



# Configuring iSupport® Asset Functionality

iSupport's Asset functionality enables you to collect and record information about any type of item. This information can be associated with a customer and pulled into an incident, problem, purchase request, or change (if enabled) for status visibility between all affected departments. Asset records must be associated with an asset type. You can associate a custom layout and enable count tracking, scanning, custom and optional fields, and maintenance and warranty notifications for an asset type. An example of the Asset entry screen is shown below.

Asset			
New View Configuration			
Save	Save and Exit	Print	Delete
File		Print Label	Generate QR Code
		Font Size	Counters
		Display	
Type	Laptop	Location	Headquarters
Name	S3 Laptop	Tag Number	C101
Manufacturer	Dell	Serial Number	123484123904881-234
Model	Inspiron	Purchase Date	12/1/2021
Source	Direct Entry	Maintenance Expiration	12/1/2023
Associated CI	Laptop - Windows	Warranty Expiration	12/1/2023
Comments	System Check Complete		
	Rule Group	Default Asset Rule Group	

Owners			
Add Remove			
Last Name	First Name	Email	Company
Johnson	Steve	sj@gwi.com	LBL Services

## Configuration Overview

### Basic Configuration

Enable Asset functionality and set up asset types for classifying similar assets and enabling scans, count tracking, custom fields, and maintenance and warranty functionality and more via the Core Settings | Feature Basics screen. Enable applicable agents via the Agents tab in that screen. See ["Configuring Asset Types" on page 4](#) for more information.

## Creating Asset Records

- After selecting an asset type, you can manually create an Asset record via the Asset entry screen.
- If your asset data is kept in an Active Directory or LDAP source, you can use the Data Source Integration feature to import (one-way) and synchronize Asset records. See [“Integrating With Data Sources” on page 33](#).
- If your data is kept in one or more Microsoft SQL Server source databases, you can import asset data into iSupport’s Asset database and synchronize with those source databases on an interval basis. See [“Importing From a Remote Asset Database and Synchronizing” on page 30](#) for more information.
- If your asset data is kept in a Comma Separated Values .csv or Microsoft Excel .xlsx file, you can import asset data into iSupport’s Asset database. See [“Importing Asset Data from a CSV or Microsoft Excel File” on page 51](#).
- You can create more than one Asset record automatically via the Asset Creation Wizard. You can enter data to populate asset fields in all records created and display prompts for entering data unique to a record. You can save your settings in a profile for use later. See [“Using the Multiple Asset Creation Wizard” on page 54](#).
- You can enable Asset records to be automatically created for machines that are involved in scheduled scans but not associated with an existing record. See [“Creating Asset Records Automatically Based on Scheduled Scans” on page 73](#) for more information.
- If you have the Service Desk Edition, you can enable automatic creation of Asset records if all of the expected quantity for a line item on a purchase order is received. Enable Purchasing functionality via the Core Settings | Feature Basics screen; see the online help for more information.

## Customizing iSupport Defaults

- iSupport includes a default Asset screen layout with a comprehensive set of fields for tracking customer and company data, but you can redesign it via the Layouts screen to include fields and tabs that are specific to your company. You can assign different layouts to asset types. See [“Configuring Screen Layouts” on page 21](#).
- You can utilize maintenance, warranty, and low unit count tracking and for an asset type. See [“Configuring Asset Types” on page 4](#).
- If there are fields you need that are not included in iSupport by default, you can create custom fields for an asset type and global custom fields that will display in the Asset screen regardless of asset type. See [“Configuring Custom Fields” on page 14](#).

## Scanning and Monitoring

- You can perform ad hoc scans on non-Windows SNMP-enabled devices in your network, computers with Windows 98 and above, or any other WMI-compliant machine (WMI must be installed and active). See the online help for more information.
- You can configure defined devices to be scanned and/or monitored automatically on a scheduled basis via scheduled scans. See [“Configuring Scheduled Scans and Device Monitoring” on page 56](#).
- You can generate and save a side-by-side comparison of asset scans. See the online help for more information.
- You can enable network monitoring to flag devices if off line, disk space is lower than a specified minimum, or a service is not running. If a device is flagged, a notification can be sent and/or an Incident or Problem record can be created and any related asset record will be associated with the newly-created record. See [“Configuring Scheduled Scans and Device Monitoring” on page 56](#).
- You can scan bar codes and print bar code labels; see the online help for more information.

## Sending Notifications

- You can use Asset rules to send Desktop and email notifications when specified conditions based on Asset record fields or events are met; for example, you can configure a rule to send a notification when an asset warranty expiration date is near. See [“Configuring Rules and Rule Groups for Assets” on page 74](#). You can use or copy and modify iSupport’s default notifications, or you can create new custom notifications. See [“Customizing and Viewing Event Notification Content” on page 84](#). You can include data from Customer Profile records and designate any applicable recipients. See the online help for more information.

## Managing Asset Records

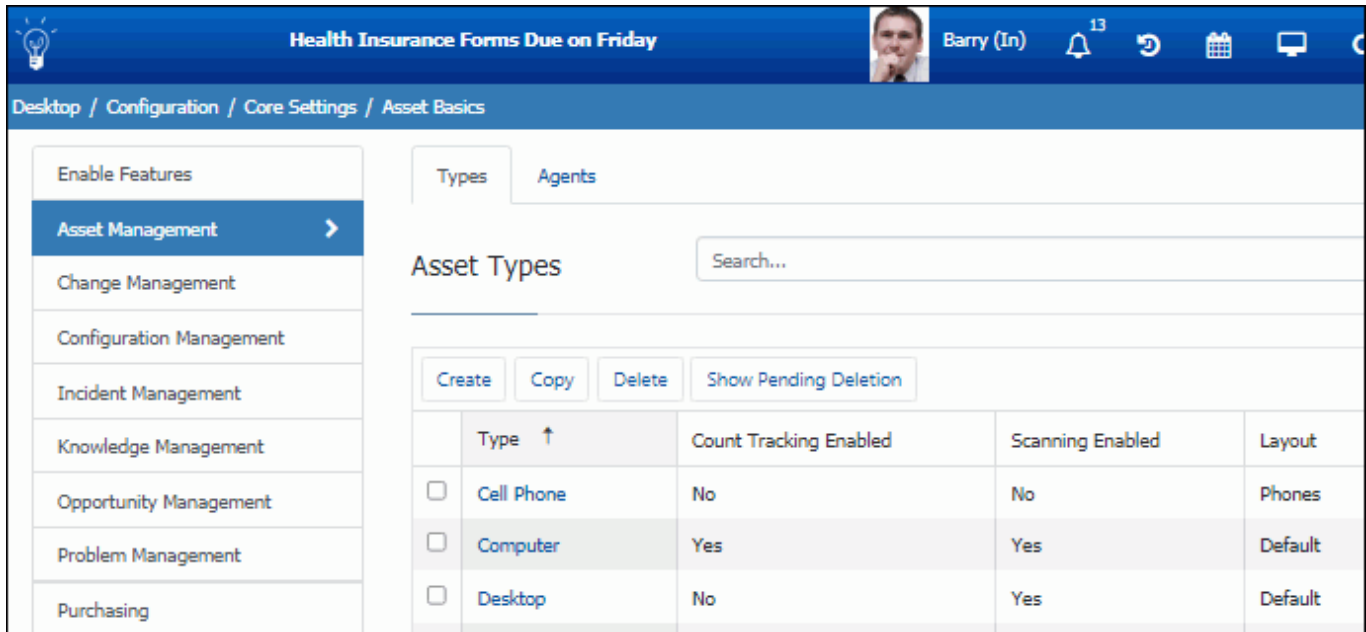
- Use the Action menu in the View component on the Desktop to perform actions such as viewing and opening multiple Asset records. See the online help for more information.
- You can automatically change field values on Asset records via Asset rules. See [“Configuring Rules and Rule Groups for Assets” on page 74](#).
- You can use webhooks to post Asset data to a web application via Asset rules. See [“Configuring Rules and Rule Groups for Assets” on page 74](#).
- You can associate a collection of assets into asset groups for viewing, reporting, and restricting access and display of an asset to members of a support representative group. See [“Creating Asset Groups” on page 12](#).
- You can configure roles/permissions for support reps and rep groups using Asset functionality via the Core Settings | Support Representatives screen. See the online help for more information.

## Using Other Work Item Functionality

- You can use Service Contract functionality to track and restrict incidents and changes associated with assets. Enable Service Contract functionality via the Core Settings | Feature Basics screen; see the online help for more information.
- If you have the Service Edition, you can utilize predefined asset types with associated vendors and products for purchase requests. Enable Purchasing functionality via the Core Settings | Feature Basics screen; see the online help for more information.
- If you have the Service Edition, you can associate configuration items to utilize data in Asset records for views, reports, and correspondence. A CMDB contains configuration items (CIs) for the resources to be tracked and the relationships between those items. Enable CMDB functionality via the Core Settings | Feature Basics screen; see the online help for more information.
- You can use the Generate QR code option in the toolbar to generate a QR code that contains a link that will display information about the record. You can also use the QR code to add an asset to an incident, problem, or change via the mobile interface, but note that the QR code reader option for selecting an asset in the HTML5 mobile interface will be hidden if using an Android device.

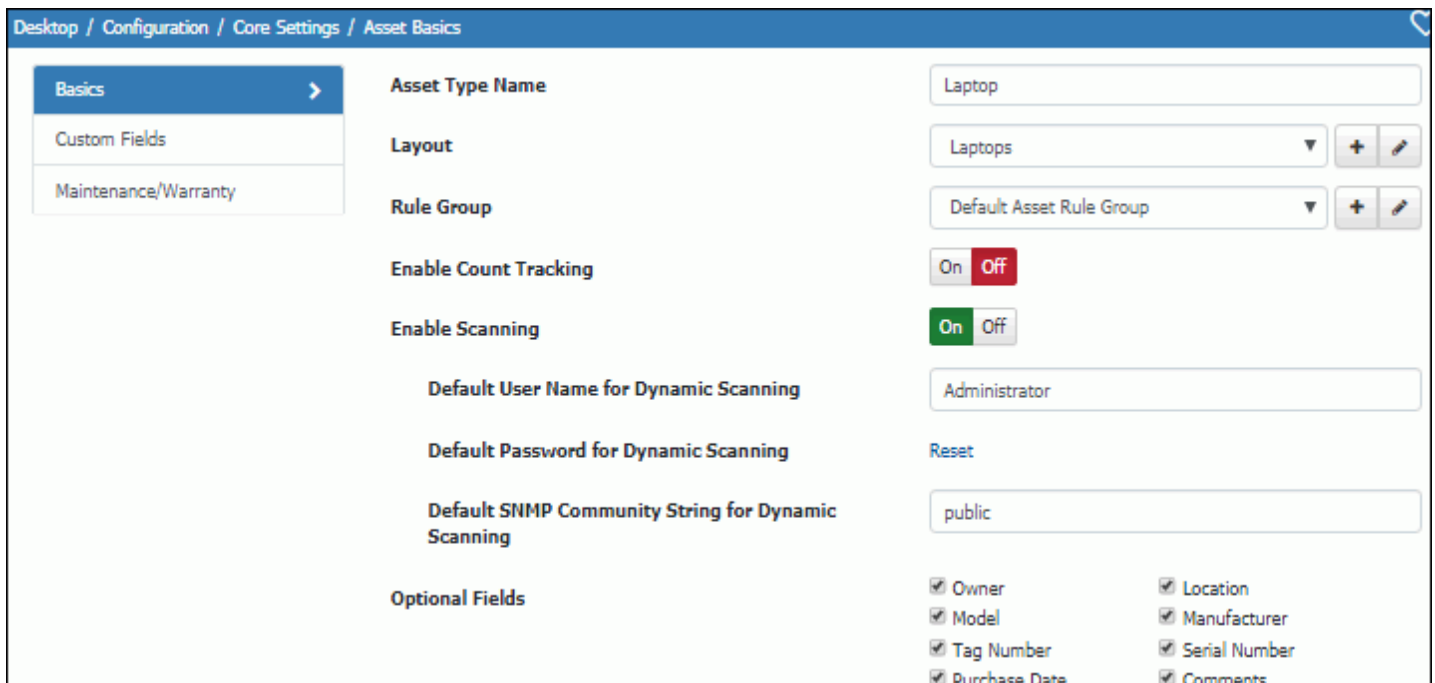
# Configuring Asset Types

Use the Asset Management Types tab in the Core Settings | Feature Basics configuration screen to set up asset types with fields and notifications for tracking similar assets (for example, printers and laptops).



Use the Show Pending Deletion link to display records that have been deleted by an iSupport user but are retained in the system because of references to other records (incidents, correspondence, etc.) The Database Maintenance agent ultimately removes these records.

Use the Basics tab to set up asset types, enter a login for running asset scans, and set up optional and custom fields.



**Asset Type Name** - Enter the name of the asset type. Asset types classify similar assets and enable custom and optional fields to display when recording information about an asset.

**Layout** - Select the layout containing the fields and tabs that will display when the type is selected in the Asset screen. Asset layouts are configured in the Asset Layouts configuration screen; see ["Configuring Screen Layouts" on page 21](#) for more information. If None is selected in this field, the layout designated as default in the Asset Layouts screen will be used when an Asset record of this type is created.

**Rule Group** - Select the Asset rule group that will take effect when an Asset record with the asset type is saved. Asset rules perform actions when specified conditions based on Asset record fields or events are met; these actions can include changing a field value, executing a webhook, and sending a notification via SMS, Desktop, or email.

**Enable Count Tracking** - Select Yes to enable Unit Count, Unit Label, Unit Cost, and Unit Price fields to appear in the Asset screen if the type is selected. When an asset with the specified type is selected in the Incident, Problem, or Change screen, a support representative with the Edit Used Count permission can enter the number of units used and decrement the unit count. A Low Unit Count notification can be configured to be sent when the minimum unit count is reached; it is sent on the schedule of the Asset Unit Count Tracking agent.

Desktop / Configuration / Core Settings / Asset Basics

Basics >

Custom Fields

Maintenance/Warranty

Notifications

Asset Type Name: Labor Hours

Layout: Labor Hours

Rule Group: None

Enable Count Tracking:  On  Off

Minimum Count Used: 1.00

Default Count Used: 1.00

Who to Notify of Low Unit Count:  Other

Email Addresses of Other Recipients: ak@gwi.com

Number of Units Remaining to Send Notification: 3.00

Enable Scanning:  On  Off

Optional Fields:

- Owner
- Model
- Tag Number
- Purchase Date
- Location
- Manufacturer
- Serial Number
- Comments

Count-related fields will be included in the Asset screen if the type is selected.

Asset New View Configuration

Save Save and Exit Print Delete Print Label Generate QR Code

File Actions

Type: Labor Hours

Name: Facilities Hour

Tag Number:

Location: HQ

Unit Label: Hour

Unit Count: 998.00

Unit Cost: \$125.00

Unit Price: \$125.00

When an asset with the specified type is selected in the Incident, Problem, or Change screen, a support representative with the Edit Used Count permission can select the Edit Count Used link, enter the number of units used, and decrement the unit count.

Name	Count Used
IT Support Hour	1.00 Hour

If a Product record with a count-enabled Asset type is selected on a purchase request and the flag to create an asset (when all items are received) is enabled, the received count will be added to the Asset Wizard for creating the Asset record.

**Minimum Count Used** - Enter the minimum amount that can be entered in the Count Used field in the Update Asset Counts dialog.

**Default Count Used** - Enter the amount to appear by default in the Count Used field in the Update Asset Counts dialog.

**Who to Notify of Low Unit Count/Email Addresses of Other Recipients** - A Low Unit Count notification can be customized via the Custom Notifications screen. Select the person to whom the Low Unit Count notification should be sent:

Select Owner to send the email to the owner assigned to the asset (in the Asset entry screen). The notification will contain asset details (for example, the name, type, and expiration date.)

Select Other to send the email to someone other than the owner. In the Email Addresses of Other Recipients field, enter the email address of this person. The notification will contain a link to the Asset record.

Be sure to enable the Asset Item Inventory Tracking agent in the Asset Agents screen; it checks unit counts and send notifications when the minimum is reached.

**Number of Units Remaining to Send Notification** - Enter the count (of total units remaining) at which the low unit count notification should be sent.

**Enable Scanning** - Select Yes if asset scans will be performed on assets assigned this asset type. Asset scans can be performed on non-Windows SNMP-enabled devices in your network, computers with Windows 98 and above, or any other WMI-compliant machine (WMI must be installed and active).

**Default User Name for Dynamic Scanning/Default Password for Dynamic Scanning** - If asset scans are enabled, enter the user name and password to be used for accessing the machine to be scanned. This login will be validated by the WMI process of the target machine in order to return the requested data. Traditionally, the login must be a member of the Administrators group of the machine to be scanned, but permissions may be modified to a different structure.

When a dynamic scan is initiated, the Dynamic Asset Scan dialog appears as shown below. If you have set up a default user name and password for the selected asset type, the support representative can select Yes in the Use Default Credentials checkbox to use this default user name and password.

If No is selected in the Use Default Credentials field, the User Name and Password fields will be enabled for entering a login.

**Default SNMP Community String for Dynamic Scanning** - If you wish to track non-Windows devices on your local subnet, enter the SNMP community string (a text string that acts as a password for a network device). Community strings are configured by administrators of network devices that support SNMP to allow varying levels of access to the devices configuration and operational settings; this grants management tools read-only access to the remote device. The default community string for read-only access to network devices is normally the word "public".

Note: If a login is used to access a Microsoft Windows XP machine, a profile and a folder are created in the Documents and Settings folder.

The Dynamic Asset Scan dialog is shown below; it appears when a dynamic scan is initiated in the Asset or Incident screen.

Check All Uncheck All View Tour

**Computer Systems**

- Computer System
- Services
- Running Processes
- Operating System
- Software Titles
- Hot Fixes

**System Ports**

- Modems
- Parallel Ports
- Port Connectors
- Network Adapters
- Serial Ports
- Logical Drives

**Peripherals**

- Infrared Devices
- Pointing Devices
- Keyboards
- Desktop Monitors

**System Hardware**

- Processors
- BIOS
- Physical Memory
- System Slots

**Hardware Controllers**

- IDE Controllers
- Video Controllers
- Floppy Controllers
- PCMCIA Controllers

**Drives**

- Disk Drives
- Floppy Drives
- CD-ROM Drives

Host Address: x.x.x.x.x

User Name:

Password:

Community: public

Scan

**Note:** If a login is used to access a Microsoft Windows XP machine, a profile and a folder are created in the Documents and Settings folder.

In the **Optional Fields** section, select the checkbox next to each field that should display when the asset type is selected in the Asset screen.

## Entering Custom Fields

In the **Custom Fields** section, select the Add link to set up a custom field that will display in the Custom Fields section when the asset type is selected in the Asset screen.

The screenshot shows a configuration form for a custom field. On the left, there is a sidebar with two tabs: 'Basics' (selected) and 'Conditional Display Options'. The main form area contains the following fields:

- Row:** A dropdown menu with the value '1'.
- Label:** A text input field containing 'Service Date'.
- Tooltip:** A text input field containing 'Date of service'.
- Required:** A toggle switch currently set to 'Off'.
- Type:** A dropdown menu with the value 'Date Field'.
- Default Value:** An empty text input field.

## Configuring Maintenance and Warranty Tracking

Use the Maintenance/Warranty tab to set up tracking of maintenance and warranty expiration dates. Expiration notifications are enabled on the Notifications tab. Be sure to enable the Asset Reminder agent on the Asset tab in the Asset Agents screen; see [“Scheduling and Running Asset Agents” on page 28](#).

The screenshot shows the 'Maintenance/Warranty' configuration page. On the left, there is a sidebar with four tabs: 'Basics', 'Custom Fields', 'Maintenance/Warranty' (selected), and 'Notifications'. The main form area is divided into two sections:

- Track Maintenance Information:** A toggle switch is set to 'On'. Below it, there are radio buttons for 'Who to Notify of Maintenance Expiration' (Owner is selected, Other is unselected). There is an empty text input field for 'Email Addresses of Other Recipients'. Below that, there are two text input fields: 'Number of Days After Asset Creation to Default Maintenance Expiration Date' (value: 255) and 'Number of Days Prior to Maintenance Expiration to Send Reminder' (value: 2).
- Track Warranty Information:** A toggle switch is set to 'On'. Below it, there are radio buttons for 'Who to Notify of Warranty Expiration' (Owner is selected, Other is unselected). There is an empty text input field for 'Email Addresses of Other Recipients'. Below that, there are two text input fields: 'Number of Days After Asset Creation to Default Warranty Expiration Date' (value: 255) and 'Number of Days Prior to Warranty Expiration to Send Reminder' (value: 2).

**Track Maintenance Information** - Select Yes to enable maintenance notification functionality, which sends notifications when a maintenance expiration date is near.



**Who to Notify of Maintenance Expiration/Email Addresses of Other Recipients** - If tracking maintenance information, select the person to whom the maintenance expiration reminder email should be sent.

- Select Owner to send the maintenance reminder email to the owner assigned to the asset (in the Asset entry screen). The notification will contain asset details (for example, the name, type, and expiration date.)
- Select Other to send the maintenance expiration reminder to someone other than the owner. In the Email Addresses of Other Recipients field, enter the email address of this person. The notification will contain a link to the asset record.

**Number of Days After Asset Creation to Default Maintenance Expiration Date** - Enter the number of days after the asset record is created to display as default for the maintenance expiration date.

**Number of Days Prior to Maintenance Expiration to Send Reminder** - Enter the number of days before the expiration date in which the maintenance notification should be sent.

**Track Warranty Information** - Select Yes to enable warranty notification functionality, which sends notifications when a warranty expiration date is near.

**Who to Notify of Warranty Expiration/Email Addresses of Other Recipients** - If tracking warranty information, select the person to whom the warranty expiration reminder email should be sent.

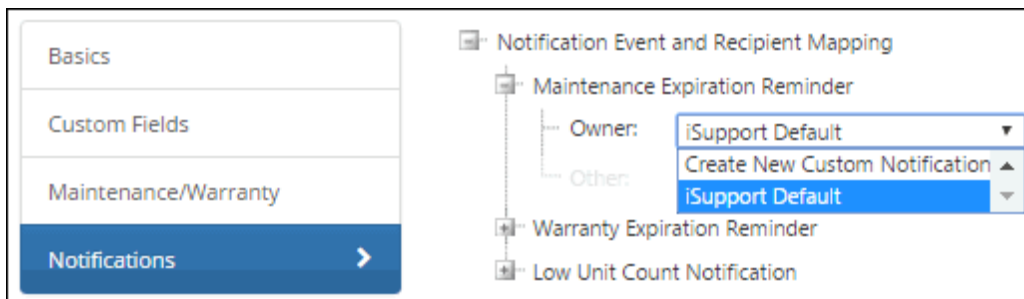
- Select Owner to send the warranty reminder email to the owner assigned to the asset (in the Asset entry screen).
- Select Other to send the warranty expiration reminder to someone other than the owner. In the Email Addresses of Other Recipients field, enter the email address of this person.

**Number of Days After Asset Creation to Default Warranty Expiration Date** - Enter the number of days after the asset record is created to display as default for the warranty expiration date.

**Number of Days Prior to Warranty Expiration to Send Reminder** - Enter the number of days before the expiration date in which the warranty notification should be sent.

## Selecting Notifications for Asset Events

Use the fields on the Notifications tab in the Asset Types screen to select notifications and recipients for maintenance/warranty reminders. You can select the default notification or a predefined custom notification; select Create New Custom Notification to access the Custom Notifications screen to create one. Note that the recipients can include both support representatives and customers, and the default notification text is different for each.



**Maintenance Expiration Reminder** - Select the recipients and notifications to be sent according to the settings on the Maintenance/Warranty tab. The notifications will be sent on the schedule of the Asset Reminder agent.

**Warranty Expiration Reminder** - Select the recipients and notifications to be sent according to the settings on the Maintenance/Warranty tab. The notifications will be sent on the schedule of the Asset Reminder agent.

**Low Unit Count Notification** - Select the recipients and notifications to be sent according to the settings on the Basics tab. The notifications will be sent on the schedule of the Asset Item Inventory Tracking agent.

## Scheduling Asset Agents

**Asset Reminder Agent/Time Agent Should Run Each Day** - The Asset Reminder agent searches for warranty and maintenance expiration dates. If it is the specified number of days before the warranty or maintenance expiration date, it will send an email reminder to the individuals specified in the Asset record. Select Yes to enable the Asset Reminder agent. After selecting Yes, use the Time Agent Should Run Each Day field to select the time the agent should run.

### Asset Reminder Agent

This agent sends notifications to the individuals specified in the Asset Configuration screen, based on the specified number of days prior to the warranty or maintenance expiration date.

Enable  Yes  No

Time Agent Should Run Each Day

**Asset Unit Count Tracking Agent** -If count tracking is enabled for an asset type and the type is selected in the Asset screen, a count and low item threshold can be entered for an asset. The count can be decremented via entries in the Incident, Problem, and Change screens and notifications can be sent to the individuals specified in the Asset Type Configuration screen when the count reached the specified minimum number of remaining units. Select Yes to enable the agent to check unit counts and send notifications when the minimum is reached. After selecting Yes, use the Time Agent Should Run Each Day field to select the time the agent should run.

### Asset Unit Count Tracking Agent

This agent sends notifications to the individuals specified in the Asset Type Configuration screen based on the specified minimum threshold of remaining units.

Enable  Yes  No

Time Agent Should Run Each Day

**Asset Scheduled Scan and Monitoring Agent** - After entering a scheduled scan and monitoring definition (see [“Configuring Scheduled Scans and Device Monitoring” on page 56](#)), select Yes in this field to enable the Asset Scheduled Scan and Monitoring agent which checks scheduled scan definitions, initiates scans according to schedule, and enables monitoring if configured in an scheduled scan definition. This agent runs every minute. Network monitoring processing adds device state change entries in the database. Use the **Monitoring includes device state change entries in the database; days to retain these entries** field to control database growth by entering the number of days in which these entries should stay in the database.

### Asset Scheduled Scan and Monitoring Agent

This agent checks scheduled scan definitions, initiates scans as scheduled, and enables monitoring if configured in an scheduled scan definition.

Enable  Yes  No

Monitoring includes device state change entries in the database; days to retain these entries

**Auto Asset Create from Scheduled Scan Agent** - Assets can be created automatically for machines that are involved in scheduled scans but not associated with an existing record; see [“Creating Asset Records Automatically Based on Scheduled Scans” on page 73](#) for more information. Enable this agent to create asset records for each machine involved in an scheduled scan that does not have an association with an asset record. It will run every hour based on the time at which the iSupport Agent Manager service is started. A dialog will appear for selecting the Asset

record to be used as a template for automatically creating records; this is a good method to use for control in building asset records.

### Auto Asset Create from Scheduled Scan Agent

This agent creates an Asset record for each asset scan that is not associated with an asset.

**Enable**  Yes  No

**Populate Asset Serial Number Field using**

**Default Asset Record Template for Automatic Asset Creation**

**Populate Asset Serial Number Field Using** - Select one of the following for populating the Asset Serial Number field when Asset records are created automatically for machines that are involved in scheduled scans but not associated with an existing record: the operating system serial number or the BIOS serial number. If the BIOS Serial Number is selected but not available, the machine name or ID defined in the scheduled scan definition will be used.

**Asset Record Template for Automatic Asset Creation** - Select this link to select the name of an existing Asset record to use as a template when the Auto Asset Create from Scheduled Scan agent is run. The record's asset type will determine the fields that will appear on the automatically-created record. See ["Creating Asset Records Automatically Based on Scheduled Scans"](#) on page 73 for a table listing how the fields are populated.

**License Management Agent** - The License Management agent scans all scheduled scans and searches for instances of the software titles specified in Software License Profile records. It compares the actual quantities found against the conditions, flags the profiles that meet the conditions, and updates the profiles with the actual quantities. Notifications are sent if configured.

### License Management Agent

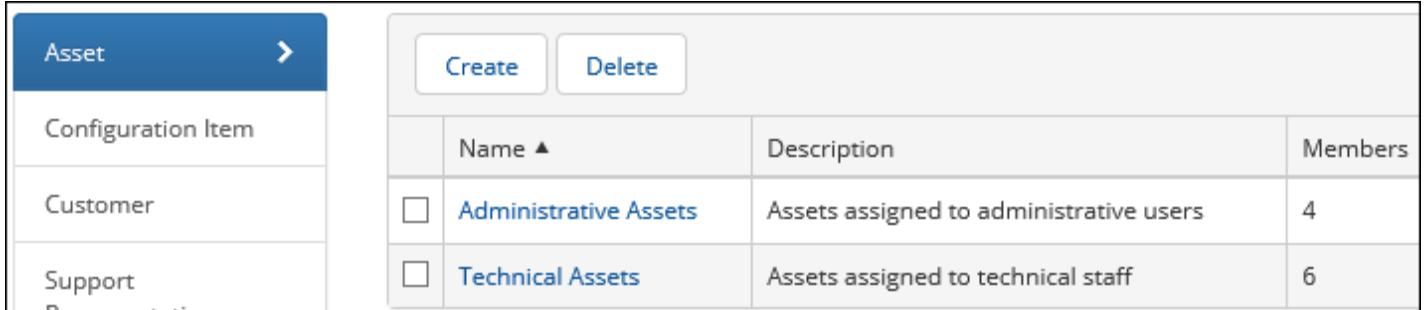
This agent scans all inventory scans and searches for the software titles specified in Software License Profile records. It compares the actual quantities found against the condition specified in the profiles, flags the profiles that meet the condition, and updates the profiles with the actual counts.

**Enable**  Yes  No

**Time Agent Should Run Each Day**

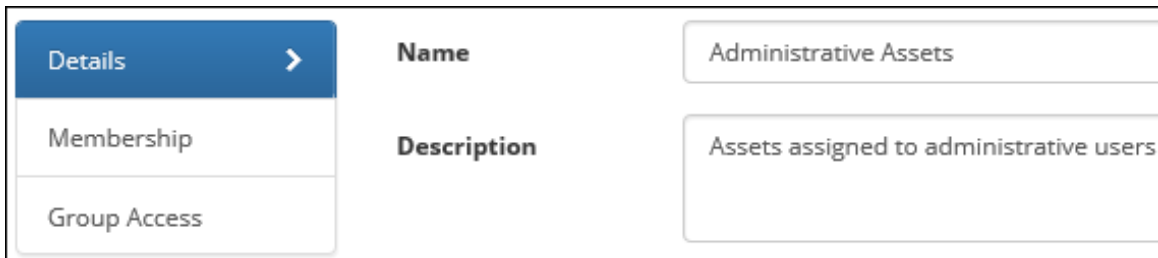
## Creating Asset Groups

Asset groups enable you to associate a collection of assets for access, viewing, and reporting. You can assign assets to a group via the Asset Group screen and the Desktop. To create a group, select the Assets tab in the Core Settings | Groups screen and then select the Create link.



