

Independent Dispute Resolution (IDR) Gateway



Administrator User Guide

Version 3.0
October 14, 2026

Table of Contents

1. Introduction	5
2. IDR Gateway Overview	6
2.1. The IDR Gateway	6
2.2. Development Phases	6
2.3. Who Should Sign Up	6
2.4. IDR Gateway Access Types	7
3. Identity Verification	8
3.1. Identity Verification Process	8
4. Create an IDR Gateway Account	9
4.1. Create an Account with a Credential Service Provider	9
4.2. Sign in with Existing CMS-Approved Credentials	12
4.3. First Time Sign In	13
5. Sign In to the IDR Gateway	17
6. Accept an IDR Gateway Invitation	19
6.1. Join an Organization	19
6.2. Accept an Administrator Invitation	21
7. Request Administrator Access	23
7.1. Administrator Responsibilities	23
7.2. Request Administrator Access	23
7.3. Create a New Organization	25
7.4. Join an Organization	28
7.5. Verify Organization Email Addresses	29
7.6. Leave an Organization	29
8. Manage Notifications	31
8.1. System Notifications	31
8.2. View Notifications from the Home Page	31
8.3. Search and Filter Notifications	32
9. Manage Organization Information	34
9.1. Organization Information	34
9.2. Manage Organization Information	34
9.3. Add an Organization Email Address	35
9.4. Remove an Organization Email Address	35
9.5. Resend Email Verification Requests	35
10. Invite Users to Join an Organization	37
10.1. Permissions	37
10.2. Roles	37
10.3. Send an Invitation	38
10.4. Resend an Invitation	39
11. Manage User Access	41
11.1. Manage User Access	41
11.2. Download a User Report	42
11.3. Search and Filter Users	43
11.4. Review Join Requests	43
11.5. Edit User Access	45
12. Manage Workspaces	47
12.1. Workspaces	47
12.2. Workspace Example	47
12.3. Create a Workspace	48
12.4. Add Users to a Workspace	49
12.5. Remove a User from a Workspace	51
12.6. Add an Email Address to a Workspace	52
13. Map Disputes	53

13.1. Administrator Managed Dispute Mapping Process	53
13.2. Dispute Mapping Methods	54
13.3. Export Filtered Data and Review Disputes	57
13.4. Manual Dispute Mapping	58
13.5. Find Dispute Numbers Using Claim Numbers	62
13.6. Bulk Dispute Mapping (File Upload)	62
13.7. Review Dispute Mapping Results	65
13.8. Dispute Mapping Errors	65
13.9. Changes to Dispute Email Addresses	66
14. Search for Disputes	67
15. Access Reports.....	69
15.1. Reports Available in the IDR Gateway	69
15.2. Understanding Report Filters	70
16. Report Privacy & Security Incidents	73
16.1. Cybersecurity or Privacy Incidents	73
Appendix A. Resources	74
IDR Gateway Help Desk Resources	74
IDR Resources	74
Appendix B. Warning and Security & Privacy Agreement.....	75
Appendix C. IDR Gateway Rules of Behavior	78
Appendix D. Administrator Quick Reference List	80
Appendix E. Acronyms & Terms	84

Table of Figures

Figure 1. IDR Gateway Access Page	10
Figure 2. Sign In/Create Your CMS Account Page.....	11
Figure 3. Verify Your Identity Alert	12
Figure 4. Warning and Security & Privacy Agreement Window.....	13
Figure 5. Rules of Behavior Window.....	14
Figure 6. Set Up Your Profile Window (Select Affiliation and Confirm Email)	15
Figure 7. Set Up Your Profile (Confirmation)	16
Figure 8. Sign In/Create Your CMS Account Page.....	17
Figure 9. Rules of Behavior Window.....	18
Figure 10. My Notifications (Invitation to Join an Organization)	19
Figure 11. My Profile Page (Invitations Section).....	20
Figure 12. Accept Invitation (Confirmation).....	20
Figure 13. My Organization Section (Invitation Accepted).....	20
Figure 14. My Profile Page (Invitations Section).....	21
Figure 15. Administrator Roles & Responsibilities Window	21
Figure 16. Profile Information (Administrator Access Accepted)	22
Figure 17. My Profile (Request Administrator Access Link)	23
Figure 18. Request Administrator Access Window (Administrator Access Process)	23
Figure 19. Administrator Roles and Responsibilities Window	24
Figure 20. Request Administrator Access Window (Join or Create an Organization)	24
Figure 21. Create an Organization (Step 1 Organization Details)	25
Figure 22. Create an Organization (Step 2 Add Organization Emails).....	26
Figure 23. Create an Organization (Step 3 Confirm Organization Creation).....	27
Figure 24. Request Administrator Access (Find an Organization to Join).....	28
Figure 25. Request Administrator Access (Find an Organization to Join, Search Results)	28
Figure 26. Email Verification Confirmation Banner	29
Figure 27. IDR Gateway Home Menu Bar	31
Figure 28. My Notifications Table	31
Figure 29. View All Notifications Button	32
Figure 30. My Notifications Page (All Active Tab)	32
Figure 31. Organization Information Page (My Organization Information)	34

Figure 32. Organization Information Page (Organization Emails Table, Enter Email Address Field)	35
Figure 33. Organization Information Page (Organization Emails Table, Pending Tab).....	36
Figure 34. Permissions Page	37
Figure 35. Organization User Summary (Invite Users Button)	38
Figure 36. Invite Users Window	38
Figure 37. My Users Table (Resend Button)	39
Figure 38. Resend Invite Window	40
Figure 39. Permissions Page (Understanding User Permissions).....	41
Figure 40. Permissions Page (Understanding Roles).....	41
Figure 41. Permissions Page (User Management Tab, My Users Table)	42
Figure 42. Permissions Page (User Management Tab, Download User Report Button)	42
Figure 43. Permissions Page (User Management Tab, Approved Users)	43
Figure 44. Permissions Page (User Management Tab, Join Requests)	43
Figure 45. Review User Request Window	44
Figure 46. Edit User Window	45
Figure 47. Workspace Example	48
Figure 48. Permissions Page (Workspace Management Tab, Create Workspace Button)	48
Figure 49. Create Workspace Window	49
Figure 50. Permissions Page (Workspace Management Tab, My Workspaces Table)	49
Figure 51. Workspace Details Page	50
Figure 52. Add Users Window	50
Figure 53. Workspace Details Page (Remove Button)	51
Figure 54. Remove User Window	51
Figure 55. Add Emails Window	52
Figure 56. Dispute Mapping Page	55
Figure 57. Unconfirmed Disputes (Maximum Results Exceeded Error)	56
Figure 58. Export Filtered Data Results Window (Unconfirmed_Disputes.csv)	57
Figure 59. Dispute Mapping Page (Unconfirmed Tab)	58
Figure 60. Confirm Disputes Window	59
Figure 61. Dispute Mapping Page (Disputes Confirmed Alert).....	59
Figure 62. Dispute Mapping Page (Confirmed Tab)	59
Figure 63. Dispute Mapping Page (Results Tab).....	60
Figure 64. Deny Dispute Ownership Window	60
Figure 65. Dispute Mapping Page (Disputes Denied Alert).....	61
Figure 66. Dispute Mapping Page (Denied Tab)	61
Figure 67. Dispute Mapping Page (Unconfirmed Line Items Tab).....	62
Figure 68. Bulk Dispute Mapping Page	63
Figure 69. Bulk Dispute Mapping Upload Window	64
Figure 70. Dispute Mapping Page (Results Tab).....	65
Figure 71. Dispute Mapping Results File	65
Figure 72. Search Results.....	67
Figure 73. IDR Disputes Search Results	68
Figure 74. Menu Bar (Reports Option).....	69
Figure 75. All Disputes Report (Maximum Results Exceeded Error).....	70
Figure 76. Sample Report (All Disputes, Filter Options).....	71
Figure 77. Privacy & Security Page (How to Report a Privacy & Security Issue).....	73

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 manage and track disputes, set up accounts, and manage permissions for users in your organization within the Independent Dispute Resolution (IDR) Gateway.

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.
- **Accept an IDR Gateway Invitation.** Gain access to an organization's dispute dashboards and reports in the IDR Gateway.
- **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.
- **Invite Users to Join an Organization.** Ask users to join your organization in the IDR Gateway.
- **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.
- **Map Disputes.** Connect open IDR disputes to your organization in the IDR Gateway using email matching.
- **Access Reports.** Retrieve various organization dispute reports.
- **Report Privacy & Security Incidents.** Contact the CMS IT Service Desk to report cybersecurity or privacy incidents.

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. For instructions on managing disputes in the IDR Gateway, refer to the Dispute Processing User Guide.

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

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. If your organization is named in disputes but relies on a third-party administrator (TPA) or other organization to manage dispute processing activities, your organization does not need to sign up for the IDR Gateway itself, but must ensure the TPA or organization responsible for managing dispute processing activities creates an IDR Gateway account.

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

Important: The IDR Gateway does not have any features that link one organization to another. Therefore, organizations named in disputes but not involved in the day-to-day management of disputes should not 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. If an organization named in disputes uses a third-party dispute processing company and wants to track its IDR disputes, it should ask its dispute processing company for a report. Administrators are able to export reports of dispute activity they can provide to parties named in disputes that do not have IDR Gateway accounts.



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 as 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. No new IDM accounts will be established.

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. A credential service provider is a trusted organization that verifies a user's identity, and creates and manages the sign-in credentials for their accounts.

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 for more information.
- **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

If you received an email invitation to join an organization in the IDR Gateway and **you do not have an IDR Gateway account**, select the link in the email and follow the steps to create an account with a credential service provider.

If you did not receive an email invitation, follow steps 1-5 to create an account.

1. Navigate to the [IDR Gateway Access](#) page.
2. Bookmark the "IDR Gateway Access" page to access the IDR Gateway in the future.



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

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

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.

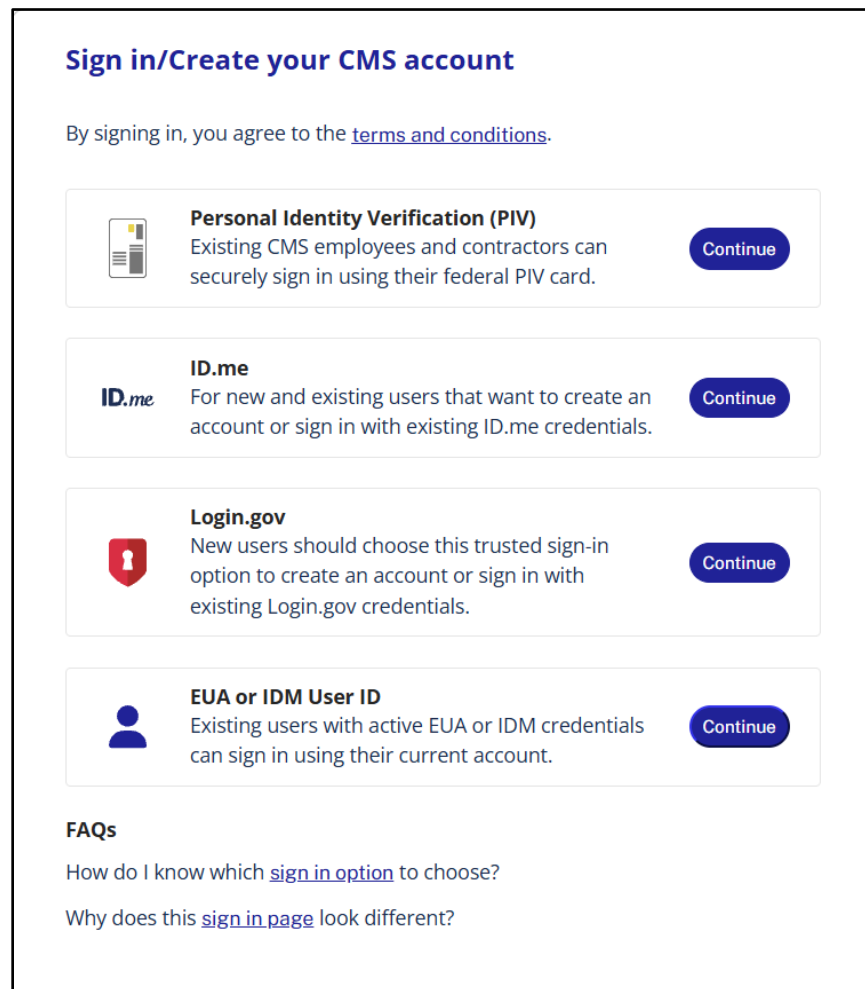
[Sign Up](#) 

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

3. 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 existing ID.me credentials.

[Continue](#)



Login.gov
New users should choose this trusted sign-in option 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

4. Select the **Continue** button of 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 for more information about the identity verification process.
 - a. Do not create a new EUA or IDM account.
 - b. Do not use the Personal Identity Verification (PIV) option.
5. Upon account creation, continue to Section 4.3.

4.2. Sign in with Existing CMS-Approved Credentials

If you received an email invitation to join an organization in the IDR Gateway and **you have existing CMS-approved credentials**, select the link in the email and reference the following steps to sign in using your existing CMS-approved credentials.

If you did not receive an invitation, reference the following steps to sign in with your existing CMS-approved credentials.

1. Navigate to the [IDR Gateway Access](#) page.
2. From the “IDR Gateway Access” page, select **Sign In**. The “Sign in/Create your CMS account” page displays.
3. Select the **Continue** button for your preferred credential service provider option.
4. Enter your credentials and select **Submit** to sign in to the IDR Gateway.
 - a. If you have an existing account **without identity verification**, the “Verify Your Identity” alert displays.

