

# System Account User Guide

Version 3.01

## Document Control: Version History

Version ID	Date	Description of Changes	Authored By
1.0		Original published draft	Integrated Award Environment
2.0	Feb 2021	Updates to guidance	Integrated Award Environment, Office of Stakeholder Engagement
3.0	Nov 2021	Extensive revisions based on user feedback. New tools for users to prepare to apply for and to manage API connections. New glossary of terminology.	Integrated Award Environment, Office of Stakeholder Engagement
3.01	Jan 2022	Updates to include how to manage system account deactivation	Integrated Award Environment, Office of Stakeholder Engagement

## Table of Contents

### [How to Use this Guide](#)

### [Overview of System Accounts, Individual Accounts, and API Keys](#)

[What's the difference between an individual account and system accounts?](#)

[Which type do I need?](#)

[What else do I need to know before I make a request for a system account or get an individual account API key?](#)

[Type of Connections and Rate Limits](#)

[Interface Specifications \(for system accounts only\)](#)

[Permissions for Data Access \(for system accounts only\)](#)

### [Individual Account API Key](#)

[Getting an Individual Account API Key](#)

[Accessing the Workspace](#)

[Requesting an Individual Account API Key \(Public API Key\)](#)

[Managing an Individual Account API Key](#)

[Individual Account API Key Security and Viewing](#)

[Individual Account API Key Rotations](#)

[API Key Rotation Tips for Individual Accounts](#)

[Removing an Individual Account API Key](#)

### [System Accounts, System Account Passwords, and System Account API Keys](#)

[Requesting Federal System Accounts](#)

[Accessing the System Account Workspace](#)

[Requesting a System Account Role](#)

[Viewing System Accounts in Your Workspace](#)

[Requesting a New System Account](#)

[Reviewing Status](#)

[Requesting Non-Federal System Accounts](#)

[Accessing the System Account Workspace](#)

[View Available System Accounts](#)

[Requesting a New System Account](#)

[Reviewing Status](#)

[Managing System Accounts](#)

[About System Account Passwords](#)

[Getting a System Account Password](#)

[Resetting a System Account Password](#)

[About System Account API Keys](#)

[Getting a System Account API Key](#)

[System Account API Key Rotation](#)

[API Key Rotation Tips for System Accounts](#)

[Other System Account Management Tasks](#)

[Editing System Accounts](#)

[Requesting a Rate Increase](#)

[Renewing System Accounts](#)

[System Account Deactivation](#)

[For More Help](#)

[Help Resources](#)

[Troubleshooting](#)

[Appendix A: Domain roles and permissions](#)

[Appendix B: Account Request Preparation Checklist](#)

[Appendix C: Account Management Checklist](#)

[Appendix D: Glossary of Terminology](#)

## How to Use this Guide

The purpose of this guide is to provide information to users of individual accounts and systems accounts that access SAM.gov information via Application Programming Interface (API).

Throughout this guide, you'll see a few options to help you get the most out of this information.

- *Italicized words or phrases* indicate important terminology. You can find a definition in the text or in a glossary at the end of this document.
- A stopwatch icon (⌚) tells you how you can take a shortcut to another part of the guide or skip to other information.
- Links to other resources, such as Frequently Asked Questions (FAQs) and websites, are included where applicable.
- Helpful tools and checklists in the appendices help you prepare for and manage your individual account API Key or system account and system account API key.

## Overview of System Accounts, Individual Accounts, and API Keys

System accounts and individual accounts are two options for connecting to SAM.gov for data transactions on a repeated basis. You need keys, called *system account API keys* or *individual account API keys*, to access these connections depending on the type of connection you select.

### What's the difference between an individual account and system accounts?

Individual Account	Non-Federal System Account	Federal System Account
<ul style="list-style-type: none"> <li>→ For individual users; this is the same as your SAM.gov user account.</li> <li>→ Access to an Application Programming Interface (API) to view public data. Can be accessed by both federal and non federal SAM.gov users.</li> <li>→ Allows you to systematically pull detailed information from SAM.gov using different parameters.</li> <li>→ Recommended if you need to request real-time, limited public data through a Representative State Transfer (REST) API service.</li> <li>→ Features: <ul style="list-style-type: none"> <li>○ Contains your own personal information</li> <li>○ May stay with you even when your role in your organization or the permissions you need to do your job change (as long as</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>→ For systems to use; must be requested</li> <li>→ An account for systems not managed by the federal government that need to connect via REST API.</li> <li>→ Allows you to systematically pull detailed information from SAM.gov using different parameters.</li> <li>→ Recommended if you request frequent or large amounts of public data through a REST API service.</li> <li>→ Features: <ul style="list-style-type: none"> <li>○ Represents a particular information technology (IT) system</li> <li>○ Is primarily for systems that need to automate the pull of data through extracts or web services</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>→ For systems to use; must be requested</li> <li>→ An account for systems owned by the federal government that need to connect via a REST API.</li> <li>→ Allows you to systematically pull detailed information from SAM.gov using different parameters.</li> <li>→ Required to request For Official Use Only (FOUO) or Sensitive data access specifically through a REST API service.</li> <li>→ Features: <ul style="list-style-type: none"> <li>○ Represents a particular federal IT system</li> <li>○ Can request access to view sensitive data through search or extracts</li> <li>○ Is primarily for systems that need to either send data to</li> </ul> </li> </ul>

your department still allows you to access the same information if you move around within it)	<ul style="list-style-type: none"> <li>○ Is useful if multiple users in your organization need to access the same extract or web service</li> </ul>	SAM.gov (such as a contract writing system) or automate the pull of data through extracts or web services <ul style="list-style-type: none"> <li>○ Is useful if multiple users in your organization need to access the same extract or web service</li> </ul>
---	---	---

## Which type do I need?

System account API keys are for any system that needs to connect to SAM.gov for large data transactions on a repeated basis. There are two types of system accounts: federal and non-federal.

Individual account API keys are for individuals that need to connect to SAM.gov for a limited number of data transactions on a repeated basis.

You do not need either of these if you only want to download prepared *data extracts*. Any user can go directly to [SAM.gov](https://sam.gov) to initiate a search and view public data.

However, if you or your system need to connect to [SAM.gov](https://sam.gov) information regularly and repeatedly, an individual account API key or system account API key may be your best option. Please note that there is some data available via API that is not available in data extracts (e.g. federal hierarchy or PSCs and location services).

As described above, everyone with a SAM.gov account can get individual-level API access. You just need to request an individual account API key to do this. If you need to connect through a system, you will need to specifically request a system account, and you will need to get and use a system account API key to access APIs for data.

🕒 For more information about how to use data extracts, view this [video](#).  
To learn more about system accounts and APIs, continue with this guide.

## What else do I need to know before I make a request for a system account or get an individual account API key?

Consider:

- [The type of connection and rate limit you need](#)
- [Interface specifications](#)
- [Permissions for data access](#)

🕒 If you are confident you have the information you need to make the request that best suits you, you can skip to the instructions for making your [individual account API key](#) or [system account](#) request.

## Type of Connections and Rate Limits

A *connection* refers to sending and receiving HTTP requests or responses for data. A *rate limit* is the number of allowed new connections in a specific timeframe (e.g. per second, minute, hour, day).

To better understand whether you need to use an individual account or a system account to access data, consider the number and type of connections you need:

Any user can request an individual account API key from their profile page. This API key can be used to get, or *pull*, public data from SAM.gov with a limited number of requests per day (see the table below).

If you need more connections for more people, request a system account. This requires additional steps and validations to get increased request volume and data access.

Keep in mind that a user with a system account is allowed to have one system account API key and one individual account API key. A user with only an individual account (non-system) may only have one individual account API key.

Connecting Source	Type of Connection	Default Rate Limit
Non-federal individual user not associated with an entity	Individual account API key	10 requests/day
Non-federal individual user associated with an entity	Individual account API key	1,000 requests/day
Federal individual user	Individual account API key	1,000 requests/day
Non-federal system	System account API key	5,000 requests/day
Federal system	System account API key	10,000 requests/day

**The rate limits listed are set by default.** Only those with a federal system account can request an [API key rate limit increase](#). These exception requests are handled on a case

by case basis, based on business justification, and may be revoked if it's determined the exceptions are putting a strain on Integrated Award Environment (IAE) systems or are not being used to the degree requested.

### Interface Specifications (for system accounts only)

Before requesting a system account, please review the *specifications* and requirements for any connection you need. Specifications include: access controls, send and response parameters, format, and any specific system requirements. All request and response details for the *REST* APIs are documented on [open.gsa.gov](https://open.gsa.gov).

### Permissions for Data Access (for system accounts only)

If you decide that you need a system account, establish what data you have a business reason to access, and what actions you will take with the information (read or write).

- If you are just pulling data, or using *GET* calls, then you will only need *read permissions* for the data (federal and non-federal users).
- If you are writing, sending, or using *POST* and *PUT* calls, then you will need *write permissions* (federal users only).
- Be aware that only federal accounts can access *For Official Use Only (FOUO)* or *Sensitive* data permissions, and only federal accounts are allowed to write data. Non-federal users can only select the *public* read permissions when submitting a system account request.

**Find your type of account on the table below to see what kind of access you can request.**

Type of Account	Read Permissions Allowed	Write Permissions Allowed
Non-federal system accounts	Yes; Public Read permissions for GET calls	No
Federal system accounts	Yes; Public Read and FOUO/Sensitive Data GET calls	Yes; Public Write and FOUO/Sensitive Data POST or PUT calls.

When you request a system account, you will be presented with a list of the SAM.gov *domains* you can get information from. Each domain represents a data set and has *permissions* specific to the domain. Knowing which domains and permissions you need will help you complete your request quickly and accurately.

🕒 Review the data sets and permissions allowed for each domain in [Appendix A](#) of this guide.

If you're interested in getting an individual account API key on your individual account, follow the steps in [Getting an Individual Account API Key](#), below.

⌚ If you will only use data through the website, or *front end*, then you do not need an individual account API key and can use data extracts and reports instead. If you plan to connect via a system account, you will need a system account API key. To proceed to instructions for requesting a system account, [skip to that section](#) now.

Remember, you can have both an individual account API key and a system account with system account API key.



## Individual Account API Key

On SAM.gov, an individual account API key is referred to as a *public API key*. These terms are interchangeable and you may see both terms used on the website and in this guide. The term *public* refers to the type of data—public data—you can view with an individual account API key.

You can use the [Account Request Preparation Checklist](#) at the end of this guide to help as you gather the information necessary to complete this process. There are two steps for getting an individual account API key.



## Getting an Individual Account API Key

### Accessing the Workspace

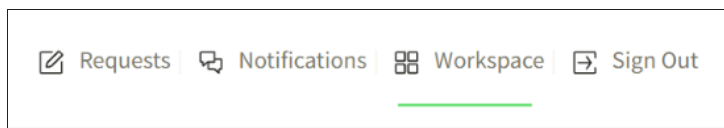


Before you can request an individual account API key, you must have a SAM.gov user account (individual account). Select “Sign In” on the header of any SAM.gov page, and complete the account form. If you already have a user account, you can skip this step, sign in using your existing account, and continue with the next instructions.

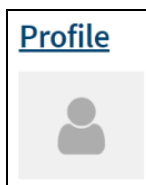
After you have an individual SAM.gov user account, you will have access to the *Workspace* where you can manage specific data or items.

You can request your individual account API key from your Profile page within the Workspace:

1. Sign into SAM.gov.
2. Your Workspace page will be displayed. If you are on another page, navigate to Workspace using the Workspace link at the top of any page.



3. On your Workspace, select the “Profile” label to display your account details page.



### Requesting an Individual Account API Key (Public API Key)



1. On your Account Details page, navigate to the section titled Public API Key (Remember: public API key and individual account API key are the same thing).
2. Select Request API Key.

#### Public API Key

Only request an API key if your profile will individually access data from this site via an API. If you are just entering through the web interface or from an agency system, then you do not need an API key. If you remove the API key from your profile, you must wait 24 hours before you can request a new API key.

Request API Key



**You now have access to an individual account API key.** You can use it to complete a limited number of calls through the site interface connections documented on [open.gsa.gov](https://open.gsa.gov) and the [table in this guide](#).

This concludes the information about requesting an individual account API Key. Continue to the next section to learn about managing your individual account API key.

### Managing an Individual Account API Key

You'll need to take action periodically to manage your individual account API key. Managing your key properly will help ensure you can use it to access information on an ongoing basis. The following topics will help you manage your individual account API key:

- [Individual Account API Key Security and Viewing](#)

- [Individual Account API Key Rotations](#)
- [Individual Account API Key Rotation Tips](#)
- [Removing an Individual Account API key](#)

### Individual Account API Key Security and Viewing

After your initial API key request, for security purposes, the API key will be hidden. Ongoing, you will need to unhide and view it on this page so that you can use it to access APIs, retrieve [rotated API keys](#), etc. Read on for steps to unhide your API key.

Here's how you can view it:



1. Select the eye icon to view your API key. A one-time password will be sent to the email address on the account for your individual account.

### Public API Key

Only request an API key if your profile will individually access data from this site via an API. If you are just entering through the web interface or from an agency system, then you do not need an API key. If you remove the API key from your profile, you must wait 24 hours before you can request a new API key.

Expires in 89 days

\*\*\*\*\*



Remove API Key

2. Retrieve the password from your email and enter it into the Enter One-time Password field in the pop up on the Public API Key section of your Account Details page.

### Enter One-time Password

Please enter your one-time password to see the API keys

Submit

[Send new code](#)

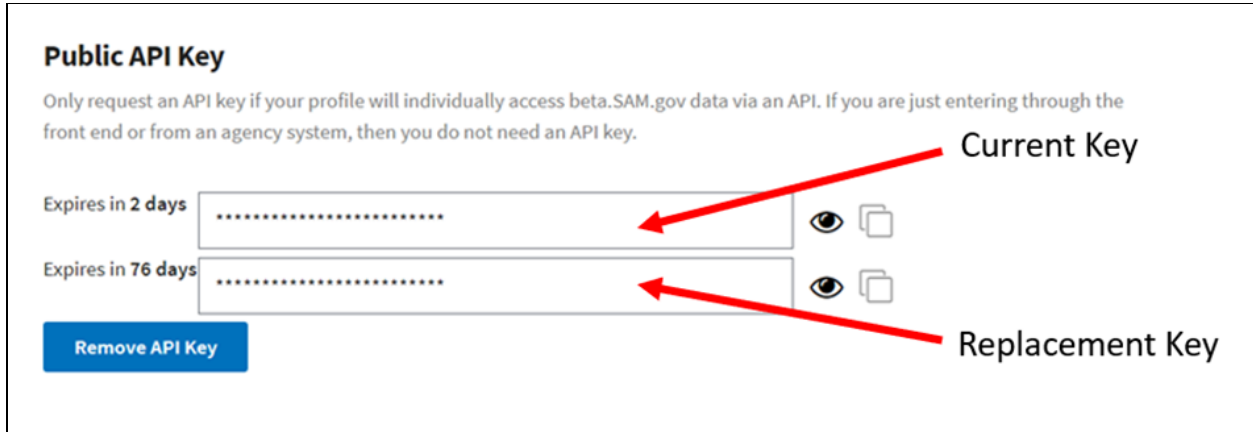
3. Select Submit to view the Individual Account API key.

Your API key will display in the Public API Key section. **You can use this process anytime you need to view your individual account API key.**

### Individual Account API Key Rotations



For security reasons, individual account API keys must *rotate* every 90 days. A new key will be *auto-generated* for you before the current key is out of date. Here's what happens:



1. You will receive a series of email notifications starting 15 days prior to when the current key will be out of date, notifying you of the upcoming need for rotation. *Always read all emails about your individual account API key so you do not miss important messages!*
2. 15 days before your current key is out of date, a replacement API key will auto-generate and display in the Public API Key section of your Profile page, below the current key.



**Public API Key**

Only request an API key if your profile will individually access beta.SAM.gov data via an API. If you are just entering through the front end or from an agency system, then you do not need an API key.

Expires in 2 days .....  

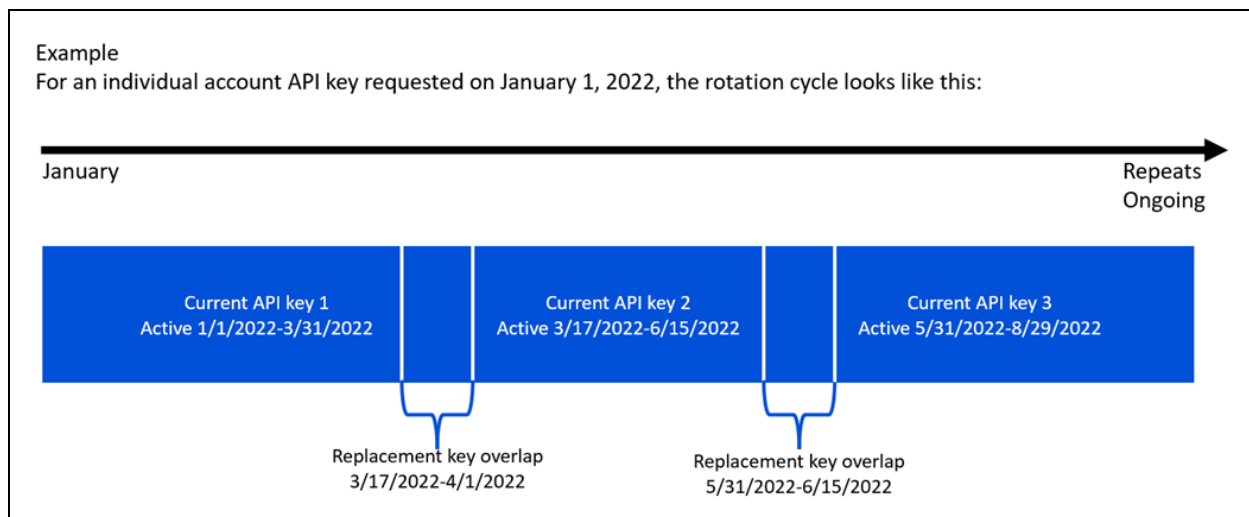
Expires in 76 days .....  

