BrassRing, Lead Manager and Onboard Pre-Release Notes - December 2021

December 2021

Table of Contents

BrassRing December Release

BrassRing new features for the release 21.12.07 are listed here.

Client Reminders

The Client Reminders section reminds clients of recently distributed important notices and links to comprehensive documentation and training for the special features recently introduced.

Enhancements - You Asked We Listened

We are proud to inform that this build introduces features that were developed in response to clients' Requests for Enhancement (RFEs). Infinite is pleased to deliver these features in response to your responses and comments.

Requests for Enhancement (RFEs)

The following features were delivered in response to the RFEs posted on Aha!

- Reqs - Req Edit Audit Trail
- Talent Gateway Account Creation - Two Factor Authentication

Dark Launch Features

Dark Launch features are those features that are released to the Staging environment only and are NOT released to the Production environment for a considerable amount of time. This process gives an opportunity and enough time to test these features thoroughly before they are available in the production environment. Clients are requested to configure and test these features and provide their feedback and inputs to your respective Infinite representatives.

There are no Dark Launch features in the December BrassRing and Lead Manager Release.

BrassRing Visible Changes

There are no Visible change features in the current release of BrassRing.

Configurable Changes

Reqs - Req Edit Audit Trail

> **NOTE**
> This feature was deployed to the Staging environment - Only with the release 21.11.15. This feature is going to be available in the Production environment starting the current release.

The audit trail is available in the History tab of the req. A new link **View field change details** is displayed next to the Req modification history. Users select this link to open a new module that displays a table of comparison between current information of the req and the previous information.

