

Beyond - Background Check Providers and Setup

Last Modified on 01/28/2021 1:39 pm CST

Background Checks & Beyond

Beyond now allows you to request different background check packages for employees directly from the employee record. We've partnered with some of the top background check providers to make it easier for your recruiters to request and complete background checks on employees without ever having to leave Beyond.

Jeremy Berry (4295098151) - Visifile

beyond-staging.ontempworks.com/employee/4295098151

Search Anything...

ACTIVITY PANEL EMPLOYEE Jeremy Berry

Jeremy Berry (4295098151)
SSN: 436-42-4632 · Eagan, MN 55121

VISIFILE DETAILS DOCUMENTS MESSAGES ASSIGNMENTS STORY REFERENCES PAY SETUP MORE

Snapshot

Id	4295098151	Hire Status	Eligible for Hire >
Job Title	--		

Contact Information

- jeremy@xip.xom
Email
- (235) 262-4829
Phone

Messages

MARCH 2020

- Buzz Offered · Mar 4th, 4:00 PM · Amelia Stout
The employee Berry, Jeremy has been offered a Job - Drivers for OrderId: 4295036295

Resume

No resume to view

Note

Our Partners



To learn more about Asurint, check out [Asurint Overview](#)



To learn more about Crimcheck, check out [Crimcheck Overview](#)



To learn more about First Advantage, check out [First Advantage Overview](#)



To learn more about PeopleG2, check out [PeopleG2 Overview](#)



To learn more about Universal Background Screening, check out [Universal Background Screening Overview](#)

Ready to Get Started?

Note In order to utilize background checks in Beyond, you will need to first contact your TempWorks Account Manager. After the initial setup is completed on the back end, you will be able to complete the following steps to complete your setup.

To complete the setup process, you will want to setup the following:


1. [Set Up Credentials](#)
2. [Set Up User Permissions](#)

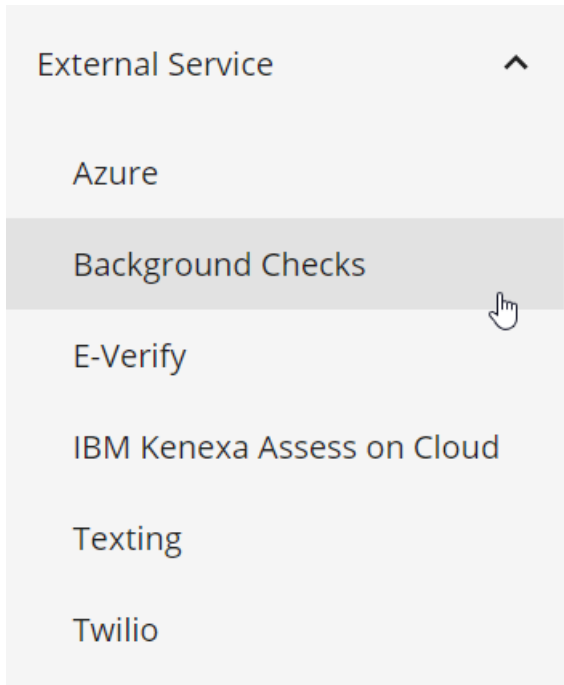
Setting Up Provider Credentials

Depending on which background check provider(s) you will use, you will need to add your account to Beyond to allow Beyond to send the necessary information to the background check provider.

Credentials can be added by any admin who has access to the System Settings section in Beyond.

To Find Background Check Credentials:

1. Navigate to the  Menu
2. Select System Settings
3. Select External Services > Background Checks

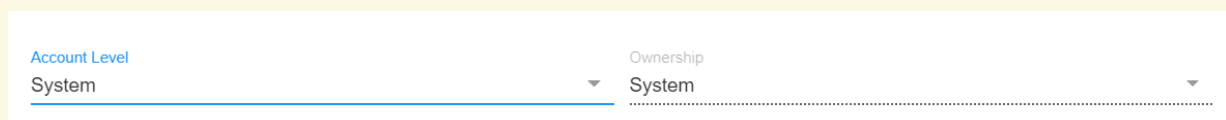


4. Select the + to add background check credentials

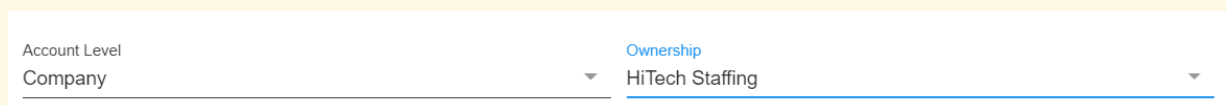
Check out the providers sections below for more information on what credentials you will need to enter.