[Remove API Key](#)

You can tell the current key from the replacement key by the **number of days indicated** until expiration. The one with fewer days is the current key—the one you've been using. The one with more days—the replacement key—is the key that will rotate in when the current key is out of date.

3. Retrieve and begin to use your replacement individual account API key as soon as possible after it is auto-generated. Both the replacement and current key will be active (you can use either) during the 15-day window before the current key is out of date.
4. The current key will go out of date at midnight at the end of the 14th day, and the replacement key will become the current key. Only the new, current key will be visible after the rotation has occurred (this cycle repeats for the life of your individual account or until you remove the individual account API key).

**Below is an example of a timeline for individual account API key rotation.** Your rotation cycle will start on whatever date you request your individual account API key.



## API Key Rotation Tips for Individual Accounts

- **You do not need to do anything to request a replacement key or start the API key rotation.** The backup key is auto-generated by SAM.gov as part of the API key rotation workflow in the system.
- Your only task for API key rotations is to **view and input the key that is current** during the time period when you want to connect through an API. In order to stay up to date, you must go get the replacement key after it is auto-generated so you can use it once the current key rotates out. During the 15-day replacement period, you may use either key to connect.
- If your individual account API key becomes out of date before you have retrieved the replacement, **you can still retrieve your replacement API Key** from the “Workspace” page under “Profile” in your SAM.gov any time. The replacement key will take effect immediately.
- API key rotation will trigger a series of reminder emails to you. The purpose of these emails is to remind you to retrieve your new (replacement) key. **We advise you read each email to understand what actions you need to take, especially if you have more than one type of account with SAM.gov. You can disregard emails for individual account API key rotations once you have retrieved your replacement key.**

🕒 Look for more tips on API key rotations and find out how to get help in the [appendix](#).

**This concludes the information about individual account API key rotations.**

### Removing an Individual Account API Key

You may wish to remove your individual account API key at some point. If you have had your API for more than 24 hours, you can remove it at any time using the steps below. For security reasons, if you want to remove an individual account API key that you recently requested, you will have to wait 24 hours from when you made the API key request before you ask to remove it. You will no longer receive reminder emails about rotating your API key after you remove it. You may remove it any time you choose after that period by following these steps:

1. Go to the Public API Key section of your profile page. Select Remove API Key.

#### Public API Key

Only request an API key if your profile will individually access data from this site via an API. If you are just entering through the web interface or from an agency system, then you do not need an API key. If you remove the API key from your profile, you must wait 24 hours before you can request a new API key.

Expires in 85 days

\*\*\*\*\*



Remove API Key



2. Verify through the popup window that will display that you want to remove the API key.
  - a. When you select “Yes, remove API key”, the API key will be deactivated and can no longer be used for connecting to the site.
  - b. When you select “No, keep API key”, the popup will be dismissed and the API key will continue to be available.



#### Are you sure you wish to remove the API key?



If you remove your API key, it will be deactivated and unavailable for use. You must wait 24 hours before you can request a new API key.

No, keep API key.

Yes, remove API key.

⌚ If you are an individual account API key user who does not also use a system account, this is the end of your section of the guide.  
You can view tools and more help in the Appendix. For comprehensive FAQs, please search [fsd.gov](https://fsd.gov).

## System Accounts, System Account Passwords, and System Account API Keys

Remember, there are two types of system accounts: federal and non-federal.

As explained in the [permissions section](#) in this guide, only federal departments or independent agencies may request federal system accounts. And, only federal accounts are permitted access to FOUO or Sensitive information. Since federal systems are allowed to request access to non-public data, there are additional access controls and security approvals integrated into the request process.

You can use the [Account Request Preparation Checklist](#) at the end of this guide to help you prepare the information necessary to complete non-federal and federal system account processes.

🕒 If you only want to learn about non-federal system accounts, you can [skip to that section](#) now.  
To learn more about federal system accounts, continue.

### Requesting Federal System Accounts

You'll need to take several steps to get a system account.



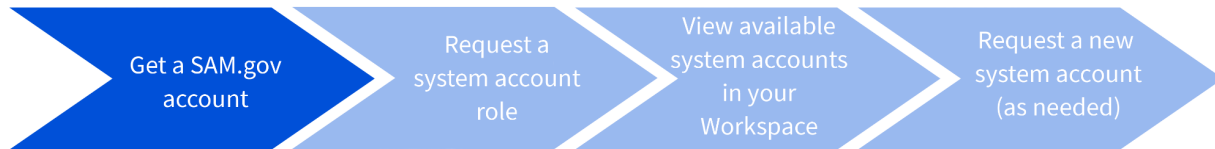
These topics will guide you through these steps:

- [Accessing the System Account Workspace](#)
- [Requesting a New System Account](#)
- [Reviewing Status](#)

🕒 If you know which topic you want to explore, you can skip to it by selecting the topic name linked to that section. If you have never requested a federal system account, we recommend starting with the first topic.



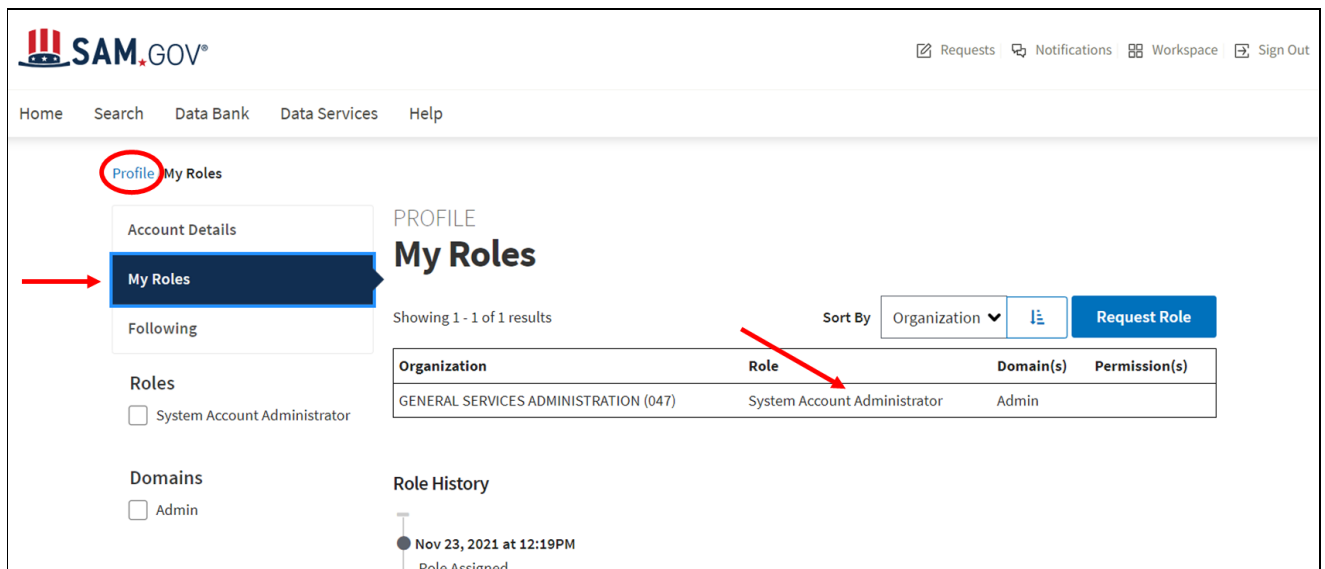
## Accessing the System Account Workspace



The first step to requesting a federal system account is to **get a SAM.gov user account** as a federal user. Select “Sign In” on the header of any page, and complete the account form using your federal government email address.

After you complete the account setup, you will have access to the *Workspace* where you can manage specific data or items. Your Workspace is tailored to you based on roles, permissions, and personal preferences.

You can view your federal roles in the Profile section of your Workspace,



The screenshot shows the SAM.GOV workspace interface. The top navigation bar includes links for Home, Search, Data Bank, Data Services, and Help. The main content area is titled 'PROFILE My Roles'. On the left, there is a sidebar with 'My Roles' highlighted. The main content area shows a table of roles with the following data:

Organization	Role	Domain(s)	Permission(s)
GENERAL SERVICES ADMINISTRATION (047)	System Account Administrator	Admin	

Below the table, there is a 'Role History' section showing a timeline of role assignments, including one on Nov 23, 2021 at 12:19PM.

## Requesting a System Account Role



As a federal user who wants to establish a system account, you must **request a system account role**. System account roles can only be granted by an agency’s system account administrator. You can check the User Directory in the SAM.gov Workspace to find your system account administrator.

The two roles you can choose from for system accounts are:

System Account Manager	System Account Administrator
<p>You can:</p> <ul style="list-style-type: none"> <li>Edit system accounts that you are responsible for</li> <li>Submit a request for a system account to be reviewed by the System Account Administrator</li> </ul> <p>You cannot:</p> <ul style="list-style-type: none"> <li>Assign or approve roles</li> </ul> <p>Your agency system administrator and GSA must approve the system account request before the system account can be created by GSA.</p> <p>The manager will receive emails about the system, including but not limited to system account renewals and API key rotation notifications.</p>	<p>You can:</p> <ul style="list-style-type: none"> <li>Submit a request for a system account to the General Services Administration (GSA) for approval</li> <li>Assign and approve roles for other people who will be managing your federal systems</li> </ul> <p>The administrator will receive emails about the system, including but not limited to system account renewals and API key rotation notifications.</p>

To request one of these roles, you must email someone in your department or agency who already has this role. Request the role directly by email, and include a description of your business need to access the information. Do not use the role request feature in your Workspace. In the event that no one at

your agency has this role, the Chief Information Officer (or similar executive) for your department or independent agency must appoint someone.

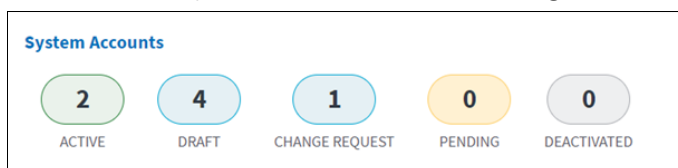
**Note:** Please do not request roles or ask about the status of a role request with the Federal Service Desk; they are only able to assist with technical issues and do not have the ability to grant you a role in SAM.gov. However, you can go to [fsd.gov](https://fsd.gov) and search the FAQs for more information about [getting and managing roles](#).

## Viewing System Accounts in Your Workspace

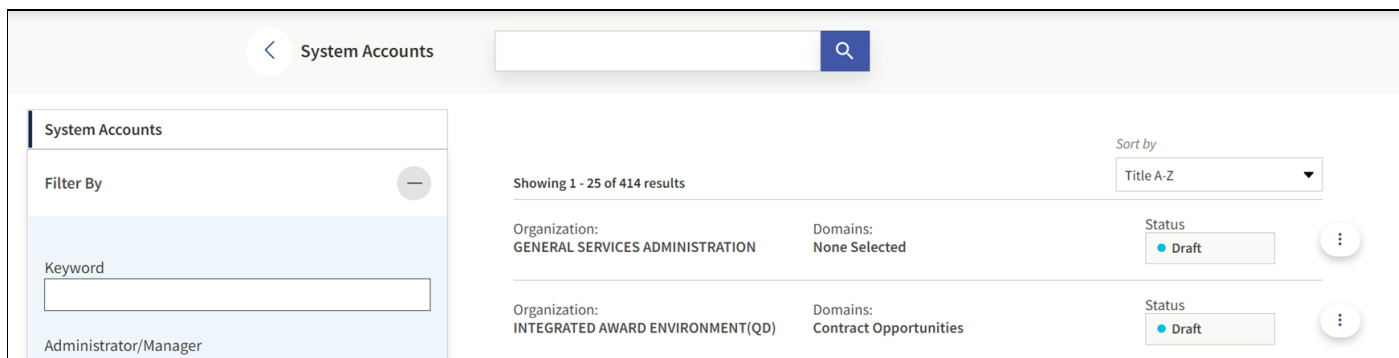


Once you have a System Account Administrator or System Account Manager role, you can **view existing system accounts available for you to access** in your Workspace. If there are other system accounts already in your federal hierarchy level, you can view and use them.

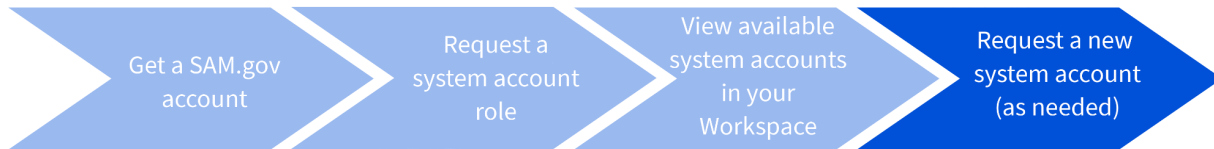
1. After you have signed in to SAM.gov, navigate to your Workspace from the header on any page.
2. Select System Accounts from the widgets to view details for your system accounts.



3. This page is known as your *Tier 2 Workspace* for System Accounts. Review this page for any system accounts to which you are already connected through your role or agency.

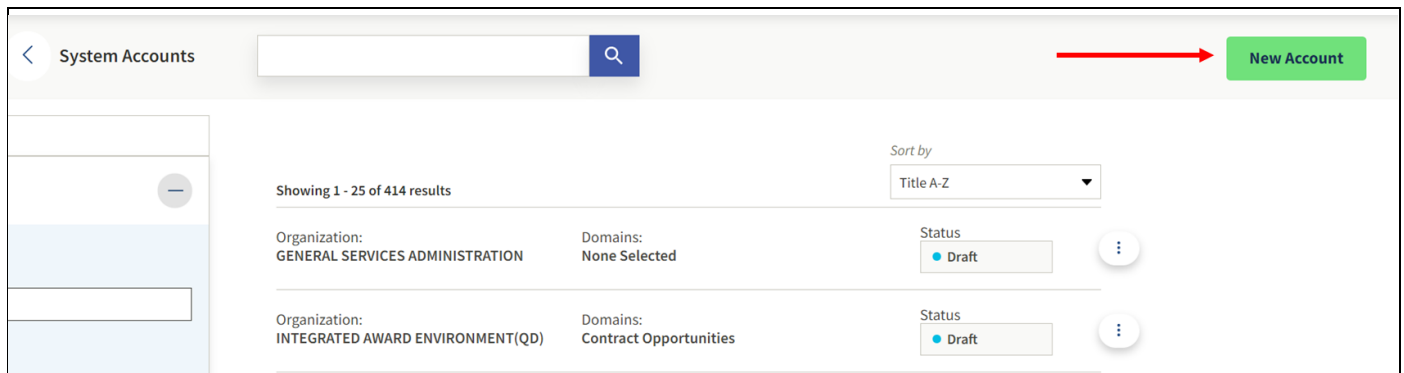


## Requesting a New System Account

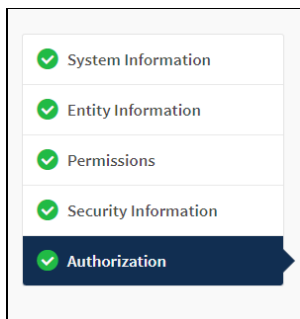


When you view the system accounts available in your Workspace, you may decide to **set up, or request, a new system account**. You can do that by following these steps:

1. From the Tier 2 System Accounts Workspace, select New Account.



On the new account request screens, you can track your progress by viewing the navigation menu.

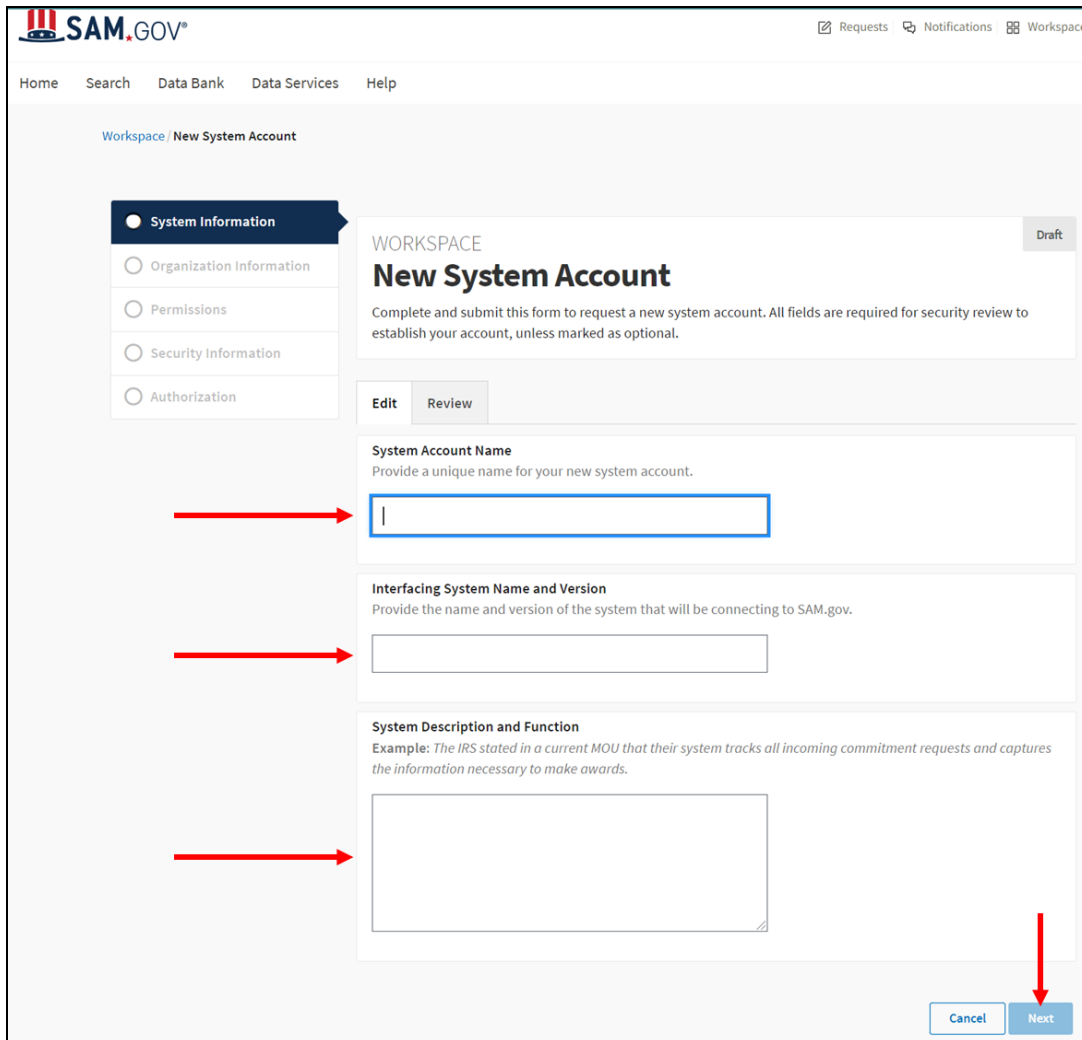


### System Information

2. Enter details for the system account you wish to establish:
  - a. *System Account Name*: Unique name that helps you and others distinguish the account from any other managed by you or others in your organization.
  - b. *Interfacing System Name and Version*: Actual full name of the connecting system and version number.

