Release 93, June 13, 2024

Wurk is a continually improving and evolving application. As part of our commitment to full transparency, we provide release notes that summarize the latest enhancements to Wurk functionality and usability.

Table of Contents

Highlights From This Release 4
Advanced Scheduler 4
Base Compensation Reporting 4
Scheduled Reports 4
MFA Refresh 4
Payroll 5
Earnings and Deductions 5
Added Columns to Earnings and Deduction Report 5
Employee Payroll Maintenance 5
Payroll Processing 5
Tax Government Forms 5
TLM 5
LOA - Restart Questionnaire 5
Scheduled Hours Display Over Midnight 6
Scheduler 6
Multi-Schedule View 6
Open Shifts 6
Copy and Paste Time Off 6
Schedule vs Actual Report 6
HR 7
Base Compensation: Audit Trail Information for Additional Compensation Added 7
HR Maintenance: Base Compensation History Report: 'As of Date' Added 7
Government Forms: EEO-1 Updated 7

Government Forms: Submit Buttons Updated 7
Incidents: Auto-Populate Fields Added to Incidents.... 7
Learning: Implementation Updates.... 8
Learning: Preferred Name 8
Cross Product 8
Reports & Charts.... 8
Email Schedule Configuration 8
Schedule Expiration 8
All Scheduled Reports 9
Expiration Warning Messages 9
Never Expire Permissions.... 10
Run Only Once 10
Security/Authentication 10
Security Authentication Level Updates 10
Authentication / Authorization - Two Factor Authentication (2FA) Refresh 11
2FA Landing Page 11
Landing Page: Defaults and Preferences Authentication: Text-based or Call-based.... 12
Remember Last Used Options 12
Dynamic Timer for the Resend Button 12
Authenticator Application Setup Page 13
Authenticator App Registration for Users with a Different MFA Method 13
Authentication Preference Destination Added Upon First Login 14
Employee Self-Service and 2FA 15
Employee Profile 2FA Widget Updates.... 15
Employee Checklists.... 16
Selection Screen.... 16
Resident and Work Location Toggle 18
Personal Experience 19
Auto Assign Role Profile with Null Role to New Users.... 19
Role Profile Auto Assignment via Import Scenarios 19
Warning Message If User Removes Role Profile.... 20

Platform 20
Würk Connect 20
Expand and Collapse Functionality 20

Highlights From This Release

Advanced Scheduler

There is now an easy way for managers to copy and paste time off periods on schedules, so they do not have to request it on behalf of their employees outside of schedules.

Base Compensation Reporting

Audit trail information for Additional Compensation has been added to audit trail report. When an employee's Additional Compensation widget is edited or new entries are added, this activity will now be reflected in an audit trail report.

Scheduled Reports

When a user creates an email schedule for saved reports, they can now select an expiration date beyond which the report will no longer be emailed automatically.

MFA Refresh

There have been significant improvements to Two-Factor Authentication (2FA) functionality. These new updates aim to improve the authentication experience, simplify the authentication workflow, and drive employee self-service. **Note:** These new features will be released **June 22nd.**

Payroll

Earnings and Deductions

Added Columns to Earnings and Deduction Report

Earnings and Deductions report has more columns for admins to see additional data.

- Now shows EE and ER blocked Last 3rd or 5th.
- Scheduled deduction EE and ER overrides.

Employee Payroll Maintenance

Mass Edit Account Taxes now includes Auto Correct, the Auto Correct checkbox is enabled, the account tax jurisdiction for FICA, MEDI, CA SDI and/or WA FLI.

Payroll Processing

Updated message in Payroll Pre-Check Report, shows the count of Pre-Check Records Reviewed against the total number of records. This is helpful for users who keep up with marking records as reviewed when they see them.

The payroll pre check report now shows if any Pay Period profile changes have been made.

Tax Government Forms

The SC withholding form is updated, Step 2 of the worksheet on the form has up to date values in the dropdown menu.

TLM

LOA - Restart Questionnaire

During the qualification questions, if one needs to restart the questionnaire process, a new Restart option is available in the Do I Qualify widget.

Example: One has made it to the third question of the questionnaire and realizes he may have answered the first question incorrectly. Selecting Restart opens a Restart Questionnaire window and choosing to restart brings him back to the first step of the same questionnaire workflow.