	Name ▲	Description	Members
<input type="checkbox"/>	Administrative Assets	Assets assigned to administrative users	4
<input type="checkbox"/>	Technical Assets	Assets assigned to technical staff	6

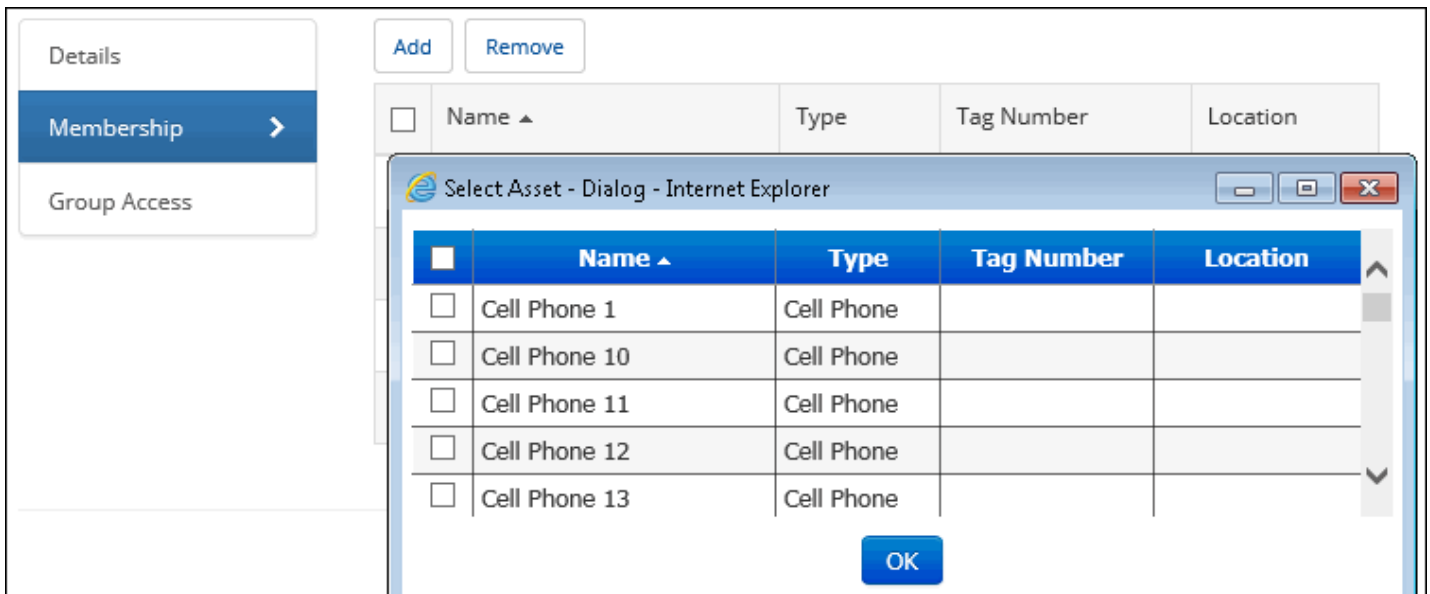
The following screen appears; enter the name and description of the group on the Details tab.



**Details** | Name: Administrative Assets | Description: Assets assigned to administrative users

## Adding Assets to Asset Groups

Use the Membership tab to add selected assets to a group.



**Membership** | Add | Remove

<input type="checkbox"/>	Name ▲	Type	Tag Number	Location
<input type="checkbox"/>	Cell Phone 1	Cell Phone		
<input type="checkbox"/>	Cell Phone 10	Cell Phone		
<input type="checkbox"/>	Cell Phone 11	Cell Phone		
<input type="checkbox"/>	Cell Phone 12	Cell Phone		
<input type="checkbox"/>	Cell Phone 13	Cell Phone		

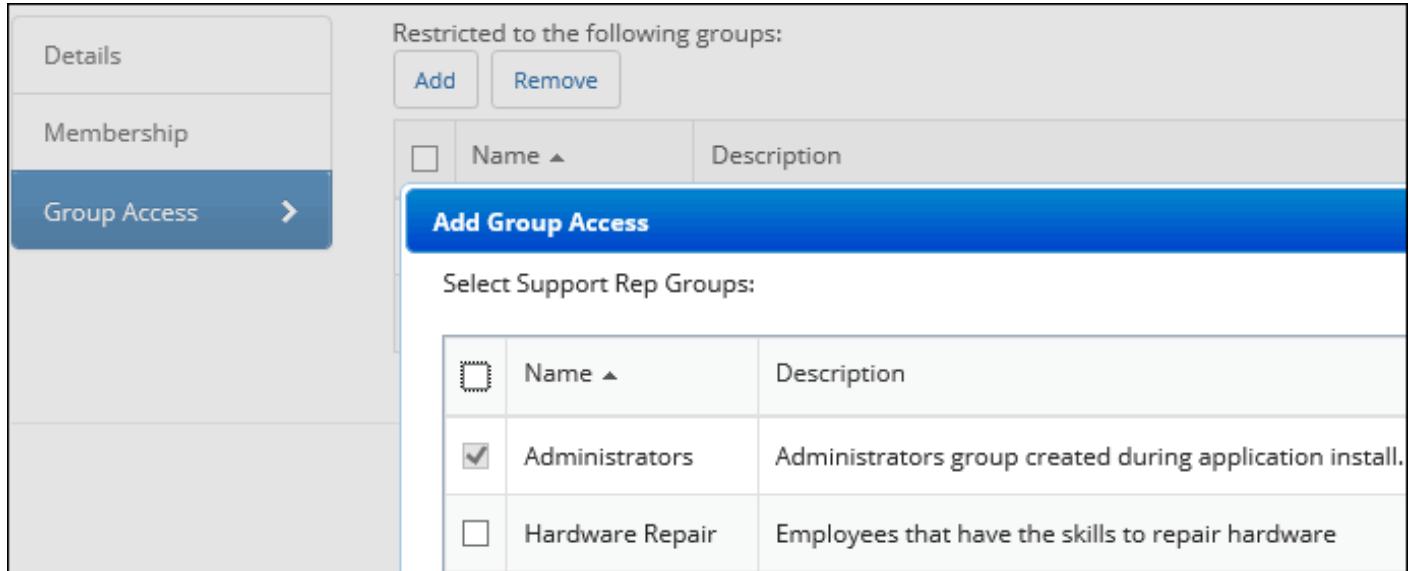
OK

To add an asset to the group, select the Add link. Select an existing asset and select OK.

## Restricting Access

Use the Group Access tab to restrict access to assets in the group to members of support representative groups. This allows only those in the related support representative group to edit Asset records in the asset group (or any other asset record not included in an asset group). If configured, a support representative can select only his/her groups to add to an asset. Other unrelated groups could be present on an existing asset; these unrelated groups could be removed but not added. Select the Add link to select the groups. After saving, assets in the group will be available

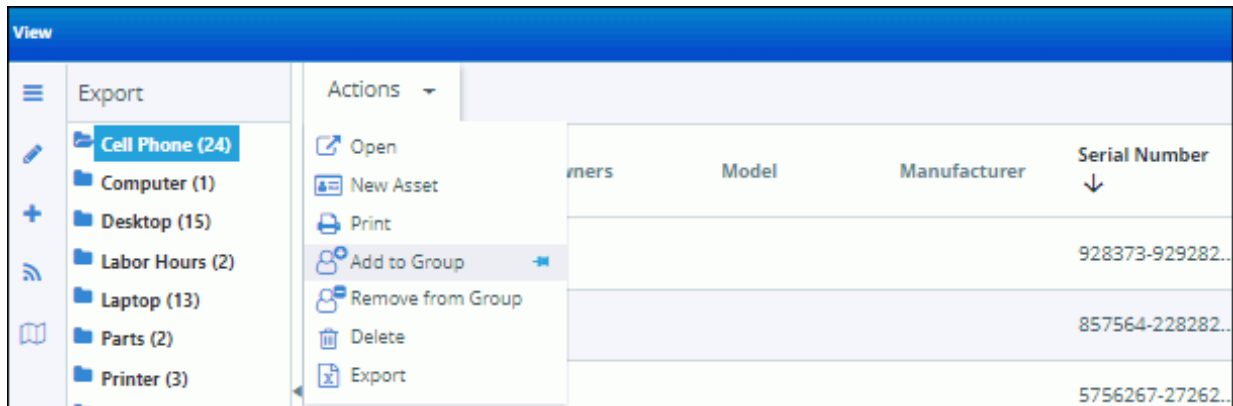
only to members of the selected support representative groups (unless a member is an owner). Note that group access permissions only restrict the ability to open a record; group access does not filter display of data in views, charts, and reports.



## Adding Assets to Groups

You can add an asset to a group when you create an Asset record via the Asset screen. In the Groups section, select a predefined group in the No Membership field and select the right arrow to move the group to the Membership field.

You can also add selected assets to a group and remove selected assets from a group via the Desktop. Select the assets via an asset view and then select the Add to Group and Remove From Group options.



# Configuring Custom Fields

To define fields for entering information specific to your company, go to Options and Tools | Customize | Custom Fields. An unlimited number of text, keyword, hyperlink, date, selection, and date/time fields can be defined. You can do the following with custom fields:

- Require custom fields to be completed before a work item is saved and/or closed
- Configure display based on defined conditions, and pull from a data source
- Map to a SQL data source and populate and synchronize options for list-type custom fields
- Use rules to set a custom field value
- Configure custom fields to appear when an associated asset type, CMDB type, cost center, or category is selected; you can control display of these additionally defined fields in screen layouts. Note that all custom fields that have met any conditional display conditions will be created upon mySupport work item submission regardless of whether they are included on a mySupport submission layout.

Property	Value
Row	1
Label	Server OS
Tooltip	Server Operating System
Required on Save	Off
Required on Close	Off
Available to Reps	On
Encrypt	Off
Type	Check Box
Data Source	None
Options	<input checked="" type="checkbox"/> Windows <input type="checkbox"/> Mac <input type="checkbox"/> Other
Max Columns	2

**Row** - Enter the row number for the position of the field. Row one will be the first field, row two will be located under the first field, and so on.

**Label** - Enter the label for the custom field.

**Tooltip** - Enter the text to display when a user hovers over the field with the cursor.

**Required on Save** - Select On to require the field to be completed before the record can be saved. Note: If an inbound email rule uses an auto-close incident template and a required custom field does not have a default value, the required custom field will not have a value in the closed incident.

**Required on Close** - Select On to require the field to be completed before a Closed status can be selected in a work item.

**Available to Reps** - Select Off to prevent support representatives from editing the field. (However, rules can change field values.)

**Encrypt** - If your business has a specific mandate regarding column level encryption and you are already using 'database at rest' encryption, send a request to iSupport's Technical Support department for a feature unlock code.

**Type** - Select the format of the field. Note that for list-type fields (Checkbox, Multiple Selection List Box, Radio Button, Single Selection Drop-Down, and Type Ahead) you can map to a SQL data source and populate and synchronize options for a field; see "[Pulling From a Data Source](#)" on page 19 for more information.

- A **Check Box** field enables multiple selections; use the Max Columns field to enter the number of check boxes to appear before a scroll bar is used.
- A **Currency** field displays a dollar sign next to the field and allows entry of the numbers 0 through 9, a decimal point, and two values after the decimal point. The dollar sign symbol that precedes a currency custom field is controlled by the server's default language, but you can override it via a setting in the web.config file (located in the directories in which the Desktop, mySupport portal, and Survey functionality are installed). The following tag in the web.config file defines globalization settings: `<globalization requestEncoding="utf-8" responseEncoding="utf-8"/>`

You can add a culture/language name setting to this tag to override the currency symbol; in the example below, `culture="en-GB"` was added to change the dollar sign symbol to the English (United Kingdom) pound symbol. `<globalization requestEncoding="utf-8" responseEncoding="utf-8" culture="en-GB"/>`

Note that the settings in the web.config file should be updated only as directed (via this guide or iSupport Technical Support); failure to do so may result in data loss or corruption. See <http://msdn2.microsoft.com/en-us/library/system.globalization.cultureinfo.aspx> for more information on defined culture settings.

- A **Date** field enables entry or selection of a date in MM/DD/YY format; a **Date Time** field enables entry or selection of a date (MM/DD/YY) and time. To disable manual entry in Date and Date Time fields and require the user to select from the calendar popup, select Yes in the Disable Manual Entry of Date Time Custom Fields field on the Advanced tab in the Custom Fields list screen.
- A **Hyperlink** field enables you to specify default text and a URL to appear in the field; the user can change those entries. You can also leave the field blank and allow the user to enter the default text and URL.
- A **Label Only** field does not display a value option; you can use it as a section header to group custom fields.
- A **Multiple Selection List Box** field enables the user to select multiple entries in a list. Use the Max Rows field to enter the number of selections to appear before a scroll bar is used.
- A **Number Only** field enables entry of the numbers 0 through 9 and a decimal point.
- A **Radio Button** field enables only one selection; use the Max Columns field to enter the number of radio buttons to appear before a scroll bar is used.
- A **Single Selection Drop-Down** field enables selection of one item in a list.
- A **Text Area** field enables text characters to be entered in a resizable field.
- A **Text** field enables text to be entered in a one-line field.
- A **Type Ahead** field initiates a search of matching options after a few characters are typed. This custom field type is only used for fields that are linked with a data source.

Examples are shown below.

Check Box	<input checked="" type="checkbox"/> Option 1 <input checked="" type="checkbox"/> Option 2 <input type="checkbox"/> Option 3	Date Field	<input type="text" value="03/08/2019"/>
Radio Button	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> I don't know	Date/Time Field	<input type="text" value="03/07/2019 3:27:00"/>
Text Area	<input type="text"/>	Single Selection Drop-Down	<input type="text" value="Option 1"/>
Text Field	<input type="text"/>	Multiple Selection List Box	<input type="text" value="Option 1"/> Option 2 Option 3
Currency Only	<input type="text" value="\$ 123"/>	Hyperlink	<a href="#">iSupport's Web Site - Edit</a>
Number Only	<input type="text" value="123"/>		

**Options** - This field displays when creating a radio button, checkbox, multiple selection list box, or single selection drop-down. Enter or paste items into this field; separate each value with a comma or return and select  Commit Items when finished. Select items to specify defaults and drag items to change the order. Options can be populated by and synchronized with a SQL data source; see ["Pulling From a Data Source" on page 19](#) for more information.

**Default Value** - Enter a value to appear as an option in the custom field by default.

- To display the current date, enter **@today**
- To display the date a specified number of days after the current date, enter **@today+n** (where *n* is the number of days to add after today's date)
- To display the date a specified number of days before the current date, enter **@today-n** (where *n* is the number of days to subtract from today's date)

**Max Columns/Max Rows** - For Check Box and Radio Button type fields, enter the maximum number of columns to display (the fields will wrap to multiple rows); for a Multiple Selection List Box type field, enter the maximum number of rows to display (causing a scroll bar to appear).

To delete a custom field, select the row number and then select the Delete link. To delete multiple custom fields, select the fields and select the Delete link. To edit a custom field, select the label link.

**Validation** - This field appears for Date, Date/Time, Currency, Text Area, and Text custom fields. Select On to enable date, date/time, currency, text area, and text custom fields to be validated upon entry (for example, the calendar picker will only make available valid dates for selection). Enter the parameters that the field will be validated



against; the parameters will vary depending on the type of field.

Basics	Row	9
mySupport Access	Label	Install Date
Conditional Display Options	Tooltip	Select a date between one and five days after today.
	Required on Save	On Off
	Required on Close	On Off
	Available to Reps	On Off
	Encrypt	On Off
	Type	Date Field
	Default Value	@Today+2
	Validation	On Off
	Date Validation Type	Between (Inclusive of Valid Start and Valid End)
	Valid Start	1 Days
	Valid End	5 Days

Note: 0 = today, positive values for future dates, negative values for past dates.

- **Date:** The calendar picker will only make available valid dates for selection by the user. Use the Date Validation Type field to specify the basis for validation and then enter the number of days before or after the current date on which to make available dates. Use zero as the current date, positive values for future dates, and negative values for past dates.

Select **Start** in the Date Validation Type field to ensure that the available dates for selection will be on or after the specified number of days from the current date. Examples:

- If you enter -2 in the Valid Start field, the dates available for selection will start two days before the current date.
- If you enter 0 in the Valid Start field, the dates available for selection will start on the current date.
- If you enter 1 in the Valid Start field, the dates available for selection will start one day after the current date.

Select **End** in the Date Validation Type field to ensure that the available dates for selection will be on or before the specified number of days from the current date. Examples:

- If you enter -2 in the Valid End field, the dates available for selection will end two days before the current date.
- If you enter 0 in the Valid End field, the dates available for selection will end on the current date.
- If you enter 1 in the Valid End field, the dates available for selection will end one day after the current date.

Select **Between** (Inclusive of Valid Start and Valid End) to ensure that the available dates for selection will be a range: starting on or after a specified number of days from the current date, and ending on or before a specified number of days from the current date. (Your entry in the Valid Start field must be less than or equal to the number of days in the Valid End field.) Examples:

- If you enter -2 in the Valid Start field and 2 in the Valid End field, the dates available for selection will start two days before the current date and end two days after the current date.

- If you enter 1 in the Valid Start field and 3 in the Valid End field, the dates available for selection will start one day after the current date and end three days after the current date.
- **Date Time:** The information above applies to this field; use the Validation Start Time and Validation End Time fields to select available times on the available days for selection.
- **Currency:** Enter a minimum amount in the Min Amount field, a maximum amount in the Max Amount field, or a minimum and maximum in both fields to specify a range. (Your entry in the Min Amount field must be less than or equal to the number in the Max Amount field.)
- **Number Only:** Enter a minimum amount in the Min Amount field and a maximum amount in the Max Amount field; the number the user enters must be between the two numbers. (Your entry in the Min Amount field must be less than or equal to the number in the Max Amount field.)
- **Text Area/Text:** Enter a minimum number of characters in the Min Length field or a maximum number of characters in the Max Length field. Enter numbers in both fields to specify a range. (Your entry in the Min Length field must be less than or equal to the number in the Max Length field.)

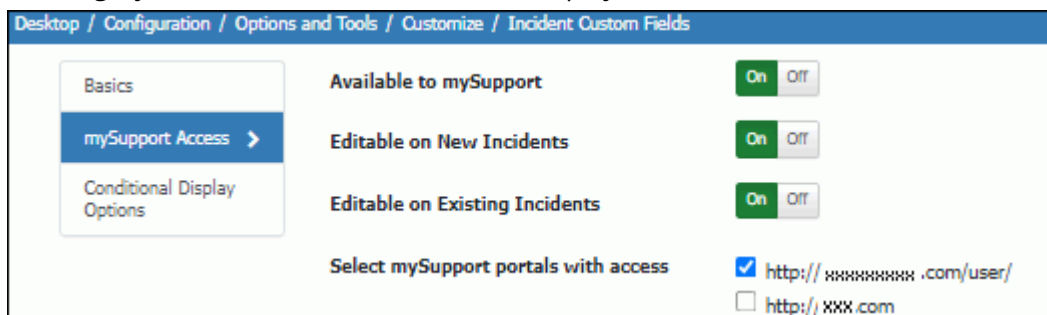
### *mySupport Access Options*

**Available to mySupport** - Select On to enable the field to appear on a mySupport portal.

**Editable On New Incidents** - This field appears if Hyperlink is selected in the Type field on the Basics tab. Select On to enable the Edit link for Hyperlink-type custom fields on mySupport. Note: On is the default value; when off, the default text and URL are validated and the Edit link is hidden in mySupport.

**Editable On Existing Incidents/Changes** - Select On to enable the custom field to be edited by customers with the mySupport Custom Fields Editor permission. Note that you can use the Allow Edit field in the Configure Field dialog for custom fields on mySupport display layouts to disable/enable an individual Customer Profile custom field to be edited by customers with the mySupport Custom Fields Editor permission.

**Select mySupport Portals with Access** - If the mySupport Access field is enabled, select the predefined mySupport portal interfaces on which the custom field can appear. Note: If custom fields are associated with more than one level of a selected category set, the fields for all levels will display.

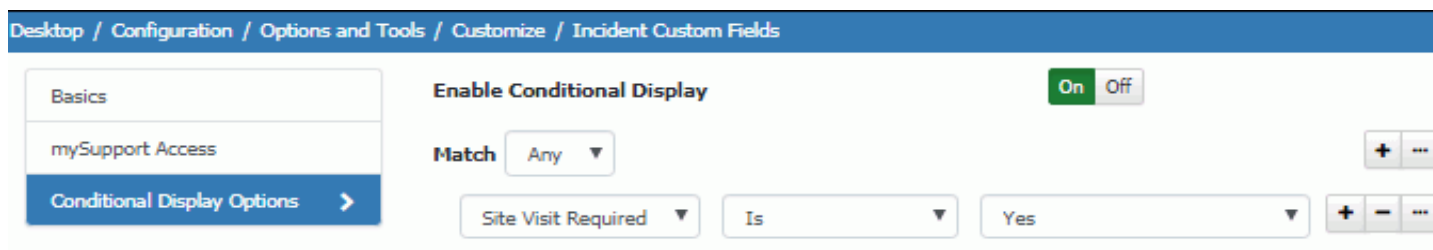


### *Setting Advanced Options*

**Disable Manual Entry of Date Time Custom Fields** - Select Yes to require that users only select from the calendar popup for Date and Date Time custom fields.

## Conditional Display Options

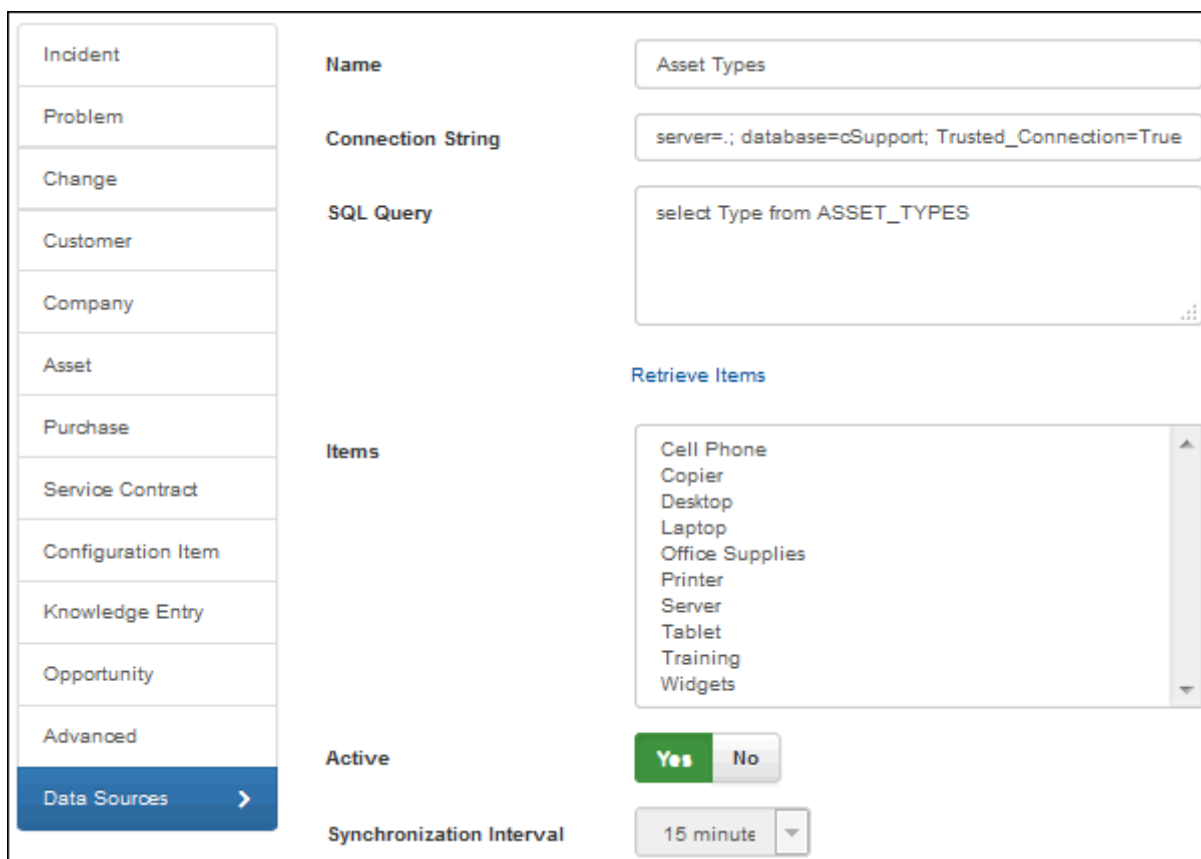
**Enable Conditional Display** - Select On to enable the Conditional Display Options fields for configuring conditions on which to base display of the custom field.



Use the Match *<All/Any>* field to specify whether you want **every** *<field>* is *<value>* search condition to be met, or **any** configured condition to be met. Use the **+** Add Condition and **-** Remove Condition options to display and remove a *<field>* is *<value>* search condition. Select the **+** Add Condition option if you wish to include another condition. You can use the **...** Add Condition Group option to put a set of search conditions to be evaluated together in a group.

## Pulling From a Data Source

You can map to a SQL data source and populate and synchronize options for list-type custom fields. Use the Data Sources tab in the Custom Fields screen to create a custom field data source definition, enter a connection string and SQL query, and specify the synchronization interval.



**Name** - Enter a name for the SQL Server source definition. This name will appear in the list that can be selected in the Data Source field in the Custom Field Definition dialog (if a list-type format is selected in the Type field).

**Connection String** - Enter the connection string for accessing the source database.

**SQL Query** - Enter the SQL query string for accessing the field options in the SQL database. Select the Retrieve Items button to populate the Items field using this string.

**Active** - Select Yes to enable synchronization and update the Options list for a custom field with the information in the SQL source database.

**Synchronization Interval** - Select the number of minutes in the interval for the synchronization to be performed.

Using the Data Source for a Custom Field

After saving, the custom field data source definition will be available for selection in the Custom Field Definition dialog. The Options field will be populated and will not be editable after synchronization.

Desktop / Configuration / Options and Tools / Customize / Incident Custom Fields

Basics > mySupport Access Conditional Display Options

Row: 4

Label: Affected Item

Tooltip:

Required on Save: On Off

Required on Close: On Off

Available to Reps: On Off

Encrypt: On Off

Type: Multiple Selection List Box

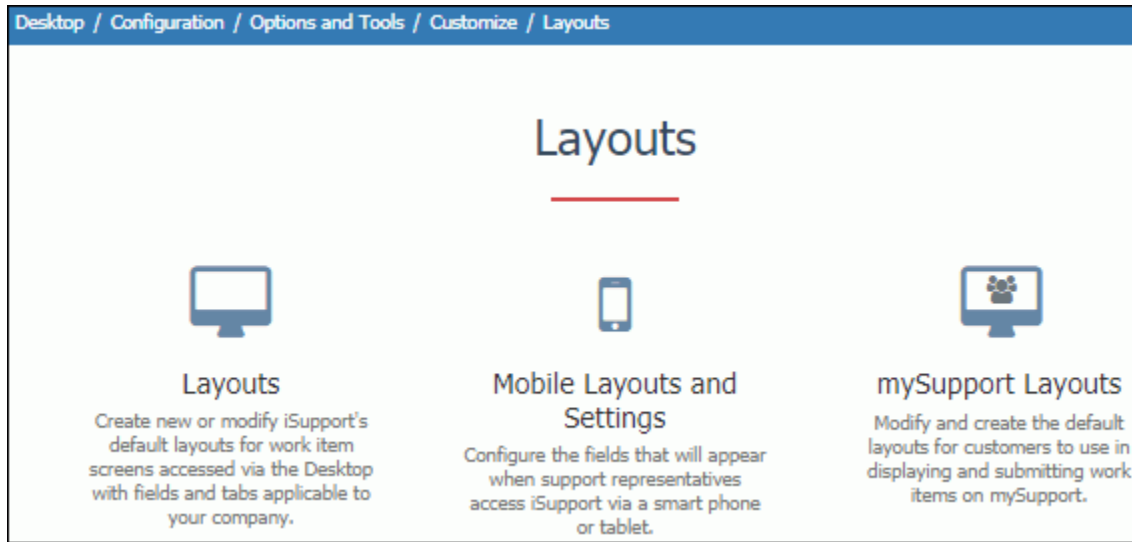
Data Source: Asset Types +

Options:  Cell Phone  Copier  Desktop  Laptop  Office Supplies

Max Rows: 2

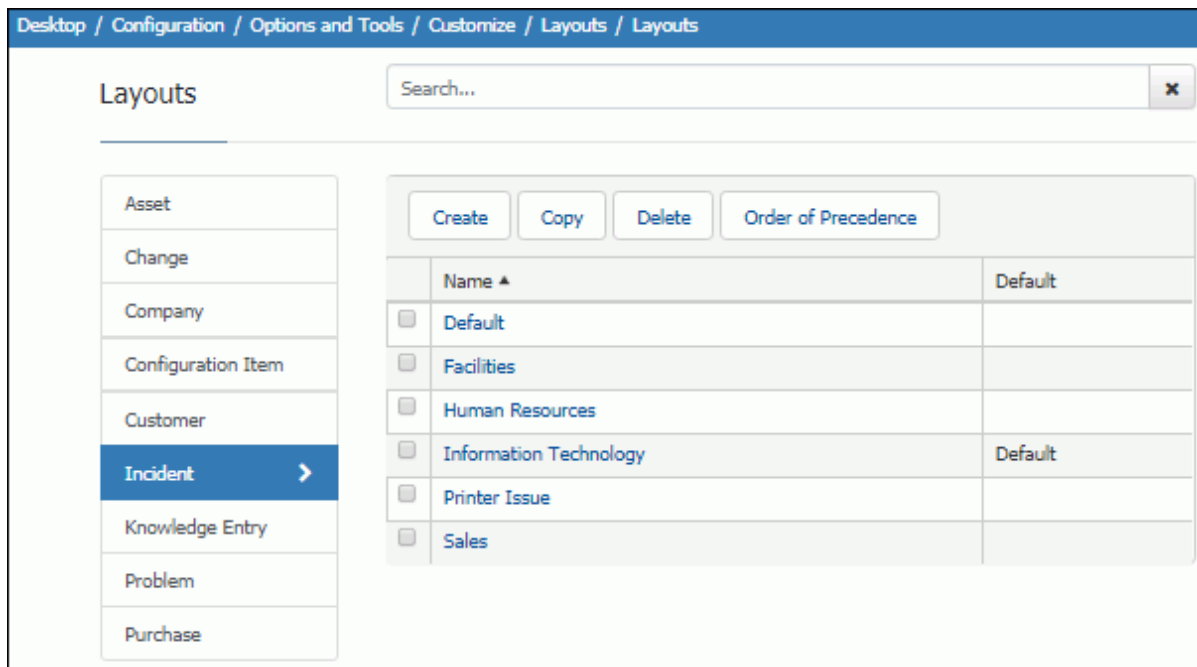
# Configuring Screen Layouts

iSupport includes default layouts for the entry screens used by support representatives, the display and submit screens used by customers on the mySupport portal, and for the mobile HTML5 interface. Use the Layouts screens to modify these layouts and/or create new ones with fields and tabs that are specific to your company.



Note that only layouts configured via the Global Settings | Mobile Settings screen will apply to the mobile HTML5 interface. Also, mySupport Customer layouts will appear when the customer selects the View Complete Profile button in the Account Settings screen on a mySupport portal.

You could create layouts based on different types of users, different types of work, etc.



You can assign different layouts to different asset and configuration item types (SD Edition), and you can assign different incident, problem, and change layouts to support representative groups, customer groups, categories. For incidents and changes, you can assign different layouts to templates and hierarchy templates. More than one layout may be applicable to incidents, changes, and assets; for example, if a layout is associated with the logged in rep's primary group as well as with the selected category for an incident. Use the **Order of Precedence** link on the those list screens to specify which layout to use when more than one reference is applicable.

The Layout screen is shown below.

The screenshot shows the 'Incident Layouts' configuration screen. At the top, a breadcrumb trail reads: Desktop / Configuration / Options and Tools / Customize / Layouts / Incident Layouts. Below this, there are three tabs: 'Layout' (selected), 'Colors', and 'Custom Menu Actions'. The main configuration area includes:

- Name:** A text field containing 'Human Resources'.
- Tutorial:** A dropdown menu set to 'Submitting HR Issues', with '+' and edit icons to its right.
- Default:** Radio buttons for 'Yes' and 'No', with 'No' selected.
- Customer Details:**
  - Title:** A text field containing 'Customer'.
  - Display Avatar:** Radio buttons for 'Left', 'Right', and 'No', with 'Left' selected.
  - Display Microsoft® Skype/Lync® Status:** Radio buttons for 'Yes' and 'No', with 'No' selected.
  - A dropdown menu labeled 'Add a field'.
  - A list of fields to be displayed: (Display Name), (Phone), (Email Address), and (Incident Counts), each with a checkbox and a gear icon.
- Main Layout:** A vertical list of fields under 'Basics' (Previous Assignee, Group, Group Type, Category \*, Rule Group, Top Level Description, Short Description, Top Level Short Descrip, Modified Date, Modified By, Author, Related Hierarchy, Feedback, mySupport Submission) and 'List Items' (Custom Fields, Associated Work Item Co).
- Details:** A preview window showing a grid of fields: Number, Status, Priority, Created Date, Closed Date, and Assignee.
- Orientation:** A dropdown menu set to 'Top'.
- Buttons:** An 'Add a Tab' button.
- Tab Selection:** A row of icons with labels and close buttons: Details (house icon), History (pencil icon), Custom Fields (document icon), Others to Notify (people icon), Assets (monitor icon), Associated Work Items (list icon), Attachments (paperclip icon), and Misc. (notepad icon).
- Text:** A text field containing 'Details'.
- Icon:** A 'Choose' button.
- Preview:** A preview window showing a field labeled 'Description'.

