

AKIXI 2.5.2 FOR ADMINISTRATORS

Software release 2.5.2 enhancements

Document Revision 2.0

Table of Contents

Table of Contents	2
Introduction	3
Features Summary	4
<i>Administration Enhancements</i>	4
Single Sign On	4
Multi-Factor Authentication	4
New Call Center Reporting User	4
BWKS Parity	4
<i>Reporting Enhancements</i>	4
Notifications	4
New User Tour	4
In Product Education	4
UI – Drag and Drop	4
Remove Repeat Callers	4
Insights Dashboard Enhancements	5
<i>Overview</i>	6
<i>Administrator Instructions</i>	6
Multi-Factor Authentication	7
<i>Overview</i>	7
<i>Administrator Instructions</i>	7
New Call Center Reporting User	9
<i>Overview</i>	9
<i>Administrator Instructions</i>	9
BWKS Parity	10
<i>Overview</i>	10
<i>Administrator Instructions</i>	10
<i>Overview</i>	11
<i>User Instructions</i>	11
UI – New User Tour	12
<i>Overview</i>	12
<i>User Instructions</i>	12
UI – In Production Education	14
<i>Overview</i>	14
<i>User Instructions</i>	14
UI – Drag and Drop	15
<i>Overview</i>	15
<i>User Instructions</i>	15
Remove Repeat Callers	16
<i>Overview</i>	16
<i>User Instructions</i>	16
Copyright & Confidentiality Notice	17
Warranty	17
Trademarks	17

Introduction

This document provides an overview of all the new features that are included within Akixi software release 2.5.2

See the Features Summary section for a concise overview of all the features included within the release.

Every feature has its own section including all the instructions required to administer and utilise the feature effectively.

Features Summary

Administration Enhancements

Single Sign On

Akixi have set up federated identity provider sign-in using OpenID Connect / SAML. Federated identity is a method of linking a user's identity across multiple separate identity management systems. It allows users to quickly move between systems while maintaining security.

Multi-Factor Authentication

To further protect user accounts, administrative users can enforce Multi-Factor Authentication (MFA).

New Call Center Reporting User

When creating a new user or modifying an existing user on an Insights site, Administrators can select Call Center Supervisor from the reporting tab.

BWKS Parity

The BroadWorks Parity setting ensures that, on removal of a BroadWorks Enterprise or Enterprise Group, associated Akixi services are automatically retired.

Reporting Enhancements

Notifications

Users can now configure notifications to be sent via browser push notification or email, to advise of key performance metrics and thresholds.

New User Tour

Users will now receive an interactive tour of the reporting platform when signing in for the first time. This helps to enhance understanding of the product out of the box and can be skipped or replayed as required.

In Product Education

A number of help icons have been embedded into the product, to help give users a readily available help resource to address commonly asked questions and enhance the user's product understanding.

UI – Drag and Drop

When maintaining the Akixi reporting repository, users can use drag and drop functionality along with keyboard shortcuts to simplify management of user report libraries.

Remove Repeat Callers

Reporting users can remove repeat abandoned calls from the same number, to help reduce the number of call records on report styles such as the Wallboard report.

Insights Dashboard Enhancements

The Insights Dashboard has been modified to display only external inbound call statistics from the previous 30 days.

