

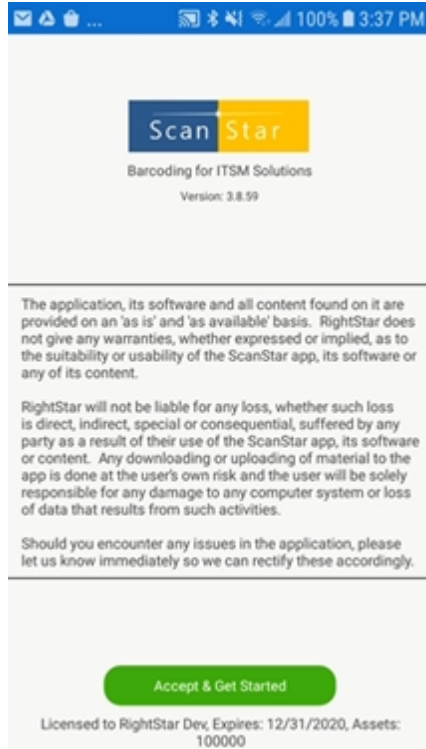
ScanStar Documentation

Table of contents

Introduction	3
FAQs	3
What's new	4
Getting Started	7
System requirements	7
Installation	7
Sign In	8
Preferences	8
Configuration	11
Using ScanStar	19
The Interface	20
Workflows	23
Receive	24
Track	25
Verify	26
Audit	26
Audit Sets	28
Incidents	29
Provider Specific	30
Atlassian Jira	30
Riada Insight	32
BMC FootPrints Service Core v12	36
BMC Remedyforce Service Desk	39
BMC Client Management	42
BMC Remedy	44
Sample Barcode Tags	47
Contacting Technical Support	49

Introduction

What is ScanStar for Smartphones?



ScanStar for Smartphones is the logical extension of our existing ScanStar barcode acquisition and data manipulation application. The new smartphone version of ScanStar will introduce new technology and new functionality to a new set of popular platforms; iOS and Android OS. These operating systems are widely used on smartphones today and are being adopted by purpose-built scanner manufacturers as well (Android OS in the case of the later).

The existing ScanStar Integration Engine will remain the foundation of the set of integrations to ITSM and ITAM products supported today as well as a new JIRA integration. The mobile client portion of the application is the major focus of this update. ScanStar's existing three Modules are updated for the new client operating systems and are now referred to as "Workflows". A new Audit Workflow has been added for the purposes of enhancing the current Verify workflow's capabilities and ease of use.

Support for the following technologies has been added:

- On-board Camera - Allows capture of barcode tags as well as the acquisition of images to assign to assets.
- Purpose built enterprise scanners with physical trigger image scanning integration
 - Zebra
 - Janam
 - Panasonic

FAQs

ScanStar v3.8.x

Frequently Asked Questions (FAQ)

Q Is this solution compatible with the iPhone?

A Yes

Q Is a server required for ScanStar?

A The only requirement at this time is a smartphone with a camera running Android v4.4 or higher or iOS 11.2 and higher.

Q How can I integrate this with my ITSM solution?

A We are currently working on a number of integrations at this time. Supported platforms include, but are not limited to:

- Riada Insight server and cloud
- Atlassian JIRA server and cloud
- BMC FootPrints v12 - with Microsoft SQL Server 2008 or higher database.
- BMC Remedyforce Service Desk
- BMC Client Management - with Microsoft SQL Server 2008 or higher database.
- BMC Remedy v9 and higher

What's new

ScanStar Smartphone Version History

ScanStar v3.8.59

- Edit workflows: fixed incorrect field formatting (expands) when data exceeds the screen width.
- Audit Properties configuration: replaced manual editing with drop down lists to pick fields.
- Track: default common fields is now optional and can be configured in the Preferences -> Advance Settings.
- Audit: optimized scanning process.
- Offline:
 - Fixed audit to display the right assets for selected tab.
 - Fixed password validation on subsequent logins.
 - Unable to save field property changes.
 - Ability to update Licensed Assets Filter.

ScanStar v3.8.58

- Insight connector changes/fixes:
 - Search field is based on sort column now
 - Ability to search by any common object type attribute
 - Support for reference object filter
 - Support for custom Statuses
- Remedyforce connector: Fixed incorrect date only field format issue
- Barcode scan Accept prompt is now optional and configurable in the preferences.
- Support for Date only expression as default value in a field.
- Fixed UI issues in dark theme on iPhone.
- Fixed attachment issue on iOS devices.
- Audit UI changes:
 - Buttons to display assets to be audited and audited in separate lists.
 - Ability to manually search on configured scan and display fields.

ScanStar v3.8.56

- Fixed Remedyforce login issue.
- Fixed BCM Receive assets issue with an invalid Device Group Id.
- Fixed activity indicator issue when saving an asset.
- Remedyforce: fixed format for date fields.

ScanStar v3.8.50

- Remedyforce bug fixes.
- Fixed configuration file sharing issue specific to iPads.
- Workflows: expression defined in default value for a field is not resolved when user edits the field.
- Offline mode: app crashes when scanning data into a reference field.
- Check assets workflow.
- System and user permissions.

ScanStar v3.8.41

- German localization fixes.
- InsightCloud bug fixes.

ScanStar v3.8.40

- ServiceNow integration is supported.
- App does not login from welcome screen when Remember Me is enabled.
- Remedyforce: reference fields not being recognized as scan fields when configured.
- Remedyforce: ScanOnce feature not working as intended.
- InsightCloud: fixed linking asset / issue upon issue creation.
- Configuration: prevent configuring all ScanFields as ScanOnce

ScanStar v3.8.35

- Insight Cloud: app now supports Insight Cloud version.
- Date Picker: switched date picker control due to compatibility issues with latest Android/iOS versions.
- Insight: Assets and Users picklist search capability. User picklist scrolling.
- Access About screen from workflows menu to display license info.
- Remedy: Receive, Track, Verify: clicking on menu crashes the app.
- Insight:Error when attaching picture taken with camera.

ScanStar v3.8.32

- Insight Cloud integration is supported now.
- Preferences: all updated info is lost when app loses focus.

ScanStar v3.8.24

- BMC Client Management: fixed object error when updating assets created with BCM Client/Discovery

- Preferences: all updated info is lost when app loses focus.

ScanStar v3.8.21

- ITSM Type is visible only when count is 2 or more.
- ScanView default is set to 40.
- AssetForm: errors/exceptions logged to app error log file.
- Preferences: menu option actions now display appropriate messages.
- Insight - users can now add a comment.
- UI enhancements: consistent fonts, layout. Moved field images into the field. Fixed overlap of text over image.
- Insight: ability to create new reference objects on the fly.

ScanStar v3.8.20

- Off-line mode: display message after menu selections in Preferences.
- Off-line mode: app crashes when copying db to downloads and if no db exists in downloads.
- Incident create configuration: unable to select fields and add to Incident form.
- Incident update: unable to save incident changes.

ScanStar v3.8.18

- BMC Client Management: ability to search users by name in lookup.

ScanStar v3.8.17

- BMC Client Management: configurable user group for pick list.
- BMC Client Management: enumerated list for applicable Financial Asset Management fields.

ScanStar v3.8.16

- BMC Client Management: incorrect license count validation for specified device group.
- Off-line mode: 2D imager trigger scanning support for Janam XT20.

ScanStar v3.8.15

- BMC Client Management - optional use of alternate device group in place of default 'All Devices' group to track devices.

ScanStar v3.8.14

- Barcode Scanning: addressed inconsistencies in Track workflow when barcode fields are of reference type (allows picking data from a related list).
- Incident Creation: app now supports creating incidents and viewing linked incidents for existing assets.

ScanStar v3.8.12

- Barcode Scanning: app is unable to read 4 character code 39 symbology.

ScanStar v3.8.11

- Receive: auto save on a barcode scan is now optional.

- Receive: scanning sequence is off when form contains scan once fields.

ScanStar v3.8.10

- Fix for sharing config file issue on Android platform.
- Signature Pad display on workflow screens are now optional.
- Insight: search query optimization.
- Picker (dropdown) fields can now be configured as scannable fields.
- Audit: scan search resulting with multiple assets now doesn't audit them automatically.
- Receive: ability to configure a scan field to be scanned only once per session.

ScanStar v3.8.6

- Janam scanning integration: app now supports reading barcode from Janam built in laser/imager.
- Remedy: error creating Asset/People relationship when People company info is unavailable.

ScanStar v3.8.4

- Option to configure Licensed Assets Filtering.
- Ability to configure parse and map substrings of barcode data.
- Configuration - addressed minor inconsistencies with pick lists on various screens.

ScanStar v3.8.2

- License validation fails when the URL in Preferences contains a '/'

Getting Started

System requirements

Server Requirements

A server is not required for the SmartPhone version of ScanStar

Scanner Requirements

Minimum Requirements:

One smartphone running on **Android** v4.4 API level 19 or higher or **iOS** 11.2 and higher. Also referred as "the scanner" in this

document. The smartphone also requires a camera with auto focus and at least 5 mega-pixels for optimal performance to scan the bar

codes.

Installation

To understand the power of ScanStar workflows, it is important that you read the [brief user guide](#) and run

through each demonstration scenario using the examples provided.

Please contact [RightStar!](#)

Sign In

Get Started / Sign In

The first time the application is run on the scanner, the welcome screen presents you with couple of options. Two dialogs to grant permissions to camera and storage are prompted consecutively. Click the 'Allow' button to continue using the application. Select the 'Accept and Get Started!' button when you are ready to begin. This will take you to the 'Preferences' screen where you are required to provide some basic information in order to continue. **Supply this basic information in order to login** into your CMDB. Choose the appropriate CMDB Provider that is applicable to you and select "Login" when you have completed the form.

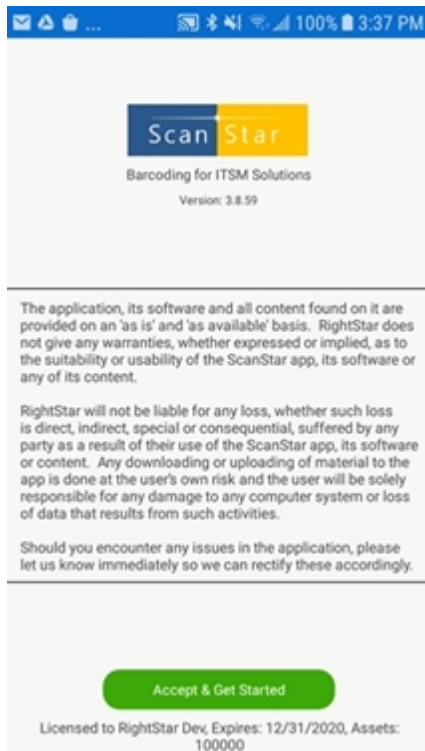


Figure 1

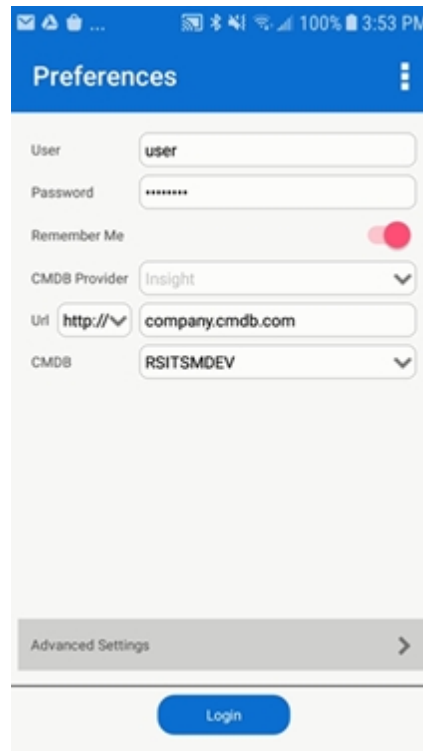


Figure 2

For users already using the application, a 'Install New Config' button will appear above the 'Accept and Get Started!' button in the welcome screen (Figure 1) if a new ScanStar configuration file has been downloaded to your device. Users can opt to install the new file by clicking the 'Install New Config' button or from the 'Preferences' screen.

Preferences

Preferences

Here is where a user can change the preferences or configure the app. This screen can be accessed either from the [Getting Started](#) or the [Workflows](#) menu option.

User: This is the CMDB Provider specific login id for your account.

Password: This is the CMDB Provider specific login password for your account.

Remember Credentials: Select "On" if you will be the only one using the scanner so as not to be prompted each time the application is started.

CMDB Provider: The target ITSM/ITAM application to which ScanStar will be integrating.