- c. *System Description and Function*: The business reason for your system connection. This includes any justification for access to non-public data and any justification for sending data to our system.
3. Select Next to continue. Red text will be displayed by any field that is incomplete or fails *validation*. Instructions let you know what to update (see an example, below). Correct the issue to continue.

Please be aware that selecting Cancel at any point in the process will delete the current edits and return you to the Tier 2 System Account Workspace.

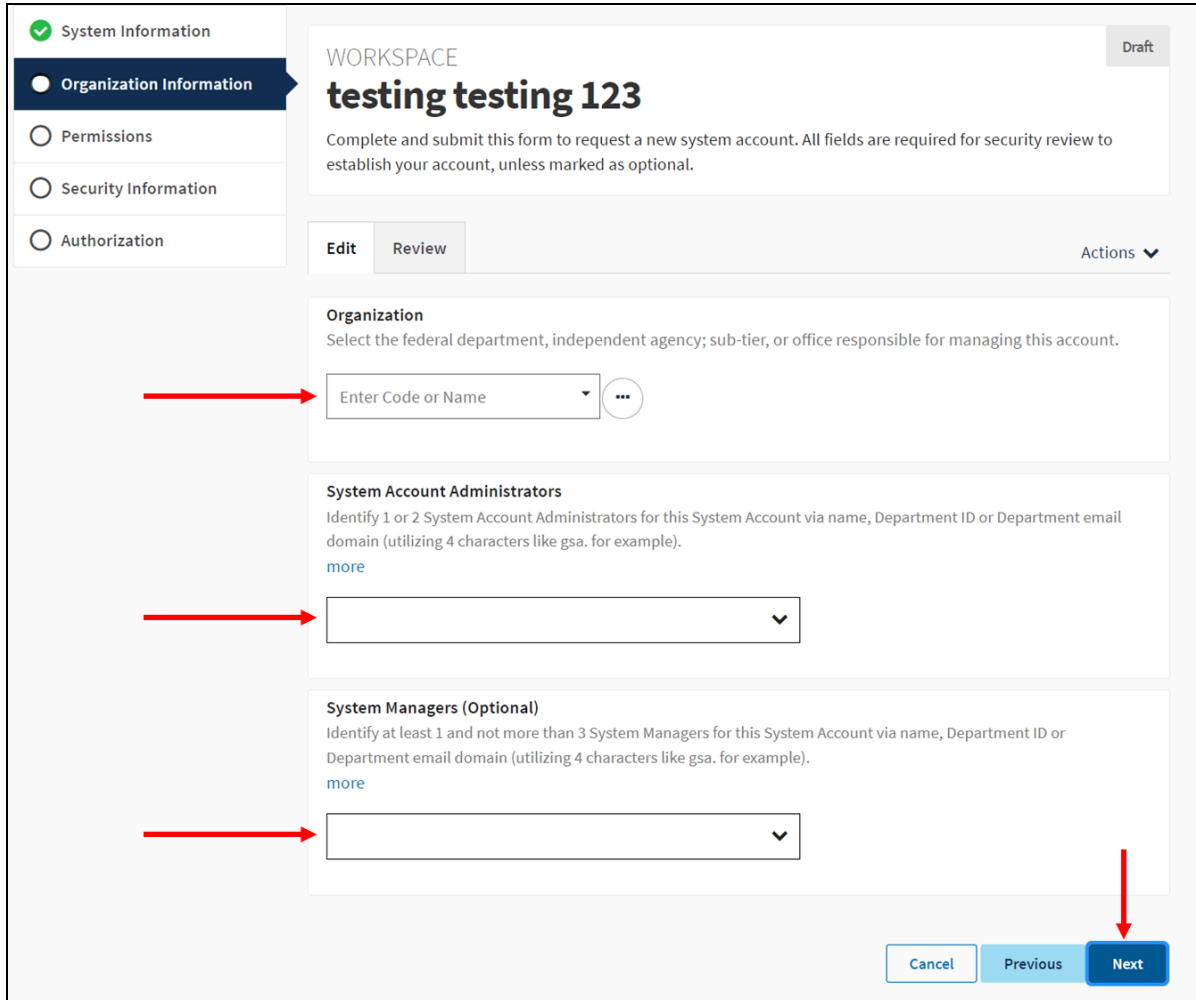


#### Organization Information

4. On the next screen enter the specific organization information for the new system account you wish to establish (see example, below):

- a. *Organization*: Required. The screen will display your organization's *hierarchy*, as permitted by your role. If your role is with a specific *sub-tier* or *office*, you will only be able to associate your account to that level. A system account administrator at a higher level will be able to manage your account and grant higher access if needed. You must enter one organization/agency, sub-tier, or office for your system account using the agency picker.
  - b. *System Account Administrators*: Required. These specific users will be listed with the account and identified as points of contact (POCs) for any communications about the system account. You will only see available administrators within your agency who have the system account administrator role already. Choose administrators from the list. We recommend organizations list at least two administrators so that there can be a backup. If you don't know the system account administrator, use the User Directory to locate one in your agency. This step must be completed in order for administrators to address your new system account request.
  - c. *System Account Managers*: Optional. Users you include here will be listed with the account and identified as points of contact (POCs) for any communications about the system account. We recommend organizations list at least two managers.
5. When all fields are complete, select Next to continue. If you need to return to the previous section, select the item from the table of contents or the Previous link at the end of the page. To delete the draft in progress and return to the Tier 2 Workspace page, select the Actions drop

down and then select Delete.



## Permissions

6. On the next screen (see example, below), select the specific permissions for the system account you wish to establish:
  - a. In advance, review [Permissions for Data Access](#) and [Appendix A](#) to identify the specific permission requirements for your system. If you do not properly justify the permission you are requesting, the account request will be rejected.
  - b. Review the Terms of Use before you submit your account request. View the Terms of Use on this screen by selecting Terms of Use. A popup window will display the full text.
  - c. Select the correct overall [Federal Information Processing Standard](#) (FIPS) categorization from the drop down menu.
7. When all fields are complete, select Next to continue. If you need to return to the previous section, select the item from the table of contents or the Previous link at the end of the page.

System Information

Organization Information

Permissions

Security Information

Authorization

WORKSPACE

Draft

testing testing 123

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit

Review

Actions

What do you need?

Terms of use

Contract Opportunities

☒ Read Public
 ☐ Read Sensitive
 ☐ Write Public
 ☐ Write Sensitive

Contract Data

☐ Read Public
 ☒ Write Public
 ☐ Read DoD Data
 ☐ Write DoD Data

Entity Information

☐ Read Public
 ☐ Read FOUO
 ☐ Read Sensitive

Federal Hierarchy

☐ Read Public Only
 ☐ Read FOUO

Assistance Listings

☐ Read Public

Wage Determinations

☐ Read Public

Reference Data

☐ Read Public

Overall FIPS 199 Categorization

Cancel

Previous

Next

*What do the white and gray checkboxes mean?*

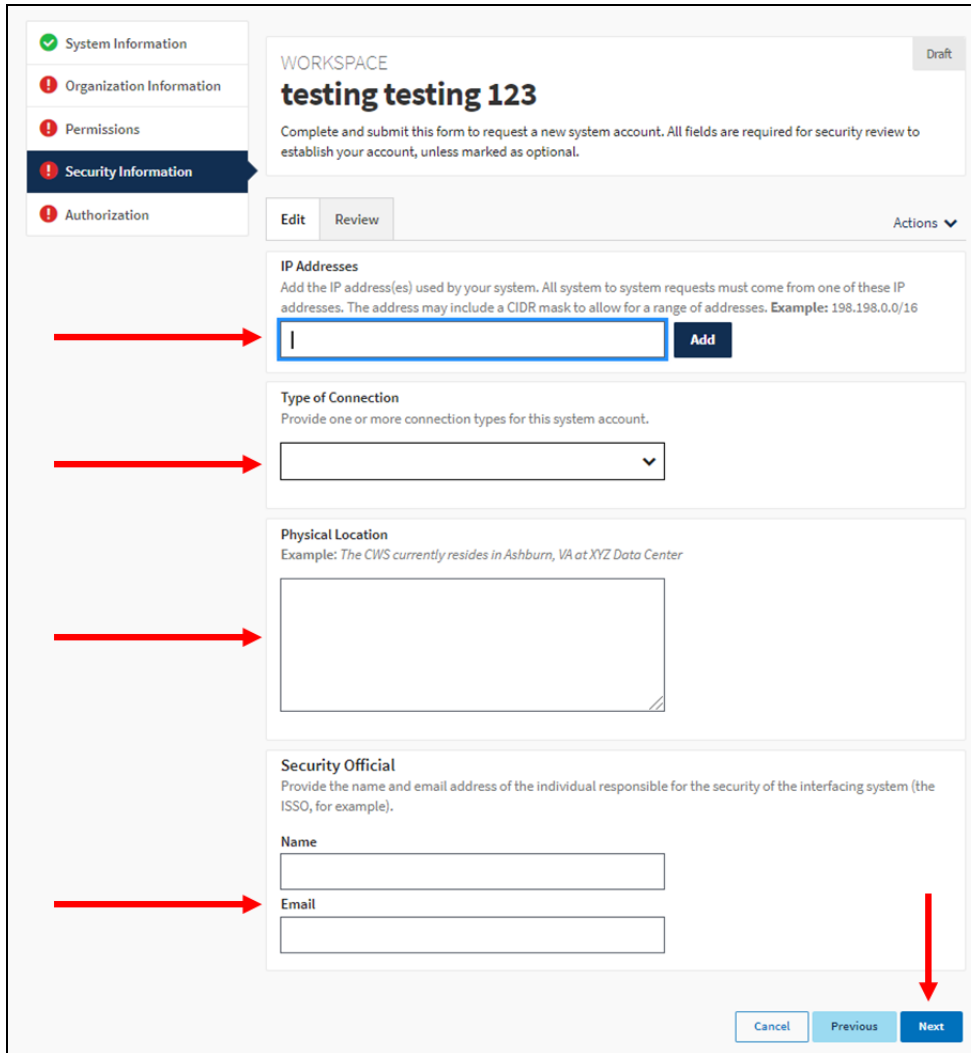
White boxes indicate permissions that are available to choose in the domain they are listed under.

Gray boxes indicate permissions that are not available to choose in the domain they are listed under.



## Security Information

8. On the next screen (see example, below), enter the specific security information for the system account you wish to establish:
  - a. IP Address: This should be the specific Internet Protocol (IP) address or addresses for the connecting system. If the IP is masked by Classless Inter-Domain Routing (CIDR), enter the range here.
  - b. Type of Connection: Select any connection the system will use, such as REST API.
  - c. Physical Location: Specify the primary physical location of the system.
  - d. Security Official: Enter contact information for your agency Information System Security Officer (ISSO) or other security personnel. Do NOT input the information for the GSA security reviewer.
9. When all fields are complete, select Next to continue. If you need to return to the previous section, select the item from the table of contents or the Previous link at the end of the page.



**System Information** (checked)  
**Organization Information** (warning)  
**Permissions** (warning)  
**Security Information** (warning) (selected)  
**Authorization** (warning)

**WORKSPACE** Draft  
**testing testing 123**  
 Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit Review Actions ▼

**IP Addresses**  
 Add the IP address(es) used by your system. All system to system requests must come from one of these IP addresses. The address may include a CIDR mask to allow for a range of addresses. **Example:** 198.198.0.0/16

Add

**Type of Connection**  
 Provide one or more connection types for this system account.

**Physical Location**  
 Example: The CWS currently resides in Ashburn, VA at XYZ Data Center

**Security Official**  
 Provide the name and email address of the individual responsible for the security of the interfacing system (the ISSO, for example).

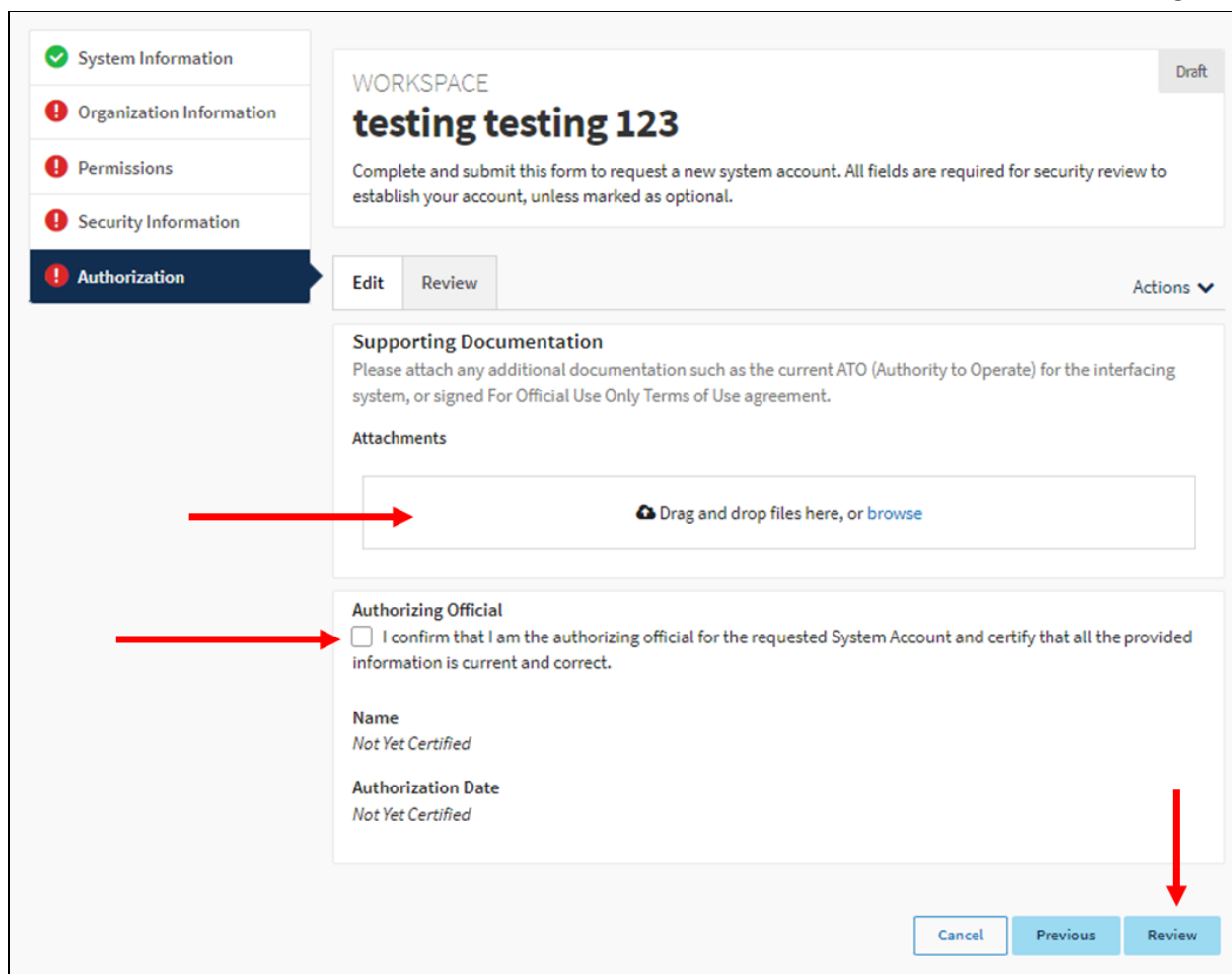
Name

Email

Cancel Previous **Next**

## Authorization

10. On the next screen (see example, below), enter the specific authorization for the system account you wish to establish. For federal system account requests, supporting Documentation **must** include Authority to Operate showing that the system meets security, privacy, and other federal standards for data access.
11. When all fields are complete, select Review to continue. If you need to return to the previous section, select the item from the table of contents or the Previous link at the end of the page.



**System Information** (checked)

**Organization Information**

**Permissions**

**Security Information**

**Authorization** (selected)

**WORKSPACE** testing testing 123 Draft

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

**Supporting Documentation**

Please attach any additional documentation such as the current ATO (Authority to Operate) for the interfacing system, or signed For Official Use Only Terms of Use agreement.