Administration Enhancements

Single Sign On

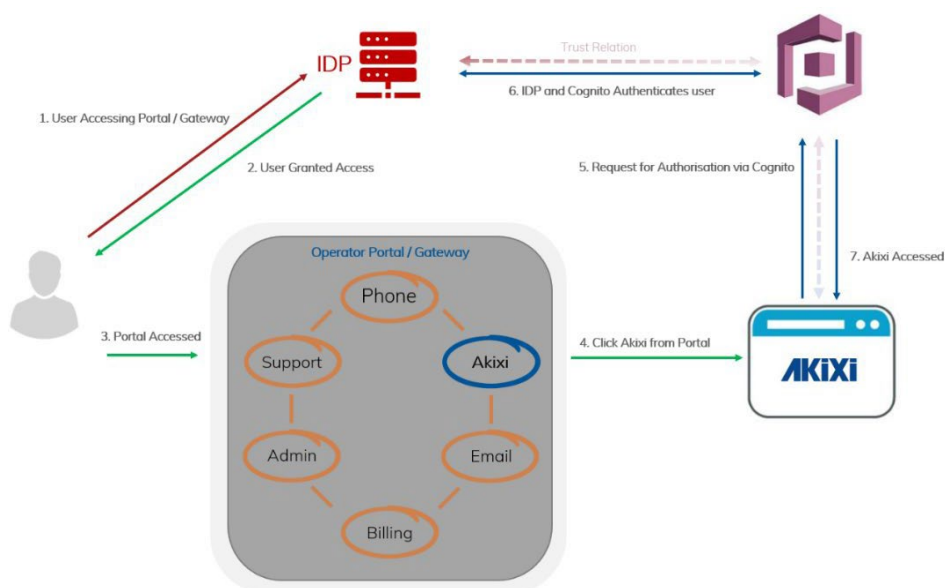
Overview

What have we done?

Akixi have set up federated identity provider sign-in using OpenID Connect / SAML. Federated identity is a method of linking a user's identity across multiple separate identity management systems. It allows users to quickly move between systems while maintaining security.

How have we done this?

Akixi's federated identity provider is setup in AWS Cognito which deals with the communication and authorization access / tokens between the Operators Portal / Gateway, IDP and the Akixi platform.



Administrator Instructions

To find out more about SSO, please speak to your Akixi BDM on how to configure SSO

Operator

Configure OpenID / SAML Connection in your single portal gateway

Akixi

Configure the Akixi user pool to communicate with the IDP

Multi-Factor Authentication

Overview

To further protect user accounts, administrative users can enforce Multi-Factor Authentication (MFA).

Once enabled against an application user, they will be prompted to complete MFA configuration on their next sign in attempt. Examples of MFA applications the user can download on their mobile device to complete this would be Google Authenticator or Microsoft Authenticator.

Administrator Instructions

1. Select the required Application User and select “Change”
2. Select the “User Details” tab
3. Tick the “Enable MFA” checkbox

The screenshot shows a web interface titled "MODIFY APPLICATION USER ACCOUNT". On the left is a navigation menu with tabs: "USER DETAILS" (selected), "PERMISSIONS", "EXTENSION/ENDPOINT", "ROLE", "REPORTING", and "SETTINGS". A red arrow labeled "2." points to the "USER DETAILS" tab. The main form contains the following fields: "Full Name:" with the value "[Full Name Not Specified]"; "Username:" with the value "mfaone"; "Email:" with the value "example@akxl.com"; "Password:"; "Email Language:" with a dropdown menu; "Password Change Required:"; "Send Welcome Email:"; and "Enable MFA:" with a checked checkbox. A red arrow labeled "3." points to the "Enable MFA" checkbox. A tooltip box is positioned over the "Enable MFA" checkbox, containing the text: "Enabling Multi-Factor Authentication (MFA) means the user will be required to enter a code from their authenticator app when logging in." At the bottom of the form are three buttons: "HELP?", "SAVE", and "CANCEL".

MFA can also be enabled by default for users newly added to a Telephony Server. This can be configured by completing the following:

1. Sign into Akixi as an administrator
2. Navigate to “Administration” > “Telephony Servers”
3. Tick the relevant Telephony Server, and click “Change”
4. Tick the “MFA Enabled By Default” box, and click “Save”

COMMUNICATION ENABLED:

COMMUNICATION STATUS:

ENABLE USER MFA BY DEFAULT ← 4.


▼ ADVANCED

Once MFA has been enabled against the application user, the user will be presented with the following screen on their next sign in attempt, where they will be prompted to do the following:

1. Open their desired authenticator app, and scan the QR code
2. Enter the code displayed in the authenticator app
3. Click on "Complete MFS Setup"

Setup Multi-Factor Authentication (MFA)

Please scan the QR code below with your [authenticator app](#).



← 1.

Then enter the code displayed in your app here.

2. →

3. ↓

On completion, the users MFA will now be enforced, and will be required on subsequent attempts by the user to access their account.

New Call Center Reporting User

Overview

When creating a new user or modifying an existing user on an Insights site, Administrators can select Call Center Supervisor from the reporting tab.