Url: This is the platform specific **Server or IP:Port** to your rest / soap API. Please refer to CMDB Provider specific documentation under 'Getting Started'.

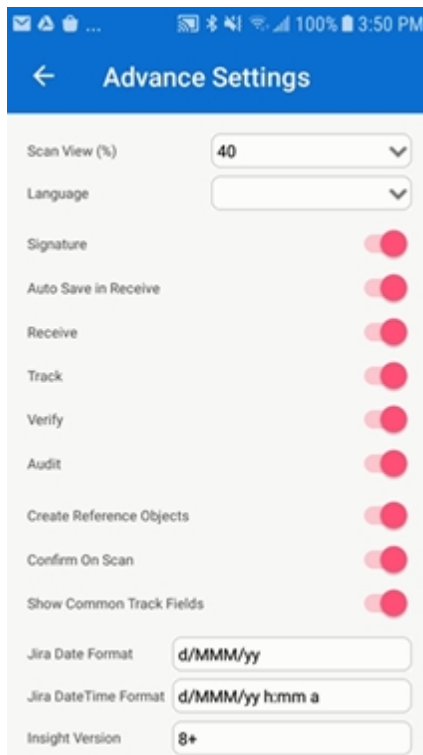
CMDB: CMDB that you will be working with ScanStar

Login: Begin using the ScanStar application

Figure 1

Advance Settings

This screen can be accessed by tapping the 'Advance Settings' option in the Figure 1.



Scan View (%): The amount of screen space used by the scanner (camera) view port.

Language: Defaults to English or any of the supported languages the device is set to. User can override.

Supported Languages: English, French , German, and Spanish

Default Language: English

Signature: The signature pad by default is available in the Receive, Track, and Verify workflows for applicable CMDB Providers and can be disabled (hidden) with this option by turning off this feature.

Auto Save in Receive: By default the data in Receive, Track, and Verify workflows is saved when a scan is complete and is applicable. This feature can be turned with this option.

Enable/disable following workflows: Receive, Track, Verify, and Audit.

Create Reference Objects: Allow creating reference object from Receive, Track, or Verify. Currently available only for Insight.

Confirm On Scan: enable/disable verification prompt upon scanning a barcode. System wide.


Show Common Track Fields: Displays common fields if no CI Type is selected in the Track workflow.

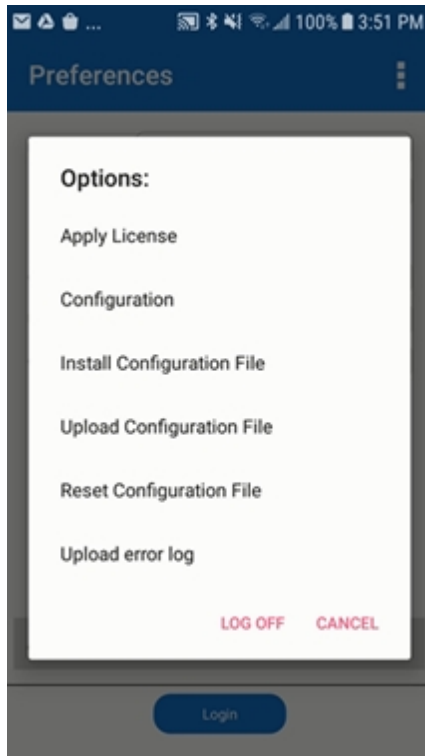
CMDB Provider Specific Settings: settings specific to a CMDB Provider can also be configured here. E.g. 'Jira Date Format', 'Jira DateTime Format' , and 'Insight Version' shown in Figure 2 are Insight specific settings.

Figure 2

Note: access to these settings can be restricted to certain users by including them in the ScanStar license. Please contact RightStar's ScanStar support.

Menus

The are menu options as shown in Figure 3 are accessible by selecting  in the top right corner of the screen. Each of the menu options are detailed below.



Apply License: ScanStar license issued by RightStar sales can be applied here. Download the ScanStar.lic file to your mobile device first and then select this option.

Configuration: ScanStar can be configured to use specific CMDB and its CI Types. Each work flow (Receive, Track, and Verify) for a CI Type can further be configured to display desired fields for the available CI Type fields. Refer to the 'Configuration' section for details.

Upload Configuration File: In case of more than one ScanStar user, the user responsible to define the 'Configuration' can share the file with other users by uploading it via email or other options presented by your scanner device.

Install Configuration File: The Configuration file shared by the admin can be downloaded to users phone. Once downloaded, launch the ScanStar app, login and in the Preferences screen select the 'Install Configuration File'. The downloaded file will automatically be installed and will log off the user. The user can login and start using the application.

Reset Configuration File: Selecting this option will delete the existing configuration file. User will have to re-enter the credentials, login and either install the configuration file or reconfigure the app.

Log Off: This option will take the user back to the 'Getting Started' screen.

Upload Error Log: Errors are logged to a local folder in the application that can be shared with RightStar to help with troubleshooting issues.


Figure 3

Configuration

ScanStar works with a single CMDB from the available list in your system. Here you will be able to pick the CI Types and its fields to be used in ScanStar. You can also define field properties, barcode fields, and audit properties here in this section. ScanStar lets you configure multiple CMDBs and users can switch between them at any given point in the Preferences screen.

CMDBs

Selecting the 'Configuration' menu from the 'Preferences' screen launches the 'CMDBs' screen as seen in

Figure 1a below. Tap on the  to add a 'CMDB' to the 'CMDBs' list. A list of available CMDBs in your system that have not been added will be displayed as shown in Figure 1b. Check the ones you would like to add to ScanStar configuration and 'Confirm'. The checked items will be added to the CMDB list.

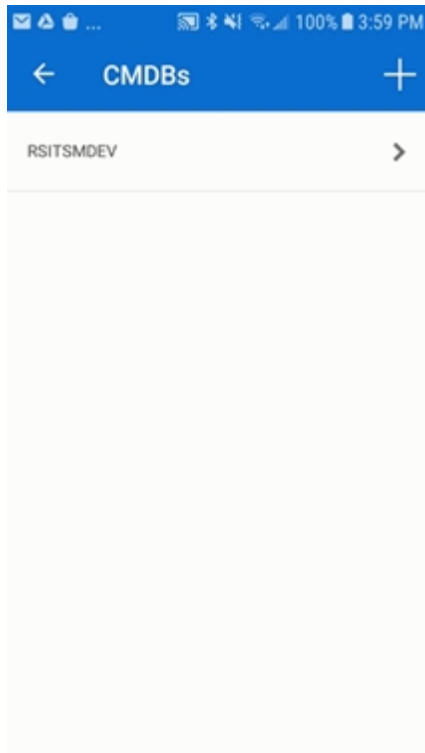


Figure 1a

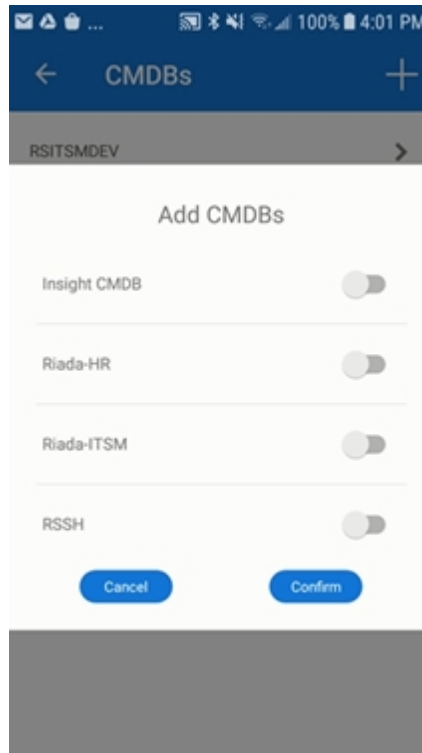


Figure 1b

CMDB

Selecting a CMDB in Figure 1a from the 'CMDBs' screen launches the 'CMDB' screen as seen in Figure 2a below. Here you can configure ScanStar for the selected CMDB.

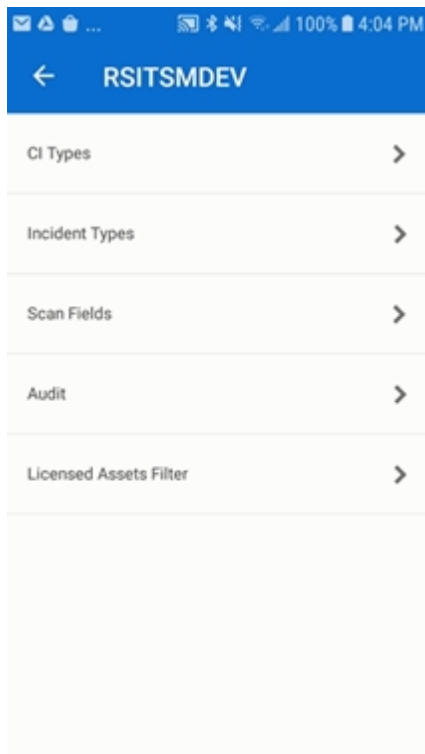



Figure 2

CITypes

The CITypes screen can be accessed from the CMDB screen seen in Figure 2a. Here you can pick the CITypes to work with in the ScanStar application by tapping the  icon on the top tool bar. The dialog will display all CITypes available in the CMDB provider that have not been already added to the ScanStar CITypes list.

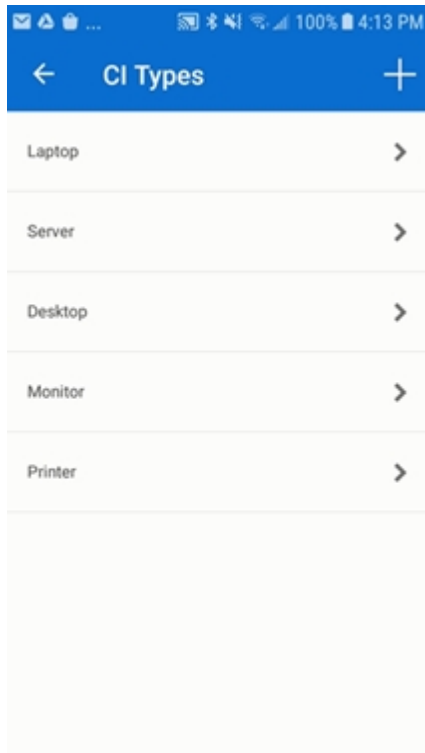


Figure 3a

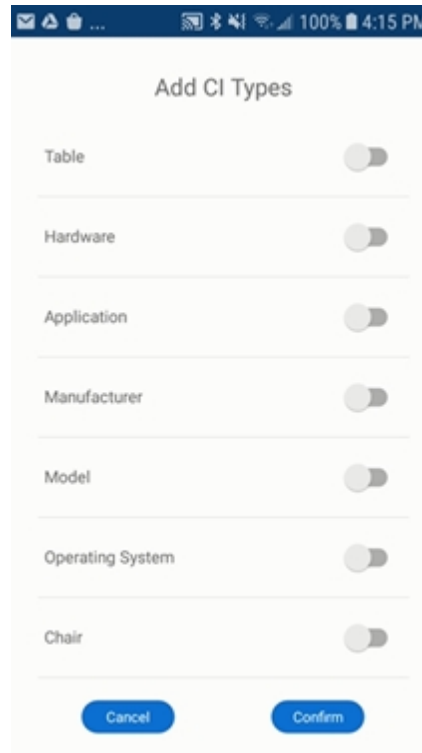


Figure 3b

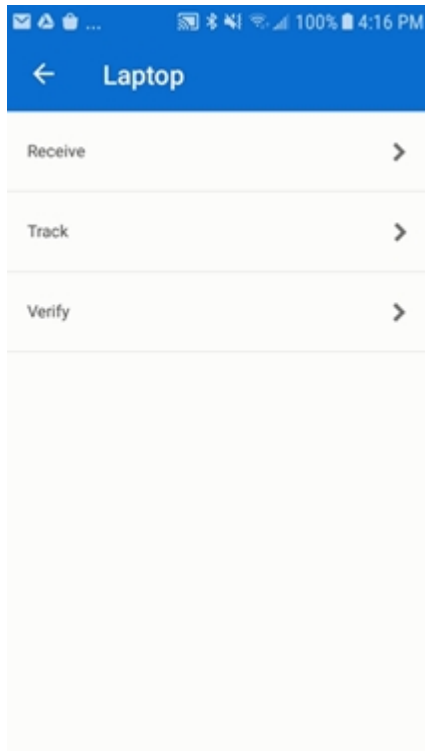


Figure 3c

There are three Workflows available for each CType selected in ScanStar. Drilling down into a CType (Figure 3a) will display the three Workflows.