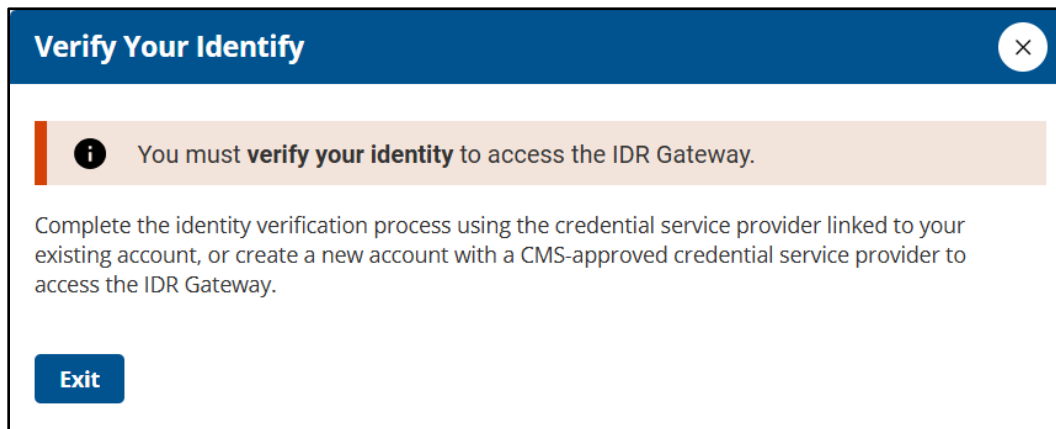


Figure 3. Verify Your Identity Alert

- b. Select the **Exit** button to close the window.
 - c. Return to the [IDR Gateway Access](#) page and select the **Sign Up** button.
 - d. Create an account with a credential service provider and complete the identity verification process. Refer to Section 4.1.
5. Continue to Section 4.3.

4.3. First Time Sign In

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



The image shows a web window titled "Warning and Security & Privacy Agreement". It is labeled "Step 1 of 4". The window greets the user as "JOHN SMITH" and instructs them to use the scroll bar to read and agree to the agreement. A legend indicates that an asterisk (*) denotes a required field. A scrollable box contains a "WARNING" about U.S. Government Data, followed by a detailed paragraph about the IDR Gateway's authorized use, monitoring, and security. Below this, there are two lines of text regarding consent to monitoring. At the bottom, there is a checkbox labeled with an asterisk and the text "I have read and agree to the Warning and Security & Privacy Agreement." To the left of the checkbox are two buttons: "Continue" and "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.

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.

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

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

Figure 4. Warning and Security & Privacy Agreement Window

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 5. Rules of Behavior Window

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 6. Set Up Your Profile Window (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 work 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 address.**
 - 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.

8. Select **Continue**. The Set Up Your Profile confirmation displays.

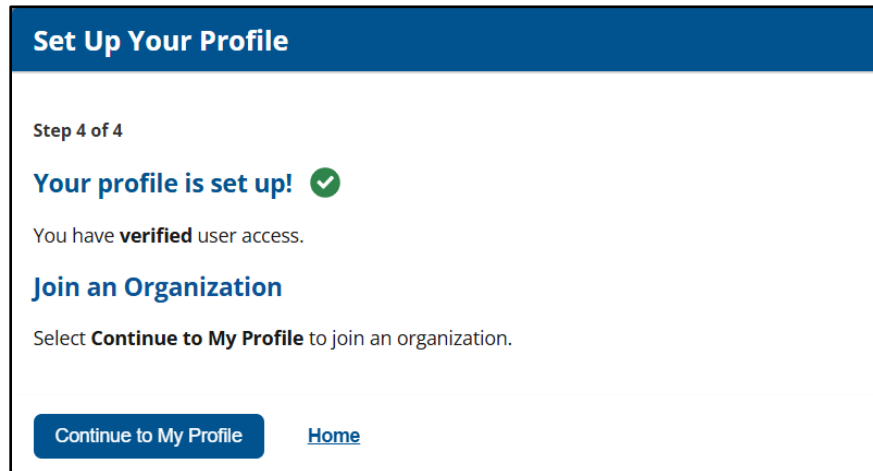


Figure 7. Set Up Your Profile (Confirmation)

9. Select the **Continue to My Profile** button to request administrator access. Refer to Section 7.
 - 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 to complete the identity verification process for your credential service provider.

5. Sign In to the IDR Gateway

After creating an account, users can sign in to the IDR Gateway from the “IDR Gateway Access” page.

1. Navigate to the [IDR Gateway Access](#) page.
2. Select the **Sign in** button. The “Sign in/Create your CMS account” page displays.

Figure 8. 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 9. Rules of Behavior Window

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. Accept an IDR Gateway Invitation

Administrators are responsible for managing membership and roles within their organization. Administrators can:

- Invite people to join their organization as a verified user.
- Invite people to join their organization as an administrator.
- Make someone an administrator who has already joined their organization.



If someone is invited to both join the organization and become an administrator, they can accept the invite to join the organization but decline the invitation to be an administrator.

Refer to Section 7.1 for more information on administrator roles and responsibilities. If you are the first administrator for an organization, refer to Section 7.

6.1. Join an Organization

If you are invited to join an organization in the IDR Gateway, you will receive a notification and an email invitation that expires in 10 business days.

Notifications		Mark as Read	Mark as Unread	Archive
Showing 1 - 2 of 2				
☐	Summary	Received Date ↓		
☐	An administrator invited you to join TestOrgA in the IDR Gateway. My Profile	Aug 18, 2026, 03:48 PM		
☐	Welcome to the IDR Gateway! Join an organization to finish setting up your profile. Join an organization	Aug 18, 2026, 09:51 AM		

Figure 10. My Notifications (Invitation to Join an Organization)

Joining an organization provides you with access to the organization dispute dashboards and reports. Refer to Section 4 for more information on creating an IDR Gateway account.



You can only join one organization at a time.
You must leave an organization before joining a different organization.

1. From the Home menu bar, select the **My Profile** option from the user menu dropdown list. The “My Profile” page displays.
2. Review the organization information in the “Invitations” section to confirm you belong to this organization.

Invitations

You have been invited to join TestOrgA.

Joining this organization will provide access to its dispute dashboards and reports. Review the organization details below and accept or decline the invitation.

Invitation: TestOrgA

Organization Address: 147 Main Street Springfield, Alabama 65498	Organization Email Addresses: idretotestorga@gmail.com	Access Type: Verified
---	--	---------------------------------

Figure 11. My Profile Page (Invitations Section)

3. Select the **Accept Invitation** or the **Decline Invitation** button. The Accept Invitation confirmation message displays.
 - a. Accepting the invitation automatically declines other pending invitations.
 - b. Accepting the invitation allows you to access the dispute dashboard and reports for the organization when they become available.

Accept Invitation

Are you sure you want to accept the invitation to join **TestOrgA**?

Accepting this invitation will automatically decline other pending invitations.

Figure 12. Accept Invitation (Confirmation)

4. Select the **Accept** button to join the organization. The organization displays in the “My Organization” section of the “My Profile” page.

My Organization

TestOrgA administrator approved your request to join the organization.

Organization Name: TestOrgA	Tax ID: XX-XXXXXXX	Organization Address: 147 Main Street Springfield, Alabama 65498	Organization Email Addresses: idretotestorga@gmail.com
Affiliation: Group Health Plan, Individual Health Insurance Issuer, View Only or Federal Employees Health Benefits (FEHB) carrier	Role:	Workspace(s):	All Disputes

Figure 13. My Organization Section (Invitation Accepted)

6.2. Accept an Administrator Invitation

If you joined an organization and receive an invitation to become an administrator, you will receive a notification and an email invitation. You can accept or decline the invitation. Accepting the invitation allows you to manage organization information, user access, and disputes on behalf of your organization. If you decline the administrator invitation, you will remain a member of the organization. Refer to Section 7.1 for more information on administrator roles and responsibilities.

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

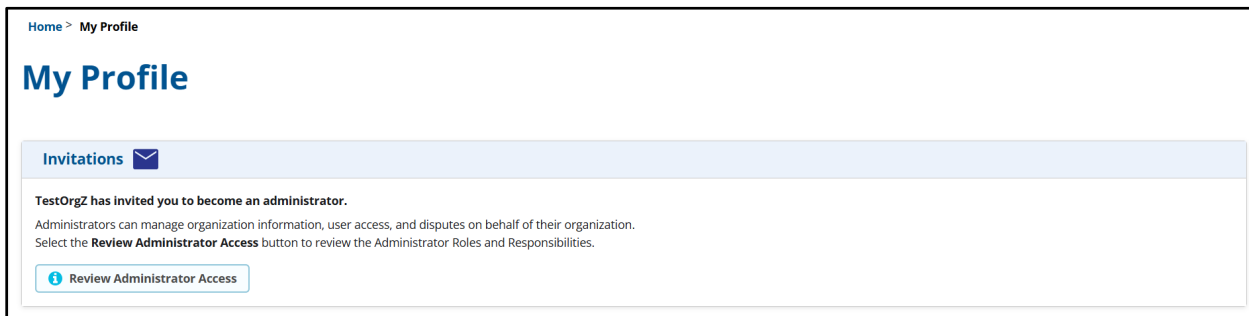


Figure 14. My Profile Page (Administrator Invitation)

2. Select the **Review Administrator Access** button. The Administrator Roles and Responsibilities window opens.

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 15. Administrator Roles & Responsibilities Window

3. Read the administrator roles and responsibilities.

4. Select the **checkbox** to indicate you are authorized to serve as an administrator for your organization, and you understand the administrator responsibilities.
5. Select the **Accept Administrator Access** or the **Decline Administrator Access** button. A confirmation displays in the “Profile Information” section of the “My Profile” page and your displayed access type changes from verified to administrator. You will receive an email notification of the change in your access type.

My Profile

Profile Information

 You have accepted administrator access. You can now manage organization information, user access, and disputes on behalf of TestOrgZ.

Current Access: Administrator	First Name: JOHN	Last Name: SMITH	Phone: 785-691-5788	IDR Gateway Credential Email: idr.eto.test@gmail.com	IDR Gateway Notification Email: idr.eto.test@gmail.com
---	----------------------------	----------------------------	-------------------------------	--	--

▼ IDR Gateway User Access Type Information

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).

Verified:

- 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.

Figure 16. Profile Information (Administrator Access Accepted)

7. 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.

7.1. 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.

7.2. 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 is a navigation bar with 'Home', 'Disputes', and 'Reports' menus, a search bar, and a user profile dropdown for 'JOHN SMITH'. Below the navigation bar, the page title 'My Profile' is displayed. A 'Profile Information' section contains a table with the following data:

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

Below this is a section titled 'IDR Gateway User Access Type Information'. It includes a paragraph: '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 main sections: 'Verified:' (highlighted with a green border and a green checkmark icon) and 'Administrator' (with a blue header). The 'Verified:' section lists:

- Can start and respond to disputes.
- Can join an organization and access the dispute dashboards and reports associated with the organization.

The 'Administrator' section lists:

- 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 17. My Profile (Request Administrator Access Link)

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

The screenshot shows a modal window titled 'Request Administrator Access'. It contains a section 'Administrator Access Process' with a numbered list:

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 are two buttons: 'Continue' (in a blue box) and 'Cancel' (as a text link).

Figure 18. Request Administrator Access Window (Administrator Access Process)

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

Request Administrator Access

Administrator Roles and Responsibilities

Review the administrator roles and responsibilities and attest you are able 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 able 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 19. Administrator Roles and Responsibilities Window

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 20. Request Administrator Access Window (Join or Create an Organization)

6. Continue to Section 7.3 Create a New Organization or to Section 7.4 Join an Organization, as required.

7.3. 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 any additional email addresses associated with the organization. The email addresses are used to ensure that submitted disputes refer 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 21. Create an Organization (Step 1 Organization Details)

3. Enter the organization information. Required information is indicated by an asterisk.

4. Select **Continue**. The Add Organization Emails 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

* **Dispute Processing Email:**

Additional Dispute Processing Emails: +

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

Figure 22. 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 Confirm Organization Creation information displays.
 - a. If an error indicates the organization already exists, refer to Section 7.4.
 - 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

Dispute Processing Email: john.smith@test.org	Additional Dispute Processing Emails:
---	--

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

Back
Create Organization
Cancel

Figure 23. Create an Organization (Step 3 Confirm Organization Creation)

8. Confirm that the organization details and organization email addresses 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 addresses within **2 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.

7.4. 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 24. 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 search results display.

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

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 7.3.
 - 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 2 business days, and then request to join the organization.
 - c. If you believe there is an error, contact IDRGatewayHelp@cms.hhs.gov.

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.

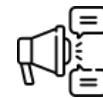


This step is only applicable for organizations that have already been set up in the IDR Gateway and already have at least one administrator.

7.5. Verify Organization Email Addresses

Administrators must verify within **2 business days** all dispute processing email addresses added when setting up the organization. If the primary organization email address is not verified within 2 business days, the organization will be removed from the IDR Gateway. If the additional dispute processing email addresses are not verified within 2 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 2 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 “Sign in/Create your CMS account” page displays.
4. Sign in to the IDR Gateway using your credentials. An email verification confirmation displays indicating the organization email address was verified.

