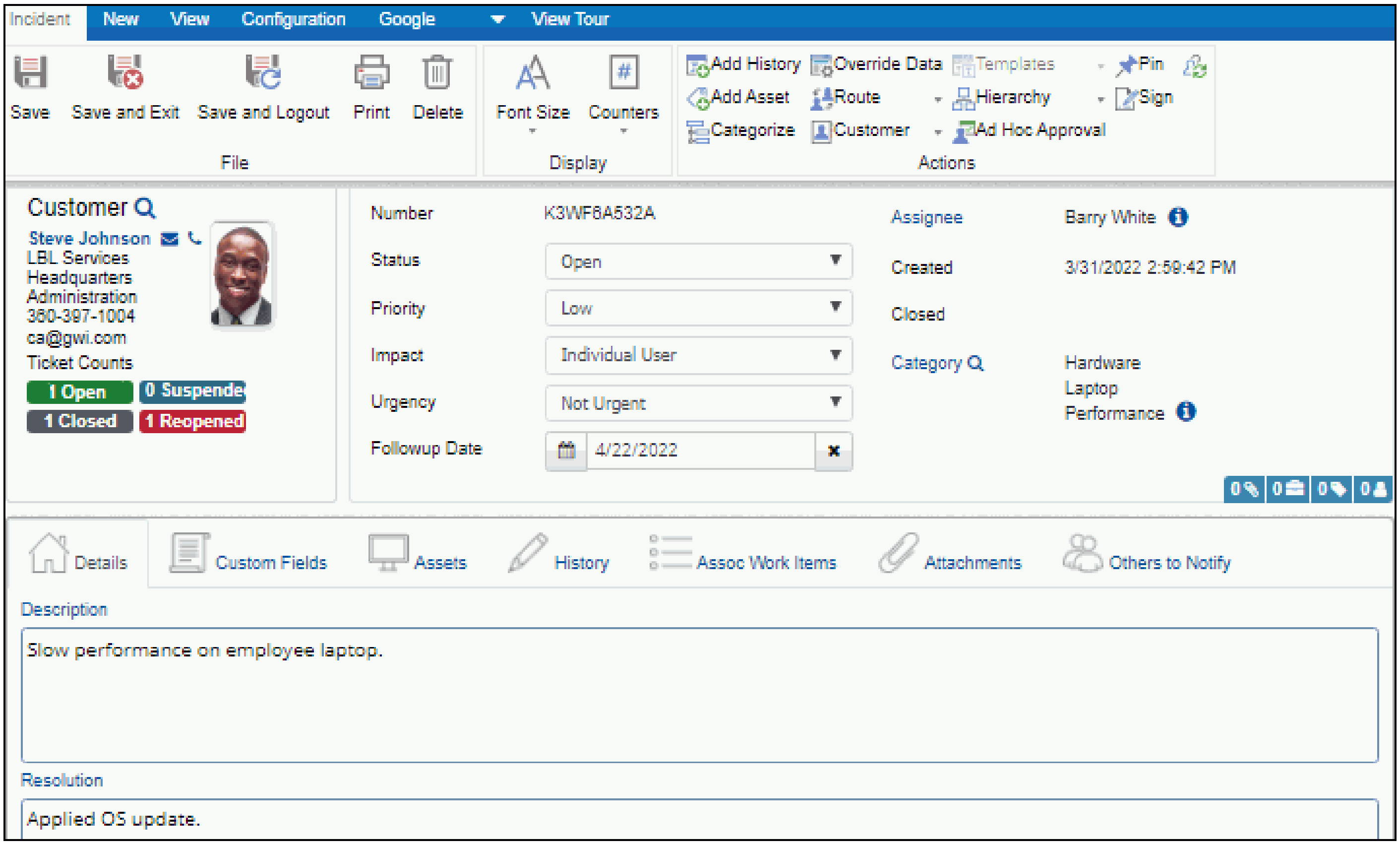
Configuring iSupport® Incident Functionality

Use iSupport's Incident Management functionality to track issues and accomplish quick restoration of service; iSupport includes numerous features for efficiently recording and resolving incidents. An example of the Incident screen is shown below.



Configuration Overview

Basic Configuration

- Set basic Incident options in Feature Basics. See "Setting Incident Basics Configuration Options" on page 4 for more information.
- Set up categories, which are custom values that you create for describing incidents, knowledge entries, problems, and changes. (Note that the same category set is used with all of those features.) A category combination is required in order to save an incident. Categories are involved in many features throughout iSupport, including reporting, knowledge searching, displaying related work items, scripts, and more. See the online help for more information.

Creating Incident Records

- You can manually create Incident records via the Incident screen. See the online help for more information.
- Customers can submit an email that will create an incident via email processing. See the online help for more information.
- Customers can submit incidents via a mySupport portal. See the online help for more information.

- If the automatic incident creation feature is enabled for chat, you can accept a mySupport customer chat request. See the online help for more information.
- You can use the Create Incident link in the Twitter Monitor and Facebook Monitor components on the Desktop. See "Facebook Applications" on page 110.
- You can schedule a single occurrence change or a recurring set of incidents to be created at a future date/time. See the online help for more information.

Customizing iSupport Defaults

- Support includes a default Incident screen layout with a comprehensive set of fields for tracking Change data, but you can redesign it to include fields and tabs that are specific to your company. You can create different layouts to assign to support representative groups, customer groups, categories, incident templates, and hierarchy templates. See "Configuring Screen Layouts" on page 34.
- You can create custom status labels for the Incident status levels of Open, Closed, Suspended, Scheduled, and Reopened. See "Defining Custom Status Labels" on page 29.
- If there are fields you need that are not included in iSupport by default, you can create custom fields. See "Configuring Custom Fields" on page 19.
- You can include a field for entering or automatically generating a custom number. See "Defining Custom Status Labels" on page 29.
- You can define custom impact and urgency values that map to priority levels. Enable impact/urgency mapping via the Feature Basics screen. See "Defining and Mapping Impact and Urgency Values" on page 31.
- You can enable your customers to submit and view Incident records on mySupport portals, and you can customize the submission and display screen layouts. See the online help for more information.
- Define Work History types to create custom entries for support representatives to select to describe the work performed on a work item. See "Configuring Work History Options" on page 6.

Sending Notifications

- You can use Incident rules to send Desktop and email notifications when specified conditions based on Incident record fields or events are met; for example, you can configure a rule to send a notification when the priority of an Incident record is modified. See "Configuring Rules and Rule Groups for Incidents" on page 46. You can use or copy and modify iSupport's default notifications, or you can create new custom notifications. See "Customizing and Viewing Event Notification Content" on page 62. You can include data from Incident records and designate any applicable recipients. See the online help for more information.
- You can send correspondence email from the Incident screen. Correspondence can include data from Incident records; correspondence templates can be utilized, and an Others to Notify list can be used for keeping those not directly involved in the loop. See the online help for more information.
- You can create a headline or add a discussion post to a selected feed from the Incident screen. See the online help for more information.

Interacting With Customers

- You can send a survey request to be completed by customers using mySupport. See the online help for more information.
- You can enable a single selection feedback survey with a question with two response choice image links in an incident notification. See "Creating Feedback Questions" on page 9 for more information.
- You can enable integration With BeyondTrust (a third-party application) for remote desktop connection and chatting; contact iSupport Technical Support for more information.
- You can enable Citrix GoToAssist remote support access (a third-party application). See the online help for more information.

- You can configure integration with Google Calendar, Google Meet, Microsoft Outlook, Zoom, and Microsoft 365 Teams to display an option in the Incident screen for initiating a meeting. See "Configuring Calendar and Meeting Integrations" on page 102 for more information.

Using Workflow Features

- You can route via name, skill, group, and location, all with or without load balancing, in the Incident screen. Enable routing methods via Feature Basics. See "Enabling Routing Methods" on page 10 for more information.
- You can use Incident rules to automatically route Incident records via round robin or load balancing. See "Configuring Rules and Rule Groups for Incidents" on page 46.
- You can automatically change field values on Incident records via Incident rules. See "Configuring Rules and Rule Groups for Incidents" on page 46.
- You can create templates to populate fields for common and reoccurring changes; see "Configuring Auto-Close and Auto-Fill Incident Templates" on page 67. You can also create hierarchy templates for tasks that have multiple activities; see "Configuring Incident Hierarchy Templates" on page 74. Both types of templates can be applied manually via the Incident screen or via Incident rules.
- You can require an Incident record to be approved before most functions can be performed. Approval cycles are initiated via Incident rules. See "Configuring Approval Cycles" on page 93.
- You can enable followup date and an acknowledgment features via Feature Basics. See "Setting Incident Basics Configuration Options" on page 4 for more information.
- You can create related incidents for an Incident record; when you close the original incident, all related incidents can be closed automatically. See the online help for more information.
- You can associate new and existing Asset records. See the online help for more information.
- If you have the Service Desk Edition, you can associate new and existing Problem, Change, and Purchase records. You can enable associated incidents to be closed when a Problem or Change record is closed. See the online help for more information.
- You can enable a prompt in the Incident screen to automatically create a knowledge entry from a closed an incident; enable this feature via Feature Basics. See "Setting Incident Basics Configuration Options" on page 4 for more information.
- You can perform ad hoc scans on non-Windows SNMP-enabled devices in the Incident screen, and associate scans with an incident. See the online help for more information.
- You can configure webhooks to post Incident data to a web application via Incident rules. See "Configuring Webhooks" on page 116.
- You can configure signing agreement text for inclusion in the Sign dialog in the Incident screen. Signing agreements can be associated with customer and support representative groups, categories, and incident and change templates. Note that this feature is not available in mySupport. See "Configuring Signing Agreements" on page 100.

Managing Incident Records

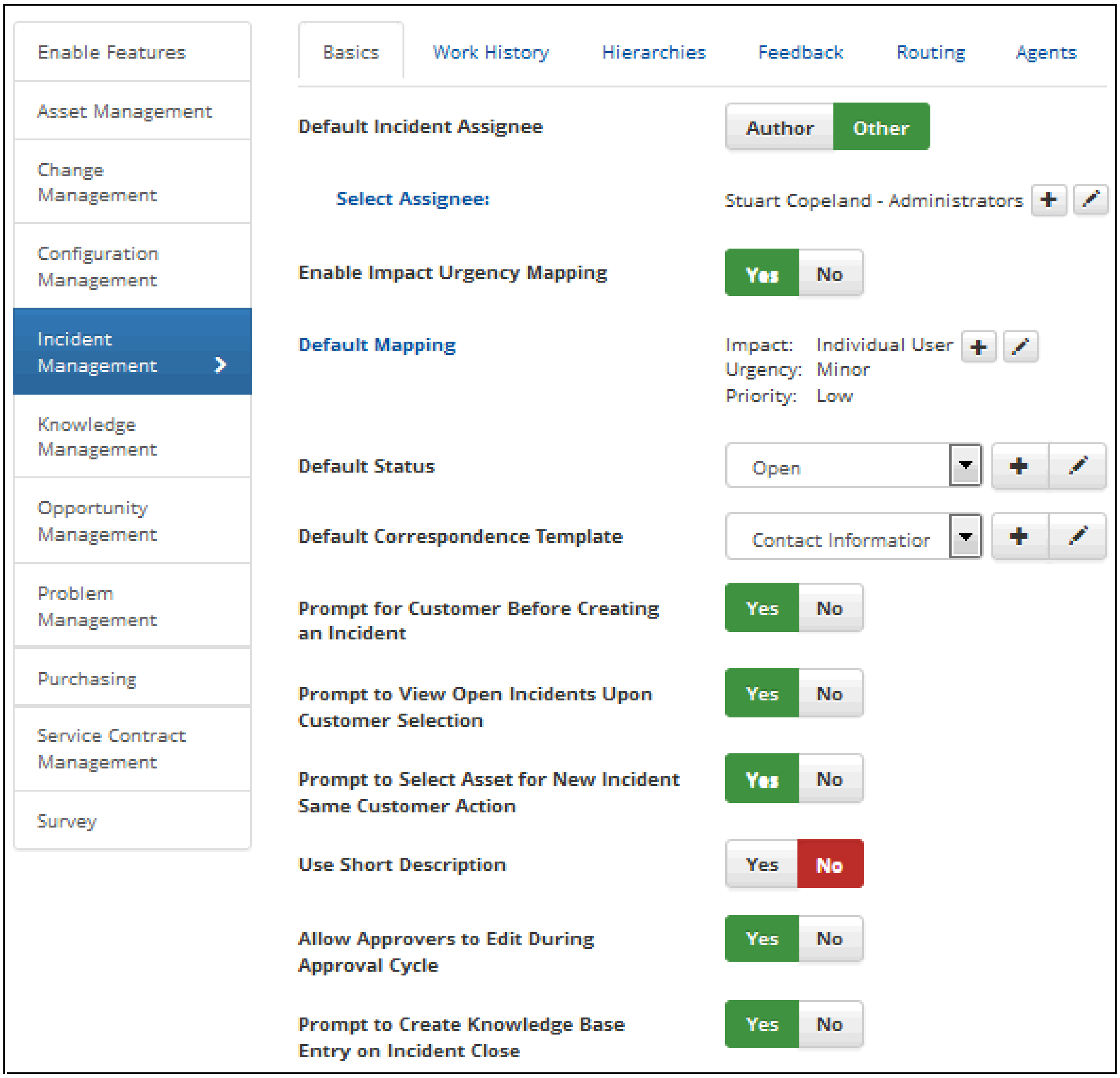
- You can use the Action menu in the View component on the Desktop to perform actions such as opening multiple items. See the online help for more information.
- You can use Service Contract functionality to track and restrict changes associated with customers, companies, and assets. See "Setting Service Contract Feature Basics Options" on page 16.
- You can archive incidents for database efficiency. See the online help for more information.
- You can configure roles/permissions for support reps and rep groups using Incident functionality via the Support Representatives screen. See the online help for more information.
- If you need to overwrite fields on a saved incident, see "Using the Data Override Feature for Incidents, Problems, and Changes" on page 101.

Setting Incident Basics Configuration Options

Use the Incident Basics screen to set options for work history (see page 6), hierarchies (see page 9), feedback (see page 9), routing (see page 10), and agents (see page 15).

Completing the Basics Tab

Use the fields on the Basics tab to set miscellaneous configuration options.



Default Incident Assignee - Select Author to assign newly-created incidents to the person who created the incident; select Other to designate a support representative to be assigned newly-created incidents. Use the + Create New and View/Edit options to access the Support Representative Profile screen.

Enable Impact Urgency Mapping - Select Yes to enable prioritization to encompass urgency (based on the amount of time a resolution is needed) and impact (usually the number of users affected). Use the Impact and Urgency screen to define impact and urgency values that map to priority levels; Use the + Create New and View/Edit options to access the Impact and Urgency Mapping screen.

In the Incident, Problem, and Change screens, the defined values will be available in the Impact and Urgency fields for selection. The specified mapped priority will appear as default but all priority levels will available if permissions are configured for the support representative to change the priority.

Default Mapping - Click this link to select the Impact, Urgency, and Priority to display by default in the Impact, Urgency, and Priority fields in the Incident screen.

Default Priority - This field appears if No is selected in the Enable Impact and Urgency Mapping field. Select the priority (Low, Medium, High, or Emergency) to assign to newly-created incidents.

Default Status - Select the status to assign to newly-created incidents. All open incident statuses will be available for selection. Use the Create New and View/Edit options to access the Custom Status Labels screen.

Default Correspondence Template - Select the correspondence template that will apply by default when a support representative initiates a correspondence via the Incident entry screen. Correspondence templates that are active and enabled for the Incident module will be available for this feature. Use the Create New and View/Edit options to access the Correspondence Template screen.

Prompt for Customer Before Creating an Incident - Select Yes to display a customer selection dialog when an incident is initially created.

Prompt to View Open Incidents Upon Customer Selection - Select Yes to display the following prompt if open incidents exist for a customer selected in the Incident screen: "Open incidents were found for this customer. Would you like to view them now?"

Prompt to Select Asset for New Incident Same Customer Action - Select Yes to, when New | Incident is selected in the Incident screen, display the assets associated with the company and customer for selection. (The Show All option will be included as well.)

Use Short Description - Select Yes to include a Short Description field in the Incident screen.

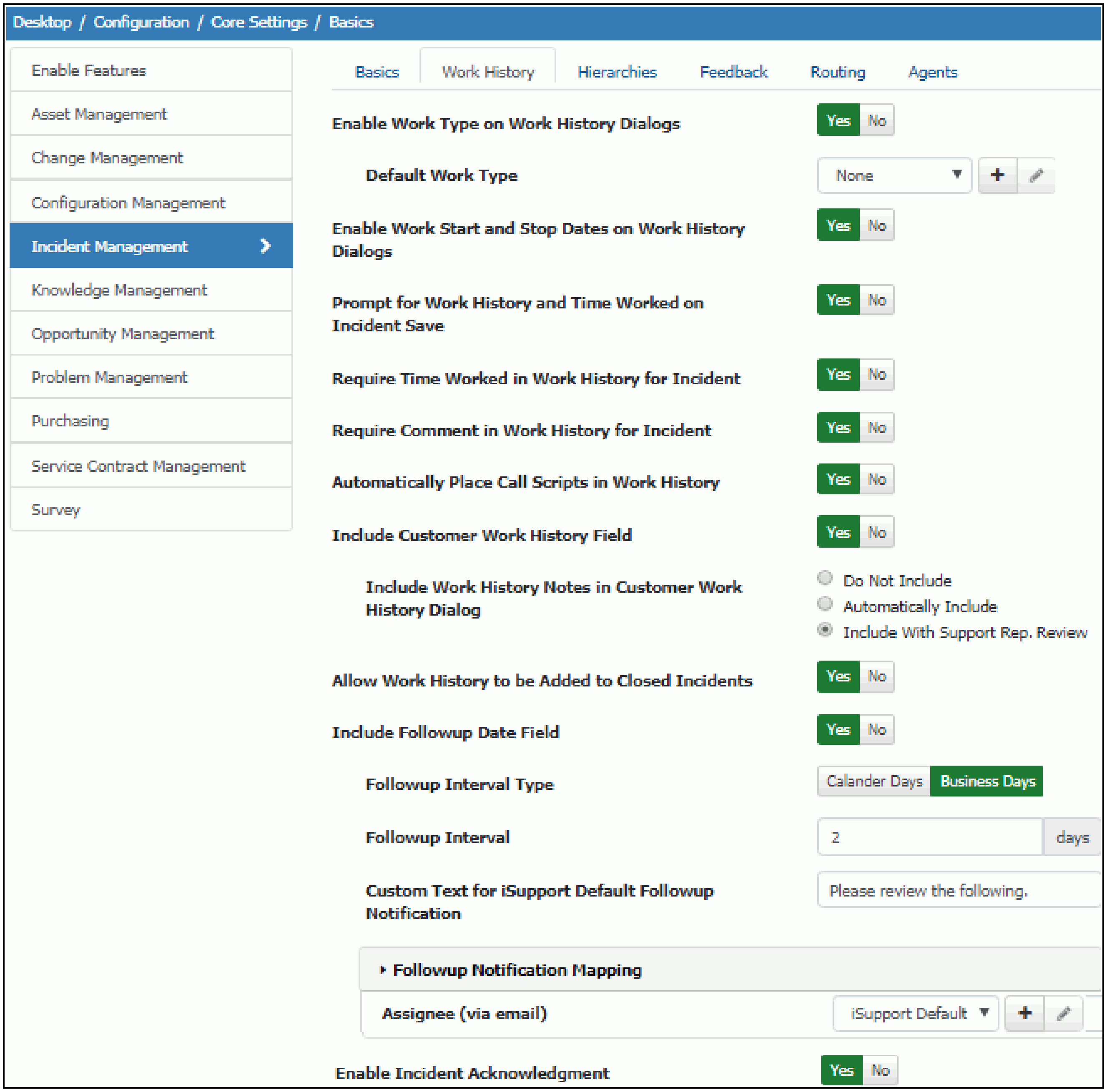
Required on Save - Select Yes to require an entry in the Short Description field before a record can be saved.

Allow Approvers to Edit During Approval Cycle - Select Yes to enable support representatives designated as approvers (or those with Approval Override) to have access to all functionality except Status in records in an approval cycle. You can configure the Pending Incident Updated notification (or any other notification) to be sent when the Edited During Approvals event occurs.

Prompt to Create Knowledge Base Entry On Incident Close - Select Yes to enable a prompt for creating a knowledge entry to display every time an incident is closed.

Configuring Work History Options

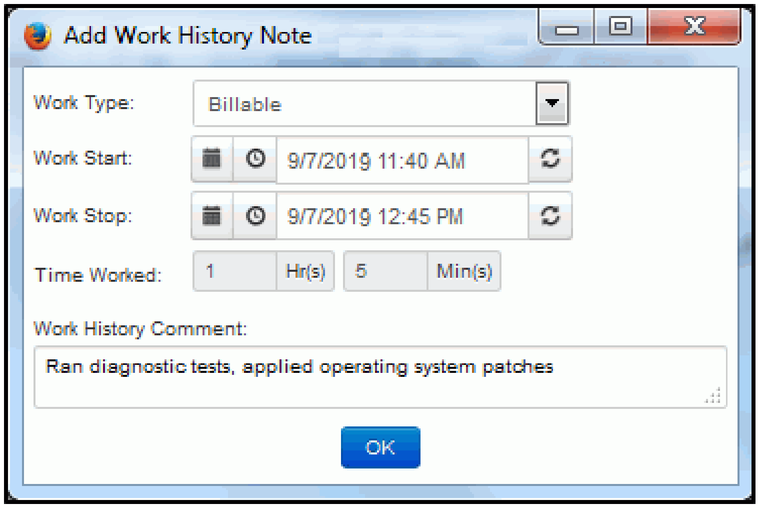
Use the Work History tab to set options for the Work History and Save dialogs in the Change screen.



Enable Work Type on Work History Dialogs - Select Yes to include a Work Type field in the Work History dialog in the Incident screen.

Default Work Type - If the Work Type field is enabled, select the work type to appear by default in that field. Use the + Create New and View/Edit options to access the Work Types entry screen; see "Configuring Work History Types" on page 33.

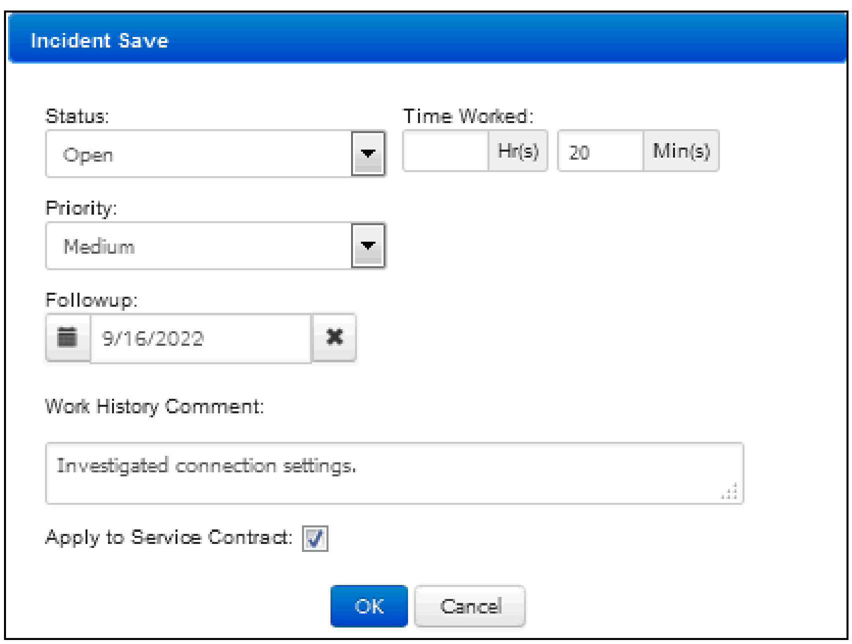
Enable Work Start and Stop Dates on Work History Dialogs - Select Yes to include Work Start and Work Stop fields in the Work History and Incident Save dialogs in the Incident screen.



The Work Start field defaults to the date and time the support representative loaded the work item. The Work Stop field defaults to the current time, but there will be at least a one minute gap between the Start and Stop times. For example, if a new incident is opened at 1:00 PM, the support representative works with the customer for 30 minutes, and then clicks the Add Work history option or saves and displays the Save dialog, the Work Start would be set to 1:00 PM and the Work Stop would be set to 1:30 PM. This Time Worked field would show the 30 minutes of time worked reflected by the gap.

Support representatives can type directly in the Work Start and Work Stop fields or use the calendar and clock options to select the date and time; the difference will populate automatically. The refresh option will set the date and time to the current date and time (but the Work Stop date and time will adjust to be at least one minute past the Work Start date and time).

Prompt for Work History and Time Worked on Incident Save - Select Yes to display the Save dialog every time a support representative saves an incident.



Require Time Worked in Work History for Incident - Select Yes to require an entry in the Time Worked field in the Incident Save dialog before the record can be saved in the Incident screen.

Require Comment in Work History for Incident - Select Yes to require an entry in the Work History Comment field in the Incident Save dialog before the record can be saved in the Incident screen.

Automatically Place Call Scripts in Work History - Select Yes to, when a call script is used, automatically include the entire call script in the Work History field. This will also make the call script editable when it appears. Call scripts are entered and associated with categories in the Category entry screen. If you select No in this field, the call script will not be editable.

Include Customer Work History Field - Select Yes to include a field on the Incident screen that includes work history notes for display when customers view their incidents on the mySupport portal. Depending on the options selected in the Include Work History Notes in Customer Work History Dialog field, the field can include the contents of the Work History field (either with or without review by the support representative).

