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.

In iSupport, Asset records can be created in the following ways:

- Create an Asset record via the Rep Desktop and the Incident, Problem, Change, and Purchase Request screens.

- **Utilize Active Directory and LDAP** as a source for Asset information via the Data Source Integration feature.

- **Import** from one or more Microsoft SQL Server source databases and **synchronize** with iSupport's Asset database.

- Import from a Microsoft Excel file.

- 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. See the online help for more information.

- Configure Asset records to be **created automatically** based on systems included in a scan.

In addition to associating Asset records with work items (incidents, problems, changes, etc.), you can scan **bar codes** and print bar code labels and **assign service contracts** for tracking and restricting incidents and changes associated with assets. Contracts can be based on work item count (a specified number of incidents and/or changes), hourly count (a specified number of hours), duration (time frame in days), or a combination (limiting the number of incidents and/or changes within a specified daily time frame). See the online help for more information.

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 3 for more information.

- 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.

- Associate a collection of assets for viewing, reporting, and restricting access and display of an asset to members of a support representative group via the Core Settings | **Groups** screen. See "Creating Asset Groups" on page 10 for more information.

Optional Customization

- Create and customize Asset event **notifications** for low unit count tracking and maintenance and warranty expirations. You can use or modify iSupport's default notifications or create new notifications via the Custom Notifications screen. See the online help for more information.

- Set up **custom fields** to include in the Incident screen via the Options and Tools | Customize | Custom Fields screen. See "Configuring Custom Fields" on page 12.

- iSupport includes a default Asset screen **layout**; go to Options and Tools | Customize | Layouts to redesign it to include fields and tabs that are specific to your company and assign layouts to asset types. See "Configuring Screen Layouts" on page 17.

Optional Integration

- Utilize Active Directory and LDAP as a source for asset information via the Options and Tools | Integrate | **Data Source Integration** screen. See "Using the Data Source Integration Feature" on page 22.

- **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. See "Importing From a Remote Asset Database and Synchronizing" on page 28 for more information.

- **Import asset data from a Microsoft Excel spreadsheet** via the Options and Tools | Integrate | **Asset Import** feature. See "Importing Asset Data from a Microsoft Excel File" on page 40.

- Configure **webhooks** for posting Asset data to a web application. See "Configuring Webhooks" on page 42.

Optional Automation Features

- Configure **scheduled scans** based on a specified range of IP Addresses, an Active Directory Path, and domain names via the Options and Tools | Automate | Asset Scanning and Monitoring screen. You can also configure **monitoring** to track the state of devices included in a scan definition and their CPU, memory, disk space, and services. See "Configuring Scheduled Scans and Device Monitoring" on page 45. Configure Asset records to be **created automatically** based on systems included in a scan; see"Creating Asset Records Automatically Based on Scheduled Scans" on page 61 for more information.

- To automatically create more than one Asset record, enter data to populate fields in all records created, and display prompts for entering data unique to a record, use the **Asset Wizard** (accessed via the Desktop menu). See "Using the Multiple Asset Creation Wizard" on page 43.

Configuring Asset Types

Use asset types to classify similar assets (for example, printers and laptops). To access the Asset Type screen, select Asset Types and click the Create link. 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 17 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.

Enable Count Tracking - Select Yes to enable Unit Count, Unit Label, Unit Cost, and Unit List Price fields to appear in the Asset screen if the type is selected and send a Low Unit Count notification if applicable. The Low Unit Count notification is configured on the Notifications tab.

Basics ❯	**Asset Type Name**	Memory Upgrade
Custom Fields	**Layout**	Default ˅ ➕ ✎
Maintenance/Warranty	**Enable Count Tracking**	**On** Off
Notifications	**Who to Notify of Low Unit Count**	☐ Owner ☑ Other
	Email Addresses of Other Recipients	sj@example.local
	Number of Units Remaining to Send Notification	2.00
	Enable Scanning	On **Off**
	Optional Fields	☐ Owner ☐ Location ☐ Model ☐ Manufacturer

The Unit Count, Unit Label, Unit Cost, and Unit List Price fields will be included in the Asset screen if the type is selected.

Unit Count	20.00
Unit Label	Stick
Unit List Price	$100.00
Unit Cost	$50.00

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 click the Update Unit Counts link, enter the number of units used, and decrement the unit count.

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.

Who to Notify of Low Unit Count/Email Addresses of Other Recipients - If enabling count tracking, 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.

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.

Entering Optional and Custom Fields

You can set up custom fields and optional fields such as Owner, Tag Number, and Location to display in the Asset screen when the asset type is selected.
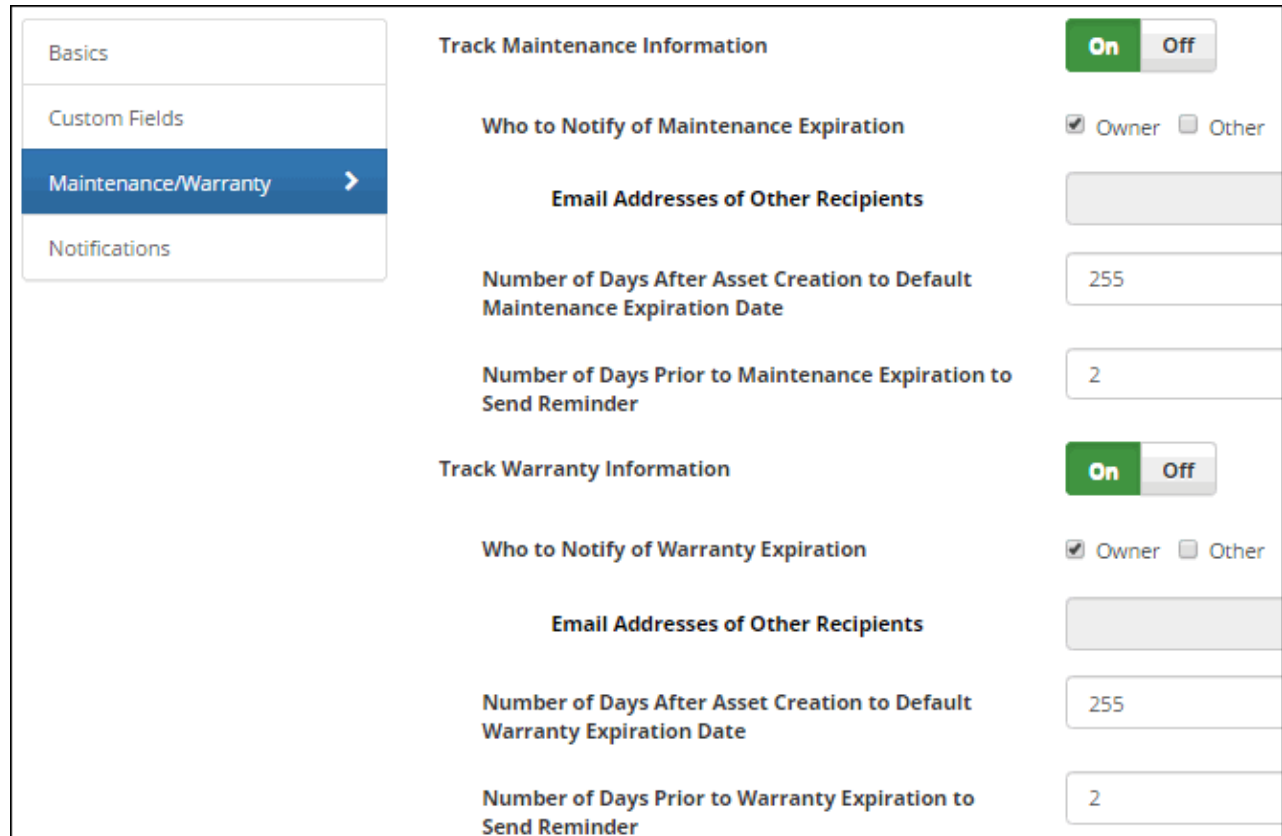
In the **Optional Fields** section, select the checkbox next to each field that should display when the asset type is selected in the Asset screen.

In the **Custom Fields** section, click 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.

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 7.

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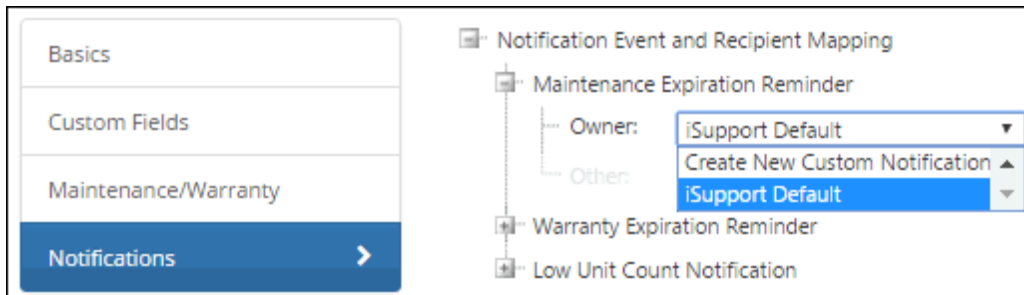
Maintenance Expiration Reminder - Select the recipients and notifications to be sent according to the settings on the Maintenance/Warranty tab. The notifications will be sent on the schedule of the Asset Reminder agent.

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

If maintenance or warranty expiration functionality is configured, schedule the Asset Reminder agent on the Agents tab.

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.

If unit count tracking is configured for an asset type, go to Feature Basics and schedule the Asset Unit Count Tracking agent on the Asset Management tab.

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.
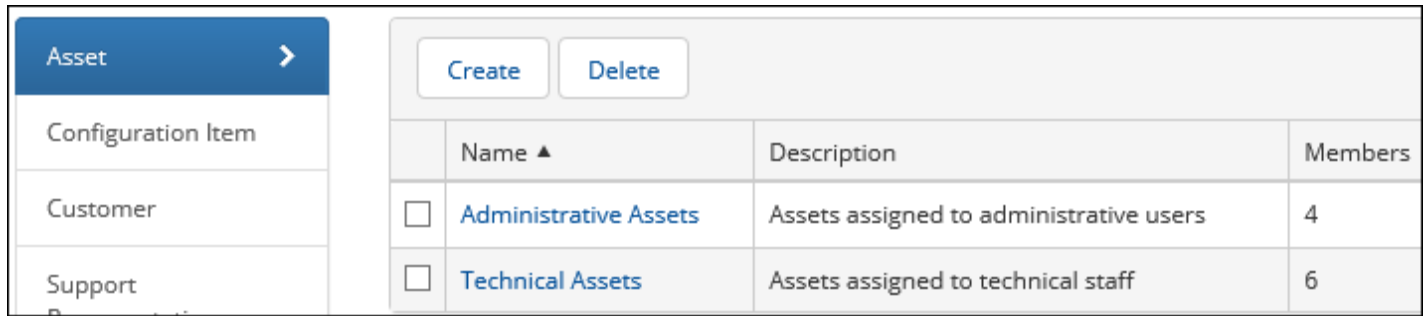
Enable   [Yes] [No] [Run Now]

Time Agent Should Run Each Day   10:30 PM ▾

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.