**Attachments**

Drag and drop files here, or [browse](#)

**Authorizing Official**

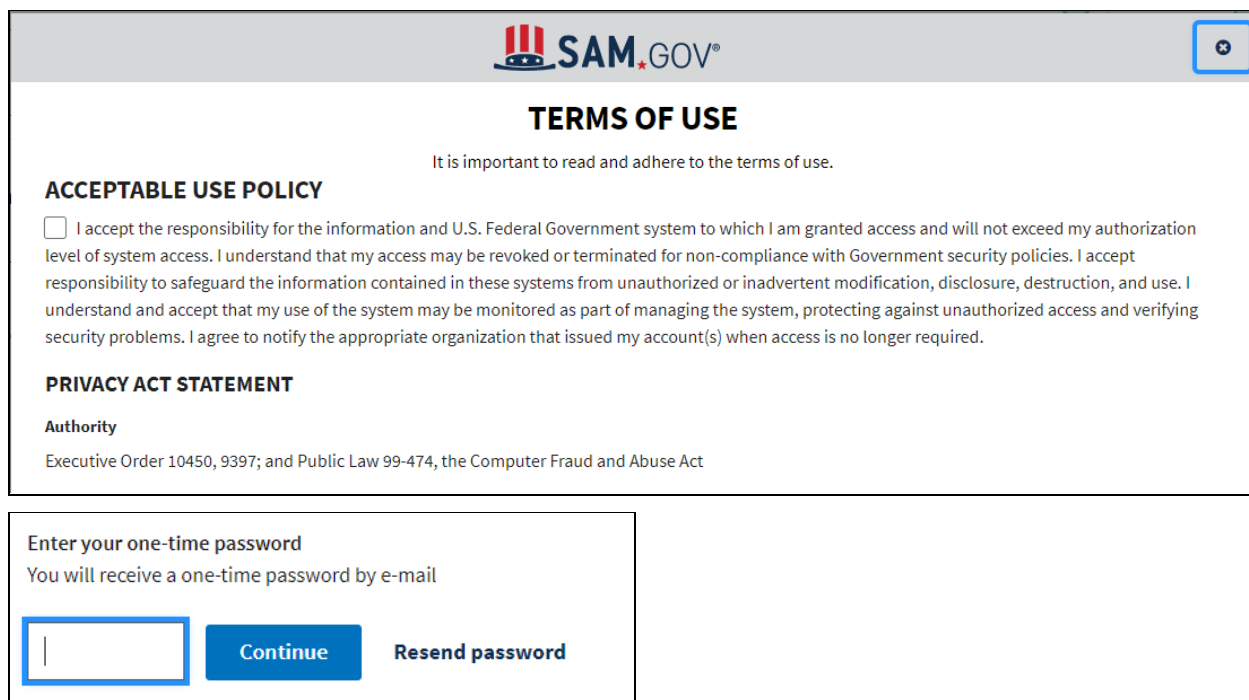
☐ I confirm that I am the authorizing official for the requested System Account and certify that all the provided information is current and correct.

**Name**  
Not Yet Certified

**Authorization Date**  
Not Yet Certified

Cancel Previous Review

12. Before final submission, review the application. Select Edit to change any section.
13. Select Submit after all sections are completed.
14. After selecting Submit, you must review all sections included in the terms of use document. At the end of the review, you must accept the terms of use by entering a one-time password sent to the email address on your own user account.



The screenshot shows the SAM.GOV Terms of Use page. At the top is the SAM.GOV logo. Below it is the title "TERMS OF USE" and a sub-header "ACCEPTABLE USE POLICY". A paragraph explains the importance of reading and adhering to the terms. A checkbox is provided for the user to accept the policy. Below this is a "PRIVACY ACT STATEMENT" section with a sub-header "Authority" and a paragraph citing Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. At the bottom of the screenshot is a form for entering a one-time password, with a text input field, a "Continue" button, and a "Resend password" link.

15. After accepting the terms of use, you will be returned to the SAM.gov home page.

Return to your workspace and select the System Account Widget. Your submitted account request will appear in the results section with a status (initial status depends on your role and the permissions you selected for the account).

Continue to [Review Status](#) for more on the approval process of your request.

## Reviewing Status

The most current status of a system account can be seen on the [Tier 2 Workspace](#).

**Request rejections:** If at any point a system account request is rejected, you will receive an email notification and the request will be moved back to draft for editing. You can resubmit the request after you complete edits.

**Notifications:** All changes to status are recorded in the history of the system account request and automated email notifications about status changes are sent to the submitter, associated system account managers and administrators, and those reviewing the request.

**Timeline & follow up:** The time required to process each status depends on the type of account (i.e. public data) and the permissions in the request.

- If your status is “Pending Review” check with your System Account Administrator.
- If your status is in “Pending Permissions Review” for more than a couple of business days, you can create an FSD ticket to request a status update on your request.

This is the sequence used to move your request through the approval process:

Step	Status	Description
1	DRAFT	System Account Managers and System Account Administrators can edit the draft.
2	PENDING REVIEW	If the original request was submitted by a System Account Manager, the request is now awaiting approval from the listed System Account Administrators, who will review and approve (or reject) the system’s business need for access.
3	PENDING PERMISSIONS REVIEW	GSA checks the account’s requested data access.
4	PENDING APPROVAL	GSA conducts a security review. If your account is not approved you will be notified via email and your request will not move forward.
5	PUBLISHED	The request has been approved and the account can now be used to access the data as requested.

**This concludes this information about how to request a federal system account.**

If you need to request a non-federal system account, start with the next section in this guide.

🕒 To learn more about system account passwords, [skip to this step](#).  
To learn more about system account API keys, [skip to this step](#).  
To learn more about system account management, [skip to this step](#).

### Requesting Non-Federal System Accounts

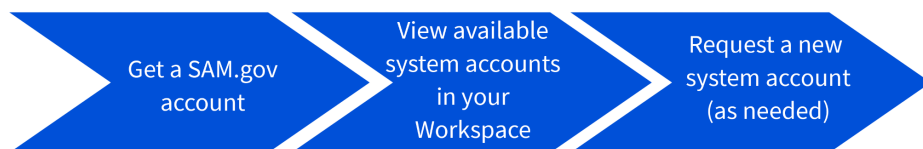
Remember, there are two types of system accounts: federal and non-federal.

A non-federal system account is for any system managed by an entity or other non-federal organization. As explained in the [permissions section](#) in this guide, non-federal entities may request read permissions of public data.

You can use the [Account Request Preparation Checklist](#) at the end of this guide to help you prepare the information necessary to complete system account processes.

⌚ If you only want to learn about federal system accounts, you can [skip to that section](#) now.  
To learn more about non-federal system accounts, continue.

Follow these steps to request your account.

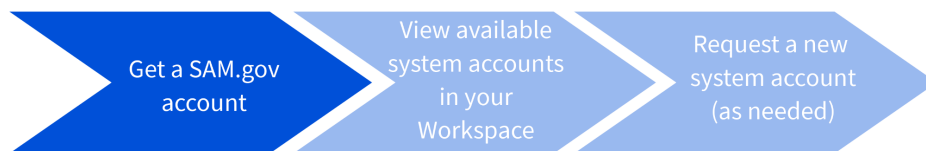


These topics will guide you through these steps:

- [Accessing the System Account Workspace](#)
- [Requesting a New System Account](#)
- [Reviewing Status](#)

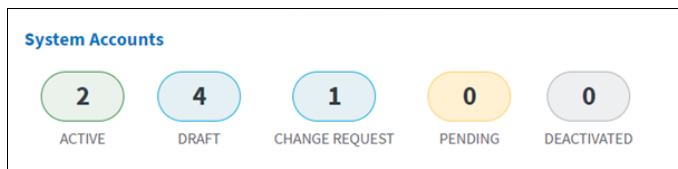
⌚ If you know which topic you want to explore, you can skip to it by selecting the topic name linked to that section. If you have never requested a non-federal system account, we recommend starting with the first topic.

## Accessing the System Account Workspace



The first step to requesting a non-federal system account is to **get a SAM.gov user account**. Select “Sign In” on the header of any page, and complete the account form.

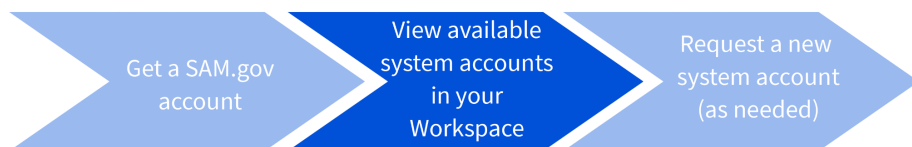
After you complete the account setup, you will have access to the *Workspace* where you can manage specific data or items. Your Workspace is tailored to you based on roles, permissions, and personal preferences. To request a non-federal system account, you will need to look for the System Accounts widget.



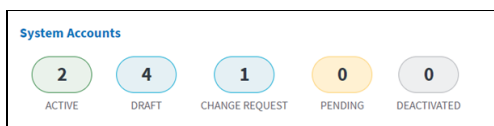
No specific roles or permissions are needed beyond the basic user profile.

## View Available System Accounts

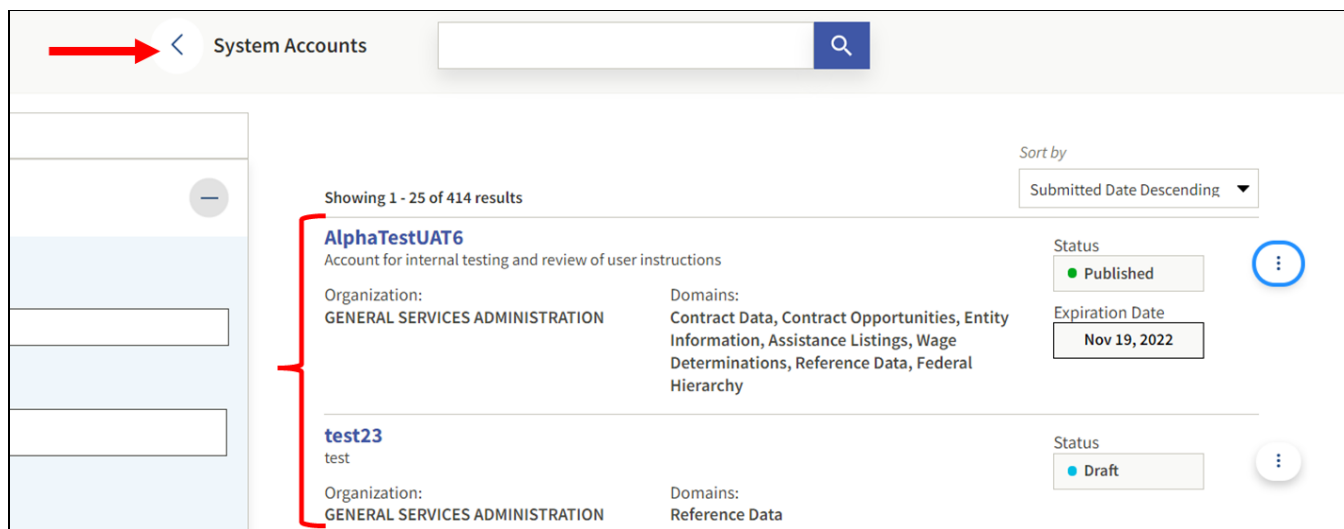
Once you have a SAM.gov account, view the system accounts that may be available to you currently:



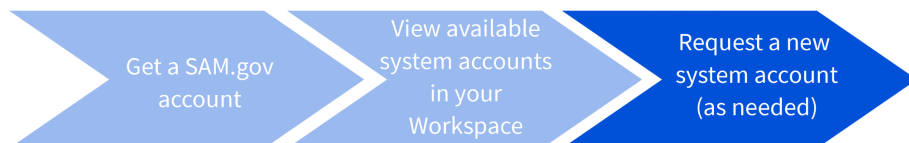
1. After you have logged in, navigate to your main Workspace from the header on any page.
2. In the System Accounts widget, you will see all the accounts that you have submitted as well as the system accounts for which you are listed as the *Other System Account Holder*. Other System Account Holder is a backup designation in case the primary requester of that system account is unable to access it. Select the System Accounts label from the widget to go to your detailed system accounts view.



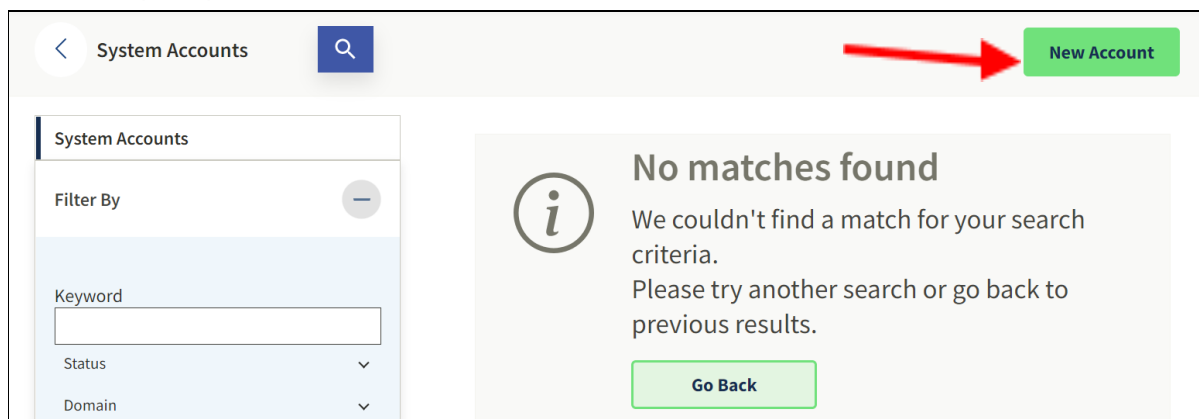
- This page is known as your *Tier 2 Workspace* for system accounts. Once you have created, submitted, or been associated with a System Account, you will be able to see those accounts on this page.



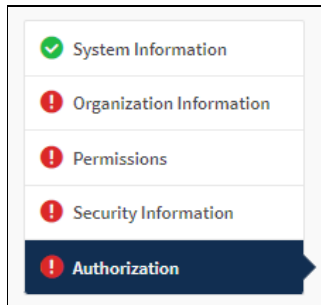
## Requesting a New System Account



- From the Tier 2 system accounts Workspace page, select New Account to start the new system account request process.



On the new account request screens, you can track your progress by viewing the navigation menu.



### System Information

2. Enter the details for the system account you wish to establish:
  - a. *System Account Name*: Unique name that helps you and others identify the account from any other you or others in your organization manage
  - b. *Interfacing System Name and Version*: Actual full name of the connecting system and version number
  - c. *System Description and Function*: The business reason for your system connection. This includes any justification for access to data.
3. When all fields are complete, select “Next” to move to the next section. Red text will appear by any field that fails validation with information on what needs to be updated. Correct the issue to move forward.

Be aware that selecting “Cancel” at any point in the process will delete the current edits and return you to the Tier 2 System Account Workspace.



Workspace / New System Account

☒ System Information

☐ Entity Information

☐ Permissions

☐ Security Information

☐ Authorization

WORKSPACE

**New System Account**

Draft

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit

Review

**System Account Name**

Provide a unique name for your new system account.

**Interfacing System Name and Version**

Provide the name and version of the system that will be connecting to SAM.gov.

**System Description and Function**

Example: *The IRS stated in a current MOU that their system tracks all incoming commitment requests and captures the information necessary to make awards.*

Cancel

Next

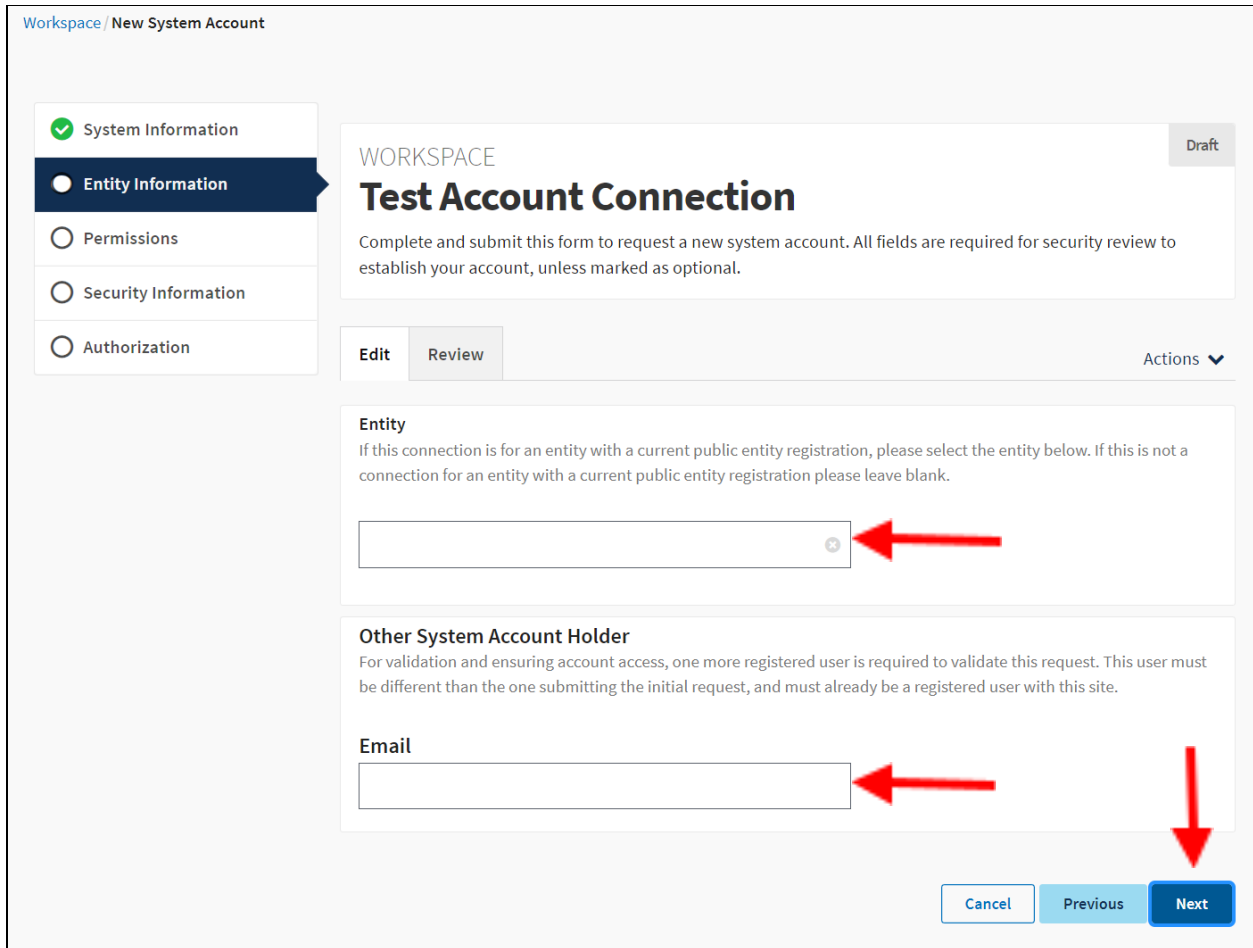
### Entity Information

4. Enter the specific entity information for the system account you wish to establish:
  - a. *Entity*: If this connection is for an entity with a current public entity registration, then you can enter that entity here using the entity picker. You can enter a single entity with a current, public entity registration. If this is not an entity with a current public registration, then you can leave this blank.
  - b. *Other System Account Holder*: Required. You must enter the email address of another non-federal user who is registered with the site. This user will be considered the joint account holder for this account and will have permission to manage this account. This

user will also be the first-level approver for the account once you submit the account. You cannot enter your own email address in this field. You will see an error message in red next to the field if you do not enter a valid email address that meets all the above requirements. The reason you must enter another email address here is so that if, for any reason, you leave your company or lose access to your account, the owner of the other email address can maintain access to the system account for your entity.