Administrator Instructions

1. Click on Reporting
2. Expand the Reporting Level dropdown list
3. Select Call Center Supervisor

The screenshot shows a dialog box titled "ADD APPLICATION USER ACCOUNT" with a close button (X) in the top right corner. On the left is a sidebar with navigation options: USER DETAILS, PERMISSIONS, EXTENSION/ENDPOINT, ROLE, REPORTING (highlighted in blue), and SETTINGS. The main area contains several configuration fields: Reporting Level, Default Reports, Reporting API, Enhanced Mobile App Features, Call Recording Integration, Read Only Report Access, and Report Template User. A dropdown menu is open for the "Reporting Level" field, showing options: NO REPORTING, None, PERSONAL REPORTING, Presence User, ONE User, INSIGHTS REPORTING, Insights User, and Call Center Supervisor. Red arrows and numbers indicate the steps: 1. points to the "REPORTING" tab, 2. points to the "Reporting Level" field, and 3. points to the "Call Center Supervisor" option in the dropdown. At the bottom are three buttons: HELP?, SAVE, and CANCEL.

BWKS Parity

Overview

The BroadWorks Parity setting ensures that, on removal of a BroadWorks Enterprise or Enterprise Group, associated Akixi services are automatically retired.

With this setting enabled, when an enterprise or enterprise group in BroadWorks is deleted, the Akixi services linked to the setup will automatically shut down, this includes partitions, telephony servers and application users.

Administrator Instructions

1. Sign into Akixi as an administrator
2. Navigate to “Administration” > “Partitions”
3. Tick the relevant Partition for existing setups, and click “Change”
4. Tick the “Maintain Parity” box
5. Click “Save”

The screenshot shows a configuration panel for 'CONFIGURATION SYNCHRONISATION'. It includes several input fields and checkboxes. A blue arrow labeled '4.' points to the checked 'MAINTAIN PARITY' checkbox. Another blue arrow labeled '5.' points to the 'SAVE' button at the bottom right of the panel. The 'ADVANCED' section is collapsed.

^ CONFIGURATION SYNCHRONISATION

TYPE ON TELEPHONY SERVER: Enterprise Group

ENTERPRISE OR PROVIDER ID:

GROUP ID:

SYNCHRONISATION TYPE: Soft

MAINTAIN PARITY: ← 4.

PERFORM SYNCHRONISATION NOW:

STATUS

SYNCHRONISATION LAST STARTED AT:

SYNCHRONISATION STATUS / ERROR:

^ ADVANCED

SAVE CANCEL

Reporting Enhancements

UI – Notifications

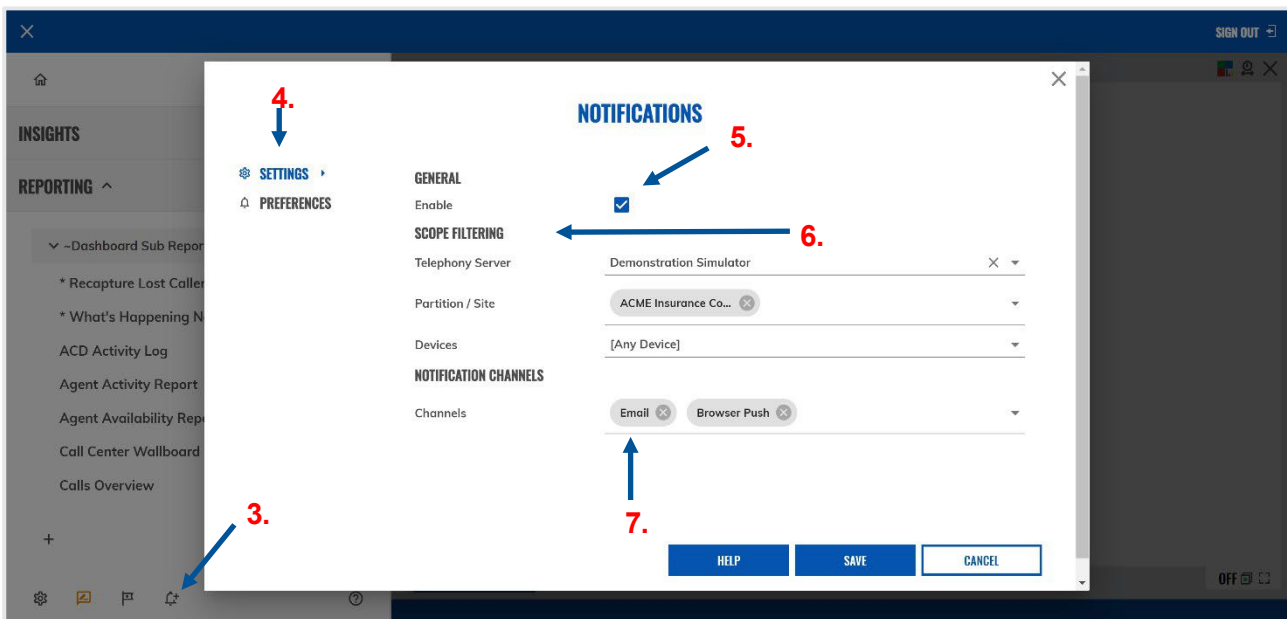
Overview

Users can now configure notifications to be sent via browser push notification or email, to advise of key performance metrics and thresholds.

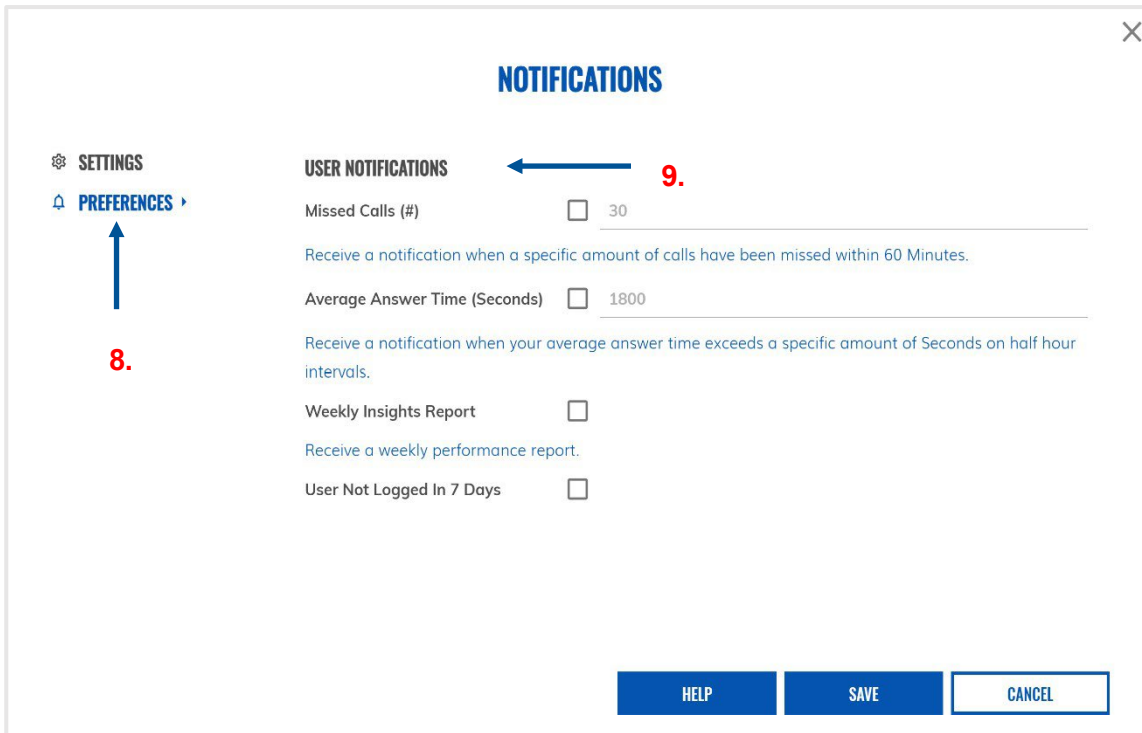
This enhancement will allow for users to keep track of key performance indicators, without the requirement to be actively signed into the application.