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 Asset Groups.

Asset	>	Create	Delete		
Configuration Item		Name ▲	Description		Members
Customer		☐ Administrative Assets	Assets assigned to administrative users		4
Support		☐ Technical Assets	Assets assigned to technical staff		6
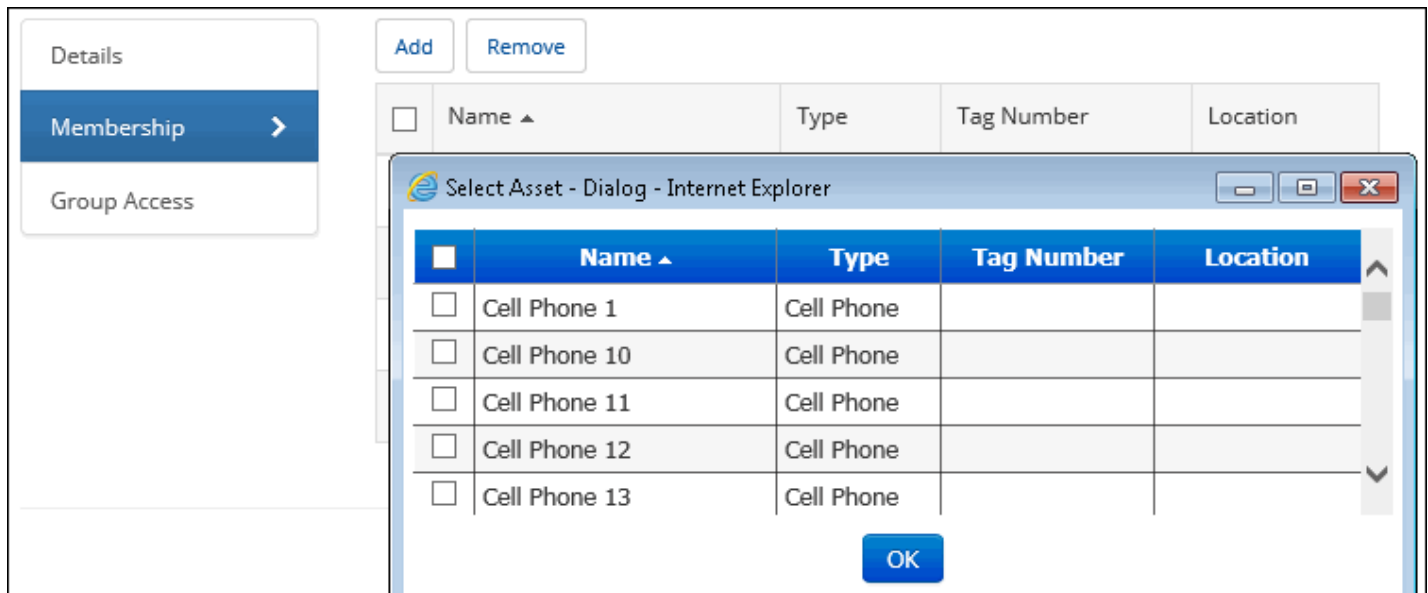
The following screen appears; enter the name and description of the group on the Details tab.

Details	>	Name	Administrative Assets
Membership		Description	Assets assigned to administrative users
Group Access			

Adding Assets to Asset Groups

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

Details		Add	Remove			
Membership	>	☐ Name ▲		Type	Tag Number	Location
Group Access						

Select Asset - Dialog - Internet Explorer

☐	Name ▲	Type	Tag Number	Location
☐	Cell Phone 1	Cell Phone		
☐	Cell Phone 10	Cell Phone		
☐	Cell Phone 11	Cell Phone		
☐	Cell Phone 12	Cell Phone		
☐	Cell Phone 13	Cell Phone		

OK

To add an asset to the group, click the Add link. Select an existing asset and click 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. Click 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 click 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 click the Add to Group and Remove From Group options.
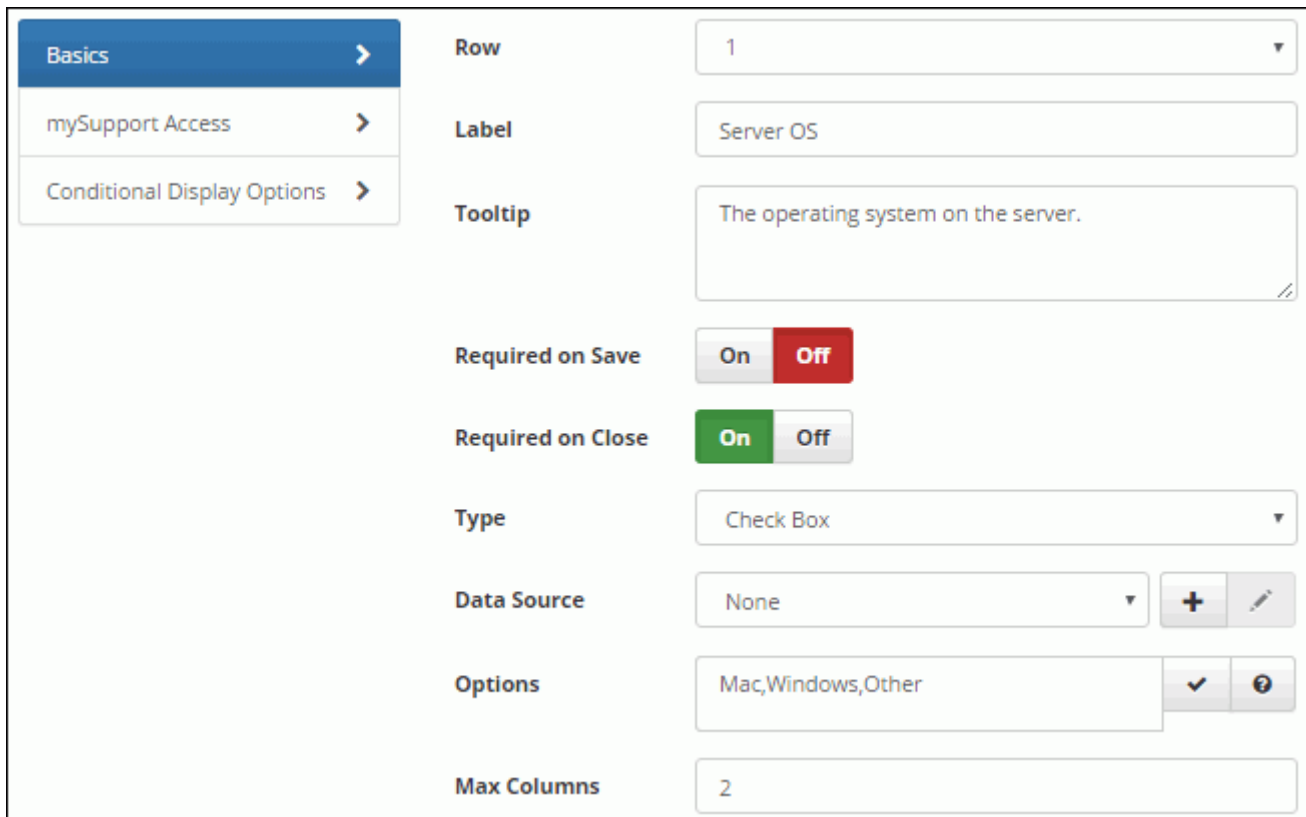
Configuring Custom Fields

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 (SD Edition)

Note that in addition to these settings you can use the Category entry screen to enter custom fields that will appear only when a category is selected in a work item screen, and use the Asset Type configuration screen to enter custom fields that will appear only when an asset type is selected.

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.

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 15 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 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 **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.

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 click the Commit Items ✔ icon 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 15 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, click the row number and then click the Delete link. To delete multiple custom fields, select the fields and click the Delete link. To edit a custom field, click the label link.

mySupport Access Options

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

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.

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 ➖ icons to display and remove a *<field>* is *<value>* search condition. Click the Add Condition ✚ icon if you wish to include another condition. You can use the Add Condition Group ⋯ icon to put a set of search conditions to be evaluated together in a group.

In this example, the field will appear if the value in Department Code custom field is 300 and the value in the Budget Code custom field is 500.

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. Click 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.
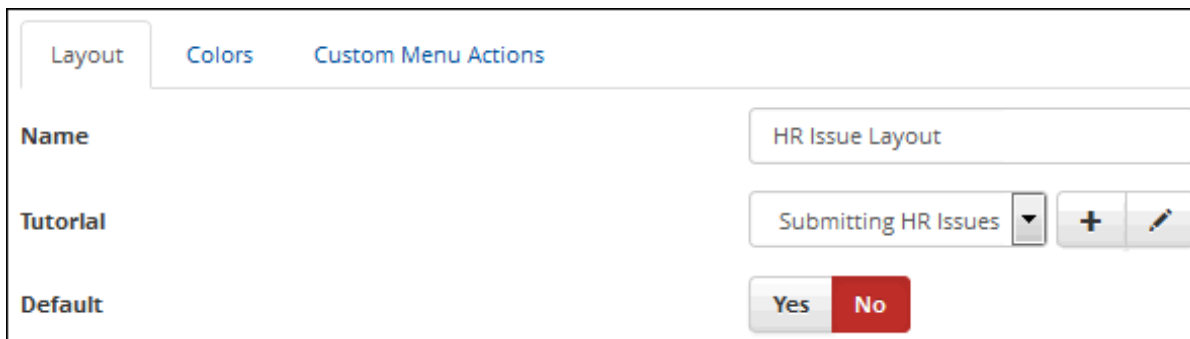
Basics >	
mySupport Access	
Conditional Display Options	

Row	5
Label	Affected Item
Tooltip	
Required on Save	On **Off**
Required on Close	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 and the display and submit screens used by customers on the mySupport portal. Use the Layout screens in each configuration module (except CMDB) to modify these layouts and use fields and tabs that are specific to your company. You could create layouts based on different types of users, different types of work, etc. Note that layouts configured via the Layout screen in each module **will not** apply to smart phones; only layouts configured via the Mobile Settings screen will apply to the mobile HTML5 interface.