Scan Fields

ScanFields can be defined in this screen and can be accessed from the CMDB screen (Figure 2a). The barcode data can automatically be populated into these fields by scanning the bar code. Only fields common across CTypes configured in ScanStar (Figure 3a) are available to be added as Scan Fields.

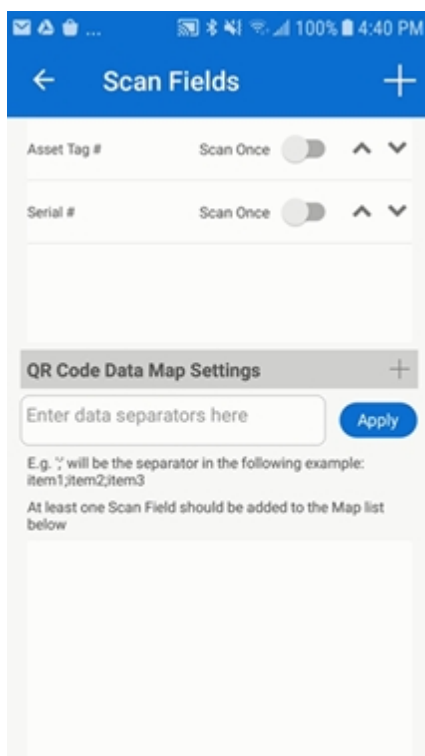


Figure 4

Scan Once: this flag property is applicable only to the Receive workflow and scans in a barcode into the field only once until cleared manually.

E.g.

1. Add a Location field to the Scan Field list in addition the two fields in Figure 4 with the Scan Once flag enabled.
2. Log into the application and navigate to the Receive workflow.
3. Scan three barcodes. This fills in the barcodes into Asset Tag #, Serial #, and Location fields.
4. The record is created in the CMDB and clears out only the Asset Tag # and Serial # and retains all other data on the screen including Location.
5. Now you need to scan only the Asset Tag # and Serial # for the next asset.

Note: This is useful only when wanting to scan once in Receive **and** be able to search on this field in the Track, Verify, and Audit workflow. Alternatively, tap on

the Location field label and scan in the barcode in the Receive workflow.

QR Code Data Map Settings

This section is applicable to scanning a QR Code that contains information that needs to be parsed and mapped into required fields in the Receive workflow.

For e.g. if the QR Code contains the following data: **'123456,Dell,Optiplex'** that needs to be parsed and mapped into the fields as follows Serial # = 123456, Manufacturer = Dell, Model = Optiplex. It can be achieved with steps below.

1. Enter the character ',' in the 'Enter data separators here' field in Figure 4 and tap on the 'Apply' button. This is the comma delimiter in the QR Code data in the example above.
2. Tap on the + icon next to the 'QR Code Data Map Settings' and select 'Serial #', 'Manufacturer', and 'Model' fields from the fields list and 'Confirm'. Make sure the fields are listed in the same order i.e.

Serial #

Manufacturer

Model

When the QR Code is scanned workflows other than Receive, the app searches for assets on all the mapped fields that are also listed as Scan Fields. In case of this example above it will be the data for the 'Serial #'. which is '123456'.

Fields

This screen can be accessed from the Workflows screen seen in [Figure 3c](#). CType fields can be added to each of the three Workflows (Receive, Track, and Verify). The field properties can be modified in the 'Modify Field Properties' dialog as in Figure 5c.

id ^ v >

Name ^ v >

Asset Tag # ^ v >

Serial # ^ v >

Manufacturer ^ v >

Model ^ v >

SS_Status ^ v >

Location ^ v >

Figure 5a

Add Workflow Form Field

AuditDate ☐

Brand ☐

Check In Date ☐

Check Out Date ☐

CheckBox ☐

Child ☐

Comment ☐

Cancel Confirm

Figure 5b

Modify Field Properties

Name

Label

Header

Default Value

Persist Default ☐

Required ☒

Read Only ☐

Hidden ☐

Parent Field

Cancel Ok

Location ^ v >

Figure 5c

Name - Name of the CMDB CType field

Label - field text to be displayed in the Workflow form

Header - text to group fields. Displays the header above the field where it is specified.

Default Value - auto populates the field with text/expression specified here.

Supported expressions:

- **{Field Name}**: A value from other fields on the form can be populated with this expression:
- **{Date}**: current date expression
- **{DateTime}**: current date and time expression

Required - This property setting is the one from the CMDB by default and can be overridden

ReadOnly - sets the field to be non-editable when enabled

Hidden - hides the field on the form when enabled

Audit Properties

You can edit the Audit properties by selecting Audit to display the 'Update Audit Properties' dialog as shown in Figure 6b.

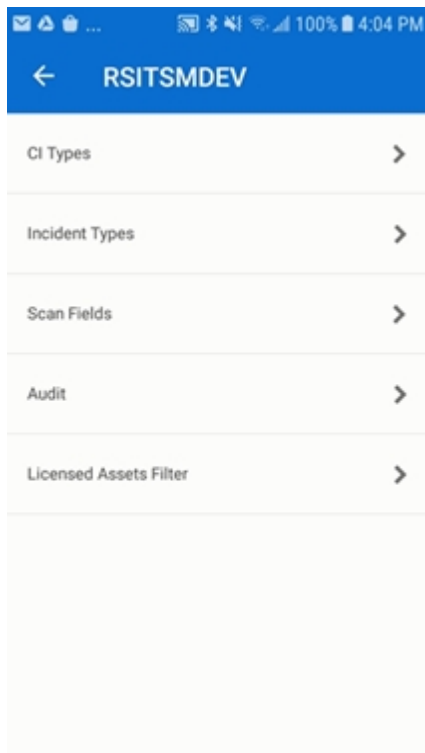


Figure 6a

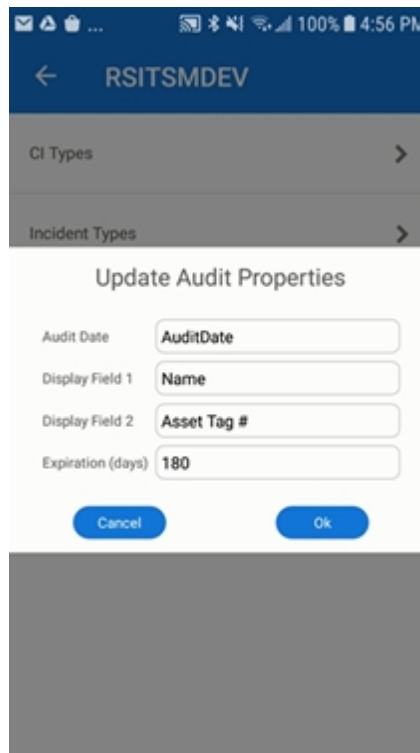


Figure 6b - Audit

Audit Date - A CITYPE date-time field in the CMDB that is used to track audited assets.

Display Field 1 - Name of the field for which the field value is to be displayed as main text for each asset in the Audit screen list.

Display Field 2 - Name of the field for which the field value is to be displayed as sub text for each asset in the Audit screen list.

Expiration (days) - Number of days the current audit is shown as audited in the Audit workflow.

Licensed Asset Filter

By default all the assets for the [CI Types](#) configured in ScanStar count toward the ScanStar license. The asset count can be further limited by specifying a valid filter for the CMDB provider. Please refer to [provider specific](#) documentation for sample filters.

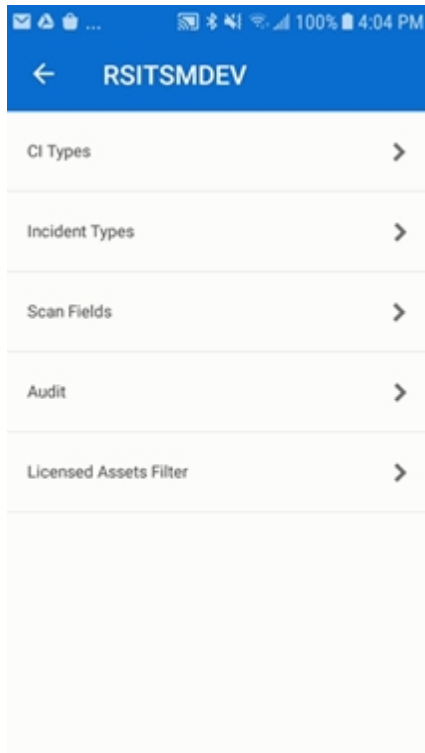


Figure 7a

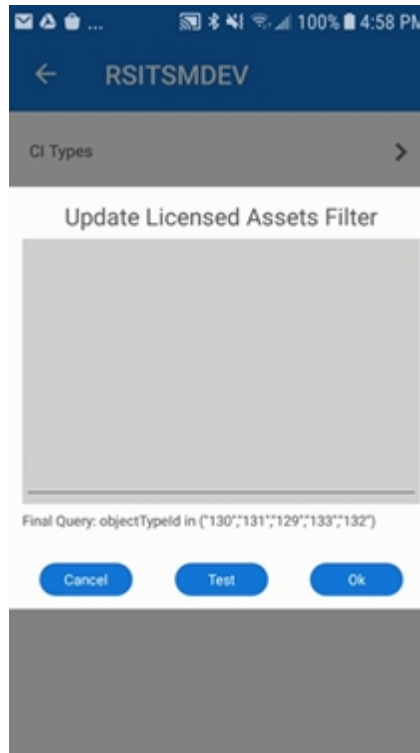




Figure 7b - Licensed Asset Filter

Incident Types

This configuration allows defining which ITSM Incident Types and fields are to be used with ScanStar. The Incident Types screen can be accessed from the CMDB screen seen in Figure 2a. The required Incident

Types from your ITSM provider can be associated with ScanStar in Figure 6a by tapping  icon, selecting the types, and confirming. You are prompted to select the ITSM, the first time you add an Incident Type. The fields/attributes for each type can be viewed in Figure 6b by tapping the Incident Type in Figure 6a. The fields for the selected type can be added by tapping the  icon in Figure 6b, selecting the fields, and confirming.

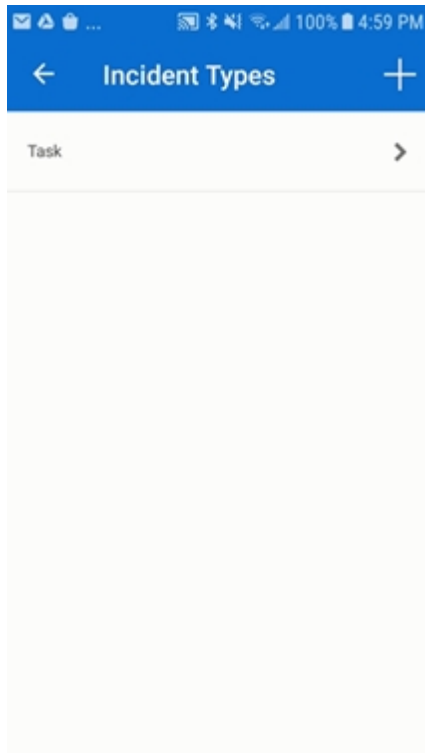


Figure 8a

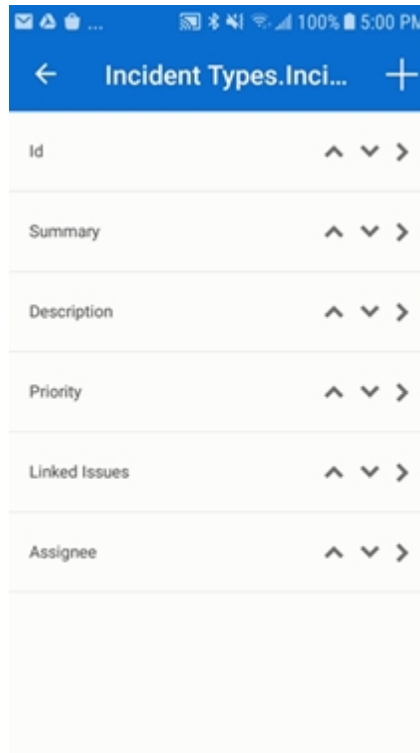


Figure 8b

Using ScanStar

Overview

To understand the power of ScanStar workflows, it is important that you read this brief user guide and run through each demonstration scenario using the examples provided.

This document will cover all four ScanStar workflows. It will serve to guide the user through the trial application by way of common use scenarios. Users should follow the instructions in each scenario carefully for a complete understanding of the application.

Terminology

- **Workflow:** Previously known as a “Module” in ScanStar for Windows Mobile, a workflow is simply a process in ScanStar to address common use cases.
- **Session:** A session is defined as a contiguous set of actions inside of a Workflow. A session begins when you enter the Workflow and ends when you exit.
- **Scanner:** For the purposes of this document, a scanner is synonymous with an Android-based smartphone capable of running ScanStar.

