

Security Page

Download the PDF of this article.

In this Article

Related Articles

As an admin, you can access and customize the security settings for your instance. Many of these features are available through the Admin Dashboard's Security page.

Secure File Scan

Overview

Improve your security by enabling Secure File Scan to check all incoming file upload field attachments on submitted forms and workflows. After a form is submitted, Secure File Scan checks all attachments for viruses and displays the results of each file scanned on the Response page. Any file(s) found to be unsafe will trigger an email notification to the content (form or workflow) owner for follow-up.

Note: This is an "all or nothing" feature where you may allow FormAssembly to scan all files submitted for all forms and workflows, or opt out of secure file scanning entirely.

Requirements

- FormAssembly Enterprise or Government plan
 - Administration Permission: Allow administrator to access security settings
-

Getting Started

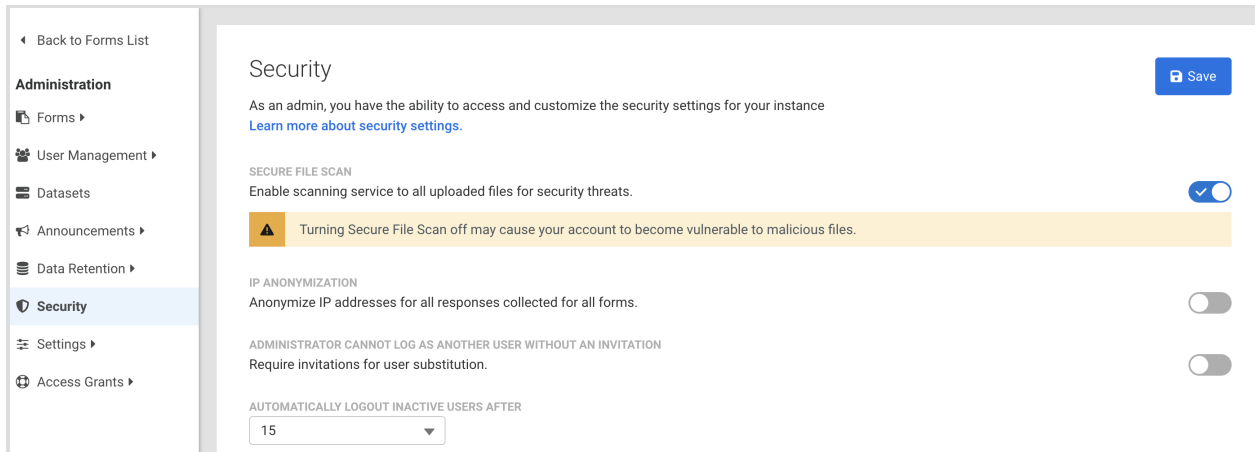
Grant Admin Access to the Security Page

1. Open the **Admin Dashboard**
2. Under "User Management", select **All Users**
3. Locate the user profile for the administrator authorized for security management
4. **Edit** the user profile
5. Open the **Permissions** tab

6. View the permissions under the **Administration** permission package
7. Expand the section for **Admin Permissions**, if not already expanded
8. Select the checkbox for “**Allow administrator to access security settings**”
9. Click **Save**

Enable Secure File Scan

- From the Admin Dashboard, click **Security** to access the Security page.
- Toggle the switch aligned with Secure File Scan to turn on the Secure File Scan feature.



Scan Notifications

Secure File Scan results are communicated in two ways - by file upload statuses on the Response page and through email notifications to the content owner.

Response Page

On the Response page, the status of the secure file scan appears in line with each instance of a file upload. Additionally, if a file upload is flagged, a banner message will appear to highlight the identified security risk.

START WORKFLOW
Close Response ▼

Form Name
Form Name- FORM ID 65

STATUS
✔ Complete

DATE STARTED
02/03/2023 11:22 AM EST

DATE COMPLETED
02/03/2023 11:24 AM EST

FORM RESPONSE ID
86

ASSIGNEE
-

DURATION
13 seconds

FORM VERSION
3

⚠ Our file scanning technology has detected that one or more files may pose a security risk and downloading it may be harmful to your device. If you wish to proceed with the download a log will be created for tracking purposes. You can see the status of each file upload below.

