

Independent Dispute Resolution (IDR) Gateway



Administrator User Guide

Version 1.0
Release 1
August 2026

Table of Contents

1. Introduction	4
2. IDR Gateway Overview	5
2.1. The IDR Gateway	5
2.2. Development Phases	5
2.3. Who Should Sign Up	5
2.4. IDR Gateway Access Types	6
3. Identity Verification	7
3.1. Identity Verification Process	7
4. Create an IDR Gateway Account	8
4.1. Create an Account with a Credential Service Provider	8
4.2. Sign In with Existing CMS-Approved Credentials	9
4.3. First Time Sign In	10
5. Sign In to the IDR Gateway	14
6. Request Administrator Access	16
6.1. Administrator Responsibilities	16
6.2. Request Administrator Access	16
6.3. Create a New Organization	18
6.4. Join an Organization	21
6.5. Verify Organization Email Addresses	22
6.6. Leave an Organization	22
7. Manage Notifications	23
7.1. System Notifications	23
7.2. View Notifications from the Home Page	23
7.3. Filter and Search for Notifications	24
8. Manage Organization Information	26
8.1. Organization Information	26
8.2. Manage Organization Information	26
8.3. Add an Organization Email Address	27
8.4. Remove an Organization Email Address	27
8.5. Resend Email Address Verification Requests	28
9. Manage User Access	29
9.1. Permissions	29
9.2. Roles	29
9.3. Manage User Access	30
9.4. Download a User Report	31
9.5. Review Join Requests	32
9.6. Search/Filter Users	34
9.7. Edit User Access	34
10. Manage Workspaces	36
10.1. Workspaces	36
10.2. Workspace Examples	36
10.3. Create a Workspace	37
10.4. Add Users to a Workspace	38
10.5. Remove a User from a Workspace	40
10.6. Add an Email Address to a Workspace	41
Appendix A. Resources	43
IDR Gateway Help Desk Resources	43
IDR Resources	43
Appendix B. Warning and Security & Privacy Agreement	44
Appendix C. IDR Gateway Rules of Behavior	47
Appendix D. Administrator Quick Reference List	49
Appendix E. Acronyms & Terms	51

Table of Figures

Figure 1. IDR Gateway Access Page	8
Figure 2. Sign In/Create Your CMS Account Page.....	9
Figure 3. Warning and Security & Privacy Agreement	10
Figure 4. Rules of Behavior.....	11
Figure 5. Set Up Your Profile (Select Affiliation and Confirm Email)	12
Figure 6. Set Up Your Profile (Confirmation)	13
Figure 7. Sign In/Create Your CMS Account Page.....	14
Figure 8. Rules of Behavior.....	15
Figure 9. My Profile Page.....	16
Figure 10. Request Administrator Access (Administrator Access Process)	16
Figure 11. Request Administrator Access (Administrator Roles and Responsibilities)	17
Figure 12. Request Administrator Access (Join or Create an Organization).....	17
Figure 13. Create an Organization (Step 1 Organization Details)	18
Figure 14. Create an Organization (Step 2 Add Organization Emails).....	19
Figure 15. Create an Organization (Step 3 Confirm Organization Creation).....	20
Figure 16. Request Administrator Access (Find an Organization to Join)	21
Figure 17. Request Administrator Access (Find an Organization to Join, Search Results))	21
Figure 18. Email Verification Confirmation Banner	22
Figure 19. IDR Gateway Home Menu Bar	23
Figure 20. My Notifications Table	23
Figure 21. View All Notifications Button	24
Figure 22. My Notifications Page (All Active Tab).....	24
Figure 23. Organization Information Page	26
Figure 24. Organization Information Page (Organization Emails Table)	27
Figure 25. Organization Information Page (Organization Emails Table, Pending Tab)	28
Figure 26. Permissions Page.....	30
Figure 27. Permissions Page (Understanding Roles).....	30
Figure 28. Permissions Page (User Management Tab)	31
Figure 29. Permissions Page (User Management Tab, Download User Report Button)	31
Figure 30. Permissions Page (User Management Tab, Join Requests)	32
Figure 31. Review User Request	33
Figure 32. Permissions Page (User Management Tab, Approved Users)	34
Figure 33. Edit User	35
Figure 34. Workspace Example	37
Figure 35. Permissions Page (Workspace Management Tab).....	37
Figure 36. Create Workspace	38
Figure 37. Permissions Page (Workspace Management Tab, My Workspaces Table)	38
Figure 38. Workspace Page.....	39
Figure 39. Add Users	39
Figure 40. Workspace Page.....	40
Figure 41. Remove User	40
Figure 42. Add Emails.....	41

1. Introduction

Welcome to the IDR Gateway Administrator Guide

This user guide supports administrators of organizations. It provides the information and step-by-step instructions needed to create an administrator account, set up an organization within the Independent Dispute Resolution (IDR) Gateway, and manage permissions for users in your organization.

More features are coming soon.



The IDR Gateway is a sign-in community that provides a secure, centralized platform to manage payment disputes. It allows users to securely access all related disputes, submit necessary forms, and easily track progress through reports and dashboards.

What You'll Learn

This user guide provides information about how to:

- **Create an IDR Gateway Account.** Get started by setting up your account.
- **Sign In to the IDR Gateway.** Access the system with your credentials.
- **Request Administrator Access.** Gain administrator-level permissions to your organization or create your organization within the IDR Gateway.
- **Manage Notifications.** Manage notification settings to stay informed about updates or actions related to your organization.
- **Manage Organization Information.** Update and maintain accurate organization details.
- **Manage User Access.** Create user roles to control a user's ability to view and respond to disputes in your organization.
- **Manage Workspaces.** Create and manage workspaces to control user access to disputes associated with your organization.

Updated user guides are published on the CMS.gov IDR Gateway page with every IDR Gateway phase. Check back for information about new IDR Gateway features.

Let's get started!

2. IDR Gateway Overview

2.1. The IDR Gateway

The IDR Gateway is a sign-in community that transitions the Federal IDR process from single-use web forms to a secure, centralized platform that parties can use to manage disputes. IDR Gateway users will be able to:

- Start and respond to disputes.
- Access dispute dashboards and reports associated with their organization.
- Track dispute information, including disputes assigned to a certified IDR entity.
- Monitor assigned disputes by process phase.
- Review notifications regarding dispute activity.

The IDR Gateway includes important new security features, including identity verification processes and protocols that permit only U.S.-based users to access the Federal IDR process.

2.2. Development Phases

The IDR Gateway will roll out in phases. In Phase 1, administrators can sign up and set up their organizations in the IDR Gateway. In Phase 2, users who are responsible for submitting dispute web forms can sign up and join an organization. During these first two phases (the sign-up period), disputes in the Federal IDR process will continue to operate through the current web forms and not in the IDR Gateway.

Once the sign-up period is complete, the Federal IDR process will fully transition into the IDR Gateway (Phase 3), integrating existing web forms and introducing new dispute dashboards and reports. Parties will need an IDR Gateway account to submit web forms through the new IDR Gateway to continue participating in the Federal IDR process. Only users who have joined an organization can access the dispute dashboards and reports linked to their organization to track the status of their disputes.



IDR Gateway access is only available for individuals located in the U.S. and its territories. This system blocks users who try to access the IDR Gateway from outside the U.S. or its territories.

2.3. Who Should Sign Up

Within the IDR Gateway, an organization is considered any company or enterprise that manages dispute processing.

Organizations that handle dispute processing must create IDR Gateway accounts. If you or your staff currently submit IDR web forms in the current Federal IDR process, you must sign up to use the IDR Gateway.

Parties that handle some dispute processing, but also uses a third-party dispute processing organization to manage disputes, should also create an IDR Gateway account for the disputes they manage.

Do not create an IDR Gateway account if your organization is named in disputes but is not involved in the day-to-day management of disputes and relies on a third-party administrator (TPA) or other organization to manage dispute processing activities. The TPA or organization responsible for managing dispute processing activities must create an IDR Gateway account.

For example, if Dr. Smith uses Corporation A to manage Federal IDR disputes, Corporation A should set up an account, but Dr. Smith should not.

Important: The IDR Gateway does not have any features that link one organization to another.



If you are an administrator, make sure your staff know that you are their IDR Gateway administrator and you manage users and disputes. You are responsible for helping your staff join your organization in the IDR Gateway.

2.4. IDR Gateway Access Types

There are two types of access to the IDR Gateway: administrator and verified. After creating an account, your access type displays on the “My Profile” page. Although IDR Gateway administrators must have administrator access, they should also understand the verified access type to effectively manage user roles and access dispute information for their organization.

Verified Access

Users who successfully complete identity verification have verified access, which allows the user to start and respond to disputes, along with the ability to join an organization and access associated dashboards and reports.

Administrator Access

Administrators have the same abilities of verified users to start and respond to disputes and view dashboards and reports. Administrators are also responsible for creating organizations in the IDR Gateway, managing organization information, inviting users to join their organization, and managing user access.

Organizations must have at least one administrator but may have between 2–10 administrators depending on the size of the organization. It is recommended that organizations should have a sufficient number of administrators to ensure timely handling of user access requests and organization updates.

3. Identity Verification

All IDR Gateway users must verify their identity with an approved credential service provider during the account creation process. Individuals who do not verify their identity cannot access the IDR Gateway. This requirement helps to prevent fraud and unauthorized access.



A **credential service provider** is a trusted entity whose functions include identity proofing applicants and registering authenticators to subscriber accounts. A credential service provider may be an independent third party.

If new users have previously verified their identity through an approved credential service provider (e.g., Identity Management (IDM) service or Login.gov), they can log in to the IDR Gateway using those credentials. If they have not previously verified their identity, they must create a new account with an approved credential service provider and complete the identity verification process before they can sign in to the IDR Gateway.

3.1. Identity Verification Process

IDR Gateway users who do not already have an account with an approved credential service provider are required to create one. To create an account, you must:

- Sign up using your email address and create a secure password. You may also be asked to set up multi-factor authentication (MFA) for added security.
- Provide identifying information, such as your full name and Social Security Number (SSN) to confirm your identity.
- Verify your identity by submitting a photo ID. You can do this by uploading a photo of an approved ID type and submitting a “selfie” through the credential service provider’s website or application or bringing your approved ID to a location where it can be verified in person.

A credential service provider will use this information to verify your identity. Credential service providers may take different approaches to verifying identity. For details on how your information is used, refer to the credential service provider’s website.

If your identity is successfully verified, you will be able to access the IDR Gateway. If the verification fails, the credential service provider will suggest troubleshooting steps, and alternative verification options.

Credential service providers are responsible for protecting your information and keeping it secure. For more information refer to the credential service provider.

4. Create an IDR Gateway Account

All IDR Gateway users must create an account and complete the identity verification process with an approved credential service provider to log in to the IDR Gateway.

For the first phase of the IDR Gateway, administrators must access the “IDR Gateway Access” page from a link provided in an email from the Federal IDR Team.

- **New Credentials.** New IDR Gateway users without existing credentials must create an IDR Gateway account using an approved credential service provider (Refer to Section 3.1 Identity Verification Process).
- **Existing Credentials.** New IDR Gateway users with existing CMS-approved credentials (such as IDM) or an existing account with another credential service provider on the IDM Sign In page (such as Login.gov) can sign in to the IDR Gateway using those credentials.

4.1. Create an Account with a Credential Service Provider

1. Select the **IDR Gateway Account Creation** link from the **IDR Gateway Administrator Sign Up** email sent from IDRGatewayHelp@cms.hhs.gov. The “IDR Gateway Access” page opens in a browser.
2. Bookmark the “IDR Gateway Access” page to access the IDR Gateway in the future.

An official website of the United States government [Here's how you know](#)

U.S. Department of Health and Human Services
Enhancing the health and well-being of all Americans

OMB Control Number: 1210-0169 Expiration Date: 11/30/2025

IDR Gateway Access

Create an IDR Gateway Account
New users must create an account.

What is the IDR Gateway?

The IDR Gateway is a sign-in community that provides a secure, centralized platform to manage payment disputes. It allows users to securely access all related disputes, submit necessary forms, and easily track progress through reports and dashboards.