Note How Hierarchy Affects Background Check Credentials:

Regardless of which provider you choose, you will be asked what account level you want to add your credentials to. This is related to Beyond [Hierarchy](#). Most systems will allow any user in the system to use the same provider credentials. This is when you set these credentials up at your highest hierarchy (System or Subsystem).



If you have different credentials for different EINs or branches, etc. you can set up each set of credentials with the specific company or branch. This is when you would set the account level to company or branch or user. Then, under Ownership, you would choose the correct entity, branch, or user.



When editing/removing credentials that are located above your current hierarchy level, you will be presented with the following message:

These credentials are above your current hierarchy and changes may affect more users than intended. Please make sure you are editing the correct credentials.

The above message has been added to provide a visual aid in the determination of editing credentials.

Providers

Each provider will have different required information that needs to be entered in the credentials section:

- [Asurint](#)
- [Crimcheck](#)
- [First Advantage](#)
- [PeopleG2](#)
- [Universal](#)

Asurint

1. Select the + in the upper right under external services > background checks
2. Choose Asurint
3. Enter the following information

Background Check Provider - Asurint

Account Level System	Ownership System
Username [REDACTED]	Password [REDACTED]
Account Id [REDACTED]	Location Id [REDACTED]

SAVE AS DRAFT

CANCEL SUBMIT

- **Account Level:** what hierarchy should this be available at? (See hierarchy note above)
 - (Optional) **Ownership:** If you are not setting this to system, select the name of the entity, branch, or user who will use this account information from the drop down
 - **Username & Password:** Provided by Asurint
 - **Account Id:** Provided by Asurint
 - **Location Id:** Additional Identifier provided by Asurint
4. Select Submit
 5. Once you have saved your credentials, a Notification URL will generate under the credential information.
You can use the copy to clipboard option to copy and provide this URL to Asurint in order to receive status

updates:

The screenshot shows the 'Asurint System' configuration page. It includes fields for Username, Password, Account Id, Location Id, and Notification URL. The Notification URL field is highlighted with a 'Copy To Clipboard' button.

Note Asurint requires each service rep using background checks to have their email on file under Beyond Menu > System Settings > Service Representatives. Check out [Beyond - Managing Your Service Representatives](#) for more information.

Crimcheck

1. Select the + in the upper right under external services > background checks
2. Choose Crimcheck
3. Enter the following information:

The screenshot shows the 'Background Check Provider - Crimcheck' configuration form. It includes fields for Account Level, Ownership, Partner Id, Client Secret, Expiration Delay, Custom Email Message, and a checkbox for Require Payment. The form also has 'SAVE AS DRAFT', 'CANCEL', and 'SUBMIT' buttons.

- **Account Level:** what hierarchy should this be available at? (See hierarchy note above)
- (Optional) **Ownership:** If you are not setting this to system, select the name of the entity, branch, or user who will use this account information from the drop down
- **Partner Id:** Provided by Crimcheck
- **Client Secret:** Provided by Crimcheck
- **Expiration Delay:** Enter a number of days before the request expires. If no date is entered, background check requests will expire after 2 weeks.
- (Optional) **Custom Email Message:** You can enter an additional note that will be sent to applicants when requesting a background check. We recommend leaving this field blank if you are not planning on

emailing the applicant additional information through Crimcheck

- (Optional) **Require Payment Checkbox:** Only check this box if you want an applicant to pay for the background check requested instead of your company

4. Select Submit

Crimcheck also requires user credentials to be set up. See [below](#) for more information.

First Advantage

Note If you are currently using our Enterprise First Advantage Integration, you may require some account updates with First Advantage. Contact your First Advantage Account Manager for more information.

1. Select the + in the upper right under external services > background checks
2. Choose First Advantage
3. Enter the following information:

The screenshot shows a form titled "Background Check Provider - First Advantage". The form contains the following fields:

- Account Level:** A dropdown menu with "System" selected.
- Ownership:** A dropdown menu with "System" selected.
- Notification Email:** A text input field with a question mark icon and a lock icon.
- First Advantage Credentials:** A section containing four fields:
 - Access Token:** A text input field with a masked value (dots).
 - Primary Account Id:** A text input field with a masked value (dots).
 - User Account Id:** A text input field with a masked value (dots).
 - User Id:** A text input field with a masked value (dots).