Figure 1. Req History Tab

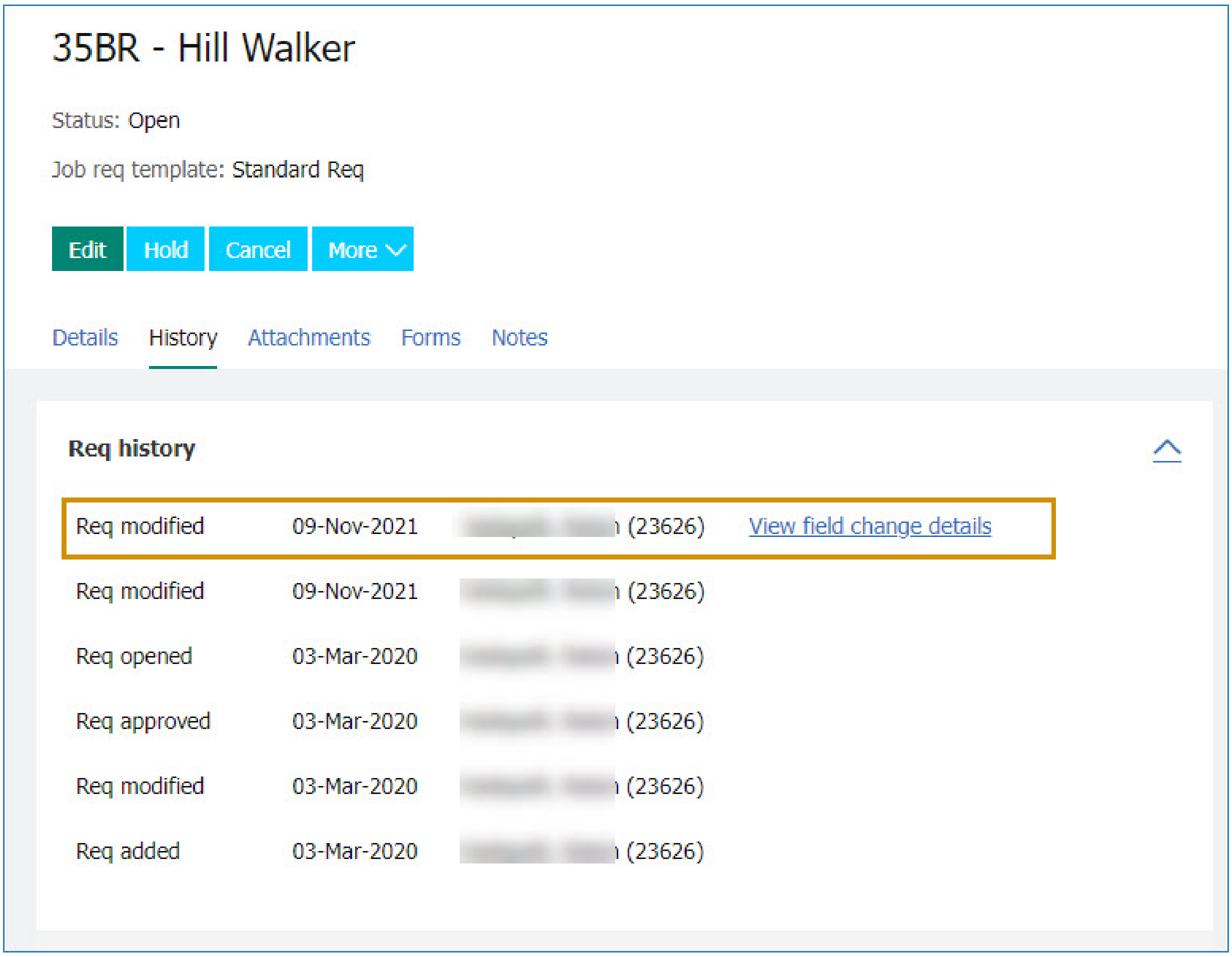
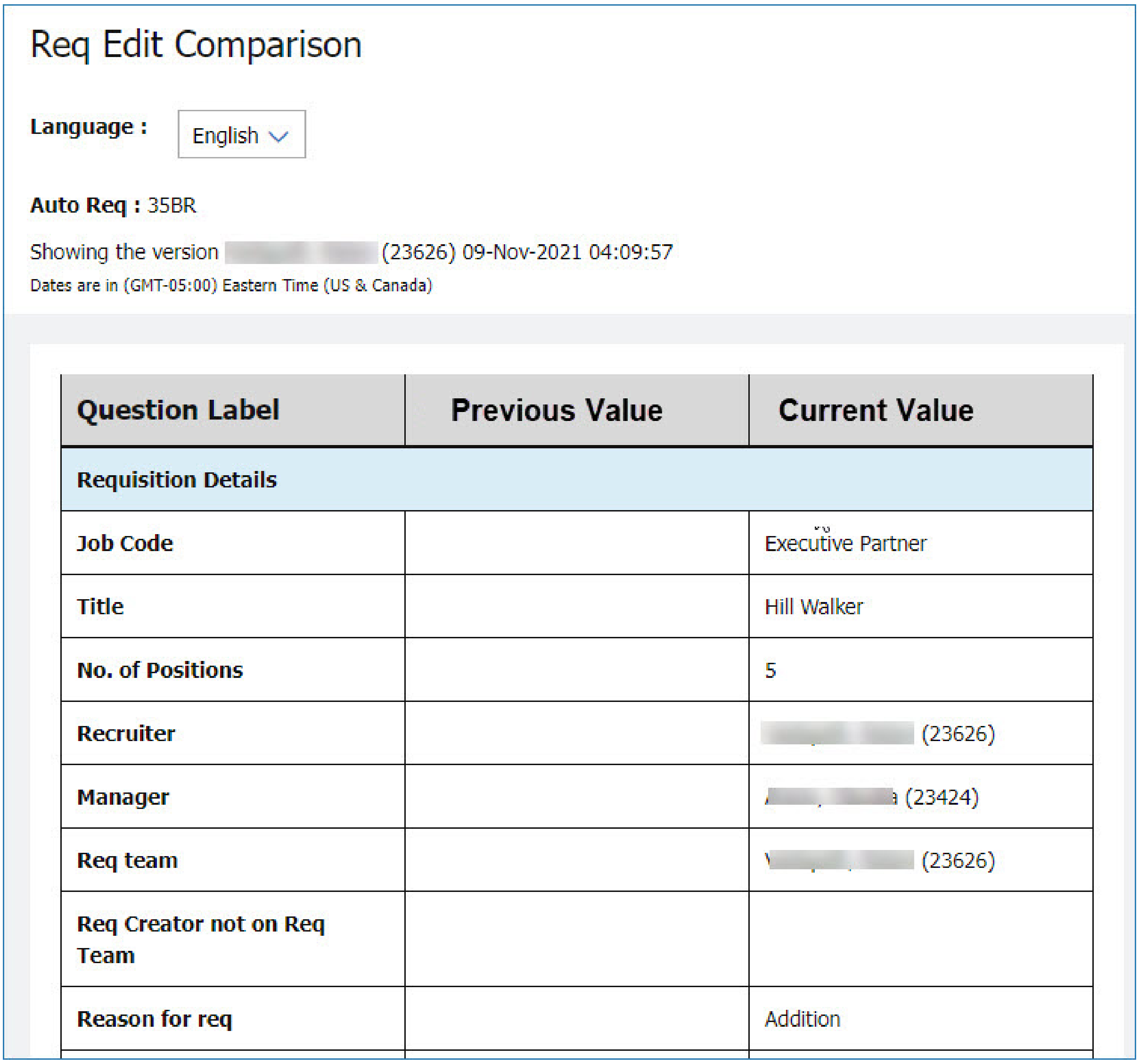