Get Started

If you already have a CMS Identify Management (IDM) account or an account through a different credential service provider available on the CMS IDM landing page (e.g., Login.gov), use your existing credentials to sign in. Do not sign up to create a new account with a different credential service provider.

Sign In

Sign in to the IDR Gateway using an existing account with a credential service provider (e.g., CMS IDM or Login.gov).

- Access to the IDR Gateway is only **available to individuals in the U.S. and its territories**.
- Sessions **time out after 30 minutes** of inactivity for security reasons.

[Sign In](#)

Sign Up

Step 1: IDR Gateway users who do not already have an account with an approved credential service provider are required to create one. To create an account, you must:

- Sign up using your email address and create a secure password. You may also be asked to set up multi-factor authentication (MFA) for added security.
- Provide identifying information, such as your full name and Social Security Number (SSN) to confirm your identity.
- Verify your identity by submitting a photo ID. You can do this by uploading a photo of an approved ID type and submitting a “selfie” through the credential service provider’s website or application, or bringing your approved ID to a location where it can be verified in person.

Step 2: Check your email for confirmation that your account was successfully created and your identity was verified.

Step 3: Sign in to the IDR Gateway to finish setting up your profile.

[Sign Up](#)

Need Help?

If you have questions about the IDR Gateway, email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059.
If you have questions about verifying your identity, contact the credential service provider you used to create your IDR Gateway account. Learn more about the verification process in the [user guide](#).

Figure 1. IDR Gateway Access Page

- From the “IDR Gateway Access” page, select the **Sign Up** button. The “Sign in/Create your CMS account” page displays.

Sign in/Create your CMS account

By signing in, you agree to the [terms and conditions](#).

Personal Identity Verification (PIV)
Existing CMS employees and contractors can securely sign in using their federal PIV card.

[Continue](#)

ID.me
For new and existing users that want to create an account or sign in with an existing ID.me wallet.

[Continue](#)

Login.gov
For new and existing users that want to create an account or sign in with existing Login.gov credentials.

[Continue](#)

EUA or IDM User ID
Existing users with active EUA or IDM credentials can sign in using their current account.

[Continue](#)

FAQs

How do I know which [sign in option](#) to choose?

Why does this [sign in page](#) look different?

Figure 2. Sign In/Create Your CMS Account Page

- Select the **Continue** button for your preferred credential service provider to start the account creation and identity verification process. During this process, you must create an account and verify your identity before you can access the IDR Gateway. Refer to [Section 3. Identity Verification](#) for more information about the identity verification process.
 - Do not create a new IDM account.
 - Do not use the PIV option.
- Upon account creation, continue to [Section 4.3. First Time Sign In](#).

4.2. Sign In with Existing CMS-Approved Credentials

- Select the **IDR Gateway Account Creation** link from the **IDR Gateway Administrator Sign Up** email sent from IDRGatewayHelp@cms.hhs.gov. The “IDR Gateway Access” page opens in a browser.
- From the “IDR Gateway Access” page, select **Sign In**. The “Sign In/Create your CMS account” page displays.
- Select the **Sign in** button for your credential service provider.
- Enter your credentials and select **Submit** to sign in to the IDR Gateway.
- Continue to [Section 4.3. First Time Sign In](#).

4.3. First Time Sign In

1. When signing in to the IDR Gateway for the first time, the Warning and Security & Privacy Agreement window opens.

The screenshot shows a web form titled "Warning and Security & Privacy Agreement". It is labeled "Step 1 of 4". The user is welcomed as "JOHN SMITH". A scroll bar is present to read the agreement. The agreement text includes a warning about U.S. Government Data, details about monitoring for security purposes, and a statement about HIPAA and other privacy laws. At the bottom, there is a checkbox for agreement, a "Continue" button, and a link to "Exit IDR Gateway".

Warning and Security & Privacy Agreement

Step 1 of 4

Welcome to the IDR Gateway, JOHN SMITH

Use the scroll bar to read and agree to the Warning and Security & Privacy agreement.

*Indicates a required field.

WARNING: This system contains U.S. Government Data and is only available to users in the U.S. and its territories. Unauthorized use of this system is prohibited.

This Federal IDR web form, including all information, documentation, and communications that are a part of the Federal IDR Portal, is provided only for authorized U.S. Government use. U.S. Government computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized U.S. Government entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

This system is subject to HIPAA and other federal and state privacy laws. Unauthorized access or misuse of this system may result in civil and criminal penalties.

Use of this computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may...

☐ *I have read and agree to the Warning and Security & Privacy Agreement.

[Continue](#) [Exit IDR Gateway](#)

Figure 3. Warning and Security & Privacy Agreement

2. Scroll down, read the agreement, and select the checkbox to agree to the terms. (The checkbox does not activate until you have reviewed the entire agreement.)

3. Select **Continue**. The Rules of Behavior window opens.

Rules of Behavior

Step 2 of 4

Rules of Behavior for Federal Independent Dispute Resolution (IDR) Gateway Users

Use the scroll bar to read and agree to the Rules of Behavior.

* Indicates a required field.

These *Rules of Behavior (RoB) for IDR Gateway Users* apply to all users who are granted access to Federal IDR process information, resources, and IT systems through the IDR Gateway. The IDR Gateway provides parties with a mechanism to engage with, track, and manage IDR payment disputes, including the submission of required information to start a dispute and upload of associated documents through web forms (e.g., Notice of Initiation [NOI], Selection/Reselection Response, and Notice of Offer [NOOF]) within a sign-in community. Users of the IDR Gateway must read, acknowledge, and adhere to the following rules prior to accessing data and/or documents and using the IDR Gateway.

A. The IDR Gateway

When using and accessing the IDR Gateway, I understand that I must:

1. Comply with federal laws, regulations, and the IDR Gateway policies, standards, and procedures and that I must not violate, direct, or encourage others to violate these policies, standards, or procedures. Not allow unauthorized use and access to the IDR Gateway information and resources. Not access the IDR Gateway information and resources outside the U.S. and its territories.
2. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing.

☐ * I have read and agree to comply with the **Rules of Behavior for IDR Gateway Users**.

[Continue](#) [Exit IDR Gateway](#)

Figure 4. Rules of Behavior

4. Scroll down, read the agreement, and select the checkbox to agree to the terms. (The checkbox does not activate until you have reviewed the rules.)

5. Select **Continue**. The Set Up Your Profile window opens.

Figure 5. Set Up Your Profile (Select Affiliation and Confirm Email)

6. Select your affiliation from the following options to indicate how you engage with the Federal IDR process:
- Provider, Health Care Facility, or Air Ambulance Provider
 - Group Health Plan, Individual Health Insurance Issuer, or Federal Employees Health Benefits (FEHB) carrier



You only need to indicate your affiliation the first time you sign in to the IDR Gateway.

7. Confirm the displayed email address you used to login is the email address you would like to use for IDR Gateway notifications.
- If you select “No”, a field displays to provide an additional email address to receive IDR Gateway notifications. **Do not use a shared inbox as your IDR Gateway notification email.**
 - If you entered an email address for IDR Gateway notifications, you must verify the email address before you can request administrator access or join an organization. Select the verification link in the email message from auto-reply-federalidrquestions@cms.hhs.gov and sign in to the IDR Gateway.



If you enter a shared inbox as your IDR Gateway Notification email address, only you can verify that email address. Anyone else who attempts to verify that email address will receive a “Not Authorized” error message.

8. Select **Continue**. The Profile setup confirmation displays.

Set Up Your Profile

Step 4 of 4

Your profile is set up! ✓

You have **verified** user access.

Join an Organization

Select **Continue to My Profile** to join an organization.

[Continue to My Profile](#) [Home](#)

Figure 6. Set Up Your Profile (Confirmation)

9. Select the **Continue to My Profile** button to request administrator access. Refer to [Section 6. Request Administrator Access](#).
 - a. If you have an existing CMS-approved account but your credential service provider did not verify your identity, a Verify Your Identity alert displays.
 - b. Refer to [Section 4.1 Create an Account with a Credential Service Provider](#) to complete the identity verification process for your credential service provider.

5. Sign In to the IDR Gateway

After creating an IDR Gateway account, and signing into the IDR Gateway for the first time, you can sign in to the IDR Gateway from the “IDR Gateway Access” page.

1. Navigate to the “IDR Gateway Access” page by selecting the link in the email inviting you to join the IDR Gateway as an administrator or opening the bookmark you created when you first signed in to the IDR Gateway.
2. Select the **Sign in** button. The “Sign In/Create your CMS account” page displays.

Sign in/Create your CMS account

By signing in, you agree to the [terms and conditions](#).

 **Personal Identity Verification (PIV)**
Existing CMS employees and contractors can securely sign in using their federal PIV card. [Continue](#)

 **ID.me**
For new and existing users that want to create an account or sign in with an existing ID.me wallet. [Continue](#)

 **Login.gov**
For new and existing users that want to create an account or sign in with existing Login.gov credentials. [Continue](#)

 **EUA or IDM User ID**
Existing users with active EUA or IDM credentials can sign in using their current account. [Continue](#)

FAQs

[How do I know which sign in option to choose?](#)

[Why does this sign in page look different?](#)

Figure 7. Sign In/Create Your CMS Account Page

3. Select the **Continue** button for the credential service provider you used to create an IDR Gateway account. By signing in, you agree to the terms and conditions.

4. Enter your credentials and select the **Submit** or **Sign in** button (depending on the credential service provider) to sign in to the IDR Gateway. The Rules of Behavior window opens.

Rules of Behavior

Rules of Behavior for Federal Independent Dispute Resolution (IDR) Gateway Users

Use the scroll bar to read and agree to the Rules of Behavior.

* Indicates a required field.

These *Rules of Behavior (RoB) for IDR Gateway Users* apply to all users who are granted access to Federal IDR process information, resources, and IT systems through the IDR Gateway. The IDR Gateway provides parties with a mechanism to engage with, track, and manage IDR payment disputes, including the submission of required information to start a dispute and upload of associated documents through web forms (e.g., Notice of Initiation [NOI], Selection/Reselection Response, and Notice of Offer [NOOF]) within a sign-in community. Users of the IDR Gateway must read, acknowledge, and adhere to the following rules prior to accessing data and/or documents and using the IDR Gateway.

A. The IDR Gateway

When using and accessing the IDR Gateway, I understand that I must:

1. Comply with federal laws, regulations, and the IDR Gateway policies, standards, and procedures and that I must not violate, direct, or encourage others to violate these policies, standards, or procedures. Not allow unauthorized use and access to the IDR Gateway information and resources. Not access the IDR Gateway information and resources outside the U.S. and its territories.
2. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing.

☐ * I have read and agree to comply with the **Rules of Behavior for IDR Gateway Users**.

[Continue](#) [Exit IDR Gateway](#)

Figure 8. Rules of Behavior

5. Scroll down, read the agreement, and select the checkbox to agree to the terms. (The checkbox does not activate until you have reviewed the rules.) The “IDR Gateway Home” page displays. Every time you sign in to the IDR Gateway, you must review and agree to the rules of behavior.

6. Request Administrator Access

After creating an account as a verified user, organization administrators must request administrator access to their organization or create their organization within the IDR Gateway if it has not already been created.

6.1. Administrator Responsibilities

Administrators must join or create an organization to serve as an administrator. Verified users requesting administrator access to an organization within the IDR Gateway must acknowledge and adhere to specific administrator roles and responsibilities. By accepting these responsibilities, administrators confirm they will manage the information, user access, and disputes for their organization within the IDR Gateway, and ensure compliance with all policies and guidelines.

6.2. Request Administrator Access

1. From the Home menu bar, select the My Profile option from the user menu dropdown list. The “My Profile” page displays.

The screenshot shows the 'My Profile' page. At the top, there's a navigation bar with 'Home' and a user menu for 'JOHN SMITH'. Below the navigation bar, the page title is 'My Profile'. A section titled 'Profile Information' contains a table with the following data:

Current Access:	First Name:	Last Name:	Phone:	IDR Gateway Credential Email:	IDR Gateway Notification Email:
Verified	John	Smith	555-555-5555	john.smith@test.org	john.smith@test.org

Below this, there's a section titled 'IDR Gateway User Access Type Information'. It states: 'The IDR Gateway offers various user access types. Your current access type is highlighted below. Learn more about access types in the user guide (link in the menu bar).' There are two access types listed:

- Verified:** (highlighted with a green border and a green checkmark icon)
 - Can start and respond to disputes.
 - Can join an organization and access the dispute dashboards and reports associated with the organization.
- Administrator** — Verified access plus:
 - Can set up and update organization information.
 - Can invite users, manage user access and manage disputes on behalf of the associated organization.