Use the **Tutorial** field to associate a tutorial that will display the first time the support representative accesses a screen with the layout. A tutorial consists of a series of steps, each with an 800x600 image and tags that a user can select to display an additional screen of content. Use the **+** Create New and **✎** View/Edit options to access the Tutorials screen to create a tutorial or view/modify the selected tutorial; see the online help for more information. In

that screen you can associate a tutorial with entry screen layouts, configuration screens, Rep Desktop dashboards, and mySupport dashboards.

Select Yes in the **Default** field to display the layout if none is associated with current support representative group, customer group, category, incident template, or hierarchy template.

For Rep Client layouts, you can use the Preview button at the bottom of the Layout screen after adding required fields to the form to display your layout. You'll need to select a record to use for displaying field data.

## Configuring Customer Details


### *Rep Incident and Change Screens*

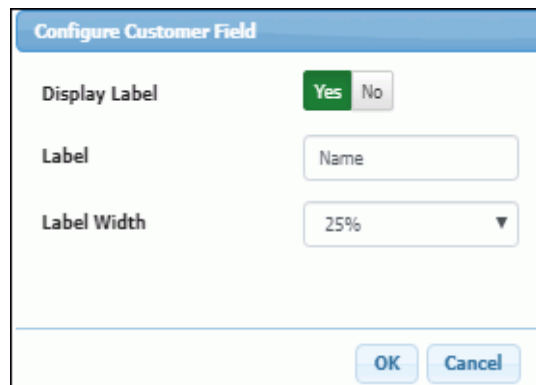
The Customer Details section will appear in the Rep Incident and Change Layout configuration screens as shown below.



The screenshot shows a configuration window titled "Customer Details". It contains three main sections: "Title" with a text input field containing "Customer"; "Display Avatar" with three radio buttons labeled "Left", "Right", and "No", where "Left" is selected; and "Display Microsoft® Skype/Lync® Status" with two radio buttons labeled "Yes" and "No", where "No" is selected. Below these is a dropdown menu labeled "Add a field". To the right is a list of available fields, each with a gear icon and a checkbox: "(Display Name)", "(Company)", "(Location)", "(Department)", "(Phone)", "(Email Address)", and "(Customer ID)".

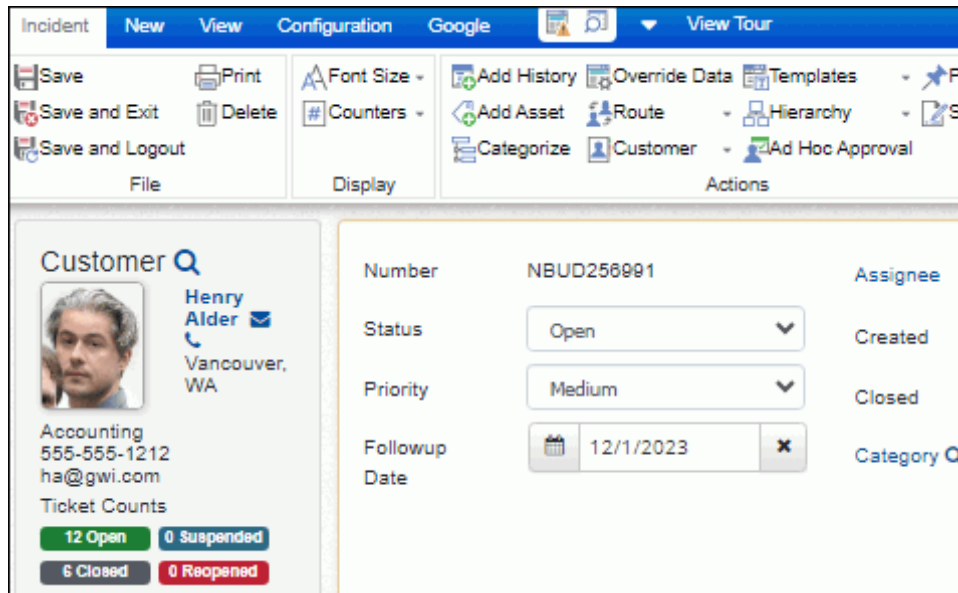
Use the **Title** field to customize the text to appear to the left of the search icon in the customer section; "Customer" will appear by default.

To include the customer's avatar (uploaded via the Customer Profile screen or the mySupport portal), select Left or Right in the **Display Avatar** field. Use the Add a Field dropdown to select the fields to appear in the upper left Customer area at the top of the Incident screen. After adding a field, select  Configure Field to enable or disable the field label, enter the field label, and select the field label width (which is a percentage of the column in which the field is included).



The screenshot shows a dialog box titled "Configure Customer Field". It has three rows of configuration options: "Display Label" with "Yes" and "No" radio buttons, where "Yes" is selected; "Label" with a text input field containing "Name"; and "Label Width" with a dropdown menu showing "25%". At the bottom right are "OK" and "Cancel" buttons.

Note that the **Ticket Counts** field will include Open, Closed, Suspended, and Reopened links in the Customer section of the Incident screen as shown in the example below.

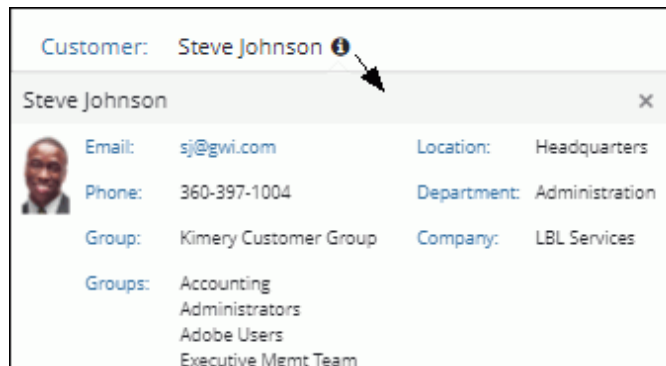


Use the **Display Microsoft® Skype/Lync® Status** field to include an icon that will display the Microsoft Skype/Lync status of a selected customer in the Incident and Change screens and enable the support representative to access Microsoft Skype/Lync functions. In order for the icon to appear, Microsoft Skype or Lync 2013 or later must be installed on your system, the support representative viewing the incident must be using Internet Explorer 10 or 11, and iSupport must be in the intranet or added to trusted sites.

### *mySupport Incident and Change Screens*

There are two methods to include fields for customer information on mySupport portals:

- The Customer field under the Basics section; this includes an information option next to the customer's name which will display a popup dialog as in the following example:





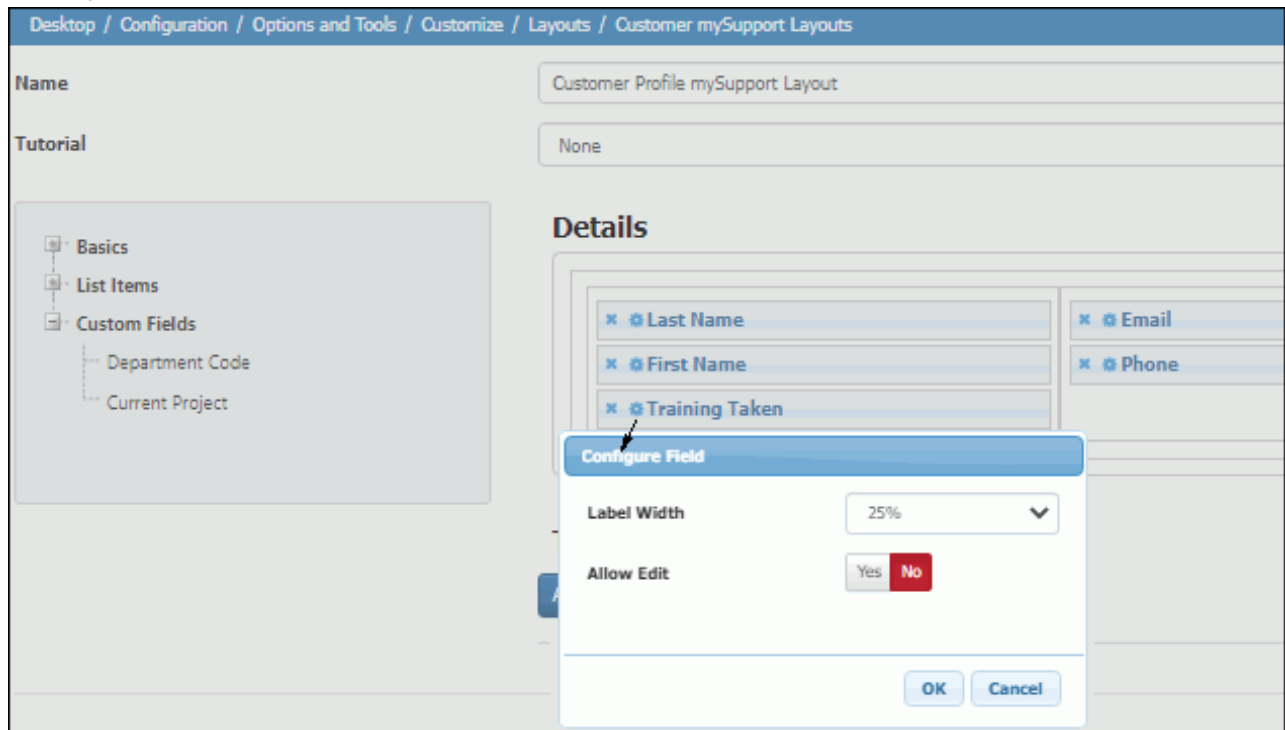
- Individual fields under the Customer Fields section

Customer Avatar:		Customer Group:	Customer Advisory Board
Customer First Name:	Steve	Customer Groups:	Adobe Users Customer Advisory Board Help Desk
Customer Last Name:	Johnson	Customer Department:	Administration
Customer Email:	<a href="mailto:sj@gwi.com">sj@gwi.com</a>	Customer Company:	LBL Services
Customer Phone:	360-397-1004		
Customer Location:	Headquarters		

Note that the Customer Group field will display the customer's primary group, and the Customer Groups field will display all of the groups in which the customer is a member.

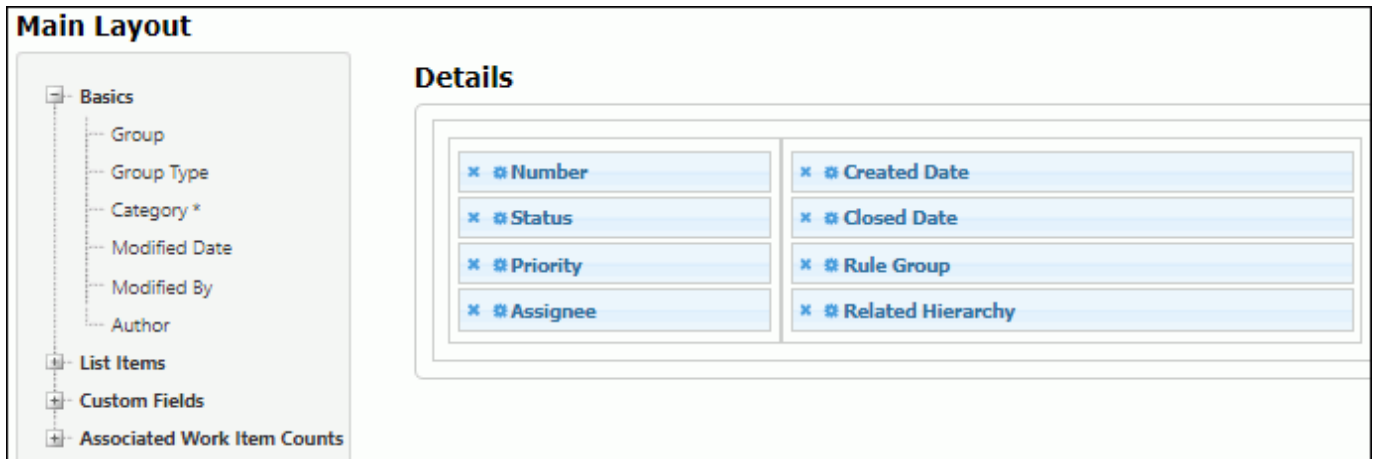
### *mySupport Customer Profile Custom Field Edit Access*

You can use the Allow Edit field on the Configure Field dialog for custom fields on mySupport display layouts to disable/enable an individual Customer Profile custom field to be edited by customers with the mySupport Custom Fields Editor permission.

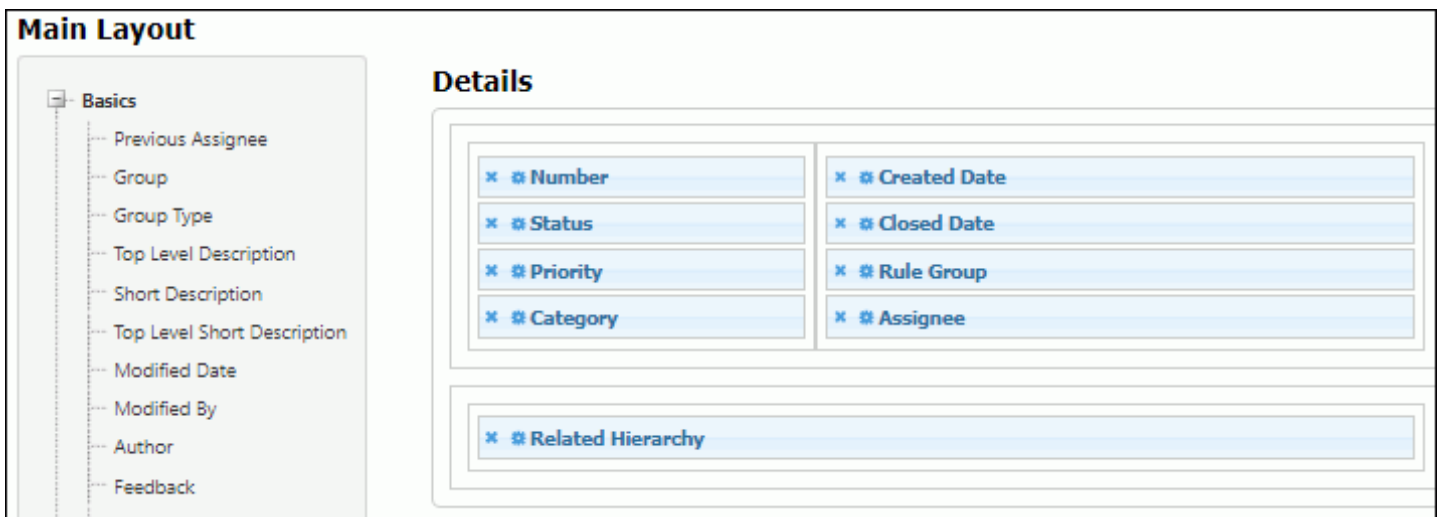


## Adding Fields and Tabs

To configure the Details section in the upper right section of the resulting screen, drag fields from the selector on the left to the middle of the Details area on the Layout screen. Required fields are designated with an asterisk in the selector on the left.

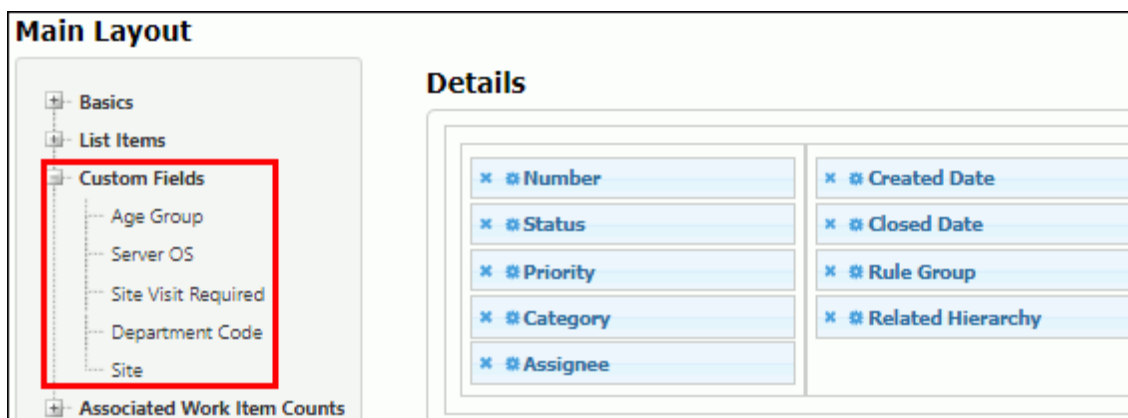



You can drag a field to the lower part of the Details section to create a subsection for a field.

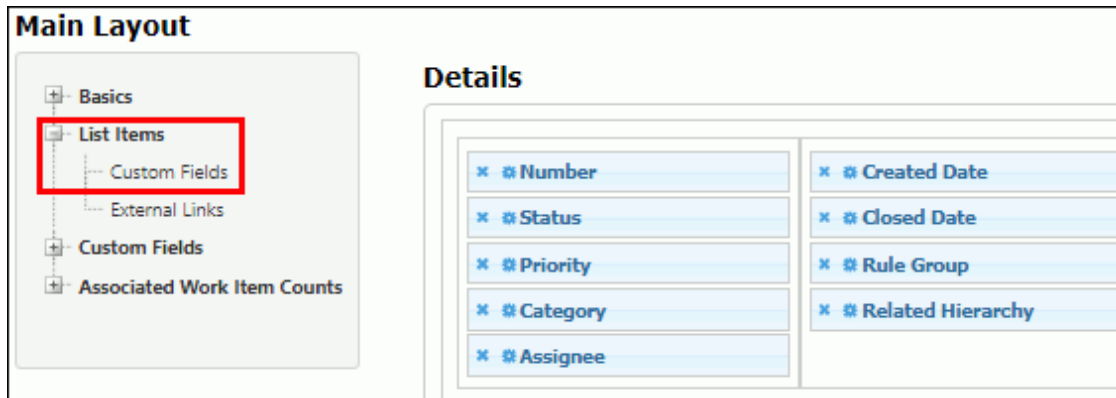


Global custom fields can be defined in the Custom Fields screen for the type of work item screen for which you're creating a layout, and additional custom fields can be defined for a category, asset type, or CI type. To include custom fields on a layout, you can:

- Drag the applicable global custom fields under the Custom Fields section individually:

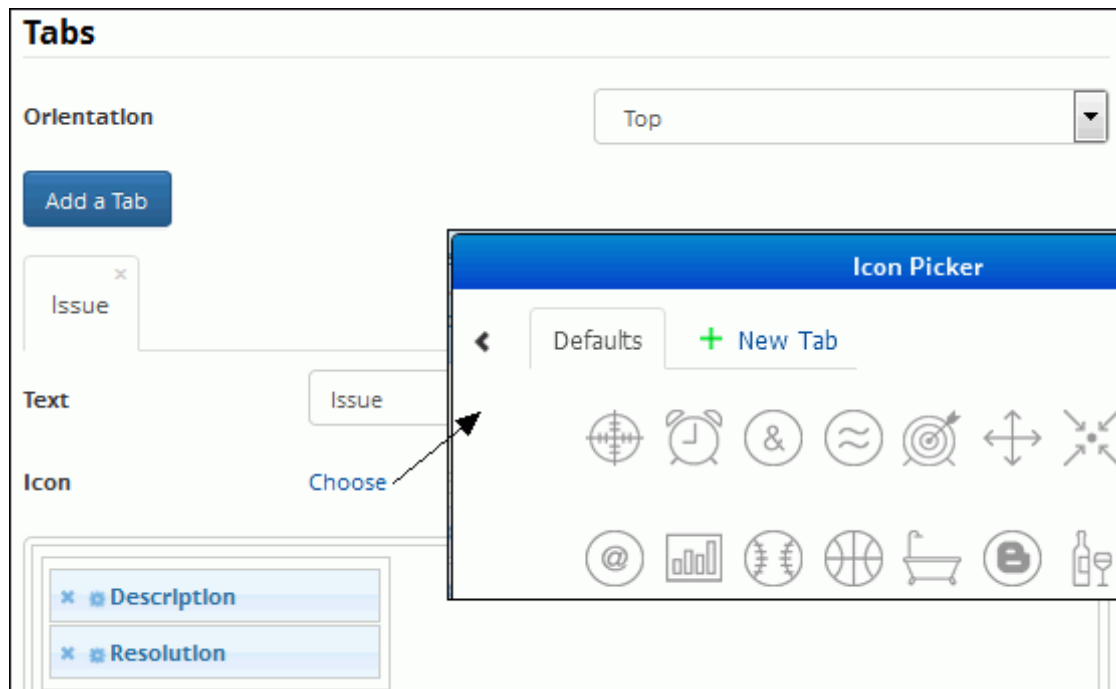


- Drag the Custom Fields field under the List Items section and then select  Configure Field to display the Configure Field dialog and select the types of custom fields to include: global custom fields, additionally defined custom fields, or both. See ["Configuring Fields" on page 28](#).

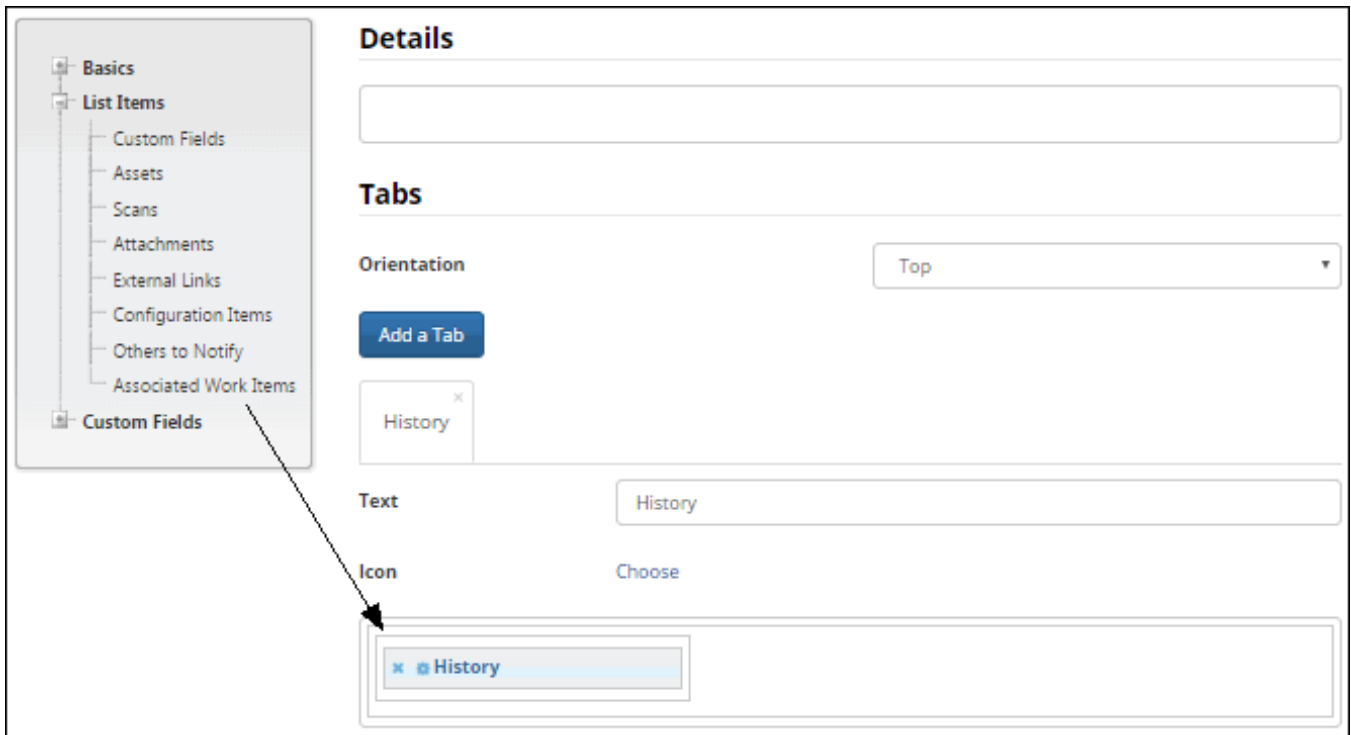


A **[Separator]** field is included for mySupport layouts; it will be blank after you drag it to the Details section or a tab. You can enter a label for it or leave it blank, and it can be used multiple times for adding blank areas to your layout. A Save Button option is included in Submit layouts; if you include it in your layout, the default Save button will still be retained at the top of the Submit screen.

Tabs can display in a row above fields or to the left of fields on the lower half of the resulting screen. To add a tab, select the Add a Tab button and then select on the new tab (named "Tab" by default). Use the Text field to enter the label for the tab. Select the Choose link in the Icon field to select a default or custom image to appear to the left of any text entered as a label. (If no text is entered, only the selected icon will appear.)




To add fields to the tab, drag fields from the selector on the left side of the Layout screen to the middle of the section below the Icon field.



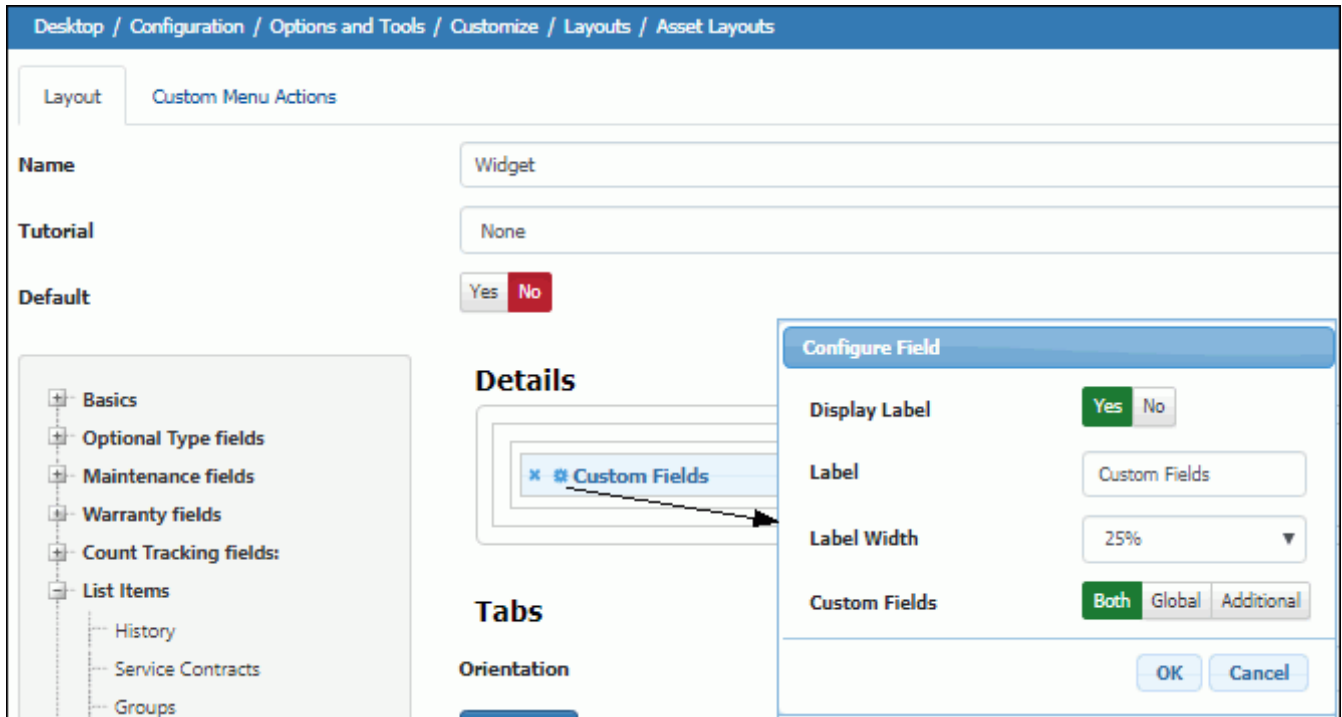
Note: The Description field is optional on mySupport incident submit layouts. The following text will be included in the Description field after submission: "Description field not included in <layout name> mySupport incident submit layout." If the layout is associated with a template, the description configured in the template, if any, will be used.

### *Configuring Fields*

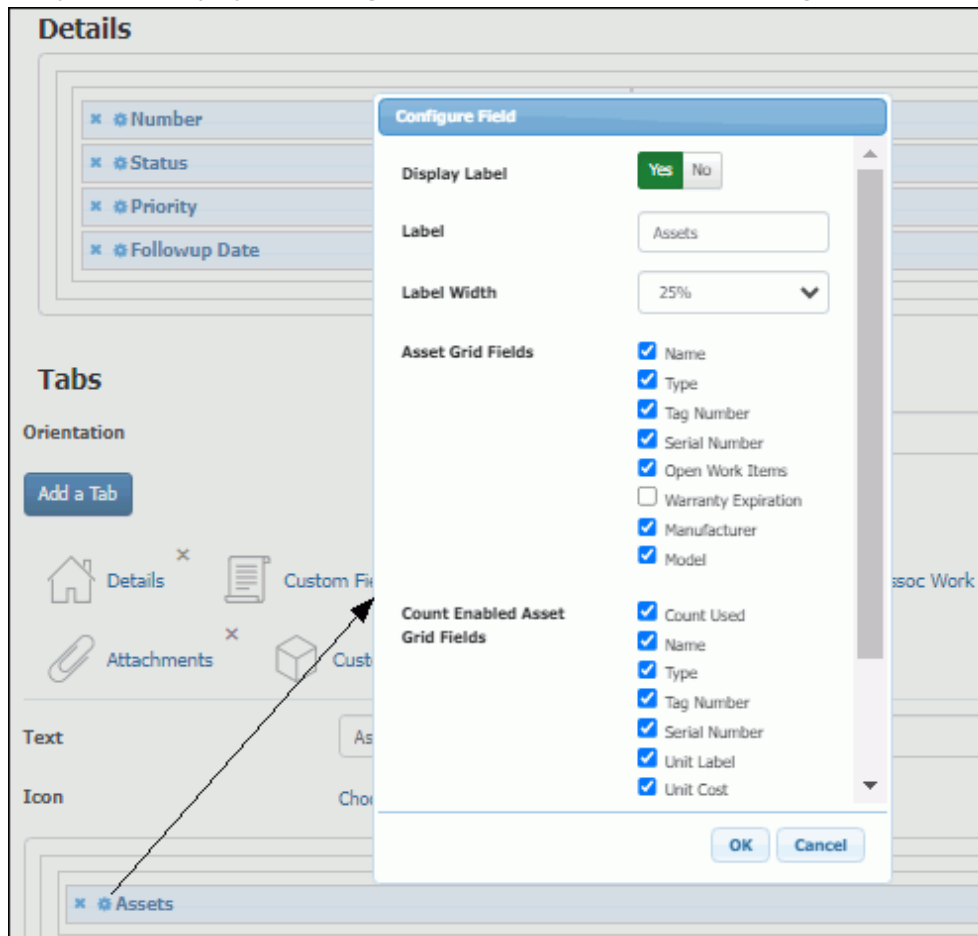
After adding a field, select  Configure Field to enable or disable the field label, enter the field label, and select the field label width (which is a percentage of the column in which the field is included). Note that the label width will not be applicable on list fields that display a label above the field.

Global custom fields can be defined in the Custom Fields screen for the type of work item screen for which you're creating a layout, and additional custom fields can be defined for a category, asset type, change type, CI type, and cost center. When you drag the **Custom Fields** field under the List Items section to include all of the custom fields at once, you can control which types of custom fields to include on layouts: global custom fields, additionally defined custom fields (defined for a category, asset type, CI type, change type, or cost center), or both. Note that all custom

fields that have met any conditional display conditions will be created upon mySupport work item submission regardless of whether they are included on a mySupport submission layout.



For work item layouts, you can display an asset grid for the Asset field via the Configure Field icon:



## mySupport Layouts

- Select Yes in the **Override Label** field to enter a field label that is different from the default. Note that this label will override any text that may be entered via the Resource Editor. See the online help for more information on the Resource Editor.