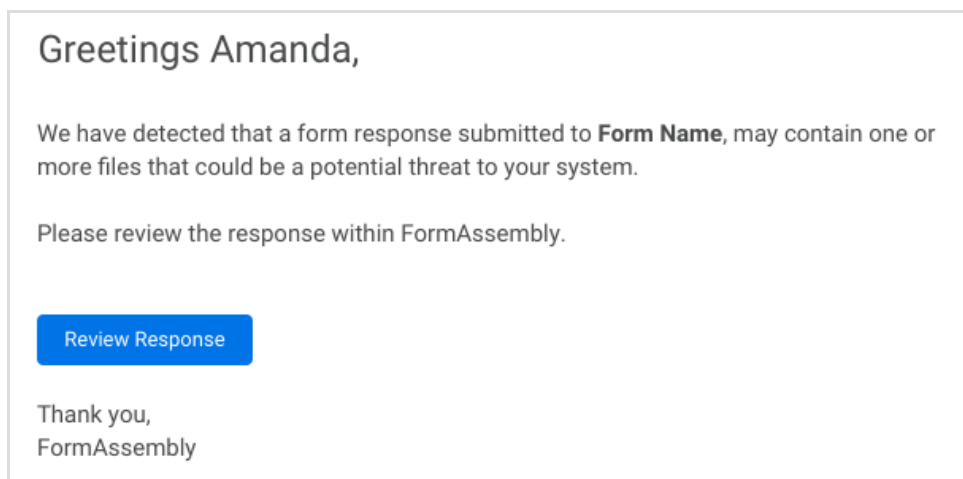
First Name	John		
Last Name	Smith		
Email	john.smith@student.com		
Upload File 1	Expenses_Report1.pdf	⚠ Attention Required	🗑️ 📄
Upload File 2	Expenses_Report2.pdf	🚫 Unable to Scan	🗑️ 📄
Upload File 3	Expenses_Report3.pdf	🕒 File Queued	🗑️ 📄
Upload File 4	Expenses_Report4.pdf	🗑️ File Deleted	

Secure File Scan Statuses

- **Attention Required** - The file is flagged due to potential risks found during the scan.
- **Unable to Scan** - The contents of this file were unable to be scanned.
- **File Queued** - The file will be scanned soon.
- If a status is not included, the file scan did not find any risks, the Secure File Scan feature is disabled, or the file upload occurred before the feature was enabled.

Email Notification

When a file is flagged with the Attention Required status, an email notification is sent to the content owner to notify them to review the response. This email arrives from noreply@formassembly.com with the subject line "A Response Requires Your Review".

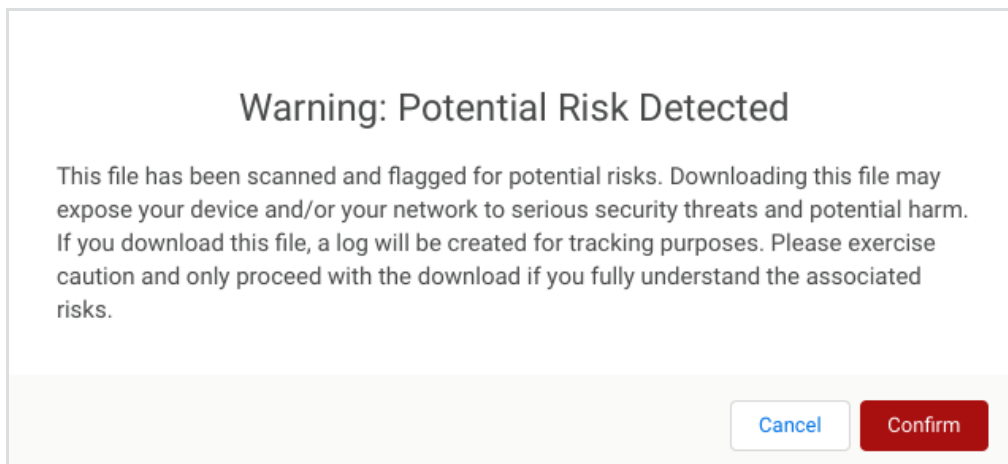


Additional Notes

Secure File Scanning does not halt any connectors or form processes. Content owners are notified of any malicious or unscannable files found, but files are still sent through any configured connectors as designated by your form or workflow's configuration.

