- (1) Sometimes the customer will receive an error message when attempting to use TIN Matching. The two most common errors are:
  - Line %1 contains invalid data or has more or less semicolons
  - 96 Hour Lockout
- (2) If the customer receives "Line %1 contains invalid data or has more or less semicolons" error message, they must correct and resubmit file.
- (3) If the customer receives "96 Hour Lockout" error message, they must wait for the system to unlock them.

3.42.8.8  
(10-01-2024)  
**Transcript Delivery  
System (TDS)**

- (1) Transcript Delivery System (TDS) allows specific tax professionals, Reporting Agents, Low Income Tax Clinics (LITC), state and local governmental agencies, and internal IRS users to request and receive transcripts electronically. Large Taxpayers are not entitled to use TDS even though they may have submitted five or more accepted returns electronically. Tax professionals and LITC representatives must have a Form 2848, Power of Attorney and Declaration of Representative or a Form 8821, Tax Information Authorization on file to access client transcripts. Reporting Agents need a valid Form 8655, Reporting Agent Authorization.
- (2) The e-Services product is available to:
  - An ERO who has successfully submitted five accepted e-file returns.
  - Circular 230 Participants, CPAs or attorneys that do not e-file and are applying only for TDS access.

**Note:** The EUP user must select the "Do Not Cleanup" button on the "Summary" page to prevent these EFINS from getting inactivated during the EFIN Cleanup process.

- Reporting agents with no minimum number of returns needed to gain access.

**Note:** TDS is manually assigned by an IEP EUP user if necessary. Prior to accessing TDS, a user must have or create a Secure Access Digital Identity (SADI) account. The TDS link defaults to principals, responsible officials, and Principal consents but must be manually assigned to a delegated user.

- Low Income Tax Clinics (LITC) - the LITC Program Office inputs these e-file applications and can also make any necessary updates through the IEP EUP.

**Note:** You must select the “Do Not Cleanup” button for these applications.

(3) The following **individual transcripts** are available through TDS:

- **Account Transcripts** show the information posted on the account, including payments, adjustments, etc., and are available for any account that is active on the IRS Master File.
- **Return Transcripts** include most lines from the original return, including attached forms and schedules, and are available for returns filed during the current and three prior years.
- **Record of Account Transcripts** are a combination of the account and return transcripts and are available for returns filed during the current and three prior years.
- **Wage and Income Documents** show income reported by payers on forms such as Form W-2, Wage and Tax Statement and Form 1099 Series. Available for the current and nine prior tax years.
- **Verification of Non-Filing** generates a letter when a taxpayer needs verification that a tax return was not filed, and is available for the current and three prior tax years.
- Additional information on Transcripts is available in IRM 21.2.3.3.1, Transcript Assistance by an IRS Representative.

(4) The following **business transcripts** are available through TDS:

- **Account transcripts** are available for any account that is active on the IRS Master File.
- **Return transcripts** are available for the current year and returns processed during the prior three processing years. BMF forms are available for Form 1065, U.S. Return of Partnership Income, Form 1120, U.S. Corporation Income Tax Return, Form 1120-H, U.S. Income Tax Return for Homeowners Association, Form 1120-L, U.S. Life Insurance Company Income Tax Return, and Form 1120-S, U.S. Income Tax Return for an S Corporation. TDS offers business taxpayers tax return transcripts that provide tax return information from the original return in addition to adjustments from the amended returns. These transcripts are available for the following forms:
  - Form 940, Employer’s Annual Federal Unemployment (FUTA) Tax Return
  - Form 941, Employer’s Quarterly Federal Tax Return
  - Form 943, Employer’s Annual Tax Return for Agricultural Employees
  - Form 944, Employer’s ANNUAL Federal Tax Return
  - Form 945, Annual Return of Withheld Federal Income Tax



**Note:** For additional information, see IRM 21.2.3.2.1, Tax Return Transcript.

- **Record of account transcripts** are a combination of the account and return transcripts and available for returns filed during the current and three prior years.
- The modified business entity transcript displays limited entity information for specific Employer Identification Number (EIN). The transcript shows the EIN, business operating division, primary name, sort name, care of name, name control, and street/foreign address. Available for TY 2023.
- The business entity transcript includes the fields from the modified business entity transcript and additional fields providing more comprehensive entity information such as the IRS establishment date, business operational date, filing requirements, and exempt organization status. Available for TY 2023.

**Note:** Additional Information is available in IRM 21.2.3.2.6, Modified Business Entity Transcript and Business Entity Transcript.

**Note:** Wage and income documents are not available for business.

**Note:** TDS will not generate transcripts if the requested year has a TC 971 AC 524 indicating taxpayer deceased account locked on file.