Prerequisites

- One smartphone running the Android operating system v4.4 API level 19 or higher. Also referred to as “the scanner” in this document.
- Barcode tags. Sample barcodes are provided [here](#).

Scenarios Summary

Using the [Receiving](#) workflow, several assets will be created to work with throughout the demonstration. The [Tracking](#) workflow will be used to move those items to the staging area. The [Verify](#) workflow will be used to deploy some of the items. The [Audit](#) workflow will be used to perform an audit of items in a facility.

Setup

You may wish to use your own 1D barcodes or print the sample barcode sheets which are provided [here](#).

Installation

Please contact [RightStar](#).

Notes

ScanStar is capable of scanning 1D and 2D barcodes including QR Codes.

The Interface

An explanation of each major component of the user interface is outlined below using the Receive Workflow screen as an example.

Action Bar



The action bar, on the top of each screen, is used for navigation throughout the application. From left to right, the icons provide the following functionality:

- Workflow indicator and back button. Shows the currently selected Workflow. Use this to return to the previous screen. Changes made to the current record will be saved.
- Photos button: The ability to view and/or add photos to the current record are located here.
- Menu button: Redundant access to the screens listed above. Future functionality will be placed here.

Data View

Name	{Asset Tag #}--(Model)	
Scan Fields		
Asset Tag #	<input type="text"/>	
Serial #	<input type="text"/>	
Asset Information		
Manufacturer	<input type="text"/>	>
Model	<input type="text"/>	>
Status	<input type="text"/>	
Location	<input type="text"/>	>
Assigned To	<input type="text"/>	
Warranty Expiration	<input type="text"/>	

The Data View contains the basic attributes defined for each Workflow in the [configuration](#) section.

The required fields are marked with red star next to the field.

Selecting a field referencing an object presents a pick list.

Selecting a date time field presents a calendar to pick a date.

Scan Field



A [Scan Field](#) is where the bar code data is stored with a bar code icon next to it. The current field to be scanned in is indicated with a blue border.

Scan Once Option



Users can optionally scan barcode data into any applicable field they wish to including that are not configured as scan fields. Tap once on the label for the field they wish to scan in a barcode. The label color changes to green. Now the related field is ready to receive the scanned barcode. The field label is reset to default once the barcode data is received into the field.

Signature Pad



A signature pad appears below the data view and can be scrolled into if hidden. A signature can be added just like editing any other field in the data view and saved along with the CI record. Signature is not supported for Footprints 12 and BMC Client Management providers at this time due to API limitation.

Scan Button



The Scan Button is used to invoke the camera view port as shown in the figure below and enable the ability to capture bar code data. The button text will change to "Stop" once the view port is enabled.

Point the view port at a bar code to scan in the data into the applicable scan field.

The Save button can be used on demand. By default the current record is saved automatically when all the bar code fields have been populated. After saving, the bar code fields are cleared but retains the remaining data preparing the data view for the next asset to be scanned.

The Clear button resets the form by clearing the data in the fields.

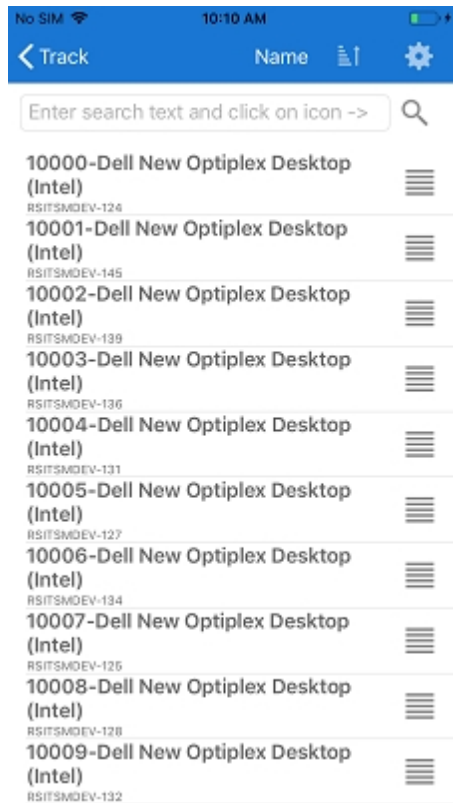
Info Bar

The Info Bar contains information about the current operation as well as additional functionality available for the currently selected Workflow.

The **CIType Type** is drop down containing the list of [configured](#) CTypes. Selecting a CType from the drop down displays the associated fields in the data view.

Users can do a quick find of an asset by entering a bar code value like Asset Tag or Serial Number in the Last Scan field and tapping the search icon.

Tapping the **search** icon when the 'Last Scan' is empty presents a pick list shown below with the assets for the ScanStar configured CTypes. This is applicable only to the Track and Verify workflows.



Attachments



This is the Tool Bar which appears on the Photos screen.

Attachment can be added to an asset by clicking the photo icon and selecting an image / document. This is applicable only if the CMDB provider supports attachments via the API.

Workflows

There are primarily four Workflows Receive, Track, Verify, and Audit to work with when a user logs into the application. Each of the Workflows is explained in detail in the subsequent topics.

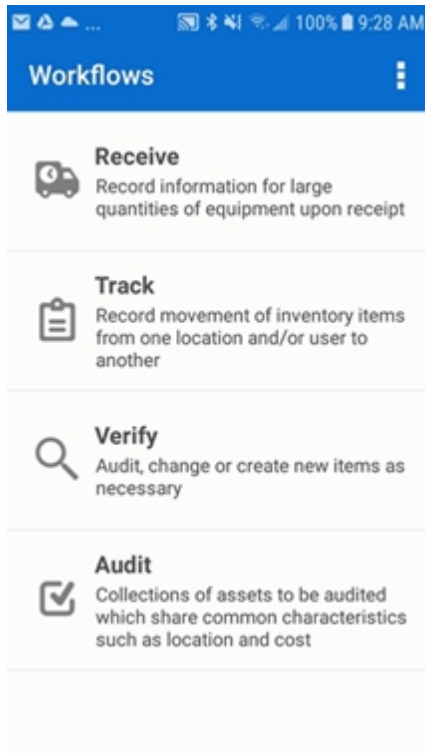


Figure 1

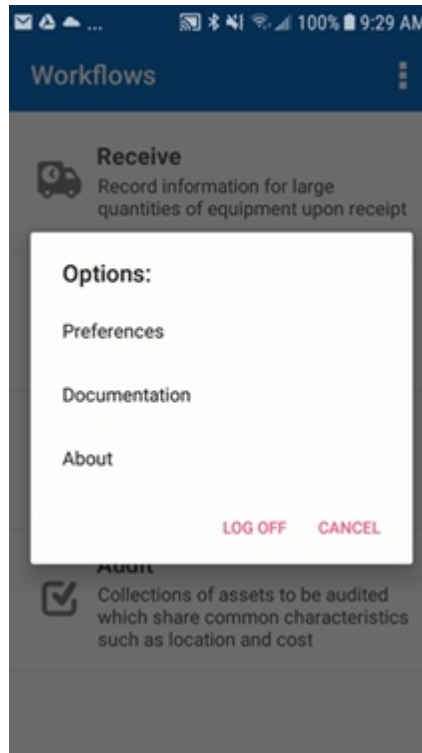


Figure 2



Figure 3

Users can access the Preferences, Documentation, About, or Log Off by selecting the  icon.

Receive

The organization receives most IT and Facilities inventory for company use through its warehouse. In the past, warehouse receiving personnel noted the receipts on company forms, and entered this data into Microsoft Excel later in order to keep a count of items available for distribution. Recordation of a typical shipment would usually take four to six hours.

With the implementation of ScanStar, the amount of time necessary to record large receipts has been drastically reduced. Now, receiving personnel simply scan each item received, recording important information about each shipment, the assets are automatically created, and the date and location of receipt is recorded in the system.

The use of barcode scanning technology which interfaces directly with the Asset Management system has reduced the time needed for data entry to less than an hour under the same circumstances.

Demonstration

A new shipment has arrived at the receiving dock; three laptops with docking stations have been delivered from Dell.

1. Log into ScanStar and select the Receiving workflow
2. First receive the laptops. Fill fields with data which is common to the items on the order:
 - Manufacturer: **Dell**
 - Model: **{Laptop or Docking Station}**
 - Lifecycle Status: **Received**
 - Received Date: **{current date/time}**
 - Purchase/Lease Cost: **{as appropriate for the items received}**
 - Building: **HQ**
 - Room: **Warehouse**
 - Organization: **RightStar Systems**
 - Location: **Receiving Dock**
 - Select the back button to return to the main Receiving screen

3. Using the sample barcode sheet, begin scanning by tapping the “Scan” button. Scan the first barcode which represents the first scan field then scan the next barcode which represents the subsequent scan field if any. Notice how after all the scan fields are populated, the record is complete and the next scan will create a new record and save the previous record. This continues for each laptop on the order.
4. Select the Stop Scanning button when you have finished scanning the first sheet of tags.
5. Repeat actions in the previous step for the docking stations, changing the model and cost prior to scanning the second sheet.
6. Return to the main menu by tapping the back button in the app or on the device.

Track

The organization's IT staff is tasked with configuration and delivery/movement of IT assets throughout the enterprise. Numerous items are distributed or recalled for repair or retirement throughout the organization on a daily basis.

Detailed records are desired to ensure accurate reporting of asset movement and assignment to the organization's employees. The ScanStar Tracking workflow allows staff to pre-fill the location, ownership, and status information then simply scan all items participating in the action (move, reallocate, etc.). The time needed to record data for multiple asset transactions is greatly reduced and the accuracy is significantly increased with the use of ScanStar asset tracking.

When the user selects this workflow, the common fields across all ScanStar configured CI Types are listed by default. This can be optionally turned off in the [Advanced Settings](#) to let the user pick a CI Type like the Receive and Verify workflows.

Demonstration

The items just received must be moved to the staging area in preparation for deployment within the organization. The assets are temporarily assigned to you – the person performing the work. The location assignment is recorded and a photo is also assigned to each piece of equipment.

Move items to the Staging area

1. Log into ScanStar and select the Tracking workflow
2. Fill fields with data which is common to the items to be deployed, including:
 - Location: **Staging**
 - Status: **Staged**
 - Asset Owner: *{User which is currently logged in to ScanStar}*
 - Notice how the new (updated) information for each item is highlighted in red. The modified data is persistent for the session until user exits the workflow.
3. Add a photo for each model to be scanned:
 - Select the Photos button on the Action Bar.
 - Select the Add Photo button on the Info Bar.
 - Choose a photo representing the model you are about to scan from the available photos on the screen. You have the option of selecting images that are stored on the scanner or from a shared, online Google Drive.
 - Note that the first photo selected is the “default” photo. To add additional photos for an asset, repeat the actions of the previous step.
4. Return to the Tracking Workflow by selecting the Back button
5. Scan either the Asset Tag or Serial Number of each of the items previously received. The information provided (attribute values and image) will be applied to the scanned item.
6. Repeat these steps for each model, changing attribute values and images as appropriate for the assets to be scanned.
7. Return to the main menu by tapping the Back button in the app or on the device.

Verify

The IT staff at ABC, Inc. spend many hours in the field deploying new assets, moving or reassigning equipment, and collecting items in need of repair or disposal.

These processes require the recordation of each change to the asset's user, location, status, and other important attribute values.

In the past, they manually recorded the asset information and then spent hours transcribing the collected data into the CMDB. The transcription process included verifying whether the asset existed in the CMDB. If it did, the staff member verified that the asset characteristics were correct before updating. If the asset did not exist, a new Inventory Item record was created in the CMDB.

With the implementation of ScanStar, the process is greatly simplified via ScanStar's Asset Verification workflow. Each asset's barcode label is scanned and a description of the asset, its owner/assignee, location, and any other pertinent information that has been configured for the workflow is displayed on the scanner's screen. If the information is correct, no action is necessary as a record of this verification is logged. Incorrect information can be changed in the field or, if the asset is not found in inventory, the asset data can be entered on the scanner and a new record is created.

Demonstration

You have been tasked with deploying a new Laptop and Workstation to Mary in accounting then pick up her old equipment from the satellite office downtown.