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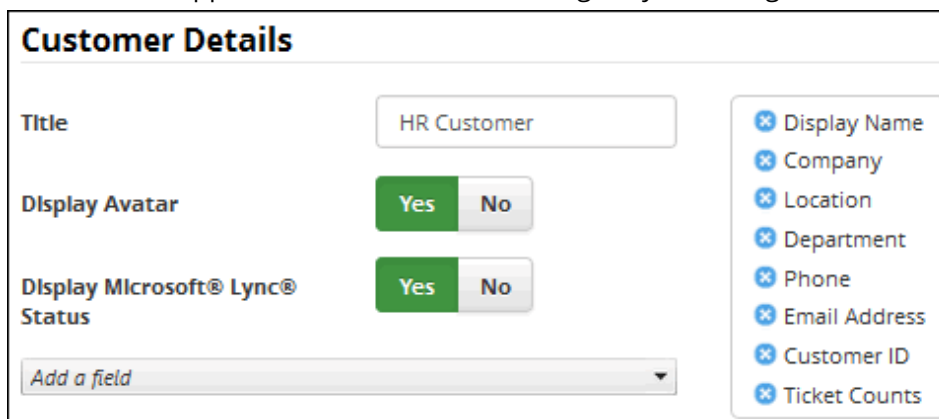
For Rep Client layouts, you can use the Preview button at the bottom of the Layout screen after adding required fields to the form to display your layout. You'll need to select a record to use for displaying field data.

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 click to display an additional screen of content. Use the Create New ➕ and View/Edit ✏ icons 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 the **Default Layout** checkbox to display the layout if none is associated with current support representative group, customer group, category, incident template, or hierarchy template.

Configuring Customer Details

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

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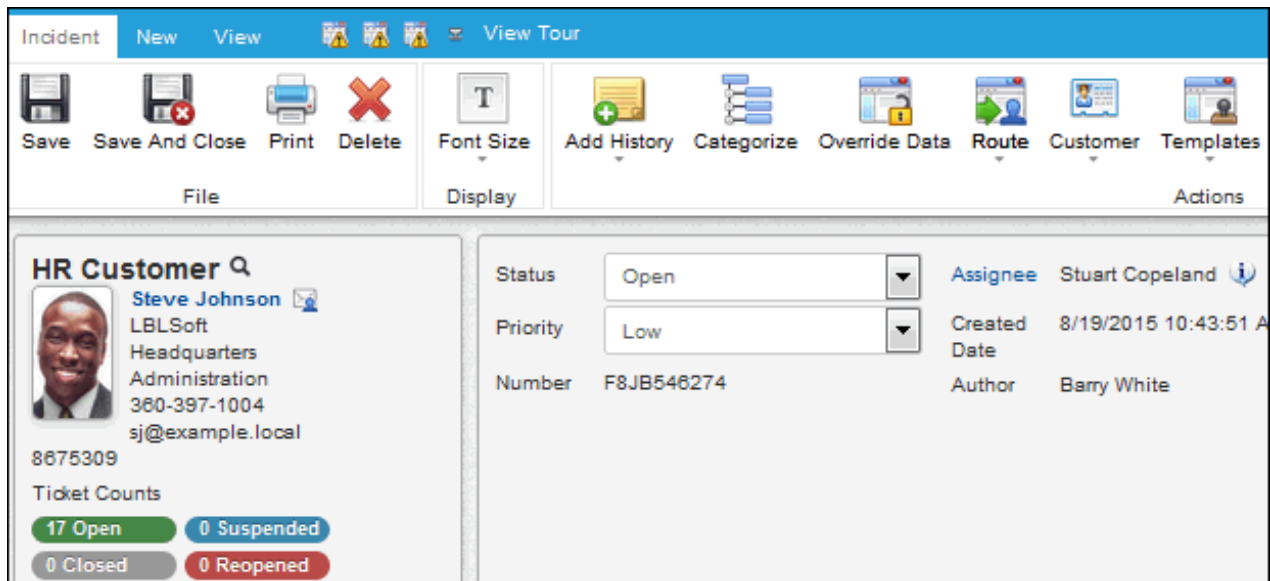
Use the **Display Microsoft® Lync® Status** field to include an icon that will display the Microsoft Lync status of a selected customer in the Incident and Change screens and enable the support representative to access Microsoft Lync functions. In order for the icon to appear, Microsoft Lync 2013 must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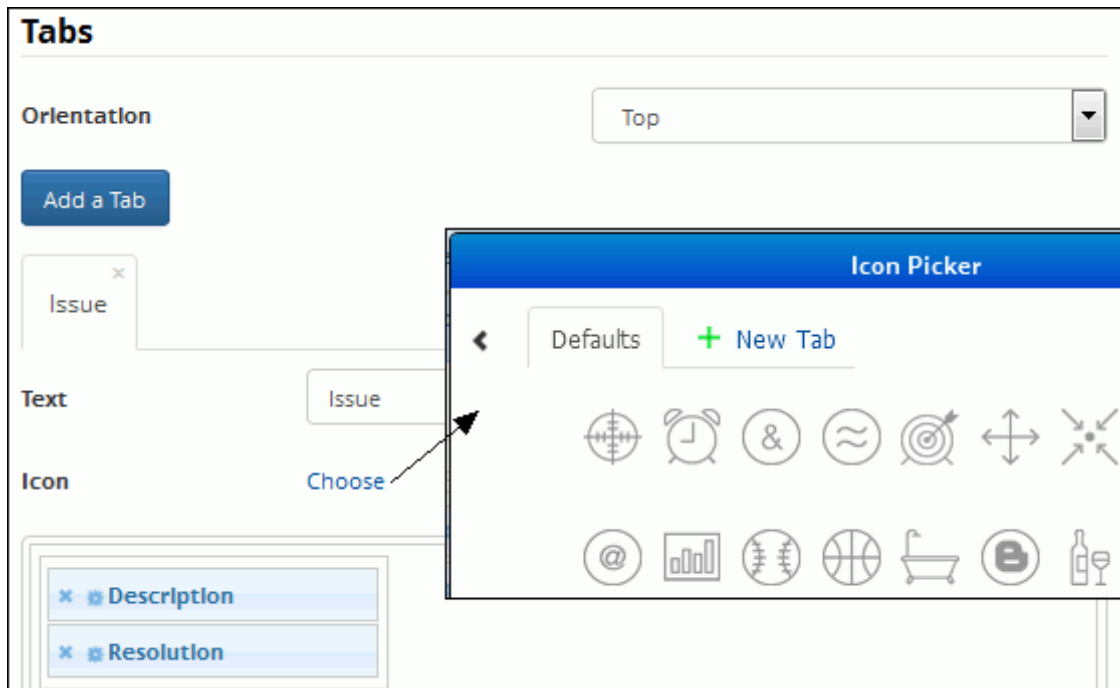
Adding Fields and Tabs

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. For custom fields, you can either drag the fields under Custom Fields individually or you can drag Custom Fields under List Items to drag all of the custom fields at once. Required fields are designated with an asterisk in the selector on the left.
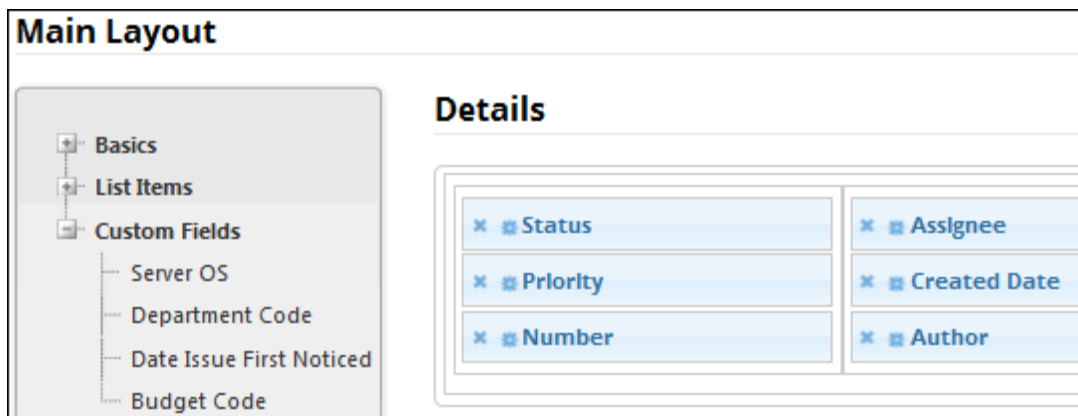

A **[Separator]** field is included for mySupport layouts; it will be blank after you drag it to the Details section or a tab. You can enter a label for it or leave it blank, and it can be used multiple times for adding blank areas to your layout. A Save Button option is included in Submit layouts; if 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, click the Add a Tab button and then click on the new tab (named "Tab" by default). Use the Text field to enter the label

for the tab. Click 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.)
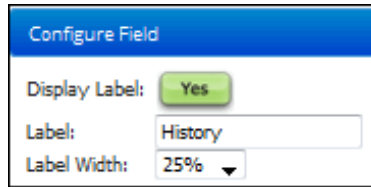