Figure 2. ***Req Edit Comparison Table***



Req Edit Comparison

Language : English

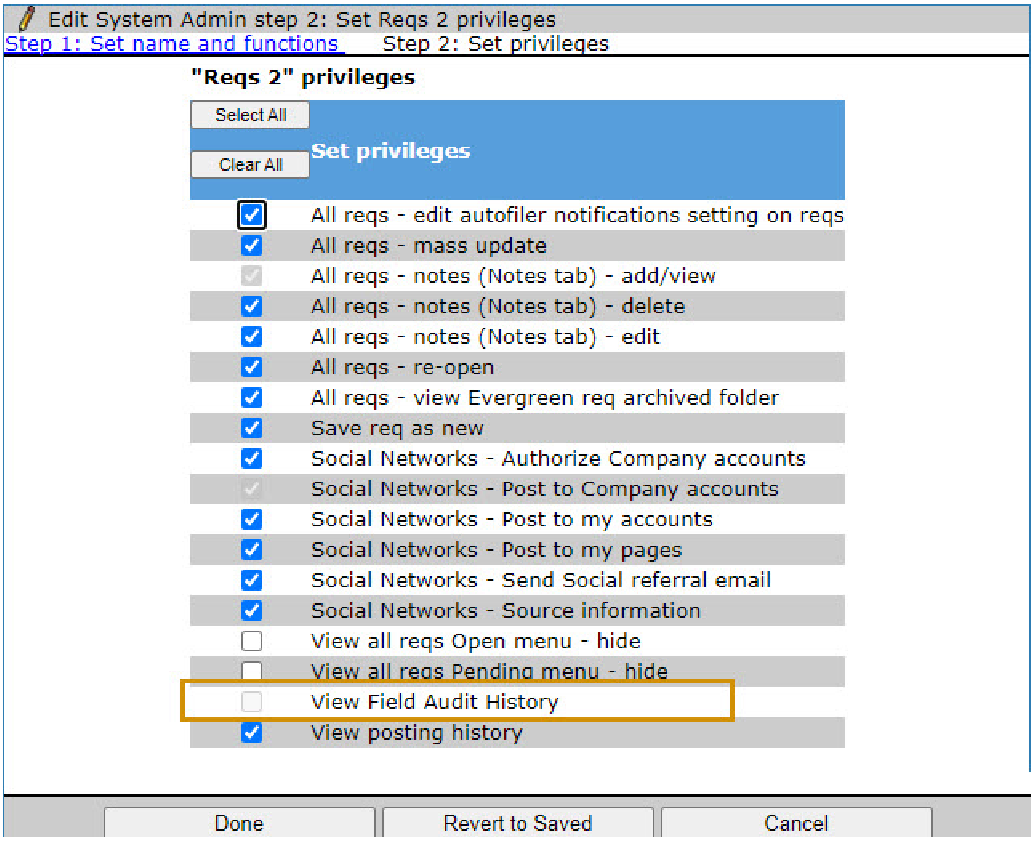
Auto Req : 35BR

Showing the version [redacted] (23626) 09-Nov-2021 04:09:57

Dates are in (GMT-05:00) Eastern Time (US & Canada)