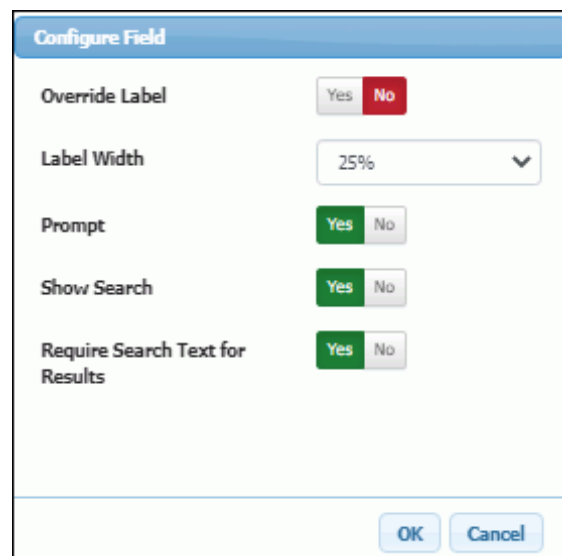


The 'Configure Field' dialog box shows the following settings:

- Display Label:** Yes (selected)
- Override Label:** Yes (selected)
- Label:** Case
- Label Width:** 25%

Buttons: OK, Cancel

- If configuring the **Category** field:

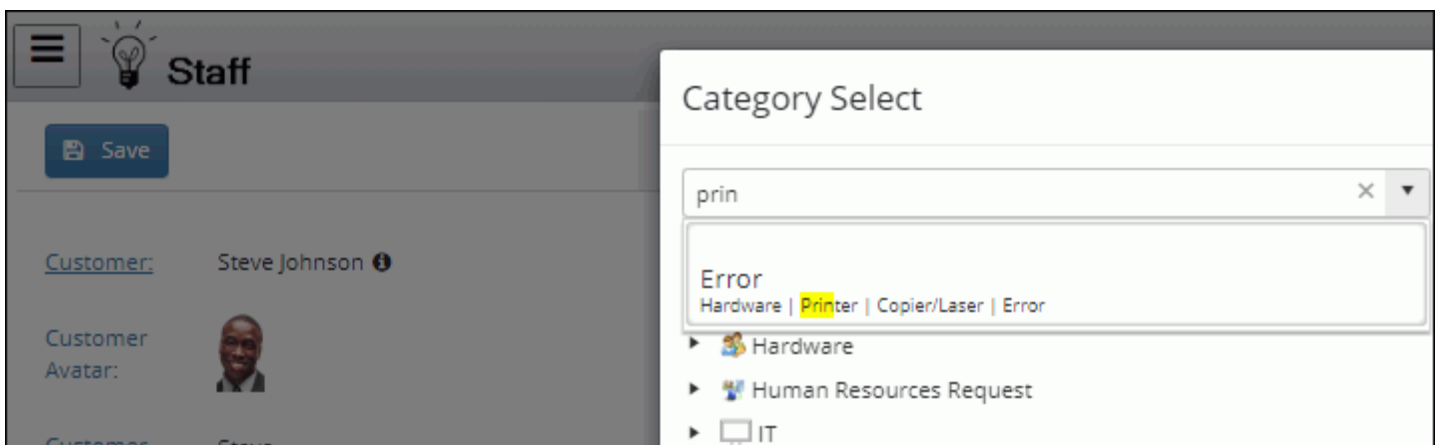


The 'Configure Field' dialog box shows the following settings:

- Override Label:** No (selected)
- Label Width:** 25%
- Prompt:** Yes (selected)
- Show Search:** Yes (selected)
- Require Search Text for Results:** Yes (selected)

Buttons: OK, Cancel

- Select Yes in the **Prompt** field to initially display the Category Select dialog when the Incident or Change Submit screen appears.
- Select Yes in the **Show Search** field to include a search field in the Category Select dialog.

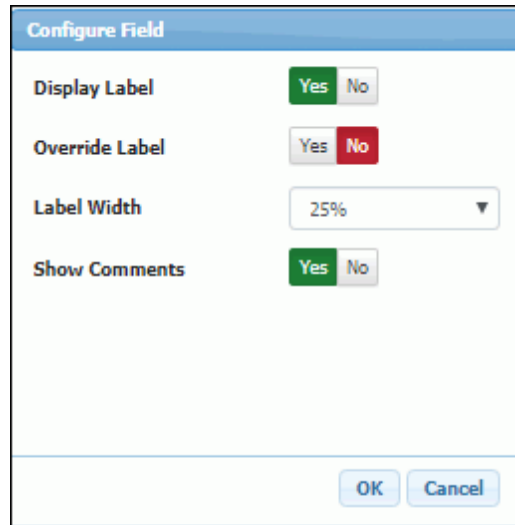


The screenshot shows the iSupport interface with the 'Category Select' dialog box open. The dialog box has a search input field containing 'prin' and a dropdown menu showing the following results:

- Error
- Hardware | Printer | Copier/Laser | Error
- ▶ Hardware
- ▶ Human Resources Request
- ▶ IT

- Select Yes in the **Require Search Text for Results** field to prevent display of the results until the user has started typing.

- If including the Assets list field, select Yes in the **Show Comments** field to control display of the Comments field that may be included (depending on the asset type).



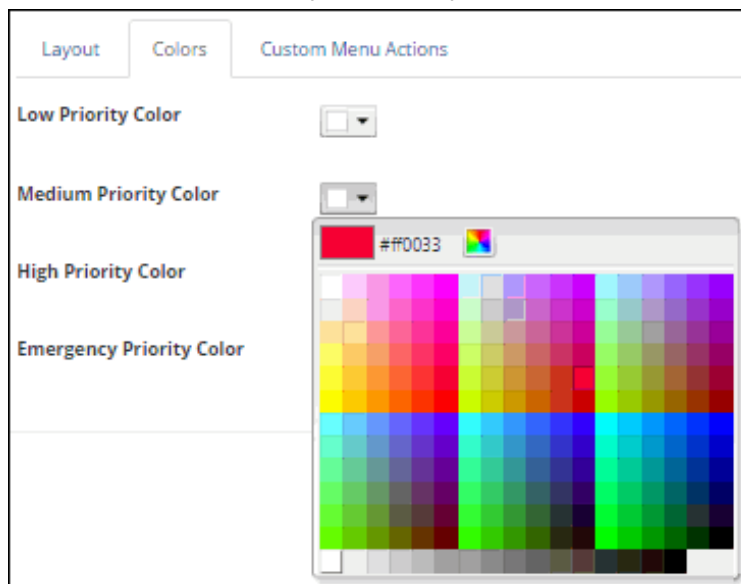
The 'Configure Field' dialog box contains the following settings:

Field Name	Value
Display Label	Yes
Override Label	No
Label Width	25%
Show Comments	Yes

Buttons: OK, Cancel

## Configuring Priority-Based Background Colors

Use the Colors tab to configure the priority-based background colors for the upper portion of the Incident, Problem, and Change screens. You can choose from the color picker or input an HTML color code.



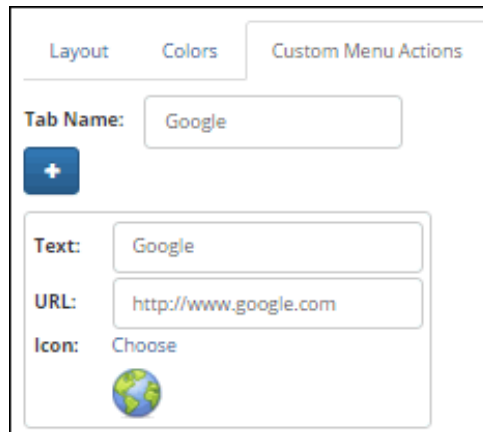
The 'Colors' configuration screen shows the following settings:

Priority	Color Selection
Low Priority Color	[Color Picker]
Medium Priority Color	[Color Picker]
High Priority Color	[Color Picker]
Emergency Priority Color	[Color Picker]

The color picker is currently open, showing a color grid and the selected color code: `##0033`.

## Configuring Custom Menu Actions

Use the Custom Menu Actions tab in the Layout screen to create a new tab, and link via an icon to a URL. Note that this tab and option will not appear in the work item screen until after the work item is saved because the URL will be generated with the work item ID appended to it.



Layout Colors Custom Menu Actions


Tab Name: Google

+

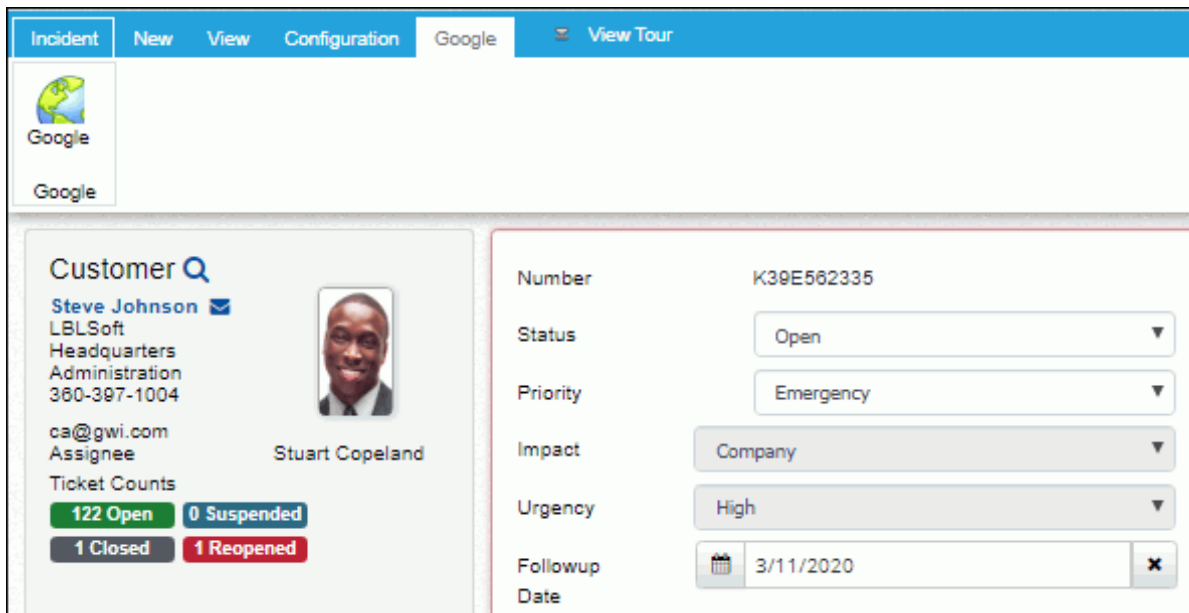
Text: Google

URL: http://www.google.com

Icon: Choose




Example:





Incident New View Configuration Google View Tour

Google

Google

Customer 

Steve Johnson  

LBLSoft  
Headquarters  
Administration  
360-397-1004

ca@gwi.com  
Assignee Stuart Copeland

Ticket Counts

122 Open 0 Suspended

1 Closed 1 Reopened

Number K39E562335

Status Open

Priority Emergency

Impact Company

Urgency High

Followup Date 3/11/2020

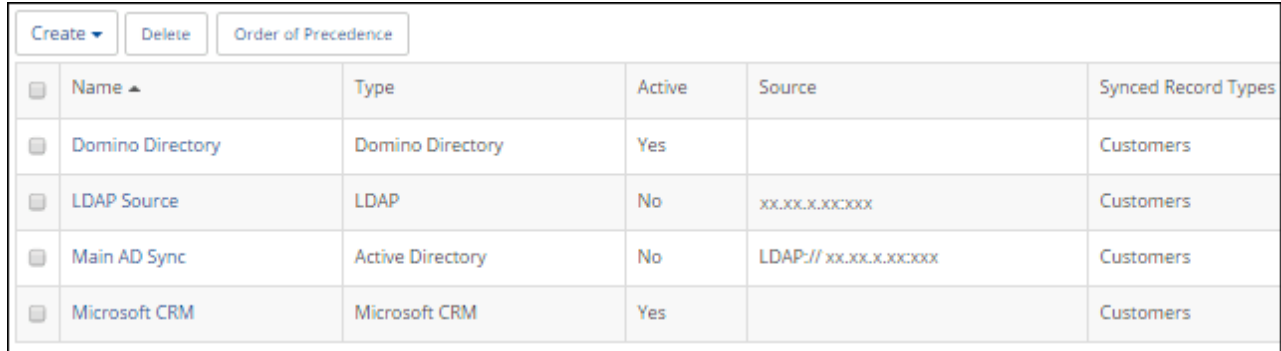


# Integrating With Data Sources

Use the Data Source Integration feature to utilize Active Directory, LDAP, or other relational databases as a source for iSupport's customer, asset, and support representative information. You can also import asset data from a .csv or Microsoft Excel .xlsx file; see [page 51](#) for more information.

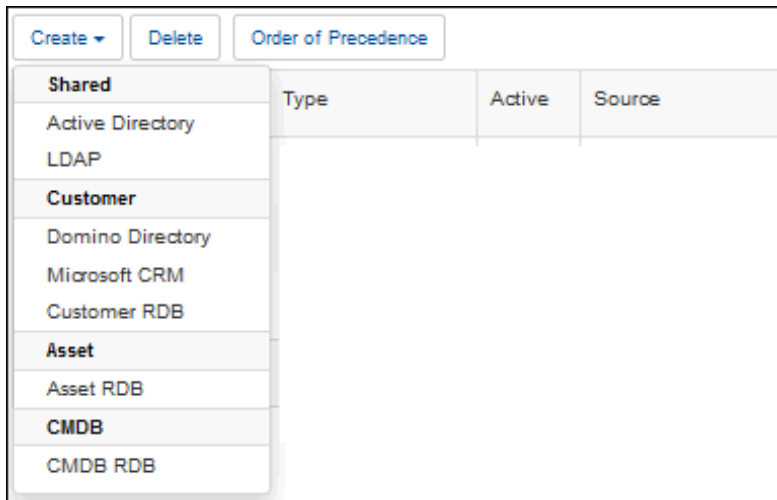
If utilizing multiple customer data sources, see ["Specifying Precedence for Multiple SQL Data Sources"](#) on [page 50](#).

To get started, select the Create link in the Options and Tools | Integrate | Data Source Integration screen.



<input type="checkbox"/>	Name ▲	Type	Active	Source	Synced Record Types
<input type="checkbox"/>	Domino Directory	Domino Directory	Yes		Customers
<input type="checkbox"/>	LDAP Source	LDAP	No	xx.xx.x.xx:xxx	Customers
<input type="checkbox"/>	Main AD Sync	Active Directory	No	LDAP://xx.xx.x.xx:xxx	Customers
<input type="checkbox"/>	Microsoft CRM	Microsoft CRM	Yes		Customers

Select the data source type.



See the following for information on specific data source types:

- Active Directory: see the next section.
- Asset RDB: [page 48](#)

## Integrating with Active Directory

The Active Directory Integration feature enables an agent that updates and synchronizes iSupport Customer Profile, Asset, and Support Representative Profile records with the information in one or more Active Directory sources.

You'll create a data source integration definition to specify the server and related settings, field mappings, and exclusions, and use sync definitions to specify the type of record you are synchronizing and the directory node and filters for the data to be synchronized. You can utilize both filtering and exclusions to specify the values that should not be synchronized; what you use will depend on how much you need to prevent from synchronizing for the level in the targeted source. You can also set default values based upon the AD sync setting entry from which a record was created. Exclusions target everything under a node in a directory and apply to all sync definitions of the same record type within a data source integration definition. Filters use syntax that can target multiple nodes in a tree, and apply to a specified base directory node in a sync definition.

The following occurs when the agent runs:

- If there is an entry in Active Directory that does not exist in the iSupport Customer Profile table, the entry is created in iSupport. In order for an entry to be added from Active Directory, it must contain a first name, last name, and email address. If mySupport access is configured, the Approved to Access mySupport field will be enabled on the automatically-created Customer Profile record.
- The first name, last name, and email address in Active Directory are compared with those values in Customer Profiles. If all of those values in an Active Directory record match all of those values in a directly entered Customer Profile, the Customer Profile record is updated with the latest information from Active Directory; if one of those values does not match, a new record is created in Customer Profiles. Therefore, more than one Customer Profile record will result if both contain one of the same values (for example, email address) but one or both of the other fields differ. For example, if there is a directly entered Customer Profile named Jon Smith with an email address jsmith@example.com and Active Directory has the rep listed with the name Jonathan Smith and the same email address of jsmith@example.com, the result will be two Customer Profile records with the same email address.
- If an entry is deleted in the Active Directory, the record will be flagged for deletion and:
  - If work items or assets are **not** associated with that name, the entry will be deleted from Customer Profiles when the Database Maintenance agent runs.
  - If work items or assets are associated with the name, the entry will remain flagged for deletion in Customer Profiles until those incident records no longer exist.

If a record in Active Directory has a value in the Manager field and an existing Customer Profile record contains that manager, the manager will be inserted in the Approver field in the Customer Profile record; otherwise, the Approver field will be blank.

**Note:** If a Customer Profile record has been synchronized with Active Directory, the synchronized fields (except for Secondary User Name) cannot be edited in the Customer Profiles screen. These fields can only be edited via Active Directory.

When the feature is enabled, the agent runs immediately and then as specified according to the configured interval. Note that the Active Directory Integration feature does not modify the contents in Active Directory in any way.

## Basics

Use the Basics tab to specify the primary connection and authentication details for accessing the data source; these settings will apply to all of the sync definitions you create for that data source.

Desktop / Configuration / Options and Tools / Integrate / Data Source Integration

The Active Directory Integration feature allows you to utilize Active Directory as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics >

Sync Definitions

Field Mappings

Exclusions

AD Source Name: Main AD Sync

Search Root: LDAP://xxx.xxx.com:636

Domain Controller: xxx-xx-xx

Connect As: Anonymous Specified User

Username: xxx\xxxxxxxxxx

Password: Reset

Test Connection

Active: On Off

Synchronization Interval: Daily 2:00 AM

**AD Source Name** - Enter a name for the AD source definition. This name will appear in the Source field in the associated Customer Profile record.

**Search Root** - Enter the directory server machine name or IP address for querying user information in the Active Directory source; precede your entry with the following: LDAP://

**Connect As** - Select Anonymous to connect to the data source as an anonymous user or Specified User to enter a login for connecting to the data source.

**Username/Password** - If anonymous Active Directory connections are not allowed in your environment, use these optional fields to enter a username and password for authentication when queries are performed. If anonymous connections are allowed, leave these fields blank.

**Active** - Select Yes to enable the Active Directory Integration agent that updates the records in iSupport with the information in Active Directory. The agent runs immediately and then continues to run as scheduled in the AD Synchronization Interval field.

**AD Synchronization Interval** - Select the amount of time in the interval for the synchronization to be performed.

### Configuring a Sync Definition

Use the Sync Definition section to select the type of record that you are synchronizing, select the directory node that contains the data to be synchronized, and enter a search filter if applicable. Select the Create link to create a sync definition.

The Active Directory Integration feature allows you to utilize Active Directory as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

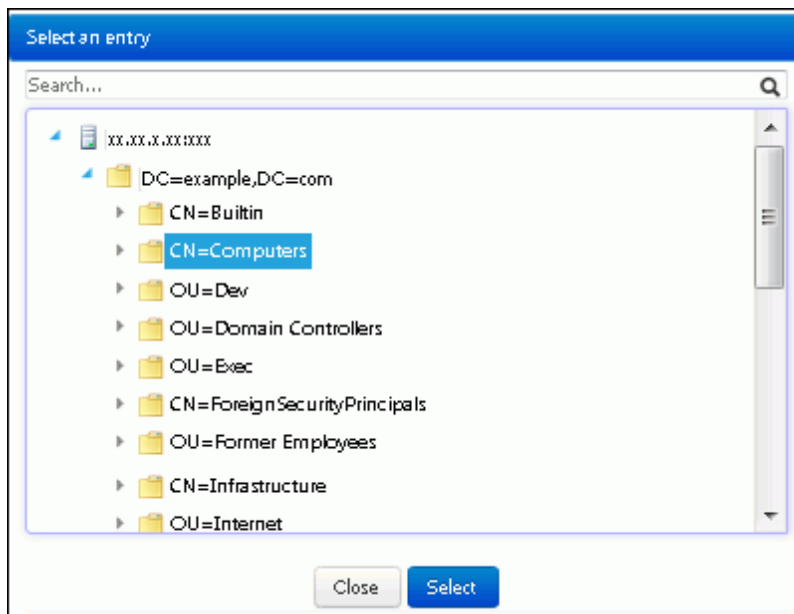
Basics	Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Sync Definitions</b> >	Sync Entries As	Assets
Field Mappings	Default Type	Desktop + / edit
Exclusions	Base DN	CN=Computers,DC=example,DC=com
	Search Filter	(& (objectCategory=Computer))

**Active** - Select Yes to enable the sync definition.

**Sync Entries As** - Select the type of record that you are synchronizing: Customer Profile. The **Enable mySupport Access** field will appear; select Yes to enable the Approved to Access mySupport field by default. If a login name and password exists in the Active Directory record, it will be included in the mySupport login fields for authentication to the mySupport portal. This is not a mapped or synchronized value; it can be edited in iSupport.

This feature utilizes LDAP (Light Weight Directory Access Protocol), which defines how information can be accessed in directories. Active Directory supports the LDAP search filter syntax as specified in RFC 1960. For information on LDAP and search filters, see <http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx#Examples>.

**Base DN** - Select this button to select the node in the directory server that contains the data to be synchronized.



**Search Filter** - Enter the conditions that must be met for returning a specific set of information to iSupport. Note that a filter is only needed if the selected Base DN contains unwanted lower level nodes or if the data source's exclusions do not already remove the unwanted nodes.

#### Examples

- All users that contain a first and last name:

```
(&
(objectCategory=Person)
(objectClass=user)
(givenName=*)
(sn=*)
)
```

- All users that contain a first and last name excluding Tom Jones and SQL Account:

```
(&
(objectCategory=Person)
(objectClass=user)
(givenName=*)
(sn=*)
(!name =Tom Jones)
(!name=SQL Account)
)
```

- All users and contacts that contain a first and last name:

```
(&
(objectCategory=Person)
(givenName=*)
(sn=*)
(|
(objectClass=user)
(objectClass=contact)
)
```

- )
  - All users and contacts that contain a first and last name, excluding Tom Jones, Barry White, and SQL Account:
 




```
(
(objectCategory=Person)
(|
(objectClass=user)
(objectClass=contact)
)
(givenName=*)
(sn=*)
(!name =Tom Jones)
(!name=SQL Account)
(!name =Barry White)
)
```
  - All users with a valid Microsoft Windows user name (*domainname\username*):
 

```
(
(objectCategory=Person)
(objectClass=user)
(givenName=*)
(sn=*)
(userPrincipalName=*@*)
(samAccountName=*)
)
```

### Setting Default Values

Use the Default Values section to set Asset field values based upon the AD sync setting entry from which a record was created. For example, if AD assets are organized into a specific OU or group that indicates other properties (such as location) and if the AD records don't have the location attribute populated in the directory, you can simply add a default value for the location field to the sync setting entry that is linked to the OU or group.

In the Force column, select Yes if you wish to have the configured default value override the AD value in cases where the attribute was populated in the source. If the Force field is set to No, the default value will only be applied if the AD attribute is either unmapped or has no value on the record.

Default Values			
	Field	Value	Force? 
	Manufacturer	<input type="text" value="Acme"/>	<input type="button" value="Yes"/> <input type="button" value="No"/>
	Location	<input type="text" value="Vancouver, WA"/>	<input checked="" type="button" value="Yes"/> <input type="button" value="No"/>

## Field Mappings

Use the subtabs to specify the attributes in your Active Directory source from which data will be pulled for corresponding iSupport fields.

The screenshot shows the 'Field Mappings' configuration page for Active Directory integration. The page title is 'The Active Directory Integration feature allows you to utilize Active Directory as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)'. The left sidebar contains navigation tabs: 'Basics', 'Sync Definitions', 'Field Mappings' (selected), and 'Exclusions'. The main content area has sub-tabs for 'Customer', 'Support Rep', and 'Asset'. Below these is a table with columns 'Field' and 'Attribute'. The 'Name' field is mapped to 'Use iSupport Default' and the 'Sync Key' field is also mapped to 'Use iSupport Default'. A search icon is visible in the top right corner of the main content area.

Mapping options include:

- Use iSupport Default which populates the default mapping; see the data map on [page 46](#) for the attributes used by default by iSupport. Note that we recommend that you use iSupport's default for the Sync Key and Avatar field because the applicable schema property may vary depending on your version of Active Directory. If iSupport Default is selected for the Groups field, all groups associated with a customer will be created via the MemberOf attribute.
- An applicable schema property. Defaults appear in the dropdown; to add an attribute, enter its exact name and it will be retained in the list.
- [Unmapped] which will enable entry in the field. Note that the First Name, Last Name, Email, Sync Key, and Login fields cannot be left unmapped for customers.

Use the Sync Key field to map to a value that is an unchanging unique identifier field in the source database.

To assign a primary group to multiple iSupport Customer Profile records, select a customer view on the Desktop and then select Add to Group on the Actions menu.

Use the Map a Custom Field button to select a custom field to add to the list of fields to be mapped.

The Active Directory Integration feature allows you to utilize Active Directory as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics Customer Support Rep Asset

Sync Definitions

Field Mappings >

Exclusions

Field	Attribute
First Name	Use iSupport Default
Last Name	Use iSupport Default
Email	Use iSupport Default
Sync Key	Use iSupport Default
Phone	Use iSupport Default
Fax	Use iSupport Default
Cell	Use iSupport Default
Location	Use iSupport Default
Department	Use iSupport Default
Title	Use iSupport Default
Login	Use iSupport Default
Secondary Login	Use iSupport Default
Address	Use iSupport Default
City	Use iSupport Default
Avatar	[Unmapped]

Dialog - Select Custom Field - M...

Search...

Search within results

Sort by (Label ▲ | Type | Pending Deletion | DefaultValue | Options)

Training Taken

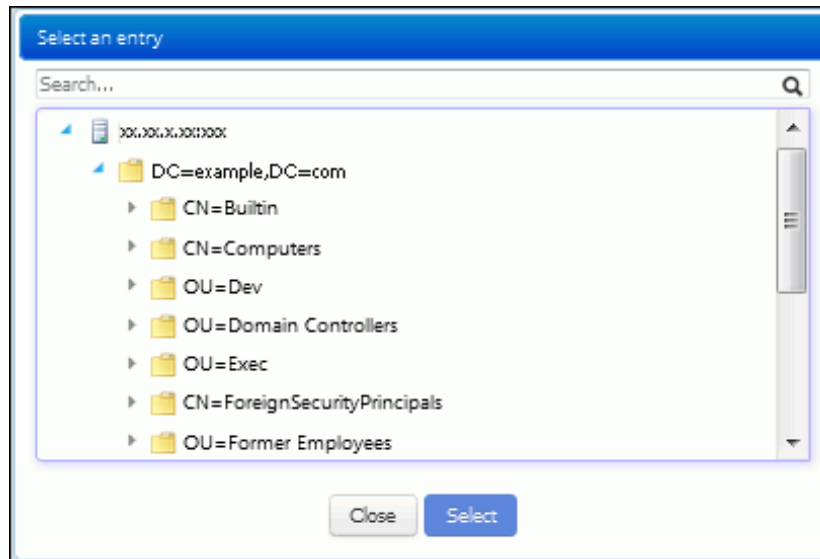
Type: List Box Category: Pending Deletion: False

Default Value:

Options: Accounting,Sales,Administration

Map a Custom Field

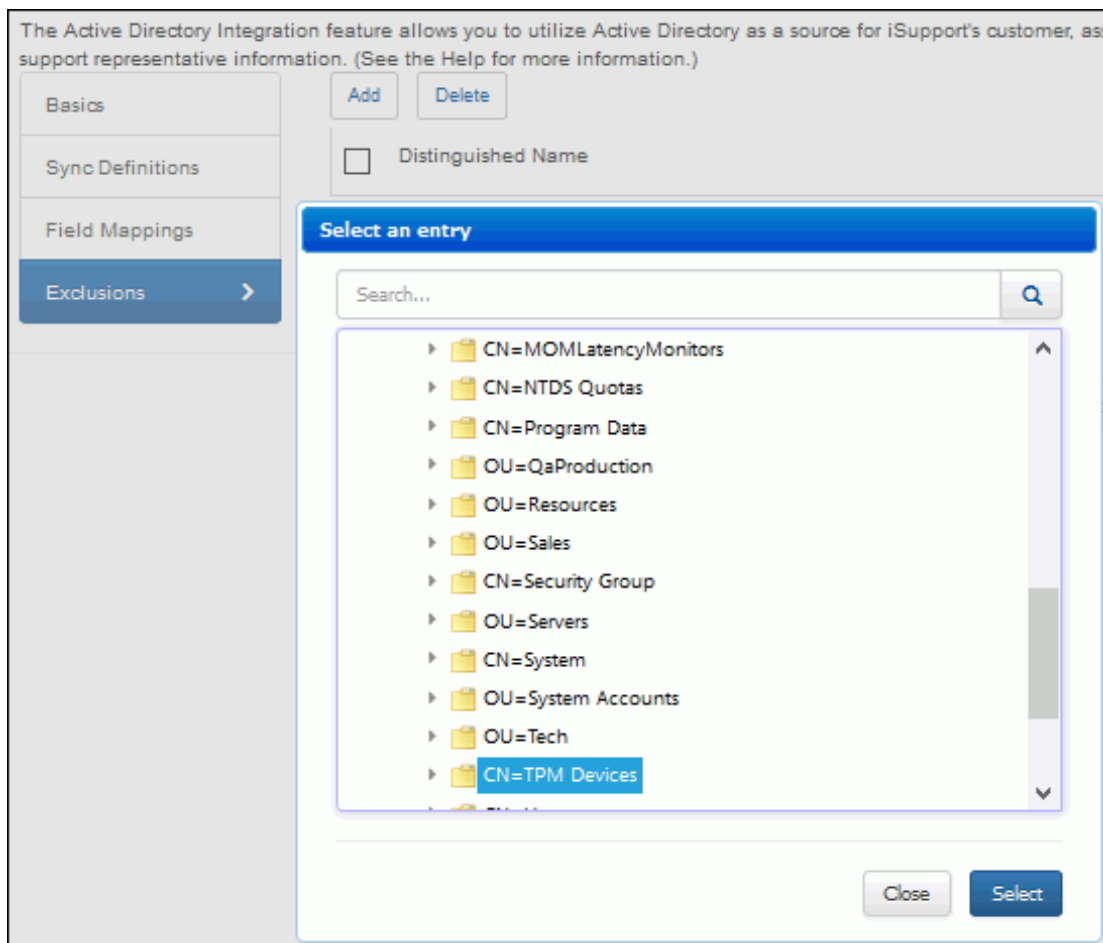
Use the Preview  button to select a record to use for verifying your selections.



Values from the record will appear next to the fields.

### *Configuring Exclusions*

Use the Exclusions tab to specify the nodes or directory objects that should not be synchronized; select the Add link to select the directory nodes or objects that should be excluded. All lower level nodes will also be excluded. Note that exclusions apply to all sync definitions of the same record type within a data source integration definition.





## Integrating with LDAP

The LDAP Integration feature enables an agent that updates and synchronizes iSupport Customer Profile records with the information in one or more LDAP sources.

You'll create a data source integration definition to specify the server and related settings, field mappings, and exclusions, and use sync definitions to specify the type of record you are synchronizing and the directory node and filters for the data to be synchronized. You can utilize both filtering and exclusions to specify the values that should not be synchronized; what you use will depend on how much you need to prevent from synchronizing for the level in the targeted source. Exclusions target everything under a node in a directory and apply to all sync definitions of the same record type within a data source integration definition. Filters use syntax that can target multiple nodes in a tree, and apply to a specified base directory node in a sync definition.

The following occurs when the agent runs:

- If there is an entry in LDAP that does not exist in the Customer Profile iSupport table, the entry is created in iSupport. In order for an entry to be added from LDAP, it must contain a first name, last name, and email address. If mySupport access is configured, the Approved to Access mySupport field will be enabled on the automatically-created Customer Profile record.

If a Windows login name exists in the LDAP record, it will be included in the mySupport User Name field for authentication to the mySupport portal. You'll need to disable LDAP integration in order to enter or change the password for accessing the mySupport portal. The password will not be changed by re-enabling LDAP integration.