Include Work History Notes in Customer Work History Dialog - This field appears if including the Customer Work History field. Select:

- Do Not Include to prevent Work History field entries from automatically populating the Customer Work History dialog in the Incident screen.
- Automatically Include to fill the Customer Work History field with the contents of the Work History field, without review by a support representative. (The Customer Work History dialog will not appear in the Incident screen.)
- Include With Support Rep. Review to fill the Customer Work History field with the contents of the Work History field and enable the support representative to edit it before including it in the Customer Work History field.

Allow Work History to be Added to Closed Incidents - Select Yes to enable support representatives to update the Work History field in incidents with a Closed status.

Include Followup Date Field - Select Yes to include a Followup Date field in the Incident screen for a followup reminder email to be sent to the assignee of an incident. After completing this and the followup date configuration fields, enable the Followup agent on the Agents tab.

Followup Interval Type - If including a followup date on the Incident screen, select the basis for the default followup date interval: calendar days (which include weekends) or business days (which excludes weekends).

Followup Interval - If including a followup date on the Incident screen, enter the number of days (after the incident open date) to be used in the calculation of the date to display by default in the Followup field. When the followup date is reached, a followup reminder email will be sent to the assignee of the incident. Once the email is sent, the date is recalculated based on the number of days entered in this field.

Custom Text for iSupport Default Followup Notification - If including a followup date on the Details tab in the Incident screen, a reminder email will be sent to the support representative on the followup day. Enter text to be included as the first line in the body of the default email text. (Note that this text will not be included in any custom notifications.) The email will also contain a document link and the caller’s name and company; this information will still be included if this field is left blank. If the iSupport Default notification is used, a newsletter-style email will be sent; if a custom notification is used, a notification will be sent for each incident.

Followup Notification Mapping - Select the notification to be sent to the assignee of the incident with a current followup date. 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.

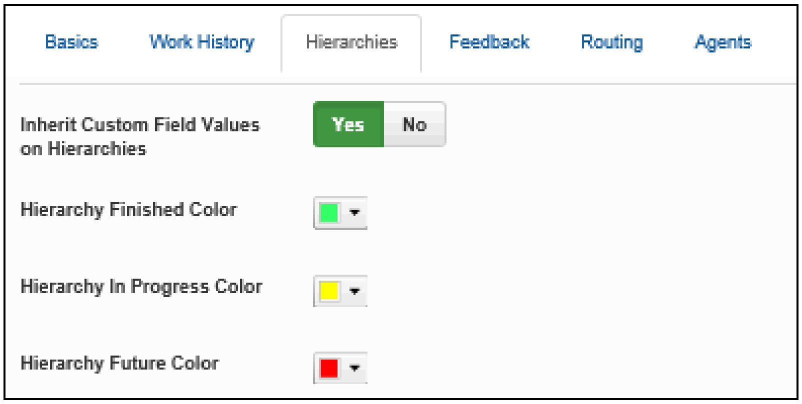
Enable Incident Acknowledgment - Select Yes to display an alert bar for new assignees to acknowledge incidents that have been:

- Created or saved from the mySupport portal or email.
- Routed manually or automatically via a rule.
- Created via direct entry with an assignee different from the current support representative.
- Created via direct entry with either an incident or hierarchy template.

When the assignee opens the incident, an alert bar will appear at the top of the screen that states: "This incident was routed to you. Click to acknowledge that you have received this ticket." When the support representative clicks the Acknowledge button, an entry will be recorded in the Audit History. You can use the Incident Rules screen to enable a notification to be sent when an incident is acknowledged.

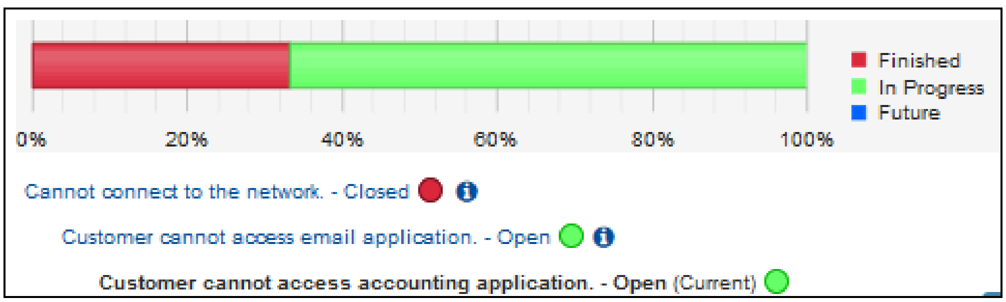
Configuring Options for Incident Hierarchies

Use the Hierarchies tab to set options for incidents created by hierarchy templates.



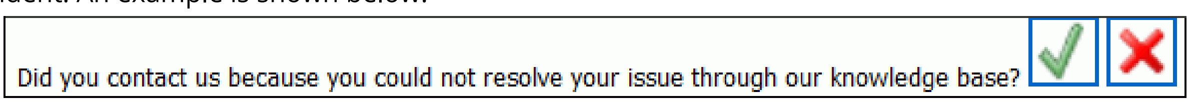
Inherit Custom Field Values on Hierarchies - Select Yes to, when custom fields are associated with a category or incident, pass the values in those fields to incidents created by hierarchy templates. See "Configuring Custom Fields" on page 19 for information on configuring custom fields; see "Configuring Incident Hierarchy Templates" on page 74 for information on configuring incident hierarchy templates.

Hierarchy Finished/In Progress/Future Color - Select the colors for the dot icons and portions of the graphic in the Related Hierarchy field that represent the percentage of work that has been completed, is in progress, and is pending due to dependencies.



Creating Feedback Questions

The Incident Feedback feature enables you to create one or more questions, each with two response choice image links, for inclusion at the bottom of an incident notification, based on a configured rule. When a customer receives the email and clicks one of the responses, the feedback question and response will be included in the Feedback field on the incident. An example is shown below.

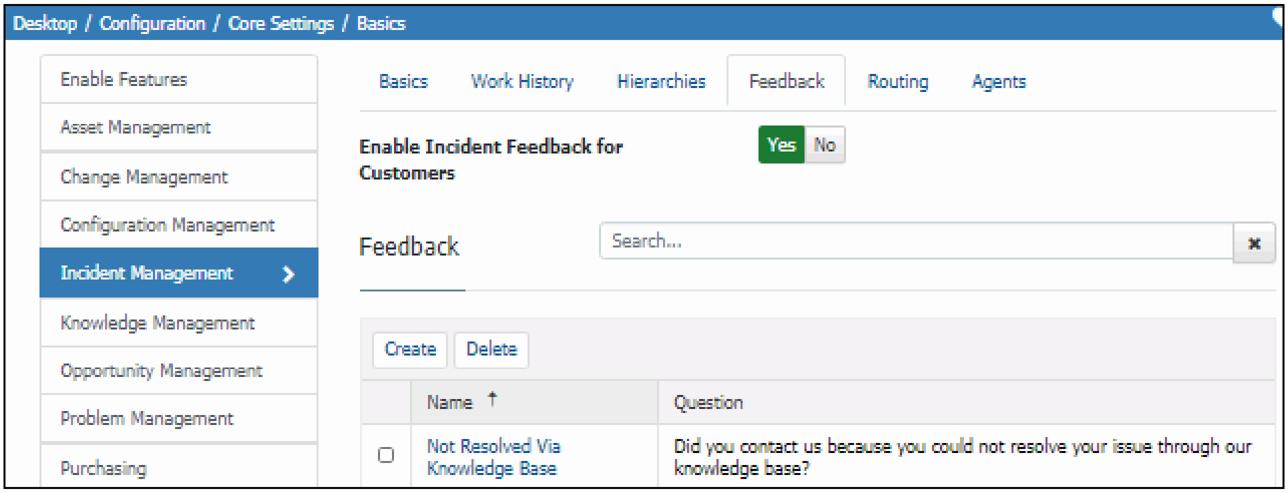


Configured Feedback Submitted text will appear to the user on a page on the mySupport portal; if more than one mySupport portal is configured, the default mySupport portal URL will be used.

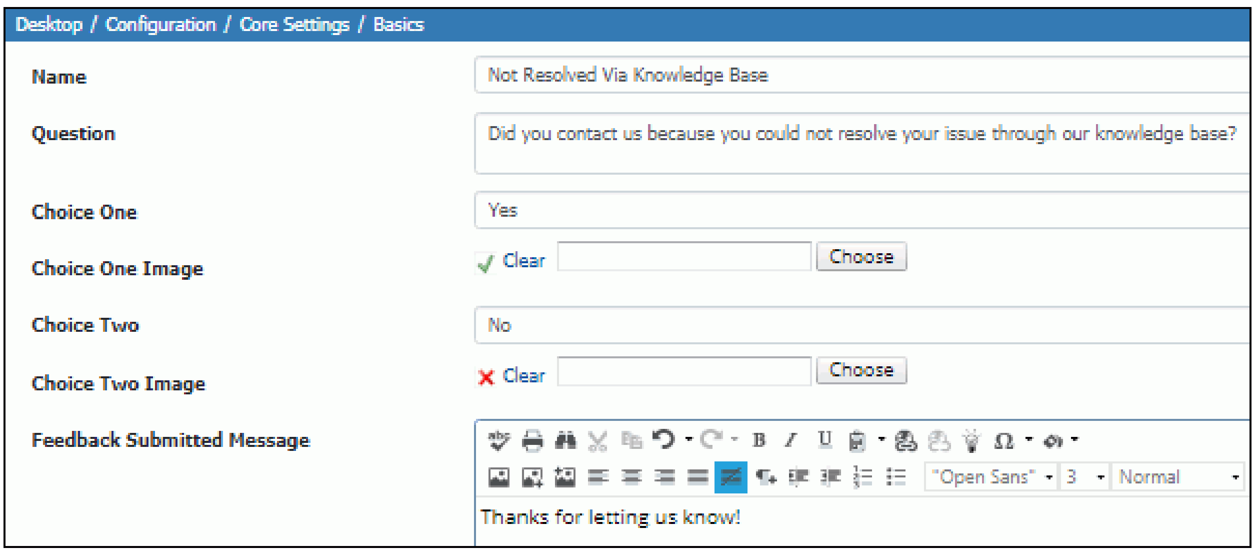
Note that only one feedback response can be set per work item; if more than one feedback request is sent related to a single work item, only the last feedback entered will display in the feedback question and response fields. Audit history will reflect all provided feedback questions and responses.

In the rule that will send the notification including the feedback question, enable inclusion of the feedback and select the question and notification. Note that this feature is intended for HTML-type mail delivery. Feedback audit history is included in the Configuration Audit Tracking screen.

Enable Incident Feedback for Customers - Select Yes to enable the Incident Feedback feature. Use the Create button to create an incident feedback question.



Enter the name, text of the question, response choices and images, and message to appear after a selection is entered.



Name - Enter the name to assign to the question.

Question - Enter the question text to be included in an incident notification (configured via the Rule screen).

Choice One/Image - Enter the text for the first response choice and select the image to appear after the question text in the notification.

Choice Two/Image - Enter the text for the second response choice and select the image to appear after the first feedback choice image in the notification.

Note that the images will only be used in the outbound notification. The feedback choice text will appear as hover text for the image in the notification and if selected will be used as the response in the Feedback field on the incident.

Feedback Submitted Message - Enter the text to appear on a mySupport portal page when the user clicks on a feedback choice image on an incident notification.

Enabling Routing Methods

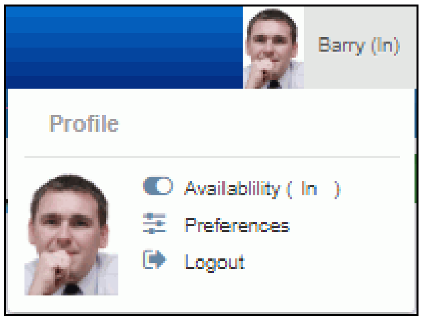
You can enable routing by name, skill, group, and location, all with or without load balancing. To set up routing:

- On the Routing tab, select the routing methods and enter skill levels and routing weights.

- If using location-based routing, set up locations in the Core Settings | Support Representatives | Locations screen.
- If using skill-based routing, set up categories in the Options and Tools | Customize | Categories screen and designate skills for support representatives in the Category screen or Support Representatives | Skills screen.
- If applicable, set up notifications in the Options and Tools | Automate | Rules screen.
- Set routing availability options for support representatives via the Core Settings | Support Representatives screen.

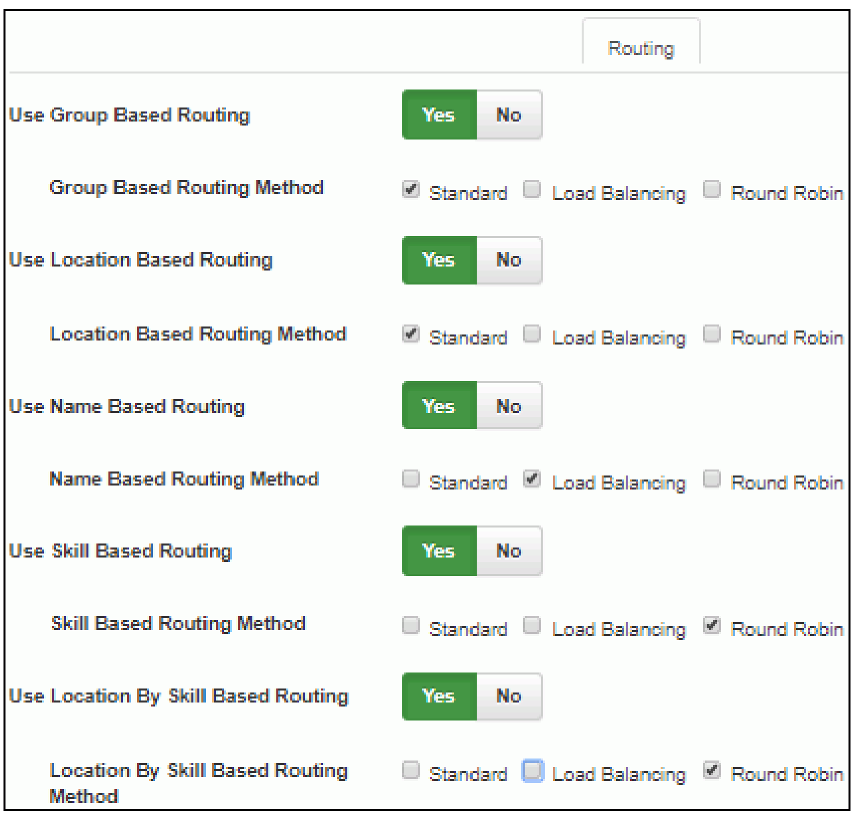
Note that routing availability can be controlled via:

- Scheduling and other options on the Routing Availability tab in the Support Representative Profile screen.
- If enabled, the Availability (In/Out) option on the Profile menu that appears after clicking a support representative's avatar/name on the Desktop.



- The Rep Manager Desktop component.

Use the Routing tab in the Basics screen to specify the type of routing to be used, the skill level labels, and load-balanced routing weights. If you enable more than one routing method, the support representative can choose the method when the work item route is initiated.



All routing methods can also include load balancing, which involves weights based on incident priority.

- For group, location, or name based routing with load balancing, the available support representative for the method with the lightest overall workload will be selected. (For example, if using group-based routing, the available support representative within the selected group with the lightest overall workload will be selected.)
- For skill-based routing with load balancing, after the categorization level is selected, a support representative is selected based on the workload of the support representatives who have the exact match of the selected categorization in their Support Representative record.

  If a support representative has worked with an incident and the incident is reassigned, he/she will be bypassed until all available support representatives with the skill or in the group or location (depending on the method selected) have worked with the incident. If all support representatives have the same weight for their incidents, a random choice is selected for the assignee.

Note that rules can route incidents via load-balancing or the round robin method.

Use Group Based Routing - Select Yes to enable incidents to be routed to available support representatives that are set up in groups. In the Incident screen the support representative will select a group and then an assignee from a list of all available support representatives in that group. Use the Group screen to set up groups and the Support Representative screen to assign support representatives to groups. A support representative can be a member of more than one group.

Group Based Routing Method - This field appears if using group based routing. Select:

- Standard - enables the support representative to select a group and then an assignee from a list of all available support representatives in that group. Groups are designated for support representatives in their Support Representative record.
- Load Balancing - allows the system to select a support representative based on current open incident statistics, including weights based on incident priority. The available support representative within the selected group with the lightest overall workload will be selected.
- Round Robin - the support representative in the group who was assigned an incident on the oldest date and time is selected.

Use Location Based Routing - Select Yes to enable location based routing, which enables the support representative to select a location and then an assignee from a list of all available support representatives in that location. Locations are specified for support representatives in their Support Representative record or in the Location configuration screen. You can associate support representative locations with customer groups for location-based routing of tickets submitted via the mySupport portal and email.

Location Based Routing Method - This field appears if using location based routing. Select:

- Standard - allows the support representative to select from a list of all available support representatives listed by the location entered in support representative profiles.
- Load Balancing - routes incidents based on current open incident statistics, including weights based on incident priority. The available support representative within the selected location with the lightest overall workload will be selected.
- Round Robin - the support representative in a selected location who was assigned an incident on the oldest date and time is selected.

Use Name Based Routing - Select Yes to enable name based routing, which enables the support representative to select an assignee from a list of all available support representatives regardless of group.

Name Based Routing Method - This field appears if using name based routing. Select:

- Standard - allows the support representative to select from a list of all available support representatives.
- Load Balancing - routes incidents based on current open incident statistics, including weights based on incident priority. The available support representative with the lightest overall workload will be selected.
- Round Robin - the support representative who was assigned an incident on the oldest date and time is selected.

Use Skill Based Routing - Select Yes to enable skill based routing, which uses the incident categorization to select qualified support representatives. After a support representative classifies the incident and selects skill-based routing, the category levels selected for the incident will appear; the support representative will select the level of categorization that exactly matches the categorization for which support representative skills should be searched. The support representative(s) that have those skills configured in their profile will appear for selection.

Skill levels are associated with category combinations in the Support Representative screen.

Skill Based Routing Method - This field appears if using skill based routing. Select:

- Standard - allows the support representative to select the level of categorization that exactly matches the categorization for which support representative skills should be searched. Support representatives with that categorization in their Support Representative record would be displayed for assignment.
- Load Balancing - selects assignees based on the incident categorization and current open incident statistics, which include weights based on incident priority. The support representative selects the level of categorization for which support representative skills should be searched, and a support representative is selected based on the workload of the support representatives who have the exact match of the selected categorization in their Support Representative record.
- Round Robin - allows the support representative to select the level of categorization for which support representative skills should be searched; support representatives who have the exact match of the selected categorization in their Support Representative record are considered. The support representative who was assigned an incident on the oldest date and time is selected.

Routing begins with skill based routing level one, and then advances to the next skill based level. If multiple support representatives have the same skill level, the load balanced routing weights are used.

Use Location By Skill Based Routing - Select Yes to enable location by skill based routing, which routes to support representatives with matching skills at a certain support representative location. You can use location by skill based routing with:

- mySupport-submitted tickets. The location selected by the mySupport customer takes precedence, then the support representative location associated with the customer's primary group, then the location associated with the company's primary group. If none are found, the default location (specified in the mySupport Portals Configuration screen) is used.
- Email-submitted tickets. The customer's profile will be searched for a primary group and associated support representative location. If there is no associated location, the customer's company record is searched for a primary group and associated location. If none are found, the location in the Default Location field on the Email Processing Basics tab will be used.

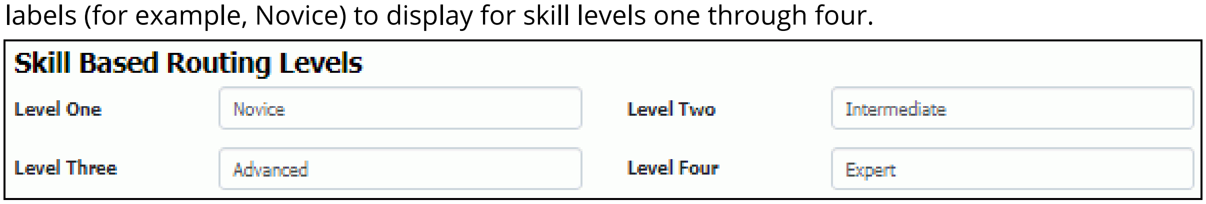
Once a location is determined, all support representatives in that location will be searched for matching skills.

Location By Skill Based Routing Method - This field appears if using location by skill based routing. Select:

- Standard - allows the support representative to select a location and the level of categorization that exactly matches the categorization for which support representative skills should be searched.
- Load Balancing - routes incidents based on current open incident statistics, including weights based on incident priority. The support representative in the selected location and category level with matching skills and the lightest workload is selected.
- Round Robin - allows the support representative to select a location and the level of categorization that exactly matches the categorization for which support representative skills should be searched. The support representatives in the selected location with matching skills are considered; the support representative who was assigned an incident on the oldest date and time is selected.

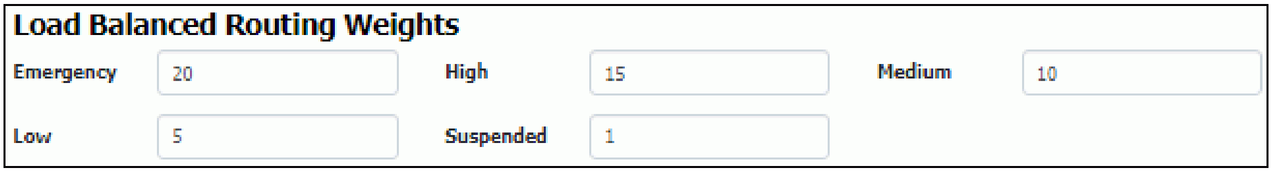
Skill-Based Routing Levels

Enter the labels (for example, Novice) to display for skill levels one through four.



Load Balanced Routing Weights

Load balanced routing involves weights based on incident priority. As discussed in the following example, a support representative's workload is calculated by multiplying the number of incidents at a certain priority level by the weight assigned to that priority level.



For example, one support representative has two incidents at emergency priority. A second support representative may have one incident at medium priority and two at low priority. If the emergency incident weight is 20, the medium incident weight is 10 and low incident weight is 5, the support representative's workloads will be calculated as follows:

- First support representative = Two incidents at emergency priority (2 X 20 = 40).
- Second support representative = One incident at medium priority and two at low priority (1 X 10) + (2 X 5) = 20.

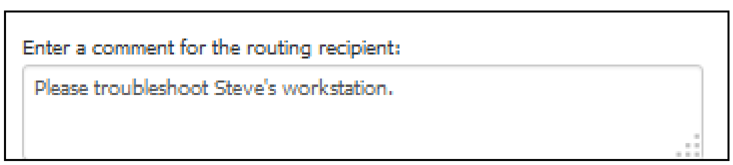
Even though the second support representative has three incidents and the first has two, the second support representative's workload is less.

Use the fields in the Load Balanced Routing Weights section to enter weights for priority levels and incidents with a suspended status. To weight all incidents the same regardless of their priority, enter a value of 1 for all five incident weight fields.

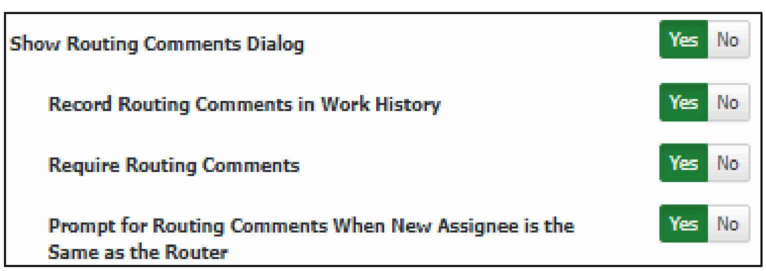
Note that rules can route incidents, problems, and changes via load-balancing and round robin.

Routing Comment Options

The Routing Comment dialog can be configured to appear in the Incident screen for the support representative to enter a note to be included in the notification email sent to the new assignee. (The note will be on the first line of the email.)



Note that the Route Comment prompt will not appear if no notifications are enabled for the routing event.



Show Routing Comments Dialog - Select Yes to display the Routing Comments dialog when an incident is routed.

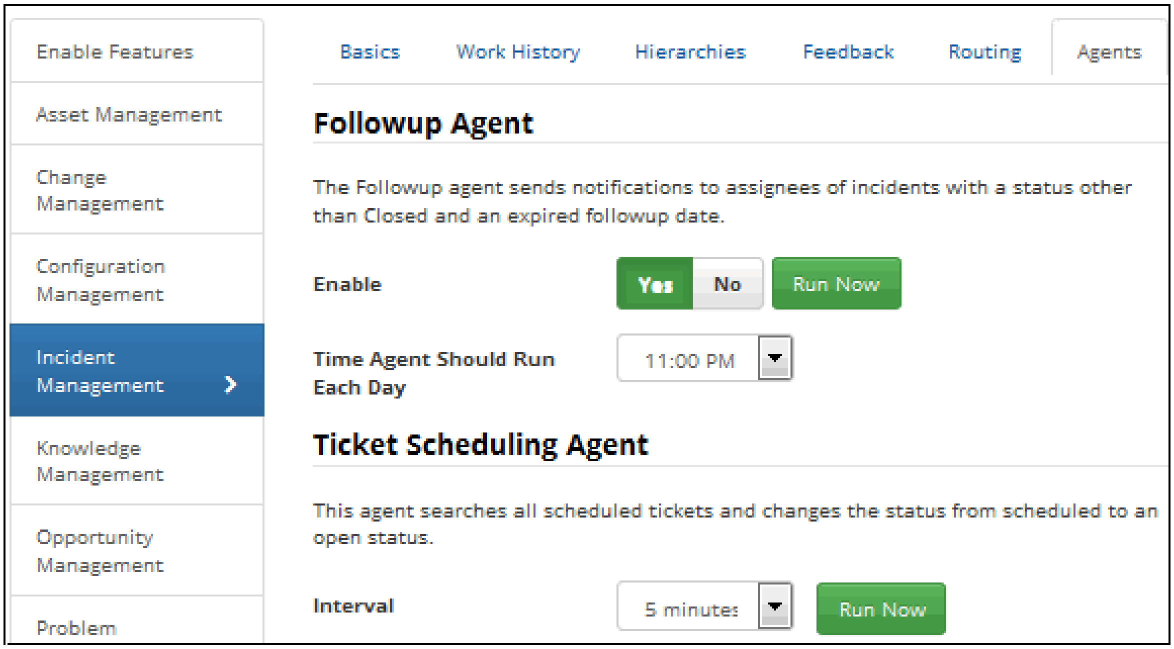
Record Routing Comments in Work History - Select Yes to, when a routing comment is entered, automatically include the comment in the Work History field.