Question Label	Previous Value	Current Value
Requisition Details		
Job Code		Executive Partner
Title		Hill Walker
No. of Positions		5
Recruiter		[redacted] (23626)
Manager		[redacted] (23424)
Req team		[redacted] (23626)
Req Creator not on Req Team		
Reason for req		Addition

A new user type privilege **View Field Audit History** is added in the Workbench User Types > Reqs2. The req history audit is available to the user types that have this new user type privilege enabled.



RTC Internal reference # 302016.

Talent Gateway Account Creation - Two Factor Authentication

Starting this release, based on configuration, clients can set up the feature of two-factor authentication for candidates that create a new Talent Gateway account. This avoids the creation Talent Gateway accounts using fake email addresses, thereby reducing fake accounts and enhanced security for the candidates.

When candidates create a new Talent Gateway account with their email address as a user name, the email address is validated using a passcode that is sent to the candidate's email address.

This feature is available only when:

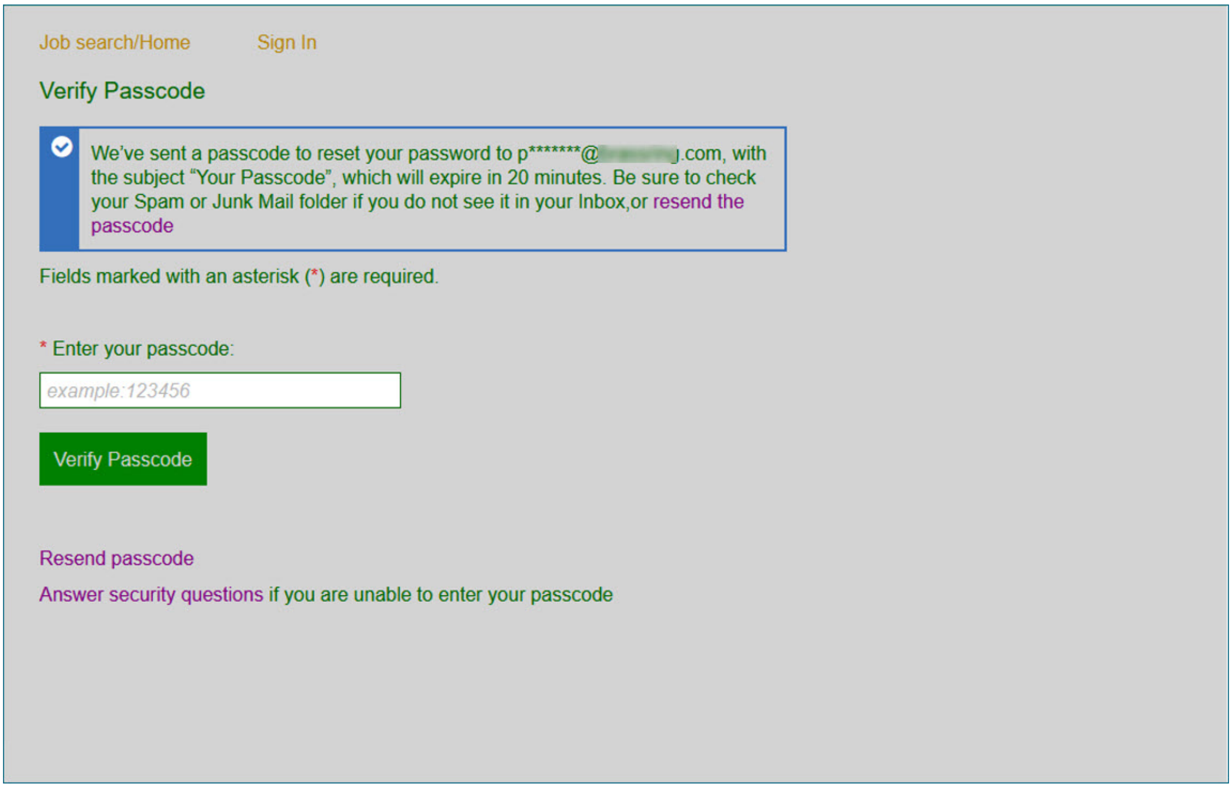
- The Talent Gateway is not Single Sign-On(SSO) based.
- The Talent Gateway setting **Sign in availability for candidates** is not set to Disable Sign-in
- The client setting **Talent Gateway login type** is set to E-mail address only.