A link 'Request Administrator Access' is provided at the bottom of the Administrator section.

Figure 9. My Profile Page

2. Select the **Request Administrator Access** link. The Request Administrator Access window opens.

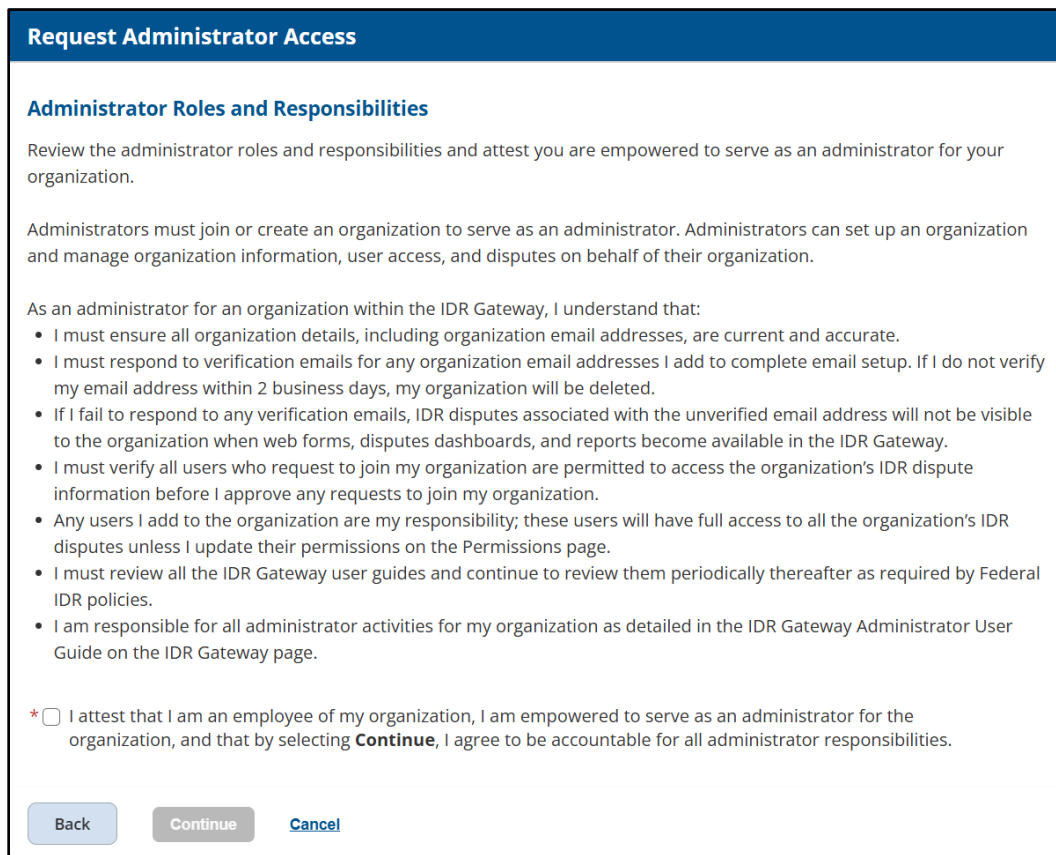
The screenshot shows a modal window titled 'Request Administrator Access'. Inside, there's a section titled 'Administrator Access Process' with the following steps:

1. Review and attest. Read and agree to the Administrator Roles and Responsibilities.
2. Join an organization. Search for and join an existing organization or create a new organization.
3. Confirm and submit. Verify the organization details and submit your administrator request.

At the bottom of the window, there are two buttons: 'Continue' (highlighted in blue) and 'Cancel'.

Figure 10. Request Administrator Access (Administrator Access Process)

3. Read the process to request administrator access and select **Continue**. The Administrator Roles and Responsibilities display.



Request Administrator Access

Administrator Roles and Responsibilities

Review the administrator roles and responsibilities and attest you are empowered to serve as an administrator for your organization.

Administrators must join or create an organization to serve as an administrator. Administrators can set up an organization and manage organization information, user access, and disputes on behalf of their organization.

As an administrator for an organization within the IDR Gateway, I understand that:

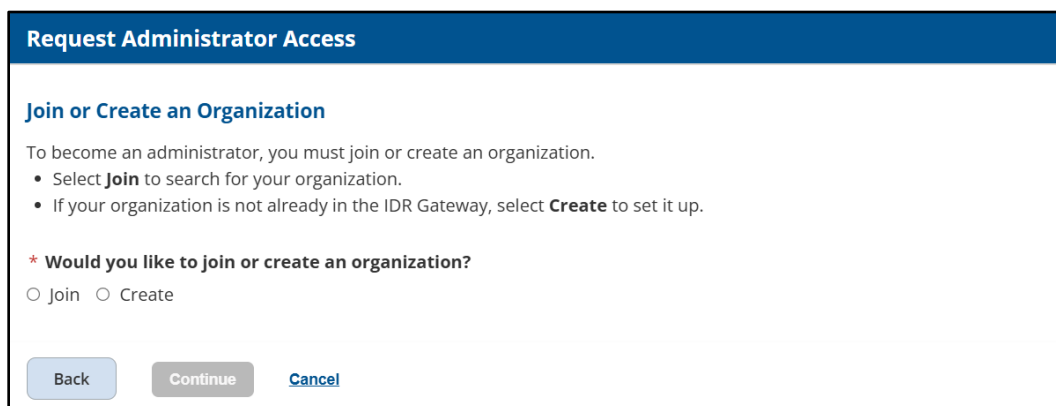
- I must ensure all organization details, including organization email addresses, are current and accurate.
- I must respond to verification emails for any organization email addresses I add to complete email setup. If I do not verify my email address within 2 business days, my organization will be deleted.
- If I fail to respond to any verification emails, IDR disputes associated with the unverified email address will not be visible to the organization when web forms, disputes dashboards, and reports become available in the IDR Gateway.
- I must verify all users who request to join my organization are permitted to access the organization's IDR dispute information before I approve any requests to join my organization.
- Any users I add to the organization are my responsibility; these users will have full access to all the organization's IDR disputes unless I update their permissions on the Permissions page.
- I must review all the IDR Gateway user guides and continue to review them periodically thereafter as required by Federal IDR policies.
- I am responsible for all administrator activities for my organization as detailed in the IDR Gateway Administrator User Guide on the IDR Gateway page.

* ☐ I attest that I am an employee of my organization, I am empowered to serve as an administrator for the organization, and that by selecting **Continue**, I agree to be accountable for all administrator responsibilities.

[Back](#) [Continue](#) [Cancel](#)

Figure 11. Request Administrator Access (Administrator Roles and Responsibilities)

4. Read the administrator roles and responsibilities and select the **checkbox** to indicate you are authorized to serve as an administrator for your organization, and you understand the administrator responsibilities.
5. Select **Continue**. The Join or Create an Organization information displays.



Request Administrator Access

Join or Create an Organization

To become an administrator, you must join or create an organization.

- Select **Join** to search for your organization.
- If your organization is not already in the IDR Gateway, select **Create** to set it up.

* Would you like to join or create an organization?

☐ Join ☐ Create

[Back](#) [Continue](#) [Cancel](#)

Figure 12. Request Administrator Access (Join or Create an Organization)

6. Continue to [Section 6.3 Create a New Organization](#) or to Section [6.4 Join an Organization](#), as required.

6.3. Create a New Organization

To create a new organization in the IDR Gateway, administrators must enter the organization information and all the email addresses used by the organization to process IDR disputes. Administrators must enter a dispute processing email address and may enter additional email addresses associated with the organization. The email addresses are used to ensure submitted disputes tie back to the organization in the IDR Gateway.

1. From the Join or Create an Organization window, select the **Create** option to create a new organization within the IDR Gateway.
2. Select **Continue**. The Create an Organization information displays.

Request Administrator Access

Create an Organization

Step 1 of 3: Organization Details

* Indicates a required field

* Organization Name: Organization Name	* Address Line 1: Street address
* Tax ID: Enter nine-digit number	Address Line 2: Apartment, Suite, etc.
* Organization Affiliation: Select	* City: City
Organization Phone: XXX-XXX-XXXX	* State: Select
	* ZIP Code: Zip code

[Cancel](#)

Figure 13. Create an Organization (Step 1 Organization Details)

3. Enter the required organization information, indicated by an asterisk.

4. Select **Continue**. The Create an Organization information displays.

Request Administrator Access

Create an Organization

Step 2 of 3: Add Organization Emails

Add organization email addresses to link related disputes in the IDR Gateway.

1. Enter the email address used by the organization for IDR disputes.
2. Enter additional dispute processing emails.
3. To request future changes to or remove organization emails later, email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059.

* Indicates a required field

* **Primary Dispute Processing Email:**

Additional Dispute Processing Emails:

[Back](#) [Continue](#) [Cancel](#)

Figure 14. Create an Organization (Step 2 Add Organization Emails)

5. From the **Dispute Processing Email** field, enter the email address used by the organization to process IDR disputes.
 - a. You must verify this email address to complete organization creation.
 - b. The request and approval to create the organization must occur before verification emails are sent.
6. Add additional dispute processing email addresses in the **Additional Dispute Processing Emails** field.

7. Select **Continue**. The Review and confirm organization details displays.
 - a. If an error indicates the organization already exists, refer to [Section 6.4. Join an Organization](#).
 - b. If an error indicates organization setup is already in progress, another user is trying to set up an organization with the same email address. You must wait until the organization is created and then join the organization when it is available.

Request Administrator Access

Create an Organization

Step 3 of 3: Review

Confirm Organization Creation

1. Confirm Details. Review the organization details carefully before creating the organization.

2. Check Your Inbox. The Federal IDR Team will email a verification link to each address.

3. Verify Emails. Click the link to verify each email. Links expire in two business days.

Organization Details

Organization Name:	Tax ID:	Organization Phone:	Address:
XYZ Health Test	35-2246158	555-555-5555	123 High Street Anycity, CA 55555

Affiliation:
 Provider, Health Care Facility, or Air Ambulance Provider

Organization Emails

Primary Dispute Processing Email:	Additional Dispute Processing Emails:
health@test.org	healthgroupa@test.org healthgroupb@test.org

If everything is correct, select **Create Organization**.

Back

Create Organization

Cancel

Figure 15. Create an Organization (Step 3 Confirm Organization Creation)

8. Confirm the organization details and organization emails are correct.
9. Select the **Create Organization** button.
 - a. The organization is created in the IDR Gateway.
 - b. An email is sent to verify the dispute processing email address and any additional email addresses entered.



Administrators must verify all email address within **two business days**. If the dispute processing email address is not verified, the organization is deleted. If additional email addresses are not verified, they are deleted from the organization.

6.4. Join an Organization

1. From the Join or Create an Organization window, select the **Join** option to search for and join your organization within the IDR Gateway.
2. Select **Continue**. The Find an Organization to Join information displays.

Request Administrator Access

Find an Organization to Join

To find your organization, enter an email address used by the organization to manage IDR disputes. If you don't know which email address to use, contact your organization administrator.

Search for Your Organization

Q Enter email address Search

Back Join Organization [Cancel](#)

Figure 16. Request Administrator Access (Find an Organization to Join)

3. Enter an email address used by the organization to manage IDR disputes in the **Search for Your Organization** field.
4. Select **Search**. The organization linked to the email address displays.
5. If your organization is found, select the **Join Organization** button.
 - a. If your organization is not found, verify you entered the correct email address. If the email address is correct, the organization does not exist yet in the IDR Gateway. Proceed to [Section 6.3. Create a New Organization](#).
 - b. If the “Organization setup in progress” alert displays, another user has requested the creation of an organization with the information you provided. Wait until the organization setup is complete, which could take up to two days, and then request to join the organization.
 - c. If you believe there is an error, contact IDRGatewayHelp@cms.hhs.gov.

Request Administrator Access

Find an Organization to Join

To find your organization, enter an email address used by the organization to manage IDR disputes. If you don't know which email address to use, contact your organization administrator.