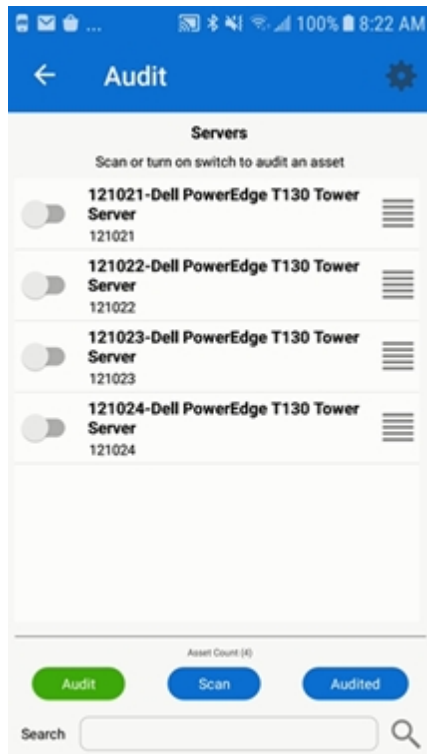
Deploy and pickup equipment

You have arrived at the 6th Street office and will record the deployment and retrieval of equipment for Mary:

1. Select the Verify workflow
2. Scan either tag on the new laptop you are issuing. Select "Stop Scanning" and note the information about its previous location and assignee. Update attribute values to reflect its new status:
 - Lifecycle Status: **Deployed**
 - Building: **Walker Building**
 - Room: **Office 11A**
 - Floor: **1st**
 - Asset User: **Mary Smith**
 - And on the details screen...
 - Location: **User's Desk**
 - Department: **Accounting**
3. Select the new location and save the changes.
4. Repeat these steps to deploy a Laptop Docking Station and to pick up items for return.
5. Return to the main menu by tapping the back button in the app or on the device.

Audit

Field Audit



Prior to implementing ScanStar, IT resources were required to physically verify all of the IT related assets exceeding a specific value. This process required the dedicated effort of the entire IT staff for an extended period of time each year. They manually recorded the asset information and then spent hours reconciling the collected data with the CMDB.

With the implementation of ScanStar, the process is greatly simplified. ScanStar provides [Audit Sets](#) – collections of assets to be audited which share common characteristics such as location and cost. ScanStar allows the user to create and edit their own [Audit Sets](#). Users can pick or add new [Audit Sets](#) by selecting the setting icon on the top right corner of the screen.

By default the Audit button is selected and lists the assets to be audited for the selected Audit Set. Tapping on the Audited button lists the assets that have been audited for the selected Audit Set. Users can manually search on configured [Scan Fields](#) or the [Audit Display Fields](#) for the selected Audit Set.

Demonstration


In this case, since we created and assigned assets to the Warehouse earlier, we will create a new Audit Set and perform an audit against these:

1. Select the Audit workflow
2. Select the settings icon from the Action Bar
3. Note that one or more Audit Sets may already exist.
4. Create a new Audit Set by selecting the Add icon on the Action Bar
5. Use the following values for the new Audit Set:
 - Audit Set Name: **Warehouse Audit**
 - Filter: **Building='HQ' and Room='Warehouse'**
 - Default: **check this box**
 - Select OK
6. Now select this new Audit Set from the list
7. Notice the list of assets that were not deployed in the previous scenarios
8. To perform the audit and mark assets as found you can tap the check-box on any of the records shown or scan either the asset or serial number tag.
9. Audit a few items but leave a few unchecked.
10. Return to the Audit workflow and confirm that your audit results are consistent with your previous action

Note:

- User will have to manually audit assets in case of multiple assets found for a barcode scan. E.g. scanning a location barcode could bring up multiple assets and will not be automatically audited. User will have manually turn on the switch for each to audit.

Audit Sets

Users can pick, add, edit, and delete Audit Set from the Audit Sets screen. Selecting the  icon prompts a dialog as shown in Figure 2 to add a new Audit Set.

Android OS: Long click on a Audit Set in the list in Figure 1 to edit or delete an Audit Set.

iOS: Slide the Audit Set to the left in Figure 1 to edit or delete an Audit Set.

Selecting an Audit Set from the list in Figure 1 executes it and lists the CIs in the Audit screen.

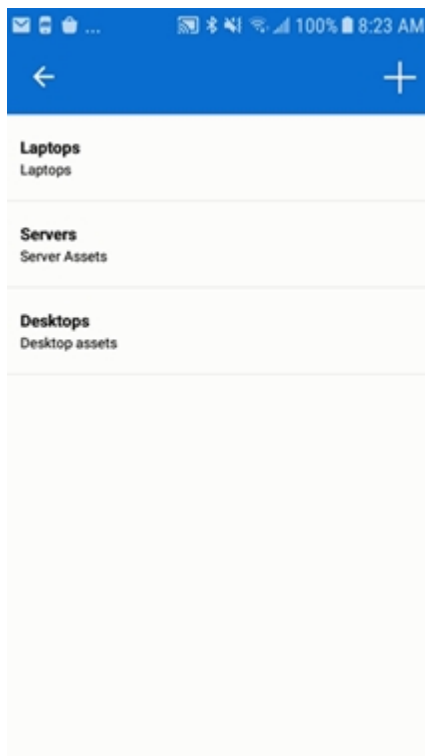


Figure 1

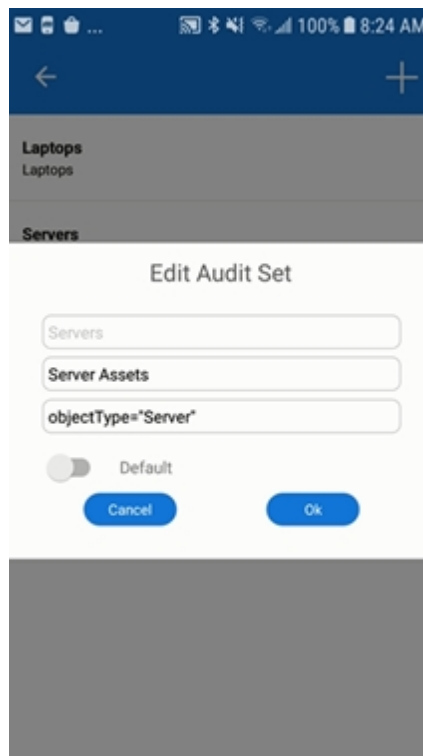


Figure 2

Audit Set Name: Name of Audit Set

Description: Brief description

Filter: criteria to limit the number CIs to audit. Please refer to CMDB [provider specific](#) documentation for appropriate syntax.

Default: executes the Audit Set by default in the Audit screen when this option is enabled.

Note: some of the filters may require a single quote in the query string like in the Figure 2. Apple has introduced smart punctuation in iOS 11 and up that replaces the standard punctuations and does not work when used in these audit set filters. Disable this option as follows: Settings -> General -> Keyboard -> Smart punctuation

Incidents

The IT technicians spend many hours in the field servicing assets.

This process requires the recording changes to the asset and related service desk incident tickets. In the past, this information was manually recorded and then spent hours transcribing the collected data into the CMDB and ITSM service desk.

With the implementation of this feature, the process is greatly simplified via ScanStar's Incident creation and update feature available in the Track and Verify workflows. Each asset's barcode label is scanned and the asset information that has been configured for the workflow is displayed on the scanner's screen. Technician can then view linked Incidents by selecting the 'Linked Incidents' menu item, select the applicable Incident, make changes, and update the ticket. The technician can also optionally create a new Incident if there is no applicable one found for the asset. The scanned asset can also be update as required.

Demonstration

You have been tasked with servicing Mary's Laptop in accounting.

Service and update asset related information

You have arrived at the 6th Street office and will record the service information for Mary's laptop upon completion:

1. Select the Verify workflow
2. Scan either tag on the new laptop you are issuing. Select "Stop Scanning" and note the information.
3. Select the menu with the three dots on the top right corner and select 'Linked Incidents'. Select 'Create Incident' if no 'Linked Incidents' found.
4. Update the Incident with required changes. E.g. notes on what was done to resolve the issue and change the status to 'Resolved'.
5. Save changes and return to Verify workflow screen.
6. Update asset information if required. E.g. change status from 'In Repair' to 'In Use'.

Note: This feature is only supported for the Insight CMDB provider at this time.

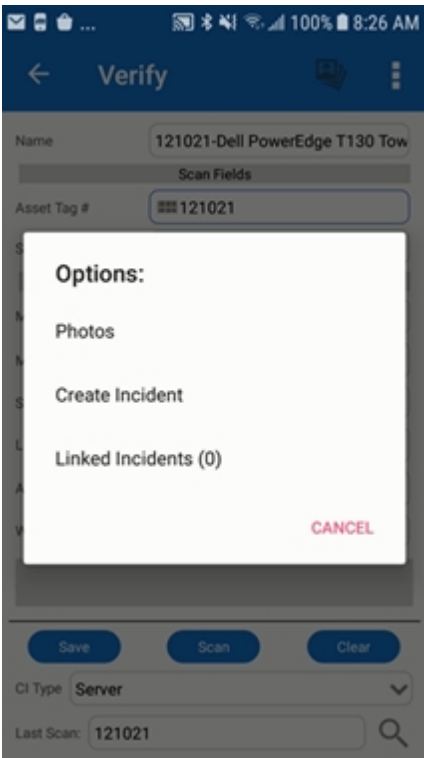


Figure 1

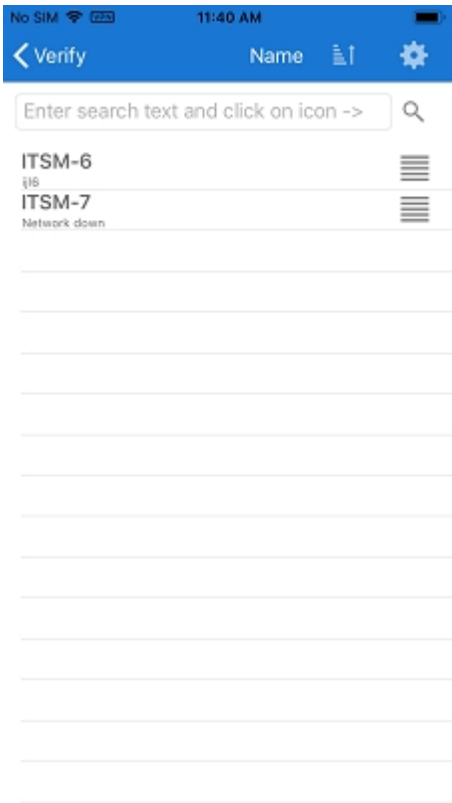


Figure 2 Linked Incidents

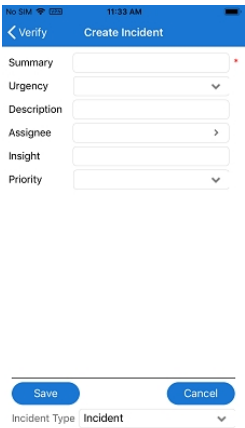


Figure 3

Provider Specific

Atlassian Jira

This page contains all Jira specific integration information.

Sign In

Preferences

User: user1

Password: ••••••••

Url: user1.atlassian.net

CMDB Provider: Jira

Remember Credentials: ☒

CMDB: RS ITSM

Scan View (%): 40

Login

User: Jira user

Password: Jira user password

Url: Jira rest url

Cloud version: http://{accountname}

On premise version: http://{servername:port}

CMDB Provider: Jira

Figure 1

Audit Sets

This section explains how to configure filters that works with Atlassian's Jira

Audit

Desktops
Desktop assets

Laptops
Laptop Assets

Add Audit Set

Audit Set Name

Description

Filter (sql style: e.g. Building='B1')

☐ Default

Cancel Ok

Filter: any where clause applicable to Atlassian's Jira [JQL](#) is supported here. Query on any Jira or custom field.

Here are a few examples

Filter	Description
issuetype = "Desktop"	List desktop assets in Jira
status = "Deployed"	List assets that have been deployed

Figure 2

Naming Convention

Each CMDB provider has unique naming convention. Since ScanStar provides a common solution to each of these providers, it has proprietary terminology that closely aligns with ITAM. Following is the mapping between ScanStar and Jira

ScanStar	Jira
CMDB	Project
CIType	IssueType
Field	Attribute
CI (configuration item)	Issue
Picklist	User pick list

Riada Insight

This page contains all Insight specific integration information.