- If an email address matches an email address in Customer Profiles and the record was directly entered via Customer Profiles, depending on the configured order of precedence, the Customer Profiles record is updated with the latest information from LDAP.
- If an entry is deleted in the LDAP, the record will be flagged for deletion and:
  - If work items or assets are **not** associated with that name, the entry will be deleted from Customer Profiles when the Database Maintenance agent runs.
  - If work items or assets are associated with the name, the entry will remain flagged for deletion in Customer Profiles until those incident records no longer exist.

When the feature is enabled, the agent runs immediately and then as specified according to the selection in the LDAP Synchronization field. The LDAP Integration feature does not modify the contents in the LDAP source in any way.

Go to the following links for more information:

- <http://www.rfc-archive.org/getrfc.php?rfc=3377> - Top level LDAPv3 Technical specs
- <http://www.rfc-archive.org/getrfc.php?rfc=2254> - Search Filters (with examples)
- <http://www.rfc-archive.org/getrfc.php?rfc=2255> - URL formats (examples for Search Root field)
- <http://www.rfc-archive.org/getrfc.php?rfc=2256> - User Schema (standard available attributes, useful for mapping)

## Configuring Basics

Use the Basics tab to specify the primary connection and authentication details for accessing the data source; these settings will apply to all of the sync definitions you create for that data source.

The screenshot shows the 'Data Source Integration' configuration page for LDAP. The breadcrumb trail is 'Desktop / Configuration / Options and Tools / Integrate / Data Source Integration'. A help message states: 'The LDAP Integration feature allows you to utilize LDAP as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)'. On the left, a sidebar contains four tabs: 'Basics' (selected), 'Sync Definitions', 'Field Mappings', and 'Exclusions'. The main configuration area includes the following fields and controls:

- LDAP Source Name:** Text input field containing 'LDAP Data Source'.
- Server:** Text input field containing 'LDAP://xx.xx.x.xxx'.
- Domain Controller:** Text input field containing 'FAB-DC-01' with a help icon.
- Use SSL:** Toggle switch with 'On' and 'Off' options; 'Off' is selected.
- Connect As:** Radio buttons for 'Anonymous' and 'Specified User'; 'Specified User' is selected.
- Username:** Text input field containing 'xx\back'.
- Password:** Password input field with masked characters.
- Test Connection:** Button.
- Active:** Toggle switch with 'On' and 'Off' options; 'On' is selected.
- Synchronization Interval:** Dropdown menu set to '15 minutes'.

**LDAP Source Name** - Enter a name for the LDAP source definition. This name will appear in the Source field in the associated Customer Profile record.

**Server** - Enter the server on which the source entries are located.

**Use SSL** - SSL is an encryption method that overlays the connection between the cSupport server and the LDAP source server. Select Yes if SSL encryption is enabled on the LDAP source server. Use the Test Connection link to verify access.

**Active** - Select Yes to enable the agent that updates the applicable records in iSupport with the information in the LDAP source. The agent runs immediately and then continues to run as scheduled in the LDAP Synchronization Interval field.

**LDAP Synchronization Interval** - Select the amount of time in the interval for the synchronization to be performed.

**Username/Password** - If anonymous connections are not allowed in your environment, use these optional fields to enter a username and password for authentication when queries are performed. If anonymous connections are allowed, leave these fields blank.

Use the fully qualified Distinguished Name for best results. If accessing a server hosting an Active Directory installation, it will work with several formats. For example, if the user name is lbladmin and it is in the lbl domain, you could enter lbladmin, lbl\lbladmin, lbladmin@lbl.soft.com. All of these entries would work, but you could also enter the full Distinguished Name for the lbladmin user account (cn=lbladmin,cn=users,dc=lbl,dc=soft,dc=com). Note that if you are connecting to a non-AD server like E-directory, the Username field must contain the fully qualified Distinguished Name.

## Configuring a Sync Definition

Use the Sync Definition section to select the type of record that you are synchronizing, select the directory node that contains the data to be synchronized, and enter a search filter if applicable.

The LDAP Integration feature allows you to utilize LDAP as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

Basics	Active	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<b>Sync Definitions</b>	Sync Entries As	Assets
Field Mappings	Default Type	Laptop
Exclusions	Base DN	OU=Machine,o=sevenSeas
	Search Filter	(objectclass=dcObject)

**Active** - Select Yes to enable the sync definition.

**Sync Entries As** - Select the type of record that you are synchronizing: Customer Profile. When synchronization occurs, the record will be created if there is an entry in the LDAP source that does not exist in iSupport. The **Enable mySupport Access** field will appear; select Yes to enable the Approved to Access mySupport field by default. If a login name and password exists in the LDAP source record, it will be included in the mySupport login fields for authentication to the mySupport portal. This is not a mapped or synchronized value; it can be edited in iSupport.

This feature utilizes LDAP (Light Weight Directory Access Protocol), which defines how information can be accessed in directories. Active Directory supports the LDAP search filter syntax as specified in RFC 1960. For information on LDAP and search filters, see <http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx#Examples>.

**Base DN** - Select this button to select the directory node that contains the data to be synchronized.

**Search Filter** - Enter the conditions that must be met for returning a specific set of information to iSupport. Note that a filter is only needed if the selected Base DN contains unwanted lower level nodes or if the data source's exclusions do not already remove the unwanted nodes.

## Setting Default Values

Use the Default Values section to set Asset field values based upon the LDAP sync setting entry from which a record was created. For example, if LDAP assets are organized into a specific OU or group that indicates other properties (such as location) and if the LDAP records don't have the location attribute populated in the directory, you can simply add a default value for the location field to the sync setting entry that is linked to the OU or group.

In the Force column, select Yes if you wish to have the configured default value override the LDAP value in cases where the attribute was populated in the source. If the Force field is set to No, the default value will only be applied if the LDAP attribute is either unmapped or has no value on the record.

Default Values			
	Field	Value	Force? ⓘ
	Manufacturer	Acme	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
	Location	Vancouver, WA	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

## Field Mappings

Use the Asset subtab under the Field Mappings tab to specify the attributes in your LDAP source from which data will be pulled for corresponding iSupport fields.

The LDAP Integration feature allows you to utilize LDAP as a source for iSupport's customer, asset, or support representative information. (See the Help for more information.)

	Customer	Support Rep	Asset
Basics			
Sync Definitions			
<b>Field Mappings</b>			
Exclusions			

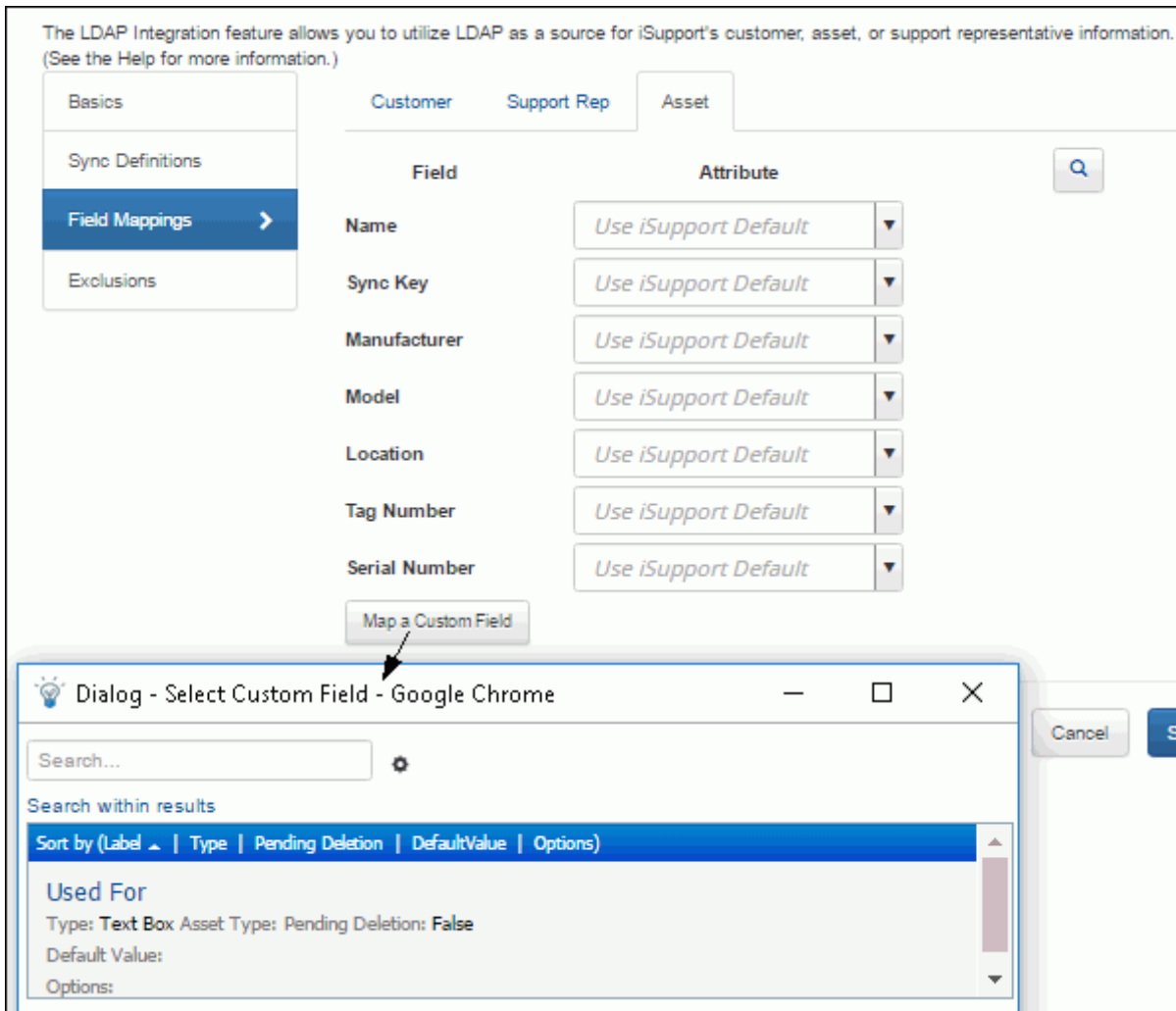
Field	Attribute	
Name	<input type="text" value="Use iSupport Default"/>	▼
Sync Key	<input type="text" value="Use iSupport Default"/>	▼


Mapping options include:

- Use iSupport Default which populates the default mapping; see the data map on [page 46](#) for the attributes used by default by iSupport. Note that we recommend that you use iSupport's default for the Sync Key and Avatar fields because the applicable schema property may vary depending on your version of LDAP.
- An applicable schema property (selected via the dropdown)
- [Unmapped] which will enable entry in the field. Note that the First Name, Last Name, Email, Sync Key, and Login fields cannot be left unmapped.

Use the Sync Key field to map to a value that is an unchanging unique identifier field in the source database.

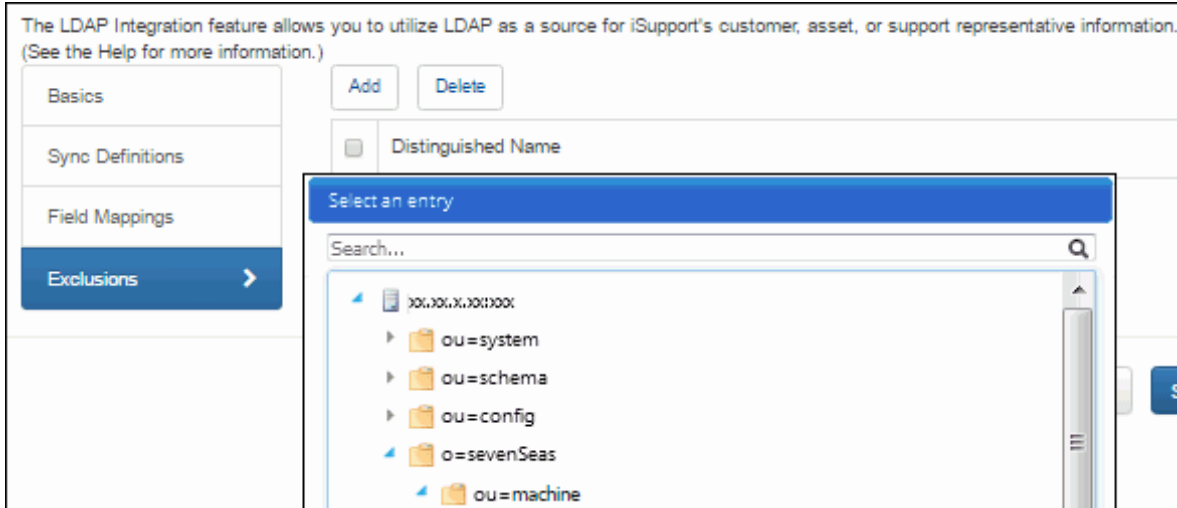
Use the Map a Custom Field button at the bottom of the screen to select a custom field to add to the list of fields to be mapped.



Use the Preview  button to select a record to use for verifying your selections. Values from the record will appear next to the fields.

## Configuring Exclusions

Use the Exclusions tab to specify the values that should not be synchronized; select the Add link to select the directory nodes or objects that should be excluded. All lower level nodes will also be excluded. Note that exclusions apply to all sync definitions within a data source integration definition.



## Active Directory/LDAP Integration Data Map

The Active Directory and LDAP Integration features map according to the following schema:

### Customers

iSupport Customer Field	iSupport Default
First Name	givenName
Last Name	sn
Email	mail
Sync Key	objectGUID - if unavailable: entryUUID and uuid
Phone	telephoneNumber
Fax	facsimileTelephoneNumber
Cellular	mobile
Location	physicalDeliveryOfficeName
Department	department
Title	title
Login	userPrincipalName - if unavailable: samAccountName, UID, and then mail property
Secondary Login	The initial synchronization process will populate the Secondary User Name field if the iSupport Services user account is a domain level user account. It is approximated by retrieving the text between the @ symbol and the next period from the user's principal name and converting it to upper case (for example, LBLSOFT would be retrieved from john@lblsoft.com) and adding a backslash, and then retrieving the <i>username</i> portion from the samAccountName field of an AD user entry.
Address	streetAddress (multiline value; first line used for Address1, any second line will be used for Address2, any third line will be used for Address3)
City	l
State	st

<b>iSupport Customer Field</b>	<b>iSupport Default</b>
ZIP	postalCode
Country	co
Manager	manager
Company	company
Customer ID	<i>(unmapped)</i>
Group	MemberOf
Avatar	jpegPhoto - if unavailable: thumbnailPhoto

## Importing From a Remote Asset Database and Synchronizing

Select Asset RDB on the Data Source Integration Create menu to import asset data from one or more Microsoft SQL Server source databases into iSupport's Asset database, and synchronize with those source databases on an interval basis. You'll enter a connection string and SQL query, and then select the Test button to display columns in the source database on the Field Mappings tab for specific field mapping options. You can schedule synchronization to occur on an interval basis. If a matching field exists in the source database, the record will be updated in iSupport's Asset database.

Use the Basics tab to specify the connection string, SQL query, authentication information, and synchronization interval.

The screenshot shows the 'Basics' tab of the 'Asset Integration Definition' configuration form. The form includes the following fields and controls:

- Name:** Asset Integration Definition
- Connection String:** Server=server.xxx.com; database=active\_assets; trusted connection=yes
- SQL Query:** Select \* from rdbassetsource
- Authentication:** Windows (selected), SQL Server
- Username:** XXXAdmin
- Password:** [Masked with dots]
- Test Connection:** Button
- Active:** On (selected), Off
- Interval:** 15 minutes

**Microsoft SQL Server Source Name** - Enter a name for the SQL Server source definition. This name will appear in the list of integration definitions and in the Source field in the associated Asset record.

**Connection String** - Enter the connection string for accessing the source database.

**SQL Query** - Enter the SQL query string for accessing the asset-specific SQL columns in the source database. Select the Test Query button to populate the SQL Columns field on the Field Mappings tab.

**Authentication/Username/Password** - Select the type of authentication to be used to access the source SQL Server database: Windows Authentication or SQL Server Authentication. If using SQL Server authentication, enter the user name and password for accessing the server. If using Windows Authentication, the database must have both of the iSupport user IDs listed, with the db\_owner and public roles.

**Active** - Select Yes to enable the Asset Synchronization agent that updates the records in the iSupport Asset database with the information in the SQL source database.

**Asset Synchronization Interval** - Select the number of minutes in the interval for the synchronization to be performed.



## Specifying Field Mappings

When the query connection is successful, use the Field Mappings tab to specify options for mapping the fields in the source database to the fields in the iSupport Asset database.

The screenshot shows the 'Field Mappings' configuration window. On the left, a sidebar has 'Field Mappings' selected. The main area is titled 'Refresh Columns'. It contains the following settings:

- Asset Name Column from Source Database:** A dropdown menu with 'NAME' selected.
- Attempt Asset Type Mapping:** A toggle switch set to 'On'.
- Asset Type Column from Source Database:** A dropdown menu with 'ID\_TYPE' selected.
- Attempt Asset Owner Mapping:** A toggle switch set to 'Off'.
- Default Owner:** A text field containing 'Unassigned'.

Below these settings are two tabs: 'Standard Fields' and 'Custom Fields'. Under 'Standard Fields', there are three columns:

- SQL Columns:** A list of columns from the source database: GUID, ID\_TYPE, ID\_INVENTORY, LOCATION, DT\_PURCHASE, DT\_WAR\_END, DT\_MAINT\_EN, COMMENTS, NAME, BEARING\_DEFL.
- iSupport Columns:** A list of columns from the iSupport database: LOCATION, DT\_PURCHASE, DT\_WAR\_END, DT\_MAINT\_EN, UNIT\_COUNT, ITEM\_COST\_PI, UNIT\_LABEL.
- Mapping:** A list of mappings: ID -> SYNC\_KEY, MFG -> MFG, MODEL -> MODEL, TAG\_NUMBER -> TAG\_NUMBER, SERIAL\_NUMBER -> SERIAL\_NU.

**Asset Name Column from Source Database** - Select the asset name column in the SQL database that contains the data to be synchronized.

**Attempt Asset Type Mapping** - Select:

- On to specify the asset type column in the source database for mapping to the iSupport asset type column. If a value in the source does not match the corresponding value a predefined type, a new type will be assigned.
- Off to assign the predefined iSupport asset type in the Default Asset Type field to all synchronized records.

**Asset Type Column from Source Database** - If On was selected in the Attempt Asset Type Mapping field, select the column to be used for mapping the asset type in the source database.

**Default Asset Type** - If Off was selected in the Attempt Asset Type Mapping field, select the predefined iSupport asset type to assign to all synchronized asset records.

**Attempt Asset Owner Mapping** - Select:

- On to specify the names of the asset owner First Name, Last Name, and Email columns in the source database and search for a matching asset owner in iSupport Customer Profiles.

If a value in the source database does not match, a new Customer Profile record will be created if Yes is selected in the Create New Customer Profile if Mapping Fails field. If No is selected in that field, the customer in the Default Owner field will be assigned.

- Off to assign the customer in the Default Owner field as the asset owner of all synchronized records.

**Owner First Name Column from Source Database** - If On was selected in the Attempt Asset Owner Mapping field, select the owner first name column in the source database to be used in the search for a matching asset owner in iSupport Customer Profiles.



**Owner Last Name Column from Source Database** - If On was selected in the Attempt Asset Owner Mapping field, select the owner last name column in the source database to be used in the search for a matching asset owner in iSupport Customer Profiles.

**Owner Email Column from Source Database** - If On was selected in the Attempt Asset Owner Mapping field, select the owner email column in the source database to be used in the search for a matching asset owner in iSupport Customer Profiles.

**Create New Customer Profile if Mapping Fails** - Select:

- On to create a new Customer Profile record if a value in the source database does not match.
- Off to assign the customer in the Default Owner field as the asset owner of all imported records.

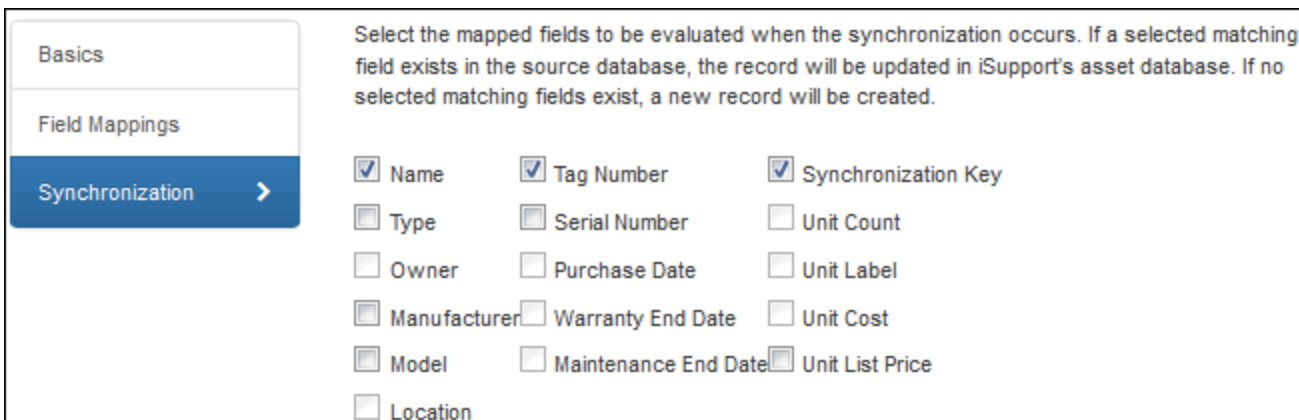
**Default Owner** - If no owner mapping was attempted or Off was selected in the Create New Customer Profile if Mapping Fails field, select the customer to assign as the asset owner for all imported records.

When you make an entry in the Connection String and SQL Query fields on the Basics tab and select the Test Query button or Refresh Columns link, the SQL Columns section will be populated with the names of the columns in the source database. The iSupport Columns field contains the columns in the iSupport's Asset database. To map a field, select a field in the SQL Columns field and the corresponding field in the iSupport Columns field. Then select the  button. The associated fields display under Mapping. To remove an entry from the Mapping section, select the entry and select the  button.

Use the Custom Fields tab to map fields in the source database to the custom fields set up for both asset types and the Asset entry screen. Then select Save to save your selections. The synchronization will occur when the Sync button is selected and/or on the interval set in the Asset Synchronization Interval field on the Basics tab.

## Selecting Fields for Asset Synchronization

Use the Synchronization tab to synchronize iSupport's Asset database with fields in a Microsoft SQL Server source database; you'll select the mapped fields to be evaluated when the synchronization occurs. If a matching field exists in the source database, the record will be updated in iSupport's Asset database.



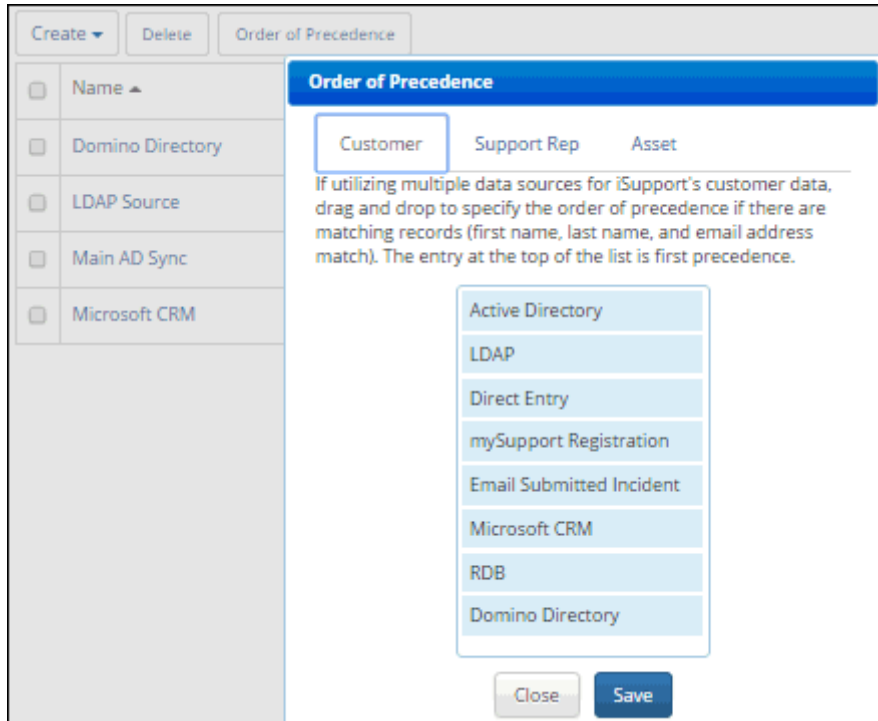
Select the mapped fields to be evaluated when the synchronization occurs. If a selected matching field exists in the source database, the record will be updated in iSupport's asset database. If no selected matching fields exist, a new record will be created.

<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Tag Number	<input checked="" type="checkbox"/> Synchronization Key
<input type="checkbox"/> Type	<input type="checkbox"/> Serial Number	<input type="checkbox"/> Unit Count
<input type="checkbox"/> Owner	<input type="checkbox"/> Purchase Date	<input type="checkbox"/> Unit Label
<input type="checkbox"/> Manufacturer	<input type="checkbox"/> Warranty End Date	<input type="checkbox"/> Unit Cost
<input type="checkbox"/> Model	<input type="checkbox"/> Maintenance End Date	<input type="checkbox"/> Unit List Price
<input type="checkbox"/> Location		

## Specifying Precedence for Multiple SQL Data Sources

If you are using multiple sources for populating iSupport's customer, support representative, and asset data, use the order of precedence link to specify the order of precedence if there are matching records. (For customers and support representatives: a match on first name, last name, and email address; for assets, a match on name.) All of

the possible data sources are listed; the top position has the highest precedence. If you are not using one of these data sources, move it down in the list.



## Importing Asset Data from a CSV or Microsoft Excel File

Use the Options and Tools | Integrate | Asset Import feature to import asset data from a comma separated value (.csv) or Microsoft Excel .xlsx file into iSupport's Asset database. Note that the Microsoft Access Object Library 12.0 must be installed for this feature. The Asset Name column or value in the source data must be unique or the entry

will be skipped; any records in the source that are skipped or can't be imported will appear in an exception report screen that appears after the import is completed.

The screenshot shows the 'Asset Import' configuration window. At the top, there's a breadcrumb trail: Desktop / Configuration / Options and Tools / Integrate / Asset Import. Below this, there are several configuration sections:

- Select spreadsheet to import:** Includes a 'Choose File' button (showing 'No file chosen') and a 'Load' button.
- Worksheet:** A dropdown menu currently set to 'Combo'.
- Attempt Asset Type Mapping:** A toggle switch currently set to 'Off'.
- Default Asset Type:** A dropdown menu set to 'Computer', with '+' and edit icons to the right.
- Attempt Asset Owner Mapping:** A toggle switch currently set to 'Off'.
- Default Owner:** A dropdown menu set to 'Unassigned', with a 'Clear' button next to it.
- Update Sync Field:** A dropdown menu set to 'Name'.
- Perform Duplicate Name Check on Update:** A toggle switch currently set to 'On'.

At the bottom, there are three columns for column mapping:

- Import Source:** A list of columns from the source spreadsheet: Name, Type, Manufacturer, Model, Location, Tag (highlighted in blue), and Version.
- iSupport Columns:** A list of columns in the iSupport system: SERIAL\_NUMBER, DT\_PURCHASE, DT\_WAR\_END, DT\_MAINT\_END, UNIT\_COUNT, ITEM\_COST\_PRICE, ITEM\_LIST\_PRICE, UNIT\_LABEL, Used For, and Laptop: Service Date.
- Mapped Columns:** A list of mapped columns: Name>NAME, Manufacturer>MFG, Model>MODEL, Location>LOCATION, and Tag>TAG\_NUMBER.

Navigation arrows are present between the columns. At the bottom right, there are 'Import' and 'Update' buttons.

Select the Browse button to select a Microsoft Excel file containing the asset information. Select the Load button to populate the Import Source column with the columns in the spreadsheet. The worksheets in the file appear in the Worksheet field; select the worksheet containing the data to import.

**Attempt Asset Type Mapping - Select:**

- On to specify the asset type column in the source database for mapping to the iSupport asset type column. If a value in the source does not match the corresponding value a predefined type, a new type will be assigned.
- Off to assign the predefined iSupport asset type in the Default Asset Type field to all synchronized records.



**Attempt Asset Owner Mapping - Select:**

- On to specify the names of the asset owner First Name, Last Name, and Email columns in the source database and search for a matching asset owner in iSupport Customer Profiles. If a value in the source database does not match, a new Customer Profile record will be created if Yes is selected in the Create New Customer Profile if Mapping Fails field. If No is selected in that field, the customer in the Default Owner field will be assigned.
- Off to assign the customer in the Default Owner field as the asset owner of all synchronized records.

**Update Sync Field -** If performing a mass Asset record update, select the Sync key to use for the update.

**Perform Duplicate Name Check On Update -** If executing a mass Asset record update, select Yes to check for duplicate names while performing the update.

**Import Source/iSupport Columns/Mapped Columns** - Map the columns in the Import Source list to the columns in iSupport.

- To map a column, select a column in the Import Source list and in the corresponding column in the iSupport Columns list. Then select the  right arrow button. The associated fields display under Mapped Columns.
- To remove an entry from the Mapped Columns list, select the entry and select the  left arrow button.

When finished, select the Import button to execute the import.

# Using the Multiple Asset Creation Wizard

The Asset Creation Wizard enables you to automatically create more than one asset record. You can enter data to populate asset fields in all records created and display prompts for entering data unique to a record. You can save your settings in a profile for use later.

The Asset Wizard option appears on the Desktop menu if the Use Multiple Asset Wizard permission has been assigned to you in your Support Representative Profile record. Select New in the first screen to start the process.

### Asset Information

**Asset Type and Quantity**  
Asset Type:  Asset Quantity:

**Asset Fields**

	Field	Prompt?
*Asset Name:	<input type="text" value="Laptop"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Owner	<input type="text" value="Steve Johnson"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Model:	<input type="text" value="Thinkpad"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Manufacturer:	<input type="text" value="IBM"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Tag Number:	<input type="text" value="C10-"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Serial Number:	<input type="text" value="94818-86182"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Location:	<input type="text" value="Headquarters"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Purchase Date:	<input type="text" value="10/18/09"/> <input type="button" value="21"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Comments:	<input type="text" value="Shipment - Computers Inc"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No

**Custom Fields**  
Used For:

Enter the asset type, quantity, and data to populate asset fields in all records created. Select Yes in the Prompt column to display prompts for entering data unique to a record. Select Next when finished.

**Asset Type** - Select the asset type to assign to all of the Asset records created. Asset types are set in the Configuration module.

**Asset Quantity** - Enter the number of Asset records to be created.

**Field column** - Enter the data to populate the corresponding fields in all of the Asset records created. With the exception of the required fields (marked with an asterisk), you can leave a field blank to leave the corresponding field blank. The Asset Name field is required.

**Prompt? column** - Select Yes to display the field on a screen for each record created so you can enter a value unique to each record.

**Custom Fields** - Enter the data to populate the corresponding custom fields on all records created. Custom fields are set in the Configuration module.

If you selected Yes for a field in the Prompt column, a screen appears for each record to be created. Enter the data unique to each record and select Next.

**Asset Fields**

**Creating Asset 1 of 5**

Tag Number:	<input type="text" value="C10-"/>
Serial Number:	<input type="text" value="94818-86182"/>

After the Asset records have been created, you can enter a name and description and save the profile. Select Finish to exit without saving.