At the bottom of the form, there are two buttons: "SAVE AS DRAFT" on the left and "CANCEL" and "SUBMIT" on the right.

- **Account Level:** what hierarchy should this be available at? (See hierarchy note above)
- (Optional) **Ownership:** If you are not setting this to system, select the name of the entity, branch, or user who will use this account information from the drop down
- **Notification Email:** This email will override the email settings you have with First Advantage that background check statuses are sent to
- **Access Token:** Token Provided by First Advantage
- **Primary Account Id:** Provided by First Advantage
- **User Account Id:** Provided by First Advantage
- **User Id:** Provided by First Advantage

4. Select Submit

PeopleG2

1. Select the + in the upper right under external services > background checks
2. Choose PeopleG2
3. Enter the following information

Background Check Provider - PeopleG2

Account Level: System

Ownership: System

Access Token: [Masked]

Location Id: [Masked] ⓘ

SAVE AS DRAFT CANCEL SUBMIT

EDIT TEST DELETE

- **Account Level:** what hierarchy should this be available at? (See hierarchy note above)
- (Optional) **Ownership:** If you are not setting this to system, select the name of the entity, branch, or user who will use this account information from the drop down
- **Access Token:** Enter the access token provided by PeopleG2
- (Optionally) **Location Id:** When a location Id is entered here, it will limit background check packages to that location Id provided by PeopleG2

4. Select Submit

Note In order to use the PeopleG2 integration, your PeopleG2 account must be configured to include location options. Reach out to PeopleG2 for more information on how to set this up.

Universal

1. Select the + in the upper right under external services > background checks
2. Choose Universal
3. Enter the following information

Background Check Provider - Universal

Account Level System	Ownership System
Account Number 100041	
Username tempworks	Password
SAVE AS DRAFT	CANCEL SUBMIT

- **Account Level:** what hierarchy should this be available at? (See hierarchy note above)
 - (Optional) **Ownership:** If you are not setting this to system, select the name of the entity, branch, or user who will use this account information from the drop down
 - **Username & Password:** Provided by Universal
4. Select Submit
 5. Once you have saved your credentials, a Notification URL will generate under the credential information. You can use the copy to clipboard option to copy and provide this URL to Universal in order to receive status updates:

Universal
System

Account Number	100041	Username	tempworks
Password	Notification URL ?	https://api-

[Copy To Clipboard](#)

[FEWER DETAILS](#)

Setting Up User Permissions

Once you have set up your provider credentials, you will need to make sure the users you want running background checks have the correct permissions. In order to do this, you will need to have access to the Security Groups section of system settings. We recommend setting this information up at system or subsystem level to make it easier to include the users you are looking for.

There are 2 permissions that you can grant related to Background Checks:




Can edit background checks.
Allows a user to create and edit background checks.



Can read background checks.
Allows a user to read background checks.

- Can Edit Background Checks - allows users to create and edit background check requests
- Can Read Background Checks - allows users to review and search for background check requests and their current status

To Find Security Group Permissions:

1. Navigate to  menu in the upper left
2. Select Security Groups
3. Select Permission
4. Either:
 - Add users to any group that already has this permission(s) OR
 - Create a new group with the permission(s) checked and add users to it (remember that users can only be part of one permissions group and will inherit all the permissions that you check.

For more information, check out [Beyond - Managing Security Groups](#).

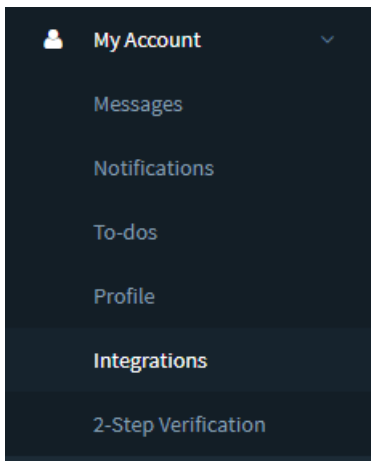
Crimcheck User Setup

In order for the Crimcheck integration to function properly, along with the addition of the System Settings, an API Key must be submitted within the User Settings of Beyond.