User Instructions

1. Sign into the Akixi application
2. Expand the hamburger icon in the top left
3. Click the bell icon
4. Select “Settings”
5. Ensure “Enable” is ticked
6. Set the required scope filtering – This will generally be set by default through user permissions
7. Select the desired notification channels



8. Select “Preferences”
9. Enable the individual notifications and threshold values required



UI – New User Tour

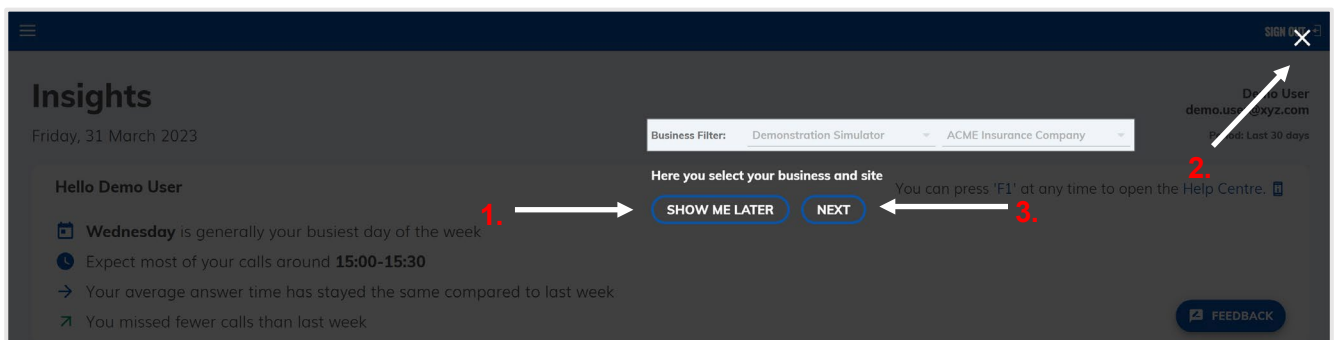
Overview

Users will now receive an interactive tour of the reporting platform when signing in for the first time. This helps to enhance understanding of the product out of the box and can be skipped or replayed as required.

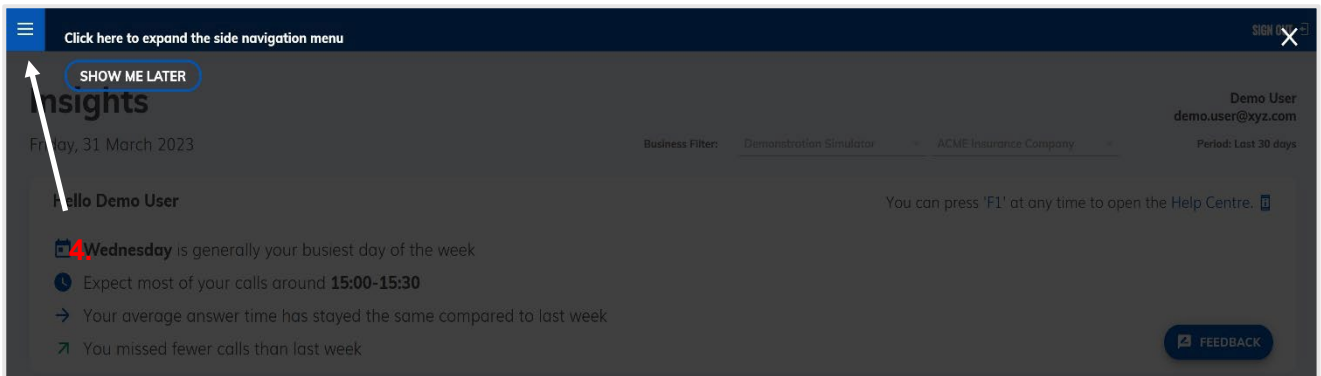
This enhancement takes individuals through a number of pages within the reporting portal, as well as assists in some basic report creation. This tour can be delayed until the next time the same page is accessed, skipped altogether or replayed if required as a refresher.