A new Talent Gateway setting **Email validation for create account** is added for this feature. Refer to the new setting in the Workbench section of this document.

When the appropriate client settings and Talent Gateway settings are configured, the following account creation workflow comes into effect:

1. Candidates attempt to create a new account on a Talent Gateway.
2. Candidates select **Don't have an account yet** link.
3. Selecting this link takes the candidates to the client's privacy policy page if that page is set up by the clients. Candidates review and accept the privacy policy to proceed further. If there is no privacy policy, they move on to the next page directly.
4. On the next page, the candidate provides their email address. The email address is first verified

   a. An error message is displayed if the email address is already present in the system.
   b. An error message is displayed if the entry is not in a proper email address format.
5. If the email address passes the verification, an email is sent to the same with a passcode that is valid for 20 minutes.
6. Candidates enter the passcode they received on the next screen.
   a. If an incorrect passcode is entered, an error message is displayed alerting the candidate that the passcode is incorrect.
   b. Each time a new incorrect passcode is entered, an error message is displayed with the number of times an incorrect passcode is entered.
   c. If the candidate provides incorrect passcode more than 5 times, the account creation process for that email address is locked for an amount of time as configured by the client in the Talent Gateway setting. The default lock out period is 10 minutes.
7. If the candidate is unable to use the passcode for any reason before it expires, they can use the Resend Passcode link to send a new passcode to their email address.
   a. When a candidate selects Resend Passcode, a new passcode is sent to their email address and the Verify passcode screen is updated.
   b. A message is displayed to the candidate stating that the passcode is resent. The message displayed is: **Passcode email sent again. This is attempt #**
   c. Each time a new passcode is requested using the Resend Passcode option, the message is updated to display the number of times the request was made and the number of times the passcode was sent.
   d. When a candidate attempts Resend passcode five times, the Resend functionality is disabled and an error message is displayed stating the maximum number of attempts were made. The candidate is prevented from using the same email address for account creation for a period of time as set in the Talent Gateway settings.
8. When a candidate provides the accurate passcode that is received to their email address, the next screen is displayed when the candidate provides their account password and selects security questions and answers.
9. By providing this information, the candidate successfully creates a new account on the Talent Gateway.



RTC Internal reference # 303292.

Custom Form Fields - Client Controlled Key

A new Client controlled key feature is added to Workbench that allows clients to manage Custom Form Field Encryption keys to secure encrypted fields within BrassRing.

Who can access or configure the Key Management functionality?

Only Workbench users, Self Service users (tier 5 and above) who have a special back-end flag enabled have access to the new Key Management menu option. The BrassRing engineering team manages the access to the key management feature in Workbench for Workbench users through requests made via a support ticket.

Users access this feature in Workbench by selecting the new Key Management menu option (Workbench > Tools > Settings > Key Management). The users must enter their Workbench password to configure client-specific encryption keys. An email is sent to your organization's designated user (Client Setting: **Key Management Notification Email**) when the key is updated by a Workbench user.

How does this feature work?