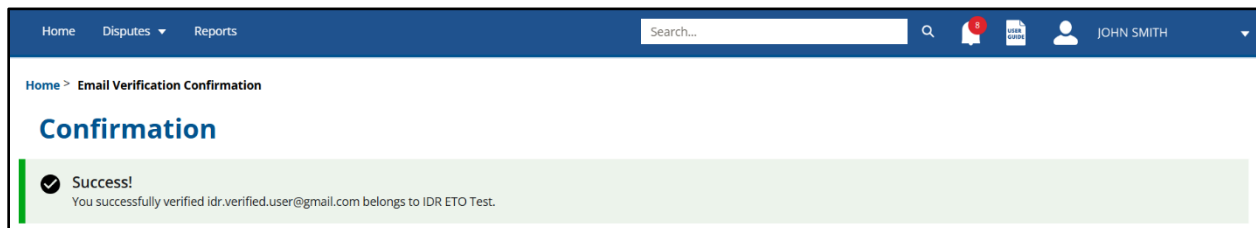


Figure 26. Email Verification Confirmation Banner

7.6. 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 11.5 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.

8. Manage Notifications

The IDR Gateway 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.

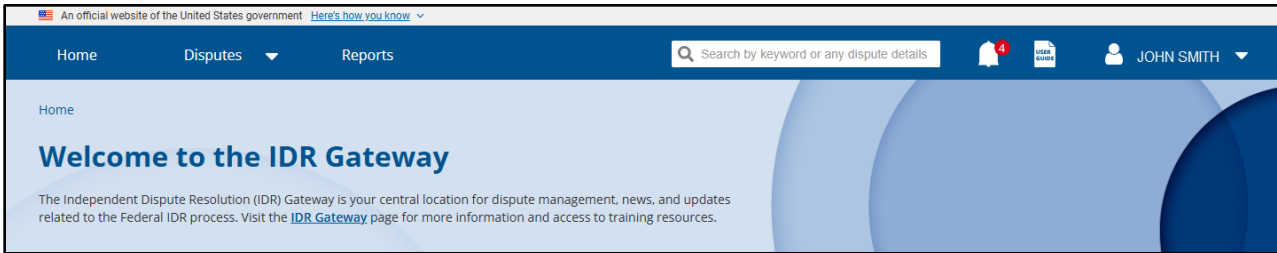


Figure 27. IDR Gateway Home Menu Bar

8.1. 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.

8.2. 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 message, the notification summary matches the email subject line. The supporting email message provides additional information not listed in the in-system notifications.
 - 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.

Notifications		Mark as read	Mark as unread	Archive
Showing 1 - 3				
☐ Summary	Received Date			
☐ Administrator Review Required: Verify this email address belongs to [Organization Name] within two business days.	09/01/2026 8:14 AM			
☐ An administrator approved your request to join [Organization Name] as an administrator. View My Profile .	09/01/2026 8:12 AM			
☐ Your request to join [Organization Name] with administrator access is pending approval.	09/01/2026 8:03 AM			

Figure 28. 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.

8.3. Search and Filter Notifications

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

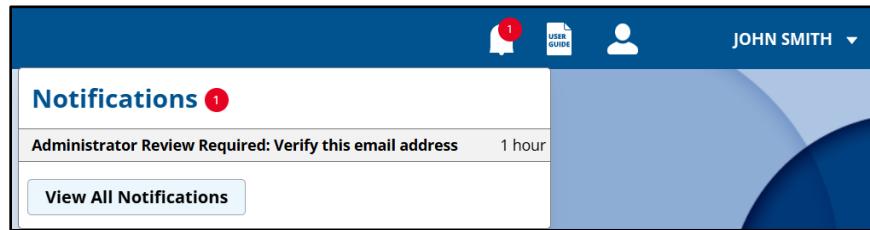


Figure 29. View All Notifications Button

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

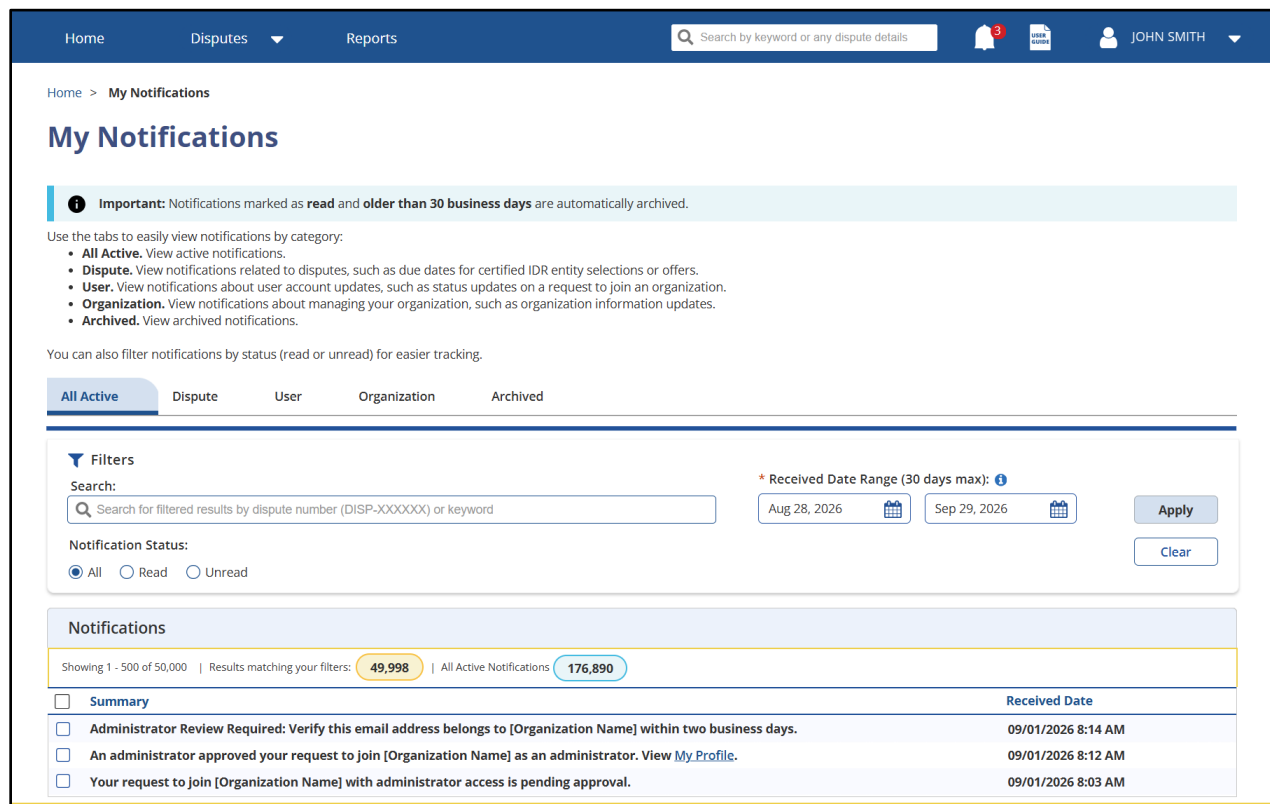


Figure 30. My Notifications Page (All Active Tab)

3. To search for a notification, enter at least three characters of a keyword or dispute number in the Filters panel search field. The search is limited to the selected table filters.



Information displayed in the Notifications table is limited to a 30-calendar-day created date range and displays up to 50,000 results.

4. To filter notifications by type, select from the following tabs.
 - 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 email addresses.
 - e. **Archived.** View archived notifications. Archived notifications are older than 30 business days or have been archived by a user using the **Archive** button.
5. To filter notifications by status, select a **Notification Status** option (All, Read, Unread) and select the **Apply** button. The results display in the table.

9. Manage Organization Information

9.1. 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.

9.2. 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 31. Organization Information Page (My Organization Information)

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 the edit button (**pencil** icon) following 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.

9.3. 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 **2 business days**. If the dispute processing email address is not verified within 2 business 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 2 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.

Organization Emails

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.

Enter Email Address Add Email

Showing 1 - 1 of 1

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

Figure 32. Organization Information Page (Organization Emails Table, Enter Email Address Field)

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.

9.4. 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.

9.5. Resend Email 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.

Organization Emails

Verified

Pending

Removed

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.

Enter Email Address Add Email

Showing 1 - 1 of 1

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

Figure 33. 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.

10. Invite Users to Join an Organization

Administrators can send email invitations to people without IDR Gateway accounts to join their organization within the IDR Gateway. Administrators can determine user access to organization disputes by selecting user permissions when sending the invitation to join the organization.

10.1. 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.

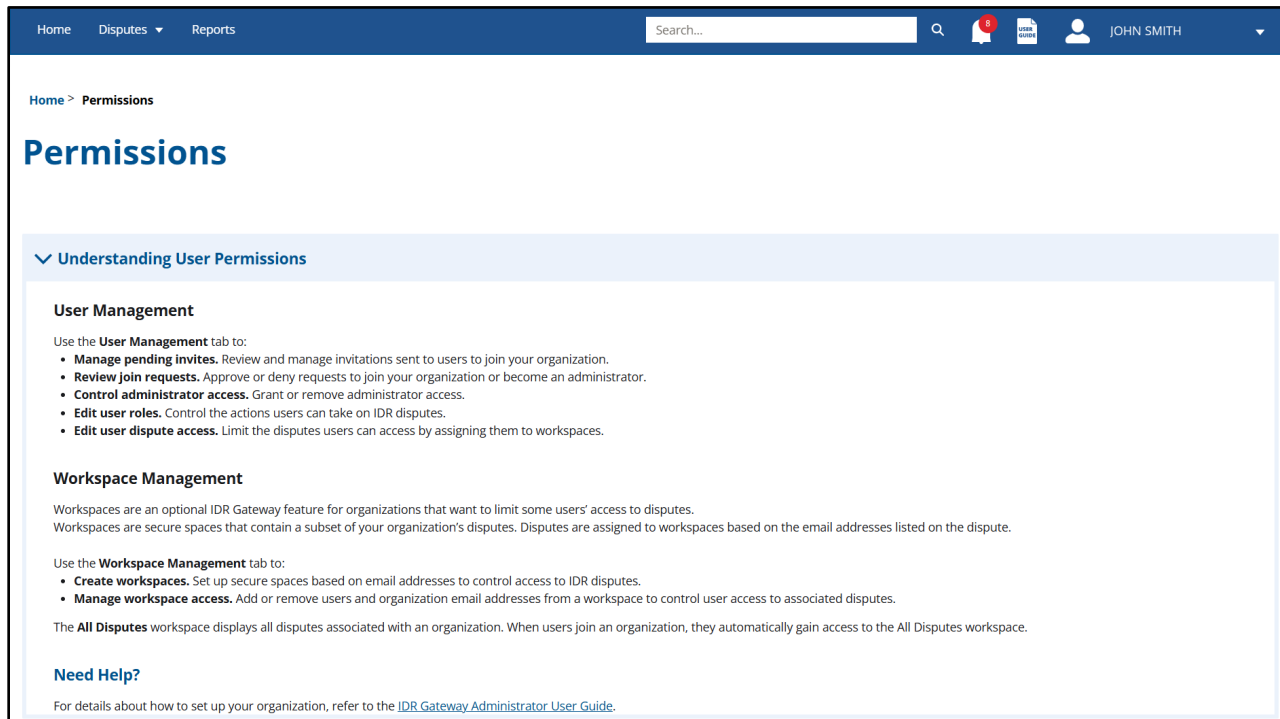


Figure 34. Permissions Page

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

10.2. 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 11.5.

Administrators can assign one of three role types to IDR 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.

10.3. Send an Invitation



Invitations expire in 10 business days.

1. From the Home menu bar, select the **Permissions** option from the user menu dropdown list. The “Permissions” page displays.
2. Select the **User Management** tab. The Organization User Summary section displays.

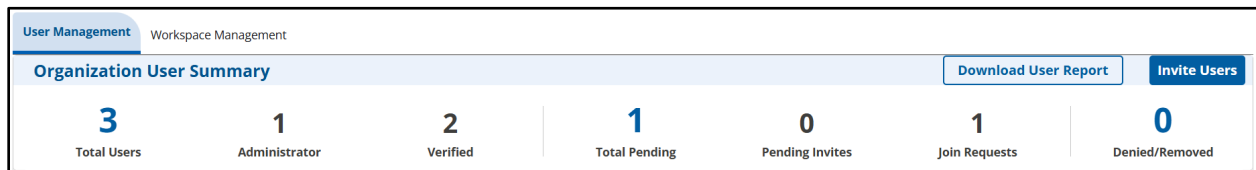


Figure 35. Permissions Page (Organization User Summary, Invite Users Button)

3. From the Organization User Summary section, select the **Invite Users** button. The Invite Users window opens.

Invite user

Complete the fields below, then select **Invite** to invite a user to join your organization.

The Federal IDR Team will send an email to the user with instructions to create an account and join the organization within the IDR Gateway. Users must create an account, verify their identity, and sign in to the IDR Gateway to complete this process. The invitation will expire in 10 business days.

* Indicates a required field

* **First Name:**

* **Last Name:**

* **Email Address:**

Assign Workspaces:
 - Select -

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

* **Assign Roles:**
 ☐ Full Access ☐ View only ☐ Initiation & Selection

[Cancel](#)

Figure 36. Invite Users Window

4. Enter user information in the required fields indicated by an asterisk (*):
 - a. First Name
 - b. Last Name
 - c. Email Address
5. (Optional) Select a workspace from the **Assign Workspaces** field to add the user to that workspace. Refer to Section 12.3 for more information.
6. 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.
7. 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.
8. Select the **Invite** button. The **Invitation sent** confirmation displays on the "Permissions" page and the invitation displays on the **Pending Invites** tab of your My Users table. The user you invited will also receive an email invitation that expires in 10 business days.

Administrators can edit roles, workspaces, and administrator access at any time from the **User Management** tab. Refer to Section 11 for more information.

10.4. Resend an Invitation

When needed, administrators can resend an invitation to join their organization within the IDR Gateway.