User Instructions

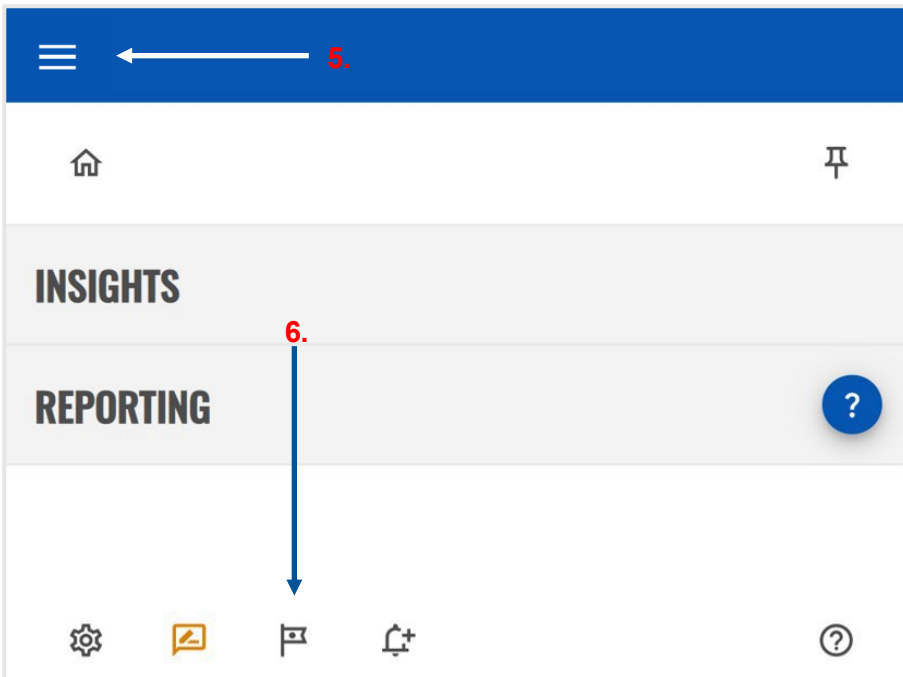
1. To postpone the tour until the next point the same resource is accessed, click the “Show Me Later” button
2. To skip the tour altogether, click the “X” icon in the top right
3. To navigate to the next step of the tour, click on the “Next” button



4. In some cases, to proceed with the tour, users will need to click on a highlighted element within the portal



5. To restart the tour, users should click to expand the hamburger icon in the top left of the portal
6. Within the expanded menu, click on the flag icon to restart the tour



UI – In Production Education

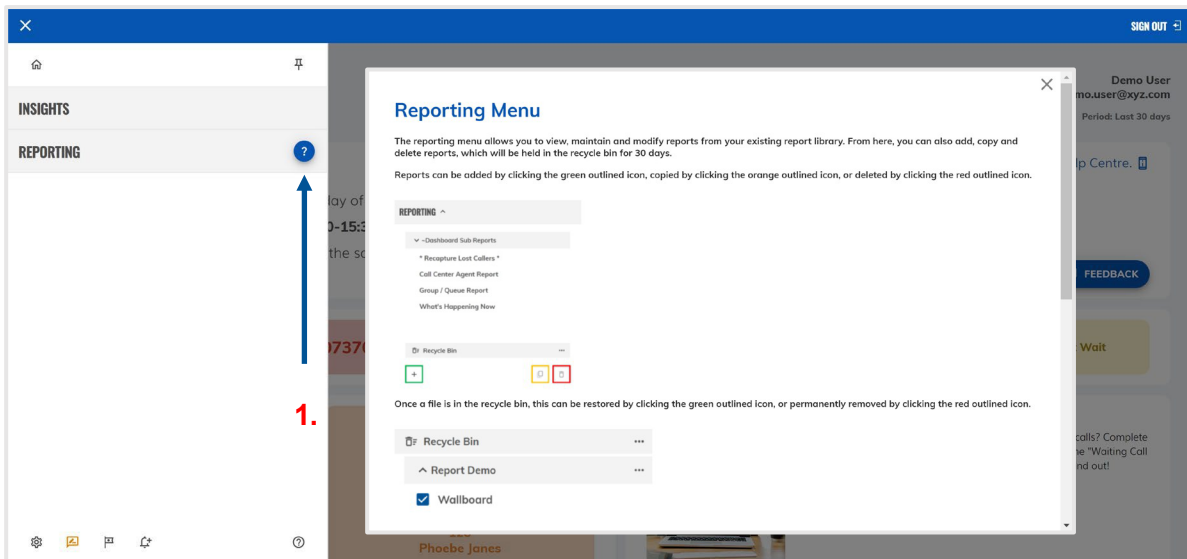
Overview

Several help icons have been embedded into the product to help give users a readily available help resource. This addresses commonly asked questions and enhance the user's product understanding.