Search for Your Organization

Q health@test.org Search

Search result found

Tax ID:	35-2246158
Organization Name:	XYZ Health Test
Organization Address:	123 High Street Anycity, CA 55555

Back Join Organization [Cancel](#)

Figure 17. Request Administrator Access (Find an Organization to Join, Search Results))

6. An administrator must review your request to join the organization as an administrator.
 - a. You will be notified when a decision is made.
 - b. Once your request to join an organization is approved, you can access organization details from the “Organization Information” page.

6.5. Verify Organization Email Addresses

Administrators must verify within **two business days** all dispute processing email addresses added when setting up the organization. If you fail to verify the dispute processing email address for the organization within two business days, the organization will be removed from the IDR Gateway. If you fail to verify the additional dispute processing email address within two business days, they will be removed from the organization.

1. Check your inbox for an email from the Federal IDR Team with a unique verification link that expires in two business days.



All email addresses must be verified before the organization can process disputes associated with those email addresses.

2. Select the verification link in the email. The “IDR Gateway Access” page opens in a browser.
3. Select **Sign in**. The “Login/Create your CMS account” page displays.
4. Sign in to the IDR Gateway using your credentials. A confirmation displays indicating the organization was successfully created.

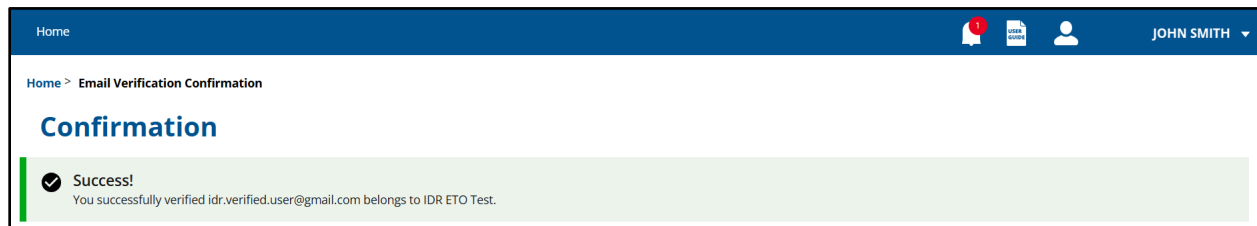


Figure 18. Email Verification Confirmation Banner

6.6. Leave an Organization

If you are the only administrator for your organization, you must assign administrator access to another user within the organization, and the new administrator must complete the administrator access process before you can leave the organization.

1. From the Home menu bar, select the **My Profile** option from the user menu dropdown list. The “My Profile” page displays.
2. In the “My Organization” section, select the **Leave Organization** button.
 - a. If you are the only administrator in the organization, refer to the steps in [Section 9.7. Edit User Access](#) to provide another user with administrator access to the organization.
 - b. If you are unable to assign a new administrator, contact IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059 for help.
3. Review and revise your affiliation, if needed.
4. Select the **Confirm** button.

7. Manage Notifications

The Home menu bar at the top of every page provides easy navigation to the IDR Gateway “Home” page, the “Notification” page, the user guide, and a dropdown list under the user’s name with links to pages specific to the user.

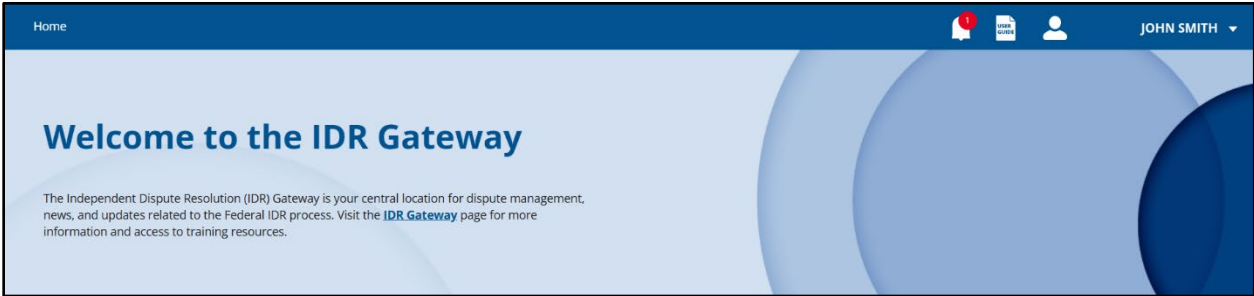


Figure 19. IDR Gateway Home Menu Bar

7.1. System Notifications

System notifications provide users with important updates or actions related to their administrator account or disputes. Users can view a summary of recent system notifications from the “Home” page or detailed notification information on the “My Notifications” page.

7.2. View Notifications from the Home Page

1. From the Home menu bar, select the **Home** button. The “IDR Gateway Home” page displays.
2. Scroll down to view the My Notifications table.
 - a. Notifications are organized by the date they are received.
 - b. If a system notification has a supporting email, the notification summary matches the email subject line.
 - c. Notifications are marked as read when the user views the notification. Dispute and organization notifications, which display for multiple users, are marked as read when the first user views the notification.
 - d. Users can manually mark the notification as unread again for other users associated with the organization.

Summary	Received Date ↓
☐ You successfully verified this email address belongs to XYZ Health Test in the IDR Gateway.	Jul 21, 2026, 02:24 PM
☐ Administrator Review Required: Verify this email address belongs to XYZ Health Test within two business days.	Jul 21, 2026, 02:22 PM
☐ IDR ETO Test created! Verify this email address belongs to XYZ Health Test in the IDR Gateway	Jul 21, 2026, 02:22 PM
☐ Welcome to the IDR Gateway! Join an organization to finish setting up your profile. Join an organization	Jul 21, 2026, 11:20 AM

Figure 20. My Notifications Table



Notifications older than 30 business days are automatically archived.

3. Select the checkbox next to a notification to enable the **Mark as Read**, **Mark as Unread**, and **Archive** buttons.
 - a. Select **Mark as Read** to unbold the notification title in the Summary column. Notifications will also be marked as read once opened.
 - b. Select **Mark as Unread** to bold the notification title in the Summary column.
 - c. Select **Archive** to remove the notification title from the Summary column.

7.3. Filter and Search for Notifications

1. From the Home menu bar, select the **Notifications (bell icon)**. The **View All Notifications** button displays.

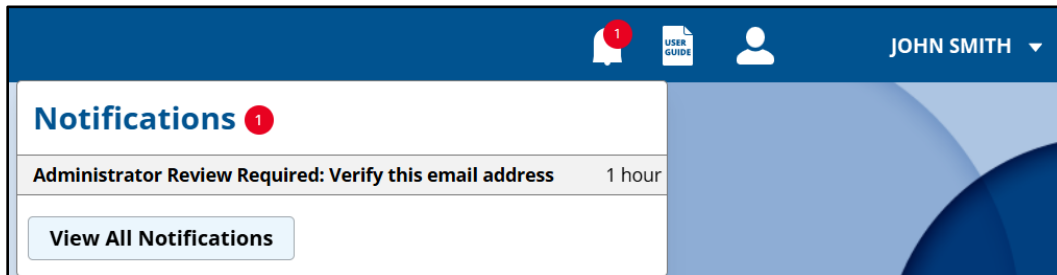


Figure 21. View All Notifications Button

2. Select the **View All Notifications** button. The “My Notifications” page displays.

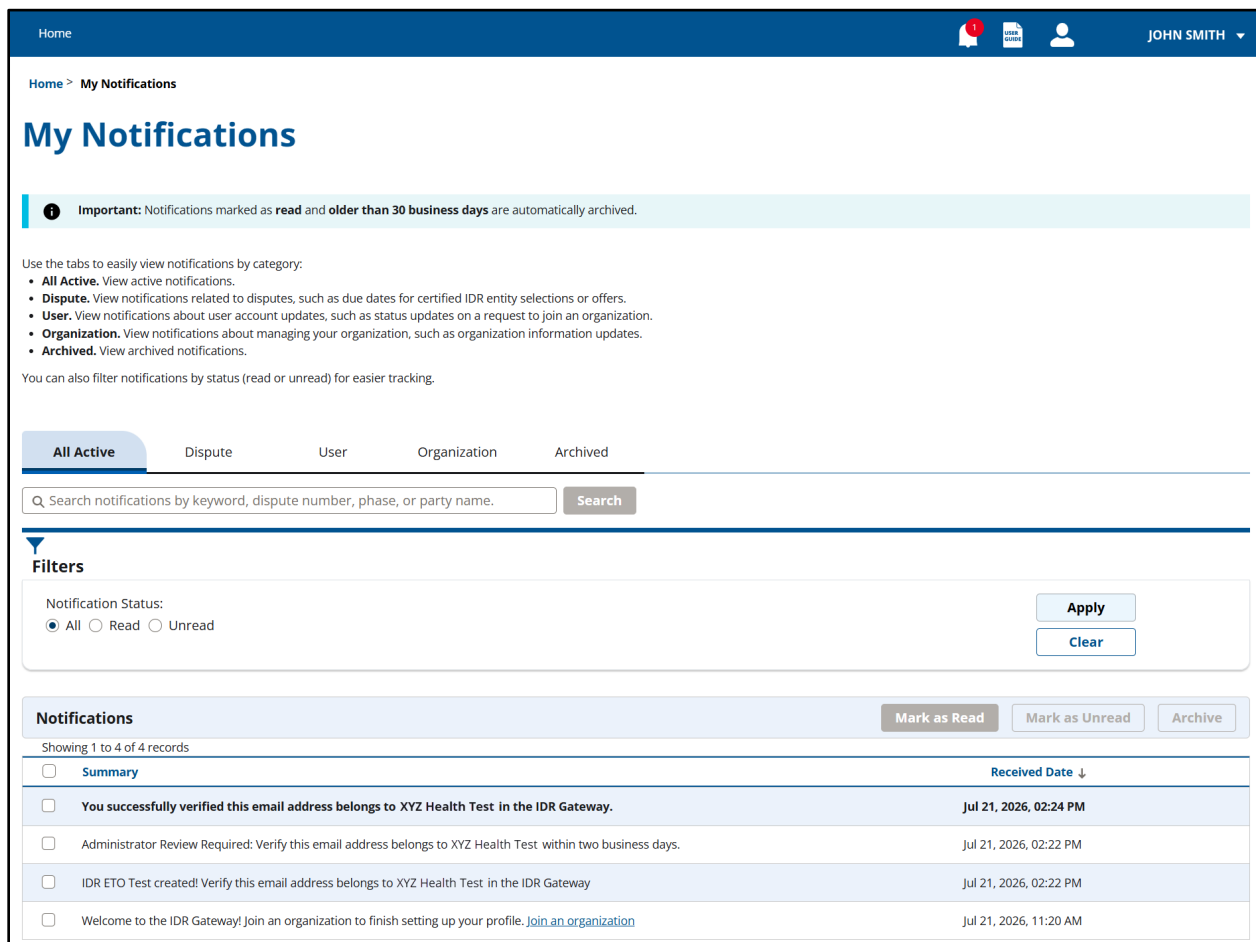


Figure 22. My Notifications Page (All Active Tab)

3. Select a tab to filter the notifications by type.
 - a. **All Active.** View all active notification types (Dispute, User, and Organization). Active notifications include both read and unread notifications that have not been archived.
 - b. **Dispute.** View notifications related to disputes, such as due dates for selecting a certified IDR entity to manage the dispute or to submit offers.
 - c. **User.** View notifications about an individual user's account updates, such as status updates on a request to join an organization or become an administrator.
 - d. **Organization.** View notifications for administrators about managing the organization, such as changes to organization information or due dates to verify organization emails.
 - e. **Archived.** View archived notifications. Archived notifications are older than 30 business days or have been archived by a user using the **Archive** button.
4. Select a **Notification Status** option (All, Read, Unread) to filter notifications by status.
5. Enter at least three characters of a keyword, dispute number, or party name to search for a notification.
6. Select the **Apply** button to display the resulting notifications.

8. Manage Organization Information

8.1. Organization Information

The “Organization Information” page provides administrators with an area to manage information about their organization, including the email addresses used by the organization to process disputes.