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

My Users							
Q Search for users in your organization							
Filters							
Workspaces:				Role:			
- Select -				- Select -		Apply Clear	
Showing 1 - 1 of 1							
	Last Name	First Name	Email	Role	Workspace	Sent Date	Actions
1	Doe	Jane	jane.doe@email.com	Full Access	All Disputes	08/19/2026	Resend

Figure 37. My Users Table (Resend Button)

3. Select the **Pending Invites** tab.

4. Select the **Resend** button in the Actions column next to the appropriate email address. The Resend Invite window opens.

Figure 38. Resend Invite Window



You can update user information when you resend the invitation, such as making the user an administrator or adding the user to a workspace.

5. Review and update the fields, as needed. Required fields are identified with an asterisk (*).
6. Select the **Resend** button. The **Invitation resent** confirmation displays at the top of the page.
 - a. The invitation displays on the **Pending Invites** tab of the My Users table until the user successfully accepts the invitation.
 - b. A **This user has joined an organization** alert displays in the window if the user has joined another organization. You can contact the user to confirm the user joined the correct organization.
 - c. A generic alert displays at the top of the page if the invitation fails to send. You should refresh the page and confirm that you entered the correct user information.

11. 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.

11.1. 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.

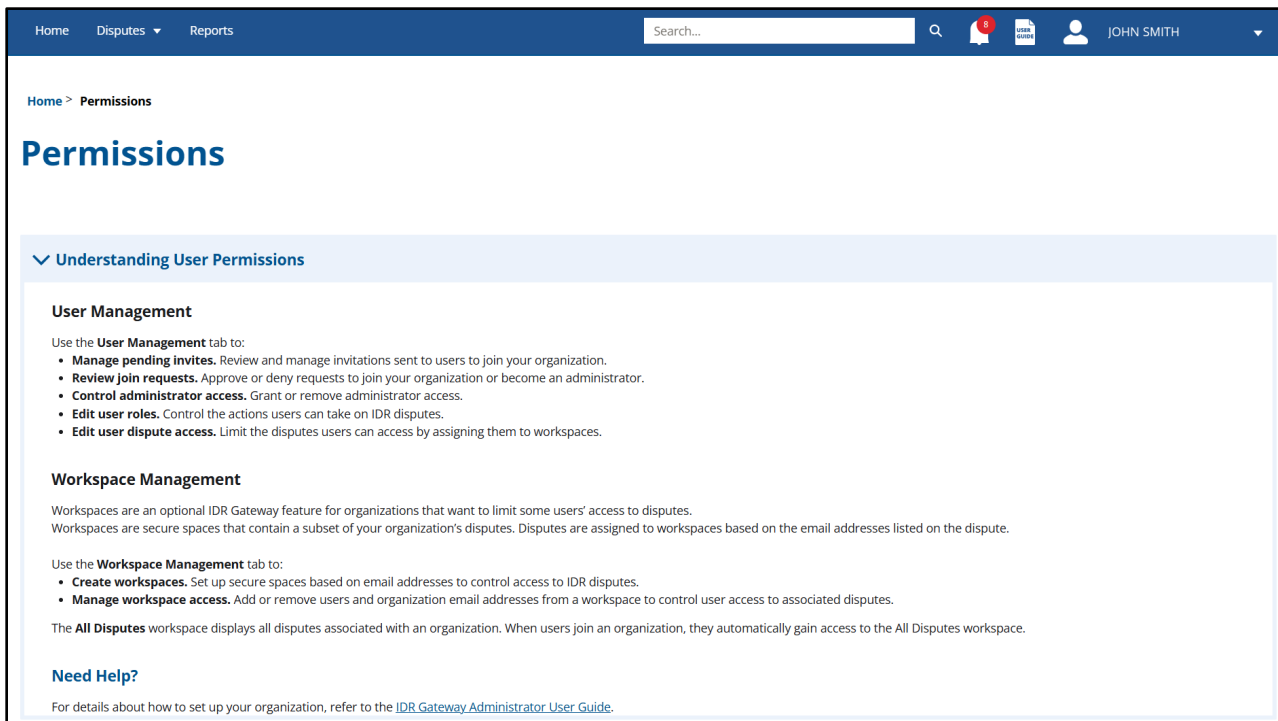


Figure 39. Permissions Page (Understanding User Permissions)

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.

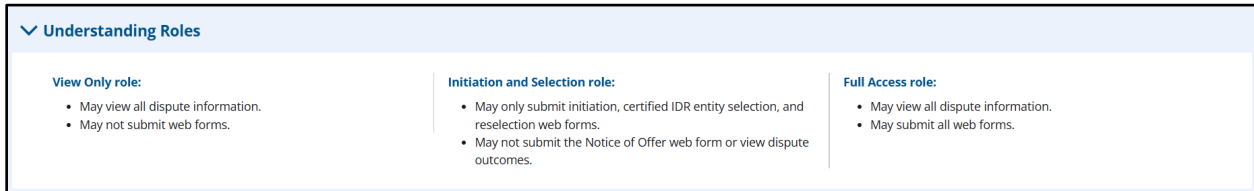


Figure 40. Permissions Page (Understanding Roles)

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 for Total Users (3), Administrator (1), Verified (2), Total Pending (1), Pending Invites (0), Join Requests (1), and Denied/Removed (0). 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 shown, but it is empty with the message 'You do not have any Pending Invites'.

Figure 41. Permissions Page (User Management Tab, My Users Table)

11.2. 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.

This screenshot is identical to Figure 41, 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 42. Permissions Page (User Management Tab, Download User Report Button)

2. Follow the prompts to download and save the file to your computer.

11.3. Search and Filter Users

Administrators can search for and filter users in the "My Users" table by access type, roles, and workspace assignments.

My Users

Search for users in your organization

Filters

Access Type: Workspaces: Role:

Showing 1 - 3 of 3

	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 43. Permissions Page (User Management Tab, Approved Users)

1. To search for users, enter text in the **Search for users in your organization** field.
2. To filter the results in the table, select from the available filter options and select the **Apply** button. The results display in the table.

11.4. Review Join Requests

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

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

User Management Workspace Management

Organization User Summary

3 Total Users **1** Administrator **2** Verified **1** Total Pending **0** Pending Invites **1** Join Requests **0** Denied/Removed

My Users

Search for users in your organization

Filters

Access Type:

Showing 1 - 1 of 1

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

Figure 44. Permissions Page (User Management Tab, Join Requests)

2. Review the user information (name, email address, 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 [X]

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 45. Review User Request Window

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 12.3 for more information.

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.

11.5. 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** tab from the side navigation panel.
2. Select the **Edit** button from the Actions column next to the user. The Edit User window opens.

Figure 46. Edit User Window

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.

12. 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.

12.1. 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 on.

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 an administrator submits a request to the IDR Gateway Help mailbox. When an email address is removed from a workspace, users in that workspace will lose access to all disputes associated with that email address.



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

12.2. Workspace Example

One example where workspaces may be helpful is a large organization with multiple teams that manage disputes through separate inboxes, supporting different clients. In Figure 47, 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.

- 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 works on disputes for Client B and Client C, so the administrator assigns Alex to Workspace B and Workspace C. Susan only works on disputes for Client D, so the administrator assigns

Susan to Workspace D. Jane works on disputes for all three clients, so the administrator does not assign Jane to any of the workspaces as Jane has access to all disputes through the All Disputes workspace.

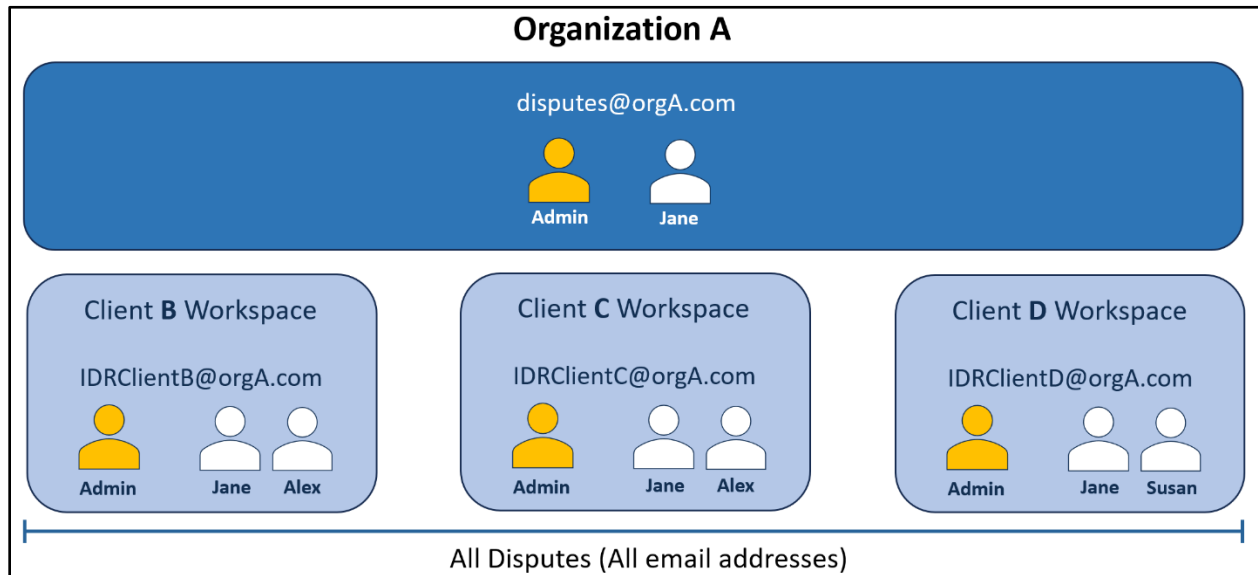


Figure 47. Workspace Example

12.3. 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.

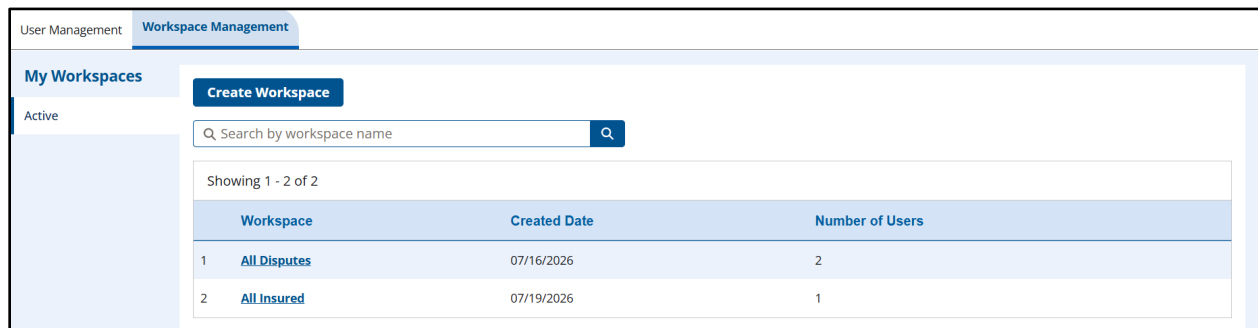
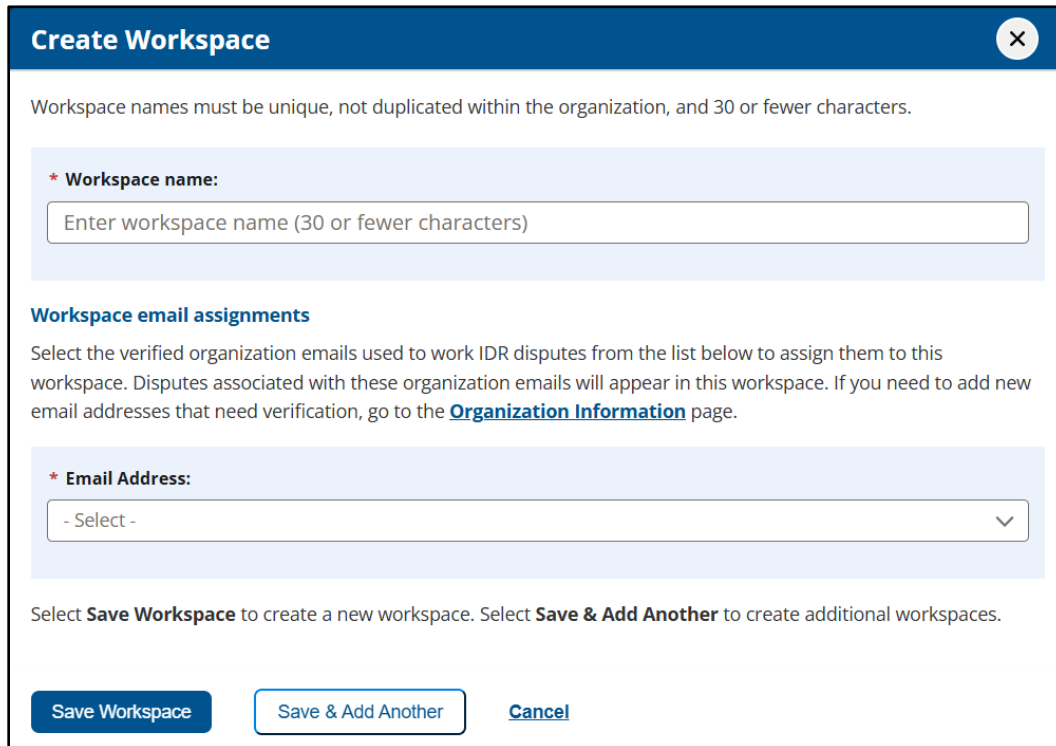


Figure 48. Permissions Page (Workspace Management Tab, Create Workspace Button)

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



Create Workspace

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

* **Workspace name:**

Enter workspace name (30 or fewer characters)

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](#)

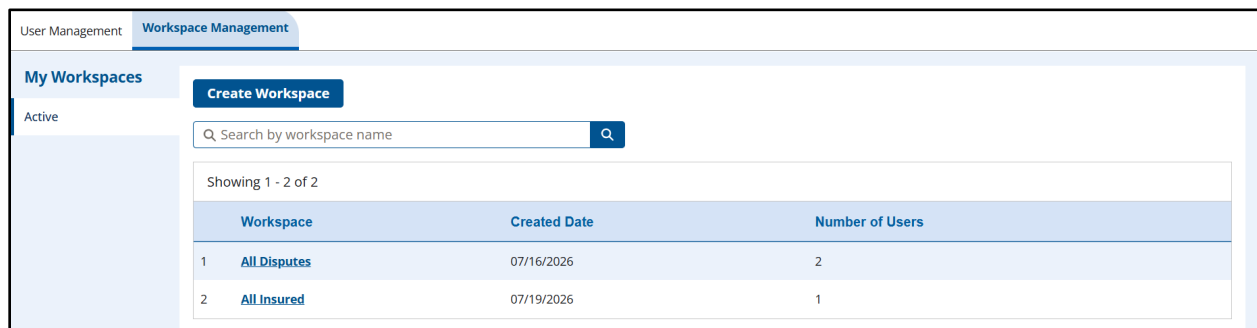
Figure 49. Create Workspace Window

4. From the **Workspace Name** field, enter a unique name for the workspace using 30 or fewer characters.
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.