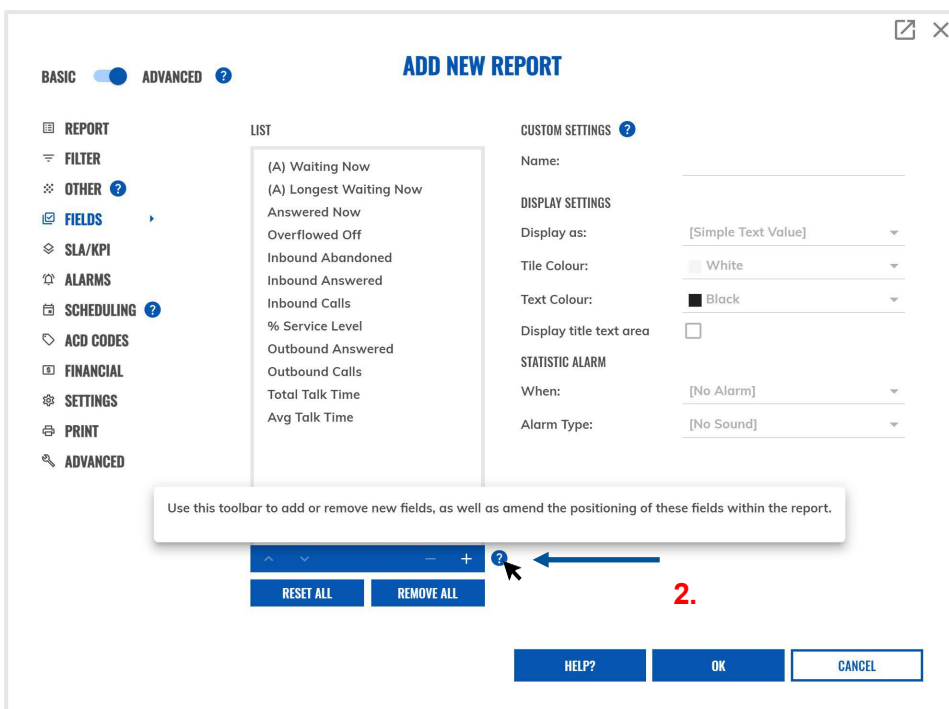
These help icons will be presented either by pop-out windows within the portal itself, or via tooltip when the user's cursor hovers over the help icon.

User Instructions

1. To access the pop-out help information, click on the help icon beside the specific item



2. To access the tooltip help information, hover the cursor over the help icon beside the specific item



UI – Drag and Drop

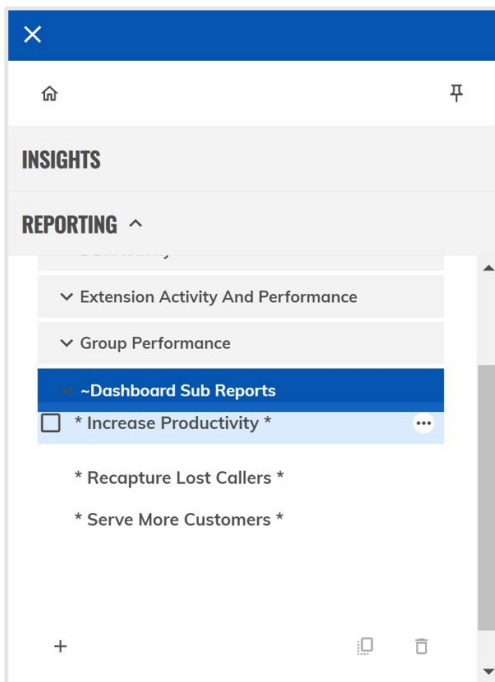
Overview

When maintaining the Akixi reporting repository, users can use drag and drop functionality along with keyboard shortcuts to simplify management of user report libraries.

This enhancement allows for users to manage their report library more easily, without the need to enter and edit reports through the modification window.

User Instructions

The user can drag and drop reports within the reporting library from one folder to another.