5. When all fields are complete, select “Next” to move to the next section. If you need to return to the previous section, select the item from the table of contents or the “Previous” link at the end of the page.

Be aware that selecting “Actions” and then “Delete” from the dropdown will delete the draft in progress and route you back to the Tier 2 Workspace page.



Workspace / New System Account

System Information

Entity Information

Permissions

Security Information

Authorization

WORKSPACE

Draft

### Test Account Connection

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit Review Actions

**Entity**

If this connection is for an entity with a current public entity registration, please select the entity below. If this is not a connection for an entity with a current public entity registration please leave blank.

**Other System Account Holder**

For validation and ensuring account access, one more registered user is required to validate this request. This user must be different than the one submitting the initial request, and must already be a registered user with this site.

Email

Cancel Previous Next

*Permissions*

6. Enter the specific permissions for the system account you wish to establish:
  - a. Choose the permissions you want to request. You can review the previous section titled “[Permissions for Data Access](#)” and [Appendix A: Domain Roles and Permissions](#) to identify the specific permission requirements for your system in advance of making your request. If the requested permission is not properly justified, the account request will be rejected.
7. Selecting “Terms of Use” will open a popup window that displays the full text of the terms of use you will be asked to acknowledge and agree to upon system account submission.
8. When all fields are complete, select “Next” to move to the next section. If you need to return to the previous section, select the item from the table of contents or the “Previous” link at the end of the page.

WORKSPACE

Draft

## Test Account Connection

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit

Review

Actions ▾

What do you need?

Terms of use

### Contract Opportunities

☐ Read Public
 ☐ Read Sensitive
 ☐ Write Public
 ☐ Write Sensitive

### Contract Data

☐ Read Public
 ☐ Write Public
 ☐ Read DoD Data
 ☐ Write DoD Data

### Entity Information

☐ Read Public
 ☐ Read FOUO
 ☐ Read Sensitive

### Federal Hierarchy

☐ Read Public Only
 ☐ Read FOUO

### Assistance Listings

☐ Read Public

### Wage Determinations

☐ Read Public

### Reference Data

☐ Read Public

Cancel

Previous

Next

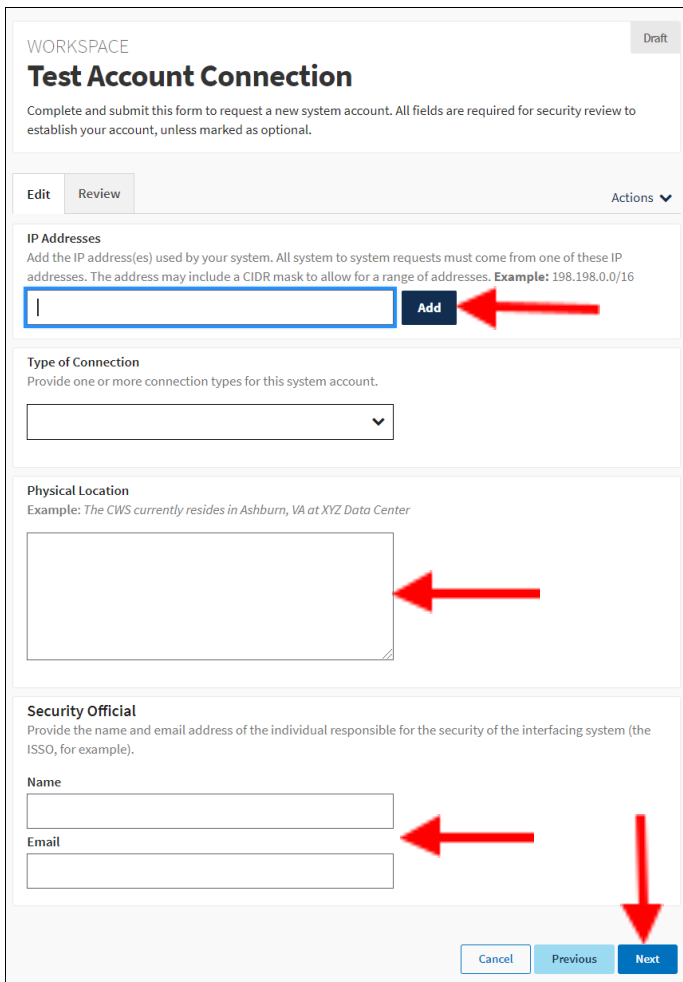
*What do the white and gray checkboxes mean?*

White boxes indicate permissions that are available to choose in the domain they are listed under.

Gray boxes indicate permissions that are not available to choose in the domain they are listed under.

## Security Information

9. Enter the specific security information for the system account you wish to establish:
  - a. IP Address: This should be the specific external Internet Protocol (IP) address or addresses for the system connecting. If the IP is masked by Classless Inter-Domain Routing (CIDR), then the range should be entered here.
  - b. Type of Connection: Any connection the system will use should be selected, such as REST API, etc.
  - c. Physical Location: The primary physical location of the system.
  - d. Security Official: Your entity's System Security Officer (ISSO) or other security personnel (NOT the GSA security reviewer).
10. When all fields are complete, select "Next" to move to the next section. If you need to return to the previous section, select the item from the table of contents or the "Previous" link at the end of the page.



**WORKSPACE** Draft

### Test Account Connection

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit Review Actions ▾

**IP Addresses**  
Add the IP address(es) used by your system. All system to system requests must come from one of these IP addresses. The address may include a CIDR mask to allow for a range of addresses. **Example:** 198.198.0.0/16

Add

**Type of Connection**  
Provide one or more connection types for this system account.

**Physical Location**  
Example: The CWS currently resides in Ashburn, VA at XYZ Data Center

**Security Official**  
Provide the name and email address of the individual responsible for the security of the interfacing system (the ISSO, for example).

**Name**

**Email**

Cancel Previous Next

## Authorization

11. Attach the specific authorization for the system account you wish to establish. The Supporting Documentation is optional (official documentation showing the system meets a prescribed set of security and privacy standards).
12. When all fields are complete, select “Review” to move to the next section. If you need to return to the previous section, select the item from the table of contents or the “Previous” link at the end of the page.

WORKSPACE
Draft

### Test Account Connection

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit
Review
Actions ▼

#### Supporting Documentation

Please attach any additional documentation such as the current ATO (Authority to Operate) for the interfacing system, or signed For Official Use Only Terms of Use agreement.

Attachments

Drag and drop files here, or [browse](#)

#### Authorizing Official

☐ I confirm that I am the authorizing official for the requested System Account and certify that all the provided information is current and correct.

**Name**  
Not Yet Certified

**Authorization Date**  
Not Yet Certified

Cancel
Previous
Review

13. Before final submission, review the application. Select “Edit” to change or update any section.
14. The final “Submit” selection will be available after all sections are completed.

✓ System Information

✓ Entity Information

✓ Permissions

✓ Security Information

✓ **Authorization**

WORKSPACE

Draft

## Test New Non Federal Account

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit

Review

Submit

Actions ▾

System Information

Unique System ID:Test New Non Federal Account

Interfacing System Name and Version:Test

System Description and Function  
Test

Edit

Entity Information

Entity:Perspecta Enterprise Solutions LLC

Other System Account Holder  
Latha Ramakrishnan

Edit

Permissions

Contract Opportunities:

Contract Data:

Entity Information:

Federal Hierarchy:

Wage Determinations:

Assistance Listings:  
read public

Reference Data:

Edit

Security Information

IP Address:

198.198.0.0/16

Type of Connection:  
SOAP APIs

Physical Location:  
Test

Security Official:  
test  
test@t.t

Edit

Authorization

Supporting Documentation

No files are attached to this application

Authorizing Official

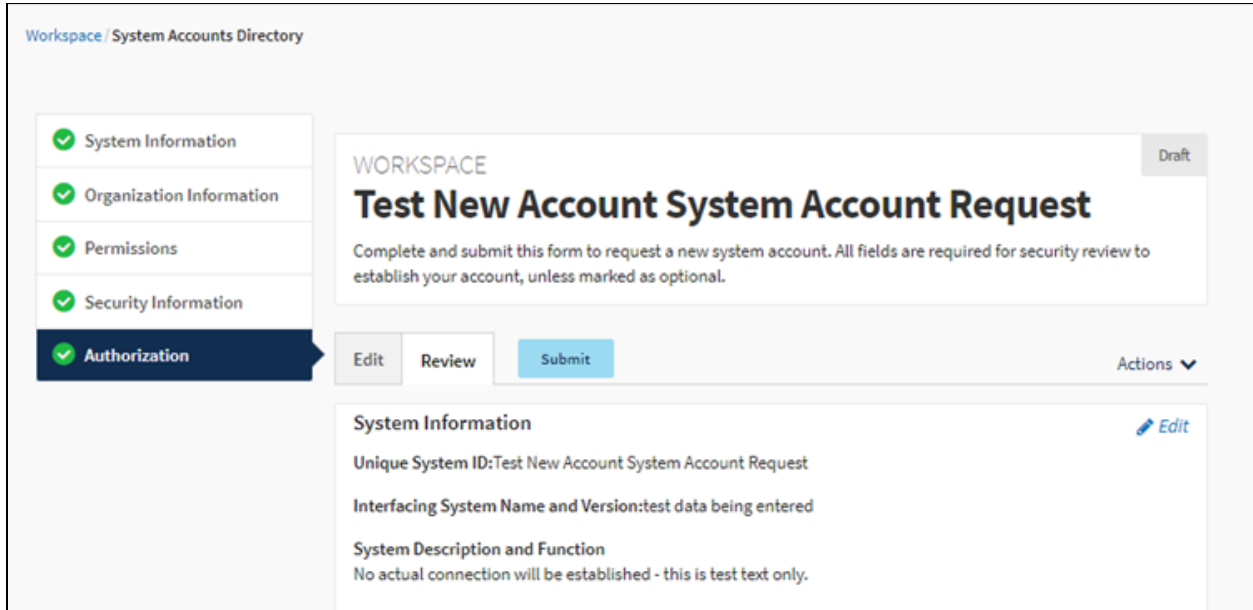
☒ I confirm that I am the authorizing official for the requested System Account and certify that all the provided information is current and correct.

Name:Test Non Fed

Date:Nov 20, 2020 10:29 am

Edit

15. After selecting “Submit,” you will be routed to accept the terms of use.



Workspace / System Accounts Directory

System Information

Organization Information

Permissions

Security Information

Authorization

Workspace

**Test New Account System Account Request**

Draft

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Edit Review Submit Actions

System Information

Unique System ID: Test New Account System Account Request

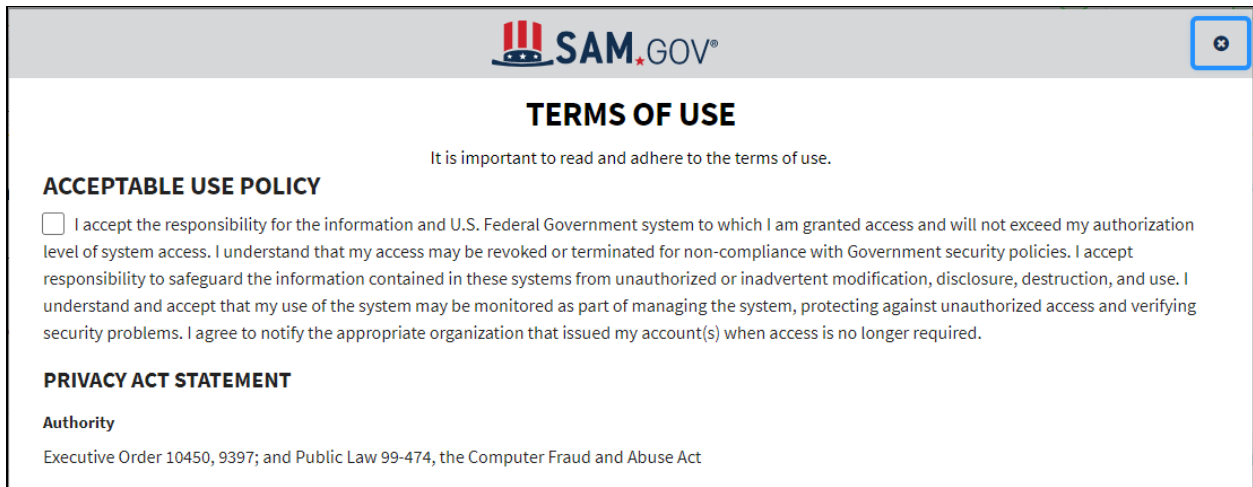
Interfacing System Name and Version: test data being entered

System Description and Function

No actual connection will be established - this is test text only.

16. You must review all sections included in the terms of use document.

17. At the end of the review, you must accept the terms of use through a one-time password sent to the email address of your user account.



SAM.GOV

**TERMS OF USE**

It is important to read and adhere to the terms of use.

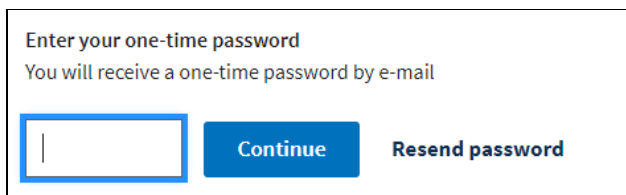
**ACCEPTABLE USE POLICY**

☐ I accept the responsibility for the information and U.S. Federal Government system to which I am granted access and will not exceed my authorization level of system access. I understand that my access may be revoked or terminated for non-compliance with Government security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

**PRIVACY ACT STATEMENT**

Authority

Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act



Enter your one-time password

You will receive a one-time password by e-mail

Continue Resend password



18. After accepting the terms of use, you will be returned to the SAM.gov home page.

Return to your workspace and select the System Account Widget. The submitted account request will appear in the results section with a status of “Pending Review.” Continue to the “Review Status” section below for more on the workflow steps the request will go through.

**After this step, your request has been submitted and will go into an approval workflow.**

### Reviewing Status

The most current status of a system account can be seen on the [Tier 2 Workspace](#).

**Request rejections:** If at any point a system account request is rejected, you will receive an email notification and the request will be moved back to draft for editing. You can resubmit the request after you complete edits.

**Notifications:** All changes to status are recorded in the history of the system account request and automated email notifications about status changes are sent to the submitter, associated system account managers and administrators, and those reviewing the request.

**Timeline & follow up:** The time required to process each status depends on the type of account (i.e. public data) and the permissions in the request.

- If your status is “Pending Review” check with your System Account Administrator.
- If your status is in “Pending Permissions Review” for more than a couple of business days, you can create an FSD ticket to request a status update on your request.

This is the sequence used to move your request through the approval process:

Step	Status	Description
1	DRAFT	The user who submitted the account and the Other System Account Holder listed on the account can edit the draft.
2	PENDING REVIEW	The Other System Account Holder listed on the account will review and approve (or reject) the system’s business need to access the data requested in the format requested.
3	PENDING PERMISSIONS REVIEW	GSA checks the account’s requested data access.
4	PUBLISHED	The request has been approved and the account can now be used to access the data as requested.

All changes to status are recorded in the history of the system account request and email notifications to the submitter, the Other System Account Holder, and those reviewing are sent automatically.

**This concludes this information about how to request a non-federal system account.**

🕒 To learn more about system account passwords, [skip to this step](#).  
To learn more about system account API keys, [skip to this step](#).  
To learn more about system account management, [skip to this step](#).

## Managing System Accounts

You'll need to take action periodically to manage your system account and system account API key. Proper management will help ensure you can use it to access information on an ongoing basis. The following topics will help both federal system account and non-federal system account holders with these management tasks:

- [Getting a System Account Password](#)
- [Resetting a System Account Password](#)
- [About System Account API Keys](#)
- [Getting a System Account API Key](#)
- [System Account API Key Rotation](#)
- [Tips for System Account API Key Rotation](#)
- [Other System Account Management Tasks](#)
- [Editing System Accounts](#)
- [Requesting a Rate Increase](#)
- [Renewing System Accounts](#)
- [System Account Deactivation](#)

You can use the [Account Management Checklist](#) at the end of this guide to help you manage your system account throughout the year.

### About System Account Passwords

**Do you need a system account password? Yes.** You will use it for two functions: accessing your system account, and connecting to APIs (where required).

Connecting to APIs: For your federal or non-federal system to connect, you may need a *system account password*, a *system account API key*, or both. Different APIs may require a password in addition to a key, while others may not.

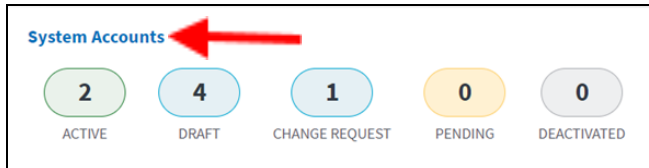
Each API has its own requirement outlined at [open.gsa.gov](https://open.gsa.gov). For example, the Contract Opportunity Interface API requires the user to pass both the System Account Password and the API Key, whereas, one of the Entity domain APIs requires just the API key and not the password. You can view the individual requirements for APIs at [open.gsa.gov/api](https://open.gsa.gov/api). Select “View API Documentation” for APIs you want to connect to using your system account.