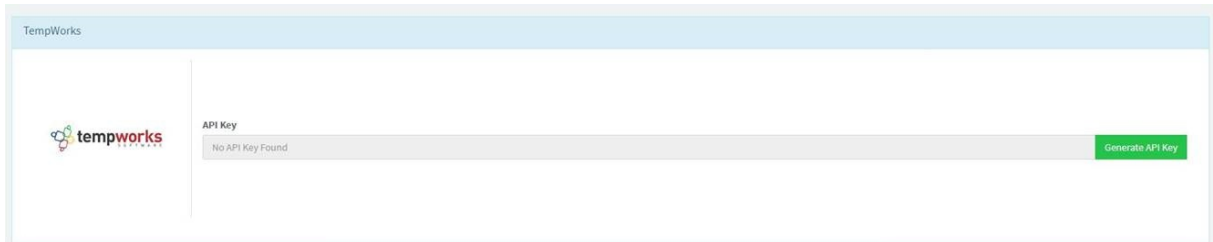
Note Every user that will be utilizing the Crimcheck integration will need to have API Key generated and entered within the User Settings of Beyond.

To retrieve the API Key:

1. Navigate to <https://clients.efetch.com/account/integrations> and log in
2. Expand the My Account dropdown on the left hand side and select Integrations:




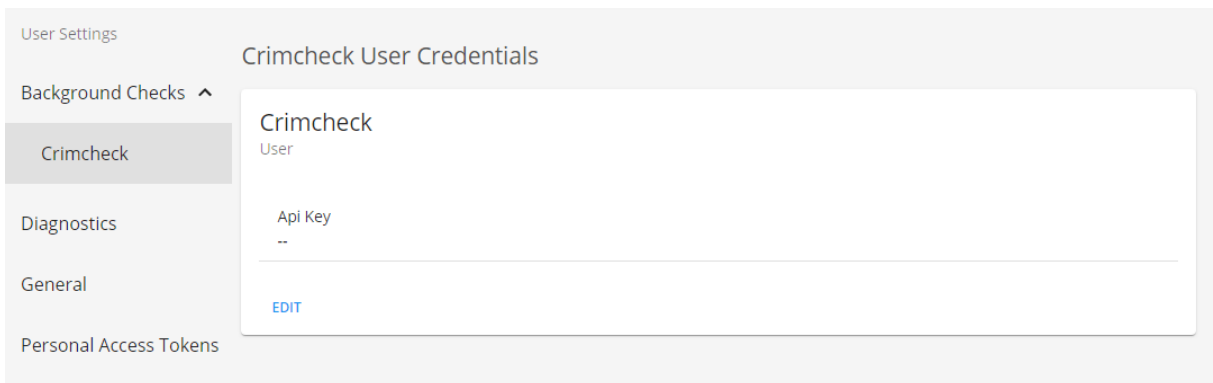
3. Find TempWorks within the list of integrations and select Generate API Key:



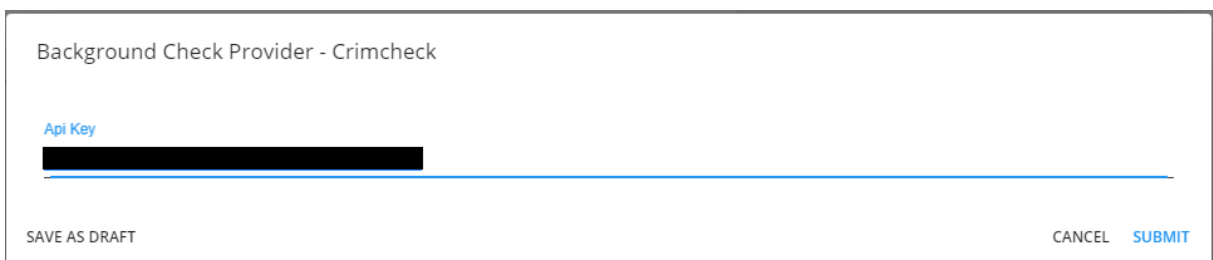
4. Copy the API Key that is shown within the field:

To finish setup:

1. Within Beyond, navigate to  menu in the upper left
2. Select User Settings
3. Select Background Checks < Crimcheck



4. Select Edit
5. Paste the API Key that had been previously copied
6. Select Submit



Note Upon submitting the API Key, an automated test will run to ensure the API Key is valid.

- If the API Key is accepted, the credentials will save as expected.
- If the API Key is not accepted, the following will show:

The credentials are invalid. The 'Crimcheck' service returned an error with the HTTP status code of '401' with the following message: Crimcheck Log Id: V2|62ec050c-ba10-4b9f-b0cd-750fa6a932d7|C69798|CD1

Related Articles