Proceeding with a Risky Download

FormAssembly provides the Secure File Scan feature, but only your own security team can recommend what to do next when a file upload is flagged. If you choose to proceed with downloading a flagged file, a confirmation message will appear. Any confirmation is logged for tracking purposes.



Multi-factor Authentication

Overview

Multi-factor authentication (MFA) is any additional method of authenticating yourself to an application other than your standard username and password combination. These can be tokens you hold, such as security keys, authenticator apps on your mobile device, or biometrics, like fingerprints. When using multiple “factors of authentication” for an online account an extra layer of security is added. If an attacker somehow gets access to your password, an account protected by multi-factor authentication would block the attacker from gaining access to your account as they would also need access to that additional factor.

Requirements

- Multi-factor authentication is available on Essentials plans and up
- An administrator must enable MFA before use is available

Further requirements for each method of multi-factor authentication will differ per method. Refer to the specific documentation pages for each method for more details.

- [Time-Based One-Time Passwords](#)
- [YubiKey](#)

Enable MFA (Administrator Required)

- Navigate to [Admin Dashboard | Security](#)

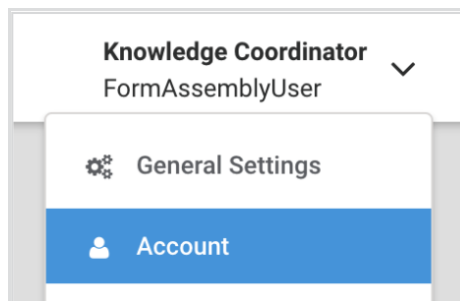
To allow users to manage MFA for their user account

- In the Multi-factor Authentication section, toggle the option to enable MFA for the instance

To force users to authenticate with MFA upon login

- In the Multi-factor Authentication section, toggle the option to Force MFA

Add a Multi-factor Authenticator



- Navigate to the “**Account**” section within your user profile
- Within the **Account Details** section, click the **Configure MFA** button
 - You will be taken to the Multi-factor Authenticators page, which displays all multi-factor authenticators you have set up for your user profile, their status (enabled or disabled), and their order of precedence.
- Click **Add Authentication Method** for a list of available multi-factor authentication options
- Select the authenticator you wish to add
 - A new disabled entry will appear on your timeline with buttons to configure or delete the added MFA method.
- Click **Configure** to continue the setup of the new MFA method.

Enable or Disable a Multi-factor Authenticator

- On the Multi-factor Authenticators page, click **Configure** on the method you wish to enable or disable.
- Within the **Status** section, select the desired option (**Enabled** or **Disabled**)
- Select **Apply** at the bottom of the configuration screen to save the selection.

Note:

- Some multi-factor authenticators require a “first-time setup” before allowing you to enable or disable them.
- If the "Force MFA" setting is enabled by your FormAssembly administrator, at least one MFA method must be enabled for your user account. To disable all MFA methods, the "Force MFA" setting must be toggled off first.

Reorder Multi-factor Authenticators on the Timeline

If you have multiple multi-factor authenticator methods set up, the timeline allows you to reorder your methods so one may challenge you before another when logging in.

- Using the drag handles to the left of each entry in the timeline, drag the entries to create your preferred order. The precedence goes in descending order.
- Click **Apply** at the bottom of the timeline to save your changes. The page will refresh and show the new order.