8.2. Manage Organization Information

1. From the Home menu bar, select the **Organization Information** option from the user menu dropdown list. The “Organization Information” page displays.

Home > Organization Information

Organization Information

As an administrator for this organization, you can manage your organization's details and add new dispute processing email addresses on this page. To edit the organization name, tax ID, or dispute processing emails addresses, contact IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059.

▼ My Organization Information

Organization Name ⓘ XYZ Health Test	Street Address 123 High Street	✎
Tax ID ⓘ 582693471	City Anycity	✎
Email ⓘ health@test.org	State California	✎
Phone (654) 321-7411	Zip Code 99901	✎
Affiliation Provider, Health Care Facility, or Air Ambulance Provider		✎

Figure 23. Organization Information Page

2. To edit organization name, tax ID, or dispute processing email addresses, contact IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059 for help.
3. Select **edit** (pencil icon) to the right of a field to edit the information in that field. Administrators can modify the following fields:
 - a. Phone
 - b. * Affiliation
 - c. * Address Line 1
 - d. Address Line 2
 - e. * City
 - f. * State
 - g. * ZIP Code
4. Update the information and select **Save**. The updated information displays in the “My Organization Information” section.

8.3. Add an Organization Email Address

Administrators must enter the email address used for processing IDR disputes when setting up the organization and then verify the address within **two business days**. If the dispute processing email address is not verified within two days, the organization is deleted from the IDR Gateway.

Additional email addresses can be added to the organization at any time. Adding and verifying the additional email addresses allows the organization to view and manage disputes associated with those email addresses. If the additional dispute processing email addresses are not verified within two business days from the date they are added to the organization, the email addresses will be removed from the organization.

1. From the Home menu bar, select the **Organization Information** option from the user menu dropdown list. The “Organization Information” page displays.
2. From the Organization Emails table, enter the organization’s email address in the **Enter Email Address** field.

The screenshot shows the 'Organization Emails' page. On the left is a sidebar with tabs: 'Verified' (selected), 'Pending', and 'Removed'. The main content area has a header with a note: 'If any of the email addresses listed below are no longer used by the organization for the Federal IDR process, email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059 with an email removal request.' Below this is a form with an 'Enter Email Address' input field and an 'Add Email' button. A table below the form shows 'Showing 1 - 1 of 1' and contains one row with the email address 'health@test.org' and the date '07/19/2026'.

Email Address	Date Verified
1 health@test.org	07/19/2026

Figure 24. Organization Information Page (Organization Emails Table)

3. Select the **Add email** button.
 - a. A verification email is sent to the organization email address. Follow the instructions in the verification email to verify the email address.
 - b. The email address displays as pending until verified. Once verified, the email address displays in the **Verified** tab list.

8.4. Remove an Organization Email Address

Administrators cannot remove organization email addresses.

Email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059 to remove or edit an organization email address. Removed email addresses display in the **Removed** tab on the Organization Emails table.

8.5. Resend Email Address Verification Requests

When needed, administrators can resend an email address verification request.

1. From the Home menu bar, select the **Organization Information** option from the user menu dropdown list. The “Organization Information” page displays.
2. Select the **Pending** tab on the Organizational Emails table.

The screenshot shows the 'Organization Emails' page with the 'Pending' tab selected. On the left is a sidebar with tabs: 'Verified', 'Pending' (active), and 'Removed'. The main content area has a header with a note: 'If any of the email addresses listed below are no longer used by the organization for the Federal IDR process, email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059 with an email removal request.' Below this is an 'Enter Email Address' input field and an 'Add Email' button. A table below shows 'Showing 1 - 1 of 1' records. The table has columns: 'Email Address', 'Verification Last Sent', and 'Actions'. One row is visible with email 'email@abchealth.com' and date '07/17/2026'. The 'Actions' column for this row contains a 'Resend' button.

Email Address	Verification Last Sent	Actions
1 email@abchealth.com	07/17/2026	<button>Resend</button>

Figure 25. Organization Information Page (Organization Emails Table, Pending Tab)

3. Select the **Resend** button from the Actions column.
 - a. A success message displays at the top of the page.
 - b. The email address remains in the **Pending** tab until verified. Once verified, the email address displays in the **Verified** tab.

9. Manage User Access

By default, users who join an organization have full access to all the organization's IDR disputes. However, administrators can control user access to the organization's disputes by managing user permissions from the **User Management** tab on the "Permissions" page.

9.1. Permissions

The "Permissions" page allows administrators to control the access users have to an organization's disputes in the IDR Gateway by managing user roles and workspace assignments. Only administrators can access the "Permissions" page.

The "Permissions" page is divided into four sections:

- **Understanding User Permissions.** Explains what administrators can do from the User Management and Workspace Management tabs to control access to disputes
- **Understanding Roles.** Explains the three user roles that modify a user's ability to view and respond to the organization's disputes
- **User Management.** Allows administrators to manage access at the user level by reviewing requests to join the organization, and updating user access types and roles
- **Workspace Management.** Allows administrators to create and manage workspaces, which are secure spaces that control the disputes a user can access

9.2. Roles

Roles control what actions users can take on disputes for the organization. When administrators review a user request to join the organization, they can select a role for the user. Administrators can also modify the user's role, as needed. Refer to [Section 9.7. Edit User Access](#).

Administrators can assign one of three role types to Gateway users:

- **View Only** roles may view all dispute information but cannot submit web forms.
- **Initiation and Selection** roles can submit initiation, certified IDR entity selection, and reselection web forms, but cannot submit offers or view dispute outcomes.
- **Full Access** roles can view all dispute information and submit all web forms.

By default, administrators are provided with full access roles given their responsibilities in the IDR Gateway. They cannot have view only or initiation and selection roles.

9.3. Manage User Access

From the **User Management** tab on the “Permissions” page, administrators can accept or deny requests to join their organization, assign roles, grant administrator access, assign users to workspaces, review denied requests to join the organization, remove access to the organization, and review users who have been removed from the organization.

1. From the Home menu bar, select the **Permissions** option from the user menu dropdown list. The “Permissions” page displays.

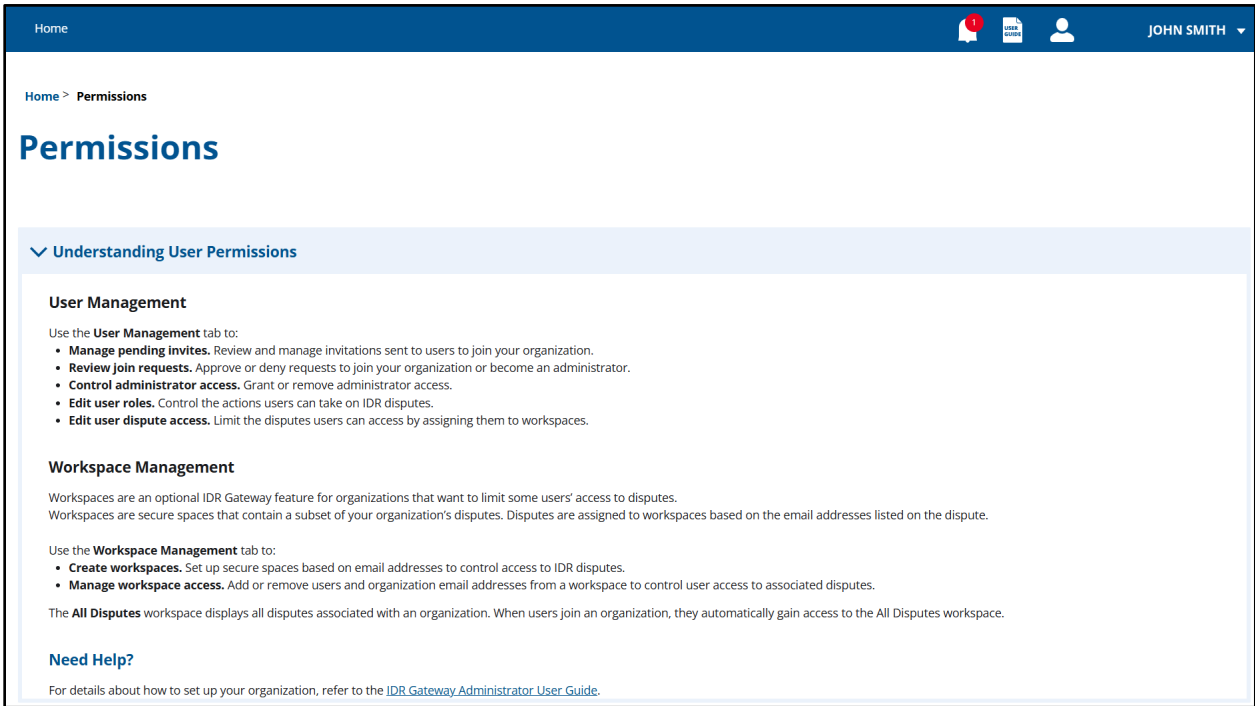


Figure 26. Permissions Page

2. Review the **Understanding User Permissions** section for information about the user management and workspace management features on the page.
3. Review the **Understanding Roles** section for information about the access permissions available for each role.

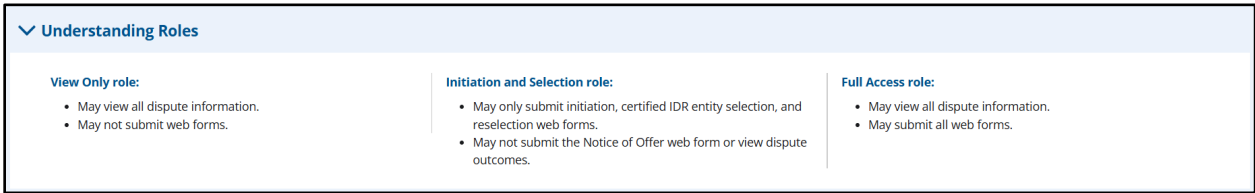


Figure 27. Permissions Page (Understanding Roles)

4. Select the dropdown arrows (caret symbol) to minimize the information sections.

5. Select the **User Management** tab. The My Users table displays.

The screenshot shows the 'User Management' tab with the 'Organization User Summary' section. It displays statistics: 3 Total Users, 1 Administrator, 2 Verified, 1 Total Pending, 0 Pending Invites, 1 Join Requests, and 0 Denied/Removed. Below this is the 'My Users' section with a search bar and filters for Workspaces and Role. A table with columns: Last Name, First Name, Email, Role, Workspace, Sent Date, and Actions is visible. A note states: 'Administrators may invite users starting Month/Year of Release 2'.

Figure 28. Permissions Page (User Management Tab)

9.4. Download a User Report

Administrators can download a comma-separated values (CSV) report of the information found in the My Users table.

1. From the **User Management** tab, select the **Download User Report** button in the "Organization User Summary" section.
2. Follow the prompts to download the file to your computer's designated download location or choose a new location.
3. Verify that the download is complete and the file is available in the designated folder.
4. Re-name and save as needed.

This screenshot is identical to Figure 28, showing the 'User Management' tab and the 'Organization User Summary' section. The 'Download User Report' button is highlighted in the top right corner of the summary section.

Figure 29. Permissions Page (User Management Tab, Download User Report Button)

9.5. Review Join Requests

Administrators can accept or deny requests to join their organization from the Join Requests table option.

1. From the **User Management** tab, select the **Join Requests** table option in the navigation panel. The users requesting to join the organization display in the table.

The screenshot displays the 'User Management' tab with the 'Join Requests' sub-tab selected. The 'Organization User Summary' section shows statistics: 3 Total Users, 1 Administrator, 2 Verified, 1 Total Pending, 0 Pending Invites, 1 Join Requests, and 0 Denied/Removed. Below this, the 'My Users' sidebar lists 'Join Requests' as the active view. The main area features a search bar and a filter for 'Access Type' set to '- Select -'. A table titled 'Showing 1 - 1 of 1' lists one user request:

	Last Name	First Name	Email	Access Type	Request Date	Actions
1	Doe	Jane	jane.doe@test.org	Verified	07/17/2026	Review

Figure 30. Permissions Page (User Management Tab, Join Requests)

2. Review the user information (name, email, access type, and request date) to determine if the user request to join your organization should be approved or denied.

3. Select the **Review** button next to a user's name. The Review User Request window opens.

Review User Request

Susan Smith would like to join XYZ Health Test.
If you approve the request, you must assign a user role.