To add fields to the tab, drag fields from the selector on the left side of the Layout screen to the middle of the section below the Icon field.
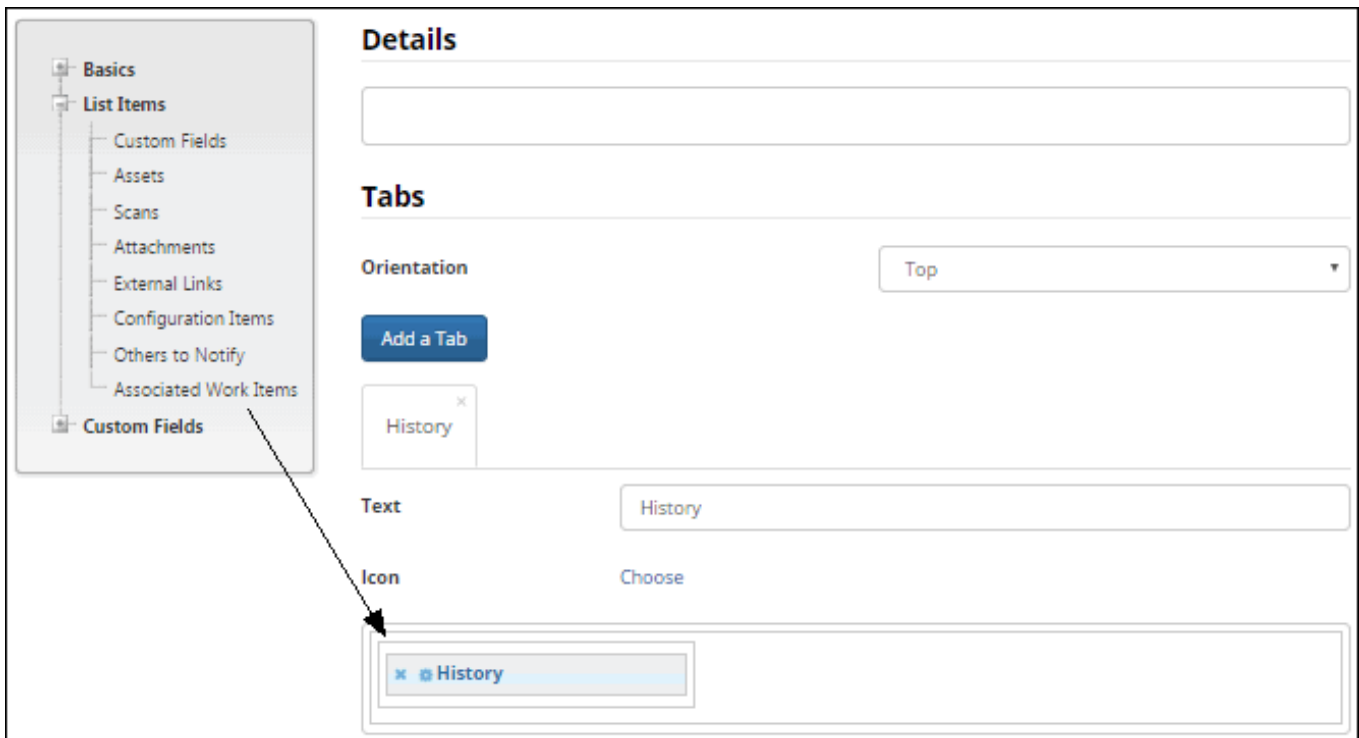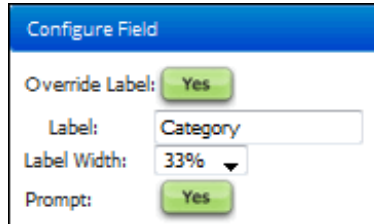
Configuring Fields

After adding a field, click the Configure Field ⚙ icon 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.

An **Override Label** field will be included for mySupport layouts; select Yes 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.
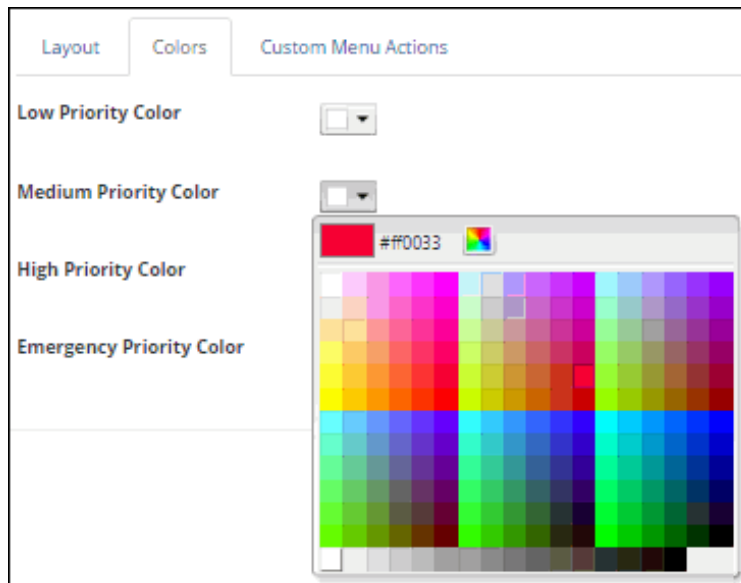

A **Prompt** field will be included for the Category field on mySupport layouts; enable it to initially display the Category Select dialog when the Incident or Change Submit screen appears.
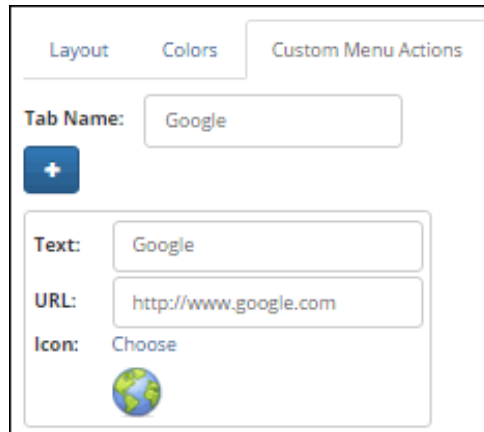
Configuring Priority-Based Background Colors

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.

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.

Using the Data Source Integration Feature

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. If utilizing multiple customer data sources, see "Specifying Precedence for Multiple SQL Data Sources" on page 39.

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

	Name ▲	Type	Active	Source	Synced Record Types
☐	Domino Directory	Domino Directory	Yes		Customers
☐	LDAP Source	LDAP	No	xx.xx.x.xx:xxx	Customers
☐	Main AD Sync	Active Directory	No	LDAP:// xx.xx.x.xx:xxx	Customers
☐	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 37

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.

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. Click the Create link to create a sync definition.

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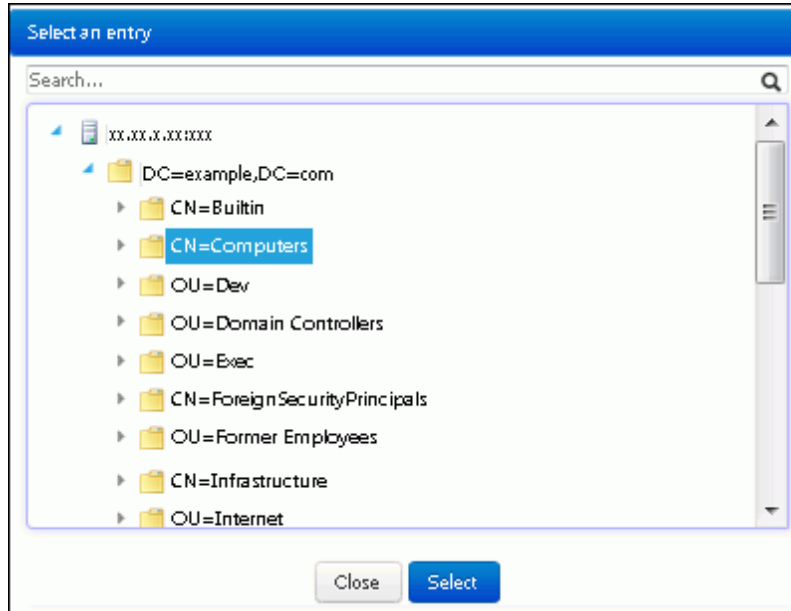
Search Filter - Enter the conditions that must be met for returning a specific set of information to iSupport. Note that a filter is only needed if the selected Base DN contains unwanted lower level nodes or if the data source's exclusions do not already remove the unwanted nodes.

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.

Field Mappings

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

Mapping options include:

- Use iSupport Default which populates the default mapping; see the data map on page 35 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 click the Add to Group icon.

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

	Field	Attribute
Sync Definitions	First Name	Use iSupport Default ▾
Field Mappings ❯	Last Name	Use iSupport Default ▾
Exclusions	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 ▾

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**

Avatar   [Unmapped] ▾

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; click 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.
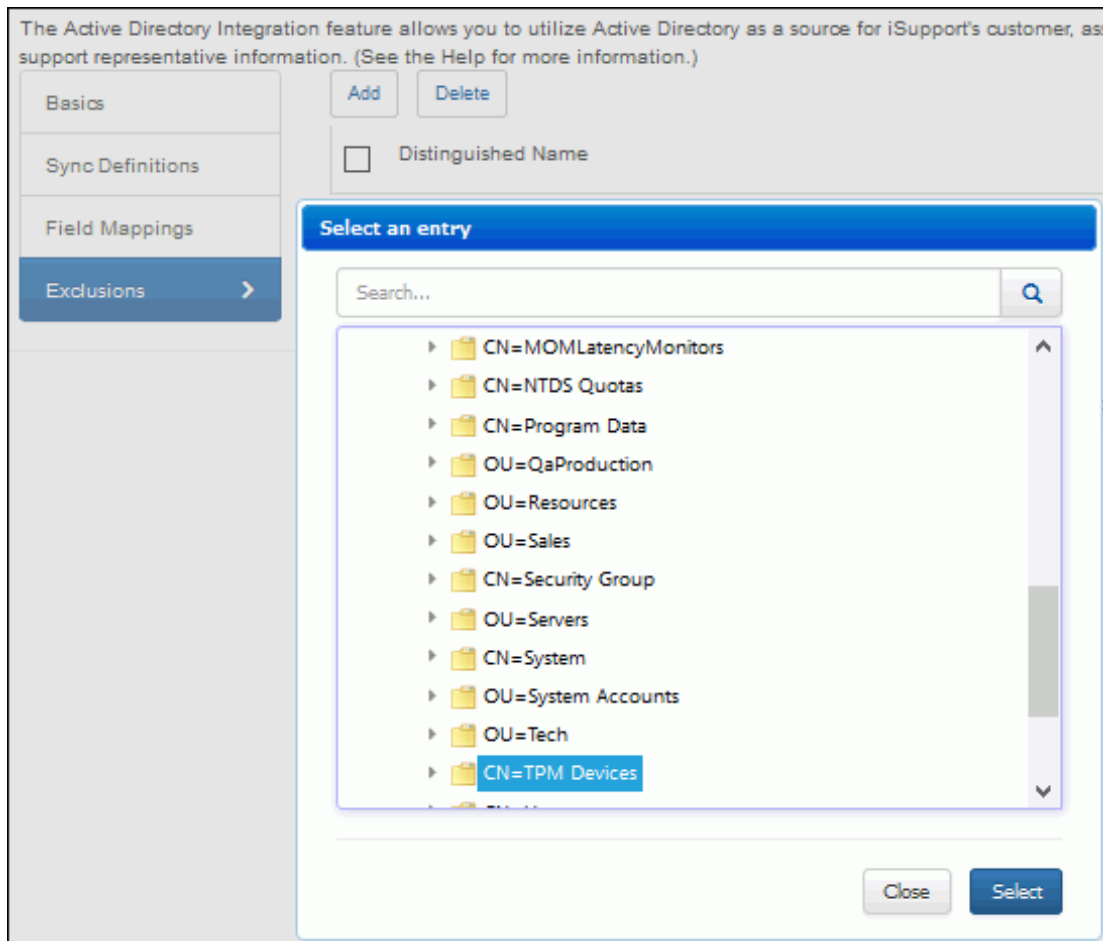
Integrating with LDAP

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.