Accessing your system account: You do not need to have a password to generate a replacement API key; that happens automatically in [API key rotations](#). However, you do need

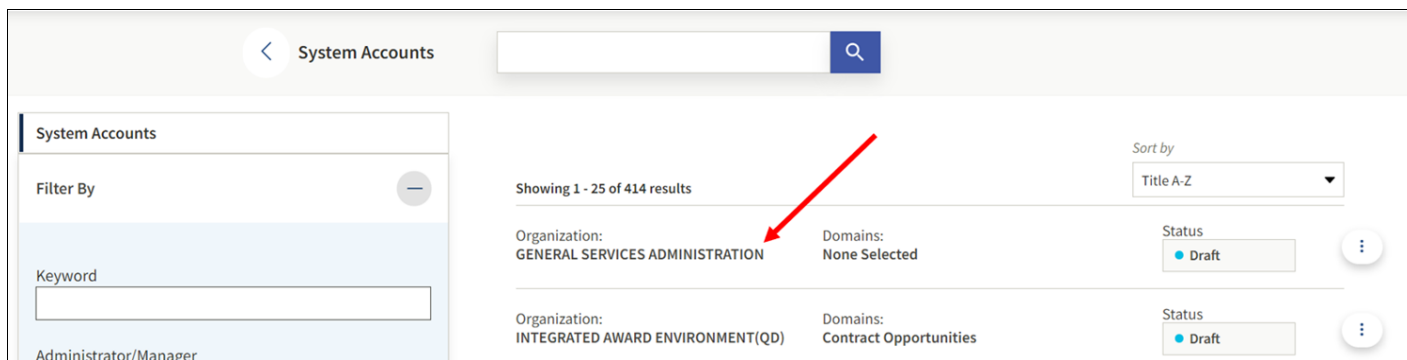
to keep your password up to date so that you can access your system account and view your API key.

## Getting a System Account Password

1. Login and navigate to your Workspace from the header of any SAM.gov page.
2. Select System Accounts from the widgets to view your system account details.



3. Navigate to the system account you want to set a password for. Select the name of the system account, which will open the account details page. The account details page includes all the information about the account that you provided when requesting it, as well as a place to establish and maintain a password.



4. On the account details page, scroll to System Account Password to create a password for the account. For security reasons, the password should meet the following requirements:
  - Be at least 12 characters
  - Have at least 1 uppercase character
  - Have at least 1 lowercase character
  - Have at least 1 numeric digit
  - Have at least 1 special character: !@#\$%^&\* \_ +
  - Should not contain part of the System Account name
  - Should not be a common or generic password
  - Should not be one of the past 24 passwords that were used on the account

System Account Password

New Password *Required*

Confirm Password *Required*

☐ Show Password

**Passwords must:**  
Be at least 12 characters  
Have at least 1 uppercase character  
Have at least 1 lowercase character  
Have at least 1 numeric digit  
Have at least 1 special character: !@#\$%^&\*~+

- Once your chosen password meets the parameters, select Save. A success message will appear, and options to reset the password will be displayed for future password changes.

System Account Password

☒ **Success**  
Password has been successfully set!

Select one of the options below  
☒ Reset Password ☐ Forgot Password

Current Password *Required*

New Password *Required*

Confirm Password *Required*

☐ Show Password

**Passwords must:**  
Be at least 12 characters  
Have at least 1 uppercase character  
Have at least 1 lowercase character  
Have at least 1 numeric digit  
Have at least 1 special character: !@#\$%^&\*~+

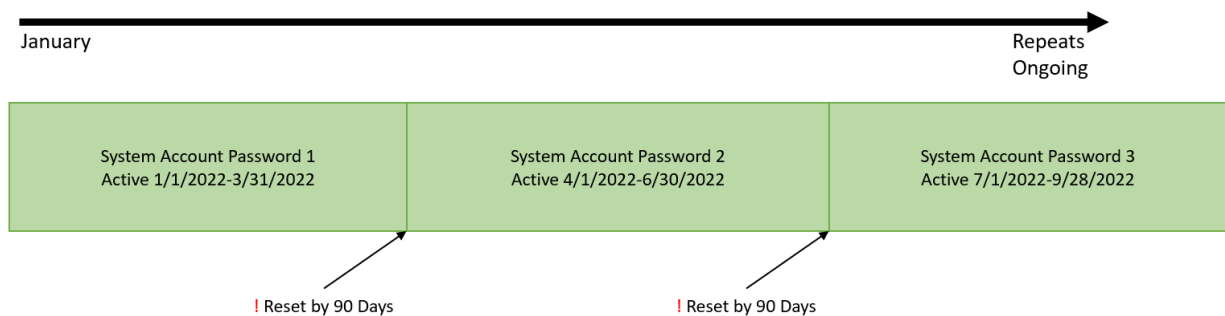
## Resetting a System Account Password

To continue using the system account, you must reset the password on the account every 90 days.

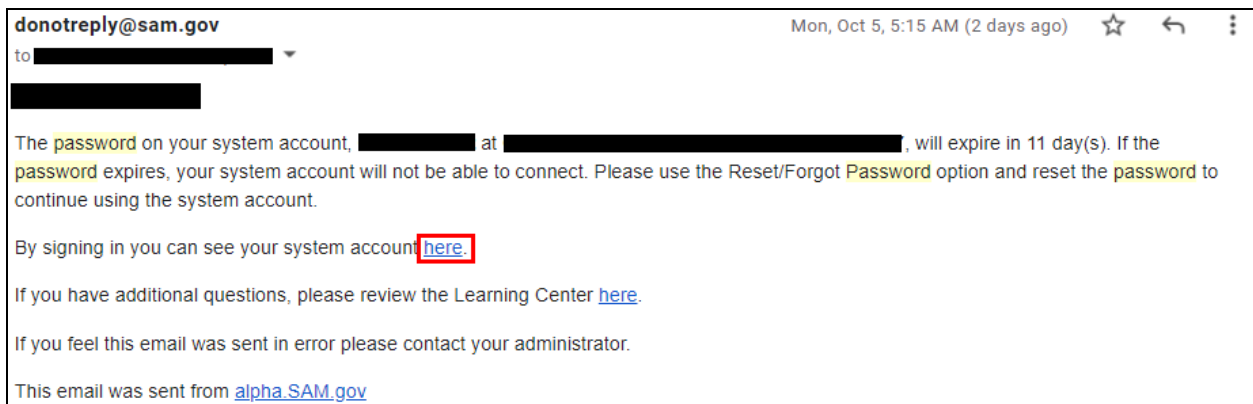
Note: System account passwords and system account API keys expire and rotate on different schedules. Resetting your password does not generate a new key (keys

are auto-generated). Please note that if your password has expired, that means you can't use it to view your system account or API key (see below). Also, APIs which are required by open.sam.gov to use both a key and a password will not be able to connect to SAM.gov. If this happens, you must resolve either your expired password, your replacement API key, or both, depending on the timing of your system account. You will receive email reminders for both of these activities throughout your use of your system account. See the [troubleshooting](#) guidance in the appendix for help with this.

Example:  
For a System Account Requested on January 1, 2022, the Password Reset cycle looks like this.



You will receive notifications prior to the expiration of the password that will contain a link to the system account details page where you can reset the account. You can also sign in to SAM.gov and navigate to your system account details page from your Workspace.



1. Follow the first steps for [Getting a System Account API Password](#) to navigate to the system accounts details page. Locate the password section and select either the Reset Password or Forgot Password option.

**System Account Password**

Select one of the options below

☒ Reset Password    ☐ Forgot Password

**Current Password** *Required*

.....

**New Password** *Required*

.....

**Confirm Password** *Required*

.....

☐ Show Password

**Passwords must:**

- ✓ Be at least 12 characters
- ✓ Have at least 1 uppercase character
- ✓ Have at least 1 lowercase character
- ✓ Have at least 1 numeric digit
- ✓ Have at least 1 special character: !@#\$%^&\*~+

**Save**

- a. Use Reset Password if you know the current password on the account. Enter your current password, the new password, and confirm the new password. Select Save to complete the process.

**System Account Password**

Select one of the options below

☒ Reset Password    ☐ Forgot Password

**Current Password** *Required*

.....

**New Password** *Required*

.....

**Confirm Password** *Required*

.....

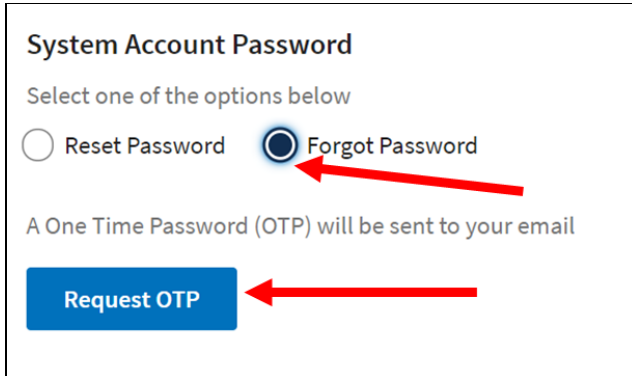
☐ Show Password

**Passwords must:**

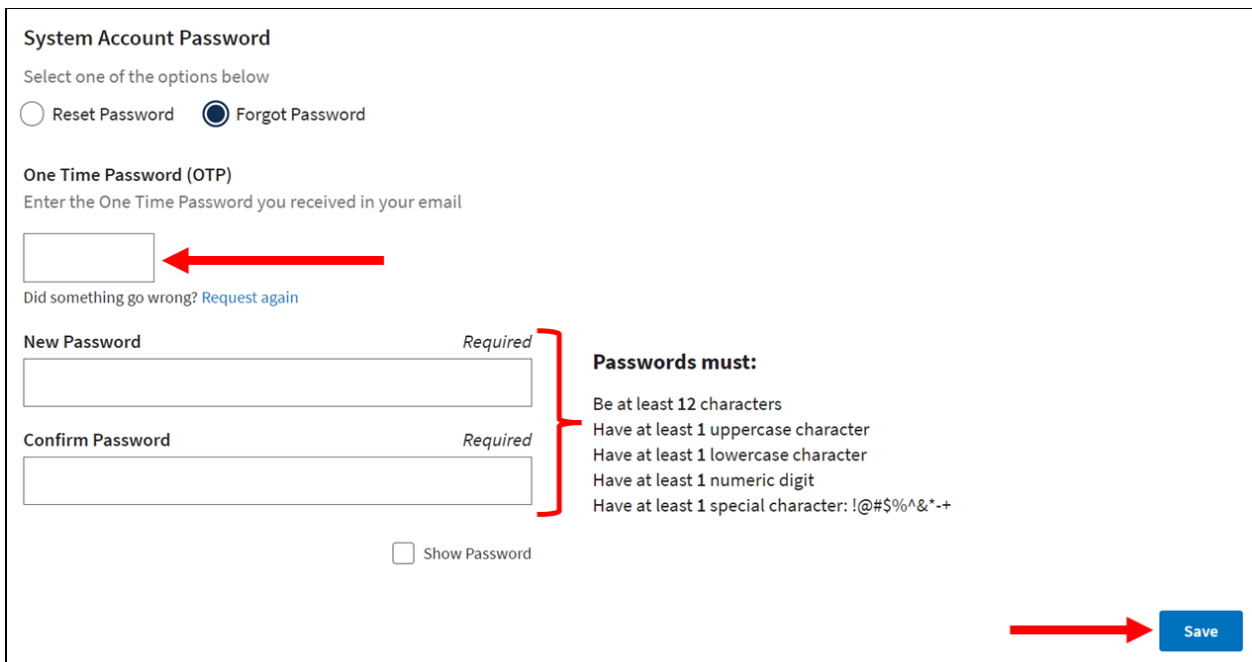
- ✓ Be at least 12 characters
- ✓ Have at least 1 uppercase character
- ✓ Have at least 1 lowercase character
- ✓ Have at least 1 numeric digit
- ✓ Have at least 1 special character: !@#\$%^&\*~+

**Save**

- b. Use Forgot Password if you do not know the current password on the account. First, select Forgot Password to receive a one-time password (OTP). This will send an email to the signed-in user email.



- c. Enter this OTP into the prompt, along with the new password of your choice. Confirm the new password and select Save.



2. Once you receive a success message, your password has been changed and you can use it.

**This concludes the information you need to know about system account passwords.**



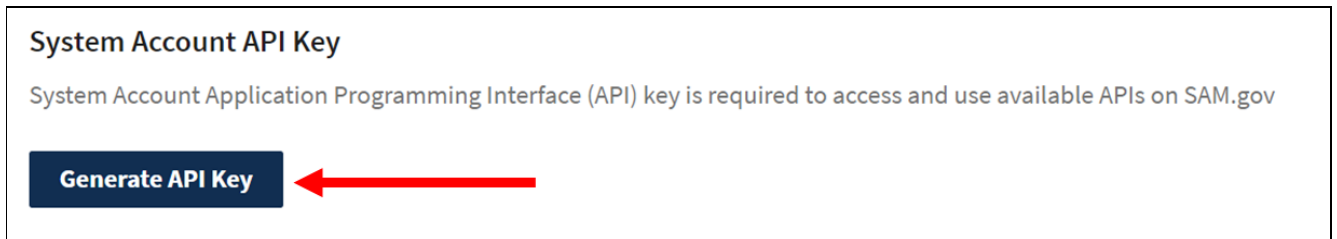
## About System Account API Keys

API keys allow your system to connect to SAM.gov to send and/or receive data. To connect, you must input a system account API key into the system that you want to connect to SAM.gov. You need to have an active key from your SAM.gov system account in your system at all times so that it can perform the calls that are allowable based on the [type connection and rate limits](#) you have. Once you input an API key, it will be good until that key rotates, at which point you must switch out the keys in order to maintain your connection. You can learn more about [system account API key rotation cycles](#) in this guide.

### Getting a System Account API Key

If this is a new system account, generate your first API key using the following steps. Future API keys will be auto-generated on a rotating basis. You can read more about [API Key rotation](#) below.

1. Sign in to your system account details page. Locate the System Account API Key section. Select Generate API Key.

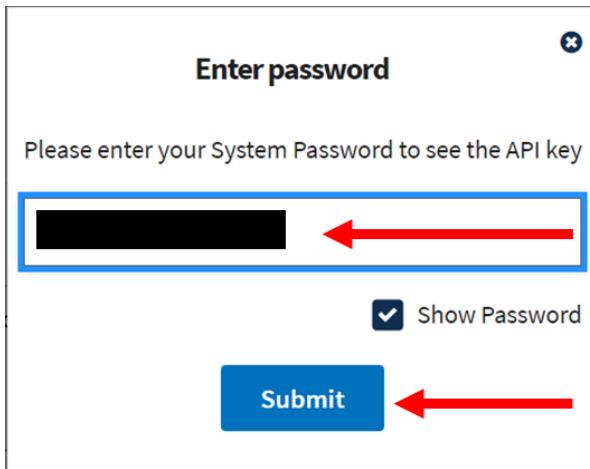


**System Account API Key**

System Account Application Programming Interface (API) key is required to access and use available APIs on SAM.gov

**Generate API Key**

2. Enter your system account password and select Submit.



**Enter password**

Please enter your System Password to see the API key

☒ Show Password

**Submit**

3. Your password will be validated to ensure that it matches the password on the account. When the validation passes, the API key displays on the screen.

The API key will be hidden when you navigate to this page in the future. To display the key, select the eye icon and enter your system account password to view the key.



### System Account API Key

System Account Application Programming Interface (API) key is required to access and use available APIs on SAM.gov

Expires in 89 days

\*\*\*\*\*

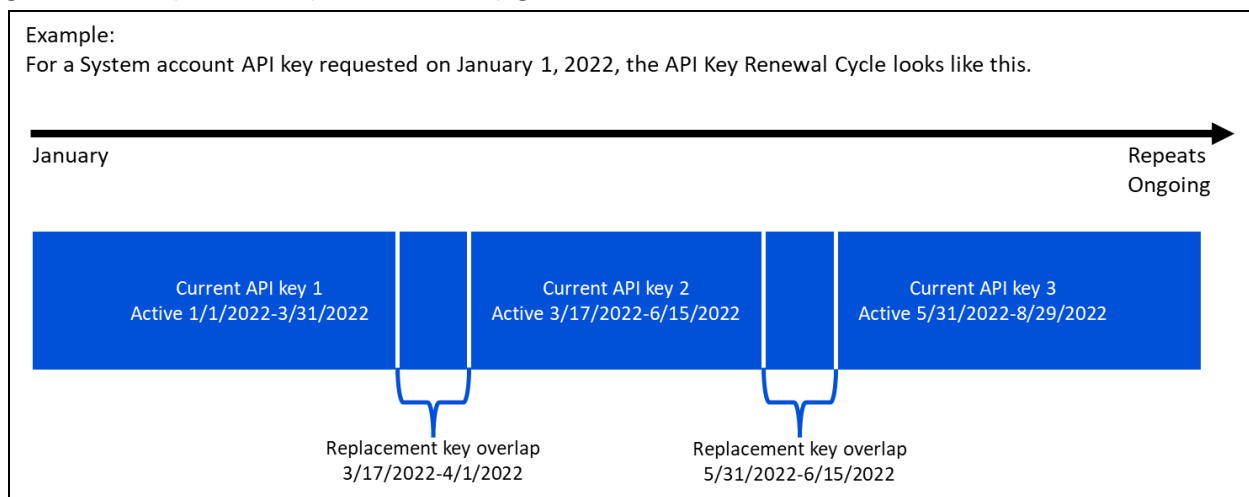
←

Input your first system account API key into your system so that it can make successful calls to SAM.gov.