Sign In

The 'Preferences' screen displays the following fields and settings:

- User: user
- Password: [masked]
- Remember Me: ☒
- CMDB Provider: Insight
- Url: http://company.cmdb.com
- CMDB: RSITSMDEV
- Advanced Settings: [button]
- Login: [button]

Figure 1

The 'Advance Settings' screen displays the following options:

- Scan View (%): 40
- Language: [dropdown]
- Signature: ☒
- Auto Save in Receive: ☒
- Receive: ☒
- Track: ☒
- Verify: ☒
- Audit: ☒
- Create Reference Objects: ☒
- Confirm On Scan: ☒
- Show Common Track Fields: ☒
- Jira Date Format: d/MMM/yy
- Jira DateTime Format: d/MMM/yy h:mm a
- Insight Version: 8+

Figure 2

User: Jira user

Password: Jira user password

Url: Insight rest api url - http://{servername:port}
Note: use https:// if applicable

CMDB Provider: Insight

CMDB: Insight object schema

Jira Date Format: enter the value of *jira.date.picker.java.format* found in the following path in Jira: Jira -> System -> General Configuration -> Advanced Configuration

Jira DateTime Format: enter the value of *jira.date.time.picker.java.format* found in the following path in Jira: Jira -> System -> General Configuration -> Advanced Configuration

Insight Version: enter '8+' if 8 and above else the full version (6.4.6) of Insight.

Picklist

Assets

The object picklist on the Track and Verify workflows can be accessed by tapping on the magnifying glass icon in the bottom right of the screen. The pick-list can be sorted only on the 'Name' attribute at this time.

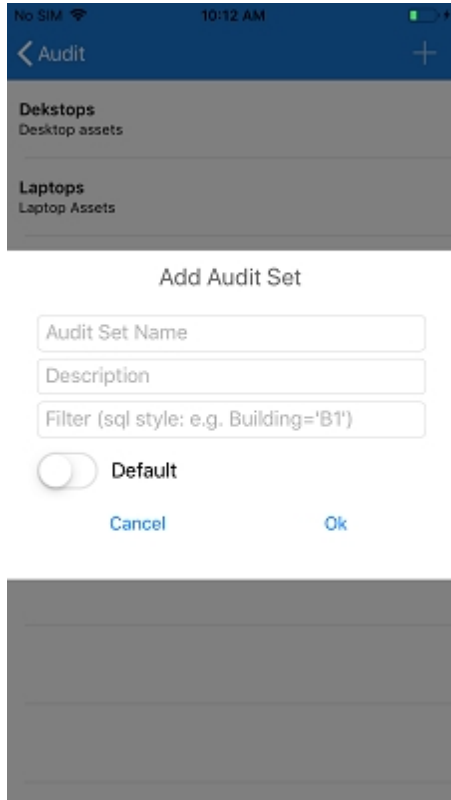
Reference attributes

Users can pick data for reference attributes from related object type list. The object picklist on the Receive, Track and Verify workflows can be accessed by tapping on the right arrow icon for the attribute. The picklist

can be sorted and searched on any attribute that is selected from the attribute list accessed via the cog wheel. The picklist also honors the filter objects configured in Insight.

Audit Sets

This section explains how to configure filters that works with Riada Insight



Filter: any where clause applicable to Riada Insight [IQL](#) is supported here. The field name is the name of the CI Type (objectType) attribute. The attribute should be available in all CI Types configured in ScanStar.

Here are a few examples

Filter	Description
objectType="Desktop"	List assets of objectType Desktop
Location="Dallas, TX"	List assets assigned to the 'Dallas, TX' location
objectType="Desktop" AND Status="Open"	List Desktop assets with Open Status

Figure 2

Naming Convention

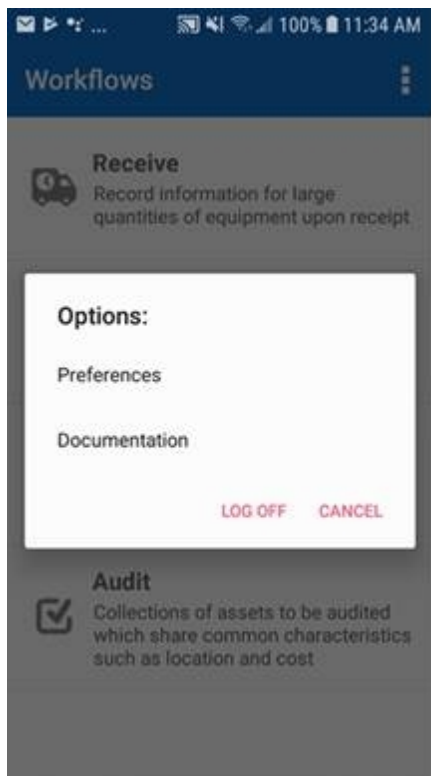
Each CMDB provider has unique naming convention. Since ScanStar provides a common solution to each of these providers, it has its proprietary naming that closely aligns with ITAM. Following is the mapping between ScanStar and Insight

ScanStar	Insight
CMDB	Schema
CIType	ObjectType
Field	Attribute
CI (configuration item)	Object
Picklist	Reference object list

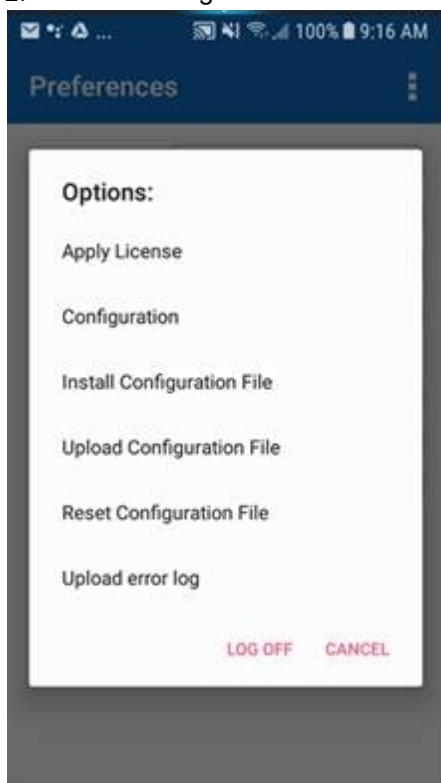
Using Insight Object QR Code to Track Assets

The app has a built in configuration feature that enables reading the object key from the Insight object's QR Code. Here are the steps to get it to work.

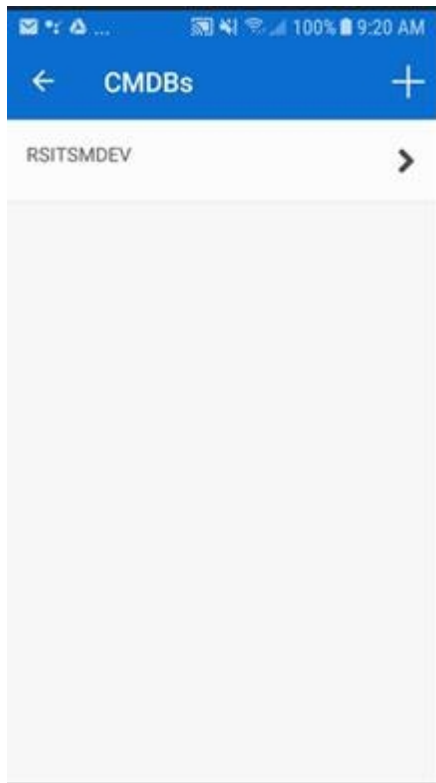
1. Log into the app and select 'Preferences' from the Workflows menu



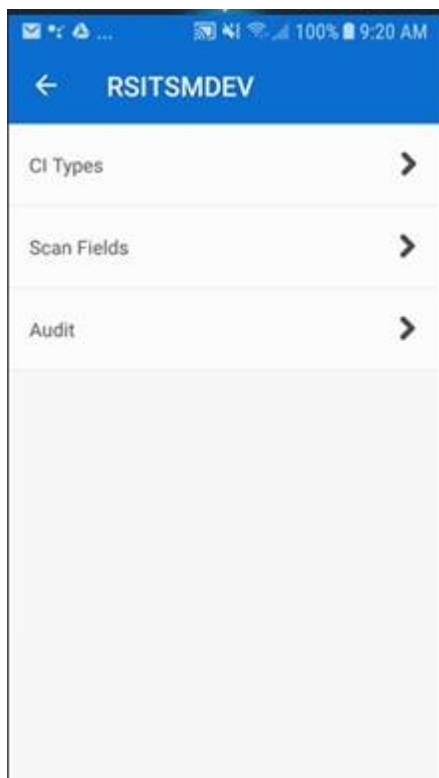
2. Select 'Configuration' from the menu



3. Select the object schema



4. Select 'Scan Fields'



5. Follow the steps below

- a. Add the 'Key' attribute under 'Scan Fields'
- b. Enter '=' in the field under 'QR Code Data Map Settings' and tap on the 'Apply' button
- c. Add the 'Key' attribute under the 'QR Code Data Map Settings' by selecting the + next to it
- d. Add the 'Ignore this item' attribute under the 'QR Code Data Map Settings' by selecting the + next to it

- e. Move up 'Ignore this item'
- f. The screen should look like as below



- 6. Login back into the app.
- 7. Select the 'Verify' workflow
- 8. Scan the QR Code for an existing object in Insight. The screen should be populated with the object data.

Linking Jira Issue(s) with Insight Object

One or more Jira issues can be linked with an Insight object with the [Incident](#) feature in ScanStar. Here are the steps to configure this feature.

1. Log into Jira and create a [custom field](#) of Insight object type if one doesn't exist already. Make sure the custom field is added to the appropriate service desk screen. See documentation [here](#).
2. In ScanStar, configure and enable the Incident feature by following the instruction [here](#). Make sure to add the Insight custom field created in step 1 to the ScanStar Incident form.
3. Edit the Insight custom field added to ScanStar Incident form in step 2 by tapping on it.
4. The 'Modify Field Properties' dialog should be displayed.
5. Enter **{IncidentLink}** in the 'Default Value' property and tap the 'Ok' button.
6. This completes the configuration
7. Login back into the app, select the 'Verify' workflow and use the feature as described [here](#).

BMC FootPrints Service Core v12

This page contains all Footprints 12 specific integration information.

Note: Only Footprints 12 running against a Microsoft SQL Server 2008 or higher database is supported at this time.

Preferences

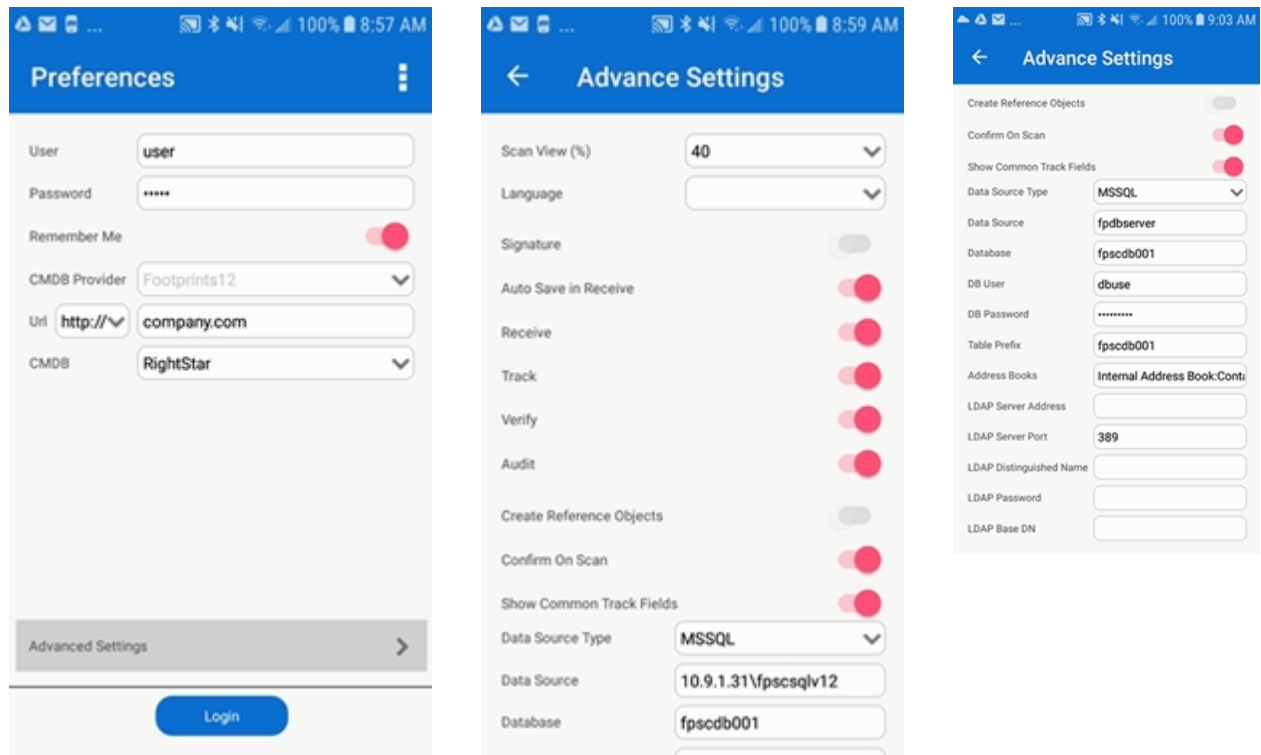


Figure 1

Note: for the security of your Footprints data, it is recommended to use a '**Database User**' only with the following minimum rights.

