Patent Electronic System Access Document

The **Patent Electronic System Access Document** serves as a source document for additional information on the components for accessing the patent electronic system. Patent Electronic System refers to EFS-Web, PAIR, and Patent Center. This document has three components:

1) Authentication process
2) Sponsorship process
3) Verification policy

Authentication Process

USPTO.gov Accounts and MyUSPTO

The Patent Electronic System uses the United States Patent and Trademark Office's (USPTO) single sign-on (SSO) system, the USPTO.gov account, for secure authentication. USPTO.gov accounts are based on email address, and each account uses the email address as the account name or user ID.

USPTO.gov accounts can be created and managed through the MyUSPTO homepage (http://my.uspto.gov/). The MyUSPTO page allows users to create accounts, change passwords, enable two-step authentication, and record personal information, including alternate email addresses and telephone numbers.

Two-Step Authentication

USPTO.gov accounts can be secured with two-step authentication. When two-step authentication is enabled, the user will be presented with a challenge to enter a temporary authentication code after providing a username and password. The temporary authentication code can be provided by one of several methods, which can be chosen by the user, such as email, a mobile code generator app, or a phone call.

When signing in with two-step authentication, the user can select a checkbox indicating that they are signing in from a trusted device. When signing in from a trusted device, the user will not be presented with a two-step challenge for 24 hours.

Signing In and Signing Out

The USPTO.gov account is part of the MyUSPTO single sign-on system. This means that a user only needs to sign in one time to access any of the services protected by MyUSPTO. For example, if a user signs in to Patent Center with their USPTO.gov account, that user will be able to access Financial Manager without signing in a second time. Conversely, signing out from one system will sign the user out from all USPTO systems.

Roles

The following Patent Electronic System roles are assigned by the USPTO as part of the USPTO's proofing process. Users can only have one of the below roles applied to their USPTO.gov account.

Proofed Practitioner	An attorney/agent who has been proofed by the USPTO's proofing process.
Proofed Practitioner Support	A paralegal/practitioner support staff who has been sponsored by a Proofed Practitioner.
Proofed Independent Inventor	An independent (pro se) inventor who has been proofed by the USPTO's proofing process.

Please note that other systems may have roles that can be applied to a USPTO.gov account in addition to one of the above Patent Electronic System roles.

Suspension

In some cases, accounts may be suspended. Suspended accounts cannot access the Patent Electronic System. The USPTO may temporarily or permanently suspend an account for violating the terms of use (e.g., if a user is harming the system or denying access to other users) without prior notice.

Authorization

Signed in users can access private data, which is non-public data related to applications associated with their customer numbers. Proofed Practitioner users can sponsor Practitioner Support Staff. A sponsored support staff individual will have access to the practitioner's private data and will be able to file on behalf of the practitioner.

Authentication Steps

In order to use a USPTO.gov account with the Patent Electronic System, the following steps must be performed:

1. Create a USPTO.gov account using MyUSPTO
    a. Prove ownership of the account email address by clicking the verification link in the automated email sent by MyUSPTO
    b. Create a secure password
    c. Record personal information (i.e., telephone number, mailing address, alternate email address)
2. Enable two-step authentication
    a. Two-step authentication is required for the Patent Electronic System, and must be enabled in the MyUSPTO settings for each USPTO.gov account
    b. Two-step authentication is available using:
        i. Email
        ii. Code generator application (e.g., Oracle Mobile Authenticator, Google Authenticator), which must be configured in the MyUSPTO settings
        iii. Automated voice phone call

    c. The account must be permanently opted in to two-step authentication by selecting the "**I want to use the two-step authentication method every time I sign into MyUSPTO.**" checkbox
3. The account owner's identity must be proven by completing the Patent Electronic System proofing process. The steps for the proofing process is located at the Getting Started – New Users page at https://www.uspto.gov/patents-application-process/applying-online/getting-started-new-users.
    a. When the proofing process is completed by the USPTO, a Patent Electronic System role will be assigned to the USPTO.gov account
    b. The proofed user will be added to the authorization database, which controls access to customer numbers
    c. Proofed user accounts cannot opt out of two-step authentication
    d. Proofed user accounts cannot change email addresses outside of the proofing process
4. Go to the Patent Electronic System
5. Sign in
    a. The user can sign in from the Patent Electronic System directly or sign in from the MyUSPTO landing page
        i. The sign in link is displayed in the header at the top of every page
    b. A signed in user can access their own private data and can perform functions appropriate to their role
    c. Suspension
        i. Suspended accounts that sign in will not be able to access private data or filing functions and an error message will be displayed to the user
6. Sign out
    a. A signed in user can sign out at any time on any page in the Patent Electronic System or in MyUSPTO
    b. A user that has signed out immediately loses access to all private data
    c.