Prompt for Routing Comments When New Assignee is the Same as the Router - Select Yes to display the prompt for routing comments if the new assignee is the same as the representative initiating the route.

Require Routing Comments - Select Yes to require a support representative to enter routing comments after routing an incident.

Enabling Incident Agents

Use the Agents tab to schedule the Incident Followup and Ticket Scheduling agents. You can click the Run Now button to execute an agent immediately.



Followup Agent/Time the Followup Agent Should Run Each Day - Select Yes to enable the Followup agent that checks all incident followup dates. The agent sends email reminders to the incident assignees for each incident with an expired followup date and a status other than a Closed status. After selecting Yes, use the Time Agent Should Run Each Day field to select the time the agent should run.

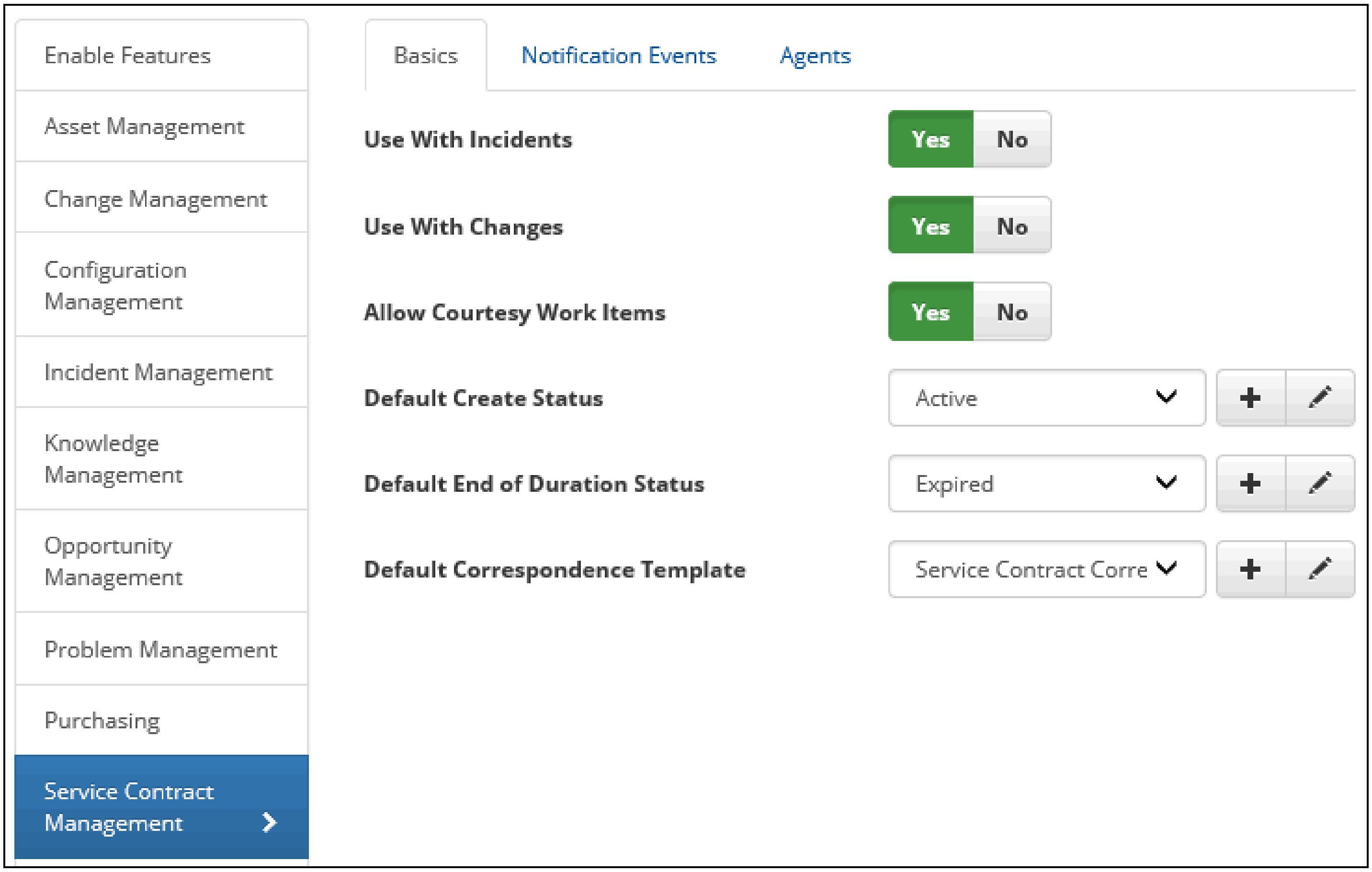
Ticket Scheduling Agent Interval - Select the number of minutes in the interval for the Ticket Scheduling agent to check all scheduled tickets for start dates/times and, if the specified date/time is reached, changes the status from Scheduled to an open status. Ticket generation times are also checked and tickets are created if the specified time is reached.

Setting Service Contract Feature Basics Options

The Service Contract Basics screen enables you to enable use of service contracts with incidents and changes, courtesy work items, Service Contract entry screen defaults, and notifications.

Completing the Basics Tab

Use the Basics tab to enable use of service contracts with incidents and changes, courtesy work items, and Service Contract entry screen defaults.



Use With Incidents - Select Yes to enable Service Contract functionality in the Incident entry screen.

Use With Changes - Select Yes to enable Service Contract functionality in the Change entry screen.

Allow Courtesy Work Items - A courtesy work item is an incident or change that does not count against the service contract in effect for a customer, company, or asset; it is created for an incident or change if the Mark This a Courtesy Work Item checkbox is enabled in the Select Service Contract dialog that appears after a customer is selected.

Select Yes to include the Mark This a Courtesy Work Item checkbox in the dialog that appears for selecting a service contract in the Incident and/or Change screens.

Default Create Status - Select the status level to display by default when a service contract is created. Use the Create + New and View/Edit options to access the Custom Status Labels screen; see “Defining Custom Status Labels” on page 29 for more information.

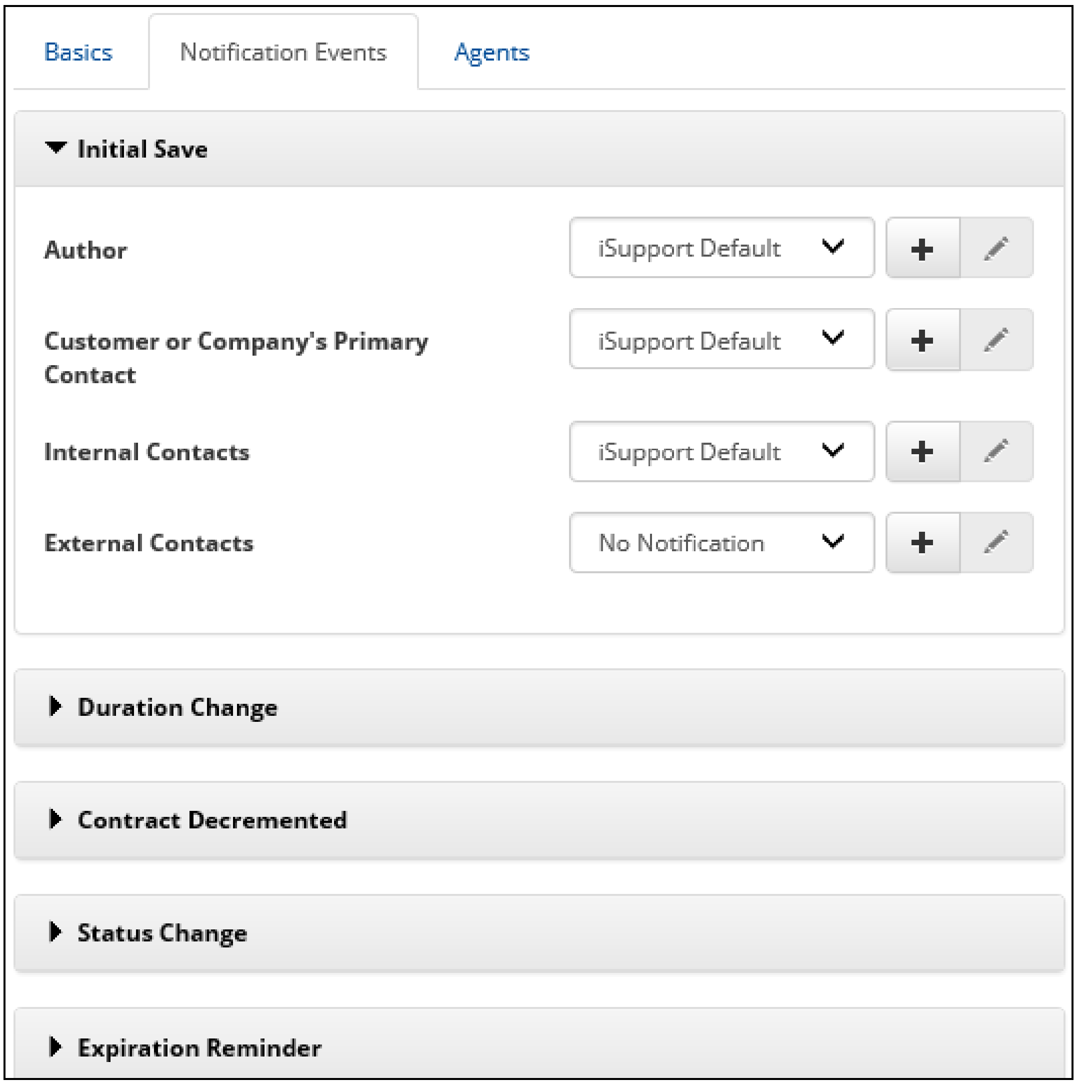
Default End of Duration Status - Select the Expired status level to assign to the contract by default when the date in the Duration End field is reached. Use the + Create New and View/Edit options to access the Custom Status Labels screen; see “Defining Custom Status Labels” on page 29 for more information.

Default Correspondence Template - Select the correspondence template that will apply by default when a support representative initiates a correspondence via the Service Contract entry screen. Correspondence templates that are active and enabled for the Service Contract module will be available for this feature. Use the Create New and View/Edit options to access the Correspondence Template screen.

Setting Up Notifications for Service Contract Events

You can configure notifications to be sent when service contract events occur such as record creation, a change to the duration of the contract, an incident or change is counted against the contract, a support representative makes a change in the Status field, or an expiration reminder is sent.

The notifications on this screen are used as defaults for the Notification Event field in the Service Contract entry screen. Use the fields below to enable specified notifications to be sent to specified recipients for Service Contract events. You can select the default notification or a predefined custom notification; use the Create New and View/Edit options to access the Custom Notifications screen. Note that these settings will be used if nothing is selected in the Notification Event section in the Service Contract entry screen and no template is selected. Notifications are sent according to the schedule of the Service Contract agent; see "Enabling the Service Contract Agent" on page 18.



Initial Save - Select the recipients and notifications to be sent when a service contract is initially saved.

Duration Change - Select the recipients and notifications to be sent when an entry is changed in the Duration fields for a service contract and the record is saved.

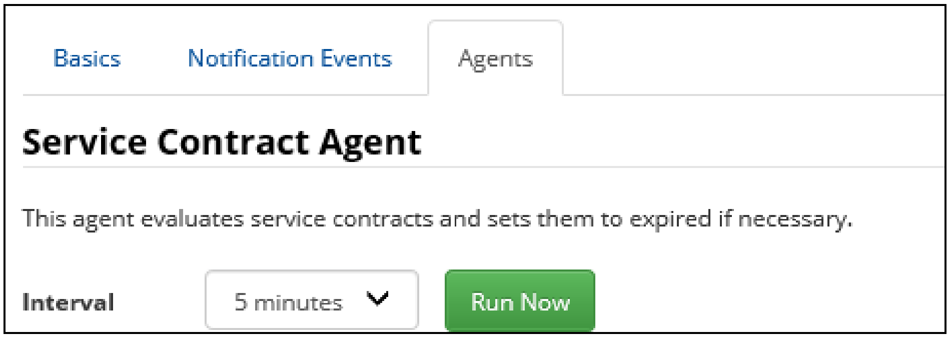
Contract Decremented - Select the recipients and notifications to be sent when an incident or change is counted against a service contract.

Status Change - Select the recipients and notifications to be sent when an entry is made in the Status field for a service contract and the record is saved.

Expiration Reminder - Select the recipients and notifications to be sent when a contract is about to expire.

Enabling the Service Contract Agent

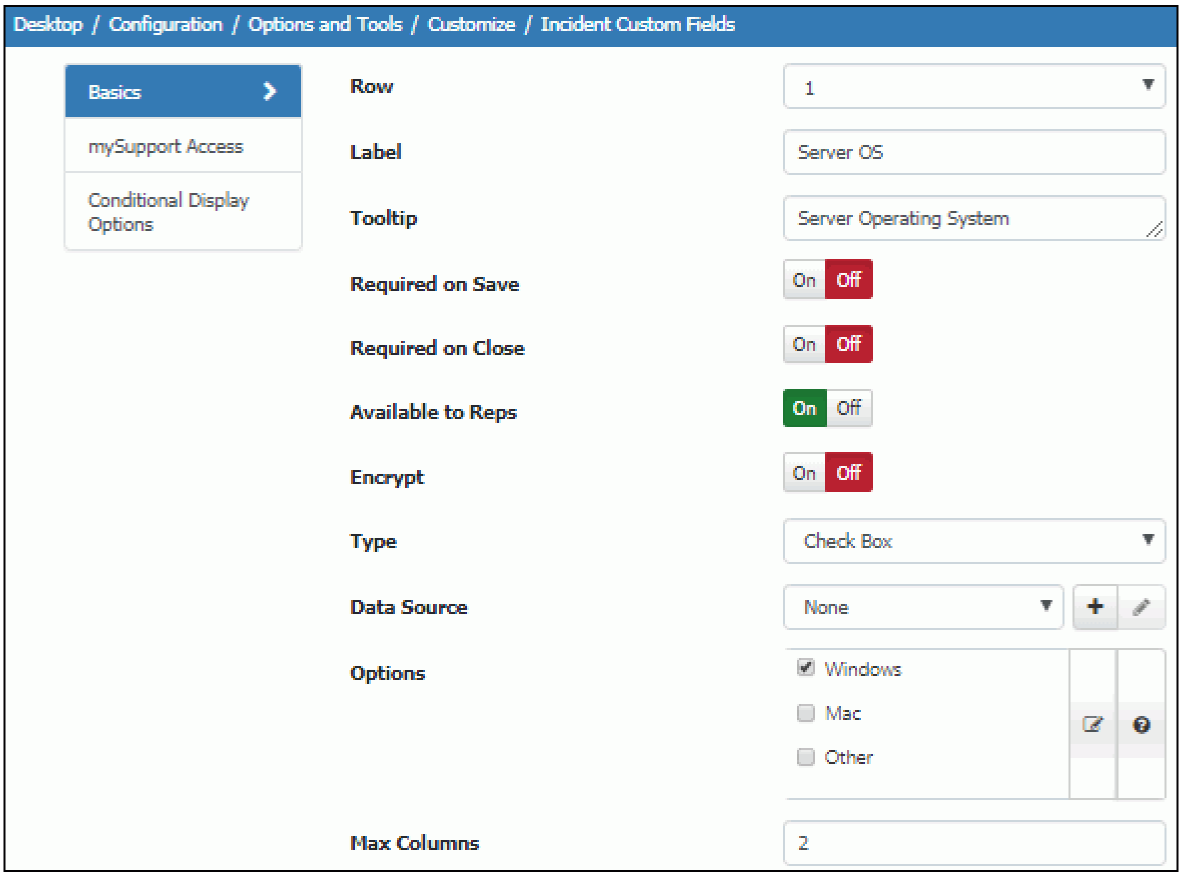
In the Service Contract Agent Interval field, select the number of minutes in the interval for the Service Contract agent to check all service contracts for counts and/or end dates/times; if the specified total count and/or end date/time is reached, the status changes to an Expired status. You can select Daily to run the agent every day at a specified start time.



Configuring Custom Fields

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

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



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

Label - Enter the label for the custom field.

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

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

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

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

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

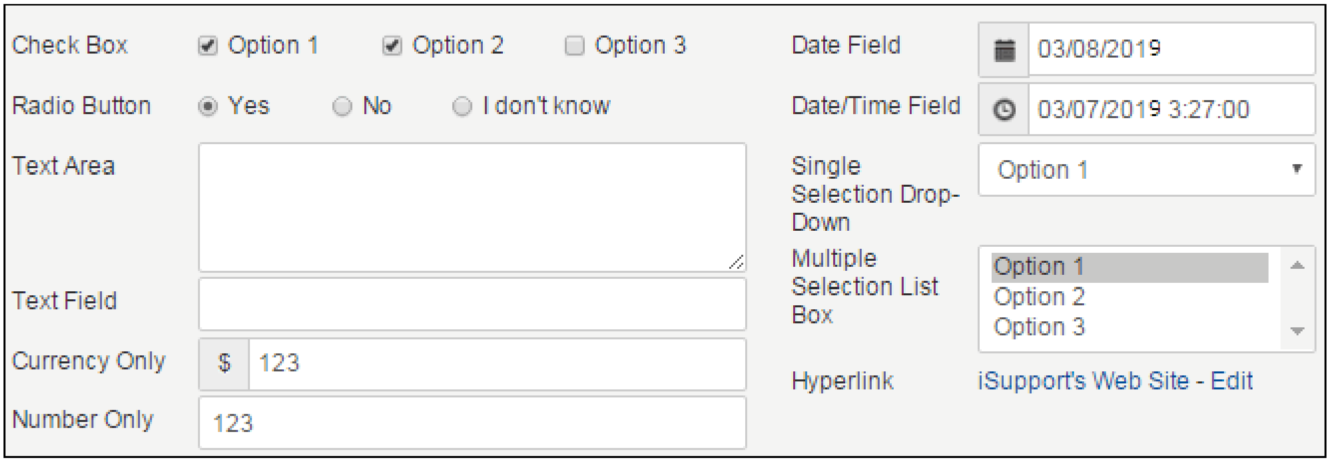
Type - Select the format of the field. Note that for list-type fields (Checkbox, Multiple Selection List Box, Radio Button, Single Selection Drop-Down, and Type Ahead) you can map to a SQL data source and populate and synchronize options for a field; see "Pulling From a Data Source" on page 24 for more information.

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

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

  Note that the settings in the web.config file should be updated only as directed (via this guide or iSupport Technical Support); failure to do so may result in data loss or corruption. See http://msdn2.microsoft.com/en-us/library/system.globalization.cultureinfo.aspx for more information on defined culture settings.
- A **Date** field enables entry or selection of a date in MM/DD/YY format; a **Date Time** field enables entry or selection of a date (MM/DD/YY) and time. To disable manual entry in Date and Date Time fields and require the user to select from the calendar popup, select Yes in the Disable Manual Entry of Date Time Custom Fields field on the Advanced tab in the Custom Fields list screen.
- A **Hyperlink** field enables you to specify default text and a URL to appear in the field; the user can change those entries. You can also leave the field blank and allow the user to enter the default text and URL.
- A **Label Only** field does not display a value option; you can use it as a section header to group custom fields.
- A **Multiple Selection List Box** field enables the user to select multiple entries in a list. Use the Max Rows field to enter the number of selections to appear before a scroll bar is used.
- A **Number Only** field enables entry of the numbers 0 through 9 and a decimal point.
- A **Radio Button** field enables only one selection; use the Max Columns field to enter the number of radio buttons to appear before a scroll bar is used.
- A **Single Selection Drop-Down** field enables selection of one item in a list.
- A **Text Area** field enables text characters to be entered in a resizable field.
- A **Text** field enables text to be entered in a one-line field.
- A **Type Ahead** field initiates a search of matching options after a few characters are typed. This custom field type is only used for fields that are linked with a data source.

Examples are shown below.



Options - This field displays when creating a radio button, checkbox, multiple selection list box, or single selection drop-down. Enter or paste items into this field; separate each value with a comma or return and select Commit Items when finished. Select items to specify defaults and drag items to change the order. Options can be populated by and synchronized with a SQL data source; see "Pulling From a Data Source" on page 24 for more information.

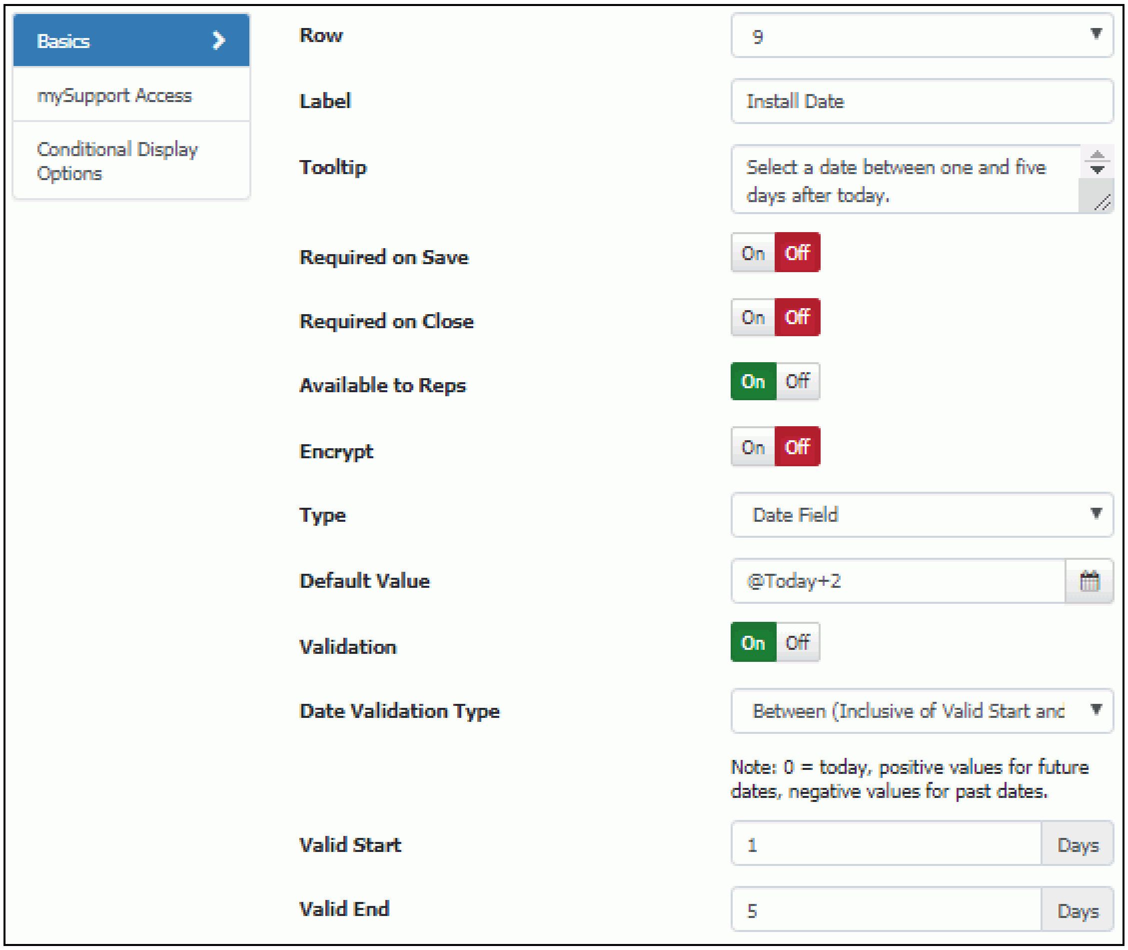
Default Value - Enter a value to appear as an option in the custom field by default.

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

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

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

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



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

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

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

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

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

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

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

- If you enter 1 in the Valid Start field and 3 in the Valid End field, the dates available for selection will start one day after the current date and end three days after the current date.