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.

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 - Click 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.

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.


Mapping options include:

- Use iSupport Default which populates the default mapping; see the data map on page 35 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.
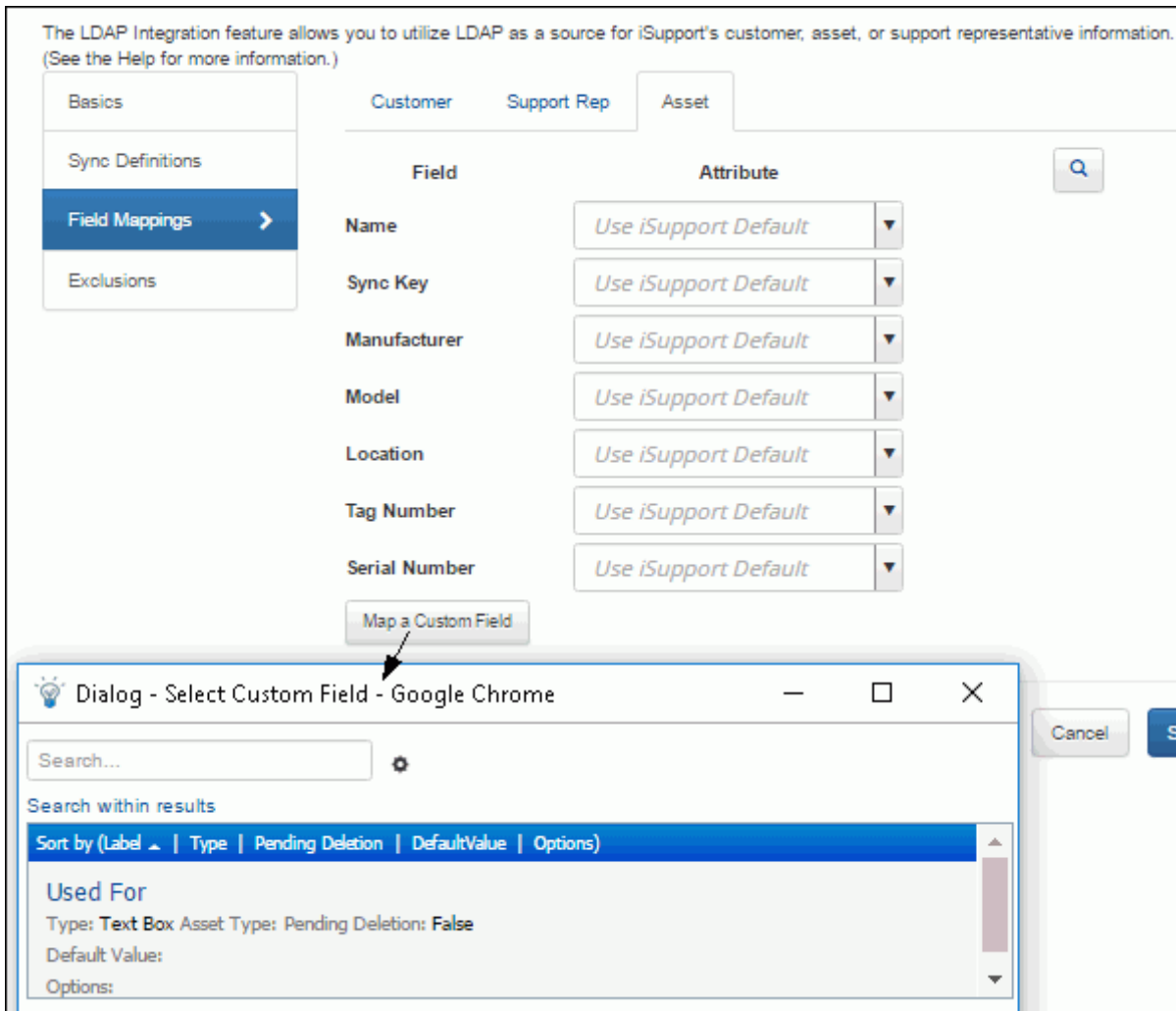
Use the Preview 🔍 button to select a record to use for verifying your selections. Values from the record will appear next to the fields.

Configuring Exclusions

Use the Exclusions tab to specify the values that should not be synchronized; click 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.
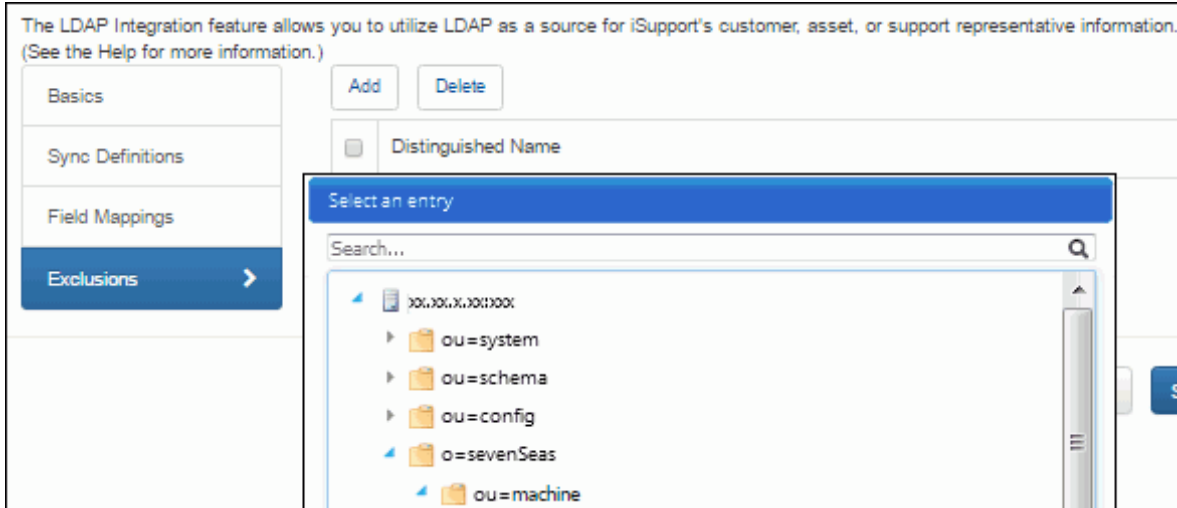
Active Directory/LDAP Integration Data Map

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 *username* 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

iSupport Customer Field	iSupport Default
ZIP	postalCode
Country	co
Manager	manager
Company	company
Customer ID	*(unmapped)*
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 click 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.

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. Click 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.

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.

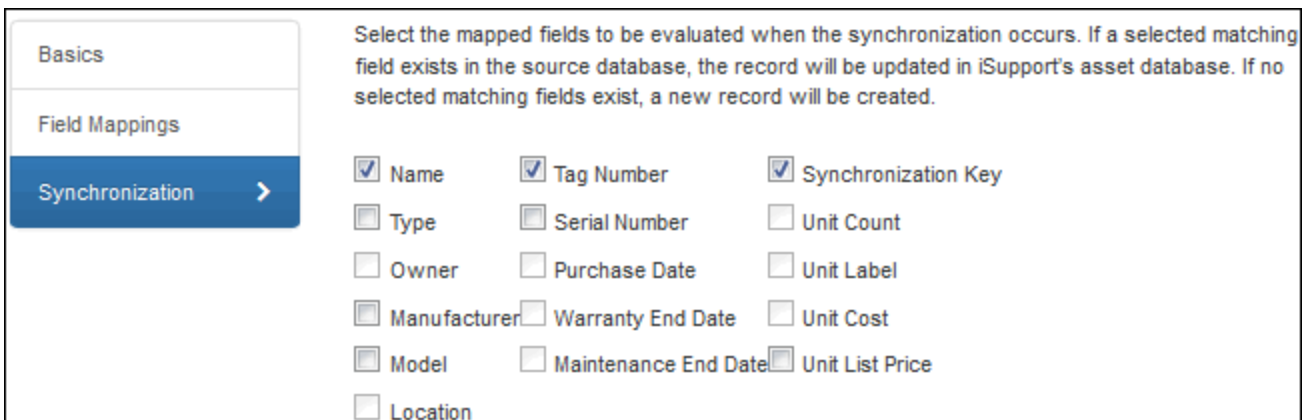- Off to assign the customer in the Default Owner field as the asset owner of all imported records.

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 click 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 click the ➡ button. The associated fields display under Mapping. To remove an entry from the Mapping section, select the entry and click 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 click Save to save your selections. The synchronization will occur when the Sync button is clicked 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.