Sponsorship Process

The sponsorship tool allows practitioners to grant or remove sponsorship for support staff individuals to work under their direction and control. The support staff individual must have already created a USPTO.gov account in order to be sponsored by a practitioner. After the sponsorship is complete, the support staff individual will be able to access the Patent Electronic System using their USPTO.gov account. The support staff individual will have access to all applications associated with the customer number(s) of the sponsoring practitioner. The support staff individual must use their own credentials when accessing the Patent Electronic System and should not use the credentials (e.g., the USPTO.gov account) of the practitioner or any other individual. Each support staff must have their own account; accounts may not be shared among support staff.

Practitioner Sponsors Support Staff

1. Practitioner signs into USPTO.gov account
2. Using the Sponsorship Tool, Practitioner selects *add sponsorship(s)*.

3. Practitioner enters the email address of the support staff person's USPTO.gov account.
    a. The entered email address must belong to an existing USPTO.gov user (See section for new Practitioner Support account creation). The sponsored user cannot be in a suspended status, a Patent Practitioner, or Pro Se inventor.
    b. If the email address does not belong to a USPTO.gov account, the practitioner will receive an error message and have the option to reenter the email address.
    c. The sponsoring Patent Practitioner will review and select Practitioner Support staff from the generated list of potential sponsorships.

Each sponsoring practitioner will establish a procedure for identity proofing sponsored users and maintain a record of that procedure. Each sponsored user must present acceptable evidence of their identity. A notary public or other identity verification service may be used by the practitioner in the process to validate the evidence of the user's identity; however, the ultimate responsibility for verification of the identity of a sponsored user rests upon the sponsoring practitioner. Verification may be performed either in-person or remotely. For further details, please refer to Verification Policy Section of this document.

In the Sponsorship tool, the practitioner selects a checkbox to certify the following:

> By sponsoring users, you acknowledge and agree to the following: The indicated Practitioner Support account(s) will be authorized in a support capacity, to all customer numbers and application information associated with your account, and you grant access through the practitioner support person's own account, to work under your direction and control in the patent electronic filing and viewing system. You are responsible under 37 CFR 11.18 for any actions that are taken under your authority by the practitioner support person using the sponsored practitioner support account. You have read and understand the Subscriber Agreement, and agree to abide by the Subscriber Agreement and the rules and policies of the USPTO regarding the Subscriber Agreement.

The Sponsoring Practitioner confirms that they want to proceed. The sponsorship is established and the support staff will have access to the customer numbers that are associated to the sponsoring practitioner.

New Practitioner Support Access to EFS-Web and Private PAIR

1. Create a USPTO.gov account in MyUSPTO and opt into two-step authentication
2. Ask the practitioner to sponsor. Prove identity to practitioner in accordance with NIST guidelines.
    a. If the practitioner sponsors the practitioner support staff individual, the user will have access to all customer numbers associated to the practitioner.
3. Support Staff are able to file and access private data in the Patent Electronic System

Removing Sponsorships

Sponsorships may be removed by either the practitioner or the support staff

Proofed Practitioner Removes Sponsorship

1. Using the Sponsorship Tool, the practitioner removes the sponsorship of the practitioner support staff individual.
2. A warning message appears to the practitioner:
   *Are you sure you want to stop sponsoring **[Practitioner Support Account]**? Once removed, **[Practitioner Support Account]** will not be able to work on your behalf.*
3. After practitioner confirms the removal, the practitioner support staff individual will no longer have access to any customer numbers associated to the practitioner's account.

Practitioner Support Removes Sponsorship

1. Using the Sponsorship Tool, the practitioner support staff individual removes the sponsorship of the practitioner support staff individual.
2. A warning message appears to the user
3. After the practitioner support staff individual confirms the removal, the practitioner support staff individual will no longer have access to any customer numbers associated to the practitioner's account. The practitioner support staff individual may no longer access the Patent Electronic System if no other sponsorships exists.

USPTO Removes Sponsorship

1. USPTO has the ability to remove access for any accounts (Practitioner, Practitioner Support, Independent Inventor) by marking the account as suspended.
   a. Suspended accounts do not have access to EFS-Web Registered, Private PAIR, and Patent Center for Registered users.
   b. Practitioner support staff do not have access to the accounts of sponsoring Practitioners who have been suspended.

Verification Policy

Each practitioner will be responsible for verifying the identity of the person using any sponsored support staff account. The sole objective of the identity proofing is to ensure the user of the sponsored support staff account is who they claim to be. The two-step identification provided by the USPTO.gov account and one-time authentication code provides assurance that the user is the owner of that account; however, it is not designed to verify the real-world identity of that user. Verification of the real-world identity of sponsored support staff is the responsibility of the sponsoring practitioner.

The identity verification requirements for accessing USPTO systems are designed in view of the Digital Identity Guidelines created by the National Institute of Standards and Technology for use by government agencies in fulfilling the requirements of the Federal Information Security Management Act of 2002 (FISMA).