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

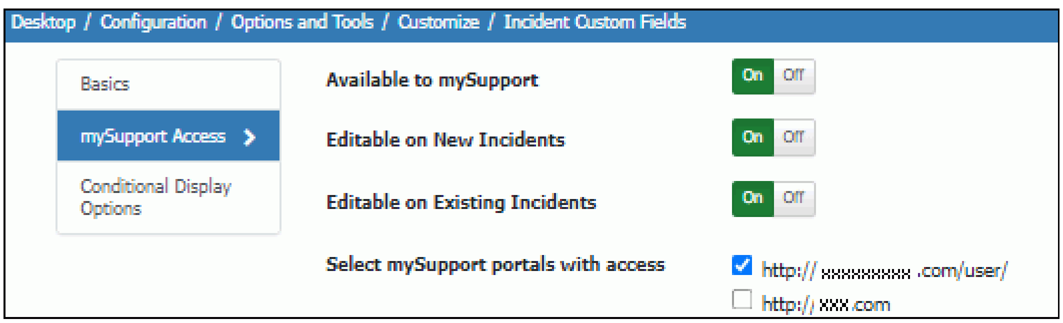
mySupport Access Options

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

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

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

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

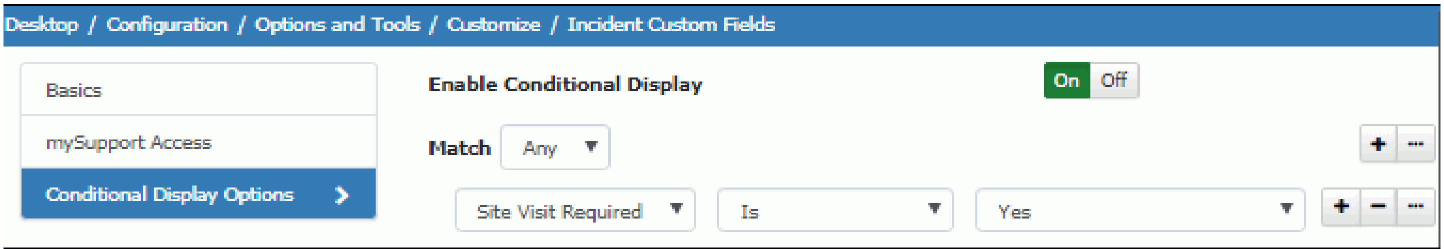


Setting Advanced Options

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

Conditional Display Options

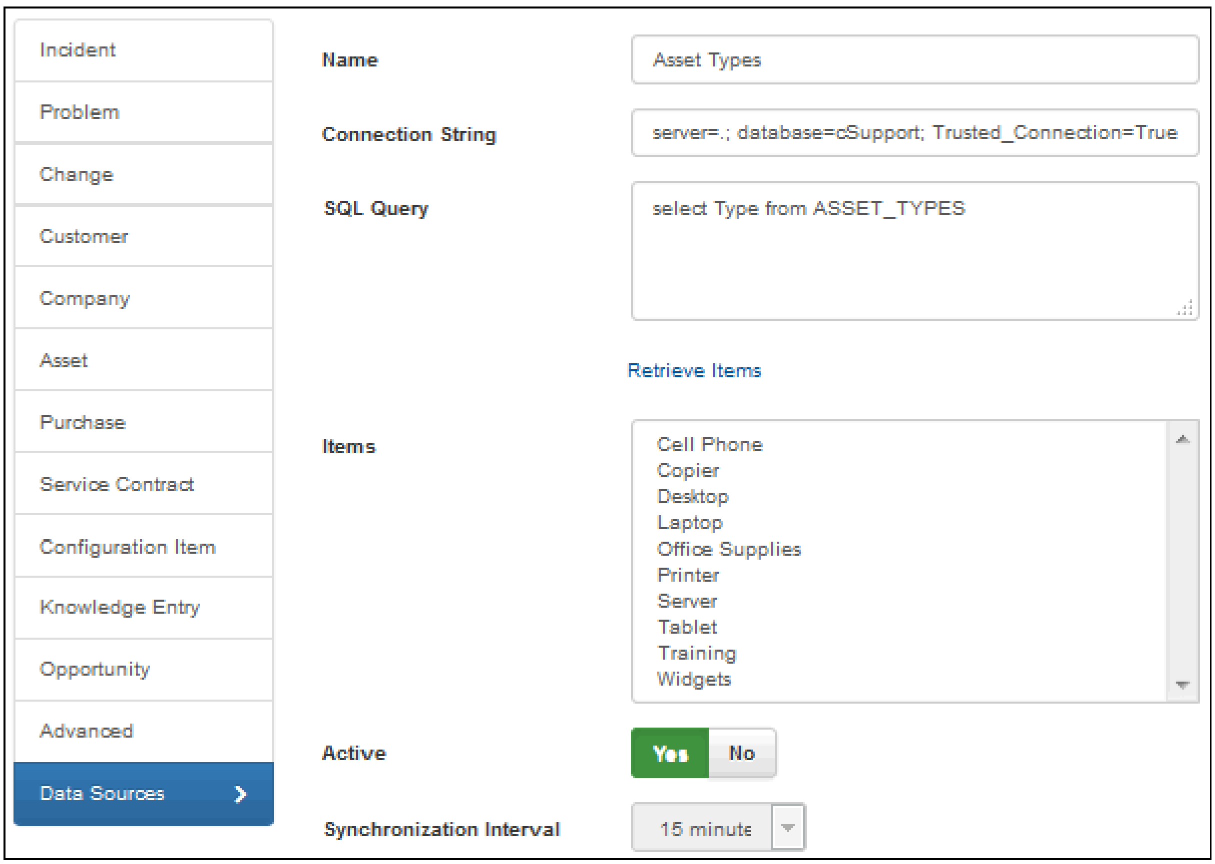
Enable Conditional Display - Select On to enable the Conditional Display Options fields for configuring conditions on which to base display of the custom field.



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

Pulling From a Data Source

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



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

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

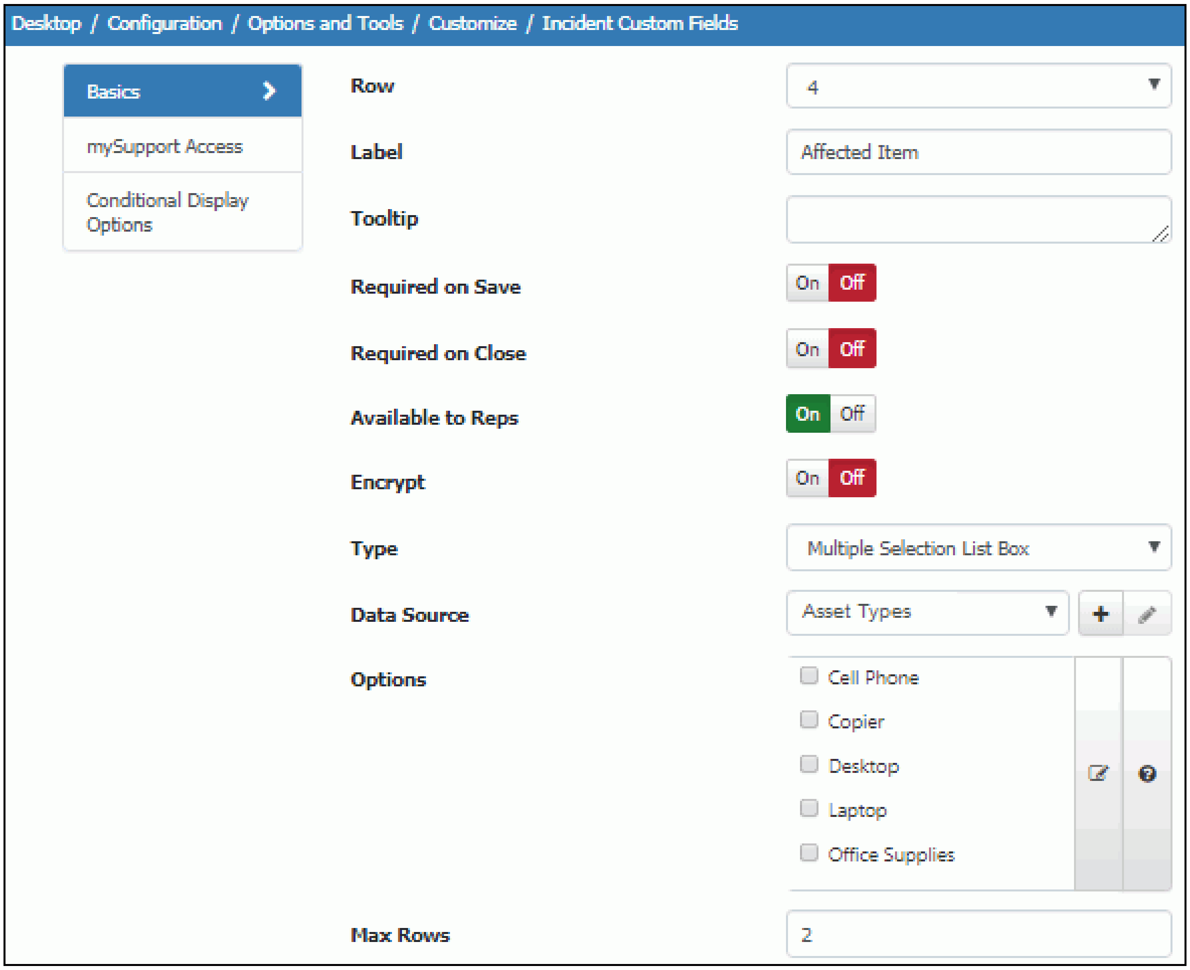
SQL Query - Enter the SQL query string for accessing the field options in the SQL database. Select the Retrieve Items button to populate the Items field using this string.

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

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

Using the Data Source for a Custom Field

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



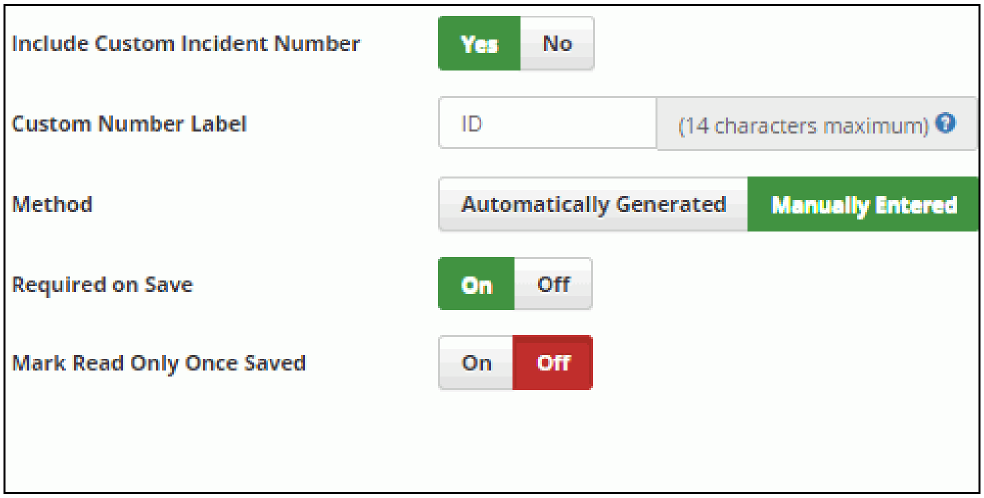
Defining Custom Numbers

You can include a field on the Incident, Problem, Change, Service Contract, and Purchase Request screens for entering a custom number, or an automatically generated number consisting of a prefix, suffix, and sequence that you configure. The number can be up to 15 characters.

The Custom Number configuration fields appear after selecting Yes in the Include Custom <record type> Number field. There are two methods for configuring custom numbers: a manually entered option or an automatically generated option.

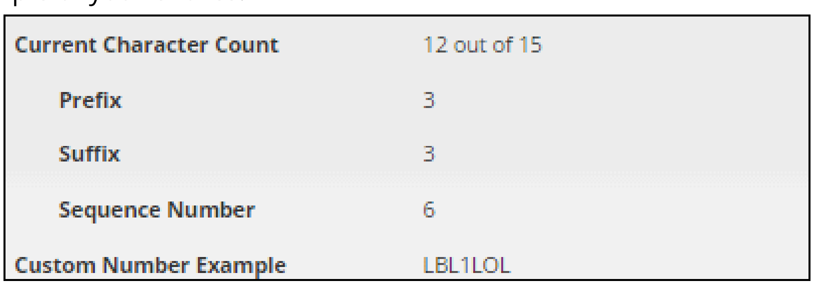
Configuring a Manually Entered Number

The Manually Entered option displays a field for entering a custom number. Select Yes in the Required on Save field to require entry in this field before the work item can be saved. Select Yes in the Mark Read Only Once Saved field to prohibit entry in the field after the work item is saved.



Configuring an Automatically Generated Number

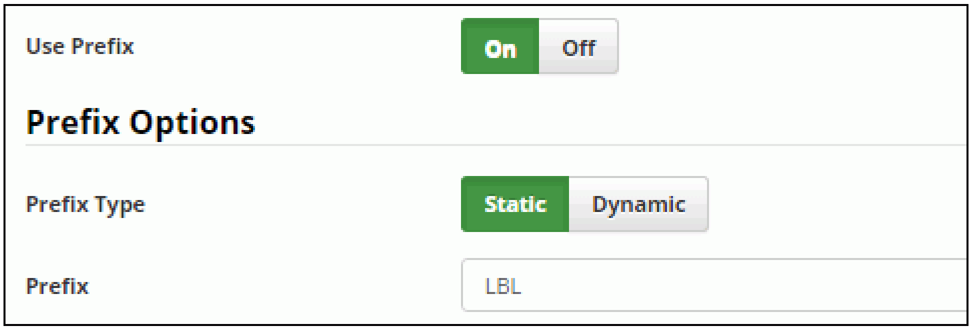
The Automatically Generated option creates numbers automatically based on prefix, suffix, and sequence settings that you configure. You can either use a static (fixed) custom prefix and suffix, restricted via a start and end number if desired. Prefixes and suffixes can be static (fixed) or dynamic; however, if you have a dynamic prefix you must have a static suffix. The number cannot exceed 15 characters; the box above the Use Prefix field contains a current character count and example of your entries.



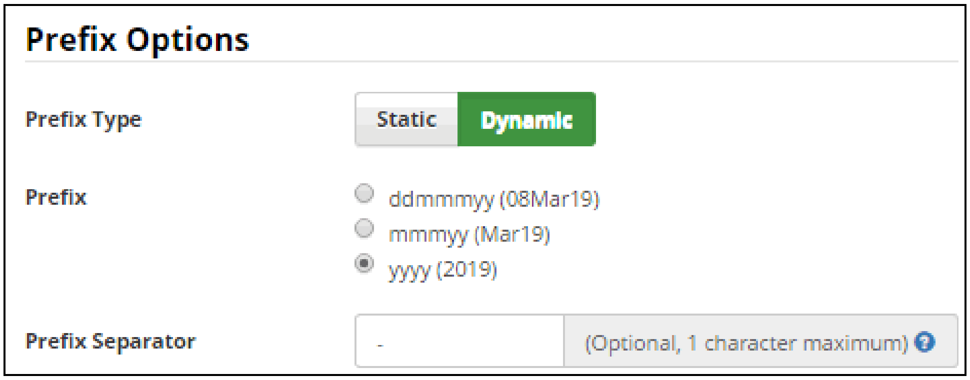
Configuring the Prefix

In the Prefix Options section, select the Use Prefix checkbox to configure characters that will precede the custom number. Then select the prefix type: static (fixed) or dynamic (a day, month, and/or year combination).

- If using a Static prefix type, enter the characters (letters, numbers, or symbols) in the Prefix field.



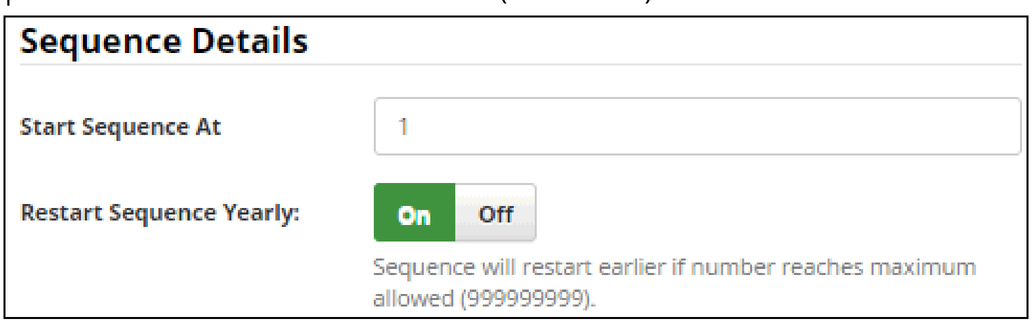
- If using a Dynamic prefix type, select the day, month, and year combination in the Prefix field. You can optionally enter a character (such as a hyphen) in the Prefix Separator field. Note that the year will change when the first work item is created after 12:00pm on December 31.



Configuring the Sequence

Use the fields in the Sequence Details section, to configure the sequence number between any configured prefix and any configured suffix.

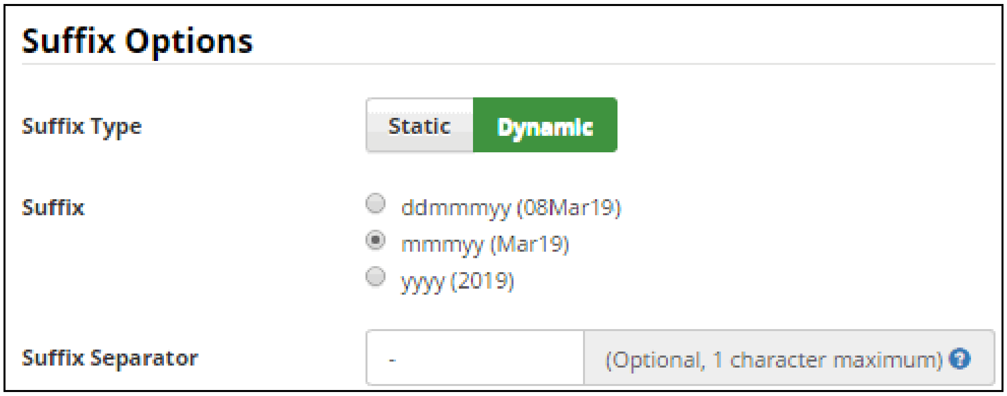
- Enter the number to start the sequence in the Start Sequence At field.
- Your selection in the Prefix field will determine the Restart Sequence field. If you select yyyy and you wish to restart the sequence when the first work item is created after 12:00pm on December 31, select Yes in the Restart Sequence Yearly field.
- If you wish to restart the sequence after the sequence number reaches a specified maximum (for example, after the sequence number reaches 1000), enter the maximum number in the Restart Sequence After field. If not specified, sequence will restart at maximum allowed (999999999).



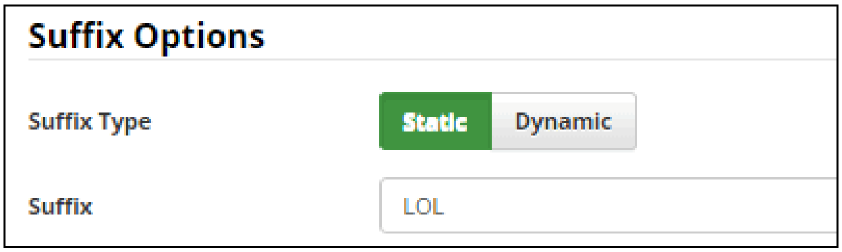
Configuring the Suffix

Select On in the Use Suffix field to configure characters that will be placed after the custom number. If using a Dynamic prefix type, you'll need to use a static suffix.

- If using a Dynamic suffix type, select the day, month, and year combination in the Suffix field. You can optionally enter a character (such as a hyphen) in the Suffix Separator field. Note that the year will change when the first work item is created after 12:00pm on December 31.



- If using a Static suffix type, enter the characters (letters, numbers, or symbols) in the Suffix field.



Defining Custom Status Labels

Use the Options and Tools | Customize | Custom Status Labels screen to create custom labels for iSupport's work item status levels. These labels will be included in views and reports, and will appear for selection in work item screens; however, you can restrict access via the Template and Support Representative Group configuration screens. Use the **Order of Precedence** link in the Custom Status Labels screen to set which will prevail if both a template and a support representative group have a restricted status.

You can also create labels that will appear to customers using mySupport.

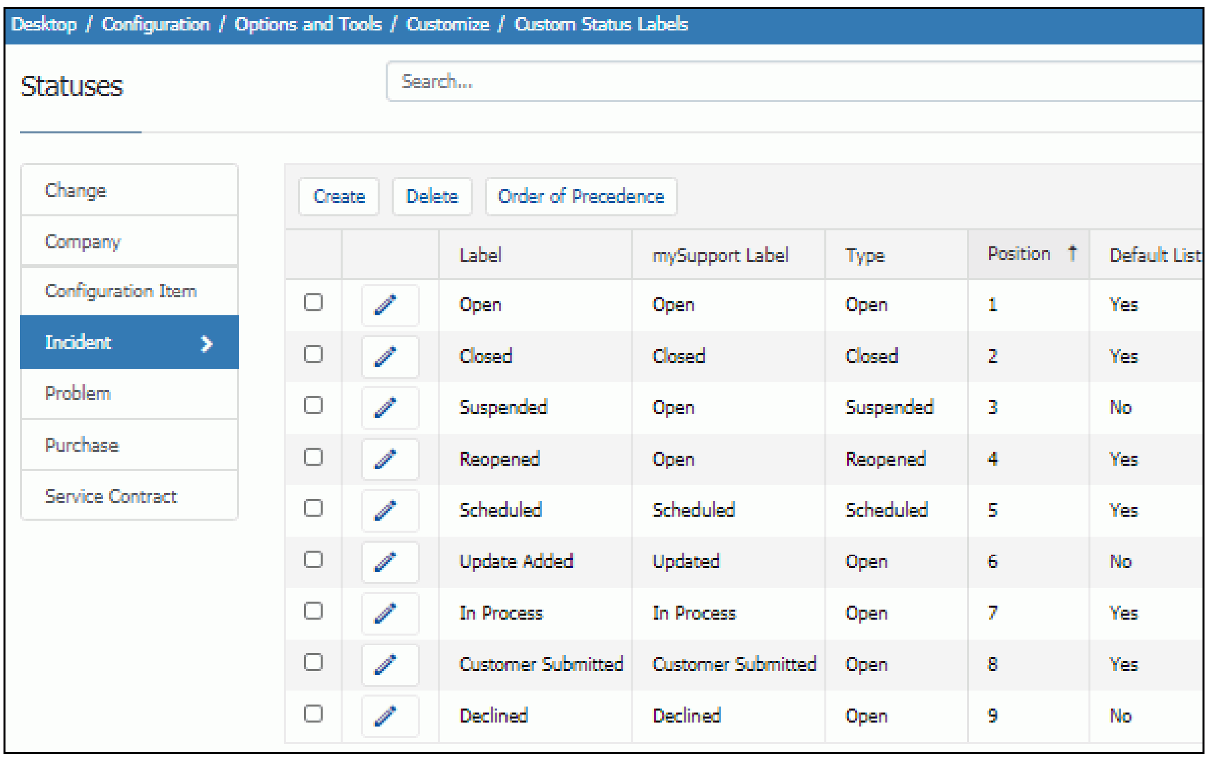
If you have the Incident Management Edition, you can define labels for the following work item types:

- Incident: Open, Closed, Suspended, Scheduled, Reopened
- Service Contract: Active, Inactive, Suspended, and Expired.

If you have the Service Desk Edition, you can define labels for the following of work item types:

- Change: Open, Closed, Suspended
- Problem: Open, Closed
- Purchasing: Open, Closed

Note: For all except Company and Configuration Item, there must be at least one status label of each type. For incidents, there must be only one Reopened and Scheduled type.



Label - Enter the name for the status.

mySupport Label - Enter the status label to appear on the mySupport portal. Enable the status label via the <*work item type*> Display tab in the Core Settings | mySupport | Portals | Options configuration screen.

Type - Select the basis for the custom status label: Open, Suspended, Reopened, or Closed. Note: Since there can only be one Reopened status label, it will not be available for new status labels.

Position - Select the number of the position for the status to display in the Status field dropdown list. (Row one will be the first status, row two will be the second status, and so on.)

Default List (incidents/changes) - Enable to include the status as an available option in the default list that will appear in the Status field when a support representative creates a new incident or change. If not enabled, the status will only display if configured for a template that has been applied, set as the default status (on Incident or Change Basics for an email account or mySupport Portal Options), or a rule configured with the Change Status Label action is met. Note that status label display can also be controlled via the Restrict Statuses/Statuses to Display fields on the

Advanced tab in the Incident and Change Templates screen and on the Work Item UI tab in the Rep Group configuration screen (applies only to each support representative's primary group).

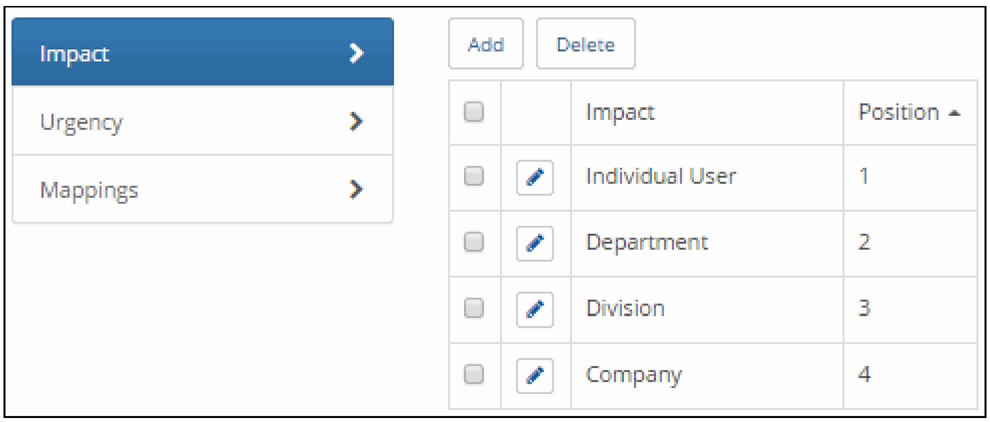
Defining and Mapping Impact and Urgency Values

Impact and urgency functionality is enabled for incidents in the Incident Management Feature Basics screen, and is permanently enabled for Problem and Change Management. Prioritization encompasses urgency (based on the amount of time a resolution is needed) and impact (usually the number of users affected); use the Impact and Urgency configuration screen to define impact and urgency values that map to priority levels. These values are used by Incident, Problem, and Change functionality.

In the Incident, Problem, and Change screens, the defined values will be available in the Impact and Urgency fields for selection. The specified mapped priority will appear as default but all priority levels will available if permissions are configured for the support representative to change the priority.