When the encryption keys are created by a Key Management System (KMS) (external system to BrassRing) the client-controlled key will be combined with the client-specific BrassRing key from the KMS to produce a final key.

The Key Management module provides the following options to the users with appropriate access:

1. Text Box. Label **Enter Client Key for Encryption**. Field Length Max: 64 Characters.
2. Text Box. Label **Re-enter Client Key for Encryption**. Field Length: 65 Chars (helps with copy-paste truncation validations) compares the Enter key text on text change and displays a black X mark when text not matched and displays a Green tick mark when text from both fields match.
3. Text Box. Label **Enter Workbench User Password**. Workbench users logged in and updating the Key must enter their Password for verification. Field Length: 100 Chars
4. Cancel and Save Buttons.
    a. Selecting Save validates the following:
        i. Validate user's Password - Invalid password error message displayed when users enter a wrong password in the password field.
        ii. Key value match between the two fields and display an inline error message if the text is not matched.
        iii. Character limit - minimum 30 and maximum 64.
        iv. Special Characters allowed : $&()./\^_:0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
    b. Selecting Cancel closes the page.
5. The page displays a link to an audit trail that tracks user activity.

Two new client settings are added for this feature in the Client settings section of the Workbench:

A new client setting **Key Management Frequency Restriction (days)** is added with a default selection of 30 days. Validation of the input allows a minimum value of 1 and a maximum of 365. This setting is used to restrict key configuration for the set number of days. For example, if the value in this setting is 30 days, a user cannot add a new key within 30 days of the last change. The module displays the date on which the last key addition was performed, and also the date after which a new key can be added.

Another new client setting **Key Management Notification Email** is added for key management communications. Clients can add one or more email addresses in this setting. A communication is sent to the email address added in this setting, each time a key management action is performed successfully by a user.

The following details are included in the email when a Key is updated:

- Subject: Key Management Notification - [ClientName]
- Body: New Encryption key has been added to the system.
- Added by: [lastname, firstname]
- Added on: [datetime stamp]
- Environment: [Env name] This message was e-mailed from a send-only account. Please do not reply.

RTC Internal reference # 302100.