Each sponsoring practitioner will establish a procedure for identity proofing sponsored support staff and maintain a record of that procedure. Each sponsored support staff must present acceptable evidence of their identity. A notary public or other identity verification service may be used by the practitioner in the process to validate the evidence of the support staff's identity; however, the ultimate responsibility for verification of the identity of a sponsored support staff rests upon the sponsoring practitioner. Verification may be performed either in-person or remotely.

Identity Proofing of Sponsored Support Staff

In accordance with NIST SP 800-63A (Digital Identity Requirements), the practitioner and their support staff are required to provide identity proof prior to getting access to the systems. The requirements are identified at https://pages.nist.gov/800-63-3/sp800-63a.html

The practitioner identity verification (proofing) has four expected outcomes:

1. Resolve a claimed identity to a single, unique identity within the context of the population of users the practitioner serves.
2. Validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated).
3. Validate that the claimed identity exists in the real world.
4. Verify that the claimed identity is associated with the real person supplying the identity evidence.

The general requirements for identity proofing sponsored support staff are as follows:

1. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.
2. Collection of personally identifiable information (PII) SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the support staff providing identity evidence for appropriate identity resolution, validation, and verification. This MAY include attributes that correlate identity evidence to authoritative sources and to provide Relying Party (RP) with attributes used to make authorization decisions.
3. The practitioner SHALL provide explicit notice to the support staff at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.
4. If practitioner process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, practitioner SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing. Measures MAY include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes. When practitioner use consent measures, practitioner SHALL NOT make consent for the additional processing a condition of the identity service.
5. The practitioner SHALL provide mechanisms for redress of support staff complaints or problems arising from the identity proofing. These mechanisms SHALL be easy for support staff to find and use. The practitioner SHALL assess the mechanisms for their efficacy in achieving resolution of complaints or problems.

6. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or standard operating procedures that specifies the particular steps taken to verify identities. The standard operating procedures SHALL include control information detailing how the practitioner handles proofing errors that result in a support staff not being successfully enrolled. For example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud counter-measures when anomalies are detected.
1. The practitioner SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the support staff and SHALL record the types of identity evidence presented in the proofing process. The practitioner SHALL conduct a risk management process, including assessments of privacy and security risks to determine:
    a. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;
    b. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the practitioner will maintain as a record of identity proofing (Note: specific federal requirements may apply); and
    c. The schedule of retention for these records (Note: practitioner may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).
2. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.
3. The entire proofing transaction, including transactions that involve a third party, SHALL occur over an authenticated protected channel.
4. The practitioner SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., inspecting geolocation, examining the device characteristics of the applicant, evaluating behavioral characteristics, checking vital statistic repositories such as the Death Master File [DMF], so long as any additional mitigations do not substitute for the mandatory requirements contained herein. In the event the practitioner uses fraud mitigation measures, the practitioner SHALL conduct a privacy risk assessment for these mitigation measures. Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement (item #7) above.
5. In the event a practitioner ceases to conduct identity proofing and enrollment processes, the practitioner SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.
6. The practitioner SHOULD NOT collect the Social Security Number (SSN) unless it is necessary for performing identity resolution, and identity resolution cannot be accomplished by collection of another attribute or combination of attributes.

Practitioner may identity proof either remote or in-person using documents that establish both identity and employment authorization from Lists A, B and C.

IST A Documents that Establish Both Identity and Employment Authorization	OR	LIST B Documents that Establish Establish Identity Authorization	LIST C Documents that Employment
1. U.S. Passport or U.S. Passport Card		1. Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address	**1.** A Social Security Account Number card, unless the card includes one of the following restrictions: (1) NOT VALID FOR EMPLOYMENT (2) VALID FOR WORK ONLY WITH INS AUTHORIZATION (3) VALID FOR WORK ONLY WITH DHS AUTHORIZATION
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)			
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa		2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address	
4. Employment Authorization Document that contains a photograph (Form I-766)			2. Certification of report of birth issued by the Department of State (Forms DS-1350, FS-545, FS-240)
5. For a nonimmigrant alien authorized to work for a specific employer because of his or her status: **a.** Foreign passport; and **b.** Form I-94 or Form I-94A that has the following: (1) The same name as the passport; and (2) An endorsement of the alien's nonimmigrant status as long as that period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form.		3. School ID card with a photograph	3. Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
		4. Voter's registration card	
		5. U.S. Military card or draft record	
		6. Military dependent's ID card	
		7. U.S. Coast Guard Merchant Mariner Card	4. Native American tribal
			5. U.S. Citizen ID Card (Form I-197)
		8. Native American tribal document	6. Identification Card for Use of Resident Citizen in the United States (Form I-179)
		9. Driver's license issued by a Canadian government authority	
		For persons under age 18 who are unable to present a document listed above:	7. Employment authorization document issued by the Department of Homeland Security
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form		10. School record or report card	
		11. Clinic, doctor, or hospital record	

I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI		12. Day-care or nursery school record	