1. A database login with Footprints database (e.g. fpscdb001 in Figure 1) as the default database and default schema as **{Table Prefix}_system**. Where **{Table Prefix}** is the value from Figure 1. The login should be mapped only to the Footprints database.
2. Add the following schema to the Footprints Securables list (database properties) with specified permissions

Table Name	Select	Insert	Update	Delete	Comments
{Table Prefix}_cmdb_xxx	Yes	Yes	Yes	Yes	all CMDB tables configured in ScanStar
{Table Prefix}_ab_xxx	Yes				all address books to be used in ScanStar
{Table Prefix}_content_repository	Yes				
{Table Prefix}_system	Yes				

Naming Convention

Each CMDB provider has unique naming convention. Since ScanStar provides a common solution to each of these providers, it has its proprietary naming that closely aligns with ITAM. Following is the mapping between ScanStar and Footprints 12

ScanStar	Footprints 12
CMDB	CMDB
CIType	CI Type
Field	Attribute
CI (configuration item)	CI

Picklist

Few of the properties for the CI picklist in workflows Track and Verify can be configured for each of the CMDB as shown in Figure 2. This screen can be accessed from the Preference's Configuration menu and then selecting a CMDB. .

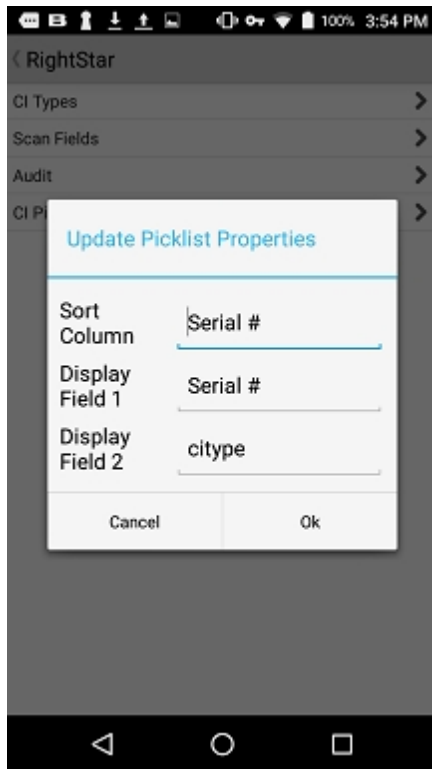


Figure 2

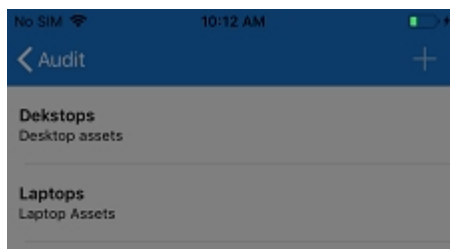
Sort Column: Default sort column. Can be only either of the display fields.

Display Field 1: Field to be displayed as the main text for each CI in the picklist

Display Field 2: Field to be displayed as the sub text for each CI in the picklist

Audit Sets

This section explains how to configure a filter that works with Footprints 12



Add Audit Set

Audit Set Name

Description

Filter (sql style: e.g. Building='B1')

☐ Default

Cancel Ok

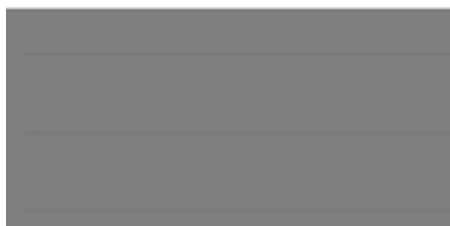


Figure 3

Filter: any where clause applicable to Microsoft SQL Server database is supported here. The field name is the nice name of the CI Type attribute and should be enclosed in square brackets. The attribute should be available in all CI Types configured in ScanStar.

E.g.

[Location] = 'New York' and [Building] = 'HQ'

BMC Remedyforce Service Desk

This page contains all Remedyforce specific integration information. ScanStar integrates with Remedyforce with the Salesforce Rest API that uses OAuth 2.0 to authenticate the client. A new salesforce connected app is required that provides the Client Id and Client Secret to be able to authenticate and obtain a session token that is used to establish subsequent communication between ScanStar and Remedyforce. See instructions [below](#) on how to create a connected app.

Sign In

Figure 1 shows the 'Preferences' screen. It includes input fields for 'User' (user@company.com), 'Password' (masked with **), 'Remember Me' (checked), 'CMDB Provider' (RemedyForce), 'Url' (https://naxxx.salesforce.com), and 'CMDB' (RemedyForce CMDB). At the bottom, there is a 'Login' button and an 'Advanced Settings' button with a right arrow.

Figure 1

Figure 2 shows the 'Advance Settings' screen. It features several toggle switches: 'Signature', 'Auto Save in Receive', 'Receive', 'Track', 'Verify', 'Audit', 'Confirm On Scan', and 'Show Common Track Fields'. Below these are input fields for 'Security Token', 'Client Id', 'Client Secret', and 'Class Filter'. The 'Class Filter' field contains a red text snippet of a SOQL query.

Figure 2

User: Salesforce username

Password: Salesforce username password

Url: Salesforce url to the login console. E.g. - <https://xxx.salesforce.com>

CMDB Provider: Remedyforce

CMDB: Defaults to 'Remedyforce CMDB' once the ScanStar configuration file is installed or configured in the app.

Security Token: Salesforce user security token if the instance is not white listed

Client Id: Client Id for the connected app created in Salesforce

Client Secret: Client Secret for the connected app created in Salesforce

Class Filter: SOQL criteria used in CMDB Class field picklist for Receive, Track, and Verify workflows. Overrides default filter.

Default Filter:

```
BMCServiceDesk__CMDBClassType__c IN ('CI and Asset','Asset') or BMCServiceDesk__Class__c='BMC_Computer System'
```

Model Picklist

The Model attribute picklist on any of the workflows (Receive, Track, and Verify) is designed to only display records for the Computer System and selected Class. For e.g. if user selects the Laptop class and then opens the Model picklist to select one, the picklist displays only Computer System and Laptop models to pick from. Users will not be able to pick a Model if the CMDB Class field is empty. If you do not see the applicable models in the picklist, set the 'Parent Field' property for the 'Model' field to CMDB_Class in the app's field configuration.

Steps to configure the 'Parent Field' property

1. Open the Preferences
2. Select the Configuration menu
3. Navigate to RemedyForce CMDB -> CI Types -> Base Element -> Receive
4. Make sure the CMDB_Class field is added to the field list
5. Now tap on the 'Model Name' field

6. Tap on the 'Parent Field' and select 'CMDB_Class'
7. Repeat 3 - 6 for the Track Verify workflows as well

Audit Sets

This section explains how to configure filters that works with Remedyforce

Filter: any where clause applicable to Remedyforce [SOQL](#) is supported here. The field name is the Remedyforce field **API** name from the Base Element object.

Here are a few examples

Filter	Description
BMCServiceDesk__PrimaryCapability__c in ('Desktop', 'Laptop')	List desktop and laptop assets
BMCServiceDesk__PrimaryClient__r.Name in ('Support', 'IT Ops')	List assets for specified primary clients
BMCServiceDesk__PrimaryCapability__c = 'Desktop' and BMCServiceDesk__Asset_Status__c = 'InProduction'	List desktop assets in production

Figure 2

Naming Convention

Each CMDB provider has unique naming convention. Since ScanStar provides a common solution to each of these providers, it has its proprietary naming that closely aligns with ITAM. Following is the mapping between ScanStar and Remedyforce

ScanStar	Insight
CMDB	CMDB
CIType	Class
Field	Attribute
CI (configuration item)	CI
Pick list	Lookups or Foreign Keys

Remedyforce Configuration

Salesforce user credentials

Please note that SSO is not supported with ScanStar this time. You will need a valid Salesforce user login to be able to use the app. If you are using SSO currently in your company to log into Remedyforce then follow the steps at this link: [Salesforce User Password Reset](#). You can then use the newly generated password for the user to log into ScanStar.

Salesforce Multi Factor Authentication

Follow the steps below if you have multi factor authentication enabled in Salesforce.

1. Have the High Assurance option turned off from the steps below.
 1. Enter the Setup option in Remedy
 2. In the quick find box type "Users"
 3. Open any Admin User by clicking on the name and then click on the profile name
 4. Scroll to Session Settings and find the Session security level required at login setting.
 5. Click Edit, and deselect High Assurance.
 6. Click Save
2. Follow the steps in the link [here](#). This enforces 2FA for browser login (desktop) and allows ScanStar to login. Make sure that the 'Two-Factor Authentication for API Logins' option is unchecked in 'Setup Tutorial: Step 1, Create a 2FA Permission Set' in the instructions.

Enabling IT Asset Management

ScanStar is a bar coding application and mostly deals with any physical inventory that can be tagged. ScanStar works best with IT Asset Management CIs In Remedyforce and it requires this option to be enabled. Here are the steps to enable the option.

1. In Remedyforce console navigate to the 'Remedyforce Administration' tab
2. Select 'Configure CMDB 2.0'
3. Select 'General CMDB Settings'
4. Check 'Enable IT Asset Management'

How to create a Connected App in Salesforce

Here are the steps to create a connected app in salesforce. Once created, the Client Id and Client Secret can be provided in the Figure 1 above to be able to login.

1. Login into Remedyforce console
2. Select 'Setup'
3. Select 'App' under the 'Build' section on the left navigator
4. Find the Connected Apps section and click New
5. Enter a unique Connected App name
6. Enter a contact email address
7. Check the 'Enable OAuth' settings under the 'API (Enable OAuth settings)' section
8. Enter a value in the Callback Url field: E.g. <https://login.salesforce.com/services/oauth2/callback>
9. Select the following options under the 'Selected OAuth Scopes'
 1. Access and manage your data (api)
 2. Provide access to your data via the Web (web)
 3. Perform requests on your behalf at any time (refresh_token, offline_access)
10. Save the changes

How to create a Public Group and add Users

A public group is required if your ScanStar license is based on number of users belonging to the specified group. Here is how to create the group and add users to it in salesforce.

1. Login into Remedyforce console
2. Select 'Setup'
3. Select 'Manage Users' under the 'Administer' section on the left navigator
4. Select 'Public Groups'
5. Click on the 'New' and follow instructions to create the new group
6. On the 'Public Groups' page, search for Users and add required users to the group.
7. Save and you are done

Linking Incidents with CI/Asset

One or more Incidents can be linked with a CI/Asset with the [Incident](#) feature in ScanStar. Here are the steps to configure this feature.

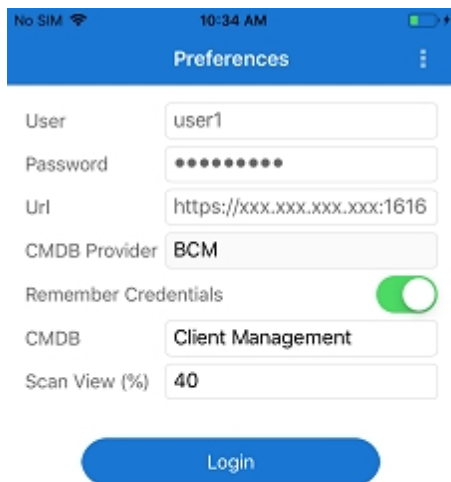
1. In ScanStar, configure and enable the Incident feature by following the instruction [here](#). This completes the configuration.
2. Login back into the app, select the 'Verify' workflow and use the feature as described [here](#).

BMC Client Management

This page contains all BMC Client Management (BCM) specific integration information. ScanStar works with BCM Devices and related object attributes for Financial Asset Management and Computer System.

Sign In

BCM specific information required to log into ScanStar.



The screenshot shows the 'Preferences' screen of the ScanStar application. At the top, there's a status bar with 'No SIM', signal strength, time '10:34 AM', and battery level. Below the title bar, there are several input fields: 'User' with 'user1', 'Password' with masked characters, 'Url' with 'https://xxx.xxx.xxx.xxx:1616', 'CMDB Provider' with 'BCM', 'Remember Credentials' with a green toggle switch, 'CMDB' with 'Client Management', and 'Scan View (%)' with '40'. A blue 'Login' button is positioned at the bottom center.

User ID: BCMuser

Password: BCMuser password

Url: http://{servername:port}

This is the BCM REST API url. The placeholder, {servername:port} should be replaced with appropriate DNS / IP and port. A sample is shown in Figure 1.