Scheduled Hours Display Over Midnight

When a scheduled shift crossed midnight, the schedule displayed on the Time Entry, Calc Detail, and Exceptions pages of the Timesheet, once for the day on which the schedule started and once again for the day the schedule ended. If the employee had the same schedule for both days, both shifts would show on the same day without a way to differentiate the two. With this enhancement, when a shift crosses midnight, the schedule now shows an indicator on the day it originated.

Scheduler

Multi-Schedule View

Additional Employee and Cost Center Filter options have been added to the Multi Schedule Overview.

Upon selection of a shift, within the shift pop-up window, the following actions icons are available:

- Unassign Employee - removes employee from being assigned to the shift and becomes an open shift on the schedule.
- Manage Shift - opens Manage Shift pop-up for manager to make edits to the shift.
- Delete Shift - deletes shift completely from schedule.
- Notes - allows for notes to be added to the shift.

Open Shifts

In the Manage Open Shifts page, managers were able to see shifts that were outside of their Managed Scheduled Cost Centers. This has been corrected to prevent visibility to other managed schedules.

Copy and Paste Time Off

There is now an easy way for managers to copy and paste time off periods on schedules so you do not have to request it on behalf of your employees outside of schedules.

Schedule vs Actual Report

The Schedule vs. Actual report was unable to be filtered to only display the managed cost centers for managers. With this enhancement, a new Security profile option within the Schedule > Views/Reports section for this report, Only for Managed Cost Centers, is available to limit the view of managers to just those within their managed cost centers.

HR

Base Compensation: Audit Trail Information for Additional Compensation Added

When an employee's Additional Compensation widget is edited or new entries are added, this activity will now be reflected in an audit trail report, accessible within the My Reports area of the application. Proper security permissions will apply. Under the 'Audit Reports' section of the 'Reports' tab of the user's security profile, ensure 'Account Info' is checked. The report is located under: My Reports > System Reports > Audit Trail > Account Info.

This information will also be available under an employee's quick links within their employee profile. Select the 'Employee Utilities/Quick Links and Actions' icon in the header containing the employee’s name, then select the 'Account Audit Trail' link. This will take you to the same audit trail report.

HR Maintenance: Base Compensation History Report: 'As of Date' Added

An **As of Date** option has been added to the Base Compensation History report that allows you to see what employees were getting paid at that time. The filter is based on the Base Compensation 'Date From' field. The report is accessed under: HR > Reports > Employee Maintenance > Base Compensation History.

Government Forms: EEO-1 Updated

An updated EEO-1 form has been added to the system and contains updated expiration dates as well as updated current and prior reporting years.

Government Forms: Submit Buttons Updated

There were inconsistencies with the Submit button in several of the government forms where some were worded 'Submit Form,' 'Submit,' and 'Submit with the form name.' The CC-305, I9, and TFN Declaration forms were updated so they will all now show as 'Submit.'

Incidents: Auto-Populate Fields Added to Incidents

Previously, while creating an Incident in the system, a manager or administrator with limited group access was not able to select their name, or possibly other employees, as the Initiator or Supervisor.

In this release, within the Comment section of an Incident, both the Initiator field and Supervisor field will be auto populated once the Incident is created. These auto-populated fields will be able to be edited by selecting another user from the look-up list.

Learning: Implementation Updates

Historically, course status wasn’t updated on reports when the Learning profile was removed from an employee's profile.

Now, course status will be updated on reports if the Learning profile is removed from an employee’s profile.

Learning: Preferred Name

Previously, an employee's 'Legal First Name,' as listed in Account Information in Wurk, populated the 'Preferred First Name' field in Learning (Schoox). Going forward, an employee's name listed in the 'First Name' field in Wurk will populate the 'Preferred First Name' field in Learning.

Cross Product

Reports & Charts

Email Schedule Configuration

With this release, users now have more flexibility in configuring scheduled reports.

Schedule Expiration

When users create an email schedule for saved reports, they can now select an expiration date beyond which the report will no longer be emailed automatically. This expiration date can be set in the Manage Email Schedules pop-up window when adding or editing a report schedule. By default, the expiration date is set for 90 days from the current date. Additional options for setting the expiration date include 365 days from the current date, or a custom date the user can enter. Recipients of the emailed report will be reminded of the report email schedule's expiration date when the expiration date is within 60 days of the current date. The expiration warning message includes a link that the user can select to open the Email Schedule Configuration and edit the expiration date if necessary.