12.4. 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 50. 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' details page. At the top, there's a navigation bar with 'Home', 'Disputes', and 'Reports'. Below it, a breadcrumb trail reads 'Home > Permissions > Workspace: All Insured'. The main heading is 'Workspace : All Insured'. Under 'Workspace Details', there are three fields: 'Status: Approved', 'Date Created: 7/19/2026', and 'Number of Users: 1'. There are 'Add Users' and 'Add Emails' buttons. Below this, 'Email Addresses in this Workspace' shows one entry: 'health@test.org'. 'Users in this Workspace' shows 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 is a 'Return to Permissions' button.

Figure 51. Workspace Details Page

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

The screenshot shows the 'Add Users' modal window. It has a search bar labeled 'Search user name to add..'. Below it, a table lists one user: Jane Doe (jane.doe@test.org) with a 'View Only' role and 'Verified' access type. There is a checkbox next to her name. At the bottom, there are 'Add Selected Members' and 'Cancel' buttons.

Figure 52. Add Users Window

- To search for users in your organization, enter text in the **Search user name to add** field.
- Select the checkbox next to each user name to add user 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.

12.5. 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' details page. It includes a breadcrumb trail: Home > Permissions > Workspace: All Insured. The page title is 'Workspace : All Insured'. Below the title, there are 'Add Users' and 'Add Emails' buttons. The 'Workspace Details' section shows: Status: Approved, Date Created: 7/19/2026, and Number of Users: 1. The 'Email Addresses in this Workspace' section shows 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 visible next to the user. A 'Return to Permissions' button is at the bottom left.

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

Figure 53. Workspace Details Page (Remove Button)

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 window has a title bar with a close button. The main text asks: 'Are you sure you would like to remove Jane Doe from the All Insured workspace?'. Below this, a warning states: '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, there are 'Remove' and 'Cancel' buttons.

Figure 54. Remove User Window

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 with 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.

12.6. 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 email addresses. The Add Emails window opens.

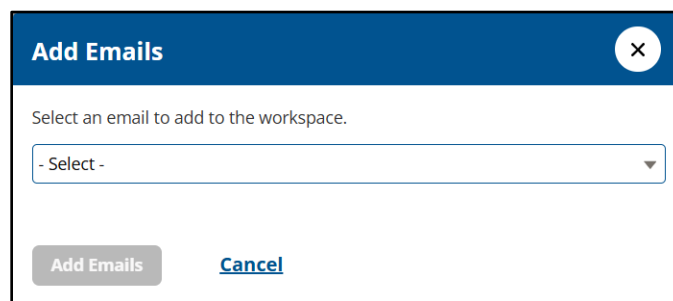


Figure 55. Add Emails Window

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, the administrators haven't added and verified the email address. Refer to Section 7.5 for more information.
 - 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 address.
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 address. Administrators can only remove an email address from a workspace by submitting a service request to CMS.

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

13. Map Disputes

As of September 2026, administrators can confirm or deny ownership of open disputes started outside the IDR Gateway from the “Dispute Mapping” page. Disputes created on or after November 13, 2026, will automatically map to an organization in the IDR Gateway that has verified one of the named party email addresses on the dispute. Therefore, on or after November 13, 2026, administrators will only need to map disputes in two situations:

1. Disputes created before November 13, 2026
2. Disputes created on or after November 13, 2026, for which an organization containing the initiating or non-initiating party’s email address did not exist in the IDR Gateway prior to the dispute creation

After the organization is created in the IDR Gateway, any disputes matched to that organization will appear in the Unconfirmed disputes table. Administrators must map unconfirmed disputes to their organization manually or with a bulk CSV upload.

13.1. Administrator Managed Dispute Mapping Process

Administrator-managed dispute mapping is a three-step process that connects open IDR disputes started outside the IDR Gateway to the organization within the IDR Gateway based on the named party’s email address on the dispute. While confirming or denying ownership of email matched disputes that are not automatically mapped is optional, unmapped disputes will not be viewable in the IDR Gateway dashboards and reports. However, parties can still access and submit the web forms for the unmapped disputes through unique links sent by email.

Step 1. Email Matching

The IDR Gateway identifies instances in which the named party email address in an open dispute started outside the IDR Gateway on or after September 14, 2026, matches the email address for an organization established in the IDR Gateway.

Administrators can view matched disputes in a table on the **Unconfirmed** tab. The IDR Gateway applies a default filter to display results for disputes created within the past 30 calendar days. If results exceed the 50,000 maximum limit with default filters, administrators can adjust the created date range and apply other available filters to further limit results. A downloadable report of the filtered data is available through the **Export Filtered Data** button.

Step 2. Review and Confirm

Administrators download the report by selecting the **Export Filtered Data** button and compare each dispute in the report to their internal records to confirm or deny ownership. If ownership of a dispute is denied, the assigned certified IDR entity must review and confirm the denial is valid.

Step 3. Dispute Mapping

The system maps the confirmed disputes to the organization within the IDR Gateway, making them available for processing on or after November 13, 2026.

13.2. Dispute Mapping Methods

Administrators can confirm or deny ownership of disputes manually or through a bulk dispute mapping (file upload) option.

- **Manual Dispute Mapping.** From the “Dispute Mapping” dropdown or page in the IDR Gateway and **Unconfirmed** tab, confirm or deny ownership of each dispute listed in the Unconfirmed Disputes table.
- **Bulk Dispute Mapping.** Confirm or deny ownership of a large number of disputes at one time by downloading a template CSV file, entering dispute information, and uploading the file to the IDR Gateway.

Refer to Section 13.3 to access the report of open IDR disputes matched to your organization.

Dispute Mapping Page

This page outlines the dispute mapping process and provides an overview of the steps to confirm disputes and to deny disputes. Tabs on the page include **Unconfirmed**, **Confirmed**, **Denied**, **Unconfirmed Line Items**, and **Results**, which display the results once the process of associating existing open IDR disputes to an organization in the IDR Gateway is complete.

Dispute Mapping

Dispute Mapping Process

Dispute mapping is a three-part process that connects open IDR disputes started outside the IDR Gateway to the organization within the IDR Gateway based on the email address on the dispute. While part of this process is optional, unmapped disputes will not be viewable in the IDR Gateway dashboards and reports. However, parties can still access and submit the web forms for the unmapped disputes through unique links sent by email.

Step 1: Email Matching

- The IDR Gateway identifies instances where the named party email address in an open dispute initiated outside the IDR Gateway before September 2026, matches an email address for an organization established within the IDR Gateway.
- Administrators can view matched disputes in a table on the **Unconfirmed** tab. The IDR Gateway applies a default filter to display results for disputes created within the past 30 calendar days.
- If results exceed maximum limits with default filters, administrators can adjust the date range and apply other available filters to further limit results.
- A report of the filtered data is available through the **Export Filtered Data** button.

Step 2: Review and Confirm

- Administrators download the report by selecting the **Export Filtered Data** button and compare each dispute in the report to their internal records to confirm or deny ownership.
- Confirmation of matched disputes is optional; as noted above, however, unmapped disputes will not be viewable in the IDR Gateway dashboards and reports.
- If a dispute is denied, the assigned certified IDR entity must review and confirm ownership.

Step 3: Dispute Mapping

- The system maps the confirmed disputes to the organization within the IDR Gateway, making them available for processing in November

> Mapping Methods

⚠ Once you deny a dispute, your organization will not be able to access information about that dispute in the IDR Gateway. If you suspect a privacy and security issue has occurred, refer to the [Privacy & Security Information](#) page for information on how to report an issue.

Unconfirmed

Confirmed

Denied

Unconfirmed L...

Results

Bulk Dispute Upload ↗

Filters

Dispute Number Search:

* Created Date Range (30 days max): ⓘ

Sep 6, 2026 📅

Oct 6, 2026 📅

Certified IDR Entity:

Email:

- Select -

- Select -

Unconfirmed Disputes

Confirm Selected Disputes

Deny Dispute Ownership

Export Filtered Data

Showing 1 - 500 of 1,000

| Results matching your filters: 1,000

| TestOrgC's total disputes: 1,000

Figure 56. Dispute Mapping Page

- **Confirmed disputes.** An administrator confirms that the organization is responsible for processing the dispute that was matched to the organization. The organization will have access to these dispute records in the IDR Gateway when the dashboards, reports, and web forms become available on November 13, 2026.
- **Denied disputes.** An administrator denies that the organization is responsible for processing of the dispute that was matched to the organization. If an administrator denies ownership of a dispute, the certified IDR entity assigned to the dispute must review documentation associated with the dispute to confirm the denial is valid. If the certified IDR entity confirms the denial, the

organization will not have access to the dispute record in the IDR Gateway when the dashboards, reports, and web forms become available on November 13, 2026.

Additional denied disputes information:

If a party denies ownership of a dispute, the IDR Gateway sends that dispute to the certified IDR entity to review the denial and any evidence to support it or not. The certified IDR entity then confirms or rejects the denial.

- If the certified IDR entity **confirms the denial** (organization does not own the dispute), the certified IDR entity should close the dispute as ineligible.
- If the certified IDR entity **rejects the denial** (organization owns the dispute), the dispute will be automatically mapped to the organization and will show on the **Confirmed** tab.

Example:

A certified IDR entity could reject a denial if it finds evidence that the email address for the organization that denied the dispute is on the Remittance Advice and the remittance has the same provider, claim number, item, or service on the dispute.

In that case, the certified IDR entity would reject the denial, and notifications are sent to the administrator.



Until the certified IDR entity review is complete, organizations must continue following Federal IDR process requirements and deadlines.

Understanding Dispute Mapping Filters

The dispute mapping tables show filtered data based on either default or user-selected filters. The filters:

- Limit the created date range to 30 calendar days
- Default to a 30-calendar-day date range
- Display up to 50,000 results

Administrators can download a CSV file of up to 50,000 results by selecting the **Export Filtered Data** button.



If filters match more than 50,000 results, the **Export Filtered Data** button is disabled and an error displays. Adjust the filters to narrow the results.

This table can only display up to 50,000 disputes. The IDR Gateway has identified 560,002 disputes that meet the currently selected filters. Current results exceed the maximum limit. Adjust the filters to narrow the results. Exported results are based on selected filters. Refer to the Dispute Processing User Guide for tips on adjusting filters.

Unconfirmed Disputes		Confirm Selected Disputes	Deny Dispute Ownership	Export Filtered Data
Showing 1 - 500 of 49,998	Results matching your filters: 176,890	ABC Organization's unconfirmed disputes: 560,002		

Figure 57. Unconfirmed Disputes (Maximum Results Exceeded Error)

13.3. Export Filtered Data and Review Disputes

Administrators should review the Unconfirmed Disputes table on the **Unconfirmed** tab or download results using the **Export Filtered Data** button and review the disputes to determine which email matched disputes are owned by the organization.



Administrators need the dispute number to confirm or deny ownership of a dispute. If the dispute number is not available, administrators can use the **Unconfirmed Line Items** tab to identify disputes by claim number. Refer to Section 13.5 for more information.

1. From the Home menu bar, select the **Dispute Mapping** option from the user menu dropdown list. The “Dispute Mapping” page displays.
2. Select the **Unconfirmed** tab to display the disputes matched to your organization. This table will display up to 50,000 unconfirmed disputes. Adjust the filters if necessary.



Refer to Section 13.2 for more information on default filters and result limits.

3. Select the **Export Filtered Data** button to download a report of email matched disputes. The Download In Progress window opens.

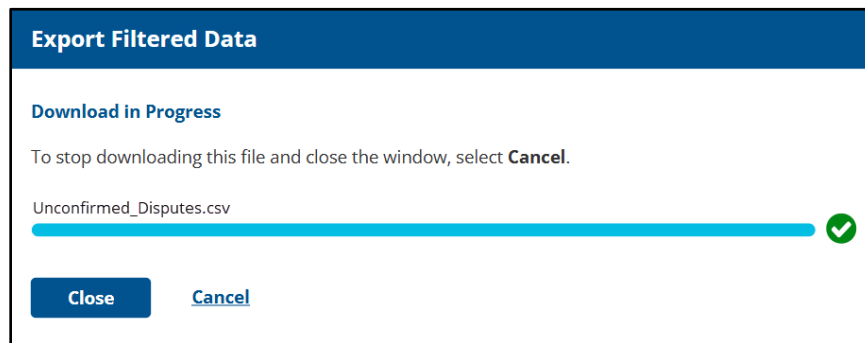


Figure 58. Export Filtered Data Results Window (Unconfirmed_Disputes.csv)

4. Select the **Close** button once the download is complete.
5. Open the report to review the disputes matched to your organization.