Delete a Multi-factor Authenticator

- On the Multi-factor Authenticators page, locate the multi-factor authentication method you wish to delete
- Click the **Delete** button
- A **Remove Authenticator** confirmation box will ask you to confirm the action. Click **Remove** to confirm.
- The page will refresh with the deleted method removed from the timeline

Note: If the "Force MFA" setting is enabled by your FormAssembly administrator, at least one MFA method must be enabled for your user account. To disable all MFA methods, the "Force MFA" setting must be toggled off first.

MFA Administration

Administrators of a FormAssembly instance can manage MFA configurations for users.

Note: The administrator must have the permission “Can manage multi-factor authentication” enabled for their account.

- Navigate to **Admin Dashboard | User Management | All Users**
- Select a user and navigate to their **Details** tab
- Locate the **Multi-factor Authentication** section
- For each MFA method displayed for the user account, the admin may select to **enable**, **disable**, or **delete**.

FAQs

What’s the difference between disabling and deleting a multifactor authenticator?

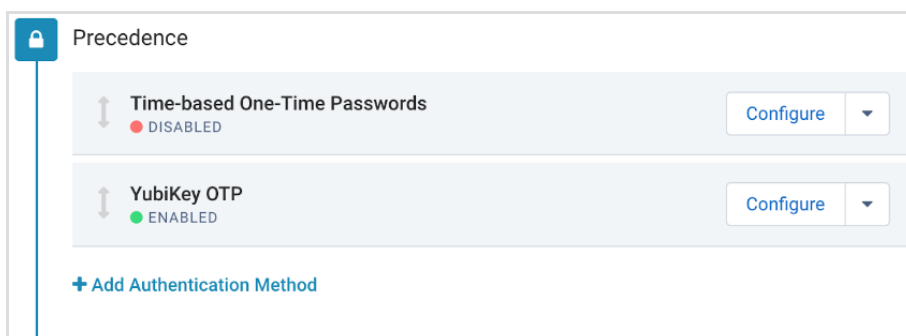
- Disabling a multi-factor authenticator means it will not challenge you to log in to your account. However, it remains set up and associated with your account, so you only need to re-enable the method to activate it again.
- Deleting a multi-factor authenticator will remove it entirely from your account. If you wish to use that authentication method again, you would completely recreate it and re-configure it from scratch.

If I have multiple multifactor authenticators set up and enabled will I need to complete each one individually before I can log in?

- No, we currently only require the success of one of the authentication challenges you may be presented with. When verified by one of your multi-factor authenticators at login, your account may be accessed.

If I have multiple multifactor authenticators set up and the one at the top is disabled, what authentication challenge will I be presented with when logging in?

- You will be presented with the authentication challenge of the top-most enabled authenticator in your timeline’s order of precedence. In the example given below, even though Time-based One-Time Passwords is set to go first, it is disabled, and so the next enabled method will be presented (YubiKey).



If I have multiple multifactor authenticators set up, and I'm having trouble with one of them, can I switch to complete another instead?

- Yes. If you have additional multi-factor authenticators enabled on your account, you will see a link to move to the next one if you're having trouble with the current one. Note that choosing to move to the next enabled method cannot be undone, and you cannot return to a previous authentication challenge.

I know my username and password but have lost access to my additional factors, how can I recover my account?

- For our Basic plan customers, you must contact FormAssembly Support and go through a proof of identity process. On completion of that, a FormAssembly Support representative will disable the multi-factor authenticators associated with your account, allowing you to log in without them.
- For our Essentials plan and higher customers, you must contact your FormAssembly instance administrator(s) to disable the multi-factor authenticators associated with your account, allowing you to log in without them.

IP Anonymization

Overview

IP Anonymization is an optional privacy setting that automatically anonymizes IP addresses collected with form submissions.

Requirements

Enterprise

Compliance Cloud

For information on upgrading, please contact our Sales Department at sales@formassembly.com.

