Trademark Filing System Access Document

(Updated January 2024)

The **Trademark Filing System Access Document** serves as a source document for additional information on the components for accessing Trademark filing systems, including the Trademark Electronic Application System (TEAS), TEAS International (TEASi), and Trademark Center. This document has three components:

1) Authentication process
2) Verification policy and identity proofing of U.S.-licensed attorneys, recognized Canadian attorneys/agents, trademark owners, and attorney support staff
3) Identity proofing process of all users

Authentication process

USPTO.gov accounts and MyUSPTO

Trademark filing systems use 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 an 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 (https://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 a two-step authentication. When the 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 user can select delivery of the temporary authentication code either by email, mobile code generator app, or a phone call.

When signing in with the two-step authentication, the user can select a checkbox to indicate that the device being used is a trusted device for that account. If the user selects that the device is trusted, the user will not be presented with a two-step challenge for the next 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 TEAS 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 roles are assigned by the USPTO as part of the verification process. Users can only have one of the below Trademark roles applied to their USPTO.gov account.

U.S.-licensed attorney	A U.S.-licensed attorney who has been verified by the USPTO's proofing process.
Canadian attorney/agent	A Canadian trademark attorney/agent who is reciprocally recognized by the USPTO and who has been verified by the USPTO's proofing process.
Attorney support staff	A paralegal/attorney support staff who has been sponsored by a U.S.-licensed attorney or Canadian attorney/agent.
Owner	An individual or juristic entity who owns a trademark, including individuals who are directly employed by the owner.

Please note that other systems may have roles that can be applied to a USPTO.gov account in addition to one of the above Trademark filing roles. For example, a U.S.-licensed patent attorney may have a patent practitioner role in the Patent electronic system, and a trademark attorney role in the Trademark filing system.

Revocation of accounts

In some cases, accounts may be revoked. Revoked accounts cannot access trademark filing systems. The USPTO may revoke 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 their own account data, which is non-public. Verified attorneys can sponsor attorney support staff. A sponsored support staff individual will be authorized to act on behalf of the sponsoring attorney to the extent allowed by law.

Authentication steps

In order to use a USPTO.gov account with trademark filing systems, 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 Trademark filing 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. For the USPTO.gov accounts of attorneys, owners, and attorney support staff the account holder's identity must be proven by completing the Trademark filing system verification process. The steps for the proofing process are located at the "Trademarks identity verification" page at https://www.uspto.gov/trademarks/apply/identity-verification. Attorney support staff must be sponsored by a verified attorney in order to work on behalf of the sponsoring attorney.
    a. When the proofing process is completed by the USPTO, a Trademark filing system role will be assigned to the USPTO.gov account.
    b. Verified user accounts cannot opt out of two-step authentication.
    c. Verified user accounts cannot change email addresses outside of the proofing process. In order to change the name or email address of the proofed user account, a new notarized form is required.
4. Go to the Trademark filing system.
5. Sign in.
    a. The user can sign in from the Trademark filing 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.
6. Sign out.
    a. A signed-in user can sign out at any time on any page in the Trademark filing system or in MyUSPTO.
    b. The Trademark filing system will automatically terminate a user's session after 30 minutes of inactivity. The user will be prompted to continue their session prior to the inactivity timeout.
    c. A user that has signed out immediately loses access to all data entered in a form.

USPTO removes access

The USPTO has the ability to remove access for any accounts (U.S.-licensed attorney, Canadian attorney/agent, Attorney support staff, or Owner) by marking the account as revoked. Revoked accounts do not have access to trademark filing systems.

Verification policy and identity proofing of U.S.-licensed attorneys, recognized Canadian attorneys/agents, trademark owners, and attorney support staff

Each U.S.-licensed attorney, recognized Canadian attorney/agent, trademark owner, and attorney support staff is required to undergo an identity proofing and enrollment "process whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified. The steps for the verification process are located at the "Identity verification for trademark filers" page at https://www.uspto.gov/trademarks/apply/identity-verification.

Patent practitioners and independent inventors who are currently Patent proofed will be considered to have met the identity proofing requirements.

Appendix A: example of an acceptable identity proofing process

The following example is based on the Digital Identity Guidelines, NIST SP 800-63A, section 4.1, as a sample of the interactions during the identity proofing process. The term "CSP" refers to "credential service provider."

1. **Resolution**
    a. The CSP collects PII from the applicant, such as name, address, date of birth, email, and phone number.
    b. The CSP also collects two forms of identity evidence, such as a driver's license and a passport. For example, using the camera of a laptop, the CSP can capture a photo of both sides of both pieces of identity evidence.
2. **Validation**
    a. The CSP validates the information supplied in 1a by checking an authoritative source. The CSP determines the information supplied by the applicant matches their records.
    b. The CSP checks the images of the license and the passport, determines there are no alterations, the data encoded in the QR codes matches the plain-text information, the identification numbers follow standard formats, and that the physical and digital security features are valid.
    c. The CSP queries the issuing sources for the license and passport and validates the information matches.
3. **Verification**
    a. The CSP asks the applicant to take a photo of themselves, with liveness checks, to match the license and passport.
    b. The CSP matches the pictures on the license and the passport to the applicant picture and determines they match.
    c. The CSP sends an enrollment code to the validated phone number of the applicant, the user provides the enrollment code to the CSP, and the CSP confirms they match, verifying the user is in possession and control of the validated phone number.
    d. The applicant has been successfully proofed.

Note: The identity proofing process can be delivered by multiple service providers. It is possible, but not expected, that a single organization, process, technique, or technology will fulfill these process steps.