In addition to this, the user can make use of keyboard shortcuts to simplify the maintenance of their report library. The keyboard shortcuts available as of release 2.5 are the following:

- Ctrl+C – Copies the selected reports
- Ctrl+V – Pastes the selected reports
- Ctrl+Delete – Deletes the selected reports

Remove Repeat Callers

Overview

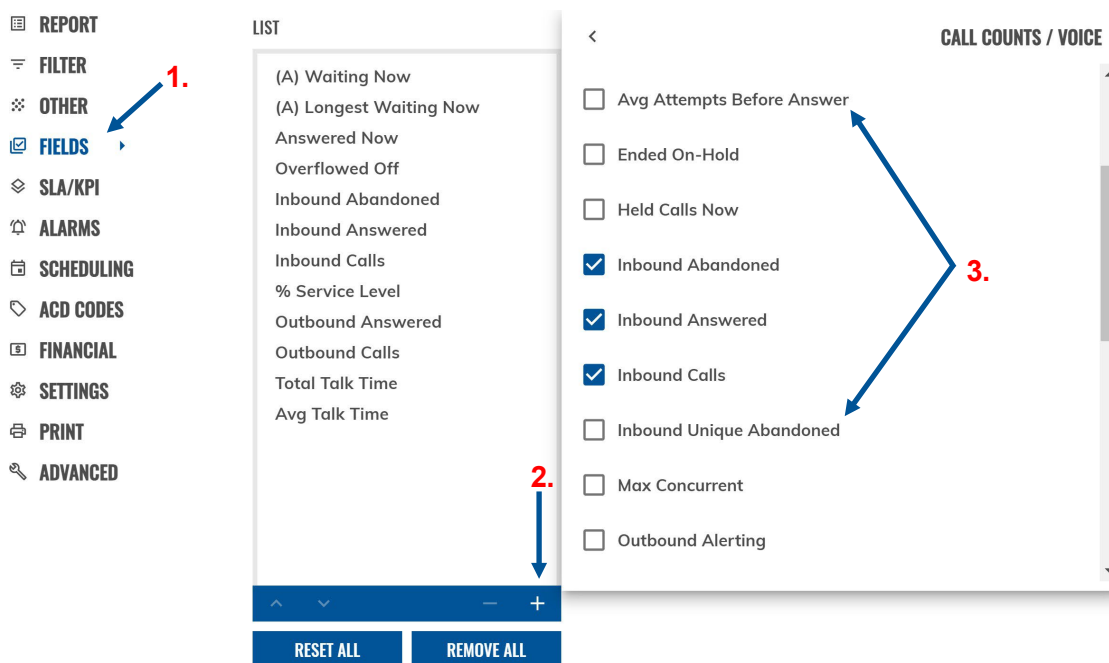
Reporting users can remove repeat abandoned calls from the same number to help reduce the number of call records on report styles, such as the Wallboard report.

This is achieved through the addition of two new fields, “Inbound Unique Abandoned” and “Average Attempts Before Answer”.

User Instructions

Reporting > Create or modify a report (e.g. Wallboard)

1. Navigate to “Fields”
2. Click on the “+” icon to add in a new field
3. Select “Call Counts” > “Voice” and tick either “Avg Attempts Before Answer” or “Inbound Unique Abandoned”



Copyright & Confidentiality Notice

Copyright © Akixi. All Rights Reserved.

Any technical documentation that is made available by Akixi Limited is proprietary and strictly confidential and is considered the copyrighted work of Akixi Limited.

This publication is for distribution under either the Akixi Non-Disclosure Agreement, the Akixi Reseller Agreement, or the Reseller Distribution Agreement only.

No part of this publication may be duplicated without the express written permission of Akixi Limited.

Akixi Limited reserves the right to make changes without prior notice.

Warranty

The Akixi Service reporting functionality, supported call flow scenarios, Akixi Service configuration and provisioning functionality and workflow examples, recommended telephony platform configuration, suggested product billing strategies, and/or any provided data examples is/are provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement.

In no event shall Akixi Limited be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the Akixi Service reporting functionality, supported call flow scenarios, Akixi Service configuration and provisioning functionality and workflow examples, recommended telephony platform configuration, suggested product billing strategies, and/or any provided data examples, or the use or other dealings of the Akixi Service, its APIs, or any associated documentation.

Trademarks

Cisco® BroadWorks® and BroadSoft M6 are trademarks of Cisco System, Inc.

All other trademarks identified herein are the property of their respective owners.