Definition

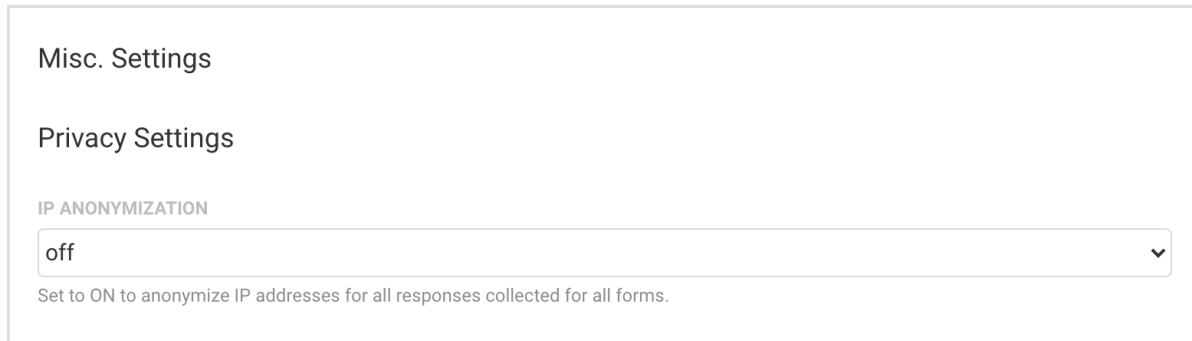
When this feature is enabled, the **last octet of IPv4 addresses and the last 80 bits of IPv6 addresses are replaced with zeros**. This guarantees that the IP address cannot be used to uniquely identify the computer used to submit a response to a form.

Note that the collection of other Personally Identifiable Information (PII) is under the responsibility of the form creator. Such information, if requested through the form, is not anonymized.

How to Enable IP Anonymization

Follow these steps to enable this feature.

1. Go to **Admin Dashboard | Settings** and navigate to the **Miscellaneous** page. From here you can view the **Privacy Settings** section.



The screenshot shows a settings panel with the following elements:

- Misc. Settings
- Privacy Settings
- IP ANONYMIZATION
- A dropdown menu currently set to "off".
- A note below the dropdown: "Set to ON to anonymize IP addresses for all responses collected for all forms."

2. Set IP Anonymization to **ON**.
3. Click the **Apply** button at the bottom of the page.

Grant Access Feature

Overview

The Grant Access Feature in FormAssembly can be used to accomplish two functions. First, if your organization is in need of support from the FormAssembly team, you can grant access to your forms so that we can better troubleshoot any issues you might be facing.

Second, as an Enterprise Administrator, you can decide the level of access you will have to your users' forms. You can either choose to be able to use the Admin Override function to log in as any of your users, or you can choose to use the Grant Access Feature where your users would need to give you permission to access their forms.

Details on how to enable and disable this feature can be found in the follow section.

Requirements

Enterprise

Compliance Cloud

For information on upgrading, please contact our Sales Department at sales@formassembly.com.

Enabling or Disabling the Grant Access Feature

When working with the Grant Access feature, you will need to visit your Admin Dashboard to enable or disable the feature.

Under the Admin Dashboard, go to **Settings** → **Miscellaneous** and then under **Privacy Settings** you can set the feature to be "on" or "off." If the feature is off, you will be able to login as any of your users without them needing to grant you access.

Privacy Settings

ADMINISTRATOR CANNOT LOG AS ANOTHER USER WITHOUT AN INVITATION

on

Set to ON to require invitations for user substitution.