13.4. Manual Dispute Mapping

Administrators can review and manually confirm or deny ownership of the open IDR disputes email matched to their organization on the **Unconfirmed** tab.

1. From the Home menu bar, select the **Dispute Mapping** option from the user menu dropdown list. The “Dispute Mapping” page displays.
2. Select the **Unconfirmed** tab to display the disputes matched to your organization. This table will display up to 50,000 unconfirmed disputes. Adjust the filters if necessary.



Refer to Section 13.2 for more information on default filters and result limits.

The screenshot shows the 'Unconfirmed' tab selected. At the top, there are tabs for 'Unconfirmed', 'Confirmed', 'Denied', 'Unconfirmed Line Items', and 'Results'. A 'Bulk Dispute Upload' link is in the top right. Below the tabs is a 'Filters' section with a 'Dispute Number Search' field, a 'Created Date Range' filter (set to Aug 28, 2026 to Sep 29, 2026), and dropdowns for 'Certified IDR Entity' and 'Email'. Buttons for 'Apply' and 'Clear' are present. Below the filters, there are buttons for 'Confirm Selected Disputes', 'Deny Dispute Ownership', and 'Export Filtered Data'. A summary bar shows 'Showing 1 - 500 of 49,998' results, with '49,998' results matching filters and '210,996' for the selected organization. The table below has columns: Dispute Number, Created Date, Initiating Party Name, Initiating Party Email, Non-Initiating Party Name, Non-Initiating Party Email, and Certified IDR Entity. The first six rows of data are visible, showing disputes from ABC Healthcare and Non-Initiating Party Group, Inc.

Dispute Number	Created Date	Initiating Party Name	Initiating Party Email	Non-Initiating Party Name	Non-Initiating Party Email	Certified IDR Entity
DISP-159874	11/6/2025	ABC Healthcare	email@abchealth.com	Non-Initiating Party Group, Inc.	stopemailingme@nipg.com	Disputes R Us
DISP-159877	11/6/2025	ABC Healthcare	email@abchealth.com	We Have Group Health Plans 4...	faxme@whgh4y.com	Resolutions, Inc.
DISP-159871	11/6/2025	ABC Healthcare	email@abchealth.com	Non-Initiating Party Group, Inc.	stopemailingme@nipg.com	Disputes R Us
DISP-159870	11/6/2025	ABC Healthcare	email@abchealth.com	Non-Initiating Party Group, Inc.	stopemailingme@nipg.com	Disputes R Us
DISP-159875	10/31/2025	ABC Healthcare	email@abchealth.com	We Have Group Health Plans 4...	faxme@whgh4y.com	Disputes R Us
DISP-159876	10/31/2025	ABC Healthcare	email@abchealth.com	We Have Group Health Plans 4...	faxme@whgh4y.com	Resolutions, Inc.
DISP-159890	10/24/2025	ABC Healthcare	email@abchealth.com	Non-Initiating Party Group, Inc.	stopemailingme@nipg.com	We Resolve

Figure 59. Dispute Mapping Page (Unconfirmed Tab)

Confirm Ownership of Disputes

1. Select the checkboxes next to each dispute number that is correctly email matched to your organization or select the checkbox in the column header row to select all disputes on the page.
 - a. To search for a dispute, enter the dispute number in the **Dispute Number Search** field. The search results are limited to the selected table filters (including the 30-calendar-day created date range filter).
 - b. To filter the disputes, select from the filter options (Created Date Range, Certified IDR Entity, or Email) and select the **Apply** button.



Reminder: Information displayed in the table is limited to a 30-calendar-day created date range and displays up to 50,000 results.

2. Select the **Confirm Selected Disputes** button. The Confirm Disputes window opens.

Confirm Disputes

You have indicated 5 disputes should be mapped to **TestOrgZ**.

* Indicates a required field.

Are you sure you want to confirm the disputes?

* ☐ I confirm the selected disputes belong to **TestOrgZ**.

Confirm Disputes

Cancel

Figure 60. Confirm Disputes Window

- 3. Select the checkbox to confirm your organization owns the selected disputes.
- 4. Select the **Confirm Disputes** button. The confirmed disputes move to the **Confirmed** tab and an alert displays the results of the dispute mapping action.

Disputes confirmed

You confirmed 1 disputes belong to **TestOrgC**. Confirmed disputes display on the **Confirmed** tab.

Figure 61. Dispute Mapping Page (Disputes Confirmed Alert)

- 5. Navigate to the **Confirmed** tab of the “Dispute Mapping” page for a list of confirmed disputes.

Unconfirmed

Confirmed

Denied

Unconfirmed Line Items

Results

Bulk Dispute Upload

Filters

Dispute Number Search:

Q

Search for filtered results by dispute number (DISP-XXXXXX)

* Created Date Range (30 days max):

Aug 28, 2026

Sep 29, 2026

Apply

Clear

Certified IDR Entity:

- All -

Email:

- All -

Confirmed Disputes

Confirm Selected Disputes

Deny Dispute Ownership

Export Filtered Data

Showing 1 - 500 of 49,998

Results matching your filters:

49,998

ABC's Organization's confirmed disputes:

210,996

Dispute Number	Created Date	Initiating Party Name	Initiating Party Email	Non-Initiating Party Name	Non-Initiating Party Email	Certified IDR Entity
DISP-159874	11/6/2025	Provider 123456	email@provider.com	Apex Insurance	apex.insurance@email.com	Disputes R Us
DISP-159877	11/6/2025	Provider 123456	email@provider.com	Apex Insurance	apex.insurance@email.com	Resolutions, Inc.
DISP-159879	11/6/2025	Provider 123456	email@provider.com	Apex Insurance	apex.insurance@email.com	Disputes R Us

Figure 62. Dispute Mapping Page (Confirmed Tab)

- 6. Navigate to the **Results** tab of the “Dispute Mapping” page for mapping details.

Unconfirmed	Confirmed	Denied	Unconfirmed Line Items	Results	Bulk Dispute Upload ↗
-------------	-----------	--------	------------------------	----------------	---------------------------------------

Mapping Results

You can download mapping results from the manual or CSV upload process. Files are archived after 30 calendar days. If you need to access a file that has been archived email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059.

Q Search disputes by number or keyword [Q](#)

Results

Showing 1 - 6 of 6

File Name	Mapping Method	Created Date	Action
OriginalFileName_04142026_163235	CSV Upload	04/14/2026	Download Results
BulkUploadFile_04142026_160245	CSV Upload	04/14/2026	Download Results
UploadProcessFile_04142026_142425	Manual	04/14/2026	Download Results
FileNameExample_04132026_111312	CSV Upload	04/13/2026	Download Results
ManualSelection_04132026_102437	Manual	04/13/2026	Download Results
ProcessedFileName_04102026_093601	CSV Upload	04/10/2026	Download Results

Figure 63. Dispute Mapping Page (Results Tab)

Deny Ownership of Disputes

1. Select the checkboxes next to the dispute numbers incorrectly email matched to your organization and select the **Deny Dispute Ownership** button. The Deny Dispute Ownership window opens.

Deny Dispute Ownership [✕](#)

⚠ This process cannot be undone.

You have indicated **2** disputes do not belong to **TestOrgZ**.

* Indicates a required field.

Are you sure you want to deny the disputes?

- If you deny the disputes, you will not be able to access the disputes in the IDR Gateway.
- A certified IDR entity will review each denied dispute to determine ownership.
- Until the certified IDR entity completes its review, you should continue to follow Federal IDR process requirements and deadlines.

* ☐ I attest the selected disputes do not belong to **TestOrgZ**.

[Deny Disputes](#)
[Cancel](#)

Figure 64. Deny Dispute Ownership Window

2. Select the checkbox to confirm your organization does not own the selected disputes.
3. Select the **Deny Disputes** button. The denied disputes move to the **Denied** tab and an alert displays the results of the dispute mapping action.
 - a. When you deny ownership of a dispute, your organization can't access information about that dispute in the IDR Gateway.
 - b. A certified IDR entity must review the denied disputes to verify the denial is valid.

Disputes denied

You denied dispute ownership for 1 disputes. Denied disputes display on the **Denied** tab. The certified IDR entity assigned to the dispute will review each denied dispute to confirm ownership. If you denied any disputes in error, contact the certified IDR entity assigned to the dispute or email IDRGatewayHelp@cms.hhs.gov.

Figure 65. Dispute Mapping Page (Disputes Denied Alert)

4. Navigate to the **Denied** tab on the “Dispute Mapping” page for a list of denied disputes.

Unconfirmed
Confirmed
Denied
Unconfirmed Line Items
Results
Bulk Dispute Upload

Filters

Dispute Number Search:
* Created Date Range (30 days max):

Certified IDR Entity:

Denied Disputes

Showing 1 - 500 of 49,998
Results matching your filters:
49,998
ABC's Organization's denied disputes:
897,026

Dispute Number	Created Date	Initiating Party Name	Initiating Party Email	Non-Initiating Party Na...	Non-Initiating Part...	Certified IDR Entity	IDRE Review	Denied Date
DISP-159874	11/6/2025	Provider 123456	email@provider.c...	Apex Insurance	apex.insurance@em...	Disputes R Us	TBD	02/27/2026
DISP-159877	11/6/2025	Provider 123456	email@provider.c...	Apex Insurance	apex.insurance@em...	Resolutions, Inc.	TBD	02/27/2026
DISP-159879	11/6/2025	Provider 123456	email@provider.c...	Apex Insurance	apex.insurance@em...	Disputes R Us	TBD	02/27/2026

Figure 66. Dispute Mapping Page (Denied Tab)

5. Until the review is complete, organizations must continue following Federal IDR process requirements and deadlines.
 - a. If the certified IDR entity confirms the denial, the dispute remains in the **Denied** tab.
 - b. If the certified IDR entity rejects the denial, the dispute moves to the **Confirmed** tab.



If you suspect a privacy and security issue has occurred, refer to the “Privacy & Security” information page for information on how to report an issue.

13.5. Find Dispute Numbers Using Claim Numbers

If administrators do not know the dispute number, they can use the **Unconfirmed Line Items** tab to identify their disputes by claim number.

1. Select the **Unconfirmed Line Items** tab from the “Dispute Mapping” page. This table displays up to 50,000 unconfirmed disputes. Adjust the filters if necessary.



Refer to Section 13.2 for more information on default filters and result limits.

2. Review entries using the Claim Number column to find the corresponding Dispute Number.

Dispute Number	Created Date	Initiating Party Name	Initiating Party Email	Non-Initiating Party Name	Non-Initiating Party Name	Certified IDR Entity	Dispute Line Item Name	Claim Number
DISP-159874	11/6/2025	Provider 123456	email@provider.c...	Apex Insurance	apex.insurance@em...	Disputes R Us	DLI-20582548	6184503V7B...
DISP-159874	11/6/2025	Provider 123456	email@provider.c...	Apex Insurance	apex.insurance@em...	Disputes R Us	DLI-20582546	618450D7B3...
DISP-159874	11/6/2025	Provider 123456	email@provider.c...	Apex Insurance	apex.insurance@em...	Disputes R Us	DLI-20582549	618450W97B...

Figure 67. Dispute Mapping Page (Unconfirmed Line Items Tab)

13.6. Bulk Dispute Mapping (File Upload)

Administrators can confirm or deny ownership of a large number of disputes at one time using the bulk dispute mapping file upload option.

Step 1: Download and complete the template.

1. From the Home menu bar, select the **Dispute Mapping** option from the user menu dropdown list. The “Dispute Mapping” page displays.
2. Select the **Unconfirmed** tab to display the disputes matched to your organization. This table displays up to 50,000 unconfirmed disputes. Adjust the filters if necessary.



Refer to Section 13.2 for more information on default filters and result limits.

3. Select the **Export Filtered Data** button to download and review the disputes email matched to your organization.
4. Select the **Bulk Dispute Upload** button. The “Bulk Dispute Mapping” page displays.

Home > Dispute Mapping > Bulk Dispute Mapping

Bulk Dispute Mapping

The bulk dispute mapping file upload option allows administrators to confirm or deny ownership of a large number of disputes at one time.

Upload information:

- **File Type.** Only upload one comma-separated values (CSV) file at a time.
- **File Size Limit.** A single upload cannot exceed 50,000 records or 5MB.
- **Format.**
 - Do not delete or overwrite the header information.
 - Dispute Number = "DISP-XXXXXX"
 - Dispute Ownership = "Confirm" or "Deny"
 - Do not include duplicate dispute numbers, closed disputes, disputes that the system did not match to your organization, or previously confirmed or denied disputes.
- **Validate.** Confirm data is correct. Denied disputes will not be accessible in the IDR Gateway.
- **Upload Time.** It may take up to 30 minutes to process a file. A notification is sent upon completion.
- **Results.** The mapping results file provides the success or failure of each dispute in the Dispute Validation column.

* Indicates a required field.

Bulk Dispute Mapping Template

1. Download the instructions.
2. Download the template.
 - Enter dispute numbers for every open dispute in the Dispute Number column. You can download a report of the disputes on the Unconfirmed tab to use to fill in this template.
 - Enter "Confirm" or "Deny" for each dispute in the Dispute Ownership column.
5. Save as a .csv file.