## System Account API Key Rotation

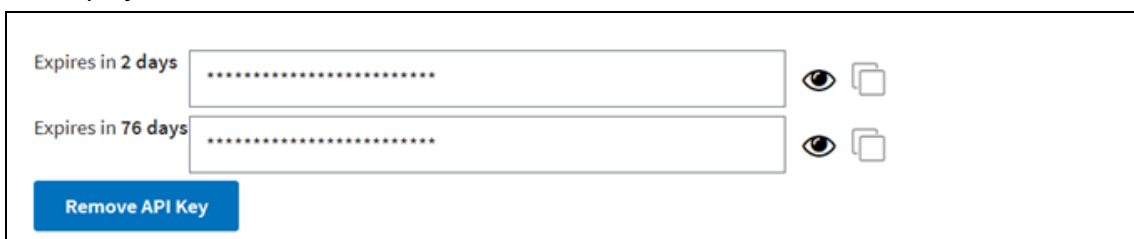
For security reasons, system account API keys rotate every 90 days. A new replacement key will be generated for you before your current key goes out of date (*rotation*). Here's what happens:



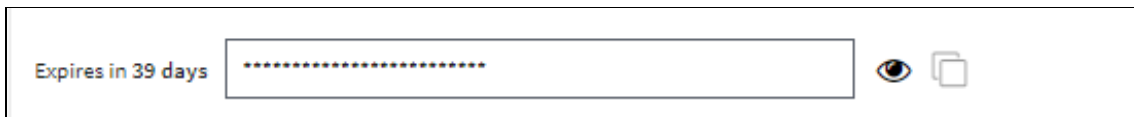
- You will receive a series of several email notifications starting 15 days prior to when your current system account API key goes out of date, notifying you of the upcoming rotation. *Please read all emails about your system accounts so you do not miss important messages!*
- 15 days before your current key goes out of date, a replacement system account API key will *auto-generate* and will appear in the Public API Key section of your System Account Details page.

- You should retrieve your replacement API key as soon as possible after it is auto-generated. Replace the current key in your system that connects through the system account. Both the replacement and current key will work during the 15-day window before expiration.
- The current key will expire at midnight at the end of the 14th day, and the replacement key will become the current key at that point. Only the new, current key will be visible, until it has 15 days until rotation.

When your system account API key is in the 15 day rotation period, the System Account API Key section will display this:



When your system account API key is not in the 15 day rotation period, you will see only one key and the number of days until expiration.



#### *API Key Rotation Tips for System Accounts*

- **You do not need to do anything to request a replacement key/ API key rotation.** The replacement key is auto-generated as part of the system account API key rotation workflow.
- Your only task for API Key rotations is to **view and use the key that is active** during the time period when you want to connect through your API. **You must trade your current key in your system for the new (replacement) key generated in your system account details before the current one goes out of date.** During the 15-day rotation period, you may use either key to connect through API, although best practice is to exchange the keys as soon as the replacement one is generated.
- **Your password expiration, system status, and API rotation cycles are not connected.** Changing your password will not cause the API key to be rotated (these are automatically generated on their own schedule). However, changing your password in a timely way will ensure you can view your system account page at all times, including when your API Key

rotates. Your system account must be approved and in active status so that the auto generation cycle knows to generate an API key for it on the prescribed schedule.

- System API Key rotation cycles will trigger a series of reminder emails to you. The purpose of these emails is to remind you to retrieve your new (replacement) key and replace your current key in your system. **You can disregard emails for System Account API rotations once you have retrieved your replacement key.** Our notification system does not know when you have retrieved your replacement key, so you can expect to continue receiving emails even after you have exchanged API keys as instructed.
- In the unlikely event that your key goes out of date and a replacement key has not been generated, **you can select Generate API Key on your account page to manually generate a key.** This option is only available after your current key goes out of date. Although this is not a common problem, if you must manually generate a new API Key after your current one goes out of date, please [report this issue to the FSD](#) so they can investigate how to ensure future auto-generation occurs on time.

You can view solutions to the top common issues in [For More Help](#) at the end of this guide. For comprehensive FAQs, please search [fsd.gov](#).

**This completes the information about how to establish and rotate system account API keys.**

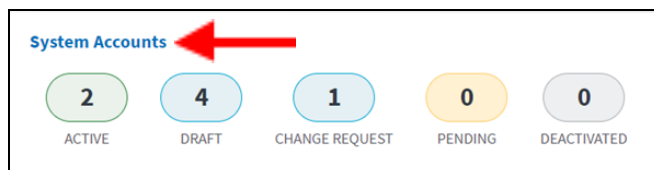
## Other System Account Management Tasks

### Editing System Accounts

After publication of the system account, you can submit a change request for any system account details. Change requests will go through a review process similar to the original submission. You can review that sequence in the Review Status sections for [federal](#) or [non-federal](#) system accounts.

To submit a change request:

1. Sign in to SAM.gov with the account associated with the system account you want to change.
2. Navigate to your Workspace from the header on any page.
3. Select System Accounts to go to your Tier 2 Workspace for System Accounts.



4. Use any of the filters to search your system accounts for the account you want to update.

System Accounts

Filter By

Keyword

Administrator/Manager

Status

☐ Draft

☐ Pending Review

☐ Pending Permissions Approval

☐ Pending Approval

☐ Published

☐ Deactivated

☐ Change Request

Domain

☐ Assistance Listings

☐ Contract Data

☐ Contract Opportunities

☐ Entity Information

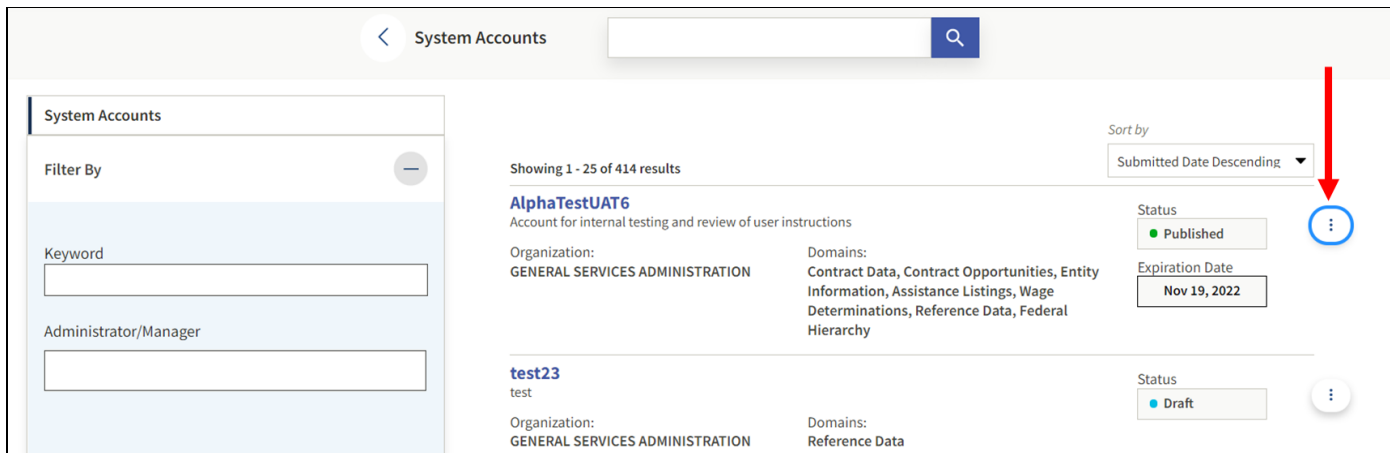
☐ Federal Hierarchy

☐ Reference Data

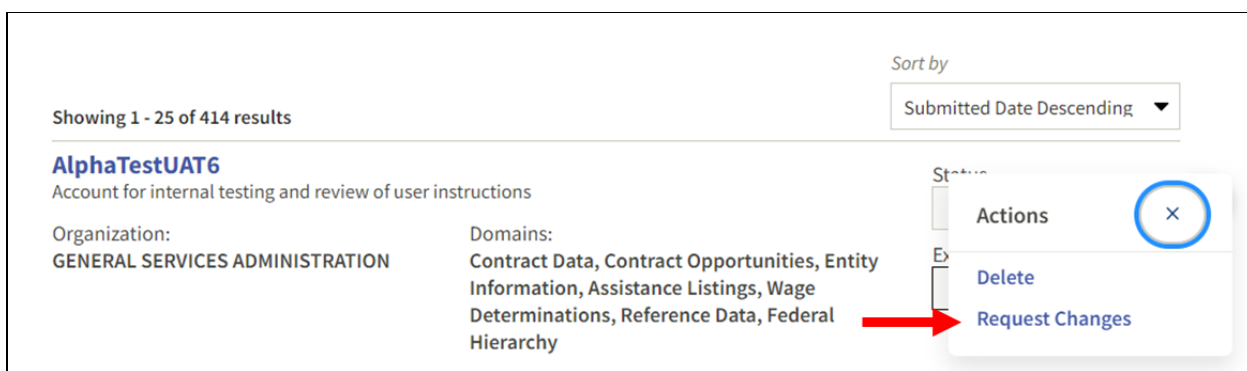
☐ Wage Determinations

Reset

5. Select Request Changes from the Actions dropdown menu.

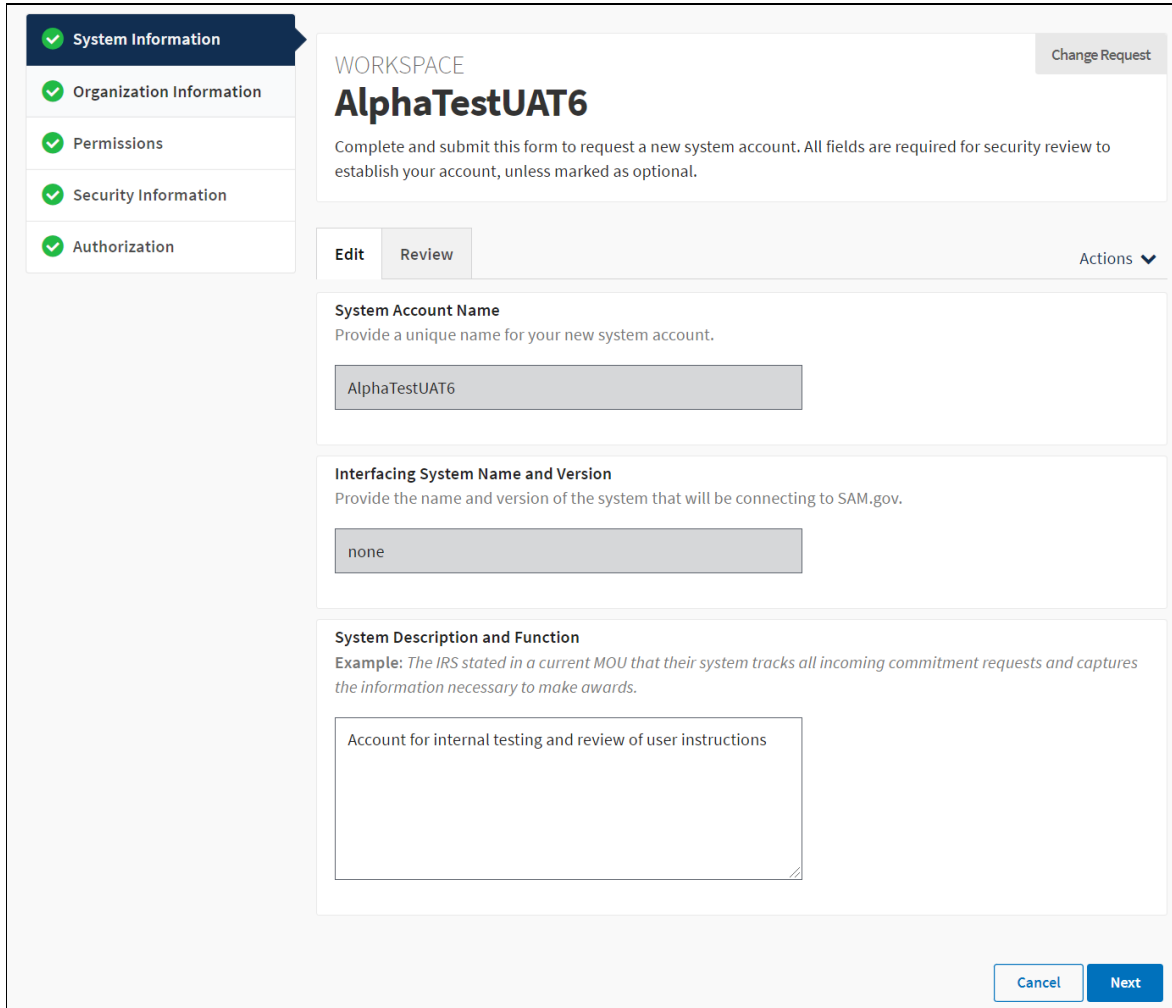


The screenshot shows the 'System Accounts' page. On the left is a filter sidebar with 'Filter By', 'Keyword', and 'Administrator/Manager' fields. The main area displays a list of accounts. The first account is 'AlphaTestUAT6', described as 'Account for internal testing and review of user instructions', with organization 'GENERAL SERVICES ADMINISTRATION' and domains including 'Contract Data, Contract Opportunities, Entity Information, Assistance Listings, Wage Determinations, Reference Data, Federal Hierarchy'. Its status is 'Published' and its expiration date is 'Nov 19, 2022'. A red arrow points to the actions menu icon (three dots) next to this account.



This close-up shows the 'AlphaTestUAT6' account entry. The actions dropdown menu is open, showing options: 'Actions' (with a close button), 'Delete', and 'Request Changes'. A red arrow points to the 'Request Changes' option.

## 6. Provide your desired changes and submit for approval.



The screenshot displays the 'Workspace' for 'AlphaTestUAT6' in the SAM.gov system. On the left, a sidebar lists navigation options: 'System Information' (selected), 'Organization Information', 'Permissions', 'Security Information', and 'Authorization'. The main content area is titled 'Workspace AlphaTestUAT6' and includes a 'Change Request' button. Below the title, a message states: 'Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.' The form has two tabs: 'Edit' and 'Review' (active). The 'Review' tab shows three sections: 'System Account Name' with the value 'AlphaTestUAT6', 'Interfacing System Name and Version' with the value 'none', and 'System Description and Function' with the text 'Account for internal testing and review of user instructions'. An 'Example' text is provided for the description: 'Example: The IRS stated in a current MOU that their system tracks all incoming commitment requests and captures the information necessary to make awards.' At the bottom right, there are 'Cancel' and 'Next' buttons.

Here's what to expect once you have requested system account changes:

- Once the changes have been approved, the account will inherit the same system account password and API key as the original account. In other words, you will not need to reset the account password or retrieve a renewed API key until either reaches the next scheduled expiration period.
- Please note that making changes will deactivate the current account, and a new, approved copy of the account will replace it. The deactivation of the current account with outdated information only occurs *after* the account changes you requested are approved. This is to ensure your system can continue to make calls without disruption, even when you make changes to the account information. This also means that you

may see a deactivated account of the same system account name. This is normal. You can continue using the new copy of the account and leave the deactivated account alone.

## Requesting a Rate Increase

[Default rates](#) are listed in the first section of this guide. Remember, only federal users of federal system accounts can request a rate increase. If you are not a federal user, or if you are using an individual account API key, your accounts are not eligible to be considered for this exception.

**Rate increases are considered rare exceptions.** Please make and document all attempts to optimize your current API calls to lower the amount of data being called; use smart query; or use extracts from SAM.gov data services to get the data you need without requesting a rate increase exception.

To request a rate increase, submit your request through FSD. Include all of the following information:

- System account user name
- System account email
- Latest system account API key
- How many API calls are you using currently and what is the anticipated future need
- Specify if the need for increase is temporary
- All endpoints, e.g. entity information, that are impacted by the increase
- Business justification for the rate increase

Rate increases will be handled on a case by case basis.

## Renewing System Accounts

For security purposes, GSA annually renews system accounts to verify that the details of the account, agreements, and points of contact (POCs) are kept current and accurate. **Note:** This is not the same as rotating your API.

For new System Accounts, the account's expiration date will be set to one year from the date of final approval. **Note:** If you submit a change request to your account, the account's expiration date will be changed to one year from the date of final approval of the change request.

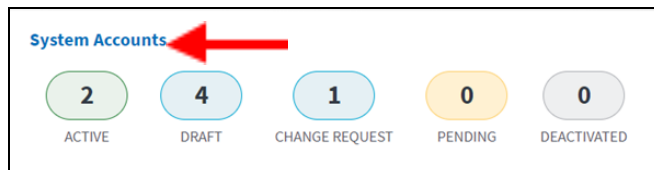
You will receive email notifications starting 30 days prior to the expiration date of the account to remind you to renew your account.

To renew a System Account:

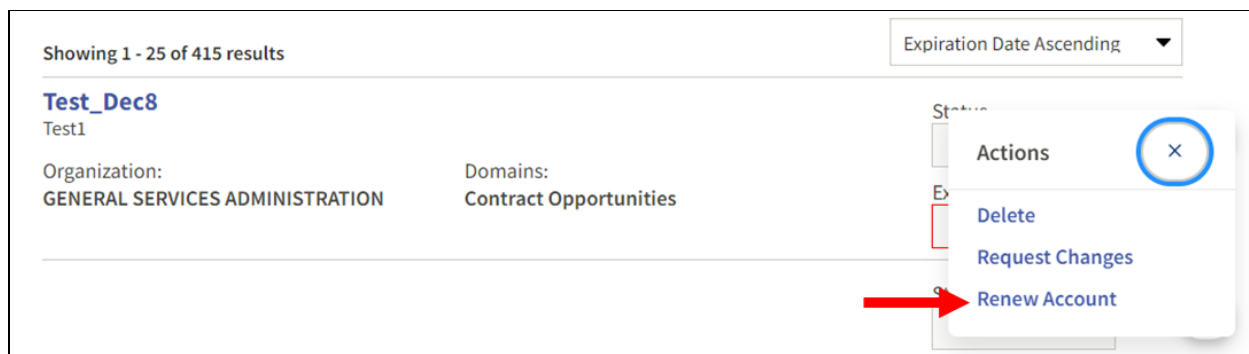
1. Sign in to SAM.gov with the account associated with the system account.



2. Navigate to your Workspace from the header on any page.
3. Select System Accounts from the widgets to go to your Tier 2 Workspace for System Accounts.



4. Use any of the filters to search your system accounts for the account which needs to be renewed. Alternatively, you can select the link provided in the email notification that you received to view the details of the System Account that needs to be renewed.
5. In the Actions drop down menu, you will have an option to Renew Account only when your account is within 60 days of needing to renew. Select this option to renew your account.



Selecting Renew Account will allow you to review the account details and submit the system account renewal for approval. If you wish to edit the details for any of the sections, you can select the edit button to make changes and then submit for approval.

✓ System Information

✓ Organization Information

✓ Permissions

✓ Security Information

✓ Authorization

WORKSPACE

Test\_Dec8

Complete and submit this form to request a new system account. All fields are required for security review to establish your account, unless marked as optional.