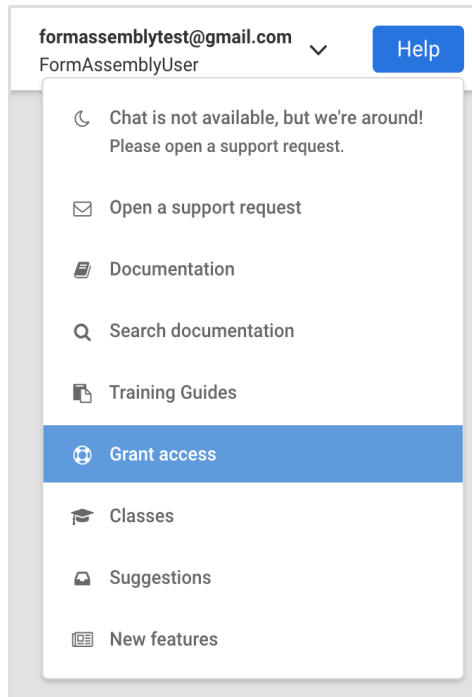
Additionally, if you would like to be able to access your users' forms without permission being needed, you will need to go to **Settings** → **User Roles** → **Administrator** and make sure that the box is checked next to **Allow administrator to access user's data**.

Allow administrator to access user's data

Please ensure that you have clicked **Apply** after making changes to either of these settings.

Getting Started

To begin, use the dropdown Help menu at the top right of FormAssembly to select **Grant Access**.



You will be taken to the Grant Access page where you will see two options: Administrator Support and FormAssembly Support.

If your users need to grant you access, as an Enterprise administrator, they would select **Go to Administrator Support**.

If you or your users need to grant access to FormAssembly in order to help troubleshoot an issue, you should select **Go to FormAssembly Support**

Grant access to my account

FormAssembly offers two ways for you to allow others to access your account for support.

Administrator Support

You may grant administrators access to your account. The administrators will be able to access your account and act "as you" for a limited time.

[Go to Administrator Support](#)

FormAssembly Support

You may grant FormAssembly Support access to your account.

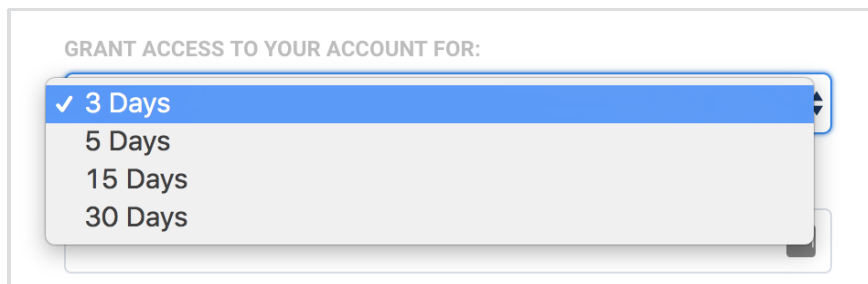
We will be able to securely log in to your account and act "as you" for a limited time.

[Go to FormAssembly Support](#)

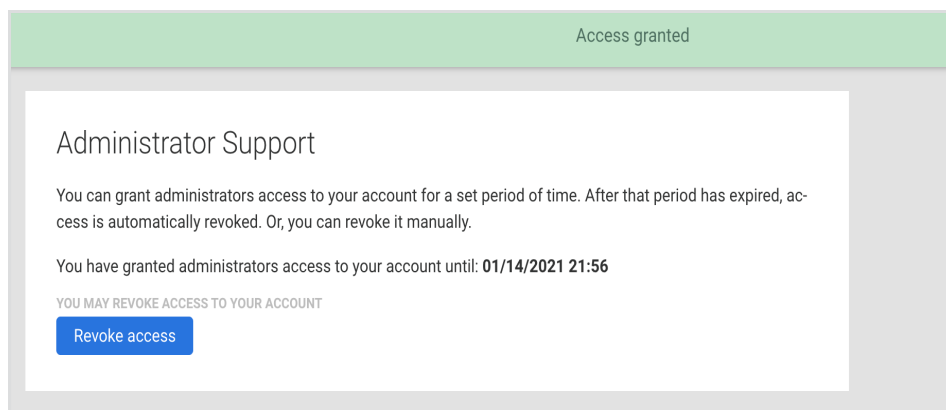
If you have selected that permission is not required for administrators to log in as users, your users will not see the Administrator Support option.