Requested Date:	User Name:	Access Type:	User Email:
Jul 17, 2026	Susan Smith	Verified	susan.smith@test.org

* Indicates a required field

* Approve user to join your organization?

☐ Approve Access ☐ Deny Access

* Does this user need Administrator access? ☐ Yes ☐ No

* Assign Roles:

☐ Full Access ☐ View only ☐ Initiation & Selection

Assign Workspaces:

- Select -

Confirm [Cancel](#)

Figure 31. Review User Request

4. From the **Approve user to join your organization?** field, select the **Approve Access** or the **Deny Access** option, as applicable for the user.
5. From the **Does this user need Administrator access?** field, select the **Yes** or **No** option to grant the user administrator access, as applicable.
 - a. If you select **Yes**, the **Assign Roles** field defaults to **Full Access** only.
 - b. You cannot change the role for an administrator.
6. From the **Assign Roles** field, select the level of access you want the user to have to the organization's disputes:
 - a. **Full Access** roles may view all dispute information and submit all web forms.
 - b. **View Only** roles may view all dispute information but may not submit web forms.
 - c. **Initiation & Selection** roles may submit initiation, certified IDR entity selection, and reselection web forms but may not submit offers or view dispute outcomes.
7. (Optional) Select a workspace from the **Assign Workspaces** field to add the user to that workspace. (Refer to Section 10.2 Create a Workspace.)
8. Select **Confirm**.
 - a. User information for approved requests displays in the **Approved Users** table.
 - b. User information for denied requests displays in the **Denied Requests** table.

9.6. Search/Filter Users

Administrators can search for and filter users by access type, roles, and workspace assignments. (Not every search and filter option is available from each table option.)

1. From the **User Management** tab, select the **Approved Users** table option in the left navigation panel.

The screenshot shows the 'My Users' interface. On the left is a navigation panel with options: 'My Users', 'Pending Invites', 'Join Requests', 'Approved Users' (selected), 'Denied Requests', and 'Removed Users'. The main area has a search bar 'Search for users in your organization'. Below it is a 'Filters' section with three dropdown menus: 'Access Type' (set to '- Select -'), 'Workspaces' (set to '- Select -'), and 'Role' (set to '- Select -'). There are 'Apply' and 'Clear' buttons. Below the filters, it says 'Showing 1 - 3 of 3'. A table lists three users with columns: Last Name, First Name, Email, Access Type, Role, Workspace, and Actions. Each row has an 'Edit' button in the Actions column.

	Last Name	First Name	Email	Access Type	Role	Workspace	Actions
1	Doe	Jane	jane.doe@test.org	Verified	View Only	All Disputes	Edit
2	Smith	Susan	susan.smith@test.org	Verified	View Only	All Insured	Edit
3	Smith	John	john.smith@test.org	Administrator	Full Access	All Disputes	Edit

Figure 32. Permissions Page (User Management Tab, Approved Users)

2. Select an option from the **Access Type** field to filter users by access type (all, verified, or administrator).
3. Select an option from the **Workspaces** field to filter users assigned to a workspace. This filter is only available for users who have been approved to join the organization.
4. Select an option from the **Role** field to filter users by role (full access, view only, or initiation and selection). This filter is only available for users who have been approved to join the organization.
5. Enter at least three characters in the **Search for users in your organization** field and select **Apply**.

9.7. Edit User Access

Administrators can assign roles, grant administrator access, assign users to workspaces, and remove user access to the organization.

1. From the **User Management** tab, select the **Approved Users** table option in the left navigation panel.

2. Select the **Edit** button from the Actions column next to the user. The Edit User window opens.

Figure 33. Edit User

3. From the *** Remove organization access?** field, select **Yes** to remove the user from the organization or **No** to keep the user in the organization.
4. From the *** Does this user need Administrator access?** field, select from the following options:
 - a. **Yes** to grant administrator access to the organization. The *** Assign Roles** field defaults to **Full Access** and cannot be modified.
 - b. **No** to deny administrator access to the organization.
5. From the *** Assign Roles** field, select the access you want the user to have to the organization's disputes:
 - a. **Full Access** roles may view all dispute information but may not submit all web forms.
 - b. **View Only** roles may view all dispute information but may not submit web forms.
 - c. **Initiation & Selection** roles may submit initiation, certified IDR entity selection, and reselection web forms but may not submit offers or view dispute outcomes.
6. (Optional) Select a workspace from the **Assign Workspaces** field to add the user to that workspace.
7. Select the **Save Changes** button. Updates display in the My User tables.

10. Manage Workspaces

Administrators can optionally use the **Workspace Management** tab on the “Permissions” page to create new workspaces, manage existing workspaces, and assign users to workspaces to control access to organization disputes.

10.1. Workspaces

Workspaces are secure spaces that contain a subset of your organization’s disputes based on the email addresses listed on the dispute. Workspaces allow administrators to control the disputes a user can work.

Every organization starts dispute activities in the All Disputes workspace, which displays all the disputes associated with an organization. When users join an organization, they automatically gain access to this All Disputes workspace. Creating additional workspaces is optional. Administrators should only create additional workspaces if they want to limit certain users’ ability to view the organization’s disputes.

To limit user access to disputes associated with specific email addresses, administrators can create a workspace, add email addresses used to manage specific kinds of disputes to that workspace, and assign users to that workspace.

The email address listed in the Initiating Party email address or Non-Initiating Party email address fields (not the Primary or Secondary contact fields) will associate disputes to an organization and will be the email address used to define a workspace. Users in a workspace can only view the disputes associated with the emails in that workspace. They cannot view all disputes associated with the organization.

Email addresses can only be removed from a workspace if the administrator submits a service request to remove the workspace email. When an email address is removed, users in that workspace will lose access to the disputes associated with that email address.



When to Use Workspaces: Administrators responsible for processing disputes on behalf of multiple parties may create new workspaces for each party, ensuring each team can only access disputes associated with their respective party.

10.2. Workspace Examples

One example where workspaces may be helpful is a large organization with multiple teams that manage disputes through separate inboxes, supporting different clients. In the figure below, Organization A has three Clients: B, C, and D. Organization A has four users – the administrator,

Alex, Susan, and Jane. The administrator creates three workspaces, one for each client, using the respective dispute processing email addresses.

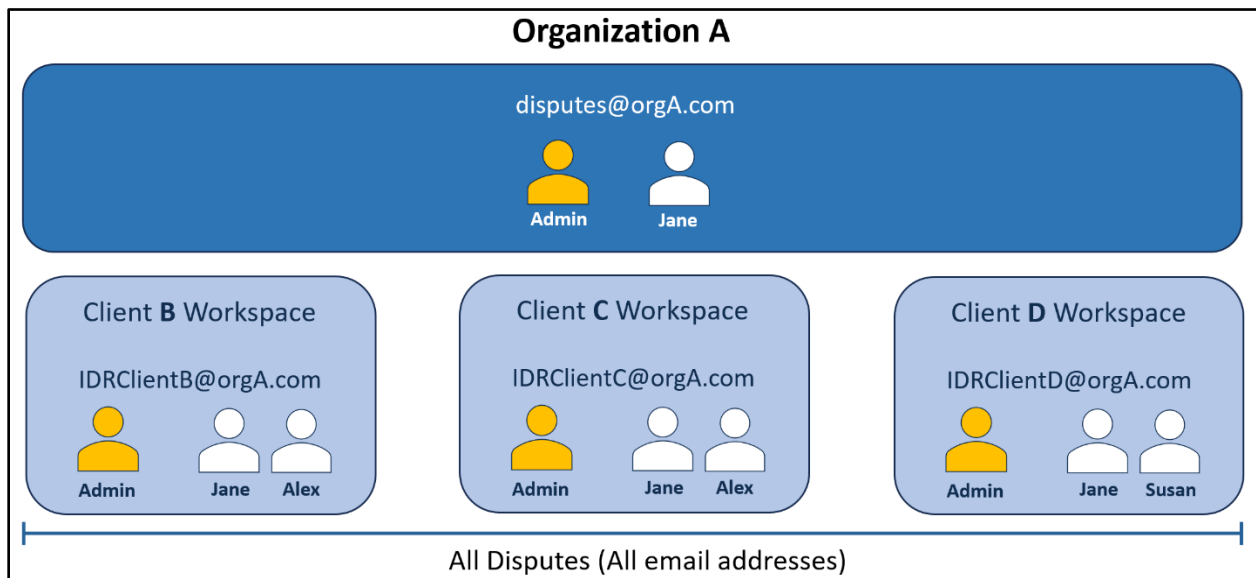


Figure 34. Workspace Example

- Client B's workspace is named Workspace B and uses the inbox email address IDRClientB@email.org.
- Client C's workspace is named Workspace C and uses the inbox email address IDRClientC@email.org.
- Client D's workspace is named Workspace D and uses the inbox email address IDRClientD@email.org.

Alex only works on Client B's disputes, so the administrator assigns Alex to Workspace B. Susan works on disputes for both Client C and Client D, so the administrator assigns Susan to Workspace C and Workspace D. Jane works on disputes for all three clients, so the administrator assigns Jane to the All Disputes workspace.

10.3. Create a Workspace

1. From the Home menu bar, select the **Permissions** option from the user menu dropdown list. The "Permissions" page displays.
2. Select the **Workspace Management** tab. The My Workspaces table displays.

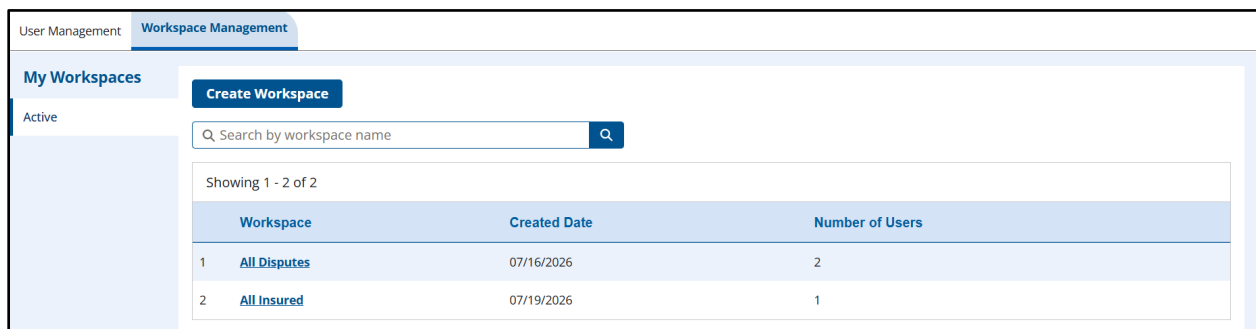
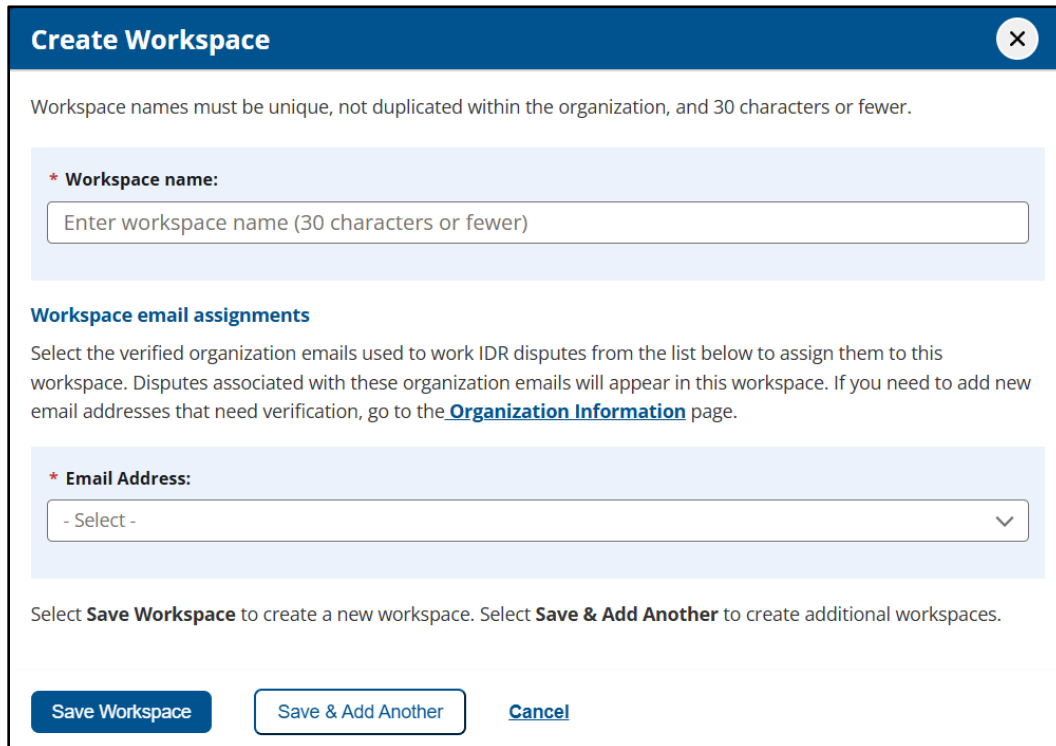


Figure 35. Permissions Page (Workspace Management Tab)

3. Select the **Create Workspace** button. The Create Workspace window opens.



Create Workspace [Close]

Workspace names must be unique, not duplicated within the organization, and 30 characters or fewer.