**Finish**

**5 out of 5 assets created.**

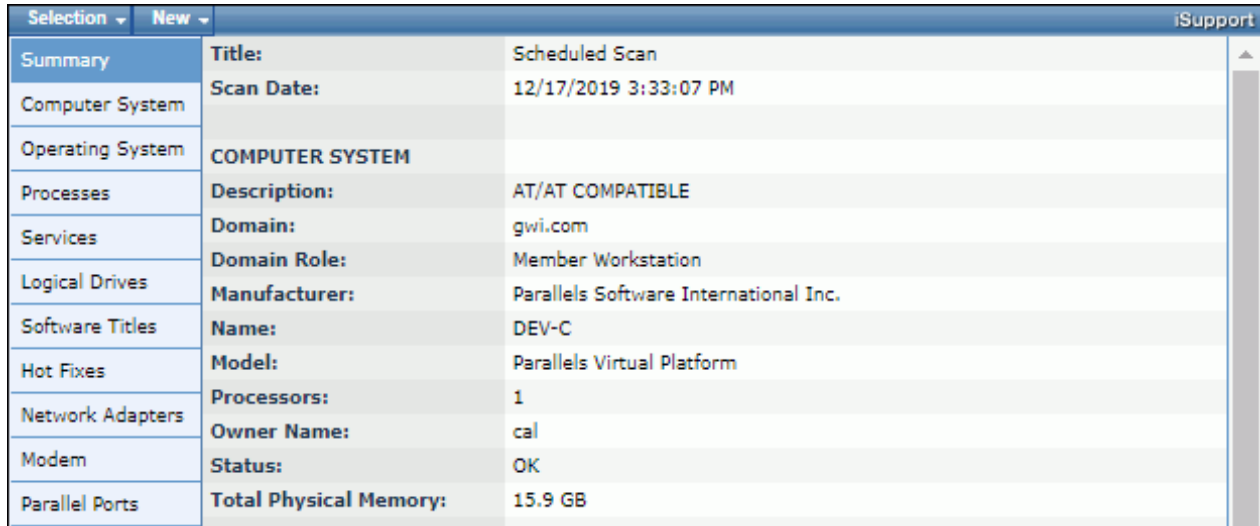
Save asset profile?

Name:

Description:

# Configuring Scheduled Scans and Device Monitoring

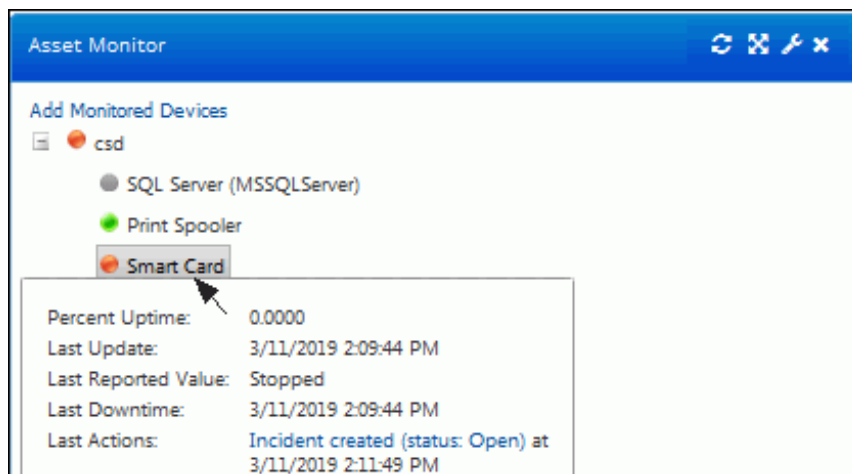
Asset scanning and monitoring can be scheduled and run automatically according to a Scheduled Scan and Monitoring Definition, which defines the machines/devices to be scanned during a specified start and end time. These scans include a comprehensive set of data; a partial example of a scheduled scan is shown below:



Selection	New	iSupport
Summary	<b>Title:</b>	Scheduled Scan
Computer System	<b>Scan Date:</b>	12/17/2019 3:33:07 PM
Operating System	<b>COMPUTER SYSTEM</b>	
Processes	<b>Description:</b>	AT/AT COMPATIBLE
Services	<b>Domain:</b>	gwi.com
Logical Drives	<b>Domain Role:</b>	Member Workstation
Software Titles	<b>Manufacturer:</b>	Parallels Software International Inc.
Hot Fixes	<b>Name:</b>	DEV-C
Network Adapters	<b>Model:</b>	Parallels Virtual Platform
Modem	<b>Processors:</b>	1
Parallel Ports	<b>Owner Name:</b>	cal
	<b>Status:</b>	OK
	<b>Total Physical Memory:</b>	15.9 GB

These scans run on the server on which iSupport is installed, on the schedule of the Asset Scheduled Scan and Monitoring agent in the Asset Agents screen. Scheduled scans are viewed on the Desktop, and can be associated with Asset records. If configured, Asset records can be created automatically and associated with machines involved in scheduled scans. Up to 15 of the most recent scheduled scans are retained for each machine associated with an Asset record. From the Scan screen or Desktop, you can generate and save a side-by-side comparison of dynamic or scheduled scans.

The Monitoring feature enables the devices defined in a Scheduled Scan and Monitoring Definition to be monitored for uptime, low disk space, and stopped services. To display monitoring results, you can create a view or use the Asset Monitor dashboard component on the Desktop. You could create a component for a range of devices to track such as buildings, IP ranges, routers, or servers. Details will appear when you hover over the device, drive, or service being monitored.

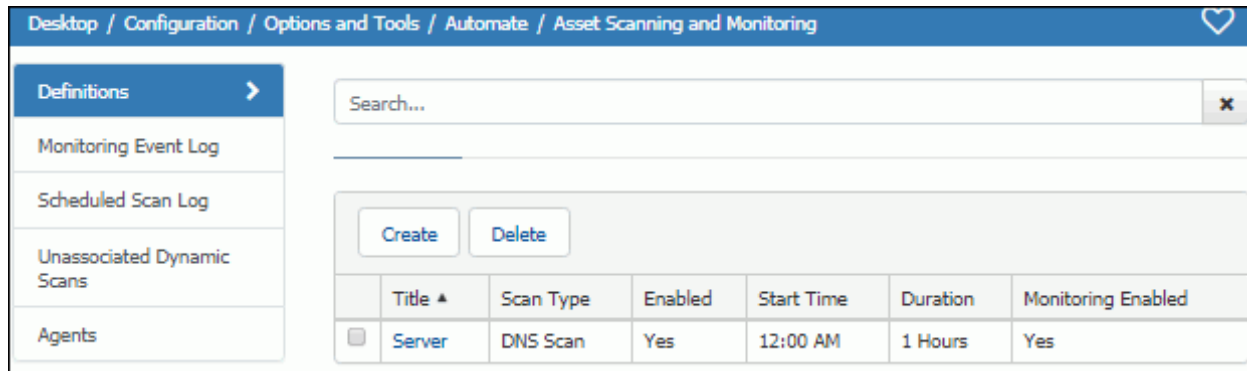


## Configuration Process

- 1 If performing asset scans and you need to add a login with local administrative rights on device or machine, right-click on My Computer that device/machine and select Manage. Under Local Users and Groups, select Groups and then double-click on Administrators. Select Add. Add the name and select OK. In the Administrators Properties dialog, select Apply and then select OK.
- 2 Ensure that WMI is installed and active on the machines to be scanned.



3 In the Asset Scanning and Monitoring screen:



Select Create on the Definitions tab to create definitions for defined devices to be scanned automatically on a scheduled basis, and/or to be monitored for uptime, low disk space, and stopped services. See [“Creating a Scheduled Scan and Monitoring Definition” on page 58](#) for more information. In that screen you can enable automatic asset creation for machines that are involved in scheduled scans but not associated with an existing record. (Note that monitoring can still be configured and enabled if asset scanning is disabled.)

4 Enable agents via the Agents tab; see [“Enabling Agents” on page 67](#) for more information. The Asset Scheduled Scan and Monitoring agent checks scheduled scan and monitoring definitions, initiates scans according to schedule, and enables monitoring. After this agent is enabled and saved, the Scan button will appear on the Basics tab in the Scan Definition screen for running the scan immediately.

5 You can use the following to view scan progress and errors:

- Use the Monitoring Event Log tab to display errors that occur while retrieving or saving the data, details regarding access to the machines included in the range to be monitored, and status information. You can use the iSupport Event Log and Microsoft® Windows7 Event Viewer to view application errors and log entries regarding the iSupport Agent Manager.
- Use the Scheduled Scan Log tab to view messages regarding the progress of scans run using scheduled scan definitions. This includes errors that occur while retrieving or saving the data, details regarding the machines included in the range to be scanned and the machines that were unreachable, and status information. These messages are stored in the cAsset database and can accumulate quickly; it is important to use the Clear All Messages link in that screen to maintain the size of the stored data. Use the Number of Days Until Auto Purge field to specify a number of days after which messages will be deleted automatically by the Database Maintenance agent on the Global tab in the Administrative Tools | Agents screen.
- Use the Scheduled Scans by Date view on the Desktop to display the most recent scan for each scanned device or create a custom view via the View and Report Designers on the Desktop.

The Unassociated Dynamic Scans tab in the Asset Scanning and Monitoring screen contains a list of dynamic scans that have been associated with an asset, but the asset’s asset type changed to non-scannable. To delete these scans, select the checkbox next to the scan and select the Delete link.

## Creating a Scheduled Scan and Monitoring Definition

Use the Basics tab on the Options and Tools | Automate | Asset Scanning and Monitoring definition screen to specify the type and timing of a scan and notification options. You can optionally enable automatic asset record creation for machines that are involved in scheduled scans but not associated with an existing record..

The screenshot shows the 'Asset Scanning and Monitoring' configuration interface. The breadcrumb trail at the top reads: Desktop / Configuration / Options and Tools / Automate / Asset Scanning and Monitoring. On the left, a sidebar contains four tabs: 'Basics' (selected), 'DNS Settings', 'Components', and 'Monitoring'. The main area is a form with the following fields and values:

Title	Server
Scan Type	DNS Scan
Scan Enabled	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Start Time	12:00 AM
Duration	1 Hour(s)
Frequency	Daily
Occurs On	
Scan On Weekends	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Email Addresses to Notify Upon Scan Completion	bw@example.local
Impersonate WMI Authentication	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Name	administrator
Password	Reset
SNMP Community	public
Enable Auto Asset Create from Scheduled Scan Agent	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Asset Record Template for Automatic Asset Creation	Scan Template - Server
Populate Asset Serial Number Field using	OS Serial Number
Last Run	3/2/2019 9:46 AM

**Scan Name** - Enter a name describing the settings in the scan definition.

**Scan Type** - Select the type of scan:

- An IP Scan searches based on a specified range of IP addresses. (You can exclude specified IP addresses.)
- An AD Scan searches based on a specified Active Directory path. You can scan all machine names known by the domain controller, or scan using an LDAP query for returning a specific set of information.
- A DNS Scan searches based on specified domain names.

**Scan Enabled** - Select Yes to allow scans to initiate based on the defined schedule and setting; otherwise, select No to prevent the scan from occurring.

**Frequency** - Select one of the following:

- Daily to run the scan every day at the time designated in the Start Time field.
- Weekly to run the scan once a week on the day designated in the Occurs On field.
- Monthly to run the scan every month on the day designated in the Occurs On field.

**Start Time** - Select the time at which the scan should be initiated.

**Duration** - Enter the amount of time (in hours) at which, if the scan is still running, the scan should be terminated.

**Occurs On** - This field is enabled if Weekly or Monthly is selected in the Frequency field.

- If Weekly is selected in the Frequency field, select the day of the week on which the scan should run. The scan will run every week on the selected day.
- If Monthly is selected in the Frequency field, select the day on which the scan should run. The scan will run every month on the selected day.

To select more than one entry, select entries while holding down the Control key. Use the Shift key to select a range.

**Scan On Weekends** - This field is enabled if Daily or Monthly is selected in the Frequency field. Select Yes to schedule the scan to run on Saturdays and Sundays.

**Email Addresses to Notify Upon Scan Completion** - Enter the email addresses to which an automatic notification should be sent when the scan completes. The notification will contain the scan definition name and the time and date of completion.

**Impersonate WMI Authentication** - Select one of the following for the login to be used to access the systems included in the scan:

- Select No to use the login that is set up for the iSupport Agent Manager (the service used to process scans).

To view the login for the iSupport Agent Manager: from the Start menu, select Programs | Administrative Tools | Computer Management. Expand the Services and Applications section and select Services. Right-click on the iSupport Agent Manager service and select Properties. The Logon tab includes the login used by the iSupport Agent Manager.

- Select Yes to enter a different login to be used to access the systems included in the scan.

**Name/Password** - Enter the login to be used to access the systems included in the scan.

**SNMP Community** - If you wish to track non-Windows devices on your local subnet, enter the SNMP community string (a text string that acts as a password for a network device). Community strings are configured by administrators of network devices that support SNMP to allow varying levels of access to the devices configuration and operational settings; this grants management tools read-only access to the remote device. The default community string for read-only access to network devices is normally the word "public".

**Enable Auto Asset Create from Scheduled Scan Agent** - Select Yes to enable the Auto Asset Create from Scheduled Scan agent which creates Asset records automatically for machines that are involved in scheduled scans but not associated with an existing record. (You can also enable and execute this agent immediately via the Agents tab.) It will run every hour based on the time at which the iSupport Agent Manager service is started.

**Asset Record Template for Automatic Asset Creation** - Select this link to select the name of an existing Asset record to use as a template when the Auto Asset Create from Scheduled Scan agent is run. It's a good idea to create an Asset record specifically for use as a template. To distinguish automatically-created Asset records after the records are created, you can create a global custom Asset field with "Auto-created" in the label; after the records are created, you can create a Desktop custom view containing that field. The asset type in the template record will determine the fields that will appear on the automatically-created record; for example, if the Owner field is not set up for the asset type, it will not appear in the auto-created record. The fields are populated as shown below.

- Asset Name - The machine name in the scheduled scan. If an asset name already exists with the machine name, a numeric value will be appended to it.
- Asset Type - The contents of the Asset Type field in the asset record used as a template
- Owner - The contents of the Owner field in the Asset record used as a template
- Model - Determined from scheduled scan results
- Manufacturer - Determined from scheduled scan results
- Tag Number - Blank
- Serial Number - Blank unless determined from scheduled scan results. You can populate this field with the operating system serial number by selecting the Populate Asset Serial Number Field with OS Serial Number option on the Asset tab in the Agents screen.
- Location - The contents of the Location field in the Asset record used as a template
- Purchase and Maintenance Expiration Dates - Blank
- Comments - Blank
- Custom Fields - The contents of the custom fields in the Asset record used as a template
- Attachments - Blank
- Dynamic Scans - Blank
- Scheduled Scan Association - The scheduled scan for the machine that did not have an associated asset record

**Populate Asset Serial Number Field Using** - Select one of the following for populating the Asset Serial Number field when Asset records are created automatically for machines that are involved in scheduled scans but not associated with an existing record: the operating system serial number or the BIOS serial number. If the BIOS Serial Number is selected but not available, the machine name or ID defined in the scheduled scan definition will be used.

### *Specifying Devices to Be Scanned and/or Monitored*

The appearance of the second tab will depend on your selection in the Scan Type field on the Basics tab.



#### IP Settings

If IP Scan is selected in the Scan Type field, the IP Settings tab appears as shown in the example below.

Use the Included IP Address Ranges fields to enter the IP addresses of the systems to be scanned.

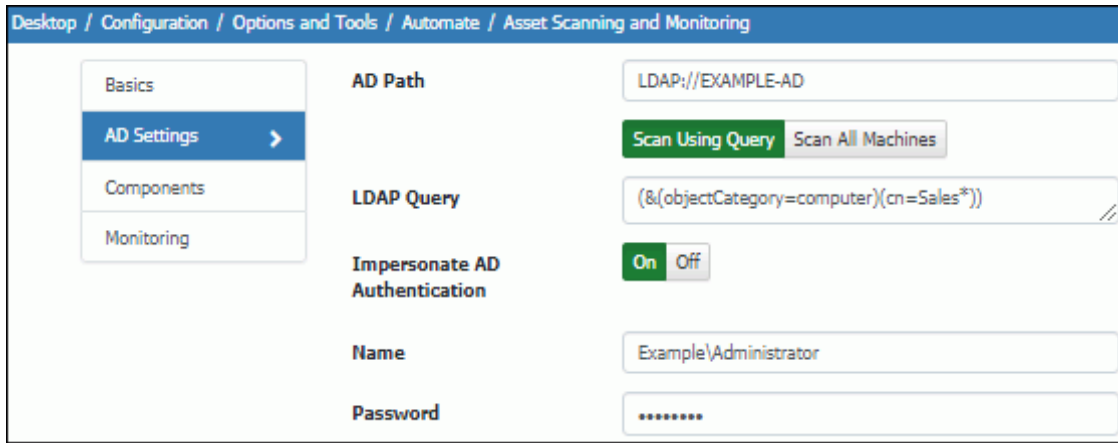
Use the Excluded IP Address Ranges fields to enter the IP addresses of the systems that should not be scanned.

To enter an IP Address range, enter the first IP address in the range in the Start Address field and the last IP address in the range in the End Address field, and then select the ↓ down arrow to move the IP range into the list. To move a

range out of the list, select the entry and then select the  up arrow. To delete a range from the list, select the entry and then select  Delete.

### AD Scan Settings

If AD Scan is selected in the Scan Type field, the AD Settings tab appears. You can specify the scan to: scan all machine names known by the domain controller, or scan using an LDAP query for locating a specific set of machines. An example is shown below.



**AD Path** - Enter the path for the Active Directory to be scanned.

**Scan Using Query/LDAP Query** - Select this field to use an LDAP query for locating a specific set of machines.

LDAP (Light Weight Directory Access Protocol) defines how information can be accessed in directories. In the example above, the query locates all machine names known by the domain controller that begin with "SALES".

Active Directory supports the LDAP search filter syntax.

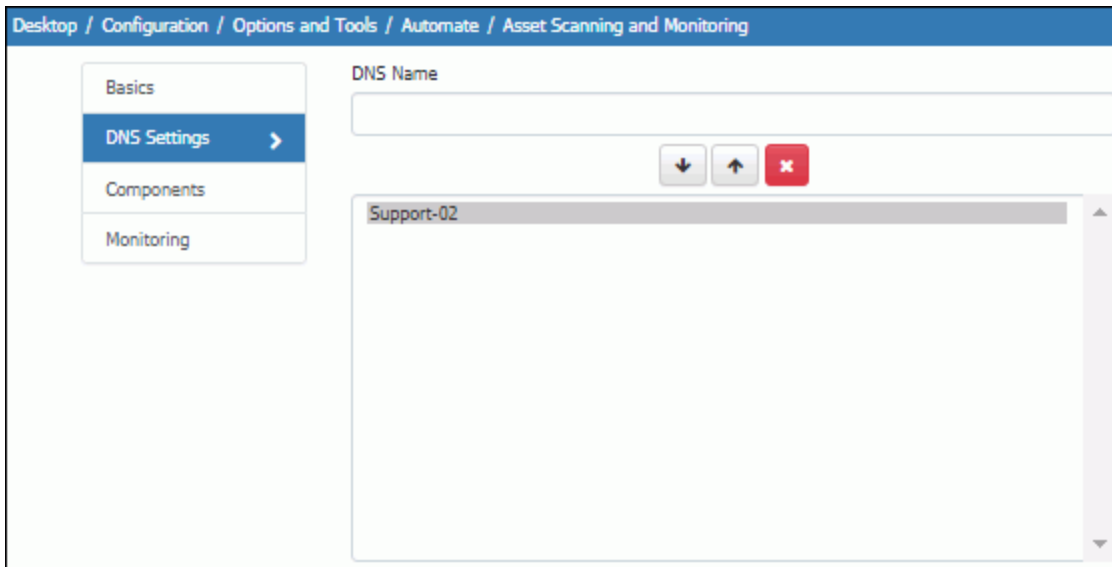
**Scan All Machines** - Select this field to scan all machine names known by the domain controller.




**Impersonate AD Authentication/Name/Password** - Select one of the following for the login to be used to access systems in the specified Active Directory:

- Select No to use the login set up for the iSupport Agent Manager (the service used to process scans). To view the login for the iSupport Agent Manager: from the Start menu, select Programs | Administrative Tools | Computer Management. Expand the Services and Applications section and select Services. Right-click on the iSupport Agent Manager service and select Properties. The Logon tab includes the login used by the iSupport Agent Manager.
- Select Yes to enter a different login to be used to access the systems in the specified Active Directory.

## DNS Settings

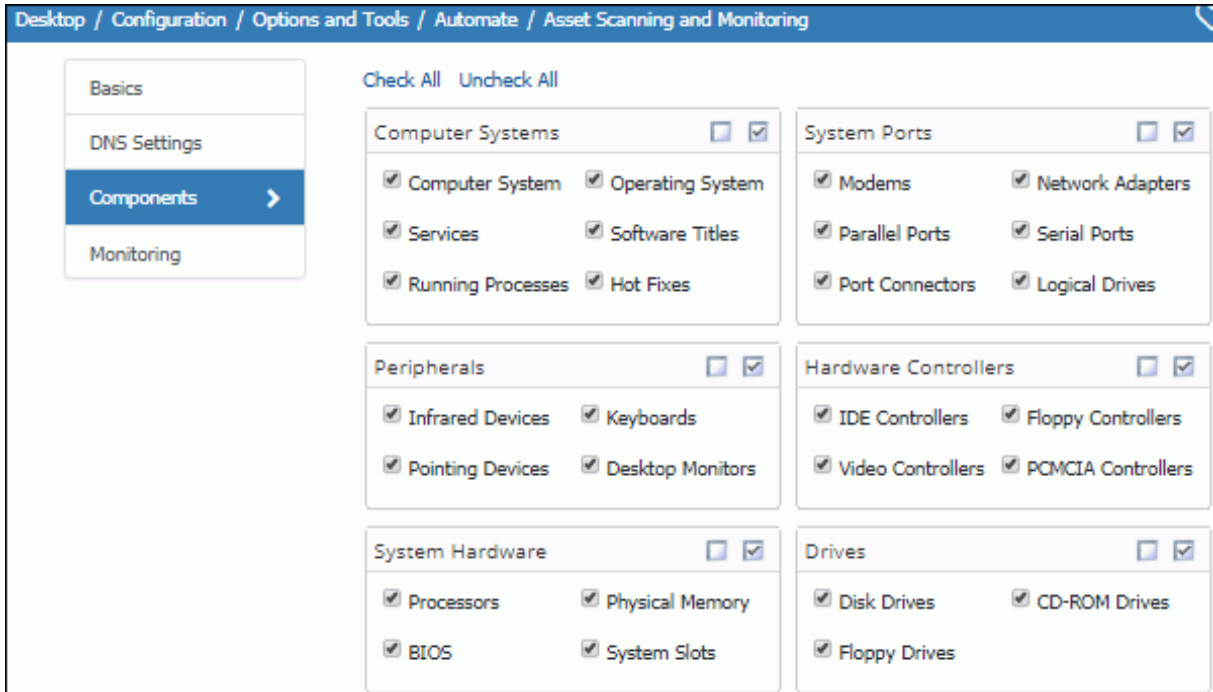
If DNS Scan is selected in the Scan Type field, the DNS Settings tab appears.



Use the DNS Name field to enter the domain names of the systems to be scanned. Wildcards are not allowed. Enter a domain name in the field on the left and select the  down arrow to move the IP range into the list. To move a range out of the list, select the entry and then select the  up arrow. To delete a range from the list, select the entry and then select  Delete.

## *Selecting Components to Scan*

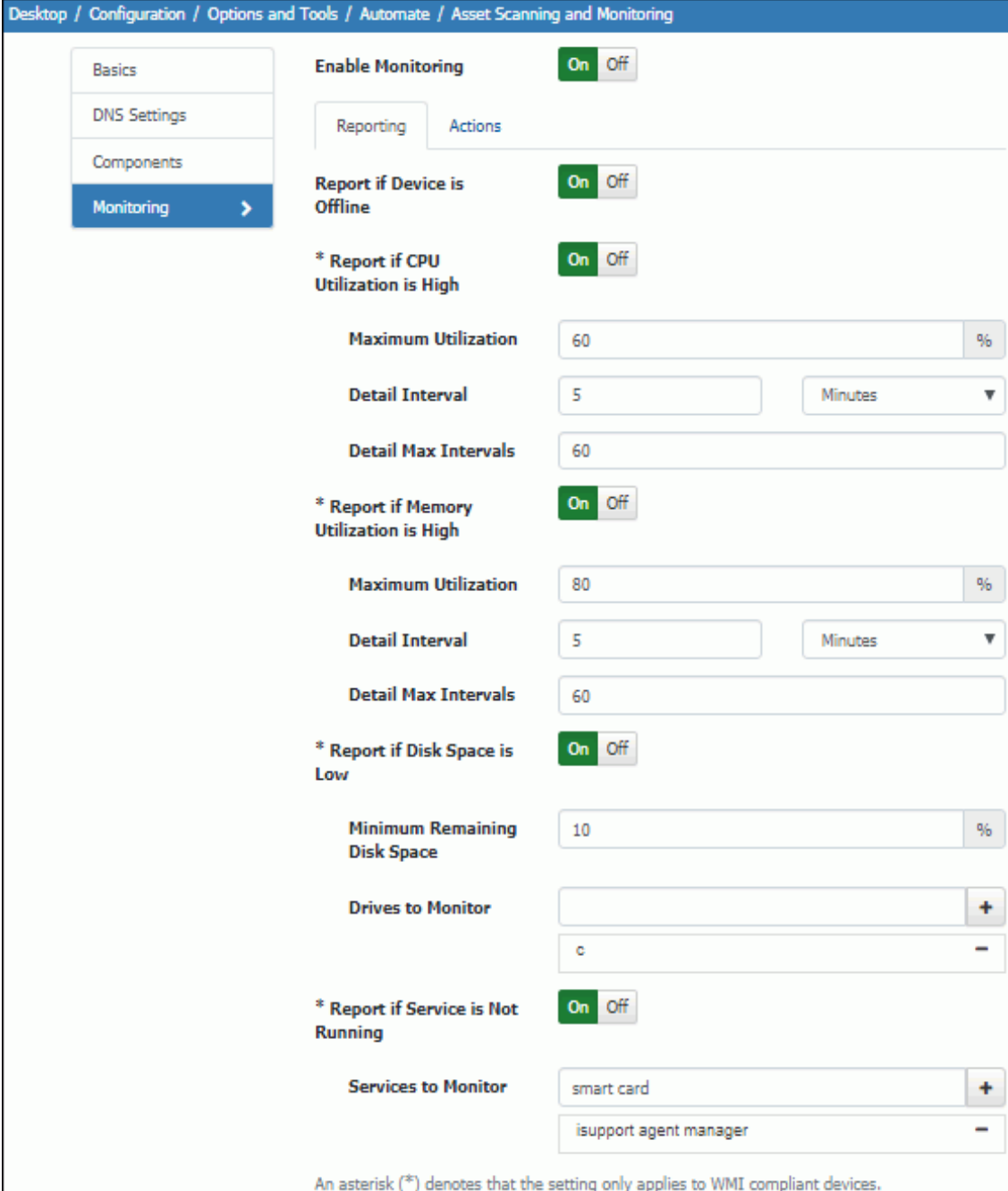
Select the types of data to include in the scan.



## Configuring Monitoring

You can optionally use the Monitoring tab in the Asset Scanning and Monitoring screen to configure monitoring that tracks the state of devices included in a scan definition and their CPU, memory, disk space, and services. Devices are flagged if any of the configured reporting thresholds are met (a monitored device is off-line or has high memory or CPU utilization, a monitored drive has disk space lower than the specified percentage, or a monitored service has a stopped state). If a device is flagged, you can configure a notification to be sent and/or an Incident or Problem record to be created. Any related asset record will be associated with the newly-created record. Monitoring results are reported via the Asset Monitor Desktop component; see [“Using the Asset Monitor Component on the Desktop” on page 68](#) for more information.

Note that monitoring can still be configured and enabled if scanning is disabled on the Basics tab.



Desktop / Configuration / Options and Tools / Automate / Asset Scanning and Monitoring

Basics  
DNS Settings  
Components  
Monitoring >

**Enable Monitoring**  On  Off

Reporting Actions

**Report if Device is Offline**  On  Off

**\* Report if CPU Utilization is High**  On  Off

Maximum Utilization 60 %

Detail Interval 5 Minutes

Detail Max Intervals 60

**\* Report if Memory Utilization is High**  On  Off

Maximum Utilization 80 %

Detail Interval 5 Minutes

Detail Max Intervals 60

**\* Report if Disk Space is Low**  On  Off

Minimum Remaining Disk Space 10 %

Drives to Monitor +  
c -

**\* Report if Service is Not Running**  On  Off

Services to Monitor +  
smart card +  
isupport agent manager -

An asterisk (\*) denotes that the setting only applies to WMI compliant devices.

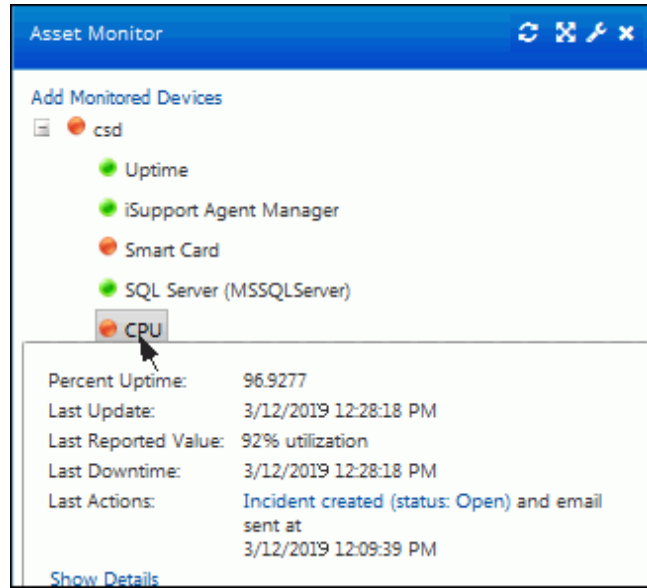
**Enable Monitoring** - Select Yes to enable network monitoring to occur for the devices specified in this definition. Note: Network monitoring requires the Asset Scheduled Scan and Monitoring agent to be enabled. Monitoring will stop and restart if a change occurs in the Asset Scheduled Scan and Monitoring Definition (monitoring was disabled, the definition was deleted, defined devices cannot be accessed, or monitoring settings have changed). Monitoring

will stop if the iSupport Asset Scheduled Scan and Monitoring agent or iSupport Agent Manager has stopped or has been disabled.

### Reporting

**Report if Device is Offline** - Select Yes to flag the device as Offline, display a red dot next to it, and initiate configured actions if the monitoring detects that the device is not responding.

**Report if CPU Utilization is High** - Select Yes to include a CPU entry in the Asset Monitor component for the device and track and report the percentage of CPU utilization. A red dot will display if the monitor detects that the percentage of CPU utilization is higher than the percentage entered in the Maximum Utilization field for the duration configured in the Detail Interval and Detail Max Intervals fields.



**Maximum Utilization** - Enter the percentage of CPU utilization at which reporting should start; if CPU utilization reaches this percentage, reporting will continue for the duration configured in the Detail Interval and Detail Max Intervals fields. Note that reporting will stop if the CPU utilization goes under this percentage.

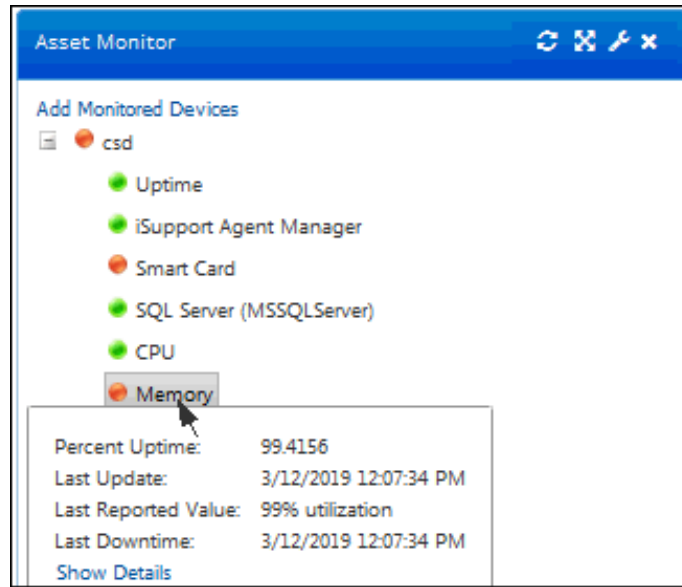
**Detail Interval** - Enter the number of minutes, hours, or seconds in the interval during which monitoring will track and report a percentage of CPU utilization above the specified maximum.

**Detail Max Intervals** - Enter the maximum amount of times that the detail interval should be repeated for the duration of maximum CPU utilization reporting.

**Report if Memory Utilization is High** - Select Yes to include a Memory entry in the Asset Monitor component for the device and track and report the percentage of memory utilization. A red dot will display if the monitor detects that



the percentage of memory utilization is higher than the percentage entered in the Maximum Utilization field for the duration configured in the Detail Interval and Detail Max Intervals fields.