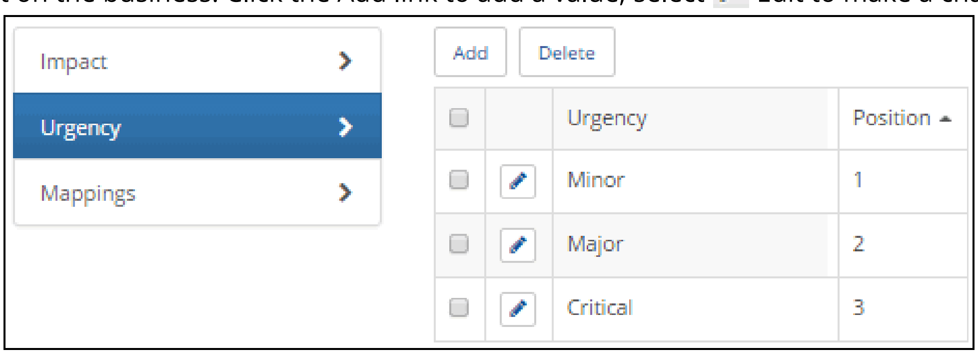
Adding Impact Values

Use the Impact tab to define values for the effect of an Incident, Problem, or Change on business processes. Click the Add link on the Impact tab to add a value; select Edit to make a change.



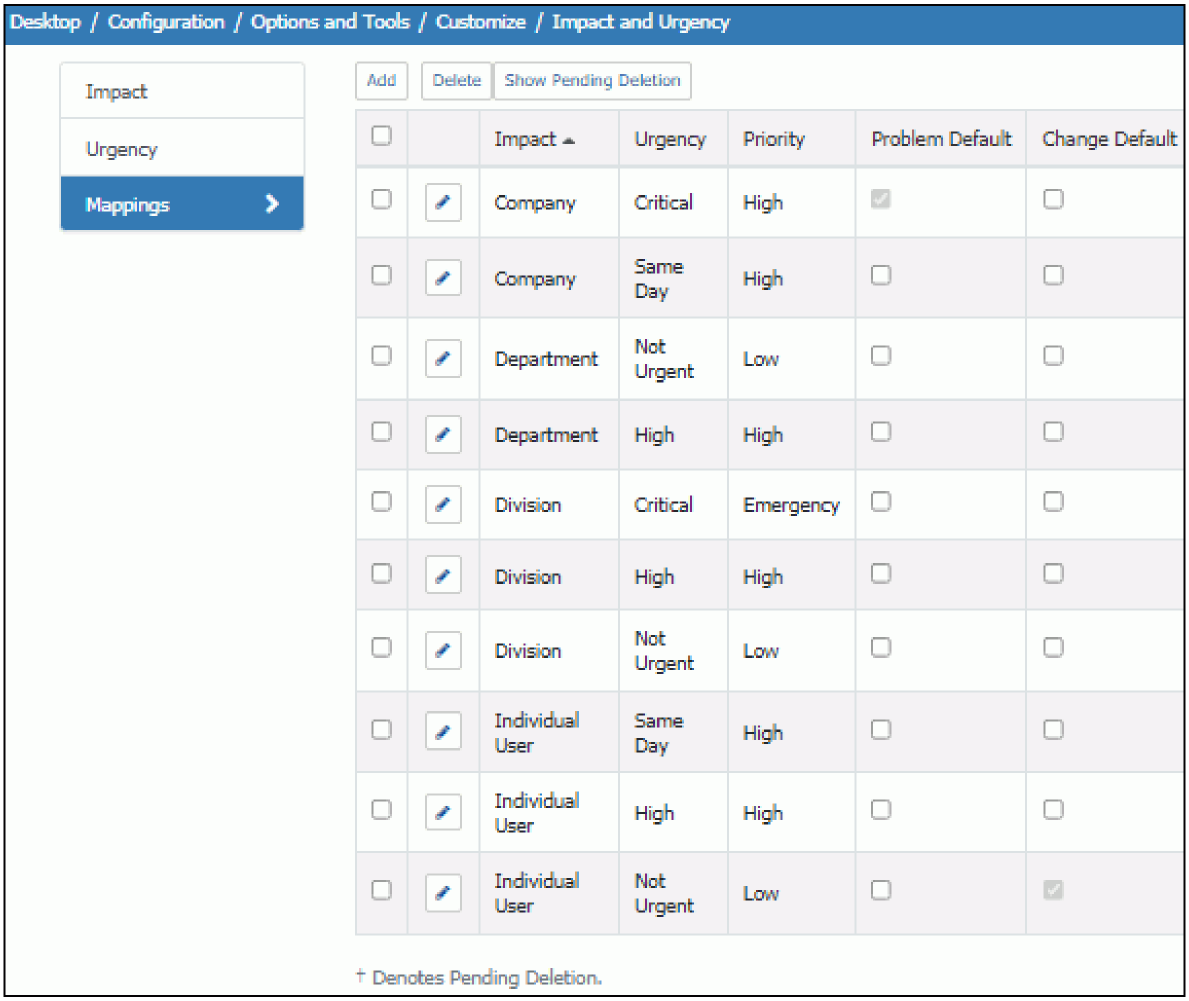
Adding Urgency Values

Use the Urgency tab to define values for the measure of how long it will be until an incident, problem, or change has a significant impact on the business. Click the Add link to add a value; select Edit to make a change.



Defining Mappings

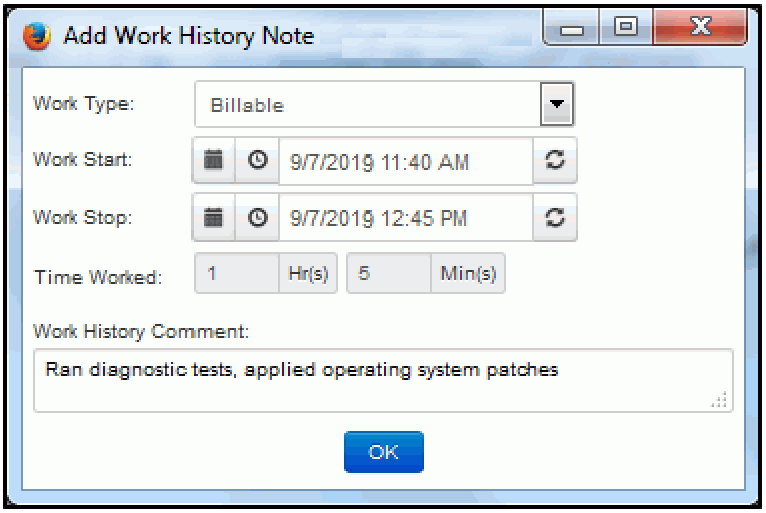
Use the Mappings tab to associate impact, urgency, and priority values and to specify the defaults to appear when the associated values are selected in the Incident, Problem, and Change screens. Click the Add link to add a value; select Edit to make a change.



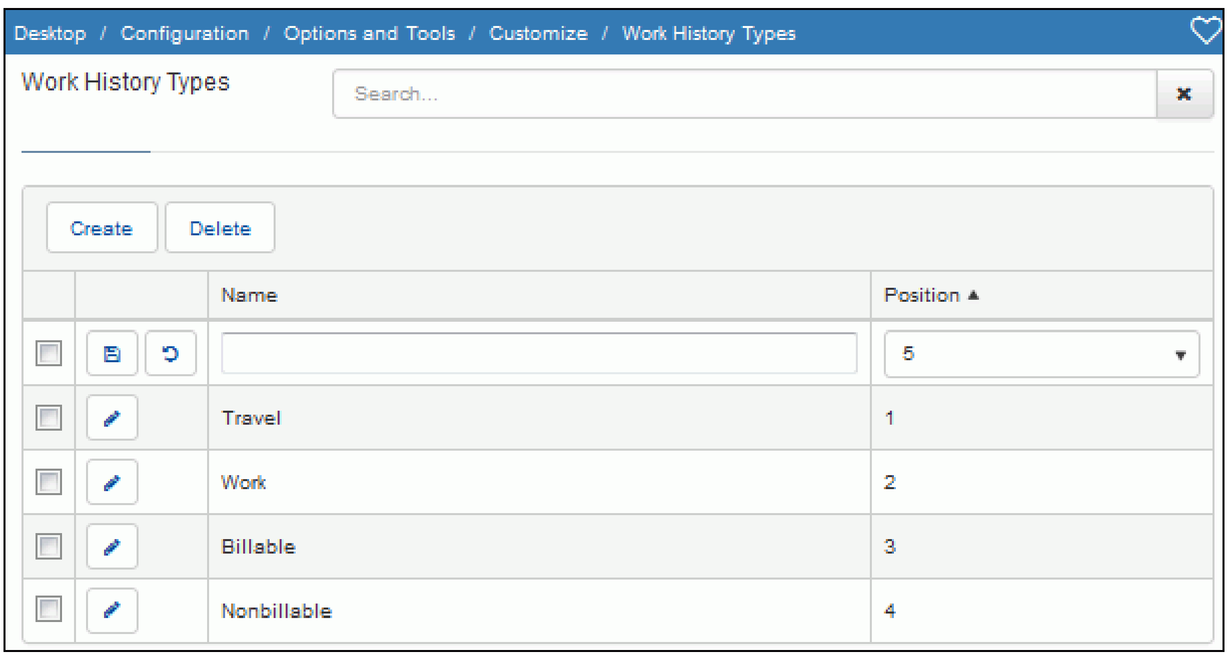
You can use the Show Pending Deletion link to display records that have been deleted by an iSupport user but are retained in the system because of references to other records (incidents, correspondence, etc.) The Database Maintenance agent ultimately removes these records. When the Show Pending Deletion link is selected, records that are pending deletion will display with a cross symbol.

Configuring Work History Types

Use the Options and Tools | Customize | Work History Types screen to create custom entries for support representatives to select to describe the work performed on a work item. As shown in the example below, these entries will display as options in the Work Type field in the Work History and Save dialogs in the Incident, Problem, Change, and Purchasing screens. The Work Type field is enabled for incidents, knowledge entries, problems, and changes in the Feature Basics screen.

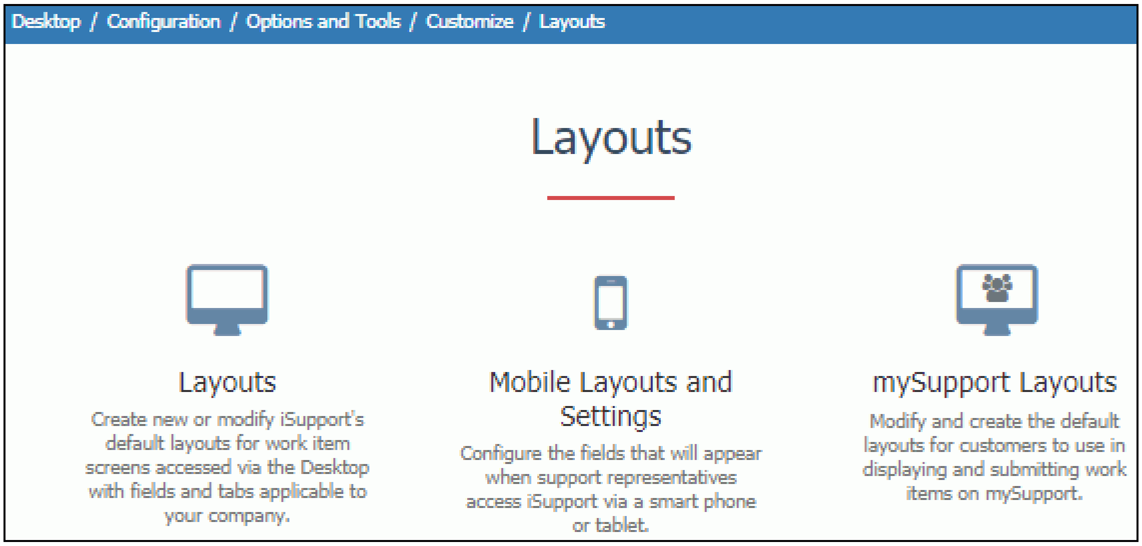


Use the Name field to enter work history types. In the Position field, select the number of the position for the status to display in the Status field dropdown list. (Row one will be the first status, row two will be the second status, and so on.)



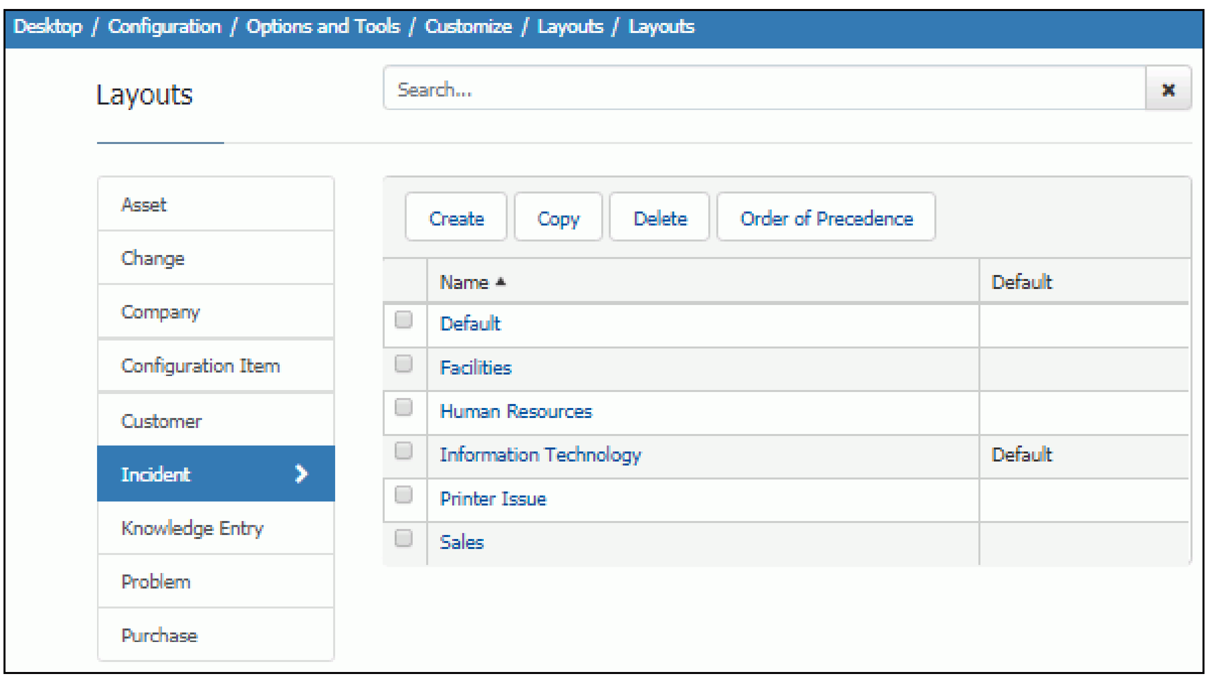
Configuring Screen Layouts

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



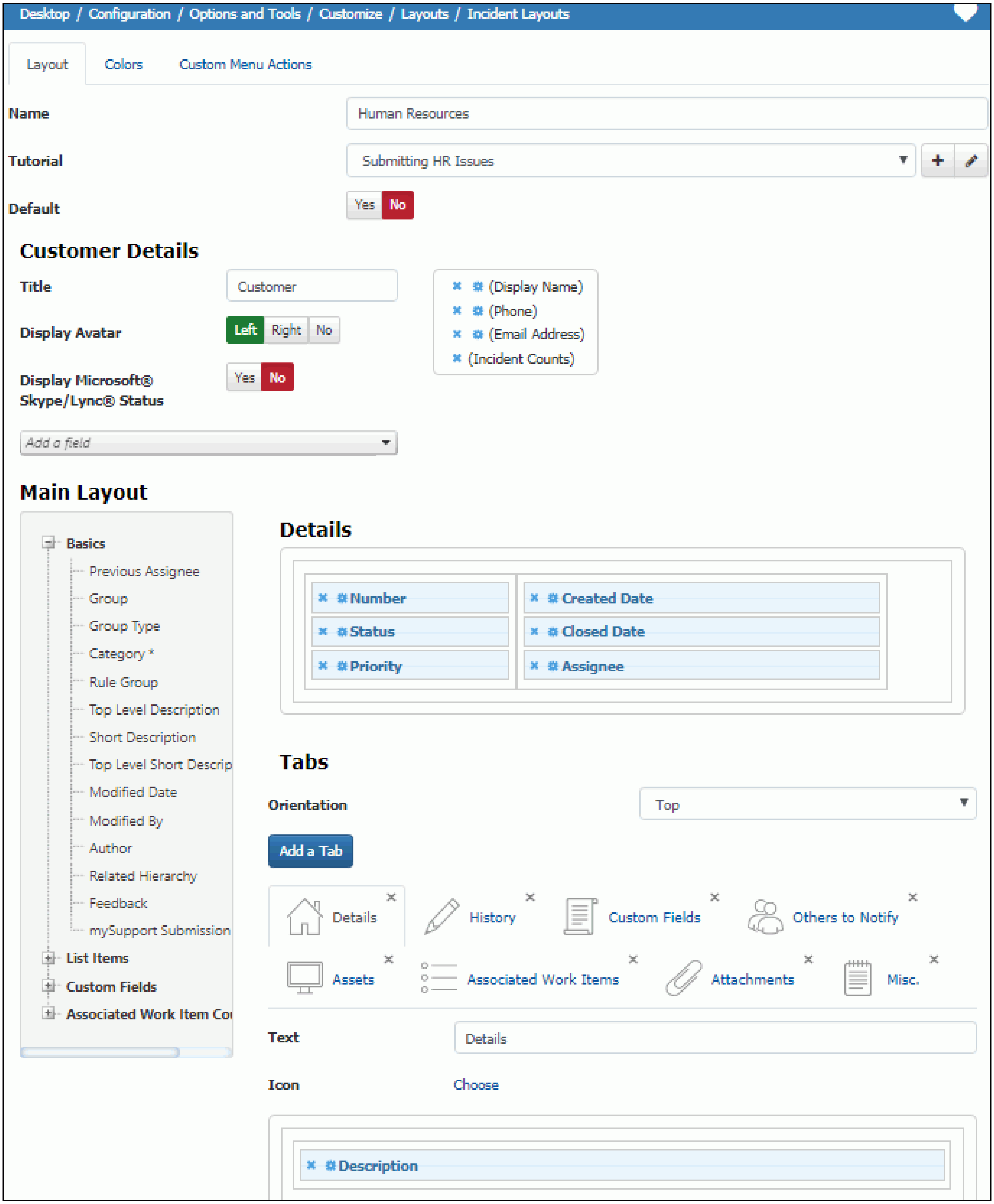
Note that only layouts configured via the Global Settings | Mobile Settings screen will apply to the mobile HTML5 interface. Also, mySupport Customer layouts will appear when the customer selects the View Complete Profile button in the Account Settings screen on a mySupport portal.

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



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

The Layout screen is shown below.



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

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

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

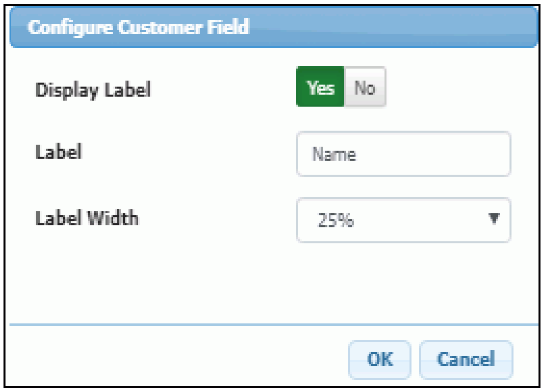
Configuring Customer Details

Rep Incident and Change Screens

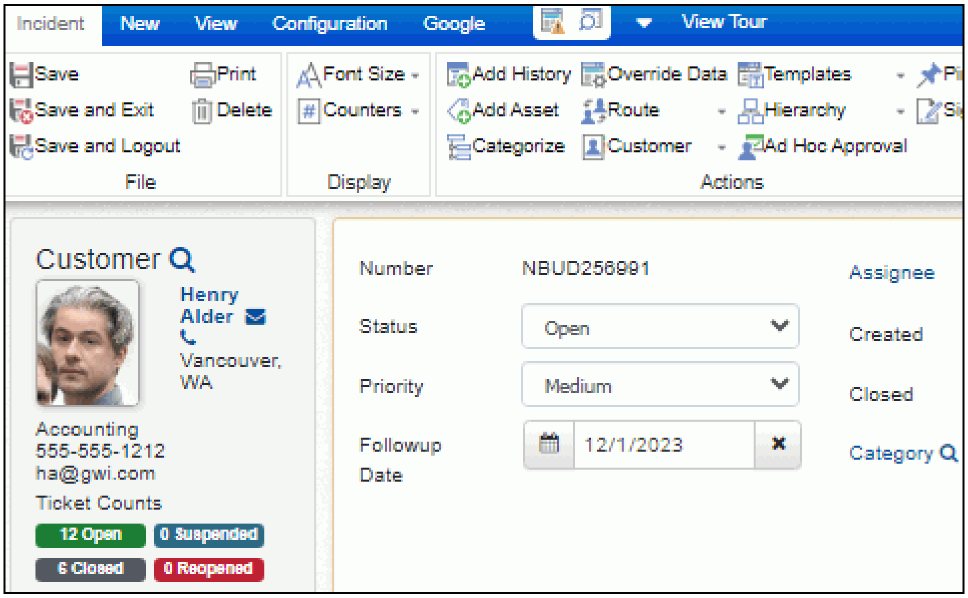
The Customer Details section will appear in the Rep Incident and Change Layout configuration screens as shown below.

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

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



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

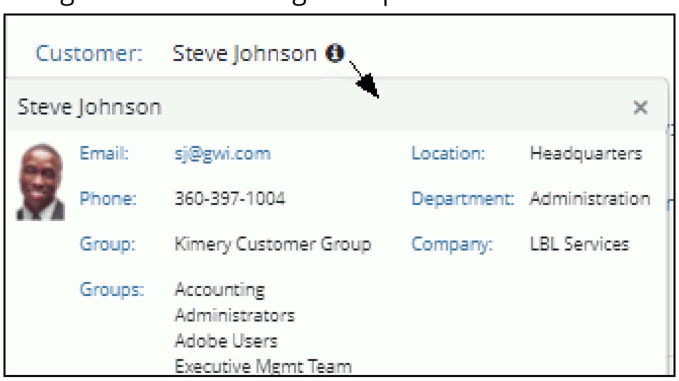


Use the **Display Microsoft® Skype/Lync® Status** field to include an icon that will display the Microsoft Skype/Lync status of a selected customer in the Incident and Change screens and enable the support representative to access Microsoft Skype/Lync functions. In order for the icon to appear, Microsoft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

mySupport Incident and Change Screens

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

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

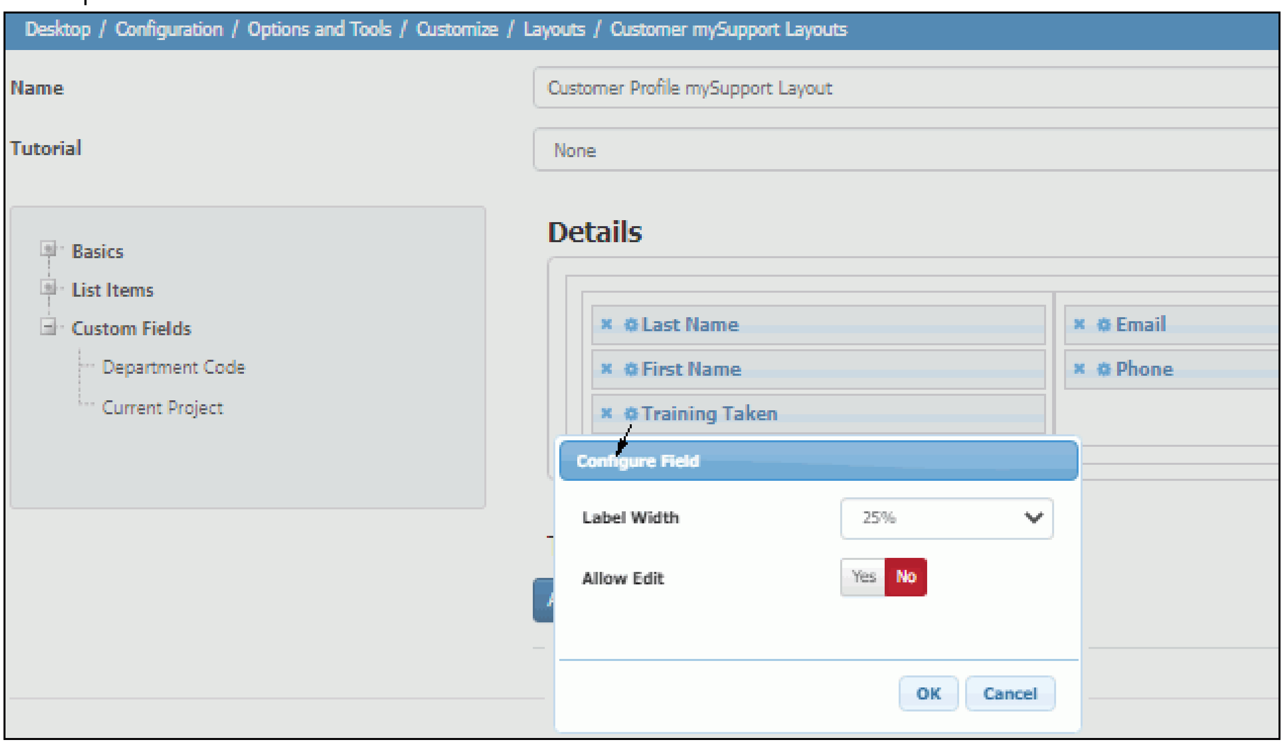


- Individual fields under the Customer Fields section

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

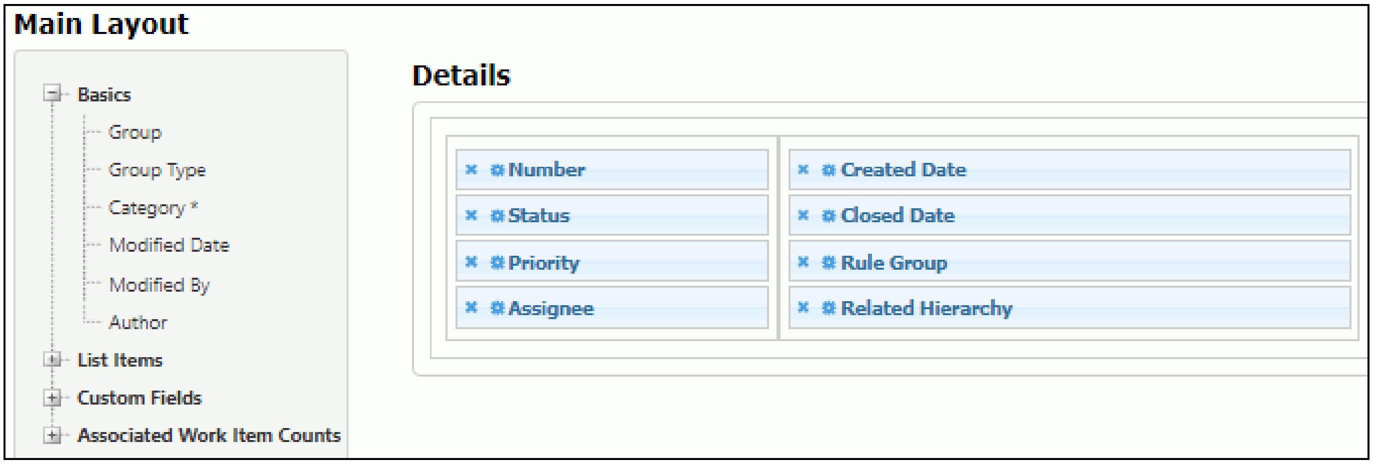
mySupport Customer Profile Custom Field Edit Access