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.
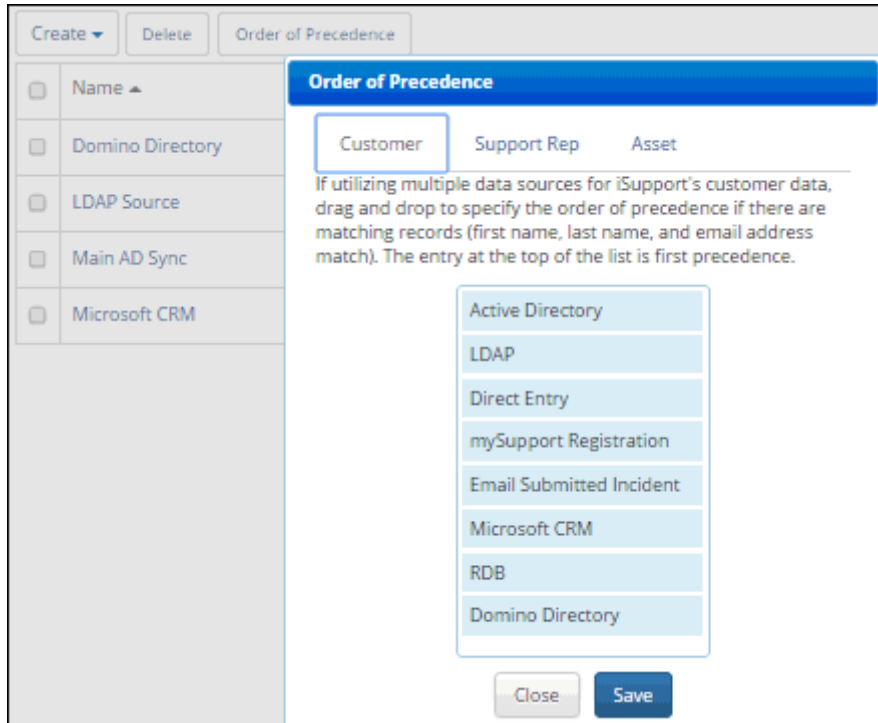
Importing Asset Data from a Microsoft Excel File

Use the Asset Import feature to import asset data from a Microsoft Excel file into iSupport's Asset database. **Note that this feature requires that the Enable 32-Bit Applications setting is enabled for the application pool associated with iSupport.** This import will only work with .xls or .csv files unless newer access drivers are installed onto the hosting server. 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.

Click the Browse button to select a Microsoft Excel file containing the asset information. Click 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.

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 click the right arrow ➡ button. The associated fields display under Mapped Columns.

• To remove an entry from the Mapped Columns list, select the entry and click the left arrow ⬅ button.

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

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 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.

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.

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. Click 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 click Next.

Asset Fields

Creating Asset 1 of 5

Tag Number:	C10-
Serial Number:	94818-86182

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

Finish

5 out of 5 assets created.

Save asset profile?

Name:

Laptop

Description:

Laptop shipment from Computers Inc.

Save

# Configuring Scheduled Scans and Device Monitoring

Scheduled scans 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	**Title:**	Inventory Scan
Computer System	**Scan Date:**	11/23/2009 1:25:35 PM
Operating System		
Processes	**COMPUTER SYSTEM**	
Services	**Description:**	AT/AT COMPATIBLE
Logical Drives	**Domain:**	nec.com
Software Titles	**Domain Role:**	Member Workstation
Hot Fixes	**Manufacturer:**	LENOVO
Network Adapter	**Name:**	DOC
Modem	**Model:**	88109AU
Parallel Ports	**Processors:**	1
Serial Ports	**Owner Name:**	Lisa
Port Connections	**Status:**	OK
Desktop Monitor	**Total Physical Memory:**	3 GB
Keyboard	**OPERATING SYSTEM**	
Pointing Device	**Name:**	Microsoft Windows XP Professional
	Version:	5.1.2600 Service Pack 3

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.
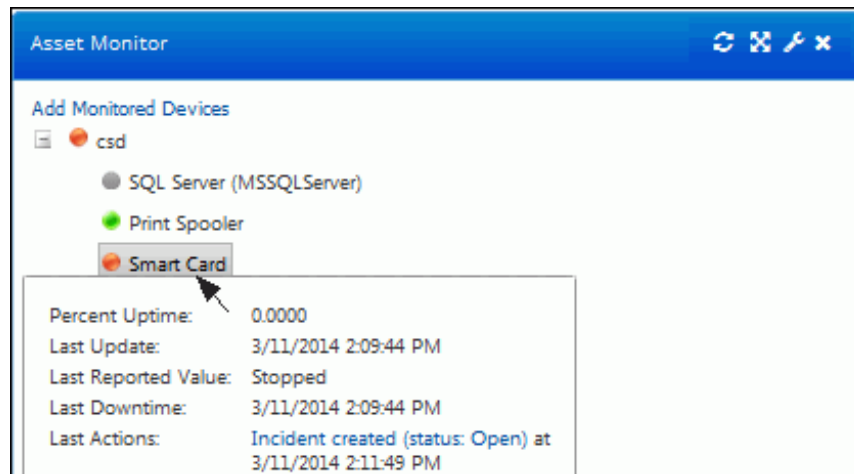
Configuration Process

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, click on Groups and then double-click on Administrators. Click Add. Add the name and click OK. In the Administrators Properties dialog, click Apply and then click OK.

2 Ensure that WMI is installed and active on the machines to be scanned.

3 Use the Scheduled Scan and Monitoring Definitions screen 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 47 for more information.

If you enabled the Auto Asset Create from Scheduled Scan Agent in the Scheduled Scan and Monitoring Definitions screen, it will run every hour based on the time at which the iSupport Agent Manager service is started.

4 Enable the Asset Scheduled Scan and Monitoring agent in the Core Settings | Feature Basics or Options and Tools | Administer | Agents screens. This agent checks scheduled scan and monitoring definitions, initiates scans according to schedule, and enables monitoring. The Scan button will appear in the Scheduled Scan and Monitoring Definitions screen after this agent is enabled. (Note that monitoring can still be configured and enabled if asset scanning is disabled.)

5 In the Scanning and Monitoring Log Maintenance screen:

- Use the Scheduled Scan Messages tab to view 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, 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 Network 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.

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

6 The Scheduled Scan and Monitoring Definitions screen enables you to configure automatic creation of asset records for machines that are involved in scheduled scans but not associated with an existing record. (The Assets tab in the Agents screen also enables you to configure this feature.) If you wish to do this, first create or find an

Asset record to be used as a template. The asset type in the template record will determine the fields that will appear on the automatically-created record. 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. See "Creating Asset Records Automatically Based on Scheduled Scans" on page 61 for more information.

7 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.

Creating a Scheduled Scan and Monitoring Definition

Use the Scheduled Scan and Monitoring Definition screen to specify the devices/machines to be scanned and monitored, specify the components to scan, and configure monitoring if desired.

Basics >	**Title** — Local Machines
IP Settings	**Scan Type** — IP Scan
Components	**Scan Enabled** — On / Off
Monitoring	**Start Time** — 12:00 AM
	Duration — 1 Hour(s)
	Frequency — Daily
	Occurs On
	Scan On Weekends — On / Off

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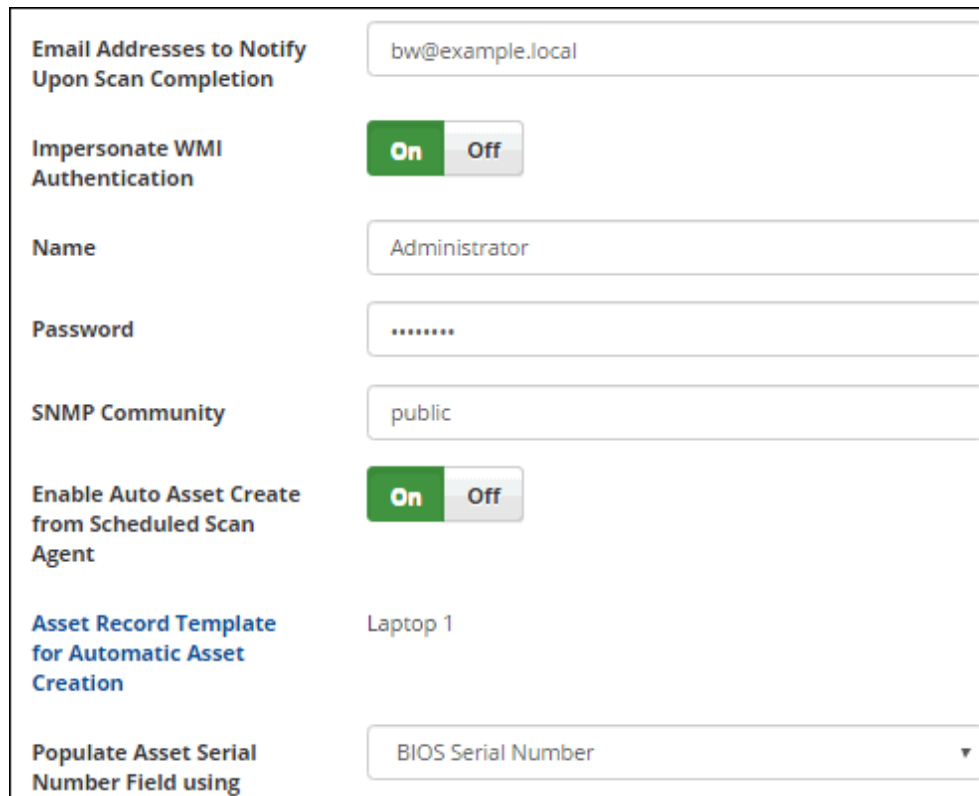
Occurs On - This field is enabled if Weekly or Monthly is selected in the Frequency field.

- 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, click on 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.

The second half of the screen is as follows:

Email Addresses to Notify Upon Scan Completion	bw@example.local
Impersonate WMI Authentication	On / Off
Name	Administrator
Password	········
SNMP Community	public
Enable Auto Asset Create from Scheduled Scan Agent	On / Off
Asset Record Template for Automatic Asset Creation	Laptop 1
Populate Asset Serial Number Field using	BIOS Serial Number ▼

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 this agent in the Agents screen.)

Asset Record Template for Automatic Asset Creation - Click 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 61 for a table listing how the fields are populated.

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 click the down arrow ⬇ icon to move the IP range into the list. To move a range out of the list, click on the entry and then click the up arrow ⬆ icon. To delete a range from the list, click on the entry and then click the Delete ✖ icon.

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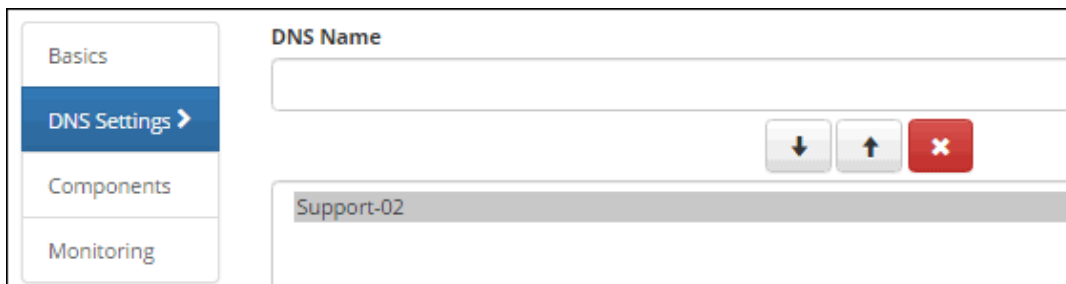
Scan All Machines - Select this field to scan all machine names known by the domain controller.