## 3.42.8.8.1 (10-01-2025) Access to Client Information

- (1) To access client information via e-Services, the user must have a Form 2848, Power of Attorney and Declaration of Representative, or Form 8821, Tax Information Authorization (TIA), on file. This authorization can be viewed on IDRS using CC CFINK and the taxpayer's TIN. Review the CC CFINK response screen for the following:
  - The Powers field must contain a "U" for unmodified.
  - The information must be complete. If the information is not complete, the customer must mail or fax the Form 2848 , Power of Attorney and Declaration of Representative, or Form 8821 , Tax Information Authorization to the Centralized Authorization File (CAF) Unit.
- (2) If the customer is using TDS and receives a CAF Failure error, research and provide the CAF number as follows:
  1. Request customer's name and address to research Integral Data Retrieval Systems (IDRS) CC RFINK or CC CFINK.
  2. Verify the name control on IDRS matches the name control on the eFile Application.
  3. Confirm there is an existing CAF number(s) for the caller.
  4. Authenticate the caller's identity by following probes found in IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication.
  5. Provide the correct CAF number when the caller is using the wrong CAF number, ONLY after verifying the practitioner's name and address match what is shown on the CAF database. If they don't match and the practitioner is actively working with their client to resolve a tax account issue as outlined in IRM 21.3.10.2 , Practitioner Priority Service (PPS) Overview, they may call the Practitioner Priority Service (PPS) at 866-860-4259 to secure transcripts. PPS is a nationwide toll-free, account related service for all practitioners and serves as the first point of contact for assistance regarding their clients' account related issues.

**Note:** You will only look up and provide the correct CAF number when providing support for TDS rejects. Refer all other requests to PPS.

3.42.8.8.1.1  
(10-01-2014)

**Centralized  
Authorization File (CAF)**

(1) The following forms must be mailed or faxed to the CAF Unit:

- Form 2848, Power of Attorney and Declaration of Representative (POA) - A taxpayer can grant authority to representatives to receive tax data and represent them before the IRS. Form 2848 covers specific tax forms and tax periods.
- Form 8821, Tax Information Authorization - A taxpayer can grant authority to any individual or organization to inspect or receive the taxpayer's confidential tax information. Form 8821 covers specific tax forms and tax periods for Form 2848.

**Note:** A signed copy of Form 2848 or Form 8821 must be retained in the authorized representative's files.

- (2) The authorization must post to the CAF database prior to them submitting a TDS request for transcripts through e-Services.
- (3) Direct customer inquiries regarding multiple CAF numbers, name change requests, etc. to CAF. You will direct callers to the appropriate CAF unit for their state. You will find CAF Unit mailing addresses and fax numbers on the CAF Unit Addresses, Fax Numbers, and State Mapping page of [irs.gov](http://irs.gov), form instructions, and in IRM 21.3.7.1.6, Audience-Processing Sites (CAF Function).

3.42.8.8.2  
(10-01-2025)  
**Rejected TDS**

(1) TDS will reject requests for transcripts if any one of the following conditions is present on the taxpayer's CAF record:

- Designation level under the column LV shows "X".
- Powers Code under the column AUTHS shows anything other than "U" (Unmodified) or I (Inspect) for Form 8821, Tax Information Authorization.
- Column RCTS shows "R" (authority to receive a refund), this is a modification for e-Services purposes.

(2) TDS will reject requests for transcripts if any one of the following conditions is present on the representative's CAF record in the CAF STATUS or STATUS field:

- Undeliverable
- Deceased
- Disbarred
- Suspended
- Resigned
- Ineligible
- Inactive

(3) TDS does not generate transcripts for any tax year where there is an Identity Theft Indicator on the account. A transcript requested by the POA for an account affected by identity theft for that year will not be generated. The letter to the practitioner will direct them to call the Practitioner Priority Service at 866-860-4259 for assistance in obtaining a transcript for years affected by identity theft.



3.42.8.8.3  
(01-23-2014)  
**Married Taxpayers**

- (1) A valid POA or TIA is required for at least one of the joint filers for the following transcripts: Account Transcript, Tax Return Transcript, and Record of Account Transcript. However, a representative is only entitled to Verification of Non-Filing and Wage and Income Transcripts for the joint filer for which they have a valid POA or TIA.

3.42.8.8.4  
(10-01-2024)  
**IRS Employees**

- (1) Advise IRS employees who experience problems using TDS to contact the Information Technology Support Desk at 866-743-5748, to open an IRWorks ticket.

3.42.8.8.5  
(10-01-2024)  
**State Users**

- (1) State users wanting to apply for the TDS product should be directed to the *State Agency Services* page on irs.gov.