BrassRing Workbench

Rules Automation Manager (RAM) - Automation Manager Trigger Migration

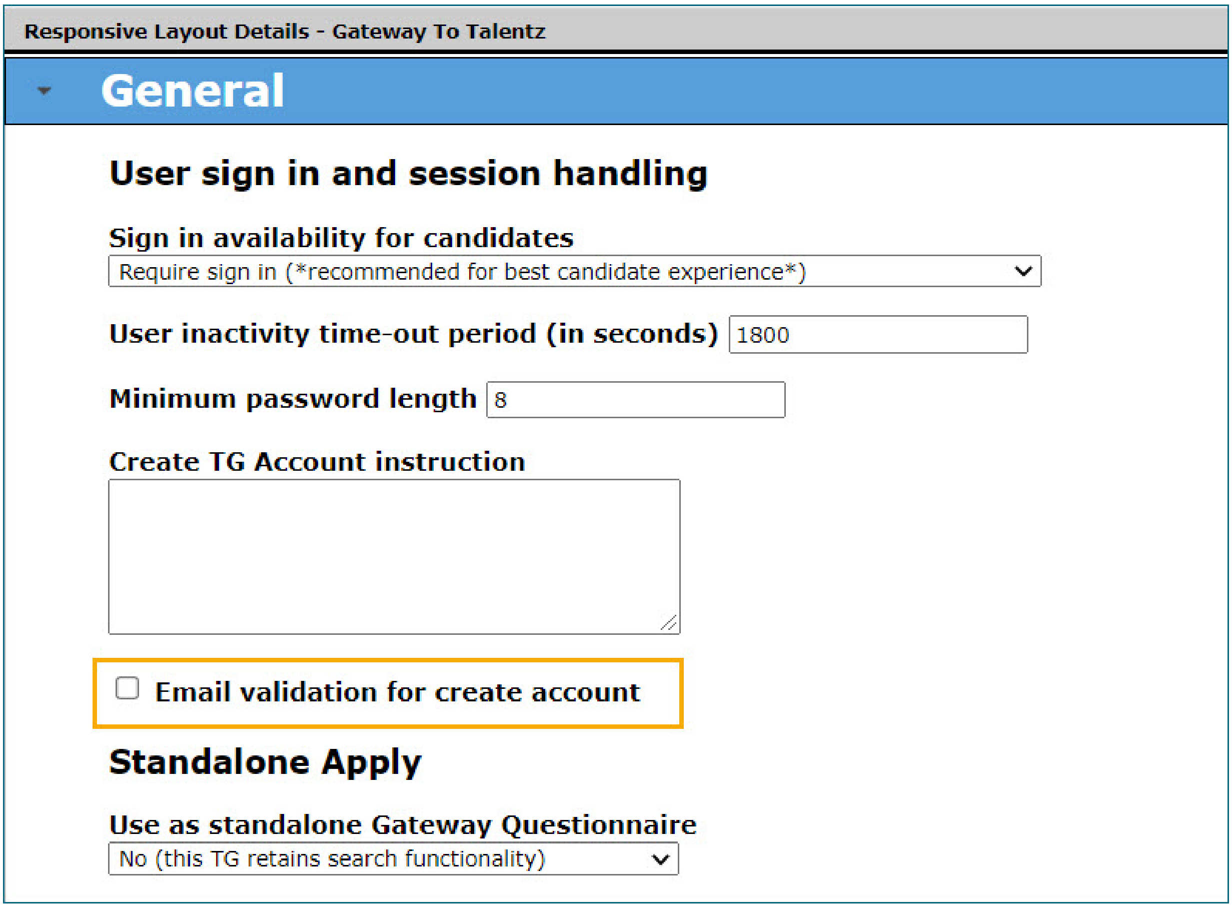
NOTE
This feature was deployed to the Staging environment during release 21.03.16. This feature is going to be available in the production environment starting the current release.

As a part of the product enhancements, the existing Automation Manager (AM) triggers are converted to RAM triggers starting this release. The AM Trigger *HR Status update - notify candidate* is converted to a RAM trigger during the current release.

Two Factor Authentication - New Talent Gateway Setting

A new Talent Gateway (TG) setting is added in the Responsive Layout Details section. The setting **Email validation for create account** is added in the General section as a checkbox. By default, the setting is unchecked. This setting is available to clients only when the client setting **Talent Gateway login type** is set to **Email address only**.

This is a required setting in the configuration of the new feature of Two-factor authentication while creating a Talent Gateway account.



This setting is a global level setting and all member Talent Gateways of a Global Talent Gateway inherit the selection made at the global level.

RTC internal reference # 304372.

Key Management - New Client Settings

Two new client settings are added for the new feature **Key Management**:

A new client setting **Key Management Frequency Restriction (days)** is added with a default selection of 30 days. Validation of the input allows a minimum value of 1 and a maximum of 365. This setting is used to restrict key configuration for the set number of days. For example, if the value in this setting is 30 days, a user cannot add a new key within 30 days of the last change. The module displays the date on which the last key addition was performed, and also the date after which a new key can be added.

Another new client setting **Key Management Notification Email** is added for key management communications. Clients can add one or more email addresses in this setting. A communication is sent to the email address added in this setting, each time a key management action is performed successfully by a user.

RTC internal reference # 302100.

Lead Manager December 2021 Release

There are no new features delivered during this release for Lead Manager.

Onboard December 2021 Release

Onboard new features for the December release are listed here.