*** Workspace name:**

Enter workspace name (30 characters or fewer)

Workspace email assignments

Select the verified organization emails used to work IDR disputes from the list below to assign them to this workspace. Disputes associated with these organization emails will appear in this workspace. If you need to add new email addresses that need verification, go to the [Organization Information](#) page.

*** Email Address:**

- Select -

Select **Save Workspace** to create a new workspace. Select **Save & Add Another** to create additional workspaces.

Save Workspace **Save & Add Another** [Cancel](#)

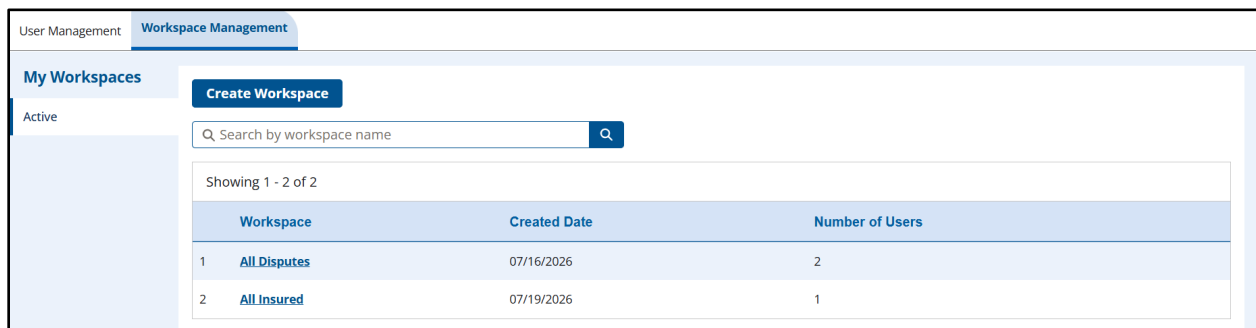
Figure 36. Create Workspace

4. From the **Workspace Name** field, enter a unique name for the workspace using 30 characters or fewer.
5. Select an organization email address from the dropdown list to add to the workspace. IDR disputes associated with the selected email addresses display within the workspace.
6. Select the **Save Workspace** button or the **Save & Add Another** button to add another email address. The new workspace displays in the My Workspaces table under the Active option.

10.4. Add Users to a Workspace

Administrators can manage users and email addresses associated with a workspace from the workspace page.

1. From the “Permissions” page, select the **Workspace Management** tab.



User Management **Workspace Management**

My Workspaces

Active

Create Workspace

Q Search by workspace name

Showing 1 - 2 of 2

	Workspace	Created Date	Number of Users
1	All Disputes	07/16/2026	2
2	All Insured	07/19/2026	1

Figure 37. Permissions Page (Workspace Management Tab, My Workspaces Table)

- From the My Workspaces table, select the workspace hyperlink in the Workspace Name column. The details page for the specific workspace displays. The title of the page reflects the name of the workspace.

The screenshot shows the 'Workspace : All Insured' page. At the top, there's a navigation bar with 'Home', 'Permissions', and 'Workspace: All Insured'. The main heading is 'Workspace : All Insured'. Below it, there's a 'Workspace Details' section with buttons for 'Add Users' and 'Add Emails'. The details include Status: Approved, Date Created: 7/19/2026, and Number of Users: 1. Below this is a section for 'Email Addresses in this Workspace' showing one email: health@test.org. Then, there's a section for 'Users in this Workspace' showing one user: Susan Smith (susan.smith@test.org) with a 'View Only' role and 'Verified' access type. A 'Remove' button is next to her name. At the bottom, there's a 'Return to Permissions' button.

Figure 38. Workspace Page

- Select the **Add Users** button. The Add Users window opens.

The screenshot shows the 'Add Users' window. It has a search bar at the top with the placeholder text 'Search user name to add..'. Below the search bar, it says 'Showing 1 - 1 of 1'. There's a table with columns: Last Name, First Name, Email, Role, and Access Type. The table contains one row for Jane Doe (jane.doe@test.org) with a 'View Only' role and 'Verified' access type. There are checkboxes next to the 'Last Name' and 'Email' columns. At the bottom, there are two buttons: 'Add Selected Members' and 'Cancel'.

Figure 39. Add Users

- Use the **Search** feature to search for user names in your organization.
- Select the checkbox next to each user name to add to the workspace.
- Select the **Add Selected Members** button. These users will now only be able to access the disputes in that workspace (unless they are also assigned to additional workspaces). The users display in the **Users in this Workspace** table.
- Select the **Return to Permissions** button to close the "Workspace Details" page and return to the "Permissions" page.

10.5. Remove a User from a Workspace

If a user is removed from a workspace, but is also assigned to another workspace, the user will remain in the other workspace without returning to the All Disputes workspace.

1. From the My Workspaces table, select the hyperlink of the workspace name in the Workspace Name column. The “Workspace Details” page for the workspace displays.

The screenshot shows the 'Workspace : All Insured' page. At the top, there's a breadcrumb trail: Home > Permissions > Workspace: All Insured. Below the title, there are two buttons: 'Add Users' and 'Add Emails'. The 'Workspace Details' section shows: Status: Approved, Date Created: 7/19/2026, and Number of Users: 1. Below this is the 'Email Addresses in this Workspace' section, showing one email: health@test.org. The 'Users in this Workspace' section shows a table with one user: Susan Smith (susan.smith@test.org) with a 'View Only' role and 'Verified' access type. A 'Remove' button is next to her name. At the bottom left is a 'Return to Permissions' button.

Last Name	First Name	Email	Role	Access Type	Actions
Smith	Susan	susan.smith@test.org	View Only	Verified	<button>Remove</button>

Figure 40. Workspace Page

2. From the Users in this Workspace table, select the **Remove** button next to the user to remove from the workspace. The Remove User window opens.

The 'Remove User' dialog box asks: 'Are you sure you would like to remove Jane Doe from the All Insured workspace?'. It includes a warning: 'If you remove this user, they will have access to all disputes in the "All Disputes" workspace, which includes every IDR dispute for the organization.' At the bottom are 'Remove' and 'Cancel' buttons.

Figure 41. Remove User

3. Select the **Remove** button to confirm you want to remove the user from the workspace.
 - a. If the user does not belong to any other workspaces, the user returns to the All Disputes workspace. This means the user will have access to all disputes associated with the organization.
 - b. If you do not want the user to have access to all your organization's disputes, you can assign the user to a different workspace.

- c. If the user belongs to another workspace, the user will no longer have access to the disputes associated to the removed workspace, but will have access to disputes in the other workspace.
- d. Once removed, the user no longer displays in the Users in this Workspace table.
4. Select the **Return to Permissions** button to close the “Workspace Details” page and return to the “Permissions” page.

10.6. Add an Email Address to a Workspace

1. From the My Workspaces table, select the hyperlink of the workspace name in the Workspace Name column. The “Workspace Details” page for the workspace displays.
2. From the “Workspace Details” page, select the **Add Emails** button to control access to disputes and assign users to a new workspace associated with specific dispute emails. The Add Emails window opens.

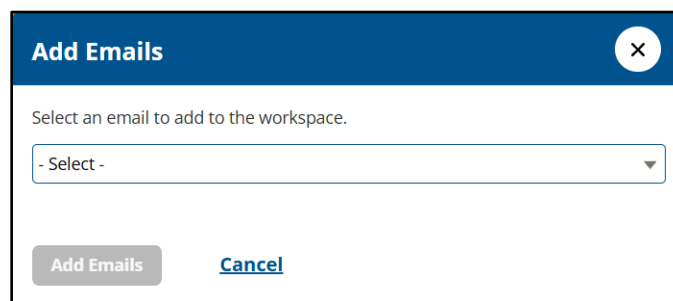


Figure 42. Add Emails

3. Select an organization email address from the dropdown list to add to the workspace.
 - a. If the email address does not display in the dropdown list, it's because administrators haven't added and verified that email address yet (Refer to [Section 6.5 Verify Organization Email Addresses](#)).
 - b. You will need to add and verify that dispute processing email address on the “Organization Information” page.
4. Select the **Add Emails** button.
 - a. The email address displays in the Email Address table.
 - b. Users in the workspace will only be able to work on disputes associated with that email.
5. Select the **Return to Permissions** button to close the “Workspace Details” page and return to the “Permissions” page.



When a new email address is added to a workspace, users can view all disputes associated with that email. Administrators can only remove an email address from a workspace by submitting a service request to CMS.

If CMS reviews and approves the request to remove an email address from a workspace, users in that workspace lose access to all disputes associated with that email, even disputes they worked previously.

Appendix A. Resources

This section of the user guide provides helpful resources to help you navigate issues you may encounter while creating an IDR Gateway account and setting up your organization, as well as additional context on the Federal IDR process.

IDR Gateway Help Desk Resources

- **IDR Gateway questions or issues?** Email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059.
- **Privacy concerns?** Email Privacy@cms.hhs.gov.
- **Questions or issues related to specific disputes or to the IDR process generally?** Email FederalIDRQuestions@cms.hhs.gov.

IDR Resources

The following resources about the No Surprises Act and the Independent Dispute Resolution are available to IDR Gateway users.

- CMS IDR Gateway page: <https://www.cms.gov/nosurprises/help-resolve-payment-dispute/idrgateway>
- CMS No Surprises home page: <https://www.cms.gov/nosurprises>
- CMS No Surprises privacy information: <https://www.cms.gov/nosurprises/privacy>
- CMS About Independent Dispute Resolution: <https://www.cms.gov/nosurprises/help-resolve-payment-disputes/payment-disputes-between-providers-and-health-plans>
- Overview of Rules and Fact Sheets related to the No Surprises Act: <https://www.cms.gov/nosurprises/policies-and-resources/overview-of-rules-fact-sheets>
- No Surprises Act training video playlist: [YouTube Playlist](#)
- No Surprises Act Toolkit: <https://www.cms.gov/nosurprises/consumer-advocate-toolkit>

Appendix B. Warning and Security & Privacy Agreement



The warning and privacy statements outline the rules for using the IDR Gateway responsibly and protecting information to ensure proper use, safeguard data, and create a secure and reliable environment for all users.

Warning

This system contains U.S. Government Data and is only available to users in the U.S. and its territories. Unauthorized use of this system is prohibited.

The Independent Dispute Resolution (IDR) Gateway, is provided only for authorized use by participants in the Federal IDR process. All information, documentation, and communications that are submitted by stakeholders in the IDR Gateway are only for authorized U.S. Government and certified IDR entity use. U.S. Government computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized U.S. Government entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Use of this system implies understanding of these terms and conditions.

* You Must Read and Agree to the Security & Privacy Agreement:

By using web forms we provide for use in connection with the Federal Independent Dispute Resolution (IDR) process, you agree to the collection and use of information as described in this Privacy Act Statement.