Bulk Dispute Mapping Instructions:
[bulk_dispute_mapping_instructions.pdf](#)

Bulk Dispute Mapping Template:
[bulk_dispute_mapping_template.csv](#)

Bulk Dispute Mapping Upload

1. Upload the file.
2. Select **Submit** to map the disputes.

Note: Mapping may take up to 30 minutes. You'll be notified upon completion and receive a mapping results file showing which disputes were successfully confirmed or denied and which disputes failed to map.

* Upload CSV File:

Choose one file

File limitations (Single .CSV file, file name 225 or fewer characters, no duplicate disputes, no more than 50,000 records, no larger than 5MB)

Submit **Cancel**

Figure 68. Bulk Dispute Mapping Page

5. Review the bulk file upload requirements:
 - a. Only upload one CSV file at a time.
 - b. A single upload cannot exceed 50,000 records or 5MB.
 - c. Do not delete or overwrite the header information in the template.
 - d. Dispute Number format must be "DISP-XXXXXX."
 - e. Dispute Ownership must be "Confirm" or "Deny."
 - f. Do not include duplicate dispute numbers, closed disputes or previously denied or confirmed disputes.
 - g. Confirm the data is correct. Denied disputes will not be accessible in the IDR Gateway.
 - h. It may take up to 30 minutes to process a file, depending on the size of the file. Results are available after processing completes.
 - i. The success or failure of each dispute is detailed in the Dispute Validation column of the mapping results file.

6. Select the **bulk_dispute_mapping_template.csv** link to download the template.
7. Open the template and copy and paste the dispute numbers into the template from the disputes previously exported. Each row should have one dispute number.
 - a. In Column A, starting in Row 2, enter each dispute number in the format: **DISP-XXXXXX**.
 - b. In Column B, next to each dispute number, enter **Confirm** if your organization owns the dispute or **Deny** if your organization does not own the dispute.
8. Save the file in the CSV format with a file name containing 200 or fewer characters.

Step 2: Upload the dispute mapping CSV file.

1. Drag and drop the saved file into the **Upload CSV File** section or select the **Upload** button to locate and upload the file.

Figure 69. Bulk Dispute Mapping Upload Window

2. Select the **Submit** button. The “File Processing In Progress” message displays and the system begins to confirm and/or deny ownership of disputes based on the information in the CSV file.
3. Select the **Return to Dispute Mapping** button to return to the “Dispute Mapping” page or select the **Begin New Upload** button to upload a new bulk dispute mapping file. When file processing is complete, a CSV file generates on the **Results** tab, and disputes move to the **Confirmed** or **Denied** tab.



Dispute mapping may take up to 30 minutes, depending on the size of the file.
Results are available after processing has completed.

13.7. Review Dispute Mapping Results

Administrators can download results for both the manual process and the bulk file upload process.

1. From the Home menu bar, select the **Dispute Mapping** option from the user menu dropdown list. The “Dispute Mapping” page displays.
2. Select the **Results** tab.

Mapping Results

You can download mapping results from the manual or CSV upload process. Files are archived after 30 calendar days. If you need to access a file that has been archived email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059.

Search disputes by number or keyword

File Name	Mapping Method	Created Date	Action
OriginalFileName_04142026_163235	CSV Upload	04/14/2026	Download Results
BulkUploadFile_04142026_160245	CSV Upload	04/14/2026	Download Results
UploadProcessFile_04142026_142425	Manual	04/14/2026	Download Results
FileNameExample_04132026_111312	CSV Upload	04/13/2026	Download Results
ManualSelection_04132026_102437	Manual	04/13/2026	Download Results
ProcessedFileName_04102026_093601	CSV Upload	04/10/2026	Download Results

< Previous 1 Next >

Figure 70. Dispute Mapping Page (Results Tab)

3. Select the **Download Results** button in the Action column. Your browser downloads the results file.
4. Open the saved file to view the results.
 - a. The **Status** column indicates if dispute ownership was successfully confirmed or denied or if an error occurred.
 - b. If an error occurred, a description of the error displays in the **Error Message** column.
 - c. Disputes mapped to your organization display on the **Confirmed** tab.

	A	B	C	D
1	Dispute Number	Dispute Ownership	Status	Error Message
2	DISP-XXXXXXX	Confirm	Success	
3	DISP-XXXXXXX	Confirm	Success	
4	DISP-XXXXXXX	Deny	Error	Dispute closed. Dispute not eligible for dispute mapping.
5				

Figure 71. Dispute Mapping Results File

13.8. Dispute Mapping Errors

If an administrator incorrectly denies ownership of a dispute, the administrator must contact the certified IDR entity listed on the dispute. If an administrator incorrectly confirms ownership of a dispute, the administrator must email the IDR Gateway Help Desk (IDRGatewayHelp@cms.hhs.gov) to make the correction.

13.9. Changes to Dispute Email Addresses

If a certified IDR entity updates one of the named party email addresses on a dispute that has been previously mapped to an email address belonging to another party, the organization associated with the email address that was removed from the dispute will no longer be able to access the dispute record in the IDR Gateway. Administrators that lose access to a dispute record in this way will receive an email and notification informing them that they no longer have access to a dispute because the certified IDR entity removed the dispute from the organization by changing the disputing party's email address. The message will be "A certified IDR entity reassigned dispute ownership in the IDR Gateway."

If the certified IDR entity incorrectly updated the email address associated with the dispute, contact the certified IDR entity listed on the dispute or email the IDR Gateway Help Desk (IDRGatewayHelp@cms.hhs.gov) for help.

14. Search for Disputes

A global search option is available from the Menu bar to allow users to search for a dispute by number or keyword (dispute details). A global search returns the first 5 results at both the dispute and dispute line item level across all open disputes and disputes closed within the previous 7 calendar days of the search. Users can view up to 200 search results by selecting the **View More** button.



If a user enters the full dispute number for a dispute that has been successfully mapped to the organization within the IDR Gateway, the global search feature will return a single result, even if the dispute was closed more than 7 calendar days prior to the date of the search. Only disputes that were open as of September 14, 2026, are currently available in the IDR Gateway.

Users can also search for disputes within the Open, Selection Due, Offers Due, and Closed tabs of the “Disputes” page to find disputes in specific phases. Refer to Sections 10.3 through 10.6 for more information on the data available on the “Disputes” page.

14.1. To search for a dispute using a global search:

1. Enter at least three characters of a dispute number, keyword, or any dispute details in the **Search** field in the Menu bar. The “Search Results” page displays.



To return fewer results, search using the exact dispute number or claim number. You can also use field names or other report values. Refer to Section 11 for more information.

Home

Disputes

Reports

DISP-1537

4

JOHN SMITH

Search Results

Disputes

5+ Results

Top Results

Disputes

Dispute Line Items

Dispute Name	Dispute Phase	Certified IDR Entity	Initiating Party	Initiating Party Email	Non-Initiating Party	Non-Initiating Party Email	Created Date
DISP-153798	Select IDRE	TBD	Healthcare ABC	jane.doe@gmail.com	Payer Co.	john.doe@gmail.com	05/07/2026, 4:43 PM
DISP-153792	Select IDRE	TBD	Healthcare ABC	jane.doe@gmail.com	ShieldPoint Corporat...	john.doe@gmail.com	05/08/2026, 2:23 PM
DISP-153789	IDRE Eligibility ...	IDR Disputes Co.	Healthcare ABC	jane.doe@gmail.com	National Group Insur..	john.doe@gmail.com	05/01/2026, 3:00 PM
DISP-153787	IDRE Eligibility ...	MediResolutions...	Healthcare ABC	jane.doe@gmail.com	National Group Insur..	john.doe@gmail.com	04/30/2026, 11:43 AM
DISP-153786	IDRE Eligibility ...	IDR Disputes Co.	Healthcare ABC	jane.doe@gmail.com	ShieldPoint Corporat...	john.doe@gmail.com	04/29/2026, 4:24 PM

View More

Dispute Line Items

Description of Item or Service	Line Item Type	Claim Number	Date of Service	Service Code	Service Code Modifier	Place of Service Code	Location of Service
ssW		04634634534	7/1/2026	12		12	AK
dedth		7656456	7/21/2026	542		54	AK
test	Bundled Item or Service	1656656	5/6/2026	3355	33, 85, 12	33	AK
test2		04634634534	4/27/2026	8512		85	AK
test3		12369855555	4/21/2026	4757		47	AK

Figure 72. Search Results

2. Select the **View More** button to view additional search results at the dispute or dispute line item level. Search results display in the table.

IDR Dispute Name	Dispute Phase	IDR Entity	Initiating Party	Initiating Party Email	Non-Initiating Party	Non-Initiating Party Email	Created
DISP-153798	Select IDRE	TBD	Healthcare ABC	jane.doe@gmail.com	Payer Co.	john.doe@gmail.com	05/07/2020
DISP-153792	Select IDRE	TBD	Healthcare ABC	jane.doe@gmail.com	ShieldPoint Corporat...	john.doe@gmail.com	05/08/2020
DISP-153789	IDRE Eligibility ...	IDR Disputes Co.	Healthcare ABC	jane.doe@gmail.com	National Group Insur...	john.doe@gmail.com	05/01/2020
DISP-153787	IDRE Eligibility ...	MediResolutions...	Healthcare ABC	jane.doe@gmail.com	National Group Insur...	john.doe@gmail.com	04/30/2020
DISP-153786	IDRE Eligibility ...	IDR Disputes Co.	Healthcare ABC	jane.doe@gmail.com	ShieldPoint Corporat...	john.doe@gmail.com	04/29/2020
DISP-153756	IDRE Eligibility ...	IDR Disputes Co.	Healthcare ABC	jane.doe@gmail.com	Payer Co.	john.doe@gmail.com	04/29/2020
DISP-153753	Submit Offer	MediResolutions...	Healthcare ABC	jane.doe@gmail.com	ShieldPoint Corporat...	john.doe@gmail.com	04/27/2020
DISP-153752	Submit Offer	IDR Disputes Co.	Healthcare ABC	jane.doe@gmail.com	National Group Insur...	john.doe@gmail.com	04/24/2020
DISP-153745	Submit Offer	MediResolutions...	Healthcare ABC	jane.doe@gmail.com	National Group Insur...	john.doe@gmail.com	04/22/2020
DISP-153743	IDRE Offer Revi...	Neutral Outcomes	Healthcare ABC	jane.doe@gmail.com	ShieldPoint Corporat...	john.doe@gmail.com	04/22/2020
DISP-153734	IDRE Offer Revi...	MediResolutions...	Healthcare ABC	jane.doe@gmail.com	Payer Co.	john.doe@gmail.com	04/22/2020
DISP-153733	IDRE Offer Revi...	MediResolutions...	Healthcare ABC	jane.doe@gmail.com	ShieldPoint Corporat...	john.doe@gmail.com	04/21/2020
DISP-153732	Payment Deter...	MediResolutions...	Healthcare ABC	jane.doe@gmail.com	National Group Insur...	john.doe@gmail.com	04/21/2020
DISP-153729	Payment Deter...	IDR Disputes Co.	Healthcare ABC	jane.doe@gmail.com	National Group Insur...	john.doe@gmail.com	04/21/2020

Figure 73. IDR Disputes Search Results

3. To filter the results, select from the available filter options and select the **Apply** button. The results display in the table.



Narrowing results by the Created Date filter reduces the time required to return search results.

4. Select the dropdown arrow next to a column name to sort the results in ascending or descending order.
5. Select a dispute number link in the IDR Dispute table to display the dispute details.

15. Access Reports

The Reports option on the Menu bar is available to help users view and filter information for their organization's disputes. Administrators will also have access to administrator-only reports currently available on the "Permissions" and "Dispute Mapping" pages. These reports include only the disputes your organization started in the IDR Gateway, or disputes started outside the IDR Gateway that your organization successfully mapped and confirmed.

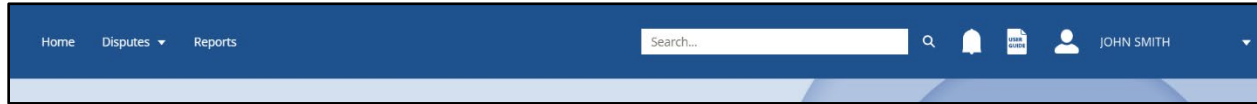


Figure 74. Menu Bar (Reports Option)

15.1. Reports Available in the IDR Gateway

Users will have access to the following reports:

- **All Disputes.** All open and closed disputes associated with your organization in the IDR Gateway that have been confirmed (mapped), and were not closed prior to September 14, 2026 (the launch of the IDR Gateway)
- **Open Dispute Line Items.** Individual qualified items or services (line items) within mapped, open disputes associated with your organization
- **Closed Dispute Line Items.** Individual qualified items or services (line items) that are closed for any reason (not eligible, settlement, withdrawn, unpaid fee, payment determination reached, or administrative closure) within mapped, closed disputes associated with your organization
- **Resubmission Requested Line Items.** Individual qualified items or services (line items) the certified IDR entity is requesting the organization to resubmit within mapped disputes associated with your organization
- **Selection Due.** All open disputes associated with your organization in the IDR Gateway that have been confirmed (mapped) where the certified IDR entity selection response is due within the next 30 calendar days
- **Offers Due.** All open disputes associated with your organization in the IDR Gateway that have been confirmed (mapped) where the submission of offers is due within the next 30 calendar days



[Refer to Section 15.2 for more information on date range filters and result limits.](#)

Administrators can also access the following administrator-only reports:

- The "Permissions" page allows administrators to download a User Report of the information in the My Users table.
- The "Dispute Mapping" page allows administrators to export filtered dispute data. Refer to Section 13.3 for the instructions to export filtered data from each of the following tabs.
 - **Unconfirmed.** Disputes email-matched to the organization that administrators review to determine which disputes are owned by the organization.
 - **Confirmed.** Disputes the administrator confirmed the organization is responsible for processing.