In addition, when setting a report schedule (where available), users can now set an expiration date when choosing a Weekday or a Days Profile schedule type.

All Scheduled Reports

Additional columns have been added to the All Scheduled Reports report to allow users to see additional details for both scheduled reports and email schedule configurations. The report also allows users to distinguish between email schedule and schedule report types in the listings. Users may have to add a column to the reports using Add Columns to capture specific configuration information.

Users can mass edit the expiration dates for email schedule configurations by selecting the configurations to edit and then using the Mass Edit Email Schedules button.

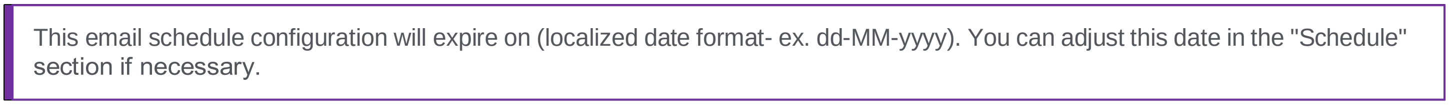
New columns available in the All Scheduled Reports report:

Column Name	Column Value
Expiration Date	Expiration dates set on scheduled reports
Type	Type of configuration for scheduled reports: Send to my completed reports, Send to delivery destination, or Email schedule
Email Schedule Name	Name provided for the email schedule configuration
Expiration Date	Expiration date tied to the email schedule configuration
Schedule Report Delivery Destination	Configured delivery destination value set for the report
Email Schedule Report Description	Email schedule configuration description
Email Schedule - Schedule Type	Schedule type for a configured email schedule: Weekdays, Days Profile, or Run Once
Enabled	Enabled state of scheduled report and email schedule configurations

Expiration Warning Messages

Users are provided with notification messages when the email schedule configuration has expired or is about to expire, ensuring they can promptly re-enable or disable the configurations as needed.

When the email schedule configuration is enabled and the **Add Expiration Date** checkbox is selected, the following informational message displays:



This email schedule configuration will expire on (localized date format- ex. dd-MM-yyyy). You can adjust this date in the "Schedule" section if necessary.

When the email schedule configuration is disabled, a warning message displays at the top of the dialog to notify the user that the email configuration is currently inactive with a previously set expiration date.

Never Expire Permissions

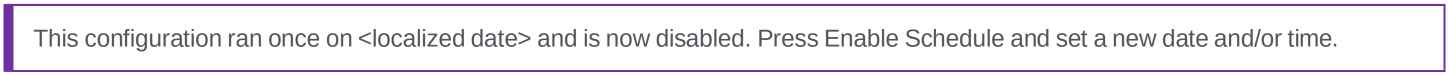
Administrators can now offer users the option to set an email schedule to "Never Expire." Users will be able to see a "Never Expire" option in the Expiration Date drop-down list when the **Display Never Expire** option is marked for the Email Saved Reports permission on the Reports tab in their security profile. The paths to set this permission are as follows:

- Settings > Profiles/Policies > Security > Reports Tab

Run Only Once

When users create an email schedule for saved reports, they can now select "Run Once" for the schedule type. This will allow users to set an email schedule that will send the report email once, after which the schedule will be disabled. Users can re-enable the schedule later and reset the schedule as needed to send the report once again.

If a user opens an existing email schedule configuration after a Run Once date and\or time has occurred, they will receive the following message:



This configuration ran once on <localized date> and is now disabled. Press Enable Schedule and set a new date and/or time.

Security/Authentication

Security Authentication Level Updates

To help ensure that users do not have a higher Authentication Level than their role is expected to have, the security permissions for the items in the table below have been adjusted appropriately.