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

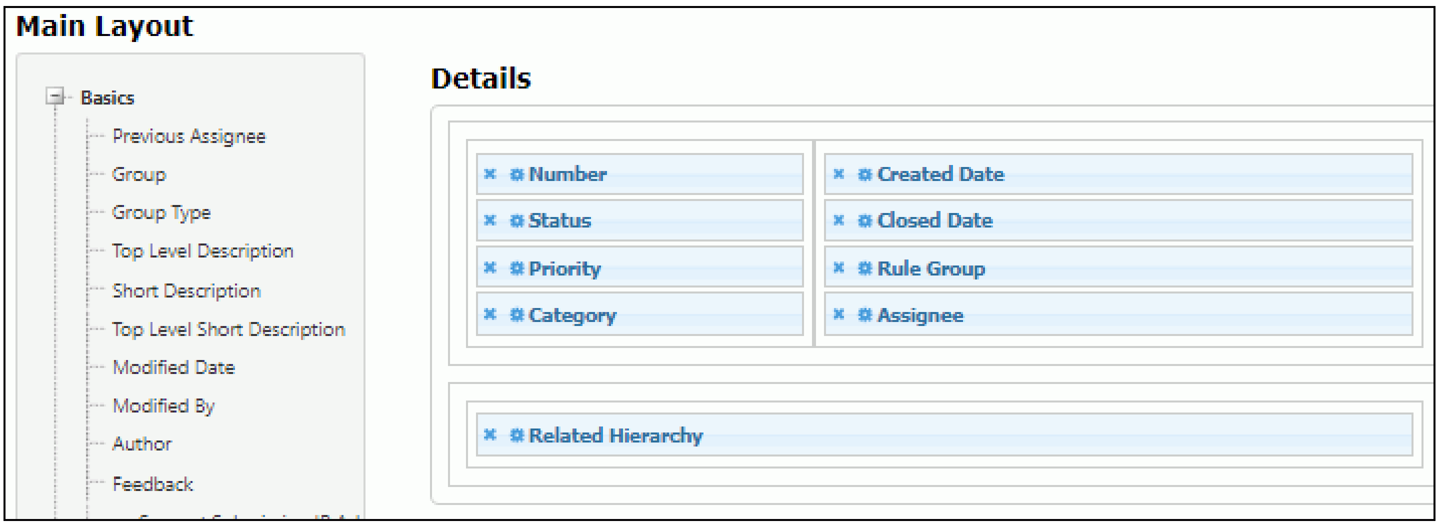


Adding Fields and Tabs

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

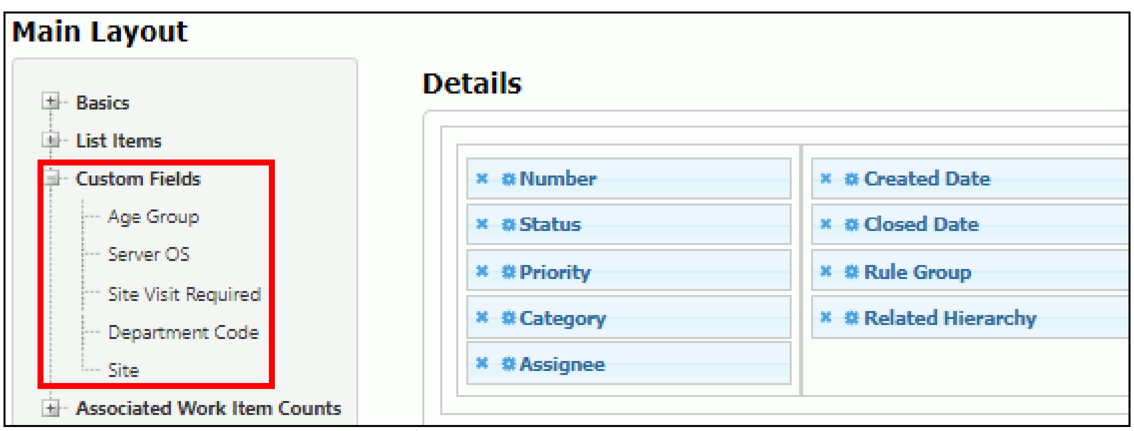


You can drag a field to the lower part of the Details section to create a subsection for a field.

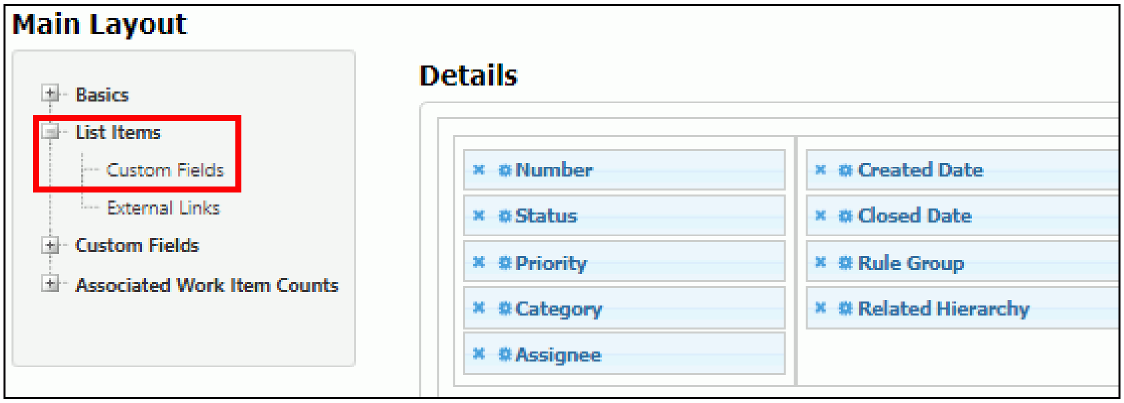


Global custom fields can be defined in the Custom Fields screen for the type of work item screen for which you're creating a layout, and additional custom fields can be defined for a category, asset type, or CI type. To include custom fields on a layout, you can:

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

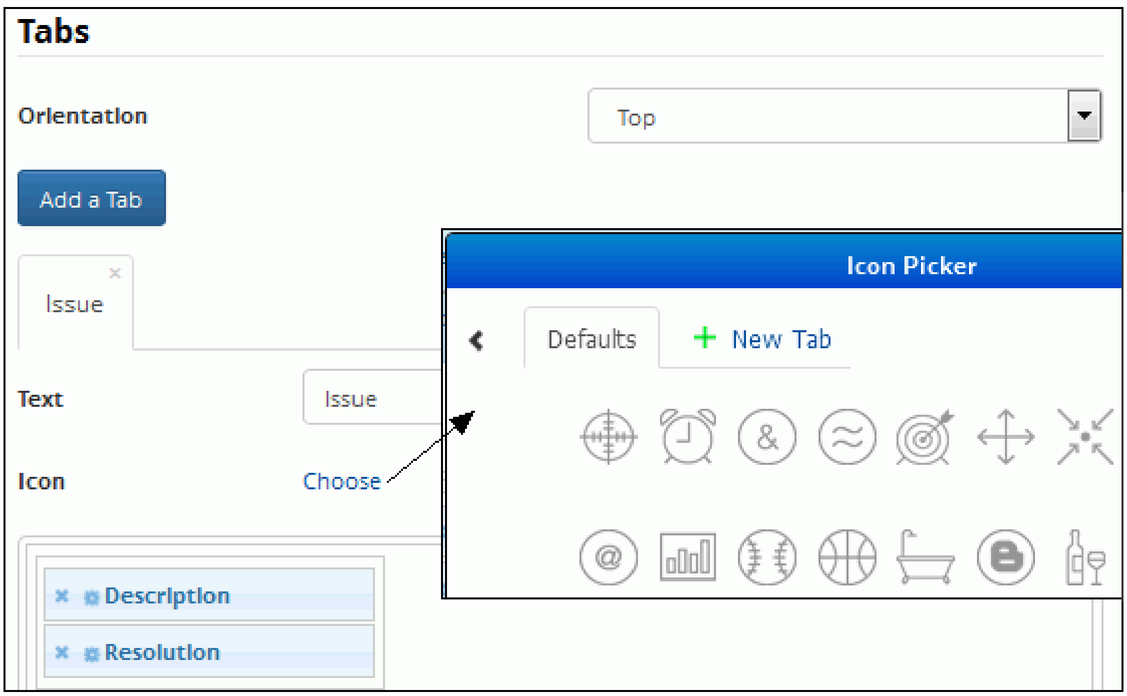


- Drag the Custom Fields field under the List Items section and then select Configure Field to display the Configure Field dialog and select the types of custom fields to include: global custom fields, additionally defined custom fields, or both. See "Configuring Fields" on page 41.

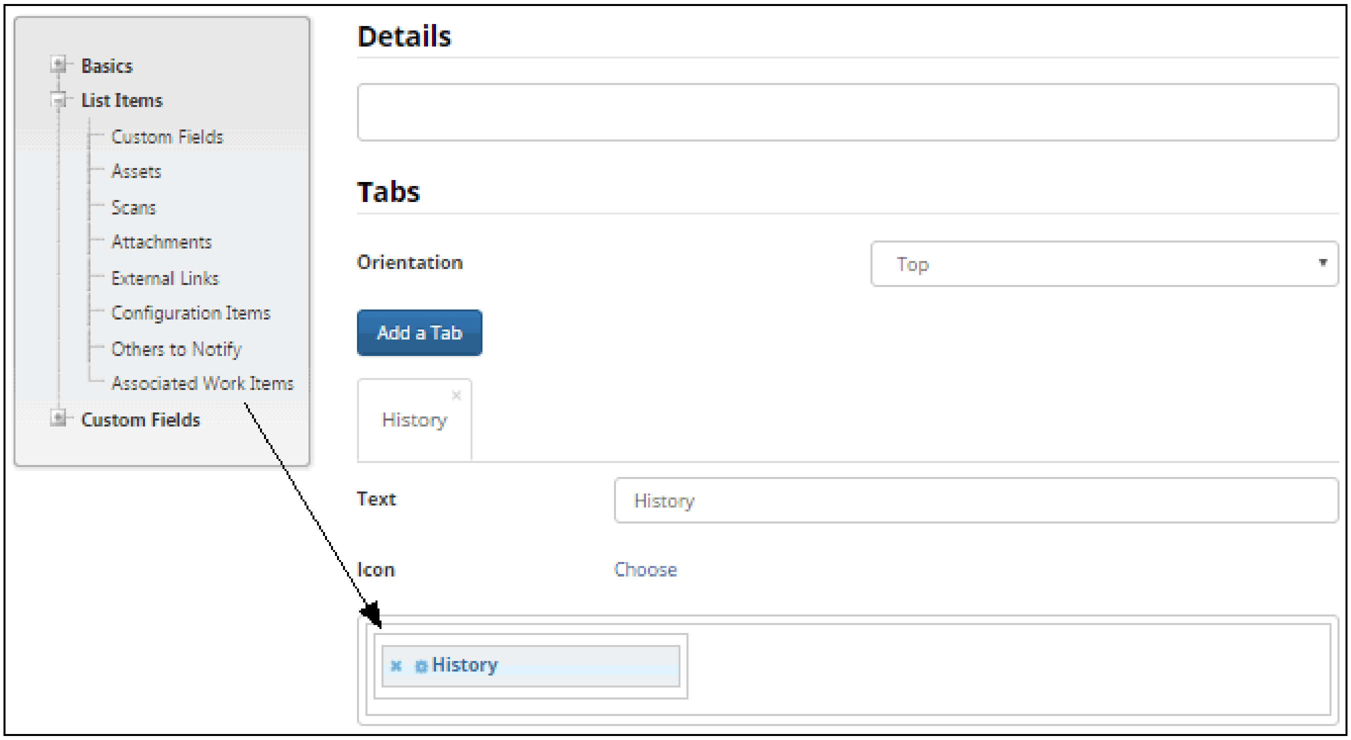


A **[Separator]** field is included for mySupport layouts; it will be blank after you drag it to the Details section or a tab. You can enter a label for it or leave it blank, and it can be used multiple times for adding blank areas to your layout. A Save Button option is included in Submit layouts; if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

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



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

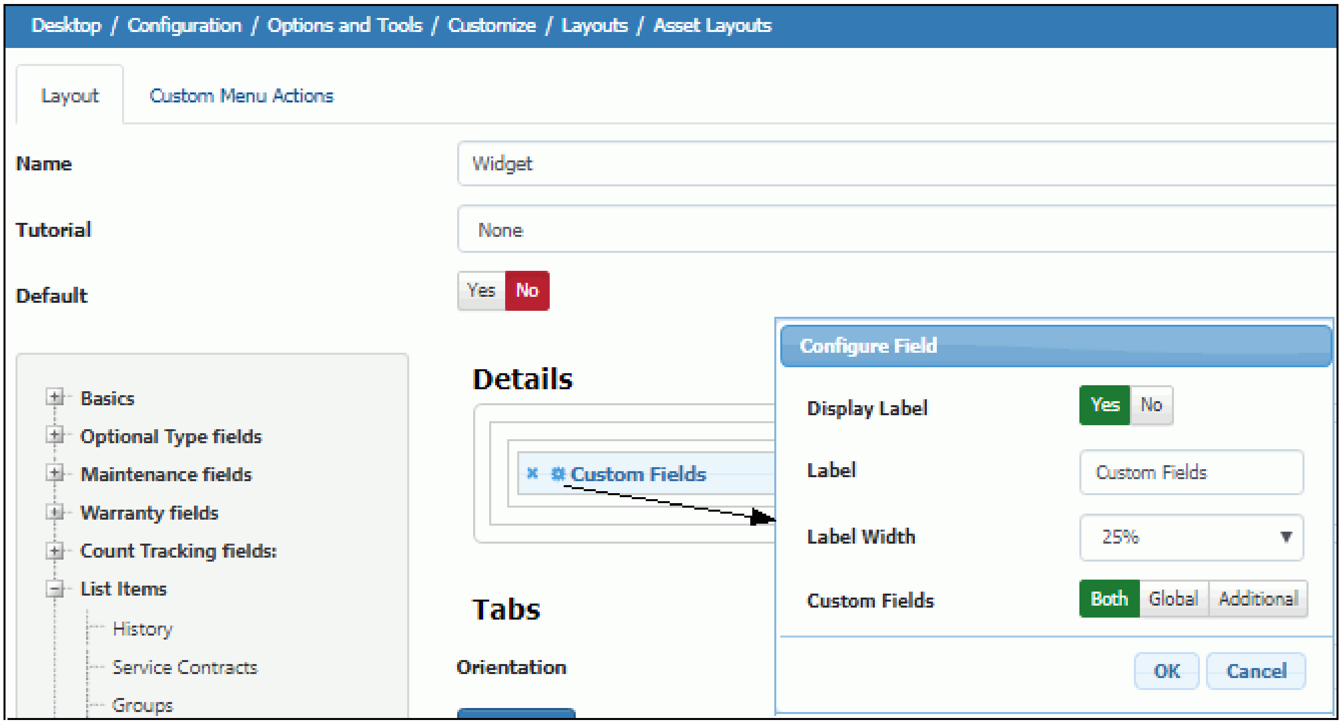


Note: The Description field is optional on mySupport incident submit layouts. The following text will be included in the Description field after submission: "Description field not included in <layout name> mySupport incident submit layout." If the layout is associated with a template, the description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

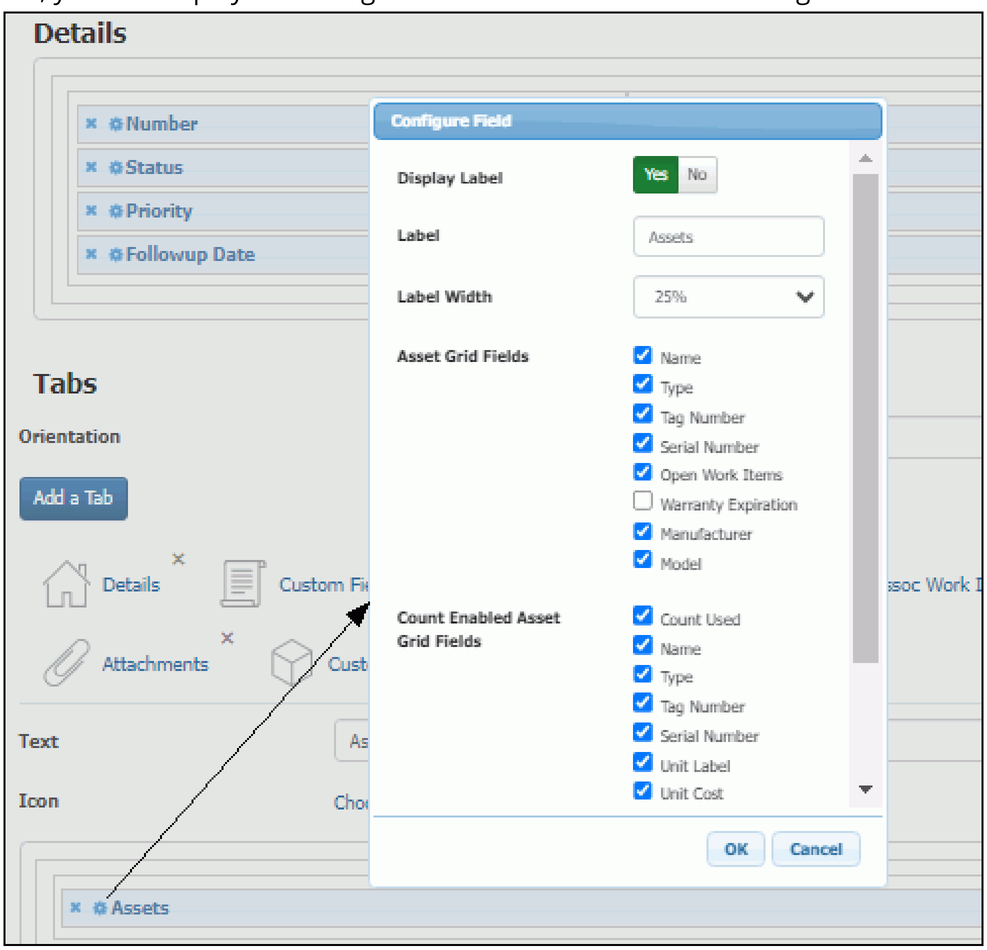
Configuring Fields

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

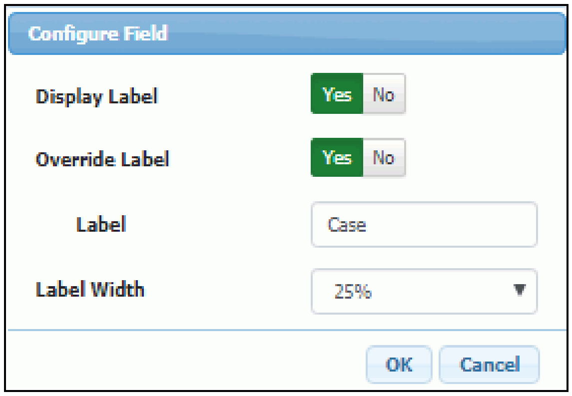
Global custom fields can be defined in the Custom Fields screen for the type of work item screen for which you're creating a layout, and additional custom fields can be defined for a category, asset type, change type, CI type, and cost center. When you drag the **Custom Fields** field under the List Items section to include all of the custom fields at once, you can control which types of custom fields to include on layouts: global custom fields, additionally defined custom fields (defined for a category, asset type, CI type, change type, or cost center), or both. Note that all custom fields that have met any conditional display conditions will be created upon mySupport work item submission regardless of whether they are included on a mySupport submission layout.



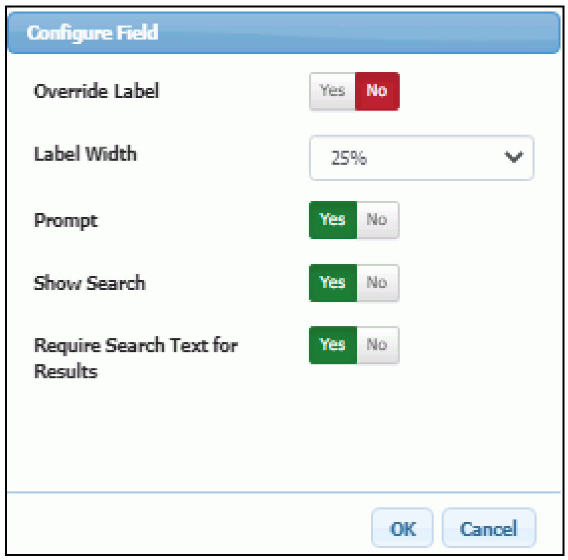
For work item layouts, you can display an asset grid for the Asset field via the Configure Field icon:



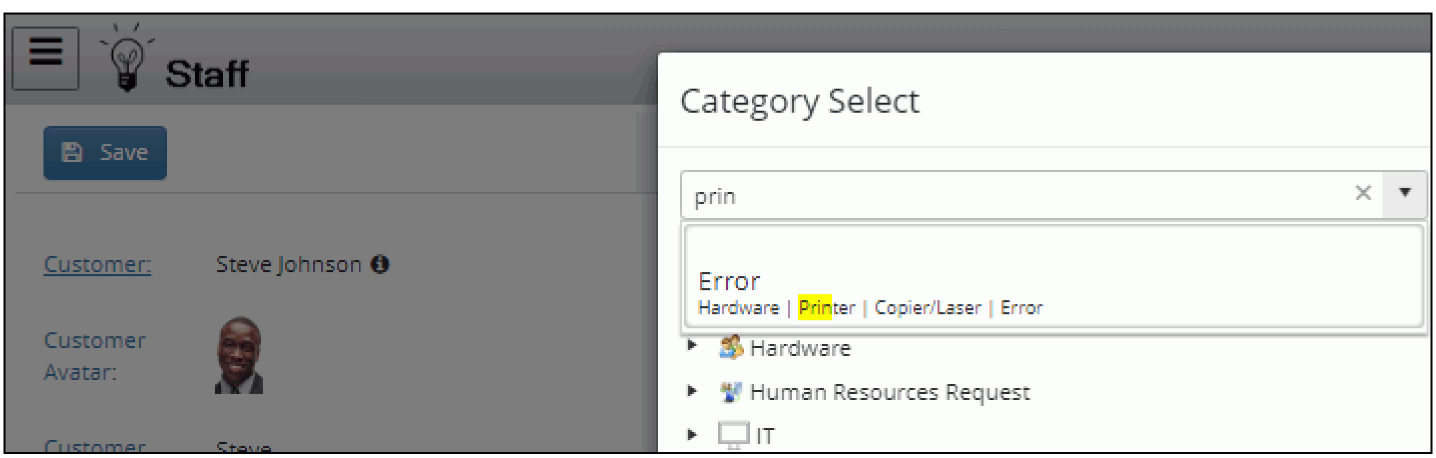
- Select Yes in the **Override Label** field to enter a field label that is different from the default. Note that this label will override any text that may be entered via the Resource Editor. See the online help for more information on the Resource Editor.



- If configuring the **Category** field:

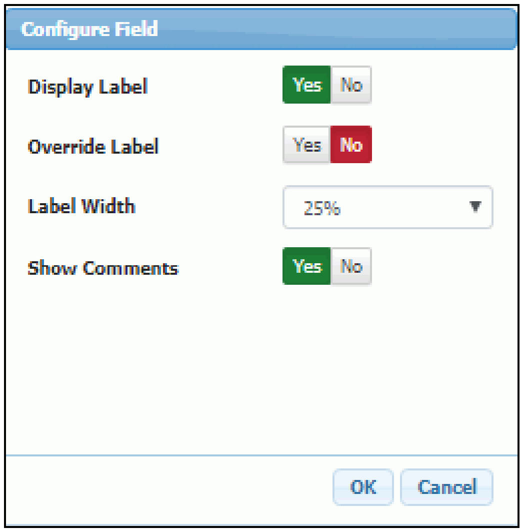


  - Select Yes in the **Prompt** field to initially display the Category Select dialog when the Incident or Change Submit screen appears.
  - Select Yes in the **Show Search** field to include a search field in the Category Select dialog.