- **Denied.** Disputes the administrator denied the organization is responsible for processing.
- **Unconfirmed Line Items.** Dispute line items email matched to the organization the administrator must review to determine if they are owned by the organization.



Filters on the “Dispute Mapping” page differ from the filters on the “Reports” page. Refer to Section 13.3 for more information on dispute mapping date range filters and result limits.

For more information on the fields included in the reports, refer to the **Field Reference Guide** located on the [IDR Gateway](#) page.

15.2. Understanding Report Filters

The reports display data based on either default filter settings or user-selected filters.

- **All Disputes.** Defaults to display all open and closed disputes created within the last 7 calendar days of the current date.
- **Open Dispute Line Items.** Defaults to display all dispute line items on open disputes created within the last 7 calendar days of the current date.
- **Closed Dispute Line Items.** Defaults to display all dispute line items on disputes closed within the last 7 calendar days of the current date.
- **Resubmission Requested Line Items.** Defaults to display all dispute line items the certified IDR entity requested the organization to resubmit, on disputes created within the last 7 calendar days of the current date.
- **Selection Due.** Defaults to display all confirmed (mapped) disputes associated with your organization where the selection response is due within the next 30 calendar days
- **Offers Due.** Defaults to display all confirmed (mapped) disputes associated with your organization where the submission of offers is due within the next 30 calendar days

Users can preview up to 2,000 results in the table. Administrators can download a CSV file with up to 50,000 results using the **Export Filtered Data** button.



If filters match more than 50,000 results, the **Export Filtered Data** button is disabled and an error displays. Adjust the filters to narrow the results.

The IDR Gateway has identified 412,047 disputes that meet the currently selected filters. Current results exceed the maximum limit. Adjust the filters to narrow the results. Exported results are based on selected filters and limited to 50,000 results. Refer to the user guides on the [IDR Gateway page](#) for tips on adjusting filters.

All Disputes

Export Filtered Data

Showing 1 - 2000 of 50,000

Results matching your filters: 176,890

ABC Organization's total disputes: 412,047

Figure 75. All Disputes Report (Maximum Results Exceeded Error)

To filter and download a report:

1. From the Menu bar, select the **Reports** button. The “Reports” page displays.
2. Select a report from the Report Name column. The selected data displays.



Results for the All Disputes, Open Disputes Line Items, Closed Disputes Line Items, and Resubmission Requested Line Items reports are limited to a 7-calendar-day date range. Results for the Selection Due Date and Offers Due Date reports are limited to a 30-calendar-day date range.

Home Disputes Reports Search... JOHN SMITH

Home > Reports > All Disputes

All Disputes

This report includes all open and closed disputes associated with your organization in the IDR Gateway that were not closed prior to September 14, 2026 (the launch of the IDR Gateway), and have been either mapped to your organization by your administrator or by the IDR Gateway system.

Reports preview up to 2,000 results. Select the **Export Filtered Data** button to export up to 50,000 results based on current filters.

Filters

Dispute Number Search:

Search for filtered results by dispute number (DISP-XXXXXX)

Apply

* Created Date Range (7 days max): Aug 28, 2026 Sep 29, 2026

Dispute Phase: Select

Clear

All Disputes Export Filtered Data

Showing 1 - 2000 of 50,000 | Results matching your filters: 48,999 | ABC Organization's total disputes: 412,047

Dispute Number	Created Date	Health Plan Type	Other Health Plan Type	Health Plan Funding Type	Health Plan State Law Opt-In	Batched?
DISP-123456	6/16/26	Church Plan	Medicare	Fully-Insured	Yes	Healthcare ABC
DISP-123457	6/16/26	Church Plan		Self-Insured	No	Healthcare ABC
DISP-123458	6/16/26	Church Plan		Self-Insured	No	Healthcare ABC
DISP-123459	6/16/26	Individual health insurance issuer		Fully-Insured	No	Healthcare ABC
DISP-123460	6/16/26	Individual health insurance issuer	Medicare	Fully-Insured	No	Healthcare ABC
DISP-123461	6/16/26	Fully insured ERISA group health plan		Fully-Insured	No	Healthcare ABC
DISP-123462	6/16/26	Fully insured ERISA group health plan		Fully-Insured	No	Healthcare ABC
DISP-123463	6/16/26	Individual health insurance issuer		Fully-Insured	Yes	Healthcare ABC
DISP-542901	8/10/26	Individual health insurance issuer		Fully-Insured	Yes	Healthcare ABC
DISP-542902	8/11/26	Individual health insurance issuer	Medicare	Fully-Insured	Yes	Healthcare ABC
DISP-542903	8/12/26	Individual health insurance issuer		Fully-Insured	Yes	Healthcare ABC
DISP-542904	8/13/26	Fully insured ERISA group health plan		Fully-Insured	No	Healthcare ABC
DISP-542905	8/14/26	Fully insured ERISA group health plan		Fully-Insured	No	Healthcare ABC
DISP-542906	8/14/26	Individual health insurance issuer		Fully-Insured	No	Healthcare ABC
DISP-542907	8/14/26	Fully insured ERISA group health plan		Fully-Insured	No	Healthcare ABC

Figure 76. Sample Report (All Disputes, Filter Options)

3. Adjust the filters to display 50,000 or fewer results, if necessary. The available filters vary by report.
 - a. For the All Disputes report, you can filter by the created date range and dispute phase.
 - b. For Open Dispute Line Item and Resubmission Requested Line Item reports, you can filter by the created date range of the dispute containing the item or service.
 - c. For Selection Due Date report, you can filter by the currently selected certified IDR entity or by the selection due date range.
 - d. For the Offers Due report, you can filter by the currently selected certified IDR entity or by the offers due day.

- e. For Closed Dispute Line Item report, you can filter by the closed date range of the dispute containing the item or service.
4. To sort the report details in ascending or descending order, select a dropdown option next to the column header, as needed.
5. To search for a dispute, enter the dispute number in the **Dispute Number Search** field. The search results are limited to the selected table filters .
6. Select the **Clear** button to remove applied filters or sorting.
7. Select the **Export Filtered Data** button to export up to 50,000 results based on current filters.

16. Report Privacy & Security Incidents

The “Privacy & Security” page explains privacy issues, indicates who to contact with questions concerning privacy and security, and how to report a privacy and security incident.

A link to the “Privacy & Security” page is located in the footer of each page within the IDR Gateway.

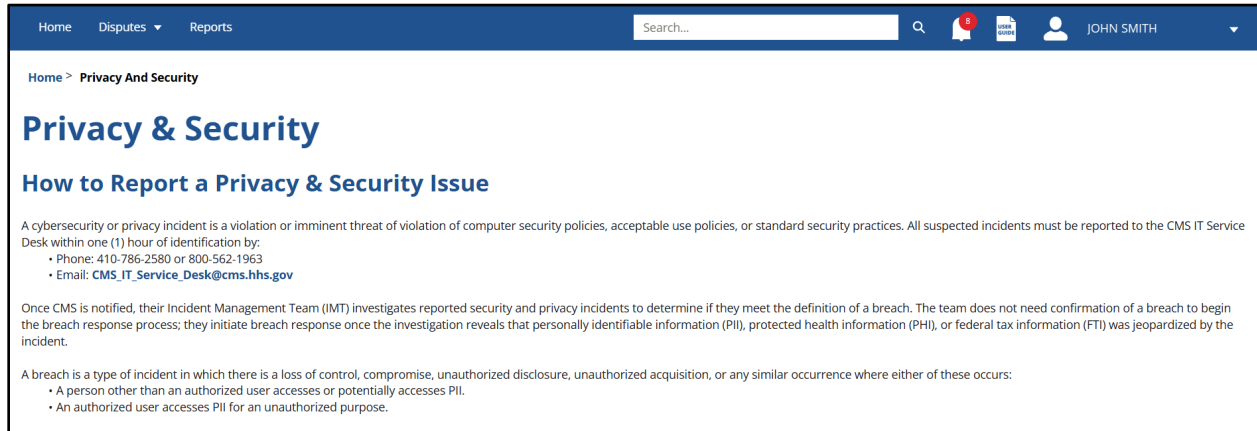


Figure 77. Privacy & Security Page (How to Report a Privacy & Security Issue)

16.1. Cybersecurity or Privacy Incidents

A cybersecurity or privacy incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. All suspected incidents must be reported to the CMS IT Service Desk within one hour of identification.

- Phone: 410-786-2580 or 800-562-1963
- Email: CMS_IT_Service_Desk@cms.hhs.gov

Once notified, the CMS Incident Management Team investigates the reported security and privacy incidents to determine if they meet the definition of a breach.

A breach is a type of incident where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or an authorized user accesses PII for an other-than-authorized purpose.

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-disputes/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 Statement:**

By using web forms that 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") manages the Federal IDR portal, including the IDR Gateway and the web forms used by parties to start payment disputes, select a certified IDR entity, and submit offers. Users may submit the web forms electronically within the IDR Gateway. 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 IDR Gateway. 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 IDR Gateway, which you should also read and be aware of how information is collected and used when on the IDR Gateway.

Permission for information submitted on IDR web forms

When submitting any Federal IDR web forms, you also 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, group health plan, health insurance issuer, or Federal Employees Health Benefits (FEHB) carrier, as applicable, regarding any related 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, and is available at <https://www.cms.gov/privacy>.

Federal Independent Dispute Resolution Process Privacy Act Statement – Effective November 13, 2026

The Departments of the Treasury, Labor, and Health and Human Services (HHS) (collectively, the Departments), and the Office of Personnel Management (OPM) are authorized to collect the information provided 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 and OPM 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. All submitted information must comply with the Privacy Act of 1974 requirements. 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 the IDR Gateway to administer the Federal IDR process, available at <https://nsa-idr.cms.gov/idrgateway/SelfRegister>. Beginning January 15, 2027, Federal IDR web forms outside the IDR Gateway will be retired, and parties must use the IDR Gateway web forms to start the Federal IDR process, select a certified IDR entity, and submit offers.

The initiating party must furnish the Notice of IDR Initiation to the Departments by submitting the “Notice of IDR Initiation” web form. 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. In addition, the email address for the named party to the dispute will be used to map the dispute to that party’s organization in the IDR Gateway to make the dispute accessible to organization users through dashboards, reports, and list views.

The information submitted through the web forms 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, which 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).

Recipients must comply with federal confidentiality requirements and implement required security measures. 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>.

Security Safeguards:

1. This system implements administrative, technical, and physical safeguards consistent with federal standards, including the Federal Information Security Modernization Act (FISMA) and The National Institute of Standards and Technology (NIST) guidance, and CMS Information Security and Privacy policies.
2. This statement provides the notice required by the Privacy Act of 1974 (5 U.S.C. 552a(e)(3)). Learn more 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.
- Understand that unauthorized disclosure of PII/PHI may result in violations of both the Privacy Act of 1974, 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.

If you have any questions about this *Rules of Behavior for IDR Gateway Users*, please contact us at IDRGatewayHelp@cms.hhs.gov.

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 to complete common administrator tasks.

Administrator Dispute Management Actions

I want to:	Actions:
Manually map disputes.	Navigate to: Dispute Mapping > Unconfirmed tab 1. Adjust filters to return fewer than 50,000 results. 2. Select checkboxes next to dispute numbers matched to your organization. 3. Select Confirm Selected Disputes . 4. Select checkboxes next to the dispute numbers NOT associated with your organization. 5. Select Deny Dispute Ownership .
Map disputes via bulk file upload.	Navigate to: Dispute Mapping > Unconfirmed tab 1. Select Bulk Dispute Upload . 2. Download the instructions. 3. Download the template. 4. Copy the dispute numbers from the results downloaded with the Export Filtered Data button and paste them into the template. 5. Enter "Confirm" or "Deny" in the Dispute Ownership column. 6. Save as a .csv file. 7. Upload saved file. 8. Select Submit .
Review dispute mapping results.	Navigate to: Dispute Mapping > Results tab 1. Review dispute mapping results.
Download matched open IDR disputes report.	Navigate to: Dispute Mapping 1. Adjust filters to return fewer than 50,000 results. 2. Select Export Filtered Data Report button.
Find dispute by claim number.	Navigate to: Dispute Mapping > Unconfirmed Line Items tab 1. Adjust filters to return fewer than 50,000 results. 2. Review entries in the Claim Number column to find corresponding Dispute Number.
Review confirmed disputes.	Navigate to: Dispute Mapping > Confirmed tab 1. Adjust filters to return fewer than 50,000 results. 2. Select Apply . 3. Select Clear to reset.
Review denied disputes.	Navigate to: Dispute Mapping > Denied tab 1. Adjust filters to return fewer than 50,000 results. 2. Select Apply . 3. Select Clear to reset.

I want to:	Actions:
Access dispute reports.	Navigate to: Home > Reports 1. Adjust filters to return fewer than 50,000 results. 2. Select Apply . 3. Select Clear to reset.

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.
Invite a user to join my organization.	Navigate to: Permissions > User Management tab 1. Select Invite Users. 2. Enter required information. 3. Select Invite.
Resend an invitation to join my organization.	Navigate to: Permissions > User Management tab > My Users table 1. Select Pending Invites. 2. Select Resend. 3. Review and update as needed. 4. Select Resend.
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 email addresses to assign to new workspace. 4. Select Save Workspace.
Add email addresses 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 email addresses 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 two 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
CSV	Comma-separated values
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
OPM	Office of Personnel Management
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
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.