Security Permission	Previous Authentication Level	Current Authentication Level
Employee Status History (Global tab, Company Setup)	High	Medium

External Pay History (**ONLY** the setting under the Reports tab > Payroll Reports)	High	Medium
Incident Types (HR tab > Incidents)	High	Medium
Resolutions (HR tab > Incidents)	High	Medium
Violations (HR tab > Incidents)	High	Medium
Skills (Global tab > Global Setup and Global tab > Object List)	High	Medium
Competency Skills (HR tab > HR Tables)	High	Medium
Checklists (HR tab > Employee section)	Medium	Low
HR Action Request (HR tab > Employee section)	Medium	Low
Employee Custom Form Items (HR tab > Employee Custom Form Items section; applies to all permissions for all forms listed)	Medium	Low
HR Actions (HR tab > HR Actions section; applies to all permissions for all actions listed)	Medium	Low

Authentication / Authorization - Two Factor Authentication (2FA) Refresh

Important Note: The MFA update features will not be delivered the day of the release. It will be rolled out on **June 22nd.**

We have made significant improvements to our Two-Factor Authentication (2FA) functionality to provide you with a smoother, more user-friendly experience. These changes enhance security and make it easier for you to access your account.

2FA Landing Page

A refreshed landing page for Multi-Factor Authentication (MFA) now includes all available options, governed by their assigned Authentication Policy, for users to authenticate . The user can choose from any available method.

Landing Page: Defaults and Preferences Authentication: Text-based or Call-based

The phone number drop-down includes the following with the country code:

- The employee's configured Text Number or Voice Number for 2FA.
- The Work Phone number is selected by default, or if the Work Phone is not present, the preferred order for the pre- selected phone number (based on availability) is: Work Phone, Cell Phone, Home Phone, the employee's configured Text Number or Voice Number for 2FA.

Remember Last Used Options

The application now remembers the last 2FA method and destination (phone number and email, if applicable) used. With this update, the user does not need to re-select their method and destination each time they need to authenticate. When a user logs in to the application using 2FA, the next time they log in to the application, it selects the method and destination they last used.

If the last method used is no longer available, then the application looks to the default based on what is available. The system chooses the default from the following areas, going down the list:

• Work Phone > Cell Phone > Home Phone > employee's configured Phone for 2FA

• Primary Email > Secondary Email > Personal Email > employee's configured email for 2FA

Dynamic Timer for the Resend Button

When users request a verification code, there is a waiting period of 60 seconds before they can request another code. To ensure that users know when they can request a new code, there is now a dynamic timer for the **Resend** button.

When a user has requested a 2FA Code, the following settings apply to the **Identity Verification Page**:

- The **Resend** button displays.
- When a user lands on the Identity Verification Page, a reverse countdown timer starts at 59 seconds and goes down to 0 seconds. When the timer is between 59 seconds and 1 second, the **Resend** button is disabled. When the timer hits 0 seconds, the **Resend** button is enabled.
- When the user clicks on the **Resend** button, the countdown timer begins again. If the user navigates away from the page, the timer continues to count down.

On the **Landing Page**, if a user selects a different destination (i.e. phone or email) within the same Two-Factor method, the timer is still in effect. If a user selects a 2FA method that already has an active timer, when they press **Send Code**, an error message appears stating:

> You need to wait 'X' seconds before you can request another code.

> **Note:** The **X** equals the seconds left until they can send a code for that specific 2FA method.

There is a timer for each 2FA method (Voice, Text, and Email). If the user logs out, or lands back on the login page, the countdown timer is reset.

Authenticator Application Setup Page

The Authenticator Application Setup page has been refreshed to provide better usability, ease of use, and an improved overall experience. Please note the following:

- If the user is not registered for an Authenticator App, the user lands on the Authenticator Application Setup page.
- The Authenticator App Setup page displays a QR code as well as an **Account name** and **key** to set up the Authenticator App.
- The checkbox for **Recertification Frequency** displays the number of days based on the Recertification Frequency defined in the user's Authentication Policy.
- **Authenticator App** is in blue text, and the following tooltip displays when hovering over the words or focusing on them:

> Popular Apps: Google Authenticator and Microsoft Authenticator

Authenticator App Registration for Users with a Different MFA Method

Users can now register an Authenticator Application during the login process so they don't have to navigate to a different screen once they login. If a user is not registered for an Authenticator Application, and the user has already authenticated with other methods in the past, when the user selects the Authenticator App-Based Authentication:

- The user is asked to authenticate first via other method(s) (Text, Voice, or Email).
- Once the user authenticates with the other method(s), the user is presented with the Authenticator App configuration screen.

The available other methods to authenticate by first are based upon what is enabled on their Authentication Policy. If the user does not have anything else enabled on their Authentication Policy, methods are provided based upon what is on their Employee Profile or MFA preference values.