3.42.8.8.6  
(10-01-2023)  
**Common TDS Problems**

- (1) Sometimes the user has problems transmitting and receiving their TDS information. The following subsections may help to resolve those issues. If the problem is still not resolved, escalate the interaction to e-Services Technical Level 2 Provider Group. Always include the ShortID in the description when elevating to Level 2.

3.42.8.8.6.1  
(09-11-2007)  
**Bulk Request Upload Error Message**

- (1) When the customer is sending a bulk file, it should not contain more than one megabyte (MB) of information. If the customer calls because of the "Bulk file contains errors" message, follow the chart below:

If ...	Then ...
The file name is not lowercase and the extension is not .txt	Advise the customer that their file name must be lowercase and the extension on the file must be .txt regardless of what software (Word, Excel, Notepad, etc.) was used to create the file. Save the file in Plain text using Notepad and the extension .txt. Then try to upload the file again.
The file is larger than 1 MB of information	Advise the customer to lower the size of the file and try to upload the file again.

**Figure 3.42.8-4 Bulk File Contains Errors Message**

3.42.8.8.6.2  
(09-05-2013)  
**Unable to Receive Business Master File (BMF) Return Transcripts**

- (1) Sometimes the customer will request BMF return transcripts currently not available through TDS. A limited number of BMF return transcripts are available through TDS. If the forms the customer is requesting are available, look up the authorities in IDRS using CC CFINK. If the customer's POA is not posted for the year(s) and form(s), advise them to submit a POA to update the CAF authorities.

- (2) For state users: if the product, form number, and tax period (year and month) is available on TDS, the product is within the years available through TDS, and the customer still cannot get the product, escalate the interaction to e-Services Technical Level 2 Provider Group.

3.42.8.8.6.3  
(10-01-2024)  
**TDS Letters Cut Off or  
Cannot Print**

- (1) Customers may experience problems with printing transcripts. If the transcript is cut off in part, or will not print at all, assist the customer based on the type of browser the customer is using.
- (2) Advise the customer that at this time e-Services supports all common internet browsers (i.e. Edge, Safari, Firefox, Chrome, etc.). Suggest the customer switch to another browser and try again.

3.42.8.8.7  
(10-01-2024)  
**Income Verification  
Express Service (IVES)  
Users**

- (1) IVES is a partially automated service that provides two to three business day processing and delivery of transcripts to participants who pay a fee for this service. Each company must complete Form 13803, Application To Participate in the Income Verification Express Service (IVES) Program, which is reviewed for suitability then entered into the EUP by IVES Coordinators in the Return and Income Verification Services (RAIVS) unit. IVES customers request transcripts by faxing a valid form from the Form 4506 family to the appropriate RAIVS unit. Once an IVES Application is established for them by the RAIVS unit, and they are given a Participants/Consolidator number, you will treat them the same as any other customer. The IRS will deliver transcripts to the customer's e-Services Secure Mailbox (Secure Object Repository (SOR)).
- (2) The Principal, Responsible Official and Delegated User assigned to use e-Services products must register individually to create and have access to a Secure Mailbox. Only the Principal can access the IVES Detail and Summary Reports.
- (3) IVES users may maintain and revise their application by logging into e-Services and clicking on the IVES Consolidator Application link, which will bring up the Main screen showing all links within the application.
  - a. Principals can make changes to the following screens: *Firm/Organization Information, Firm/Organization Address, Business Point of Contact, Establish Location(s), and Authorized User(s)*.
  - b. Responsible Officials can only update authorized user(s).
  - c. Delegated Users cannot make changes to the application but can retrieve transcripts.
  - d. The user will submit all other application changes (including Principal Information changes) on a revised Form 13803, Application to Participate in the Income Verification Express Service (IVES) Program, and fax it to the RAIVS unit.

**Note:** Even though the "IVES Consolidator Application: Principal Information" page shows an edit button, changes to Principal Information will not be made using e-Services. These changes must be completed by submitting a revised Form 13803 to RAIVS.

- (4) If the customer received transcripts without an approved form from the Form 4506 family, refer the customer to the RAIVS unit where they faxed their request.
- (5) Refer the customer to the RAIVS Program office for the following issues:

- a. Application was previously sent to RAIVS and there has been no response.
- b. Customer has trouble accessing the reports (transcripts).
- c. Customer has questions about billing or is disputing a billed amount.
- d. Assistors should also refer to KM000593, Income Verification Express Services (IVES).

**Note:** Raise disputes with the program office within 15 days from the date of the invoice.

## 3.42.8.9 (12-19-2017) Miscellaneous E-Services

- (1) The following subsections provide general information related to e-Services.