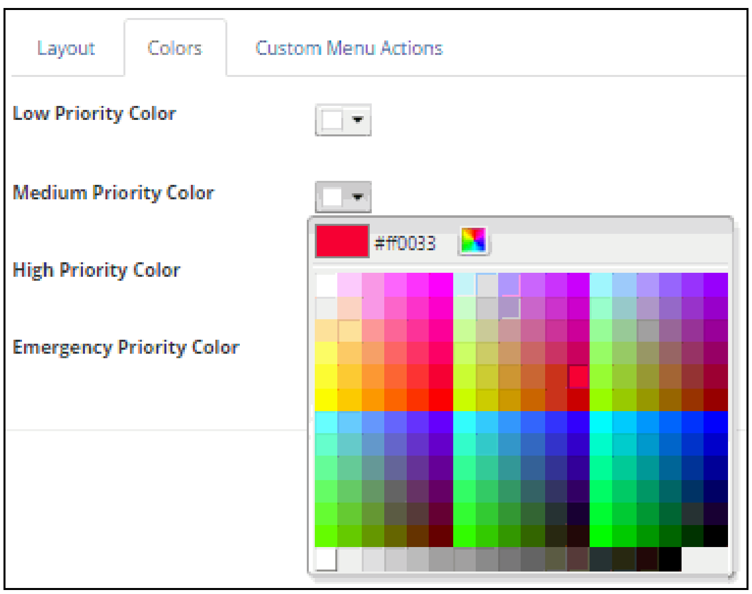
  - Select Yes in the **Require Search Text for Results** field to prevent display of the results until the user has started typing.

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



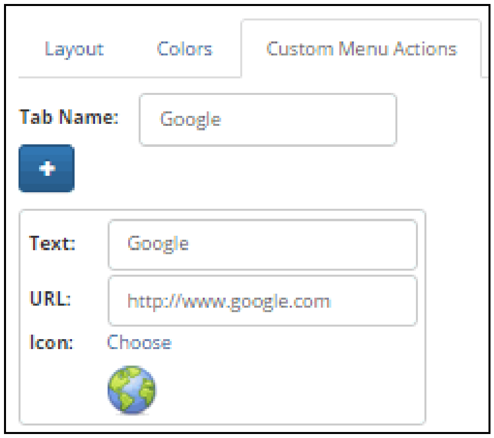
Configuring Priority-Based Background Colors

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.

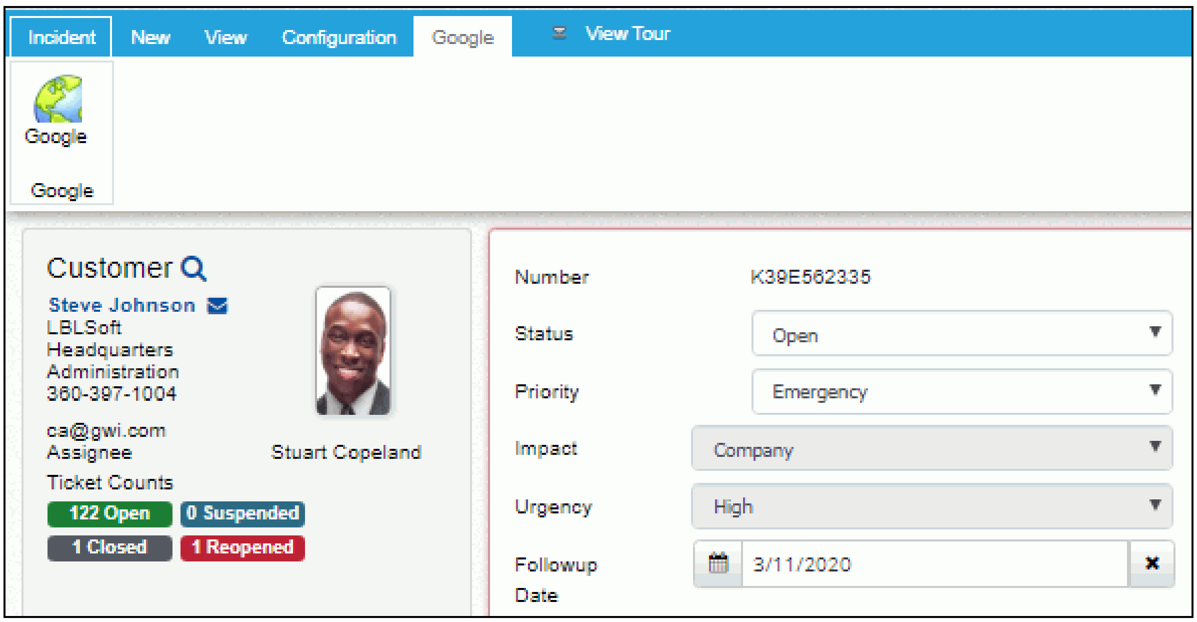


Configuring Custom Menu Actions

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



Example:



Configuring Rules and Rule Groups for Incidents

Overview

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

- Change values in the Assignee, Category, Customer, Impact, Urgency, Status, Followup Date, and Priority fields, as well as in any custom fields. An email server account and template can also be set for an incident.
- Create a related incident and apply an incident template or hierarchy template
- Send notifications via email, Desktop, or SMS
- Route via load balancing or the round robin method
- Initiate an approval cycle
- Execute a webhook for posting Incident data to a web application

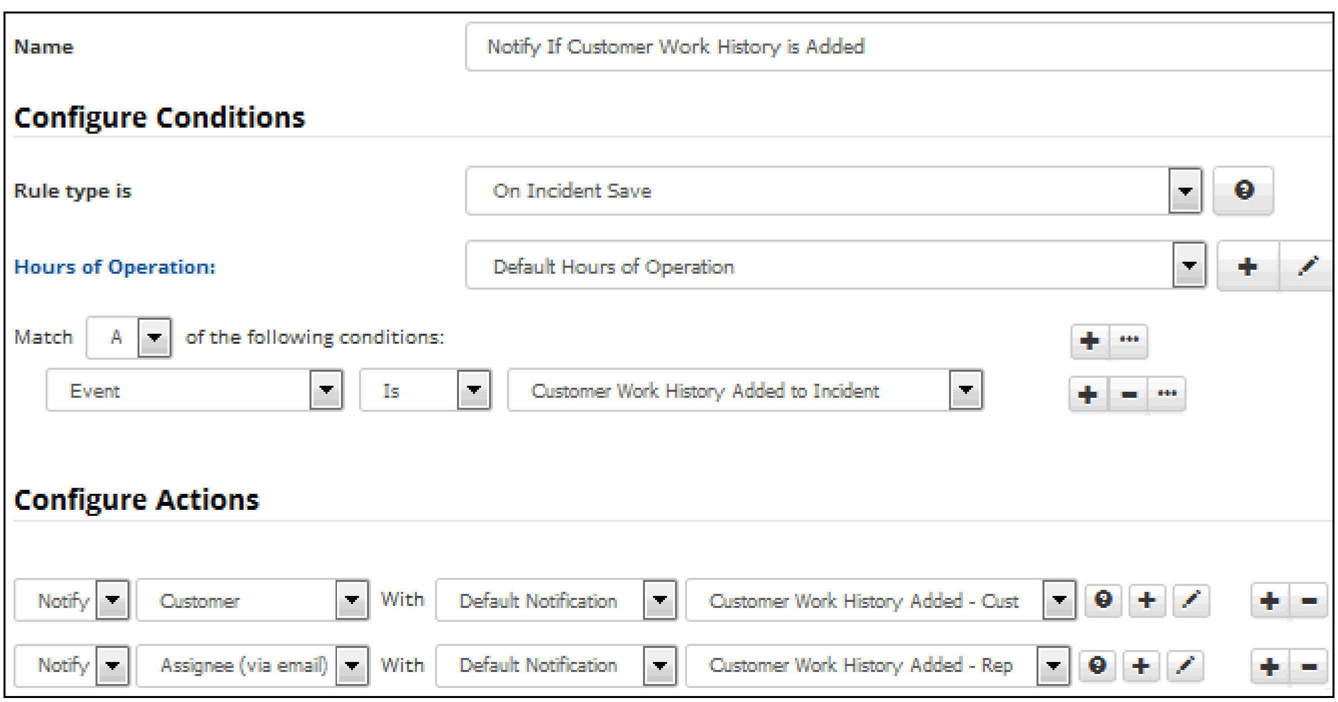
In order for a rule to be evaluated, it must be included in a **rule group**. When an incident is saved, the matching rule group is first determined. Then, all rules in that matching rule group are evaluated. If a rule's conditions are met, its actions are performed.

Rule groups are applied to incidents through customers, companies, category combinations, and incident and hierarchy templates. (If a customer profile does not have an associated rule group, the rule group associated with the customer's company will be used for the customer.) You can specify the order of precedence if multiple rule groups apply, and the rule group designated as default will be used if none are applicable. Note that rules in the associated rule group will not execute while an incident is pending approval.

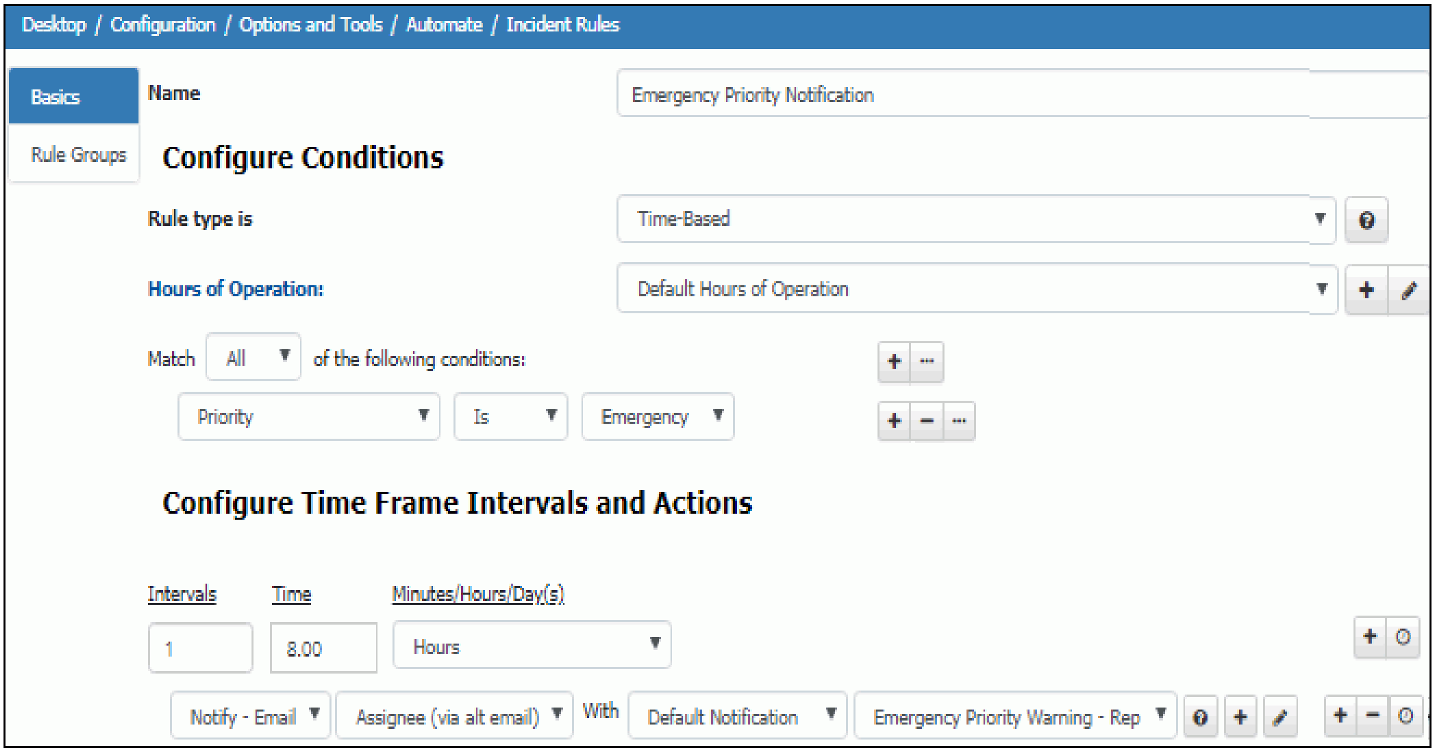
A default incident rule group will be included in iSupport on installation or upgrade. Upgrades will convert previously configured Service Level Agreement functionality into rules and rule groups. You can use the Incident Rule Groups screen to create new rule groups and assign them to customers, companies, category combinations, and incident and hierarchy templates. (You can also assign rule groups via those entry screens.) See "Creating Rule Groups" on page 59 for more information.

Rule Types

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



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

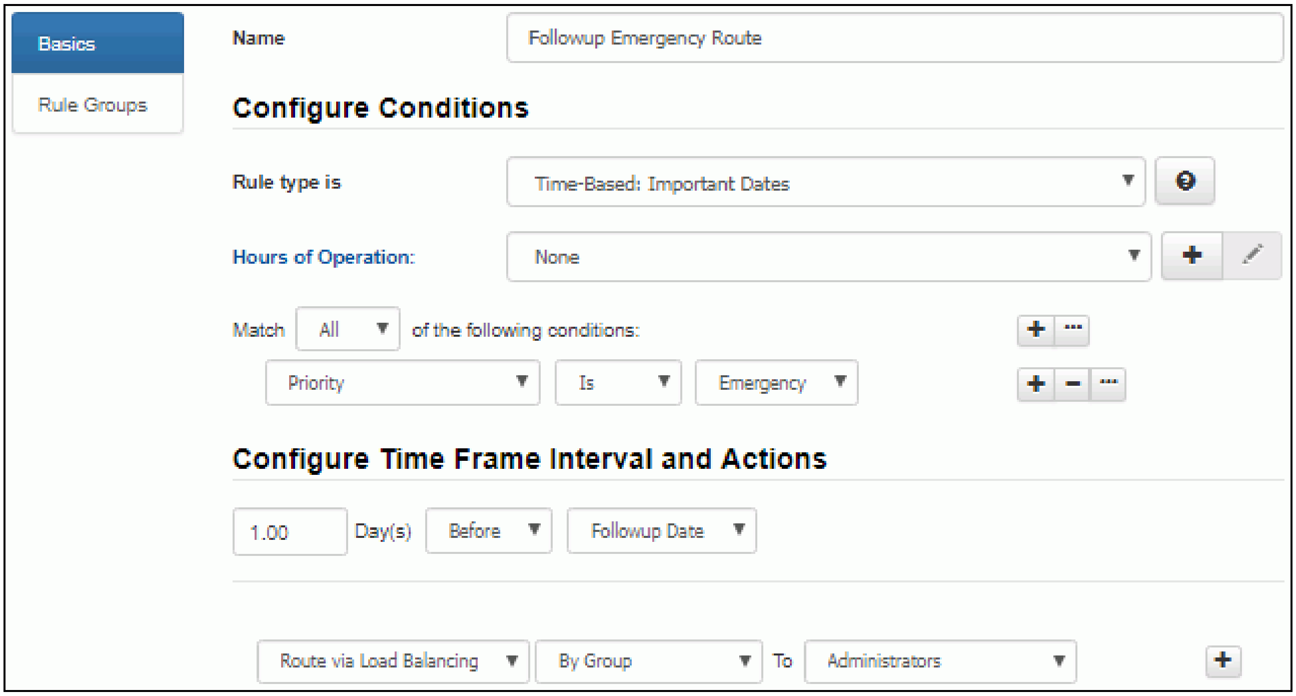


If the conditions required to meet the rule do not change before the interval time frame is reached, the agent performs the actions specified. If conditions change prior to the recorded date and time:

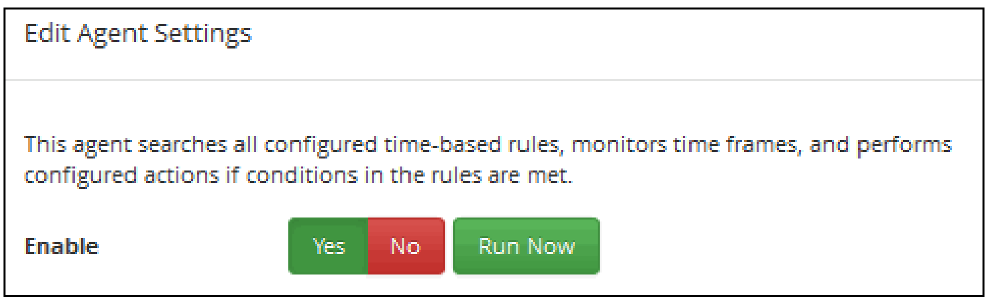
- **Time-Based** rules will clear all pending actions and if conditions are met again the time frame will restart.
- **Time-Based: Cumulative** rules will suspend all pending actions and if conditions are met again the time frame will include previous amounts of time in which conditions were met.

If a rule contains conditions with the Customer Work History Added, Work History Added to Incident, or Acknowledged events, the rule will be triggered immediately when the event occurs (even if the incident hasn't been saved). Any other changes in the incident will not be saved until you save the incident.

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



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



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

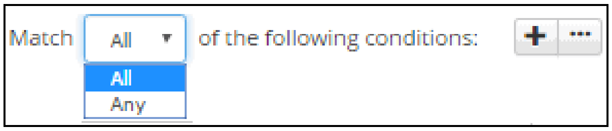
Creating Rules

Rule creation involves entering a name for the rule, selecting the type of rule, selecting one or more conditions and time frame intervals if applicable, and then selecting one or more actions to perform if those conditions are met. The type of rule will determine the fields that appear. All rules include conditions and actions; see the following sections “Configuring Conditions” on page 49 and “Configuring Actions” on page 50 for more information. See “Creating Time Frame Intervals for Time-Based Rules” on page 55 for information on configuring interval time frames and actions to perform with each set of intervals.

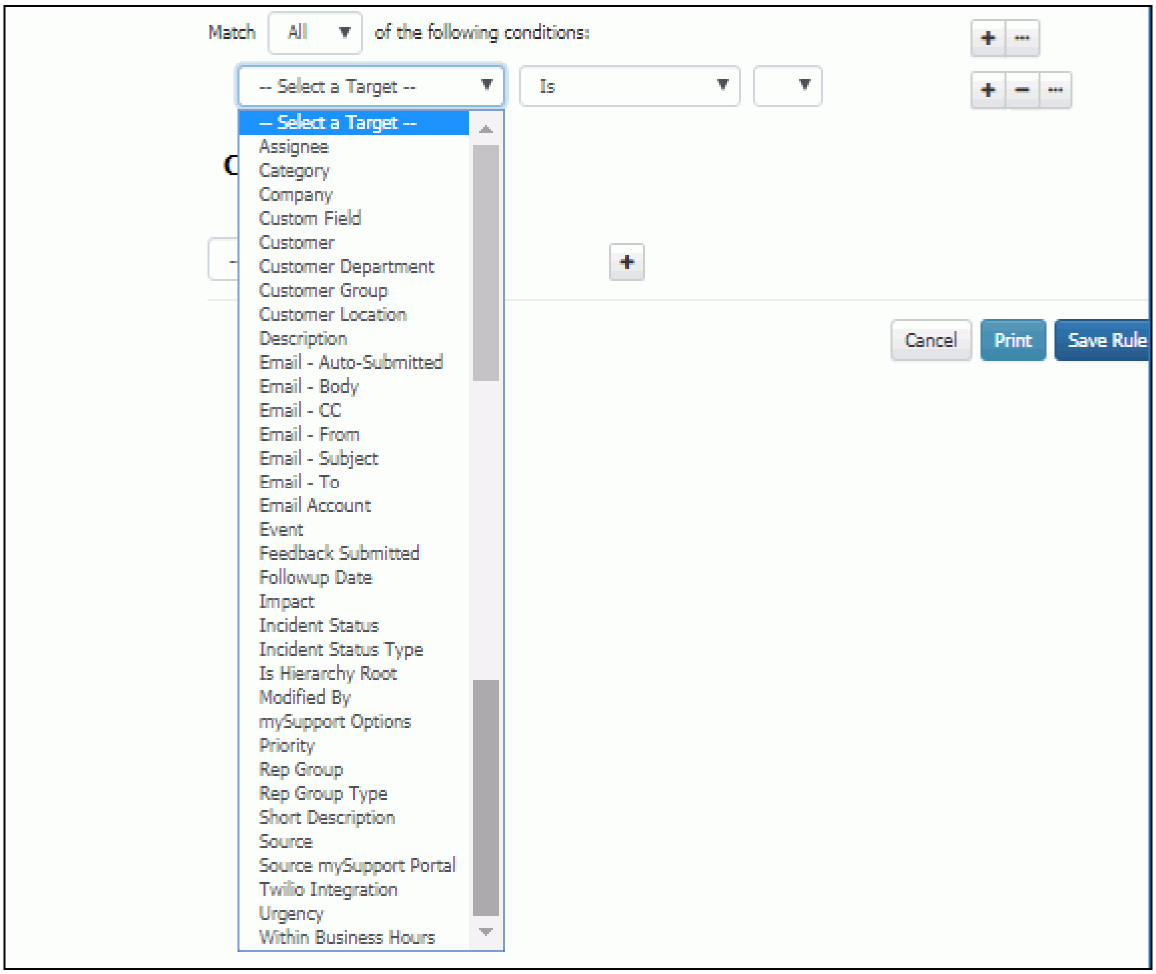
A configured **Hours of Operation** definition of 24 hours a day/seven days a week or selected date and time ranges can be used for the effective time frame for a time-based rule and for an on-save rule with a condition that includes "Within Business Hours". The default Hours of Operation definition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

Configuring Conditions

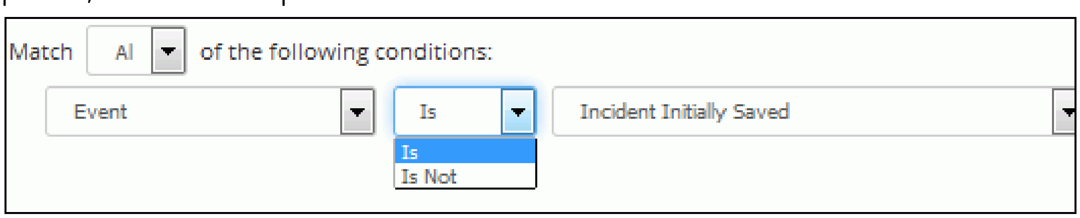
Use the first Match <All/Any> of the Following Conditions field to specify whether you want **every** configured condition in this rule to be met, or **any** configured condition in this rule to be met.



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



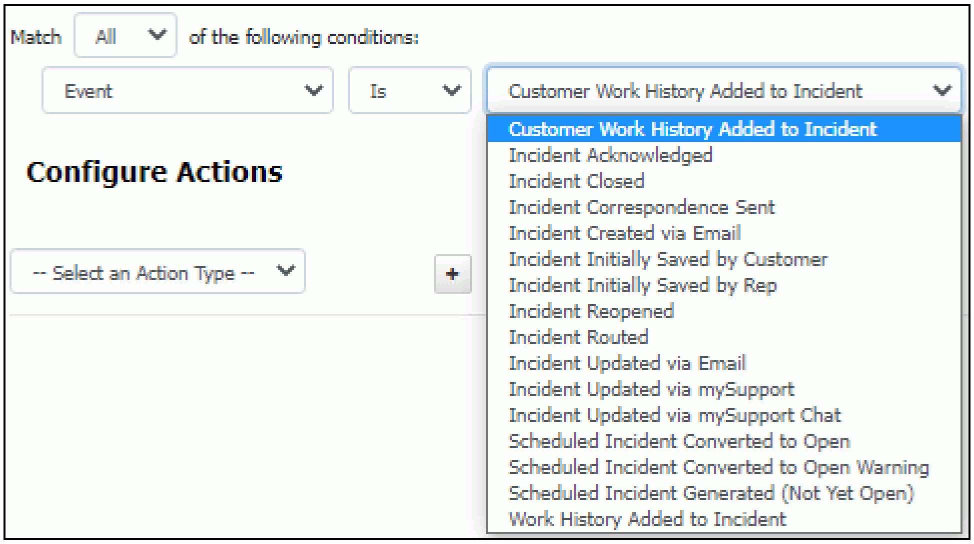
In the next dropdown, select the comparison method.



Note that:

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

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



Note: If a rule contains conditions with the Customer Work History Added, Work History Added to Incident, or Acknowledged events, the rule will be triggered immediately when the event occurs (even if the incident hasn't been saved). Conditions for all of the rules in the rule group will be evaluated and actions will be performed if conditions are met. Any other changes in the incident will not be saved until the support representative saves the incident.

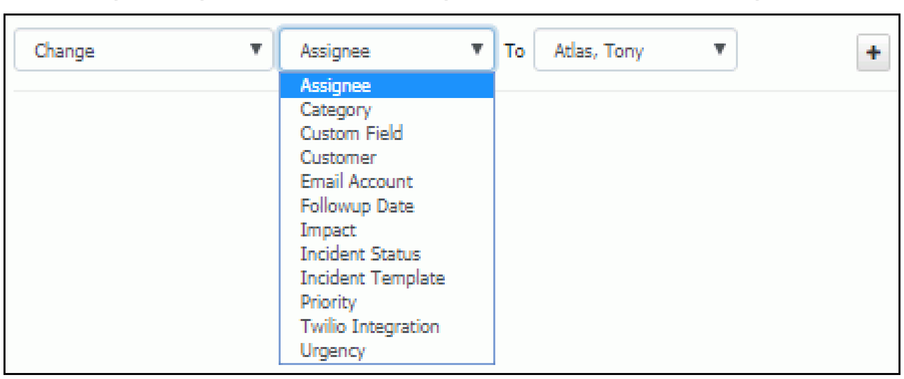
Select ✚ Add Condition if you wish to include another condition. You can use the ⋯ Add Condition Group option to put a set of conditions to be evaluated together in a group.