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 click the down arrow ➡ icon to move the IP range into the list. To move a range out of the list, click on the entry and then click the up arrow ⬆ icon. To delete a range from the list, click on the entry and then click the Delete ✖ icon.

Selecting Components to Scan

Select the types of data to include in the scan.

Check All   Uncheck All

Basics

DNS Settings

Components ›

Monitoring

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

Hardware Controllers

☑ IDE Controllers
☑ Video Controllers
☑ Floppy Controllers
☑ PCMCIA Controllers

System Hardware

☑ Processors
☑ BIOS
☑ Physical Memory
☑ System Slots

Drives

☑ Disk Drives
☑ Floppy Drives
☑ CD-ROM Drives

Configuring Monitoring

You can optionally use the Monitoring tab in the Scheduled Scan and Monitoring Definitions 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 56 for more information.

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

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.
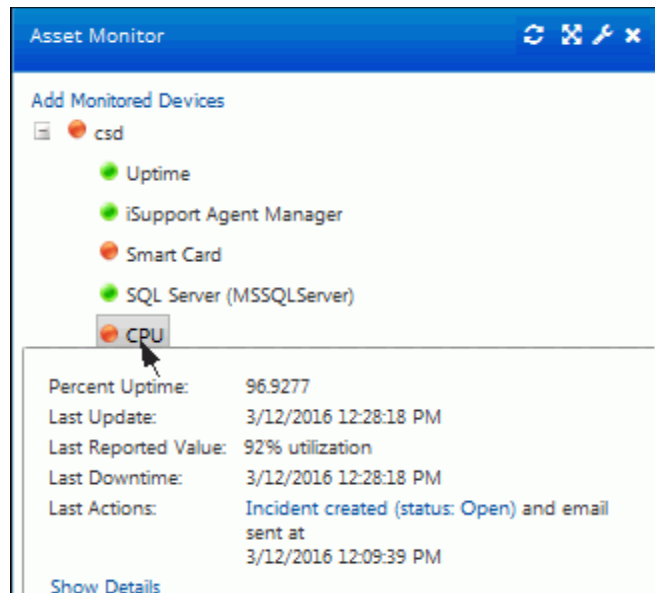

Maximum Utilization - Enter the percentage of CPU utilization at which reporting should start; if CPU utilization reaches this percentage, reporting will continue for the duration configured in the Detail Interval and Detail Max Intervals fields. Note that reporting will stop if the CPU utilization goes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

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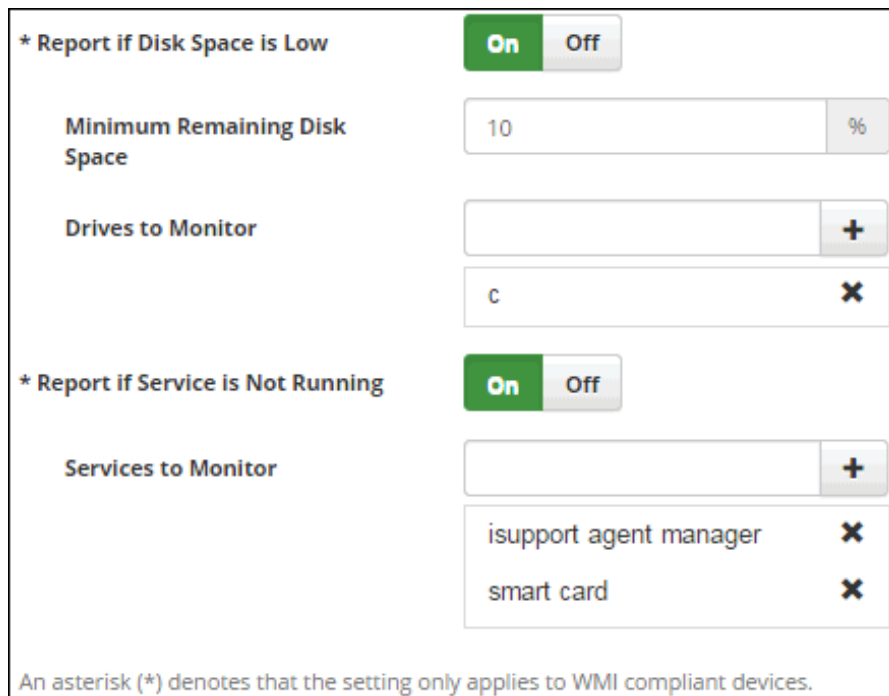
Report if Memory Utilization is High - Select Yes to include a Memory entry in the Asset Monitor component for the device and track and report the percentage of memory utilization. A red dot will display if the monitor detects that

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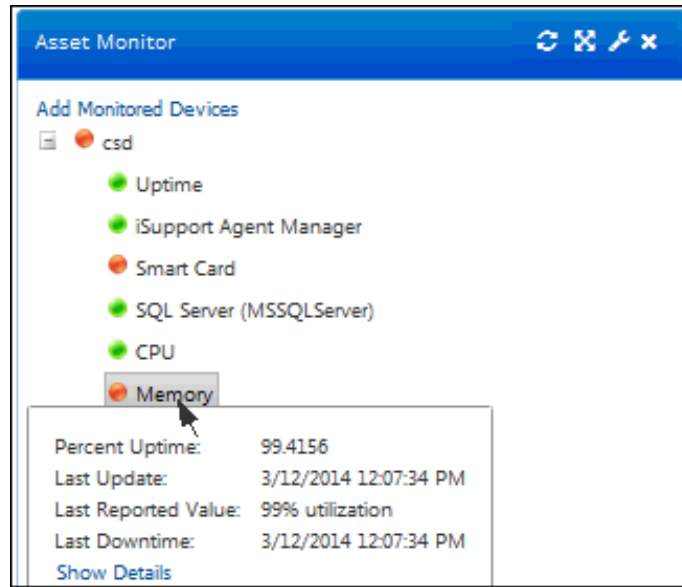
Maximum Utilization - Enter the percentage of memory utilization at which reporting should start; if memory utilization reaches this percentage, reporting will continue for the duration configured in the Detail Interval and Detail Max Intervals fields.

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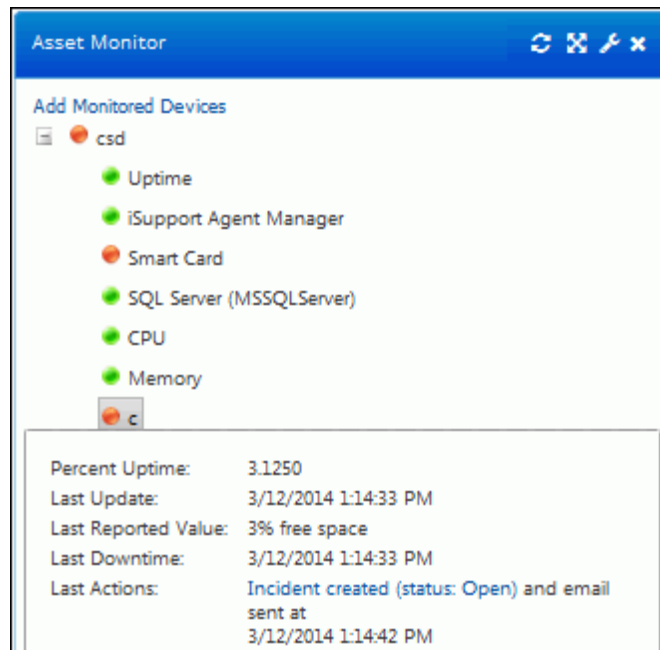
Minimum Remaining Disk Space - If Yes is entered in the Report if Disk Space is Low field, enter the percentage of disk space at which the specified drive(s) should be flagged for low disk space.

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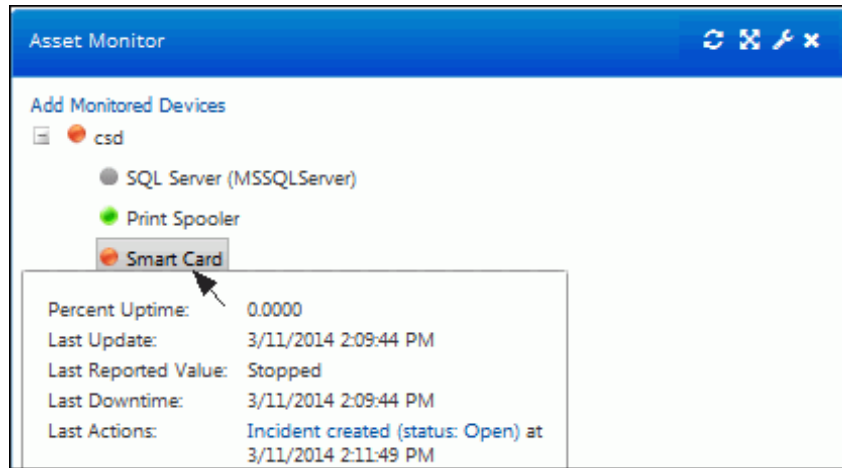
      Services to Monitor - Enter the display names of the services to monitor for a stopped state.

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.

Scheduling the Asset Scheduled Scan and Monitoring Agent

After entering a scheduled scan and monitoring definition, enable the Asset Scheduled Scan and Monitoring agent in the Asset Agents screen. This agent checks scheduled scan and monitoring definitions and initiates scans according to schedule. The Scan button will appear in the Scheduled Scan and Monitoring Definitions screen after this agent is enabled.

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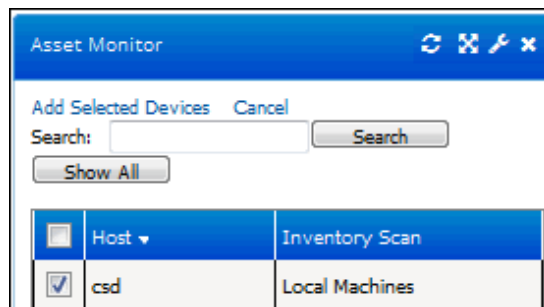
The state of monitored items and devices will be indicated by green, red, yellow, and gray dots; you can display details in a tooltip by hovering over the item or device name.