If the user does not have any other methods enabled and does not have anything on their employee record or MFA preference record, they are sent directly to the Authenticator App configuration page without having to Multi-Factor Authenticate.

Authentication Preference Destination Added Upon First Login

> **Important:** When a user is logging in **for the first time**, they may not have any existing contact information (phone number and email address) associated with their profile. For this scenario **only**, users can add their own phone number and email address during the first login so they can useTwo-Factor Authentication and access the application.

In this scenario, when the user provides their phone number or email address during the initial login process, if the provided information is valid, then:

- The system verifies the contact information.
- The user can choose to receive verification codes based on the Two-Factor method configuration in their assigned Authentication Policy.
- Upon successful setup, the user can use the method and destination for Two-Factor Authentication.

When an accurate phone number or email address is not provided, the following occurs:

- If the user does not provide their phone number or email address, but they do have an Authenticator Application as an option, they are directed to the Authenticator App Setup page.

> **Note:** If the user does not have Authenticator App enabled in their Authentication Policy, the user **cannot** skip adding an email address or phone number.

- If the user does not have voice, text, or email enabled as a Two-Factor option, but they have an Authenticator App enabled, they are directed to the landing page with the Authenticator App selected.
- If the user provided an incorrect phone number or email address, they can edit the phone number or email address before they verify their identity. If the user does not provide a valid phone number or email address, they receive an error message stating that the phone number or email address is invalid.

Employee Self-Service and 2FA

Users can now see the number and email they have configured for 2FA so they can decide if they need to update it or remove it. The page title is renamed Two-Factor Authentication (My Information > Two-Factor Authentication), and the following additional updates are applied:

- The button previously titled Change Virtual Code Settings Information is now titled Save.
- The Security Permission under ESS > Personal Settings is now named Two-Factor Authentication.
- The Widget title is now Two-Factor Authentication.

When a user lands on the page the phone numbers and email addresses are filled in and unmasked in the appropriate input fields. The user can Update and Clear the following details for Authentication depending upon the Authentication Methods enabled in their Authentication Policy:

- Text number
- Voice number
- Email Address

The user must enter their login password before updating the information. When the user clicks on the Save button, if there is no error, the details are updated. The fields are in the following order:

- Text Message Number
- Voice Call Number
- Email Address
- Password (required field)

Employee Profile 2FA Widget Updates

Users need to see the Two Factor Authentication (2FA) methods and destinations available for an employee in case the employee experiences any issues. The following updates have been made to the Employee Profile 2FA widget:

- The Two-Factor Available Options table has been removed.
- The Two-Factor Registration Status title is renamed to Two-Factor Authentication Options.
- The Two-Factor methods display based upon what is enabled in the user's assigned Authentication Policy.
- All phone numbers (Employee record and self-configured option) that can be used for Two-Factor Authentication display in the column for Text Message and Voice (second column).
- All email addresses (Employee record and self-configured option) that can be used for Two-Factor Authentication display in the second column.

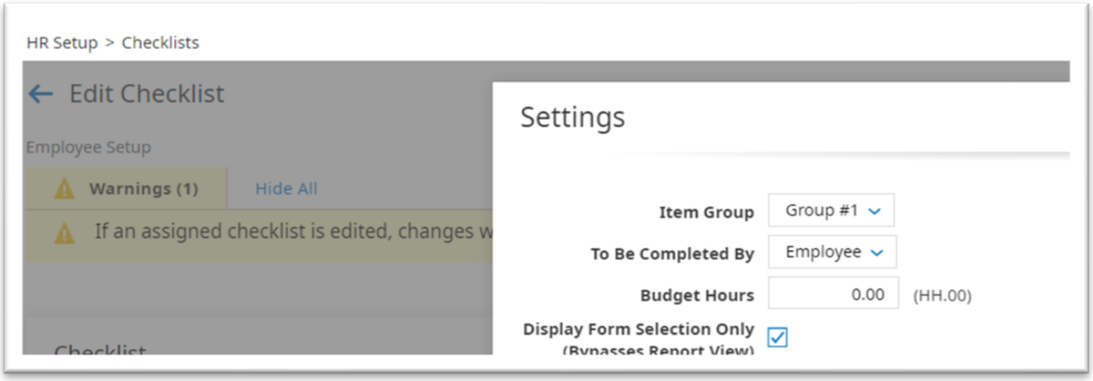
  • If an Authenticator Application is not configured, a value of Not Configured displays in the second column.