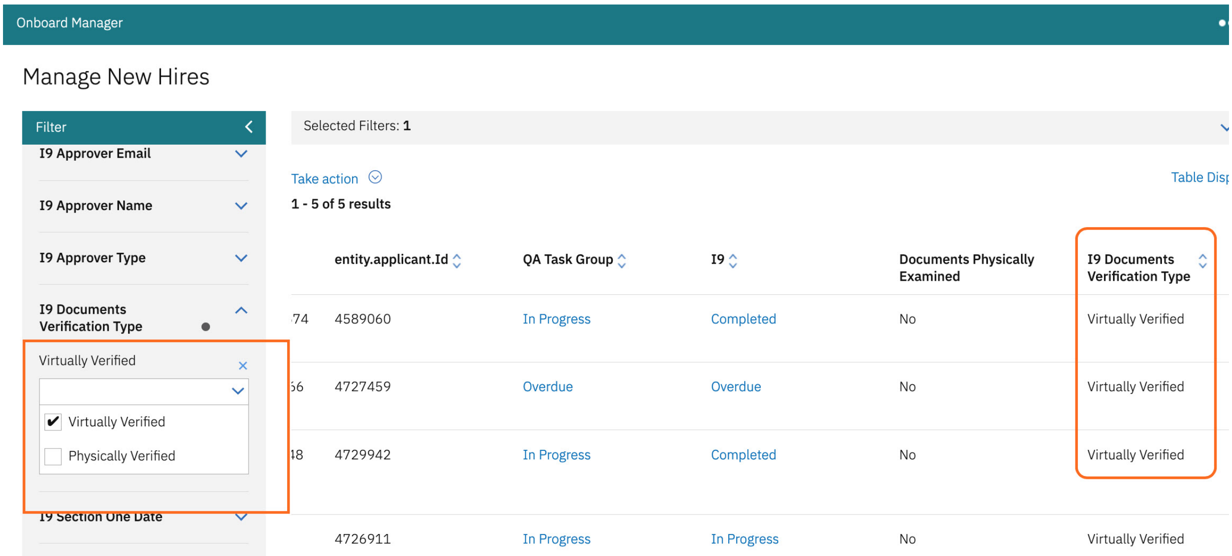
Onboard Visible Changes

Onboard new features for the current release are listed here.

I9 Section 2 - Virtual Verification

Due to the impending situation, clients are opting for virtual verification of the documents. However, clients would like to track and report whether the verification was done physically or virtually.

A new field is added to keep track of the type of verification. Users select the appropriate option based on the type of verification after the verification is completed. Based on the data entered in this field, clients can generate a report on the number of verifications done virtually.



RTC internal reference # 303481.

E-Verify - Search Update

When hiring managers try to filter for a string field (Everify DHS case Status field) the results include not just the search string, but additional tags to the search string.

For example, If a search is performed for "closed/employment_authorized" in the filter only "closed" status fields should be displayed in the results. However, previously, "closed (no_action_fnc)" or "closed employment_authorized" were being displayed.

Starting this release, updates were made to the search so that the hiring managers get only the results that are an exact match in the IQA environment.

RTC internal reference # 304136.

State Forms - Updated

The following set of state tax forms are updated during the current release:

- Nebraska 9N
- Arizona US A-4
- Arizona US A-4V

- Arizona US WEC
- Arizona US A-4C

RTC internal reference # 304191.

Onboard Configuration Changes

Onboard configurable features for the current release are listed here.

Integration Enhancements - I9 Section 3 Node for Exports

Previously, the I9 section 3 was a stand-alone and there was no provision for exports directly by the PSE team. Section 2 was being used for exports because of this reason.

Starting this release, a new node is created for the I9 Section 3 basic information exports. Data from the following fields can be exported by the PSE team based on this change:

- Section 3 Document Title
- Section 3 Document Number
- Section 3 Expiration Date
- Section 3 HR Sign Date

RTC internal reference # 245427.

Onboard Fixed Defects

The following defects are fixed during the current release.

Table 1. Fixed Defects

RTC Defect Number	Defect Description
303569	TS006680700 - Nebraska Release Form Upload - Save and Finish Later
303602	TS006706846 - Users added to the escalation/reminder email when they should not be
303603	TS006707276 - Condition was met but activity was not present - Age less than 14
304098	30348100036438 - Unable to complete Section 3
304541	00043692 - SC w4 state form is missing mapping
304035	00032994 - Onboard start activity was not autocompleted for two NewHires