- 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.
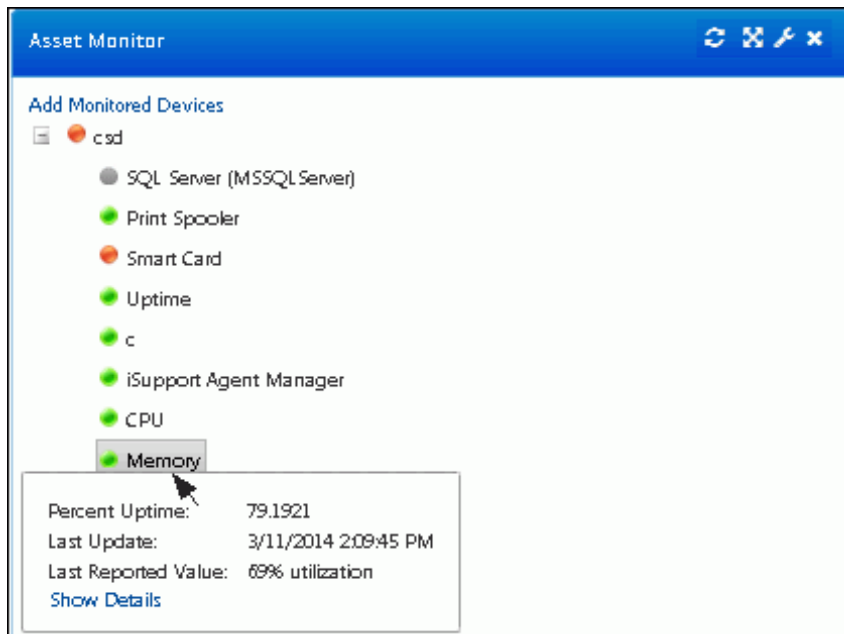
- A yellow dot will appear if, after everything has been working correctly as described above, the iSupport Asset Scheduled Scan and Monitoring agent or iSupport Agent Manager service has stopped or has been disabled.
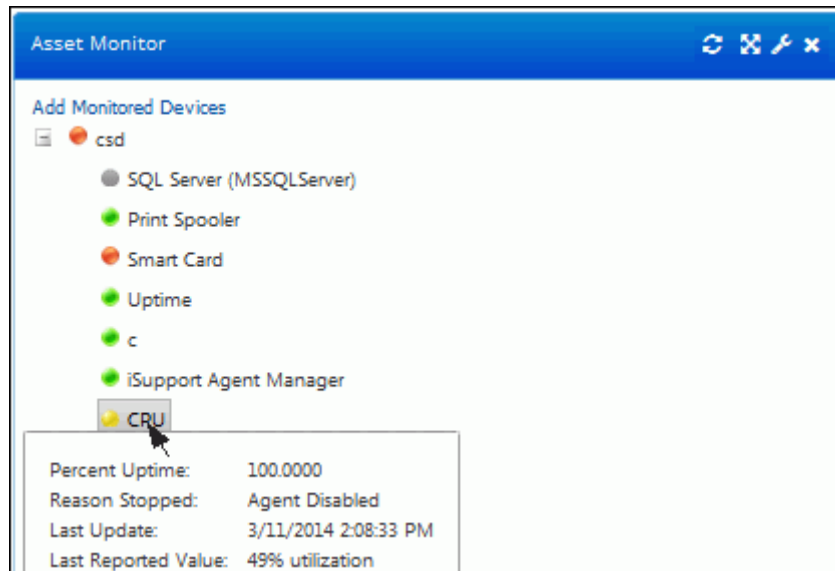
- A gray dot will appear for a monitored item or device on which the WMI listeners cannot be started (for example, if an error occurred with permissions).
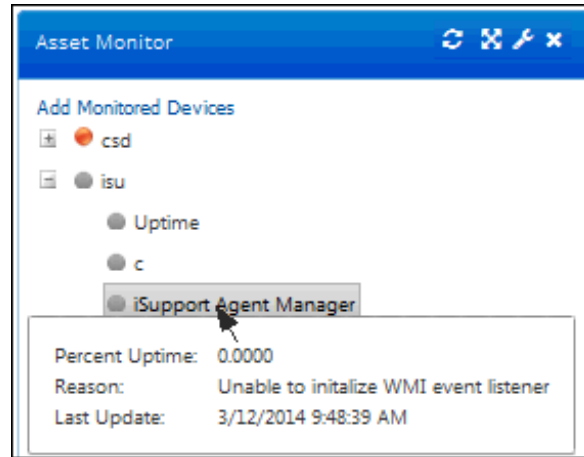
- A red dot will appear if, after everything has been working correctly, a problem occurs with the item or device being monitored such as a service stoppage or a configured threshold that is not met (if any of the configured reporting thresholds are met (a monitored device is off-line or has high memory or CPU utilization, a monitored drive has disk space lower than the specified percentage, or a monitored service has a stopped state). Click the Show Details link in the tooltip to display a chart of the occurrences at which a configured threshold was exceeded and other details.
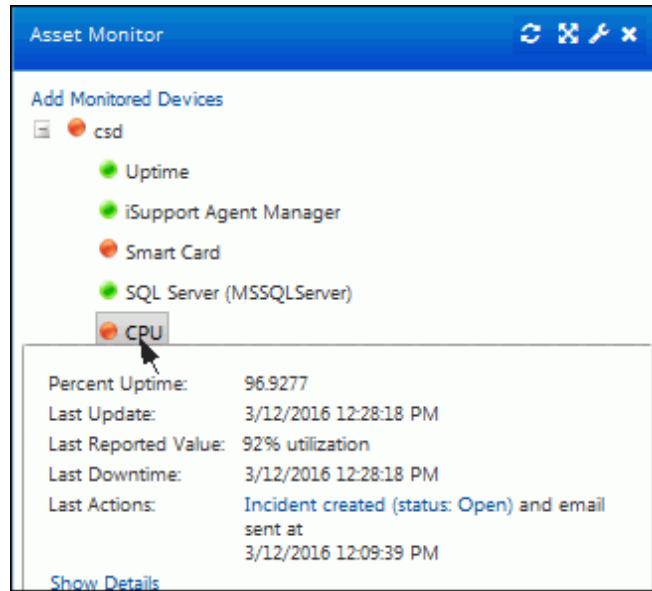
The Show Details link will appear in the tooltip if a configured threshold was exceeded; click it to display a chart of the occurrences at which a configured threshold was exceeded and other details:
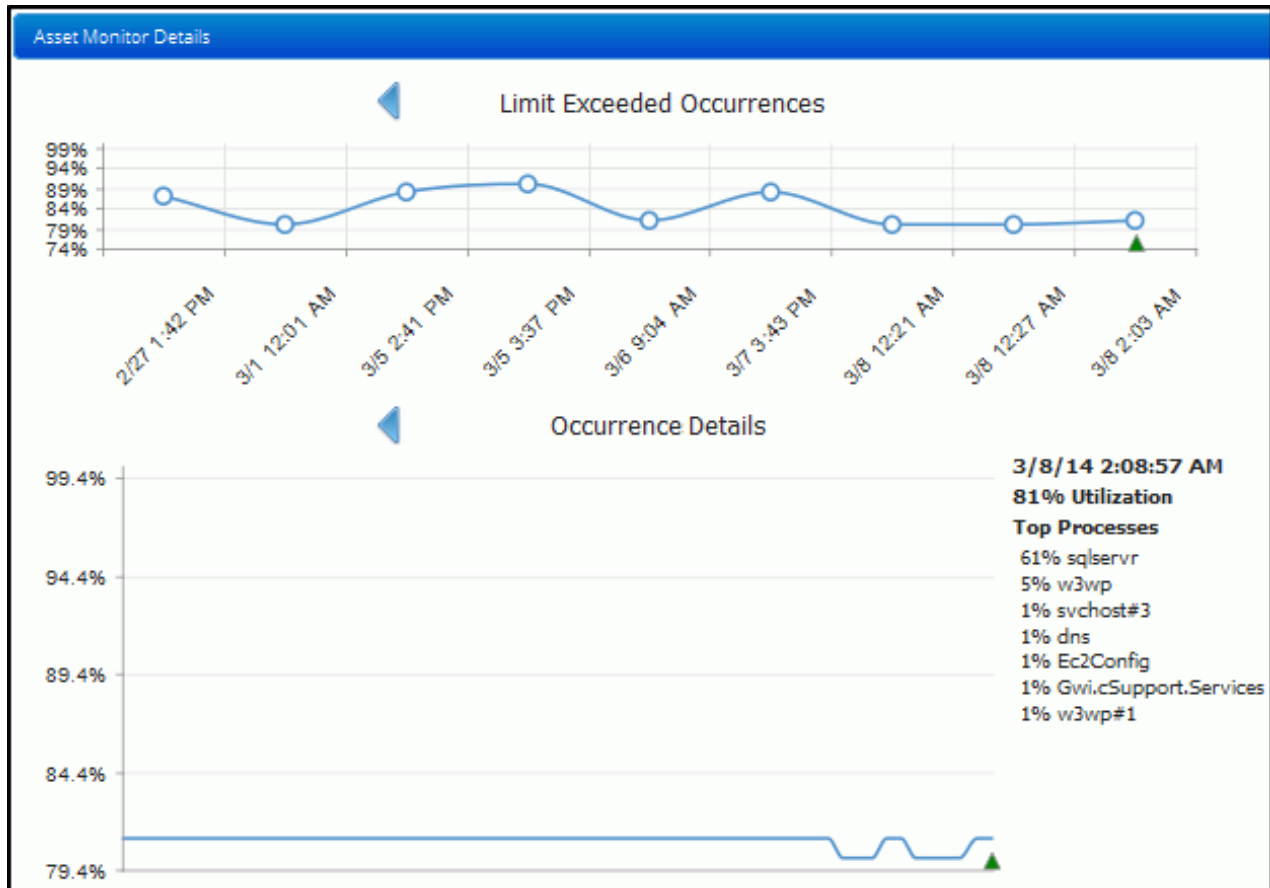
Displaying Scanning and Monitoring Log Messages

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.

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.

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.

To delete these scans, select the check box next to the scan and click 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 - Click 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.

Copyright