Granting Administrator Access

Once you click on **Go to Administrator Support** you will be taken to the Administrator Support screen, where your users will be able to select how many days account access will be granted (3, 5, 15, or 30 days). Once that selection has been made, they will need to confirm their password and click the **Grant Access** button.



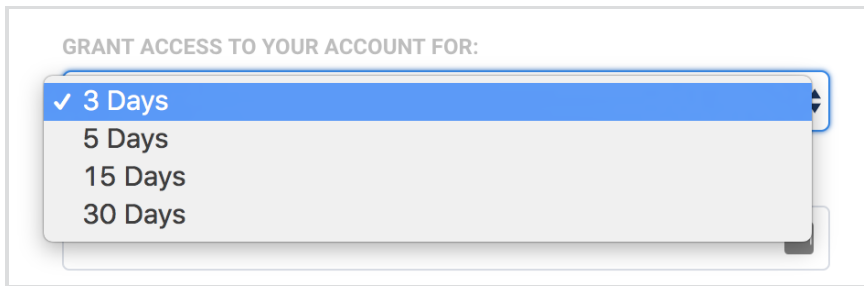
Provided the user's password is correct, they will be taken to the confirmation screen which will give the date that administrator access has been provided until. The user can choose to revoke this access at any time by clicking the **Revoke Access** button.



Granting FormAssembly Access

For Enterprise Cloud customers, if the need arises for you to grant the FormAssembly support team access to your account, you can do so by clicking the **Go to FormAssembly Support** button.

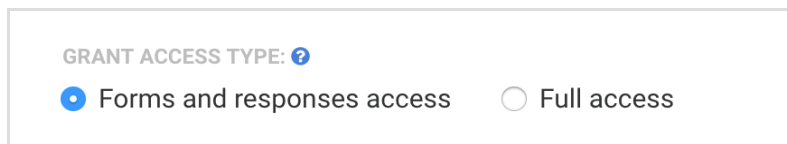
Next, you will need to select the number of days (3, 5, 15, or 30) that access will be granted for.



GRANT ACCESS TO YOUR ACCOUNT FOR:

- ✓ 3 Days
- 5 Days
- 15 Days
- 30 Days

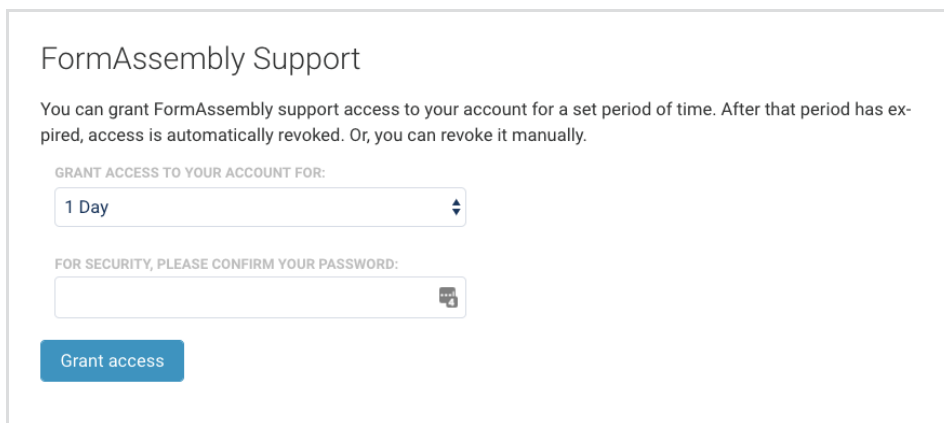
You will also need to select the access type. Selecting **Forms and Responses** will grant access to your forms, connectors, notifications, processing options, and form responses. Selecting **Full Access** will grant access to all of these options plus the Admin Dashboard (if you are an administrator), General Settings, and Account Pages.



GRANT ACCESS TYPE: ?

Forms and responses access Full access

Once that has been selected, you will need to enter your FormAssembly password and click the **Grant Access** button to give access to the FormAssembly support team access.