The Centers for Medicare & Medicaid Services (CMS) ("us," "we," or "our") operates the web forms used by parties to start payment disputes available on <https://nsa-idr.cms.gov/paymentdisputes>. Users may submit the forms electronically by completing the Notice of IDR Initiation web form. The information on this page tells you about our policies regarding the collection, use, and disclosure of personal information we receive from users of the web forms. It also includes specifics about personal information and other information that may be collected about you. A separate [IDR Website Privacy Policy](#) provides more information about CMS website privacy information for the Federal IDR portal, which you should also read and be aware of how information is collected and used when on the Federal IDR portal.

Permission for information submitted on IDR web forms

When submitting any Federal IDR web forms, you represent that you are authorized to submit the web form, as well as to receive any communications about the payment dispute, its status, or a final decision related to the payment dispute. For example, if you submit the Notice of IDR Initiation web form, you represent that you are authorized to start the dispute on behalf of the health care provider, health care facility, provider of air ambulance services, plan, issuer, or Federal Employees Health Benefits (FEHB) carrier, as applicable, regarding any claim(s) for the qualified IDR item(s) and/or service(s) to the participant's, beneficiary's, or enrollee's plan.

CMS.gov Privacy Policy

Protecting your privacy is very important to us. This privacy policy describes what information we collect, why we collect it, and what we do with it, available at <https://www.cms.gov/privacy>.

Federal Independent Dispute Resolution Process Privacy Act Statement – effective August 14, 2026

The Departments of the Treasury, Labor, and Health and Human Services (HHS) (collectively, the Departments), are authorized to collect the information on submitted web forms and any supporting documentation under Internal Revenue Code sections 9816(c) and 9817(b), ERISA sections 716(c) and 717(b), PHS Act sections 2799A-1(c) and 2799A-2(b), and 5 U.S.C. 8902(p). This law directs the Departments to establish a process to restrict surprise billing for participants, beneficiaries, and enrollees of group health plans, health insurance issuers offering group or individual health insurance coverage, and FEHB carriers who receive emergency services from nonparticipating health care providers or health care facilities, non-emergency services from nonparticipating health care providers at participating health care facilities, and air ambulance services from nonparticipating health care providers of air ambulance services.

We need the information provided about parties to the Federal IDR process to manage Notices of IDR Initiation and to otherwise support resolution of payment disputes and our oversight of the Federal IDR process. Do not include personally identifiable information (PII) or protected health information (PHI) in the payment dispute web form submissions unless specifically requested. The information collected through the payment dispute web forms will be used to verify the eligibility of disputes for the Federal IDR process and to resolve payment disputes. The Departments have established access to administer the Federal IDR process, available at <https://www.cms.gov/nosurprises>.

The initiating party must furnish the Notice of IDR Initiation to the Departments by submitting the notice through the [Independent Dispute Resolution](#) web page. If a dispute is eligible, the contact information provided on the Notice of IDR Initiation web form will be used to send the parties a notice identifying and/or confirming the certified IDR entity assigned to the dispute. This information provided will be shared with the certified IDR entity for consideration and for the purpose of enabling the certified IDR entity to make eligibility and payment determinations. We will also use the information as part of the ongoing operation of the Federal IDR process, including managing and reporting on the Federal IDR process, and performing oversight and quality control activities in relation to certified IDR entities. We may also use the information to evaluate whether a certified IDR entity or its staff have any conflicts of interest that would preclude it from making a payment determination. The information may further be used to combat fraud and noncompliance within the Federal IDR process and respond to any concerns about the security or confidentiality of the information.

Providing the requested information is voluntary. If any plan, issuer, FEHB carrier, health care provider, health care facility, or provider of air ambulance services, or any third-party administrator knowingly fails to provide correct information on submitted web forms or knowingly and willfully provides false or fraudulent information, they may be subject to penalties and other enforcement actions.

To manage disputes within the Federal IDR process, we will need to share certain information with people or entities outside of CMS. Recipients must comply with federal confidentiality requirements and implement required security measures, and may include:

1. A certified IDR entity, which we have certified to make payment determinations. The certified IDR entity will only use this information for the purpose of making payment determinations;
2. Contractors engaged to perform functions related to or in support of the Federal IDR process, including contractors that will support the payment of certified IDR entity fees and administrative fees;
3. Business Associates and other authorized entities who have executed appropriate agreements and maintain compliance with federal privacy and security requirements;

4. All parties to a dispute and their authorized representatives;
5. Other federal agencies that are responsible for implementing and overseeing plans that are subject to the Federal IDR process, including the Departments and OPM; and
6. Anyone else as required by law or allowed under the Privacy Act System of Records Notice associated with this collection entitled, "Complaints Against Health Insurance Issuers and Health Plans (CAHII)," System No. 09-70-9005, 66 FR 9858 (Feb. 12, 2001), as amended, 83 FR 6591 (Feb. 14, 2018).

This statement provides the notice required by the Privacy Act of 1974 (5 U.S.C. § 552a(e)(3)).

You can learn more about how we handle your information at:

<https://www.cms.gov/nosurprises/privacy>.

Contact Us

If you have any questions about this Privacy Act Statement, please contact us at

Privacy@cms.hhs.gov.

Appendix C. IDR Gateway Rules of Behavior



The IDR Gateway Rules of Behavior (RoB) apply to everyone who accesses its information and resources. They are instructions setting mandatory conduct for users when accessing the IDR Gateway to ensure proper use, safeguard data, and create a secure and reliable environment for all users. All users must agree to follow these rules before signing in to the IDR Gateway.

A. The IDR Gateway

When using and accessing the IDR Gateway, I understand that I must:

- Comply with federal laws, regulations, and the IDR Gateway policies, standards, and procedures and that I must not violate, direct, or encourage others to violate these policies, standards, or procedures. Not allow unauthorized use and access to the IDR Gateway information and resources.
- Not access the IDR Gateway information and resources outside the U.S. and its territories.
- Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing.
- Review all the IDR Gateway user guides when initially granted access to the IDR Gateway and periodically thereafter as required by Federal IDR policies.
- Be accountable for my actions while accessing and using the IDR Gateway information and information systems.
- Sign out of the IDR Gateway whenever not actively working within it.
- Not enter personally identifiable information (PII) or personal health information (PHI) in any fields in the IDR Gateway. This includes, but is not limited to, patient names, social security numbers, medical record numbers, health plan beneficiary numbers, and any other unique identifying characteristics as defined by the Privacy Act of 1974 and HIPAA Privacy Rule.
- Redact any PII/PHI from documents before uploading them to the IDR Gateway. This includes reviewing all attachments, embedded content, and metadata to ensure complete removal of sensitive information in accordance with HIPAA Privacy Rule requirements, Privacy Act provisions, and the National Institute of Standards and Technology (NIST) SP 800-88 Rev. 2, Guidelines for Media Sanitization.
- Understand that unauthorized disclosure of PII/PHI may result in violations of both the Privacy Act of 1974 and HIPAA regulations, potentially leading to civil and criminal penalties.
- Implement appropriate administrative, technical, and physical safeguards to protect any sensitive information that may be accessed through the IDR Gateway.
- Report all suspected and identified information security incidents and privacy breaches to FederalIDRQuestions@cms.hhs.gov as soon as possible, without unreasonable delay and no later than within one (1) hour of occurrence/discovery. This reporting requirement applies to any potential exposure of PII/PHI, regardless of the circumstance or scale of the incident.

B. No Expectation of Privacy

When using and accessing the IDR Gateway information and systems, I understand that I would have no expectation of privacy. I acknowledge there would be no expectation of privacy when using the IDR Gateway information, resources, and systems and activity within the IDR Gateway may be monitored, recorded, and audited at any time.

C. Password Requirement

When creating and managing my password, I understand that I must comply with the following baseline requirements:

- Comply with all of the IDR Gateway's password requirements.
- Create passwords with minimum of 15 characters.
- Not use common or compromised passwords.
- Protect my passwords and other access credentials from disclosure and compromise.
- Promptly change my password if I suspect or receive notification that it has been compromised.
- Immediately select a new password upon account recovery.
- Not use another person's account, identity, password, or allow others to use my account to access the IDR Gateway. This includes not sharing passwords or providing passwords to anyone, including system administrators.
- Only use authorized credentials to access the IDR Gateway and will not attempt to bypass access control measures.

SIGNATURE

I have read the above Rules of Behavior for IDR Gateway Users and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or the IDR Gateway's information, security policies, and standards may result in suspension of access privileges, revocation of access to the IDR Gateway, deactivation of accounts, monetary fines, removal or debarment from work on federal contracts or projects, and/or criminal charges that may result in imprisonment.

I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing officials. I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 U.S.C. 2071, which the IDR Gateway RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

I have read and agree to comply with the provisions stated in the Rules of Behavior for IDR Gateway Users.

Appendix D. Administrator Quick Reference List

Use these tables to quickly locate the steps needed to complete common administrator tasks.

Notification Actions

I want to:	Actions:
Archive a notification.	Navigate to: Home > My Notifications 1. Select checkbox by notification. 2. Select the Archive button.
Allow other members of my organization to read the notification I just read.	Navigate to: Home > My Notifications 1. Select checkbox by notification. 2. Select Mark as Unread .

Organization Actions

I want to:	Actions:
Edit information about my organization.	Navigate to: Organization Information 1. Make edits as needed. 2. Select Save .
Leave an organization.	Navigate to: My Profile > My Organization 1. Select the Leave Organization button. 2. If you are the organization's only administrator, you must assign another administrator first. 3. Review and revise your affiliation, as needed. 4. Select Confirm .

User Actions

I want to:	Actions:
Assign another administrator to my organization.	Navigate to: Permissions > User Management tab > My Users table 1. Select Join Requests or Approved Users tab. 2. Locate user. 3. Select Edit . 4. Grant user administrator access. 5. Select Save Changes .
Edit user roles.	Navigate to: Permissions > User Management tab > My Users table 1. Select Approved Users tab. 2. Select Edit . 3. Adjust as needed. 4. Select Save Changes .

I want to:	Actions:
Remove user administrator access.	Navigate to: Permissions > User Management tab > My Users table 1. Select Approved Users tab. 2. Select Edit . 3. Remove administrator access. 4. Select Save Changes .
Review requests to join my organization.	Navigate to: Permissions > User Management tab > My Users table 1. Select Join Requests tab. 2. Select Review button. 3. Select Approve or Deny Access . 4. Select Yes or No to assign administrator access. 5. Select Assign Role radio button. 6. (Optional) Select from Assign Workspaces dropdown list. 7. Select Confirm .

Workspace Actions

I want to:	Actions:
Create workspace.	Navigate to: Permissions > Workspace Management tab 1. Select Create Workspace . 2. Enter unique workspace name. 3. Select verified organization emails to assign to new workspace. 4. Select Save Workspace .
Add emails to a workspace.	Navigate to: Permissions > Workspace Management tab 1. Select Active tab. 2. Select workspace name from My Workspaces table. 3. Select Add Emails . 4. Select emails from dropdown list. 5. Select Add Emails .
Manage workspace users.	Navigate to: Permissions > Workspace Management tab 1. Select Active tab. 2. Select workspace name from My Workspaces table. To add users: 1. Select Add Users . 2. Search and select names. 3. Select Add Selected Members . To remove users: 1. Search and select names. 2. Select Remove . 3. Select Remove to confirm.

Appendix E. Acronyms & Terms

The following acronyms and terms are used in this user guide and throughout the IDR Gateway.

Acronym/Term	Definition
Access Type	The IDR Gateway offers three user access types: verified and administrator.
Credential Service Provider	A credential service provider is a trusted entity whose functions include identity proofing applicants and registering authenticators to subscriber accounts. A credential service provider may be an independent third party.
CMS	Centers for Medicare & Medicaid Services
FEHB	Federal Employees Health Benefits
HHS	Department of Health and Human Services
IDM	Identity Management
IDR	Independent Dispute Resolution
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
NSA	No Surprises Act
PHI	Personal Health Information
PII	Personally Identifiable Information
Role	The IDR Gateway offers three user access roles controlled by the organization administrator: view only, initiation and selection roles, and full access roles.
SSN	Social Security Number
the Departments	The Department of Health and Human Services, the Department of Labor, and the Department of the Treasury
TPA	Third-Party Administrator
Workspace	Workspaces are secure spaces organizations use to grant or restrict access to disputes based on the email addresses assigned to the workspace.

This communication was printed, published, or produced
and disseminated at U.S. taxpayer expense.