- If an Authenticator Application is configured, a value of Configured displays in the second column.
- If there is no phone number available for use with text messages or voice Two-Factor Authentication, a value of **Not Configured** displays.
- If there is no Email address available for use, a value of **Not Configured** displays.

Employee Checklists

Withholding Forms in Checklists: Display Form Selection Only (Bypasses Report View) Option

Users may only want to see the Withholding Forms related to their residential and primary work location addresses, which allows them to quickly locate and complete the forms without spending extra time trying to locate them. Users with access to Checklists (Security Permission Checklists enabled under Global > Global Setup > Checklists) who create or edit the Screen Link - My Form Withholding checklist item inside of a Checklist now have a new option in the settings, **Display Form Selection Only (Bypasses Report View)**.



HR Setup > Checklists

Edit Checklist

Employee Setup

Warnings (1) Hide All

If an assigned checklist is edited, changes w

Checklist

Settings

Item Group: Group #1

To Be Completed By: Employee

Budget Hours: 0.00 (HH.00)

Display Form Selection Only (Bypasses Report View): ☑

When the Screen Link – My Form Withholding Checklist Item is created or edited inside of a Checklist, this new option allows users to bypass the Withholding report screen. Once enabled, when users open the Screen Link – My Form Withholding checklist item from the Checklist (the corresponding checklist item assigned to them), then the Withholding report is not shown, and instead users are taken directly to the Form Selection page. If needed, users can still disable the option to see the full list of available Withholding Forms.

This option is unchecked by default in existing or newly created Checklist Items of this type.

Selection Screen

If the Display Form Selection Only (bypasses Report View) checkbox is enabled in the Screen Link-Withholding Checklist Item configuration, and a user opens the Checklist and the My Form Withholding

Checklist Item, a new screen displays with the list of Federal and State Withholding Forms. This screen provides the same data as the **Add New** screen, such as:

- Name of Territory or State
- Name of Form (user clicks on the name to add the form)
- Form Code

> **Note:** Some states like New York and North Carolina have two forms, so the new approach attempts to keep these next to each other in the layout.

Users can search for State, Form Names, and Code Names on the screen. A warning message displays explaining the following:

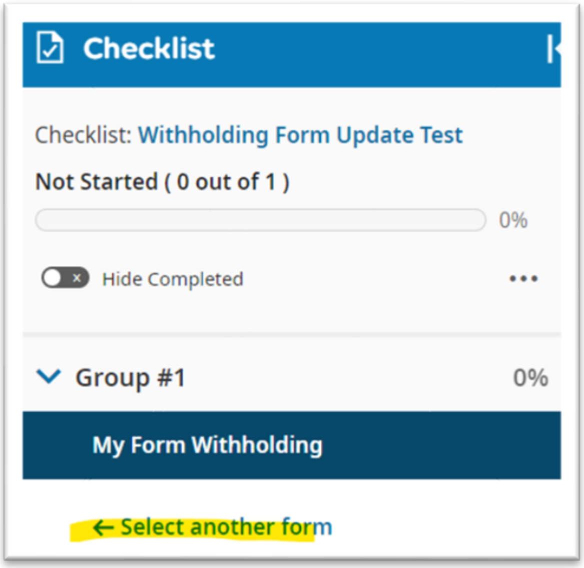
> Your security settings prevent you from starting a W4 form. Please contact your system administrator.

When the Display Form Selection Only (Bypasses Report View) option is enabled or disabled by a System Administrator or Company Administrator for in-progress Checklists, any Checklists with this item currently assigned must be reassigned to reflect the change. Newly assigned Checklists include the update.

Links in the selection are not disabled even if certain Forms have been submitted or approved, the page is accessed outside of the Checklist panel, or the Checklist Item step has been marked as Complete. Links are always enabled on this screen no matter the actions made by the user.

Select Another Form Option

When the Withholding Form Selection appears, a **Select another form** option in the Checklist Item list on the left side panel allows users to return to the Form Selection page. If a user selects this option, they are navigated to the Form Selection screen, and the form that was previously in focus is retained.