FormAssembly Support

You can grant FormAssembly support access to your account for a set period of time. After that period has expired, access is automatically revoked. Or, you can revoke it manually.

GRANT ACCESS TO YOUR ACCOUNT FOR:

1 Day

FOR SECURITY, PLEASE CONFIRM YOUR PASSWORD:

Grant access

Note: If you are a Single Sign-On (SSO) user through Salesforce, you will not be required to enter your password during this step.

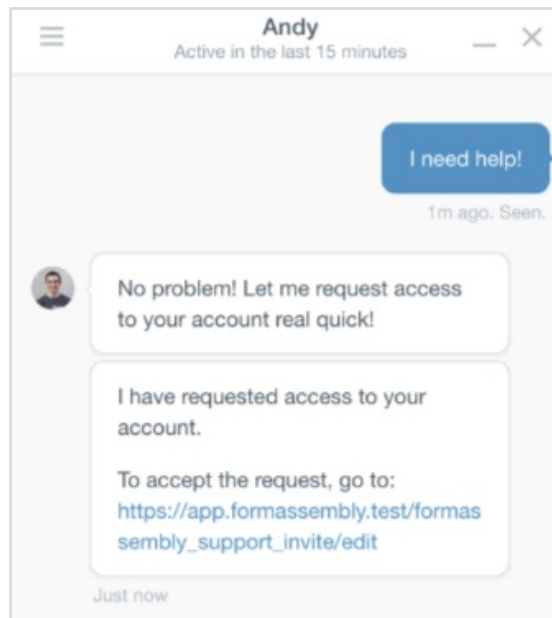
Once access has been granted to FormAssembly, you will be able to see your current access grants at the bottom of the page. You can also choose to revoke access should you need to.

You have granted FormAssembly Support access to your account.

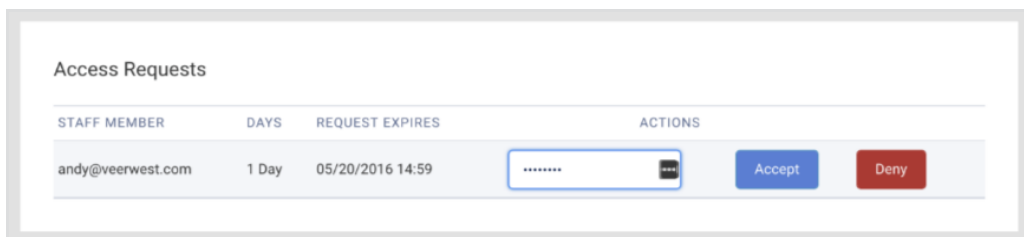
GRANTED	EXPIRES	ACCESS CODE	ACCESS LEVEL	ACTIONS
10/04/2017 17:45	10/07/2017 17:45	443d9e07-a2fa-4ca6-8e3f-494a96ef5786	Forms & responses ?	Revoke access

FormAssembly Access Request

Our support team may also request access through our in-app support chat. If you are in need of assistance or troubleshooting, our support team can send you a direct link to grant access to your account.



Once you click on the link, you'll be taken to Grant Access page where you'll be able to see any pending Access Requests. Simply enter your password and choose **Accept**, or choose Deny if you do not wish to grant access.



Once you have granted access, you will see the green Access Granted banner across the top of the page and you will see that a new Access Grant has been added to your list of Current

Access Grants at the bottom of the page.

You have granted FormAssembly Support access to your account.

GRANTED	EXPIRES	ACCESS CODE	ACCESS LEVEL	ACTIONS
10/04/2017 17:45	10/07/2017 17:45	443d9e07-a2fa-4ca6-8e3f-494a96ef5786	Forms & responses ⓘ	Revoke access

From there, the FormAssembly support team will be able to access your account to further assist you with any troubleshooting.

Reviewing Access Grants

If you are an administrator and you need to review the active Access Grants for your instance, they are accessible on the Admin Dashboard sidebar. You have a dropdown menu labeled **Access Grants** from which you can view both Admin Support grants and FormAssembly Support grants.