### 3.42.8.9.1 (10-01-2024) PIN Rules/Inquiries

- (1) The new e-Services user is prompted to create a PIN. This PIN is used to electronically sign their e-Services applications.
- (2) If a user already has a PIN, no change is necessary.
- (3) The customer may voluntarily change their PIN by logging in and selecting the "Modify PIN" link. The customer will:
  - Enter a new five-digit numeric PIN.

**Note:** The PIN can't be all the same numbers, can't begin with zero and can't be the same as the last PIN.

  - Re-enter the PIN.
  - Click the "submit" button to save the changes.
- (4) Once the PIN is affixed to an electronic document, it indicates that the person making any changes is authorized to do so.

### 3.42.8.9.2 (10-01-2022) Secure Mailbox

- (1) The system assigns each registered user a Secure Mailbox (Secure Object Repository (SOR)) to place or deposit data. Users access this data by clicking the **Mailbox** link from the drop down menu under the e-Services link found in the navigation tool bar along the top of each e-Services page. For most of the products, the system sends an email to the user alerting them it placed data in their Secure Mailbox. Depending on the type of data, and whether it shows read or left unread, the system automatically deletes the files. The delete time-frames are as follows:

Product	Read	Unread
TDS	3 business days	30 business days
TIN Matching	3 business days	30 business days
Business Rule Changes	3 business days	30 business days

**Figure 3.42.8-5 Secure Mailbox Delete Time frames**

## 3.42.8.9.3

(12-08-2023)

**Missing Links**

- (1) To see links, the caller must have created a Secure Access Digital Identity (SADI) Account. To troubleshoot missing links follow the guidance below based on the type of user.
- (2) ERO:
  - Verify the caller is using the correct link on irs.gov.
  - Verify the correct Organization Link was selected. If they previously selected their Responsible Official (RO) (DBA name with Address) link, have them try their Principal link (Legal Name without Address).
  - In EUP, verify the “Services Authorized For” tab has Transcript Delivery System and/or Reporting Agent Transcript Delivery System checked. If user created the application correctly as Circular 230 but didn’t document correctly (i.e., comment was not added to e-file application), assistor can check the Transcript Delivery System box under “Services Authorized For”.
  - Verify the caller has “Authorities” checked by selecting the View icon next to their Name on the “Authorized Users” page.
- (3) Circular 230 User:
  - Verify the caller is using the correct link on irs.gov. The caller should select “Transcript Delivery System (TDS)” then “Access TDS” button and login.
  - Verify the e-File Application was created and documented correctly for Circular 230 access.
  - In EUP verify the “Services Authorized For” tab has Transcript Delivery System checked. If the box is checked and everything above is verified, toggle the check box next to Transcript Delivery System and have the caller log back into the system.
- (4) TIN Matching User, API Client ID, TDS State User, or State EFIN User:
  - Verify the caller is using the correct link on irs.gov.
  - Verify the caller is listed on the appropriate application.
- (5) Affordable Care Act (ACA) Application for Transmitter Control Code (TCC), Information Returns (IR) Application for TCC or Information Returns Intake System (IRIS) Application for TCC Users:
  - Verify the caller is using the correct link on irs.gov.
  - Verify the correct Organization Link was selected.
- (6) To troubleshoot missing Organization Links:
  - Close browser and clear cache/cookies. See IRM 3.42.8.6.1.3, Clear Cache, for more information
  - Verify the caller is a Principal, Principal Consent, RO and/or Delegated User with authorities. Only 14 organization links can be seen.
- (7) If the caller continues to receive an error or cannot see the appropriate links or Organization links after following the guidance above, document the issue and what steps were taken to resolve the issue. Escalate to an incident, provide the incident number to the caller and assign to e-Services Technical Level 2 Provider group.

## Exhibit 3.42.8-1 (10-01-2025)

### Acronyms

The below table contains frequently used acronyms and their meanings.

ACRONYM	MEANING
ACA	Affordable Care Act
CAF	Centralized Authorization File
EFIN	Electronic Filing Identification Number
EPSS	Electronic Products and Services Support
ERO	Electronic Return Originator
EUP	Employee User Portal
FIRE	Filing Information Returns Electronically
HRA	High-Risk Authentication
IDT	Identity Theft
IEP	Integrated Enterprise Portal
IP PIN	Identity Protection PIN
IVES	Income Verification Express Services
OLA	Online Account
PIN	Personal Identification Number
POA	Power of Attorney
PUB	Publication
RAIVS	Return and Income Verification Services
RO	Responsible Official
SADI	Secure Access Digital Identity
SOR	Secure Object Repository
TDS	Transcript Delivery Service
TSO	Technical Services Operation
TIA	Tax Information Authorization
TIN	Taxpayer Identification Number