Checklist

Checklist: Withholding Form Update Test

Not Started (0 out of 1)

0%

Hide Completed

Group #1 0%

My Form Withholding

← Select another form

Tip: The Mass Delete option for Checklists and Checklist Items never impacts the created Withholding Forms stemming from the Checklist Item.

Resident and Work Location Toggle

When the Withholding Form Selection appears, a toggle, **Forms For My Location**, that allows the user to switch between:

- Their resident and work location.
- Their related State Withholding Forms and all available forms.

The logic for this new toggle relies upon the following conditions:

- The Withholding Form that displays in the list is shown based upon the state found in the account's personal home address in their Employee Profile via the Personal Information widget in the **State** field.
- The Withholding Form that displays in the list as it relates to their work location is based upon the address defined for the Default Cost Center(s) assigned to the user. If no default Cost Center address is defined, the **State** field for the Company is used when there is a single EIN, or the address for the account's assigned EIN is used when there are multiple EINs.

Personal Experience

Auto Assign Role Profile with Null Role to New Users

The application now automatically assigns a Role Profile to new users who are added without a Role Profile assigned to them. This includes users who are manually hired via the Employee Information report, via the Applicant portal, via HR Actions, or via import.

To ensure that hiring administrators are aware of the change in behavior in case they purposefully leave this field blank, a tooltip has been added under Employee Information > Hire > Other Settings > Role Profile and Applicant Information > Hire > Other Settings > Role Profile. The tooltip explains:

> Role profiles are used to personalize experiences. If left blank, the system will override.

> **Note:** This functionality does not impact any users who already have a Role Profile assigned to them.

Role Profile Auto Assignment via Import Scenarios

The following scenarios are accommodated when automatically assigning Role Profiles to employees added via import:

- If the company has a default Role Profile configured, then the default Role Profile value is used.
- If the employee being imported already exists and has a Role Profile assigned to them, their existing Role Profile is used.
- If the company does not have a default Role Profile configured and a default Security Profile is configured, when the Security Profile is passed in the import file, the Role Profile is auto-assigned based on the Security Profile passed in the import file.
- If the company does not have a default Role Profile configured and a default Security Profile is configured, when a Security Profile is not passed in the import file, the Role Profile is auto-assigned based on the default Security Profile.
- If the company does not have a default Role Profile configured and a default Security Profile is not configured, when a Security Profile is passed in the import file, the Role Profile is auto-assigned based on the Security Profile passed in the import file.
- If the company does not have a default Role Profile configured and a default Security Profile is not configured, when a Security Profile is not passed in the import file, the Role Profile is left blank for the imported employee.

Warning Message If User Removes Role Profile

A warning message now displays if a Role Profile is removed from a user. Role Profiles are used as a method to accurately target users to provide them with relevant content and information. If a user does not have a Role Profile, they do not receive the correct content.

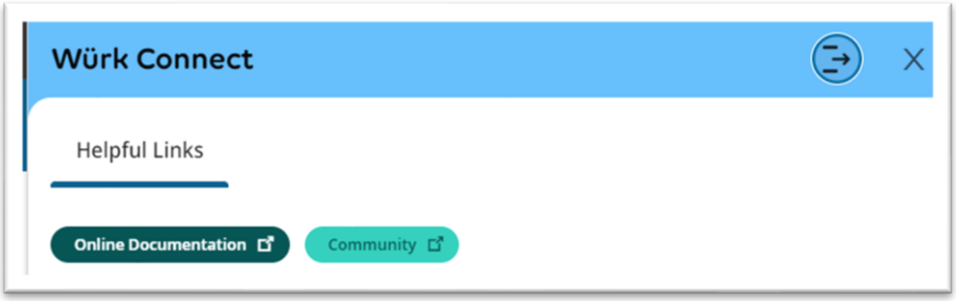
Platform

Würk Connect

Expand and Collapse Functionality

The Expand and Collapse functionality of the Würk Connect panel has been updated with a new icon, and it is moved to the top right of the panel. Selecting the Expand icon expands the panel into a larger state, allowing for more screen space for the Würk Connect content, if needed.

The icon updates to a collapsed state once expanded, and selecting the Collapse icon collapses the panel back to its original size.


Würk Connect
Helpful Links
Online Documentation
Community