Change Request

Edit

Review

Actions ▼

System Account Name

Provide a unique name for your new system account.

Test\_Dec8

Interfacing System Name and Version

Provide the name and version of the system that will be connecting to SAM.gov.

Test1

System Description and Function

Example: The IRS stated in a current MOU that their system tracks all incoming commitment requests and captures the information necessary to make awards.

Test1

Cancel

Next

You will receive a notification in your email when the account receives final approval or rejection. When you sign in to SAM.gov again and look in your system accounts, you will notice that the expiration date has been extended another year and the account is renewed.

## System Account Deactivation

If your system account shows a “Deactivated” status, you will need to take action to restore your connection from your system to SAM.gov APIs.

At the time of deactivation, the system account API key, system account password, and other authentication methods are blocked and cannot be used.

Deactivated status does *not* mean your account is locked; it is permanently deactivated and a connection cannot be reinstated without a new system account request.

Following are reasons an account may be deactivated and what you can do.

Deactivation Cause	Your Next Steps
Someone with permission chose to deactivate the account.	If you wish to re-establish a connection between your system and SAM.gov, <a href="#">request a new system account</a> .
Your ATO is no longer in effect.	<ol style="list-style-type: none"> <li>1. Verify the state of your systems ATO, and retrieve the updated version from your IT department, if necessary</li> <li>2. Create a <a href="#">new System Account Request</a></li> </ol>
Someone with permission submitted a change request for the system account.	This action automatically creates a new system account, and deactivates the old one once the updated account is published. <a href="#">Use the new account created as a result of the change request instead.</a>

To research the system account deactivation further, view the system account history (if your ATO is still active). Otherwise, please reach out to other system account administrator(s) at your non-federal entity or federal agency.

**This concludes the information about managing system accounts.**



## For More Help

### Help Resources

- [Troubleshoot](#) issues with system accounts, system account API keys and individual account API keys
- [System Account FAQs](#)
- [Individual Account API FAQs](#)
- [Training Videos](#)
- Conduct your own [keyword search](#)

Chat or Create a Help Desk Ticket at [FSD.gov](https://fso.dhs.gov)

**Did you know that providing the right information in your initial FSD ticket helps reduce the time to helping you?** Without the need to call back and forth, the helpdesk can investigate sooner and respond more quickly.

Please include as much of the following as possible on your FSD Help Desk tickets:

1. State whether it's a public API key or a system account API key you are having trouble with
2. Provide your account user name
3. Provide your account email
4. Provide the actual FULL API key (copy and paste into ticket or send a screenshot)

### Troubleshooting

- Always read emails sent to you about individual accounts and API keys and system accounts and API keys. When you receive an email, look for which of your accounts it references.
- It's best practice to retrieve your API key on the first day of the 15 day rotation window, when you receive the notification email.
- If your individual account API key becomes out of date before you have retrieved the replacement, you can still retrieve your replacement API Key from the "Workspace" page under "Profile" in your SAM.gov any time. The replacement key will take effect immediately.

- If your system account API key becomes out of date before you have traded the current one out in your connected system, you can still retrieve your replacement system account API Key from the System Account page and replace it at any time to reconnect to your system account. The replacement key will take effect immediately.
- In the unlikely event that you receive a code 403 error, first make sure you are using the correct and up-to-date key. If the error persists, [open a ticket](#) with the Federal Service Desk as soon as you notice it.
- In the unlikely event that your key becomes out of date and another key has not been generated, **you can select Generate API Key on your system account page (for system account API key) or on your user account Profile page (for individual account API key) to manually generate a key.** This option is only available *after* your current key becomes out of date. Although this is not a common problem, if you must manually generate a new API key after your current one expires, please [report this issue to the FSD](#) so they can investigate how to ensure timely future auto-generation.
- Deactivated accounts are not “locked.” Your account will not become deactivated only because your password expired or you need to renew your account. You can investigate the action that caused the deactivation by viewing your account history. Only those with permissions in your (non-federal) entity, or permissions for a federal system account can deactivate a system account. Also ensure that your ATO is up to date and if not, file a new ATO for security review before requesting a new system account.

## Appendix A: Domain roles and permissions

Keep in mind that:

- As a non-federal user, you will have access to public data only.
- As a federal user, you will have access to both public and FOUO data.

The domain data sets and the permissions allowed within that domain are:

Domain	Permission	Definition
Contract Opportunities	Read Public	This permission grants access to the public APIs for active and inactive contract opportunity notices. Users already have access to view the public Contract Opportunity data on the site.
	Read Sensitive	This grants access for a system to obtain a read-only copy of all contract opportunities data for an organization in the federal hierarchy, to include published active and inactive notices, draft notices, and any sensitive but unclassified attachments. The system request must detail the business need for this level of access specific to accessing controlled but unclassified documentation that has been uploaded.
	Write Public	This grants access for a contracting office system to write (submit/post) contract opportunities data for a federal hierarchy organization to include published active and inactive notices and draft notices while excluding any sensitive but unclassified attachments. The system request must detail the business need for this level of access to post pre- or post-award contract actions, and must specify the contracting office(s).
	Write Sensitive	This grants access for a contracting office system to write (submit/post) contract opportunities data for a federal hierarchy organization to include published active and inactive notices, draft notices, and sensitive

		but unclassified attachments. The system request must detail the business need for this level of access to post pre- or post-award contract actions with controlled but unclassified documentation, and must specify the contracting office(s).
Contract Award Data (Coming Soon)	TBD	<i>Note: Contract award data is still authoritative in FPDS.gov, and is not yet available in SAM.gov.</i>
Entity Information	Read Public	Users already have access to view the public entity registration and exclusion data on the site. This permission grants access to APIs for public entity registration and exclusions data only.
	Read FOUO	Federal government users already have access to view FOUO information on the website when they log in using their federal government user account. This role additionally grants a federal government system access to FOUO information in the SAM FOUO extracts and APIs. FOUO information includes all public data plus non-public entity registrations, FOUO points of contact, Dun and Bradstreet (D&B linkage, D&B monitoring, and size metrics). The system request must detail the business need for this level of access to FOUO data.
	Read Sensitive	This role grants the federal government user access to sensitive registrant information using the SAM.gov website, extracts, and web services. Sensitive information includes all FOUO information plus the banking information for Electronic Funds Transfer (EFT) and TIN. The system request must detail the type of system (financial or contract writing), the business need to specifically view sensitive entity data, and the business need to access TIN data or EFT actions.
Federal Hierarchy	Read Public Only	Users already have access to view the public federal hierarchy data on the site. This permission grants access to the public APIs for active department and sub-tier federal hierarchy data only.

	Read FOUO	Federal government users already have access to view FOUO information on the website for their federal organization when they log in using their federal government user account. This permission additionally grants the federal government user access to FOUO information in the federal hierarchy API. FOUO information includes all public data plus the department through office-level data and full hierarchy lookups of active and inactive data, which includes both public and FOUO data. inactive notices, draft notices, and sensitive but unclassified attachments. The system request must detail the business need for this level of access to FOUO data.
Assistance Listings	Read Public	This grants access to the public API for active published assistance listings public data and the historical index for archived assistance listings.
Wage Determinations	Read Public	Users already have access to view the public wage determinations data on the site. This permission grants access to the public APIs for active published and inactive wage determinations Service Contract Act (SCA) and Davis-Bacon Act (DBA) public data only.
Reference Data	Read Public	This grants access to the public APIs for location services which shall only be used to validate data before sending contract opportunities to the site for fields such as the state, city, zip, and country.



## Appendix B: Account Request Preparation Checklist

You will need the following information to request your individual account API key, system account, or system account API key. Gathering this information in advance may make the process more efficient. Please consult the appropriate sections of this guide for full details.

For **both** individual accounts and system accounts:

- ☐ Decide whether you want to request an individual account API key using your individual account, or request a system account with system account API key
  - ☐ Review the [definitions](#) in this guide
  - ☐ Determine your [connection and rate limit](#) needs
  - ☐ Review available [permissions and roles](#) for the domains you want to connect to. Document the business need for the permissions and roles you want to request.
  - ☐ Review [interface specifications](#) on [open.gsa.gov](#)
- ☐ Keep track of which email address is associated with the account you request so you can receive all notifications.

For **federal system accounts** only, also include:

- ☐ Business needs for the information and the roles and permissions you're requesting a system account for.
- ☐ The system administrator for your area so you can follow up on your request as needed. Reminder: Do not contact the FSD for status updates on your request.
- ☐ The following for your [new system account request](#):
  - ☐ Name you want to give your system account
  - ☐ Full name and version number of the connecting system
  - ☐ Business reason for the connection type and rate level you're requesting
  - ☐ Your department/agency, sub-tier, or office
  - ☐ IP address of the account you want to establish
  - ☐ [Type of connection](#)
  - ☐ Physical location of the system
  - ☐ The name and email address of your agency Information System Security Officer (ISSO)
  - ☐ Supporting documentation for your request: Authority to Operate, Memorandum of Understanding, other approved documentation showing the connecting system meets security, privacy, and other federal standards for data access.

For **non-federal system accounts** only, also include:

- ☐ Name you want to give your system account
- ☐ Full name and version number of the connecting system
- ☐ Business reason for the data you're requesting, [connection type, and rate level](#)
- ☐ Entity information:
  - ☐ Entity: If this connection is for an entity with a current public entity registration, then you can input that entity. If this is not an entity with a current public registration, then you can leave this blank.
- ☐ Other System Account Holder: This is a mandatory field. You must enter the email address of another person associated with your entity. This user will be considered as the joint account holder for this account and will have permissions to manage this account. This user will also be the first-level approver for the account once you submit the account. You cannot enter your own email address in this field.

## Appendix C: Account Management Checklist

Below is a checklist to help you manage your individual account API key or system account and system account API key.

### At all times

- ☐ Know which email is associated with your account(s) so that you can get all related email notifications, approvals/denials, one-time temporary passwords, or password reset help.
- ☐ Read all emails about your accounts. Do not discard without fully reading and understanding the notifications. Make sure you understand which account the email was sent to address.
- ☐ If the details of your system account change, submit a [change request](#) right away.
- ☐ Keep track of important dates, such as:
  - system account renewal date, including if it changed when you updated information
  - system account password expiration dates
  - system account API key rotation dates
  - individual account API key rotation dates
- ☐ If your account becomes deactivated, view your account history and the [protocol](#) in this guide, or talk to another system account administrator to decide next steps.

### Every 90 Days

- ☐ Change your system account [password](#).
  - ☐ Watch your email for notification that your password will soon expire.
- ☐ For API Keys, begin using the rotated key provided in your SAM.gov account:
  - ☐ Watch your email for notifications that your API key will soon be replaced.
  - ☐ Retrieve your replacement individual account or system account API key as soon as it is auto-generated in your account (15 days before it is out of date).
  - ☐ [FOR SYSTEM ACCOUNTS ONLY](#): After you retrieve your replacement API key, you must rotate the current one in your system before it becomes out of date to avoid disconnection between your system and your SAM.gov system account.

### Annually

- ☐ [Renew](#) your system account.
  - This option is available within 60 days of the account renewal deadline.
  - Accounts must be renewed each year, one year from when they are approved.
  - The renewal date for an account may change if you submit a change request and it is approved. The new date will be one year from the approval of your change request.

## Appendix D: Glossary of Terminology

**Agency System:** A system managed by a federal agency. May connect to get or send SAM.gov data through APIs using a system account and system account API key.

**API Key:** An electronic code generated by SAM.gov for an individual account or system account that allows an API to connect and provide data.

**Connection:** Refers to sending and receiving HTTP requests or responses for data.

**Deactivate:** When a system account is deactivated, it cannot be reactivated. A deactivated account is not “locked.” The only way to re-establish connection between the system and SAM.gov is to request a new system account.

**Data Extract:** A way of viewing collections of data directly in the SAM.gov website. Any user can go directly to SAM.gov and initiate a search to view public data.

**Domain:** A domain is a functional area or set of related data in SAM.gov. Usually, domains are related to a former (legacy) system that was transitioned into SAM.gov. The names of the domains explain what type of data they are. For example, assistance listings is the name of the domain that lists federal financial assistance programs.

**Expiration/Expire:** Refers to the end of a password’s life. Passwords expire and must be reset every 90 days.

**FOUO:** For Official Use Only. Includes sensitive information about entities from SAM.gov such as TIN, EDI, etc. Note that only federal accounts can access For Official Use Only (FOUO) or Sensitive data permissions.

**Front End:** The part of a website you interact with as a user. All the things you see or use when you visit SAM.gov. Includes the look and feel, content, and how you navigate the website.

**GET call:** Refers to when data is being requested from a specific source, in this case, SAM.gov. If you are just pulling data, or using GET calls, then you will only need read permissions for the data (federal and non-federal users).

**Hierarchy:** An entity or agency’s structure within SAM.gov. Enables information about the organization to be kept within the access of the hierarchy (and not accessible to those not within the hierarchy).

- The federal hierarchy is the authoritative source for managing and referencing federal funding and awarding organizations. It is a directory that organizes federal government users and establishes relationships between each department or independent agency's sub-tiers and its offices.
- Civilian departments and independent agencies in the federal hierarchy have three levels: Department/independent agency, Sub-tier agency, Office.

**Individual Account:** The account you use to log in to the SAM.gov website. You can request an API key attached to your individual account.

**Individual Account API Key:** For individuals that need to connect data from SAM.gov, this allows a limited number of data transactions on a repeated basis.

**Interfacing System Name:** The name of the agency system or other system that will connect to SAM.gov through a system account.

**Interfacing System Version:** The version of the agency system or other system that will connect to SAM.gov through a system account.

**Office:** The lowest organizational level of a department/independent agency's federal hierarchy.

**Other System Account Holder:** A backup person designated as a system account contact in case the primary requester of that system account is unable to access it, leaves the organization, etc. This user will be considered the joint account holder for this account and will have permission to manage this account. This user will also be the first-level approver for the account once you submit the account.

**Permission:** A permission is tied to a specific role and allows a user to perform a specific task. Permissions may be configurable to the role.

**POST call:** Refers to when data is being processed to a specific source, in this case from you to SAM.gov. If you are writing, sending, or using post and put calls, then you will need write permissions (federal users only).

**Public:** Refers to a type of data or access to data in SAM.gov, in contrast to FOUO or Sensitive Data.

**Public API Key:** Another term for individual account API key; commonly used as a label on-screen in SAM.gov.

**PUT call:** A PUT method puts a file or resource at a specific place in a set of data. If a file or a resource already exists in that specific place, PUT replaces that file or resource. If no file or resource is there, PUT creates one. If you are writing, sending, or using post and put calls, then you will need write permissions (federal users only).

**Pull:** Refers to getting data from a source, in this case SAM.gov, with a limited number of requests per day.

**Rate Limit:** The number of allowed new connections in a specific timeframe (e.g. per second, minute, hour, day).

**Read permission:** refers to access to view data from a system (vs. writing or adding data to a system). If you are writing, sending, or using post and put calls, then you will need write permissions (federal users only).

**REST API:** “Representational State Transfer” API. An API that conforms to the principles of the REST architecture model, making it possible for you to receive a “representation” of the information you request when you use this API. REST APIs are available for connection and referenced on [open.gsa.gov](https://open.gsa.gov).

**Renewal:** Refers to the annual, required renewal of system accounts. Your password must be up to date when you begin your renewal so that you can use it to get into your system account and complete the renewal process.

**Rotation:** Refers to the rotation of individual account API keys and system account API keys every 90 days.

**Sensitive:** See *FOUO*.

**Service:** A modular application within SAM.gov that helps you interact with the tasks and information it represents. For example: Data Services is a service that encapsulates APIs, system accounts, data extracts, etc.

**Specification:** In this context, how an API behaves and connects with other APIs.

**Sub-Tier:** The first layer down within a department or independent agency in the federal hierarchy.

**System Account:** System accounts allow those seeking to connect their systems directly to SAM.gov through extracts or web services. They are used primarily for:

- Systems with the intent of regularly pushing or pulling large amounts of data
- Systems accessing non-public, For Official Use Only (FOUO) data (federal accounts only)
- Using a Contract Writing System (CWS)

A federal system account is for a system managed by a federal department or agency. As federal systems are allowed to request access to non-public data, there are additional access controls and security approvals needed that are integrated automatically into the request process.

**System Account API Key:** For any system that needs to connect to SAM.gov, this allows large data transactions on a repeated basis. There are two types of system accounts: federal and non-federal.

**System Account Administrator:** A role within SAM.gov that allows the person who has it to:

- Submit a request for a system account to the General Services Administration (GSA) for approval
  - Assign and approve roles for other people who will be managing your federal systems
- The administrator will receive emails about the system, including but not limited to system account renewals and API key rotation notifications.

**System Account Manager:** A role within SAM.gov that allows the person who has it to:

- Edit system accounts that you are responsible for
- Submit a request for a system account to be reviewed by the System Account Administrator

This role cannot assign or approve roles

The agency system administrator and GSA must approve the system account request before the system account can be created by GSA.

The manager will receive emails about the system, including but not limited to system account renewals and API key rotation notifications.

**System Account Name:** The unique name you choose for your requested system account so that you can tell it apart from other system accounts that will be visible within your hierarchy.

**System Account Password:** A password that provides access to a system account.

**System Account Role:** A role within SAM.gov that can work with system accounts and those who use them.

**System Description and Function:** A description provided within the system account request that describes the system that will connect to it and says what its function is.

**Tier 2 Workspace:** A page that shows further details about different widgets in your SAM.gov workspace.

**Validation:** While making a request, each section you complete will check to make sure that you've completed all required fields before you can continue to the next section.

**Widget:** A modular object in the SAM.gov workspace that shows information about a specific service, i.e. the System Account widget. Selecting the widget goes to the tier 2 workspace for that service.

**Workspace:** In SAM.gov, the workspace is a place in the website that shows services, widgets, and information you can interact with related to your account, profile, roles, services, etc.

**Write Permission:** refers to the ability to add and/or overwrite information in SAM.gov via a system account using an API connection. This is only permitted for federal system account users.