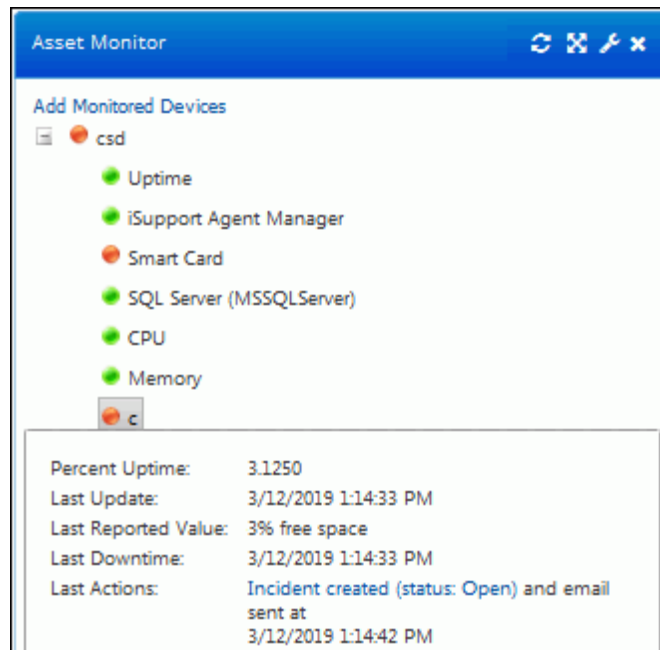


**Maximum Utilization** - Enter the percentage of memory utilization at which reporting should start; if memory utilization reaches this percentage, reporting will continue for the duration configured in the Detail Interval and Detail Max Intervals fields.

**Detail Interval** - Enter the number of minutes, hours, or seconds in the interval during which monitoring will track and report a percentage of memory utilization above the specified maximum.

**Detail Max Intervals** - Enter the maximum amount of times that the detail interval should be repeated for the duration of maximum memory utilization reporting.

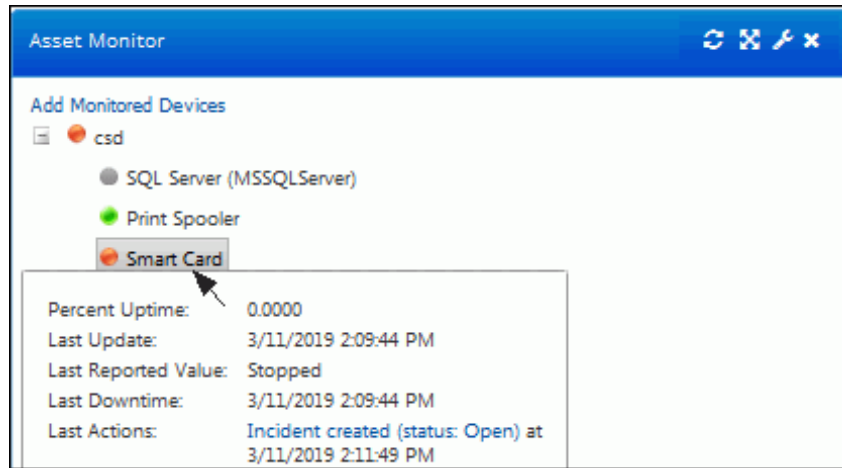
**Report if Disk Space is Low** - Select Yes to include one or more specified drives in the Asset Monitor component and track and report the amount of free space. A red dot will display if the monitor detects that the amount of remaining disk space is less than the percentage entered in the Minimum Remaining Disk Space field.



**Minimum Remaining Disk Space** - If Yes is entered in the Report if Disk Space is Low field, enter the percentage of disk space at which the specified drive(s) should be flagged for low disk space.

**Drives to Monitor** - If Yes is entered in the Report if Disk Space is Low field, enter the names of the drives to monitor for a low disk space state.

**Report if Service is Not Running** - Select Yes to include specified service(s) in the Asset Monitor component and display a red dot if the monitor detects that a specified service has a stopped state.



**Services to Monitor** - Enter the display names of the services to monitor for a stopped state.

### Actions

Complete the following fields to send an email and/or create an Incident or Problem record if any of the configured reporting thresholds are met (a monitored device is off-line or has high memory or CPU utilization, a monitored drive has disk space lower than the specified percentage, or a monitored service has a stopped state).

**Delay** - Enter the amount of time after a configured threshold is met during which action should not be taken (in case it is immediately corrected after that point; for example, a server restart may correct a service stoppage).

**Send Email/Recipients** - Select Yes to send an email to one or more email addresses (separate with a comma or semicolon) if any of the configured reporting thresholds are met. The email will be sent if the state is still detected after the amount of time specified in the Delay field. Email content is as follows; it cannot be customized.

- Drive Off Line

Subject: iSupport Monitoring Notification: <device> did not respond

Body: The device '<device>', being monitored by the <Scheduled Scan and Monitoring Definition name>, did not respond on <date> at <time>.

- Services Stopped

Subject: iSupport Monitoring Notification: The service <service> on <device> is not running

Body: The <service> service on <device>, being monitored by the <Scheduled Scan and Monitoring Definition name>, was in a Stopped state on <date> at <time>.

- Low Disk Space

Subject: iSupport Monitoring Notification: <device> has exceeded the specified disk space limit

Body: The <drive> drive on '<device>', being monitored by the <Scheduled Scan and Monitoring Definition name>, has reached or exceeded its minimum disk space remaining limit on <date> at <time>. There is currently <amount of disk space remaining> free disk space remaining.

- Memory Utilization

Subject: iSupport Monitoring Notification: <device> has exceeded the specified memory utilization limit.

Body: The memory on '<device>', being monitored by the <Scheduled Scan and Monitoring Definition name> scheduled scan definition, reached or exceeded its configured maximum percentage of memory utilization of <configured maximum percentage of memory utilization>% on <date> at <time>.

- CPU Utilization

Subject: iSupport Monitoring Notification: <device> has exceeded the specified CPU utilization limit.

Body: The CPU on '<device>', being monitored by the <Scheduled Scan and Monitoring Definition name> scheduled scan definition, reached or exceeded its configured maximum percentage of CPU utilization of <configured maximum percentage of CPU utilization>% on <date> at <time>.

**Create Work Item** - Select Yes to create an Incident or Problem record if any of the configured reporting thresholds are met. The record will be created if the state is still detected after the amount of time specified in the Delay field.

**Work Item Type** - If Yes is selected in the Create Work Item field, select the type of work item to create: Incident or Problem. Note that the notification content (listed above) will be included in the Description field; if a template is specified, the notification content will be included after the template's description.

**Incident Template** - If creating an incident, select an incident template to apply to it.

**Default Assignee** - If creating an incident or problem/, select the support representative to assign to it.

**Default Customer** - If creating an incident, select the customer to assign to it.

**Categorization** - If creating a problem, select the categorization to assign to it.

**Default Mapping** - If creating a problem, select the impact, urgency, and priority mapping to it.

## Enabling Agents

After entering a scheduled scan and monitoring definition, you'll need to enable the Asset Scheduled Scan and Monitoring agent which checks scheduled scan and monitoring definitions and initiates scans according to schedule. After this agent is enabled and saved, the Scan button will appear on the Basics tab in the Scan Definition screen for running the scan immediately.

**Asset Scheduled Scan and Monitoring Agent** - Select Yes to enable the Asset Scheduled Scan and Monitoring agent which checks scheduled scan definitions, initiates scans according to schedule, and enables monitoring if configured in an scheduled scan definition. This agent runs every minute. Network monitoring processing adds device state change entries in the database. Use the **Monitoring Includes Device State Change Entries in the Database; Days to Retain These Entries** field to control database growth by entering the number of days in which these entries should stay in the database.

**Auto Asset Create from Scheduled Scan Agent** - Select Yes to enable the Auto Asset Create from Scheduled Scan agent which creates Asset records automatically for machines that are involved in scheduled scans but not associated with an existing record. (You can also enable and execute this agent immediately via the Agents tab.) It will run every hour based on the time at which the iSupport Agent Manager service is started.

**Asset Record Template for Automatic Asset Creation** - Select this link to select the name of an existing Asset record to use as a template when the Auto Asset Create from Scheduled Scan agent is run. It's a good idea to create an Asset record specifically for use as a template. To distinguish automatically-created Asset records after the records are created, you can create a global custom Asset field with "Auto-created" in the label; after the records are created, you can create a Desktop custom view containing that field. The asset type in the template record will determine the fields that will appear on the automatically-created record; for example, if the Owner field is not set up for the asset type, it will not appear in the auto-created record. The fields are populated as shown below.


- Asset Name - The machine name in the scheduled scan. If an asset name already exists with the machine name, a numeric value will be appended to it.
- Asset Type - The contents of the Asset Type field in the asset record used as a template
- Owner - The contents of the Owner field in the Asset record used as a template
- Model - Determined from scheduled scan results
- Manufacturer - Determined from scheduled scan results
- Tag Number - Blank
- Serial Number - Blank unless determined from scheduled scan results. You can populate this field with the operating system serial number by selecting the Populate Asset Serial Number Field with OS Serial Number option on the Asset tab in the Agents screen.

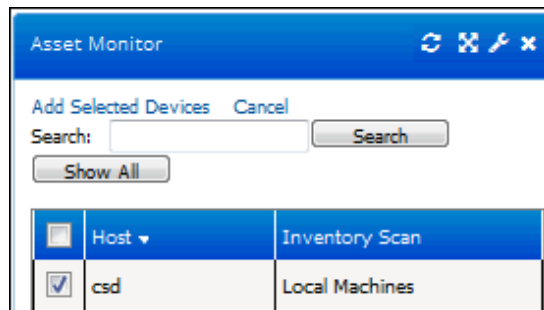
- Location - The contents of the Location field in the Asset record used as a template
- Purchase and Maintenance Expiration Dates - Blank
- Comments - Blank
- Custom Fields - The contents of the custom fields in the Asset record used as a template
- Attachments - Blank
- Dynamic Scans - Blank
- Scheduled Scan Association - The scheduled scan for the machine that did not have an associated asset record

**Populate Asset Serial Number Field Using** - Select one of the following for populating the Asset Serial Number field when Asset records are created automatically for machines that are involved in scheduled scans but not associated with an existing record: the operating system serial number or the BIOS serial number. If the BIOS Serial Number is selected but not available, the machine name or ID defined in the scheduled scan definition will be used.

## Using the Asset Monitor Component on the Desktop

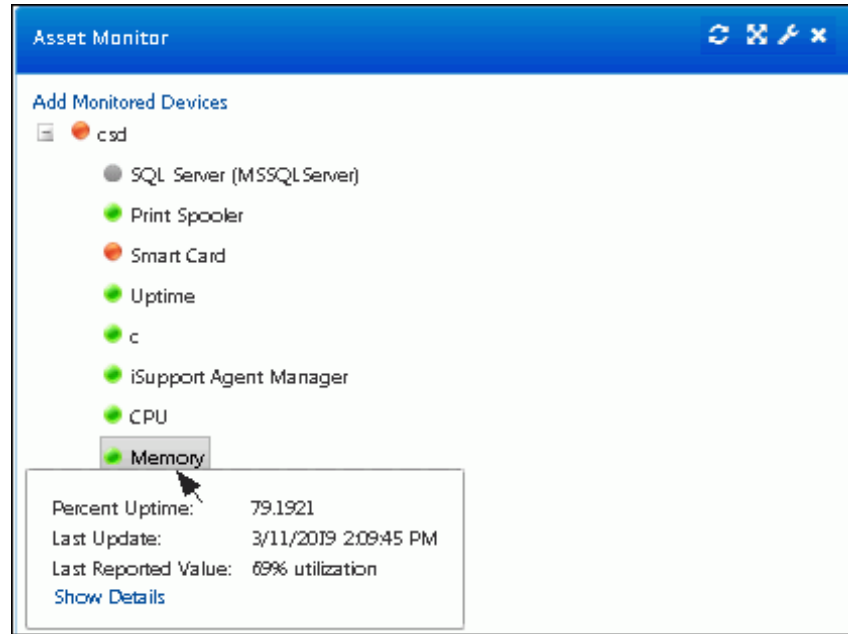
Use the Asset Monitor component to display results of monitoring configured in a scheduled scan and monitoring definition, including the state of devices and their CPU, memory, disk space, and services.

When you add the Asset Monitor  component to a dashboard, an Add Monitored Devices link will appear for you to select the devices to appear in the component. Select the devices in the Host column and then select the Add Selected Devices link.

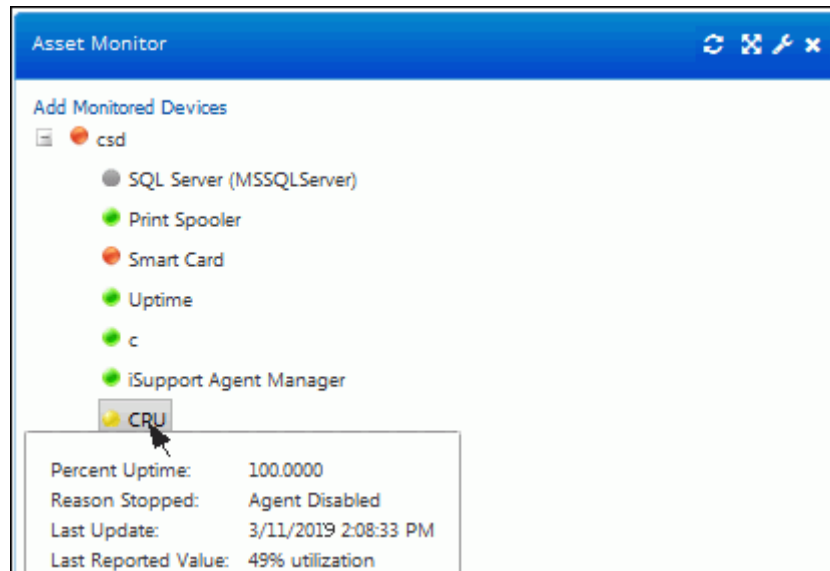


The state of monitored items and devices will be indicated by green, red, yellow, and gray dots; you can display details in a tooltip by hovering over the item or device name.

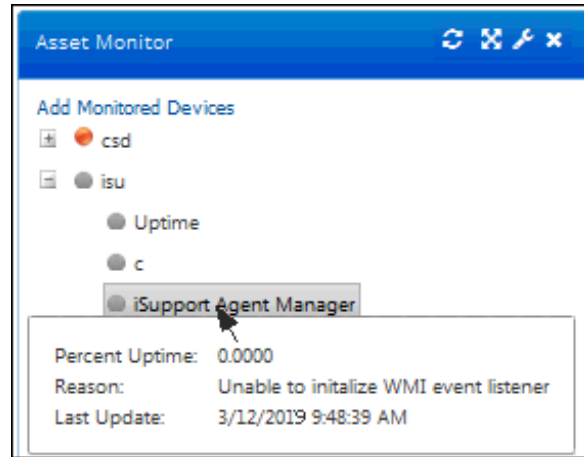
- A green dot will indicate that all monitoring settings in the Asset Scheduled Scan and Monitoring Definition are configured correctly, the Asset Scheduled Scan and Monitoring agent is working correctly, and the item or device is detected by monitoring and meeting configured thresholds.



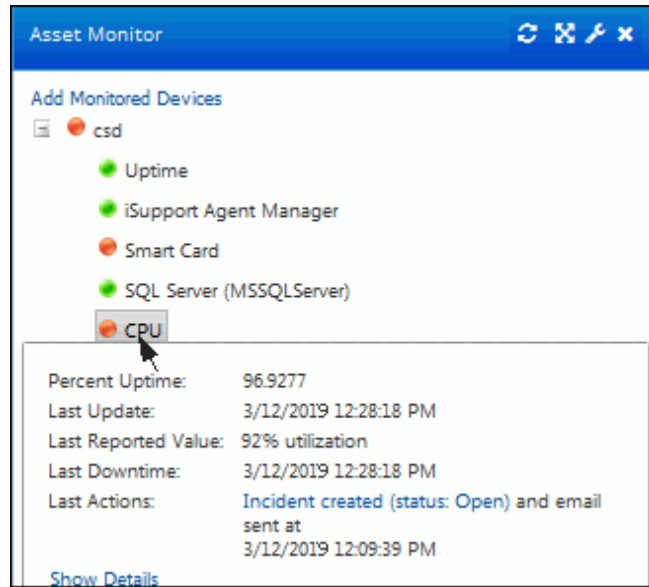
- A yellow dot will appear if, after everything has been working correctly as described above, the iSupport Asset Scheduled Scan and Monitoring agent or iSupport Agent Manager service has stopped or has been disabled.



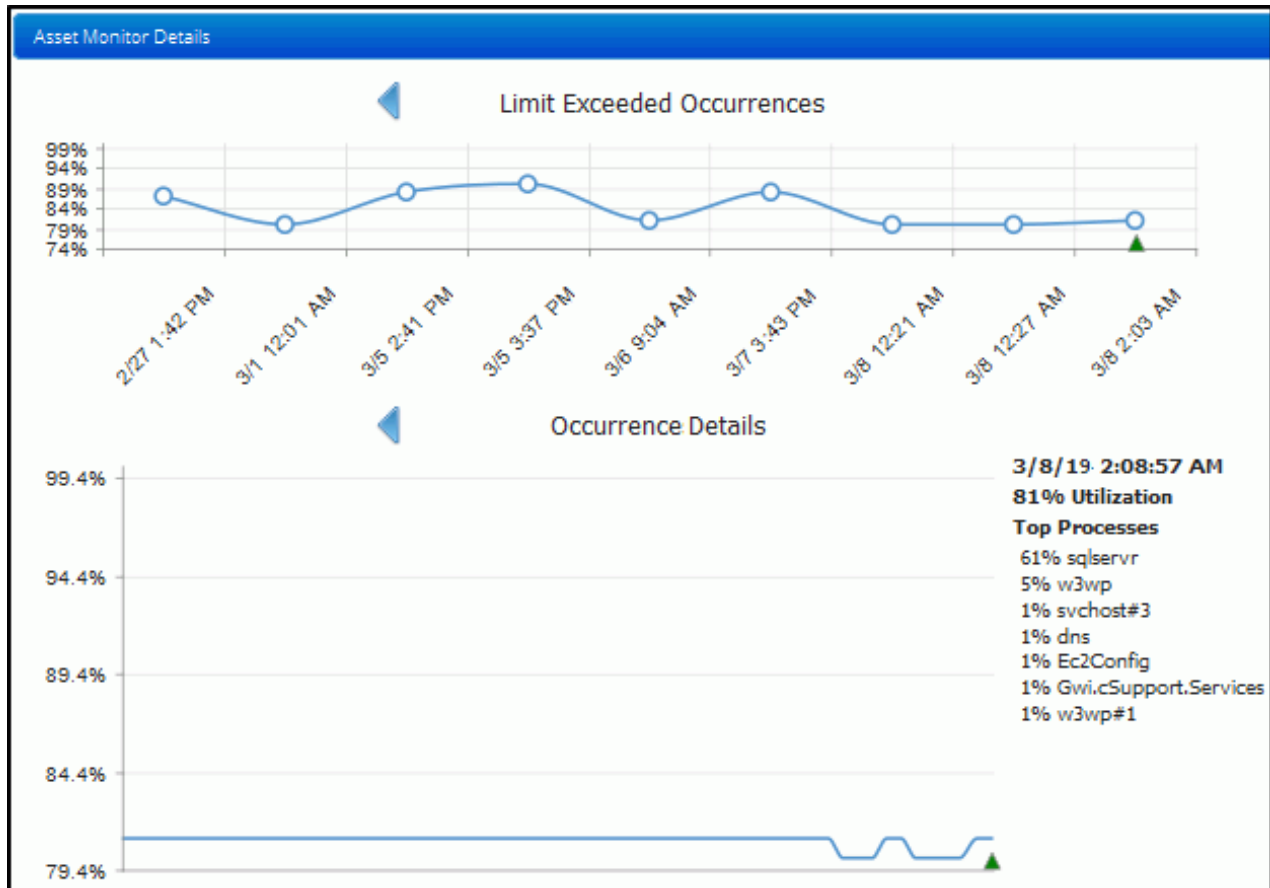
- A gray dot will appear for a monitored item or device on which the WMI listeners cannot be started (for example, if an error occurred with permissions).



- A red dot will appear if, after everything has been working correctly, a problem occurs with the item or device being monitored such as a service stoppage or a configured threshold that is not met (if any of the configured reporting thresholds are met (a monitored device is off-line or has high memory or CPU utilization, a monitored drive has disk space lower than the specified percentage, or a monitored service has a stopped state). Select the Show Details link in the tooltip to display a chart of the occurrences at which a configured threshold was exceeded and other details.



The Show Details link will appear in the tooltip if a configured threshold was exceeded; select it to display a chart of the occurrences at which a configured threshold was exceeded and other details:



## Displaying Scanning and Monitoring Log Messages

### Monitoring Event Log Messages

Use the Monitoring Event Log tab in the Scanning and Monitoring Log Maintenance screen to display errors that occur while retrieving or saving the data, details regarding access to the machines included in the range to be monitored, and status information.

Definitions	Refresh	Clear All Messages	Number of Days Until Auto Purge: 15	
<b>Monitoring Event Log</b> >	Date/Time	Scan Definition	Host	Message
Scheduled Scan Log	2/17/2019 3:32:59 PM	one off	10.16.1.250	Initializing WMI event listeners.
Unassociated Dynamic Scans	2/17/2019 3:32:59 PM	one off	10.16.1.250	Stopping WMI disk space monitoring due to inventory scan definition changes.
Agents	2/17/2019 3:32:59 PM	one off		Initializing uptime monitoring.

Monitoring will only begin if the device is initially in a good state (online with the configured minimum disk space and services running). Monitoring will stop and restart if a change occurs in the Asset Scheduled Scan and Monitoring Definition (monitoring was disabled, the definition was deleted, defined devices cannot be accessed, or monitoring settings have changed). Monitoring will stop if the iSupport Asset Scheduled Scan and Monitoring agent or iSupport Agent Manager has stopped or has been disabled.

## Scheduled Scan Messages

The Scheduled Scan Messages tab in the Scanning and Monitoring Log Maintenance screen contains messages regarding the progress of scans run using scheduled scan and monitoring definitions. This includes:

- Errors that occur while retrieving or saving the data.
- Details regarding the machines included in the range to be scanned, and the machines that were unreachable.
- Status information such as when the scan was started and stopped.

Definitions	Refresh Page	Clear All Messages	Number of Days Until Auto Purge:	15
Monitoring Event Log	Date/Time ▾	Scan Definition	Host	Status
<b>Scheduled Scan Log &gt;</b>	2/17/2019 3:33:07 PM	one off		Database Writer stopped.
Unassociated Dynamic Scans	2/17/2019 3:33:07 PM	one off		Scanner stopped.
Agents	2/17/2019 3:33:05 PM	one off		Database Writer started.
	2/17/2019 3:33:05 PM	one off		Scanning stopped.
	2/17/2019 3:33:05 PM	one off	10.16.1.250	Scan complete.
	2/17/2019 3:32:58 PM	one off		Scanning started.
	2/17/2019 3:32:58 PM	one off	10.16.1.250	Initiating Scan.

Use the Number of Days Until Auto Purge field to specify a number of days after which messages will be deleted automatically by the Database Maintenance agent (scheduled via the Global tab in the Administer | Agents screen).

**Note:** These messages are stored in the cAsset database and can accumulate quickly. It is important to use the **Clear All Messages** link or the Number of Days Until Auto Purge field to maintain the size of the stored data.

You can use the iSupport Event Log and **Microsoft® Windows Event Viewer** to view application errors and log entries regarding the iSupport Agent Manager.

## Unassociated Dynamic Scans

The Unassociated Dynamic Scans tab in the Scanning and Monitoring Log Maintenance screen contains a list of dynamic scans that have been associated with an asset, but the asset's type changed to non-scannable.

Definitions	Delete			
Monitoring Event Log	<input type="checkbox"/> Scan Date	Title	Machine Name	Scanned By
Scheduled Scan Log				
<b>Unassociated Dynamic Scans &gt;</b>				
Agents				

To delete these scans, select the check box next to the scan and select the Delete link.



# Creating Asset Records Automatically Based on Scheduled Scans

Assets can be created automatically for machines that are involved in scheduled scans but not associated with an existing record. To do this, you'll need to do the following:

- 1 Create or find an asset record to be used as a template for creating records. The asset type in the template record will determine the fields that will appear on the automatically-created record; for example, if the Owner field is not set up for the asset type, it will not appear in the auto-created record. The fields are populated as shown below.
  - Asset Name - The machine name in the scheduled scan. If an asset name already exists with the machine name, a numeric value will be appended to it.
  - Asset Type - The contents of the Asset Type field in the asset record used as a template
  - Owner - The contents of the Owner field in the Asset record used as a template
  - Model - Determined from scheduled scan results
  - Manufacturer - Determined from scheduled scan results
  - Tag Number - Blank
  - Serial Number - Blank unless determined from scheduled scan results. You can populate this field with the operating system serial number by selecting the Populate Asset Serial Number Field with OS Serial Number option on the Asset tab in the Agents screen.
  - Location - The contents of the Location field in the Asset record used as a template
  - Purchase and Maintenance Expiration Dates - Blank
  - Comments - Blank
  - Custom Fields - The contents of the custom fields in the Asset record used as a template
  - Attachments - Blank
  - Dynamic Scans - Blank
  - Scheduled Scan Association - The scheduled scan for the machine that did not have an associated asset record

To distinguish automatically-created asset records after the records are created, you can create a global custom Asset field with "Auto-created" in the label; after the records are created, you can create a Desktop custom view containing that field.

- 2 Enable the Auto Asset Create from Scheduled Scan agent which creates asset records for each machine involved in an scheduled scan that does not have an association with an asset record. It will run every hour based on the time at which the iSupport Agent Manager service is started. You can execute this agent immediately via the Assets tab in the Agents screen. A dialog will appear for selecting the Asset record to be used as a template for automatically creating records; this is a good method to use for control in building asset records for your scheduled.

**Asset Scheduled Scan and Monitoring Agent/Monitoring...days to retain these entries** - Select Yes to enable the Asset Scheduled Scan and Monitoring agent that checks scheduled scan definitions, initiates scans according to schedule, and enables monitoring if configured in an scheduled scan definition. This agent runs every minute. Network monitoring processing adds device state change entries in the database. Use the Monitoring ...Days to Retain These Entries field to control database growth by entering the number of days in which these entries should stay in the database.

**Populate Asset Serial Number Field Using** - Select Yes to populate the Asset Serial Number field with the operating system serial number when Asset records are created automatically for machines that are involved in scheduled scans but not associated with an existing record.

**Default Asset Record Template for Automatic Asset Creation** - Select this link to select the name of an existing Asset record to use as a template when the Auto Asset Create from Scheduled Scan agent is run. The record's asset type will determine the fields that will appear on the automatically-created record.

# Configuring Rules and Rule Groups for Assets

Use the Asset Rules screen to create **rules** that will perform actions when specified conditions based on Asset record fields or events are met. This functionality can be used to:

- Change a field value
- Send notification via email, Desktop, and SMS
- Execute a webhook for posting Asset data to a web application
- Execute a Slack webhook for posting Asset data to a Slack web application

In order for a rule to be evaluated, it must be included in a **rule group**; rule groups are applied to assets through asset types. (A default rule group will apply if none are applicable.) When an Asset record is saved, the matching rule group is first determined. Then, all rules in that matching rule group are evaluated. If a rule's conditions are met, its actions are performed.

You can use the Asset Rule Groups screen to create new rule groups and assign them to asset types. See [“Creating Rule Groups” on page 82](#) for more information.

## Rule Types

- **On Asset Save** rules do not incorporate time frames; when an Asset record is saved, rules in the associated rule group are evaluated, and if true, their actions are performed.

Desktop / Configuration / Options and Tools / Automate / Asset Rules

**Basics**

Name: Change Company Owner Rule

**Configure Conditions**

Rule type is: On Asset Save

Hours of Operation: None

Match: All of the following conditions:

Event is Asset Initially Saved

**Configure Actions**

Change Company Owner To LBLSoft

- **Time-Based** and **Time-Based: Cumulative** rules incorporate time frames with conditions; when conditions are true upon Asset record save, the date and time that the interval time frame would be reached is recorded and monitored by the Time-Based Rule agent.

**Name** Asset 4 Hr Checkout Desktop Notification

---

**Configure Conditions**

Rule type is Time-Based ▼ ⓘ

Hours of Operation: Default Hours of Operation ▼ + ✎

Match All ▼ of the following conditions: + ...

Custom Field ▼
Checked Out
Is
▼
Set Value: Yes
+ - ...

---

**Configure Time Frame Intervals and Actions**

Intervals	Time	Minutes/Hours/Day(s)				
1	4.00	Hours ▼	+ ⌛			
Notify - Desktop ▼	-- Select Recipients -- ▼	-- Select Support Reps -- ▼	-- Select Support Groups -- ▼	Monitor Asset Checkout	+ - ⌛	
<span style="border: 1px solid #ccc; padding: 2px;">Associated Assets' Owners ✕</span>						

If the conditions required to meet the rule do not change before the interval time frame is reached, the agent performs the actions specified. If conditions change prior to the recorded date and time:

- **Time-Based** rules will clear all pending actions and if conditions are met again the time frame will restart.
- **Time-Based: Cumulative** rules will suspend all pending actions and if conditions are met again the time frame will include previous amounts of time in which conditions were met.
- If a date or date/time custom field is created for assets or the Maintenance or Warranty feature is enabled in Feature Basics, **Time-Based: Important Dates** enable you to specify a number of days before or after the value in a specified date field. This type of rule will be evaluated when the defined number of days before or after the

value in the specified date field occurs. Actions will be performed if the rule's conditions are met at the time the Time-Based Rule agent runs..

The screenshot shows a configuration interface for a rule named "Maintenance Expiration Notification".

**Configure Conditions**

- Rule type is: Time-Based: Important Dates
- Hours of Operation: None
- Match: All of the following conditions:
  - Manufacturer: Acme

**Configure Time Frame Interval and Actions**

- Interval: 2.00 Day(s) Before Maintenance Expiration Date
- Action: Notify - Email Associated Assets' Owners With Default Notification Asset Maintenance Notification - Owner

If you are configuring Time-Based and Time-Based: Cumulative rules, ensure that the Time-Based Rules agent is enabled via the button in the Rules list screen.

**Edit Agent Settings**

This agent searches all configured time-based rules, monitors time frames, and performs configured actions if conditions in the rules are met.

**Enable** [Yes] [No] [Run Now]

**Note:** If you change a condition, time interval, or time value in an existing time-based rule and interval timers are in process for any records associated with it, the timers will be reset.

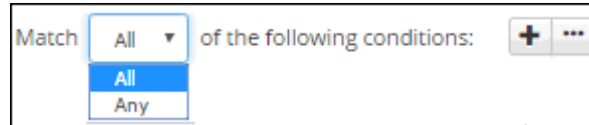
## Creating Rules

Rule creation involves entering a name for the rule, selecting the type of rule, selecting one or more conditions and time frame intervals if applicable, and then selecting one or more actions to perform if those conditions are met. The type of rule will determine the fields that appear. All rules include conditions and actions; see the following sections ["Configuring Conditions" on page 77](#) and ["Configuring Actions" on page 78](#) for more information. See ["Creating Time Frame Intervals" on page 79](#) for information on configuring interval time frames and actions to perform with each set of intervals.

A configured **Hours of Operation** definition of 24 hours a day/seven days a week or selected date and time ranges can be used for the effective time frame for a time-based rule and for an on-save rule with a condition that includes "Within Business Hours". The default Hours of Operation definition assigned to a rule group will apply if no definition is selected for one of its rules. If a definition is selected for both a rule and its rule group, the definition assigned to a rule will take precedence.