CMDB Provider: BCM

Device Group ID: BCM device group id to be used with ScanStar. Default is 'Device Groups' -> 'Out of the Box' -> '**All Devices**' with an id of **147**. For details, refer to 'Creating Device Group in BCM' section below.

Figure 1

Creating Device Group in BCM - Optional

By default, ScanStar uses the out of the box 'All Devices' group to count toward the ScanStar licensed devices. A custom query can be created and assigned to a custom group to limit the number of devices to be used with ScanStar. Here are the steps to create the custom query and group.

Log into the BCM console.

Create ScanStar Query

1. In the left navigation tree, right click on 'Queries' and select 'Create Query'.
2. Enter the Name as 'ScanStar', select Type as Device, and click Ok to create the query.
3. Select the newly created 'ScanStar' query and in the right pane select the 'Criteria' tab.
4. Add required criteria by right clicking in the empty space in the 'Criteria' tab and selecting 'Add Criterion'. Preview and test your query.
5. Go back to the 'Criteria' tab and change the 'Query Status:' to 'active'.

Add Query to Device Group

1. Right click on the 'ScanStar' query and select 'Create Device Group'.
2. Name it 'ScanStar' and click Ok.

Create Query to get ScanStar Device Group ID

1. In the left navigation tree, right click on 'Queries' and select 'Create Query'.
2. Enter the Name as 'Get ScanStar Device Group ID', select **Type** as '**Device Group**', and click Ok to create the query.
3. Select the newly created query and select the 'Criteria' tab in the right pane.
4. Right click in the empty space in the 'Criteria' tab and select 'Add Criterion'.
5. Select 'Name' from 'Available Criteria', set the 'Operator' as 'Is Not Null', and click the add icon (plus sign). Click Ok to finish adding criteria.
6. Preview to make sure it works.
7. Go back to the 'General' tab and double click on the 'Free Query' row and check the 'Free Query' check box. Click Ok.
8. Select the 'SQL' tab and replace the query with the following:

```
SELECT DISTINCT Groups.GroupName, Groups.GroupID FROM Groups WHERE
( (Groups.GroupName IS NOT NULL) ) AND GroupTypeID = 101 AND RootNode IS NULL AND
Groups.GroupName like 'ScanStar%' ORDER BY Groups.GroupName ASC
```
9. Verify the SQL syntax of the query
10. Test by previewing the query. Make sure to select 'Query Result By' equals 'SQL Result'

Updating the new Device Group ID in ScanStar (after installing and configuring the app)

1. Log into the ScanStar app on your device and navigate to the Preferences screen.
2. Update the 'Device Group ID' with value from step 11 under '**Create Query to get ScanStar Device Group ID**' section.
3. Login

Best Practices to use ScanStar with BCM

ScanStar is a convenient mobile asset tracking application that compliments the auto discovery software. However, if not implemented and used correctly, it could lead to creating duplicate records in the database causing a nightmare to maintain the assets and beat the purpose of using these software. Here are our recommended practices for various scenarios.

Create new assets in the BCM database from ScanStar

Many customers like to record newly delivered assets into the BCM database before deploying them on the network. So, they use ScanStar's 'Receive' workflow to create the assets in the BCM database. IT personnel then prepare the assets and add them to network. Now BCM scans the newly added assets to the network and creates a record in the database since it cannot find a matching record with the same device name. Now there are two records in the database for the same asset. Here are the steps to avoid duplicates.

1. Configure the Device Name in ScanStar to be a scan field: Navigate to Preference -> Configuration -> Client Management -> Scan Fields -> Add '**Name**' and '**Asset Tag**' fields to the scan field list.
2. In the ScanStar's Receive screen fill in all the non-scan fields then scan the service tag barcode for the asset into the '**Name**' and '**Asset Tag**' fields when receiving each of the assets.
3. The records are created in the BCM database for the new assets.
4. Name each of the assets to match its service tag before deploying to the network.
5. After deploying the assets, the BCM scan should update the records created from ScanStar (steps 1-3) instead of creating duplicates

Question: what happens when customer would like to rename the computer with a different name after step 5? ScanStar will still pull up the record by the Asset Tag but how will BCM handle this situation?

Create new assets in the BCM database via BCM scanning

In this scenario, customer deploys new assets to the network and let the BCM scanning create corresponding records in the database. ScanStar is used only to update existing asset's information to Track, Verify, or Audit.

How does ScanStar recognize an asset? Will the HostId be populated by the BCM scan and this data is

bar-coded as serial number on the asset? OR will the asset have a barcode with name of the asset?

Update existing assets in the BCM database from ScanStar

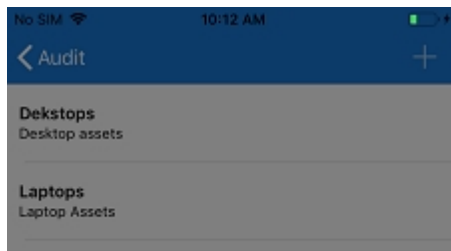
In this case ScanStar will overwrite existing data.

Update existing assets in the BCM database via BCM scanning

Will BCM overwrite existing data?

Audit Sets

This section explains how to configure filters that works with BCM



Filter: anywhere clause applicable to BCM is supported here. The field name is the name of the CI Type (Device) attribute .

Filter in following E.g. lists all server devices

Type=server

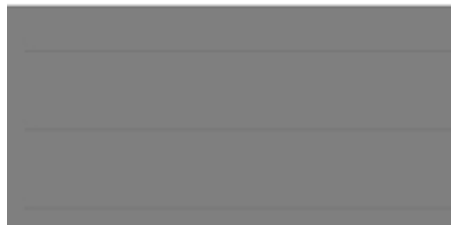


Figure 2

Naming Convention

Each CMDB provider has unique naming convention. Since ScanStar provides a common solution to each of these providers, it has its proprietary naming that closely aligns with ITAM. Following is the mapping between ScanStar and BCM

ScanStar	BCM
CMDB	Device
CIType	Type
Field	Attribute
CI (configuration item)	Device
Picklist	Reference object list

BMC Remedy

This page contains all Remedy specific integration information.

Sign In

Remedy specific information required to log into ScanStar.

User ID: Remedy user

Password: Remedy user password

Url: servername:port
The servername is the DNS or the IP of Remedy server. The port is the Jetty server's port number as configured in Remedy.
e.g. http://1.2.3.4:8443

CMDB Provider: BCM

Data Set Id: Remedy Data Set to be used in ScanStar

Classes: Classes to be used in ScanStar configuration

Figure 1

Best Practices to use ScanStar with Remedy CMDB

Changes to Remedy

1. It is always recommended to create an Asset by scanning it to a non-production dataset and reconcile that dataset into production dataset (BMC.ASSET). Do not scan a new Asset into BMC.ASSET directly unless your Asset Management process demands it.
2. To scan into a non-production dataset, create a new dataset ID called SCAN.ASSET in the BMC Atrium CMDB.
3. In the Atrium CMDB, create the following jobs
 - a. A new out of the box "Identify and Merge" job to reconcile the scanned Assets in SCAN.ASSET dataset into the production BMC.ASSET dataset. Make sure to schedule this job or manually run.
 - b. To keep scanner dataset always up to date, create another out of the box "Identify and Merge" job, this would be coming from BMC.ASSET to SCAN.ASSET. This job would need to be scheduled or ran manually.
4. If you try to scan an Asset into the BMC.ASSET dataset directly and it creates duplicates, then check the Asset in ITSM Asset Management to make sure that the Serial Number or Asset Tag are unique to an Asset.
5. If there are duplicate Assets in the BMC.ASSET dataset, then delete one of the duplicates by setting the Status to "Delete" and run a "Purge" reconciliation job to physically delete the duplicate Asset, so it does not interfere with production Assets.
6. Also if using SCAN.ASSET dataset to create new Assets, then periodically check any Assets in the SCAN.ASSET dataset that are already reconciled (Reconciliation ID != "0" and same the Asset exists in the BMC.ASSET dataset), and create a new "Purge" reconciliation job to clean up the SCAN.ASSET dataset for old reconciled Assets.
7. If you want to preserve any scanned Assets for review later and do not want it to interfere with

production Assets, then use a new Reconciliation job of Activity Type “Copy” to copy over the scanned assets into a temporary dataset like “REVIEW.ASSET”. You can also use the “Compare” Activity Type to compare a scanned Asset in SCAN.ASSET dataset with production dataset BMC.ASSET.

ScanStar

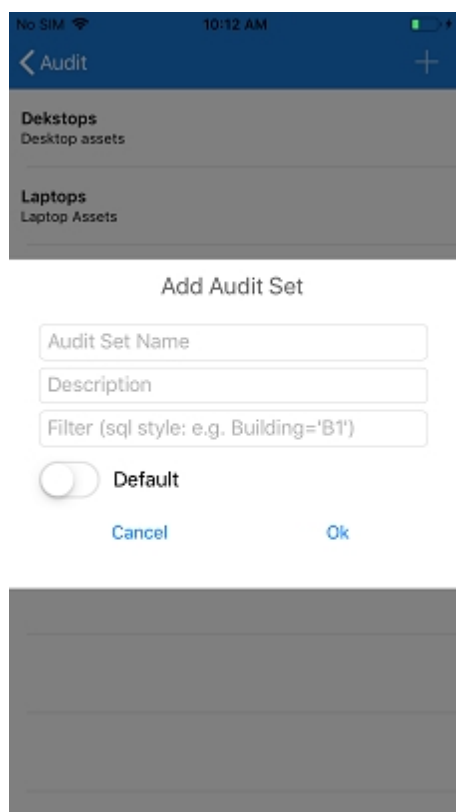
1. In the app “Preferences” set the Data Set Id to SCAN.ASSET. This way the “Received Assets” get created in the SCAN.ASSET dataset. This is also a good practice for testing the ScanStar App for the first time.
2. “Verify” mode can be used to set additional fields or to change fields of a previously scanned Asset. It's a powerful feature to use.
3. The “Owner” field has no validation rules behind it to verify that the person is a valid person in ITSM or CMDB.
4. In “Verify” mode, the “People” field displays the latest “Used By” People record related to the Asset in ITSM Asset Management -> People tab, if there are multiple People related to the Asset in the “Used By” role.
5. In “Verify” mode, when setting the “Received Date,” make sure the soft keypad is not visible on the smart phone screen before selecting (touching) the “Received Date” field to set it or change it.
6. In “Receive” or “Verify” mode, the Product Name, Manufacturer, Model, etc. will not display any drop down values unless they are configured in the ITSM Foundation data “Product Catalog” for a given “Product Categorization Tier 1, 2 and 3”. Configure them before use with ScanStar App.

People field in Workflows

This People field in each of the Receive, Track, and Verify workflow forms relates to the People tab in Remedy Asset Management's CI form. If missing, this field can be added to any of the workflow forms via the app configuration. Tapping on this field will list all the People records from which you can select a user to relate to the CI. Currently the CI / People relation created via ScanStar is assigned to the 'Used by' role by default and can be only modified from the Remedy console.

Audit Sets

This section explains how to configure filters that works with Remedy



Filter: any where clause applicable to Remedy is supported here. The field name is the Remedy field **Label** name in the CI Type (class).

Here are a few examples

Filter	Description
'Class Id' = "BMC_COMPUTERSYSTEM"	List computer system assets
'AssetLifecycleStatus' = "Deployed"	List assets that have been deployed

Figure 2

Naming Convention

Each CMDB provider has unique naming convention. Since ScanStar provides a common solution to each of these providers, it has its proprietary naming that closely aligns with ITAM. Following is the mapping between ScanStar and Remedy

ScanStar	Remedy
CMDB	Remedy CMDB
CIType	Classes
Field	Attribute
CI (configuration item)	CI
Picklist	Reference object list

Sample Barcode Tags

Sample Barcode Labels for Dell Laptops

Asset Tag	Serial Number
 121021	 SN001151
 121022	 SN001152
 121023	 SN001153

Sample Barcode Labels for Dell Docking Stations

Asset Tag	Serial Number
 121024	 SN001154
 121025	 SN001155
 121026	 SN001156

Contacting Technical Support

Contacting Technical Support

If you purchased your product from one of our distributors, you should contact that distributor for support assistance.

RightStar Technical Support is available from 8 a.m. to 6 p.m. Eastern Time, weekdays. You can contact Technical Support via telephone, Internet mail, and the World Wide Web home page. Outside of support hours, you may leave a voice message.

Before requesting support, check for [known issues & FAQs](#). If you still cannot resolve the issue please have the following information available:

- CMDB Platform
- ScanStar version
- Mobile device manufacturer, model and operating system
- Specific steps to reproduce the problem
- All information about the environment

Support Email: scanstar@rightstar.com