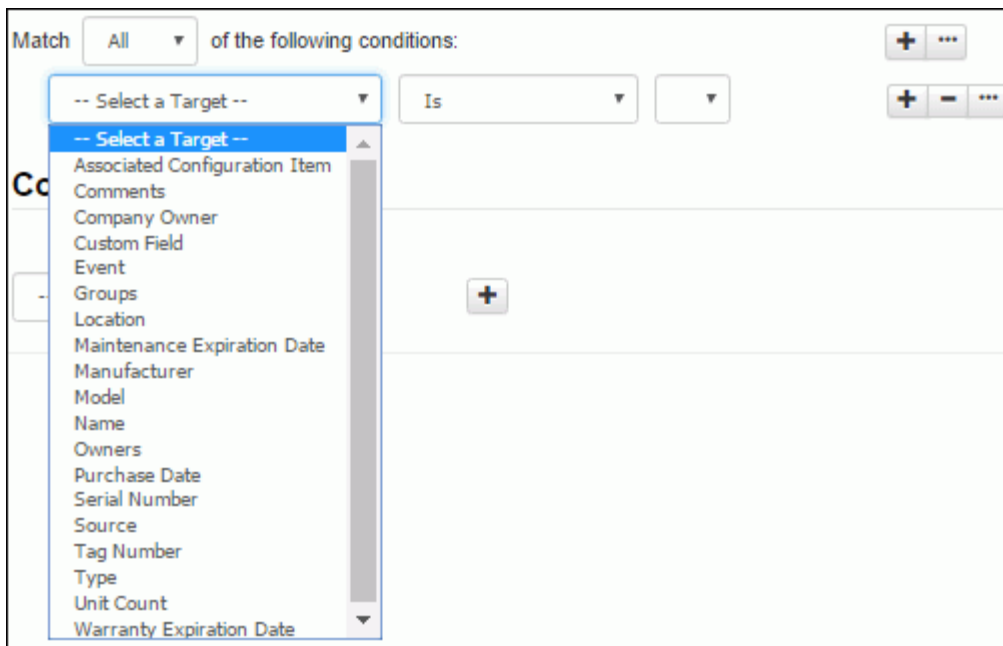
## Configuring Conditions

Use the first Match <All/Any> of the Following Conditions field to specify whether you want **every** configured condition in this rule to be met, or **any** configured condition in this rule to be met.



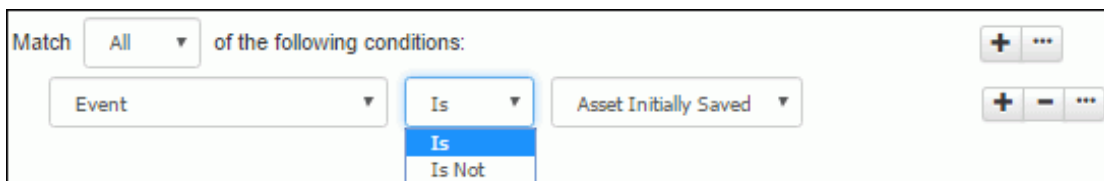
A screenshot of the 'Match' dropdown menu. The text 'Match' is followed by a dropdown menu currently showing 'All'. Below the dropdown, the text 'of the following conditions:' is followed by a '+' button and a '...' button. The dropdown menu is open, showing 'All' and 'Any' as options.

Use the **+** Add Condition and **-** Remove Condition options to display and remove a set of condition dropdown fields (a list of fields, a list of comparison methods, and a list of values applicable to the selected field) to evaluate upon asset save. In the Select a Target dropdown, select what to evaluate: an asset field or event, or whether it is within business hours.



A screenshot of the condition configuration interface. The 'Match' dropdown is set to 'All'. Below it, there is a dropdown menu for 'Select a Target' which is open, showing a list of asset fields: Associated Configuration Item, Comments, Company Owner, Custom Field, Event, Groups, Location, Maintenance Expiration Date, Manufacturer, Model, Name, Owners, Purchase Date, Serial Number, Source, Tag Number, Type, Unit Count, and Warranty Expiration Date. To the right of the target dropdown is a dropdown for the comparison method, currently set to 'Is'. Further right is a dropdown for the value, currently set to 'Asset Initially Saved'. There are '+' and '-' buttons for adding and removing conditions, and a '...' button for adding a condition group.

In the next dropdown, select the comparison method.



A screenshot of the comparison method dropdown menu. The text 'Match' is followed by a dropdown menu currently showing 'All'. Below the dropdown, the text 'of the following conditions:' is followed by a '+' button and a '...' button. The dropdown menu is open, showing 'Is' and 'Is Not' as options. The 'Is' option is selected.

Note that:

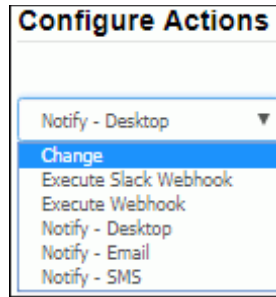
- **Contains** returns a true result if the value is included in the field but other characters are included in a field as well; the value can be embedded in a word.
- **Is** returns a true result if the value is the only set of characters included in a field.

Finally, select the value to be used with the comparison method.

Select **+** Add Condition if you wish to include another condition. You can use the **...** Add Condition Group option to put a set of conditions to be evaluated together in a group.

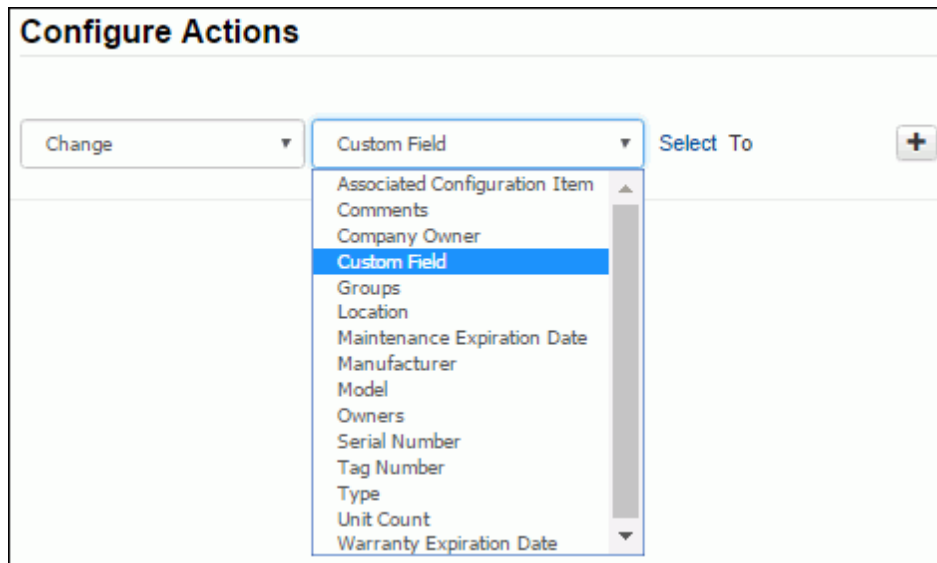
## Configuring Actions


Use the Actions section to select the actions to perform when the conditions are met. After creating the first action you can use the **+** Add Action option to create another action. Use the Remove Action **-** option to remove any action lines.





You can configure the following actions:

- **Change a field** by selecting Change, the field to change, and the value to change it to. For the Groups and Owners fields, there are Add, Remove, and Reset options; the Reset option will result in the removal of any existing owners or groups and addition of the one specified.



- **Execute a configured webhook** for posting Asset data to a web application. See [“Configuring Webhooks” on page 89](#) for more information.
- **Execute a configured Slack webhook** for posting Asset data to a Slack web application.
- **Send a notification** via Desktop notification, email, or SMS.
  - **Desktop notification:** To display an entry in the  Notification list on the Desktop, select Notify - Desktop, one or more recipients, and the text to appear in the Desktop Notification dropdown and/or popup. Options on the Desktop Notifications tab in Preferences (accessed by selecting the avatar/login) determine if an entry will appear as a popup or list entry.

**Email:** If sending a notification via email, select Notify - Email, the recipient, and the notification to be sent.

You can select the default or a custom notification; select the  Show Notification option to display the contents of a selected notification. If possible the notification options will include one of iSupport’s default notifications that match the condition or recipient. Use the **+** Create New and  View/Edit options to access the Custom Notification screen; see [“Customizing and Viewing Event Notification Content” on page 84](#) for more information.

**SMS:** To send an SMS notification, select Notify - SMS, the recipient, and the notification to be sent. The contents of the SMS Text field in the custom notification will be sent; if that field is blank or if it is a default notification, the contents of the Subject field will be used. If sending to a support representative, the message

will be sent to the following in their Support Representative record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the address in the Alt Email field; if that is unavailable, the address in the Email field. If sending to a customer, the message will be sent to the following in their Customer Profile record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the SMS email from mySupport (email to text); if that is unavailable, the address in the Email field. See ["Configuring Twilio Integrations" on page 87](#) for more information on Twilio integration.

**Configure Actions**

Notify - SMS ▼ Associated Assets' Owners ▼ With Custom Notification ▼ Notify Owner Low Unit Count SMS ▼ ⓘ + ✎ +

## Creating Time Frame Intervals

### Time-Based: Important Dates Rules

If a date or date/time custom field is created for assets or the Maintenance or Warranty feature is enabled in Feature Basics, Time-Based: Important Date rules enable you to specify a number of days before or after the value in a specified date field. This type of rule will be evaluated when the defined number of days before or after the value in the specified date field occurs. Actions will be performed if the rule's conditions are met at the time the Time-Based Rule agent runs.

Name

**Configure Conditions**

Rule type is  ⓘ

Hours of Operation:  + ✎

Match  of the following conditions:

+ ...  
+ - ...

**Configure Time Frame Interval and Actions**

Day(s)

Notify - Email ▼ Associated Assets' Owners ▼ With Default Notification ▼ Asset Maintenance Notification - Owner ▼ ⓘ + ✎ +

### Time-Based and Time-Based: Cumulative Rules

With Time-Based and Time-Based: Cumulative rules, the Time Frame Interval Settings section will include Intervals, Time, Minutes/Hours/Day(s) fields as well as a set of fields for entering an action to be performed when the condition is met for the interval time frame. The difference between these rules is that, if conditions change prior to the configured interval settings, **Time-Based** rules will clear all pending actions and the time frame will restart if

conditions are met again; **Time-Based: Cumulative** rules will suspend all pending actions and if conditions are met again the time frame will include previous amounts of time in which conditions were met.

**Name** Asset 4 Hr Checkout Desktop Notification

**Configure Conditions**

Rule type is Time-Based

Hours of Operation: Default Hours of Operation

Match All of the following conditions:

Custom Field Checked Out Is Set Value: Yes

**Configure Time Frame Intervals and Actions**

Intervals	Time	Minutes/Hours/Day(s)
1	4.00	Hours

Notify - Desktop -- Select Recipients -- -- Select Support Reps -- -- Select Support Groups -- Monitor Asset Checkout

Associated Assets' Owners

In the Configure Time Frame Intervals and Actions section, use the Intervals field to specify the number of times a time frame should be established and monitored, and use the Time and Minutes/Hours/Day(s) fields to specify the amount and unit of time (in minutes, hours, or days) in the time frame. *Note that the Day(s) option is calculated with one day equal to 24 business hours.* Use the dropdowns in the indented actions line to specify the actions to perform if conditions are met for that interval time frame. In the example above, the asset will be monitored for a four-hour time frame; if the Checked Out custom field has a value of Yes for the entire four hours, "Monitor Asset Checkout" will appear to the asset owner(s) in the Desktop Notification Center.

History entries related to time-based rules will include the term "exceeded" if conditions have not been met within a defined interval, and the term "fulfilled" if a rule is invalidated or reset due to a change in rule configuration.

### Configuring Multiple Time Frame Intervals

You can select Add Interval to add another interval time frame set and actions to perform if conditions are met for that interval time frame. The Move Down and Move Up options will appear for changing the order in which the interval time frames will be evaluated. In the example below, the asset will be monitored for a four-hour time frame; if the asset type remains at Widgets and the unit count remains at two for the entire four hours, the Asset Low Unit Count Notification - Owner notification will be sent to the asset owner. The asset will then be monitored for an



additional four-hour time frame; if the Checked Out custom field has a value of Yes for the entire four hours, the Eight Hour Checkout Notification will be sent to Barry White.

Name: Asset 8 Hr Checkout Notification

### Configure Conditions

Rule type is: Time-Based: Cumulative

Hours of Operation: Default Hours of Operation

Match: All of the following conditions:

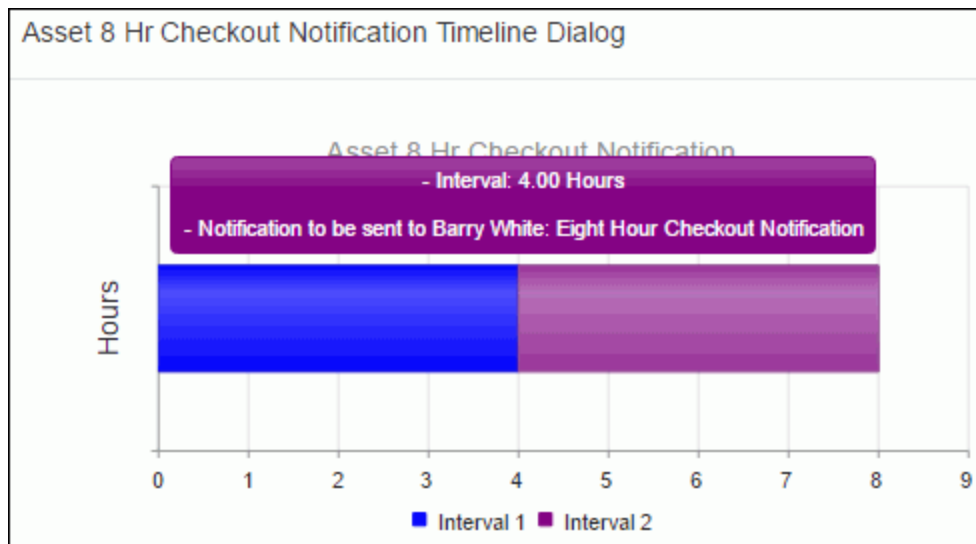
Custom Field Checked Out Is Set Value: Yes

### Configure Time Frame Intervals and Actions

Intervals	Time	Minutes/Hours/Day(s)	
1	4.00	Hours	+ -
Notify - Desktop -- Select Recipients -- -- Select Support Reps -- -- Select Support Groups -- Monitor Asset Checkout + - -			
Associated Assets' Owners ✕			
1	4.00	Hours	+ - - +
Notify - Email Selected Support Rep White, Barry With Custom Notification Eight Hour Checkout Notification + - -			

### Displaying a Timeline for Configured Time Frame Intervals

Use the View Timeline button at the bottom of the screen to display a dialog with a gauge chart depicting the time frames for each interval; actions will appear when you hover over a time frame with your mouse.



## Printing a Rule

Select the Print button to display a summary of your entries.

Rule Name:	Asset 8 Hr Checkout Notification
Target Entity:	Asset
Type:	Time-Based
Cumulative:	Yes
Conditions:	Match all of the following conditions: If Custom Field Checked Out is Yes
Actions:	Repeat 1 time(s) every 4.00 hours Desktop Notification to be sent to Associated Assets' Owners: Monitor Asset Checkout Repeat 1 time(s) every 4.00 hours Notification to be sent to Barry White: Eight Hour Checkout Notification
Rule Groups:	

[Print](#) [Close Window](#)

## Associating Rules With Rule Groups

After creating a rule, you'll need to include it in a rule group. You can do this via the Rule Group tab in the Rules screen, or via the Rule Group screen. On the Rule Groups tab, select the Add link. Rule groups configured via the Rule Group screen appear; select the applicable group(s) and select OK.

Basics	<a href="#">Add</a> <a href="#">Remove</a>	
<b>Rule Groups</b>		
<input type="checkbox"/>	Name ▲	Position in Group
<input type="checkbox"/>	Default Asset Rule Group	1 ▼

All rules in the rule group associated with an Asset record are evaluated when the record is saved; the Position field determines the order in which actions are taken when conditions are met. If rules in a group contain duplicate actions, the position will determine the rule that will take precedence.

## Creating Rule Groups

Select the Create link in the Asset Rule Groups screen to create a rule group that can be used as default and/or applied to asset types.

Rule Groups		Search... <span>✕</span>
<b>Asset</b> >	<a href="#">Create</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Rules</a>	
Change	Name ▲	Default
Email	<input type="checkbox"/> Default Asset Rule Group	Default

Complete the fields at the top of the Rule Groups screen.

The screenshot shows the 'Rule Groups' configuration screen. On the left, there are two tabs: 'Basics' (selected) and 'Asset Types'. The main area is titled 'Checkout Notification Rules'. It includes a 'Name' field with the value 'Checkout Notification Rules', a 'This is the default Asset Rule Group' checkbox (checked), and a 'Hours of Operation' dropdown menu set to 'Default Hours of Operation'. Below this is a section titled 'Add Rules to This Rule Group' with two tabs: 'On Save' and 'Time-Based'. There are three buttons: 'Add', 'Remove', and 'Create'. A table below shows a list of rules with columns for 'Name' and 'Position'. One rule is listed: 'Asset 4 Hr Checkout Desktop Notification' with a position of '1'.

**Name** - Enter a name for the rule group; this name will appear in the Asset screen when the rule group is in effect for an asset.

**This is the Default Asset Rule Group** - Select this checkbox to designate the rule group as the one to apply if no rule group is associated with the asset type.

**Default Hours of Operation** - Select the Hours of Operation definition that will apply if no definition is selected for a time-based rule or for an on-save rule with a condition that includes "Within Business Hours" in the rule group. Use the Create New and View/Edit options to access the Hours of Operation definition screen.

### *Adding Rules*

Use the Add link on the On Save and Time-Based tabs to add previously configured rules to the rule group. All rules in the rule group associated with an asset are evaluated when the asset is saved; the Position field determines the order in which actions are taken when conditions are met. If rules in a group contain duplicate actions, the position will determine the rule that will take precedence. You can use the Create button to create a rule and add it to the current rule group.

### *Assigning a Rule Group to an Asset Type*

Use the Add link on the Asset Type tabs to associate the rule group with one or more asset types. You can also do this via the Asset Type screen.

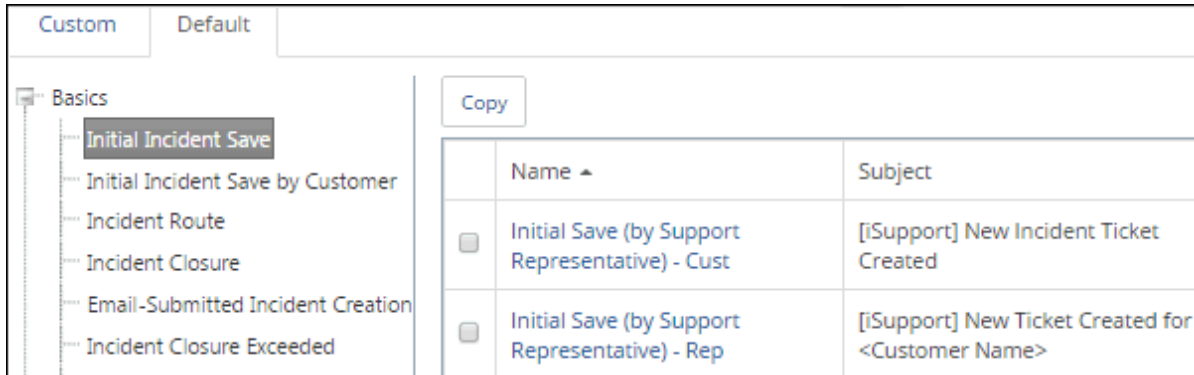
The screenshot shows the 'Asset Rule Groups' screen. The breadcrumb trail at the top reads: 'Desktop / Configuration / Options and Tools / Automate / Asset Rule Groups'. On the left, there are two tabs: 'Basics' and 'Asset Types' (selected). The main area shows a list of asset types with checkboxes: 'Type', 'Cell Phone', 'Desktop', and 'Laptop'. The 'Laptop' checkbox is checked.

# Customizing and Viewing Event Notification Content

Go to Options and Tools | Customize | Custom Notifications to view and customize the content of notifications for iSupport events. All default notifications include "[iSupport]" preceding the subject text, but you can remove that text by creating a custom notification. Event notifications are initiated in two ways:

- For iSupport's Asset, CMDB, Alert, Discussion Digest, and View Subscription functionality, notifications are sent via s configured in the Options and Tools | Administer | s screen.
- For modules with rule-based functionality (Customer, Incident, Problem, Change, Opportunity, Email, Discussion Post, Purchasing, and Knowledge), notifications are sent via rules that will perform actions when specified conditions are met. (The Time-based rule monitors time frames for time-based rules, however.)

In the Custom Notification screen, you can display and copy iSupport's default notifications via the Default subtab, and create new custom notifications via the Custom subtab.



## About Recipients

Recipients for default notifications can include both support representatives and customers, and the default notification text is different for each. Support representative notifications (designated as "Rep") typically contain customer details, the priority, the assignee, the URL to Desktop incident, and the URL to Mobile incident. Customer default notifications (designated as "Cust") typically contain a link to the record on a mySupport portal; this link will go to the URL specified in the mySupport Portal Configuration screen.

Duplicates will be checked in order to prevent a recipient from receiving the same notification more than once. However, duplicate notifications to the same recipient may still occur. For example, if the incident creation notification is configured to be sent to the Customer and CC: Others to Notify as well as the Assignee and CC: Others to Notify, and the customer is on the Others to Notify list, the customer could receive a customer-targeted incident creation notification as well as a support representative-targeted incident creation notification, and the link on the support representative-targeted incident creation notification may not be accessible to the customer. Use the Others to Notify views on the Desktop to review potential notification recipients.

Recipient email addresses are validated; if a blank address exists, no attempt will be made to send it. Automatic notifications sent via agent will note errors in the Event Log. If an agent is run manually, errors will also display in a dialog after the agent runs. The SMTP server will be checked for responsiveness; if it is unresponsive, an error will be included in the log and processing will stop for that time. The notification failure threshold is 36 hours and all attempts will be stopped after that point. If a component of a notification is missing and cannot be resolved, an error will be included in the log and the notification will be deleted after 36 hours.

## Creating a Custom Notification

Use the Custom Notifications screen to select the delivery priority, enter subject and body text, and attach files for a custom notification. You can include data from the associated record via the Include Field link.

The screenshot shows the 'Custom Notifications' configuration screen. At the top, a breadcrumb trail reads: Desktop / Configuration / Options and Tools / Customize / Custom Notifications. The form contains the following fields and controls:

- Name:** A text input field containing 'Initial Save (by Support Representative) - Rep'.
- Delivery Priority:** A button group with three options: 'Low', 'Normal' (selected and highlighted in green), and 'High'.
- Include Attachment(s) from Incident:** A button group with two options: 'On' and 'Off' (selected and highlighted in red).
- Subject:** A text input field containing 'New Incident Created for <Customer Name>'.
- SMS Text:** A text input field containing 'New Incident for <Customer Name>'. Below it, the text 'Subject used if unspecified' is displayed.
- Attachments:** A button labeled 'Attach a file'.
- Design Template:** A text input field containing 'None'.
- Notification Message:** A section with a blue header 'Include Field' and a rich text editor. The editor toolbar includes icons for undo, redo, bold, italic, underline, link, unlink, list, and indent. The font is set to 'MS Sans Ser...' and size to '2'. The message body contains the text: 'This <Priority> priority incident ticket was created for <Customer Name>.' Below the message, there is a section for 'Customer Details' with the text 'Name: <Customer Name>'.

**Name** - Enter a name for the custom notification.

**Delivery Priority** - Select the priority level to assign to the email: High, Normal, or Low.

**Design Template** - If desired, select the design template with the elements (text and images) to appear around the body of the correspondence template and support representative signature (if applicable). You can select the Create New or View/Edit options to access the Design Template screen; see ["Configuring Design Templates" on page 86](#) for more information.

**SMS Text** - Enter the text to be sent when a rule using the Notify - SMS action is met. Note that if this field is blank or if it is a default notification, the text in the Subject field will be used.

If sending to a support representative, the message will be sent to the following in their Support Representative record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the address in the Alt Email field; if that is unavailable, the address in the Email field. See ["Configuring Twilio Integrations" on page 87](#) for more information.

If sending to a customer, the message will be sent to the following in their Customer Profile record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the SMS email from mySupport (email to text); if that is unavailable, the address in the Email field.

**Subject/Notification Message** - In the Subject field, enter the subject line for the email notification.

On the Body tab, enter the body of the email notification. You can select the Notification Message link to display a larger window for entry. Use the Include Field link to add field values from the current record. The field will be

included in brackets, and the field data will be inserted into the email when it is generated. (If data does not exist for a required field, nothing will be inserted; the field area will be blank.)

You can append **:label:string** to the <URL to x> include fields so the link displays as linked text rather than the full URL. The <Rep URL to Read Online> and <mySupport URL to Read Online> include fields will include a link for viewing the email on the web (typically for customers who aren't able to see an email properly rendered with linked images via their mail client).



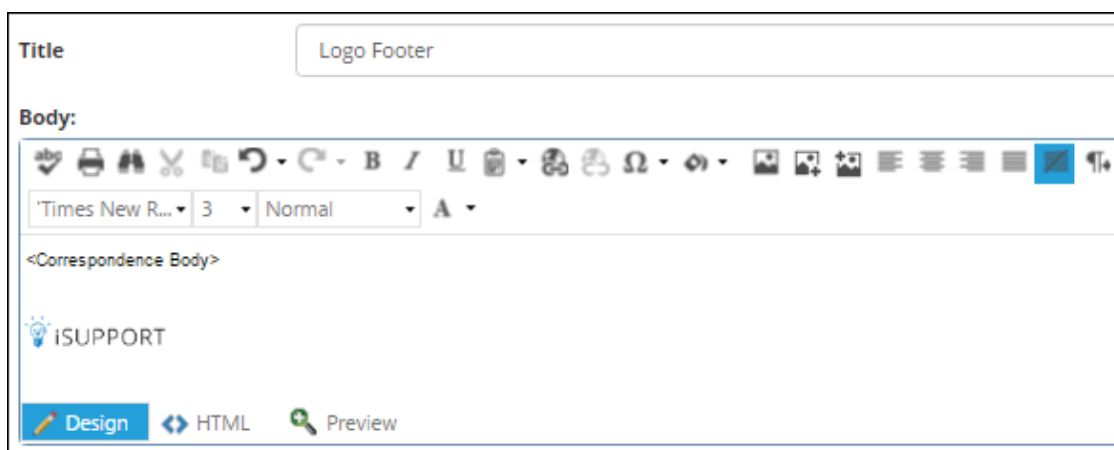
**Include Attachment(s) from <record type>** - For all modules except Asset, CMDB, Discussion Posts, Security, and Alerts, select this checkbox to associate any attachments from the referenced work item type to the notification when it is sent.

**Attachments** - Use the Attachments tab to attach a file to be sent with the notification.

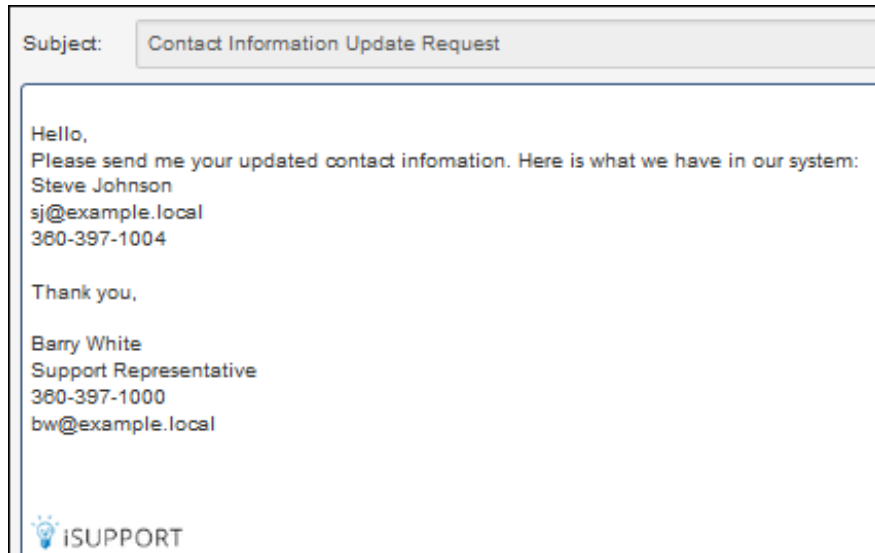
**Note:** If data does not exist for a required field, nothing will be inserted when the email is generated. The field area will be blank.

## Configuring Design Templates

Use design templates to add common design elements such as header and footer text or images to outbound email generated from iSupport. Use the Design Templates tab in the Core Settings | Email screen to enter a title and text and images; the <Correspondence Body> tag indicates where the email data will be inserted when the design template is applied.



If a support representative sending a correspondence with the design template has a signature block, design elements that are after the <Correspondence Body> tag will appear after it.



## Displaying the Notification Queue

Use the Notification Queue option under Options and Tools | Administer to display all notifications that have not been sent. You can use the checkboxes to restrict the notifications to appear in the screen, and delete any notifications that you do not wish to be sent.

View:  Incident  Change  Problem  Purchase  Service Contract  Configuration Item

<input type="checkbox"/>	Type	Event	Date Created ▾	Number
<input type="checkbox"/>	Purchase	Initial Purchase Request Save	2/2/2019 2:32:49 PM	G22F435A17
<input type="checkbox"/>	Purchase	Initial Purchase Request Save	2/1/2019 11:25:28 AM	G21C3639A7
<input type="checkbox"/>	Service Contract	Initial Save	1/26/2019 10:31:17 AM	G1RB351683

## Configuring Twilio Integrations

iSupport integrates with Twilio for sending iSupport notifications to support representatives via SMS (Short Message Services) messaging. Rules with the Notify - SMS action will send the contents of the SMS Text field in the specified notification; if that field is blank or if it is a default notification, the text in the Subject field will be used.

If sending to a support representative, the message will be sent to the following in their Support Representative record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the address in the Alt Email field; if that is unavailable, to the address in the Email field. If sending to a customer, the message will be sent to the following in their Customer Profile record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the SMS email from mySupport (email to text); if that is unavailable, the address in the Email field.

Rules can change the Twilio integration (phone number to which an iSupport SMS notification is sent) used for a work item.





# Configuring Webhooks

Use the Webhooks screen to configure webhooks for posting iSupport data to a web application. You will specify a web application URL for iSupport to post data to and the fields containing the data you want to receive, and iSupport will post the field data to the URL when configured rule conditions and time frames are met.

In the Webhooks screen, enter the name of the webhook definition that will be used in the Rule screen and URL to which iSupport data should be posted. Drag the iSupport data source fields containing the data you want to receive into the frame on the right, and enter the corresponding fields on your web form in the Parameter Name column. Note that you can drag field rows vertically to reposition fields. Use the Content Type field to enable the output to be set to JSON (JavaScript Object Notation) Mime type and display the text of what the webhook will generate.

The screenshot shows the 'Incident Webhooks' configuration interface. At the top, the breadcrumb trail reads: Desktop / Configuration / Options and Tools / Integrate / Incident Webhooks. The main form includes the following fields:

- Name:** Webhook
- URL:** http://xxxxxxxxxxxxxxxx/webhookexamples/webhook
- Content Type:** x-www-form-urlencoded (selected), JSON (highlighted in green)

Below these fields is a section titled 'Parameters & Payload Example'. On the left, a tree view under 'Basics' lists fields: Identifier, Number, Status, Status Identifier, and Priority. In the center, a table maps iSupport fields to parameter names:

iSupport Field	Parameter Name
Number	Number
Identifier	Identifier

On the right, a JSON payload is displayed: 

```
{ "Number": "Number", "Identifier": "Identifier" }
```

Use the applicable Rule screen to configure the conditions and time frame on which the post action will occur. Select the rule type, enter the condition(s) to be met in order to initiate the post, select the Execute Webhook action, and then select the webhook definition. Be sure to add the rule to a rule group.

The screenshot shows the 'Incident Rules' configuration interface. The breadcrumb trail is: Desktop / Configuration / Options and Tools / Automate / Incident Rules. The 'Basics' tab is selected, and the 'Webhook Rule' is being configured.

**Name:** Webhook Rule

**Configure Conditions**

- Rule type is:** Time-Based
- Hours of Operation:** None
- Match:** All of the following conditions:
  - Custom Field: Current Project Is Set Value: Beta

**Configure Time Frame Intervals and Actions**

Intervals	Time	Minutes/Hours/Day(s)
1	0.50	Hours

**Actions:** Execute Webhook (Action) | Webhook (Definition)