Configuring Actions

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

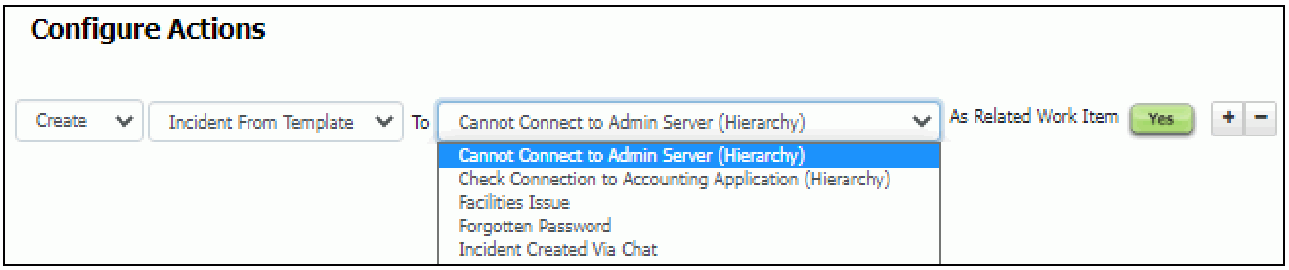
You can:

- **Change a field** by selecting Change, the field to change, and the value to change it to.



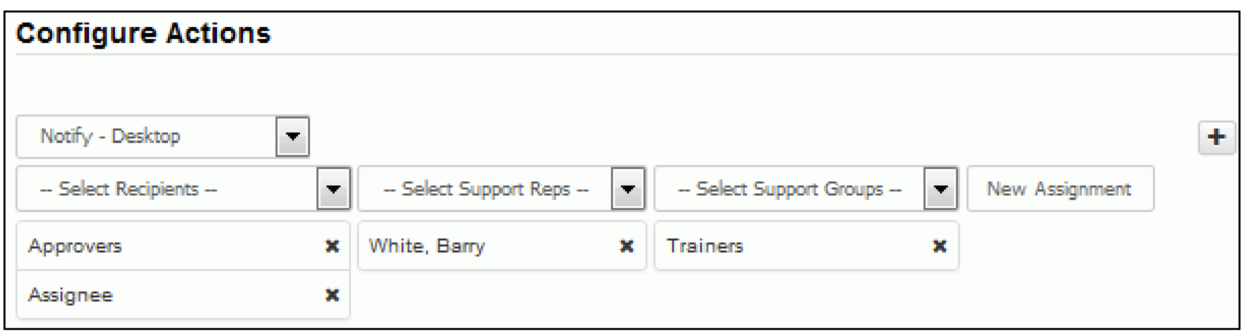
- **Execute a configured webhook** for posting Incident data to a web application. See "Configuring Webhooks" on page 116 for more information.

- **Create an incident** and apply an incident template or hierarchy template by selecting Create, Incident From Template, the template to apply. In the As Related Work Item field, select Yes to create the work item as related to work items created from the selected template, or No to create the work item as separate from work items created from the selected template.

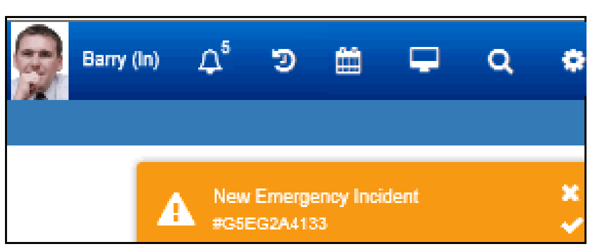


You can select the default or a custom notification. If possible the notification options will include one of iSupport's default notifications that match the condition or recipient.

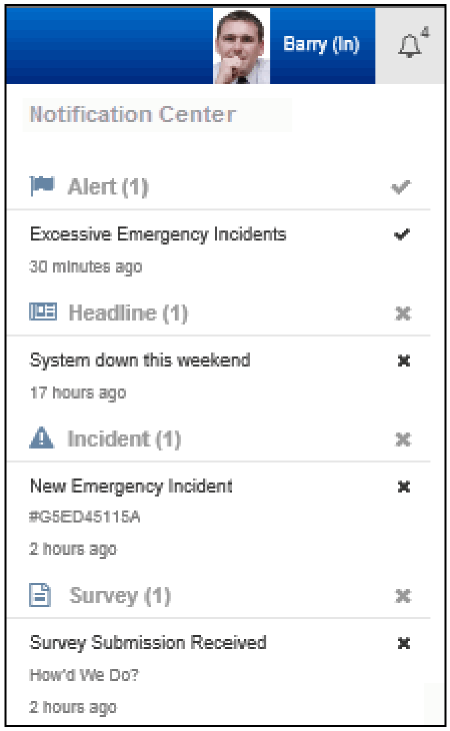
- The **Include Feedback field** appears if the Incident Feedback feature is enabled and configured (via the Incident Basics screen) and Customer is selected as the notification recipient. This feature includes a question with two response choice image links at the bottom of an incident notification; when a customer receives the email and clicks one of the responses, configured submission text will appear on a page on the mySupport portal, and the feedback question and response will be included in the Feedback field on the incident. (Note that this feature is intended for HTML-type mail delivery.) Select Yes in the Include Feedback field to include the configured question and responses at the bottom of the notification sent by the rule.
- **Send a notification** via desktop notification, email, or SMS.
  - **Desktop notification:** To display an entry in the  Notification list on the Desktop, select Notify - Desktop, one or more recipients, and the text to appear in the Desktop Notification dropdown and/or popup.



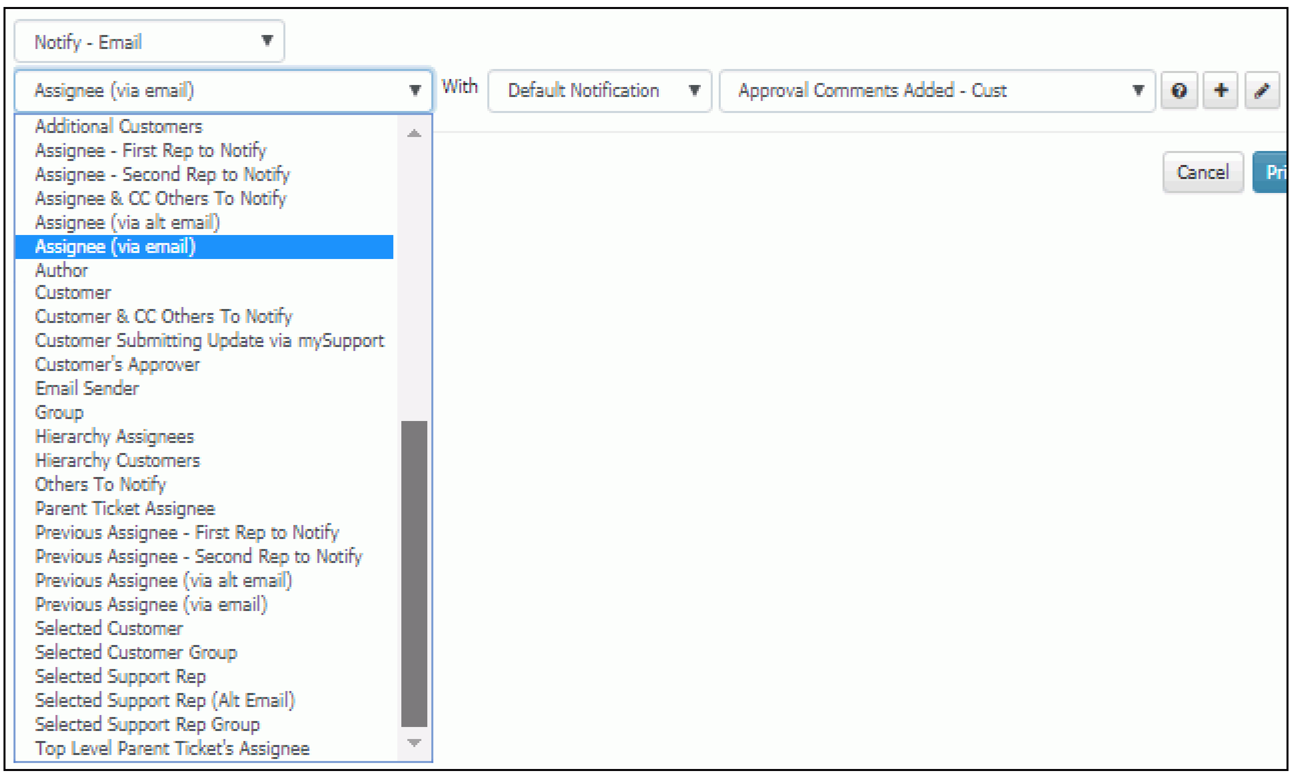
Options on the Desktop Notifications tab in Preferences (accessed by clicking the avatar/login) determine whether or not an entry will appear as a popup or list entry. An example of a desktop notification popup is shown below:



An example of the dropdown is shown below.



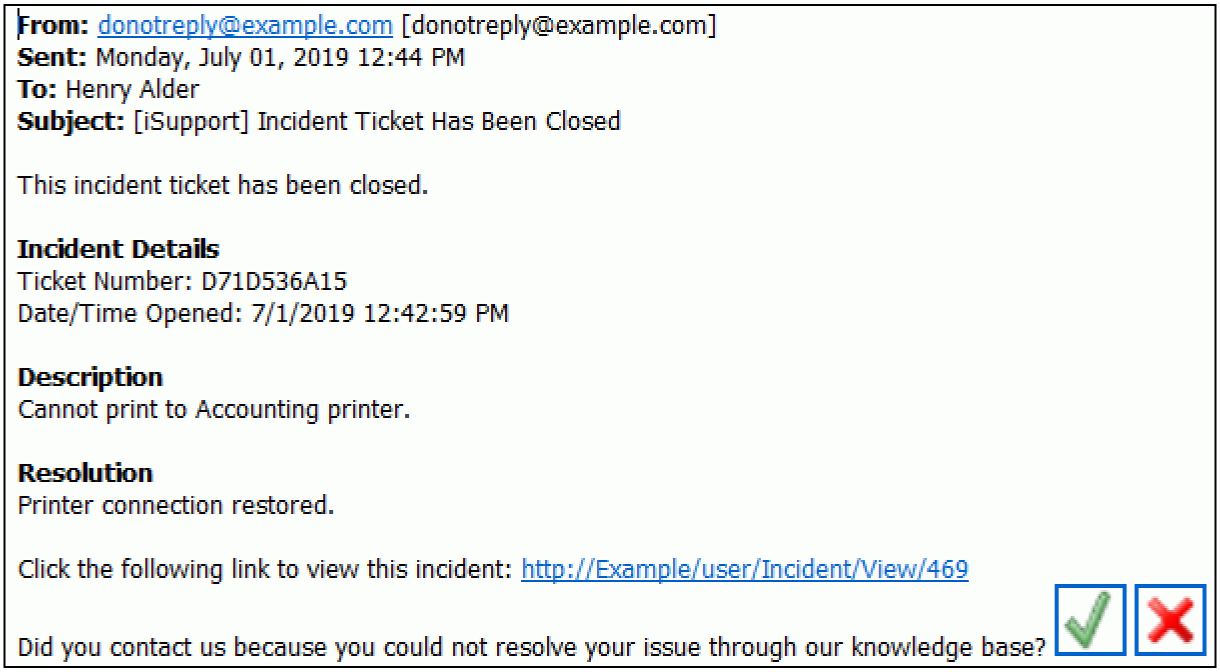
- **Email:** If sending a notification via email, select Notify - Email, the recipient, and the notification to be sent.



You can select the default or a custom notification; select Show Notification to display the contents of a selected notification. If possible the notification options will include one of iSupport's default notifications that match the condition or recipient. Use the + Create New and View/Edit options to access the Custom Notification screen; see "Customizing and Viewing Event Notification Content" on page 62 for more information.

Adding Feedback

If the Feedback feature is configured in Feature Basics, you can include response choice image links at the bottom of an incident notification.



From: donotreply@example.com [donotreply@example.com]
Sent: Monday, July 01, 2019 12:44 PM
To: Henry Alder
Subject: [iSupport] Incident Ticket Has Been Closed

This incident ticket has been closed.

Incident Details
Ticket Number: D71D536A15
Date/Time Opened: 7/1/2019 12:42:59 PM

Description
Cannot print to Accounting printer.

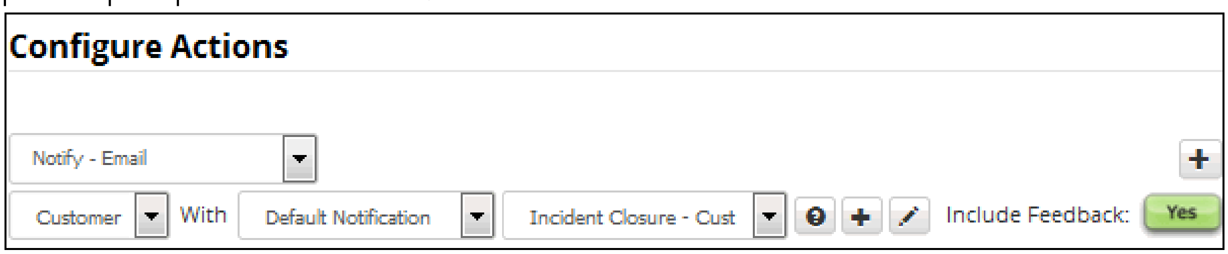
Resolution
Printer connection restored.

Click the following link to view this incident: http://Example/user/Incident/View/469

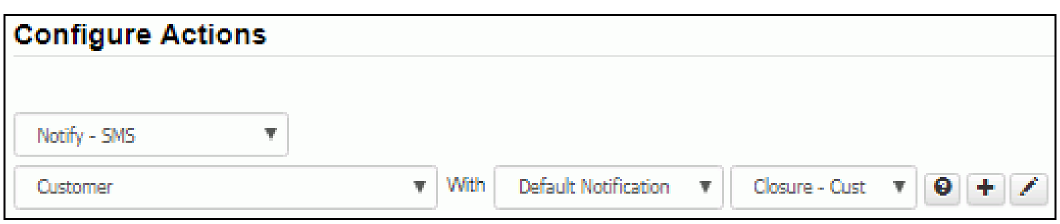
Did you contact us because you could not resolve your issue through our knowledge base?

When a customer receives the email and clicks one of the responses, configured submission text will appear on a page on the mySupport portal, and the feedback question and response will be included in the Feedback field on the incident. Note that this feature is intended for HTML-type mail delivery.

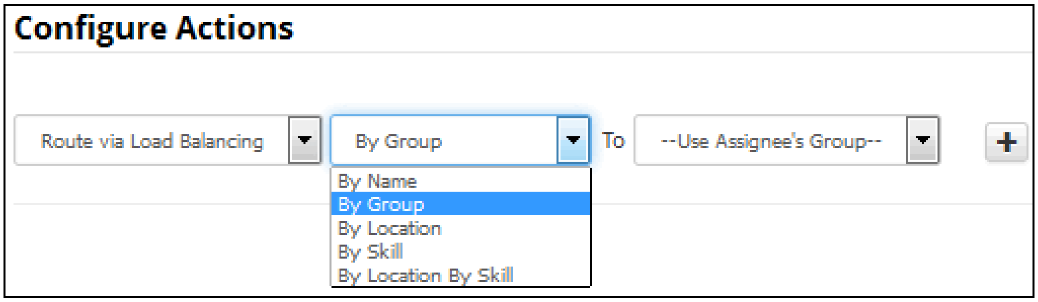
The Include Feedback field will appear if the Feedback feature is configured; select Yes to include the specified prompt in the notification.



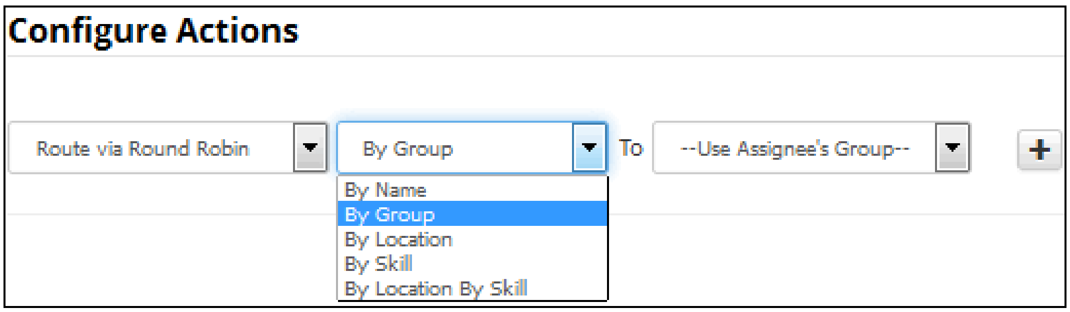
- **SMS:** To send an SMS notification, select Notify - SMS, the recipient, and the notification to be sent. The contents of the SMS Text field in the custom notification will be sent; if that field is blank or if it is a default notification, the contents of the Subject field will be used. If sending to a support representative, the message will be sent to the following in their Support Representative record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the address in the Alt Email field; if that is unavailable, to the address in the Email field. If sending to a customer, the message will be sent to the following in their Customer Profile record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the SMS email from mySupport (email to text); if that is unavailable, the address in the Email field. See "Configuring Twilio Integrations" on page 65 for more information on Twilio integration.



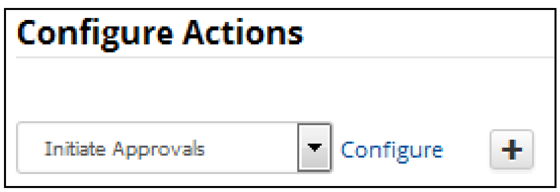
- **Route the Incident record via load balancing** by selecting Route via Load Balancing, the route method, and the recipient if applicable. Load-balanced routing is enabled on the Incident Management tab in the Feature Basics screen.



- **Route the Incident record via round robin** by selecting Route via Round Robin, the route method, and the recipient if applicable. Round robin routing is enabled on the Incident Management tab in the Feature Basics screen.

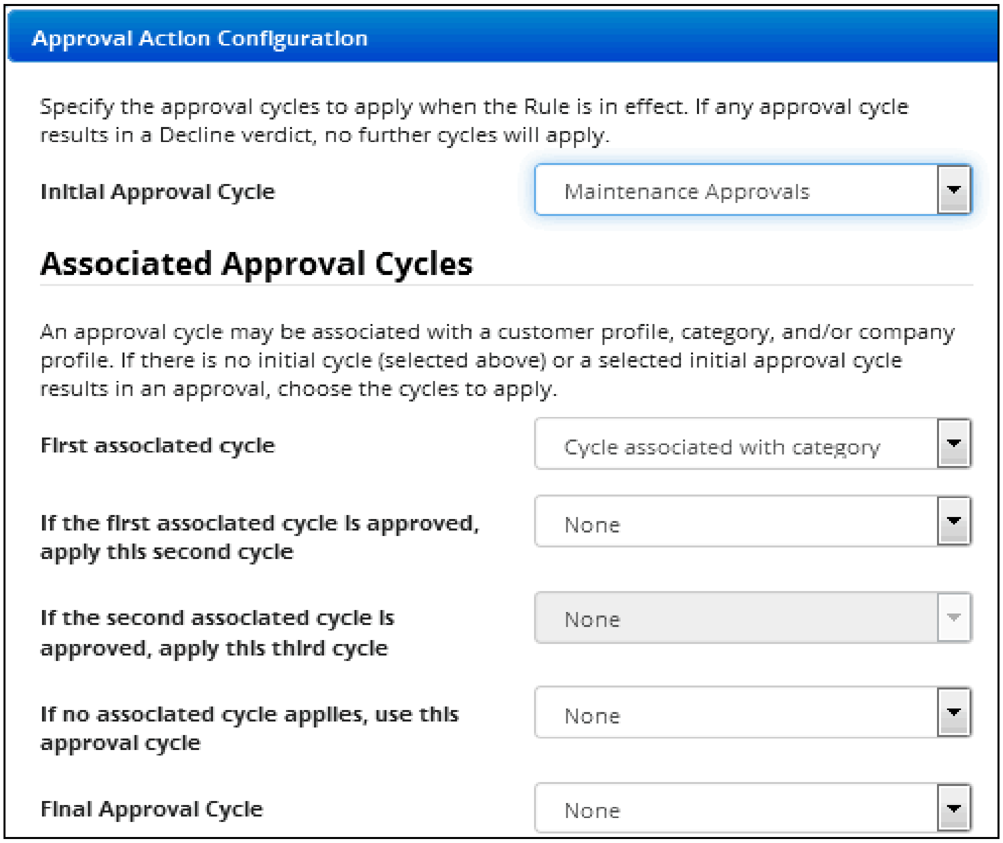


- **Initiate approvals** by selecting Initiate Approvals and clicking the Configure link. Approval cycles are enabled on the Basics tab in the Core Settings | Global Settings screen.



iSupport's Approval feature requires an incident to be approved by designated approvers before it can be closed. The rule in effect can initiate one or more approval cycles, and approval cycles can be associated with customers, companies, categories, and incident and hierarchy templates.

The Approvals dialog appears for you to specify the initial approval cycle, any additional cycles to apply if there is no initial approval cycle or the initial cycle results in an approval, and the final cycle to apply. Note that any changes to these settings will not affect current incidents pending approval, and rules in the associated rule group will not execute while an incident is pending approval.



Initial Approval Cycle - Select the predefined approval cycle to apply when the rule group is in effect for the incident.

First Associated Cycle - Select the approval cycle to apply if there is no initial approval cycle or the cycle specified in the Initial Approval Cycle field results in an approval.

If the First Associated Cycle is Approved, Apply This Second Cycle - This field appears if an associated cycle was selected in the previous field. Select the approval cycle to apply if the cycle specified in the First Associated Cycle field results in an approval.

If the Second Associated Cycle is Approved, Apply This Third Cycle - This field appears if an associated cycle was selected in the previous field. Select the approval cycle to apply if the cycle specified in the previous field results in an approval.

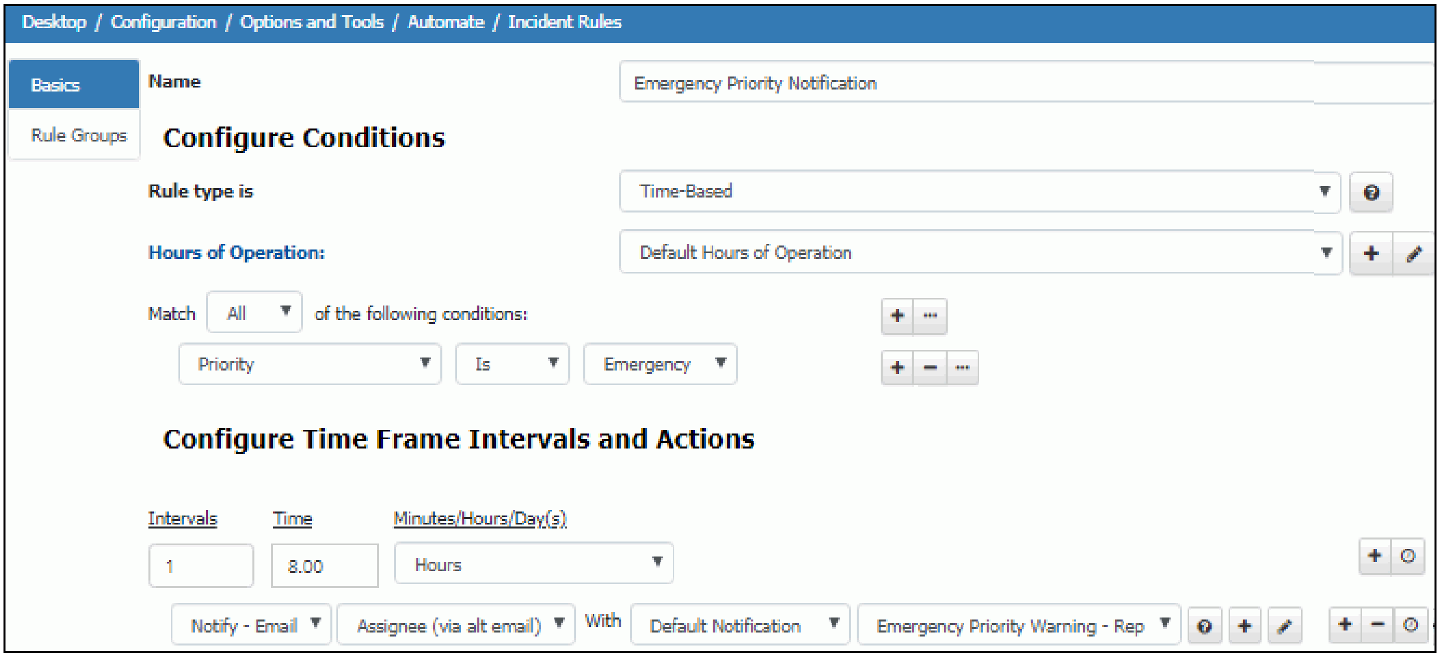
If No Associated Cycle Applies, Use This Approval Cycle - This field appears if Cycle Associated With Customer, Cycle Associated With Category, Cycle Associated With Company, or Cycle Associated With Template was selected in one or more of the previous three fields. Select the predefined approval cycle to apply if there are no approval cycles associated with the customer, customer's company, template, or categorization of the incident or change.

Final Approval Cycle - Select the predefined approval cycle to apply after all previously applied cycles result in an approval.

Creating Time Frame Intervals for Time-Based Rules

Time-Based and Time-Based: Cumulative Rules

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

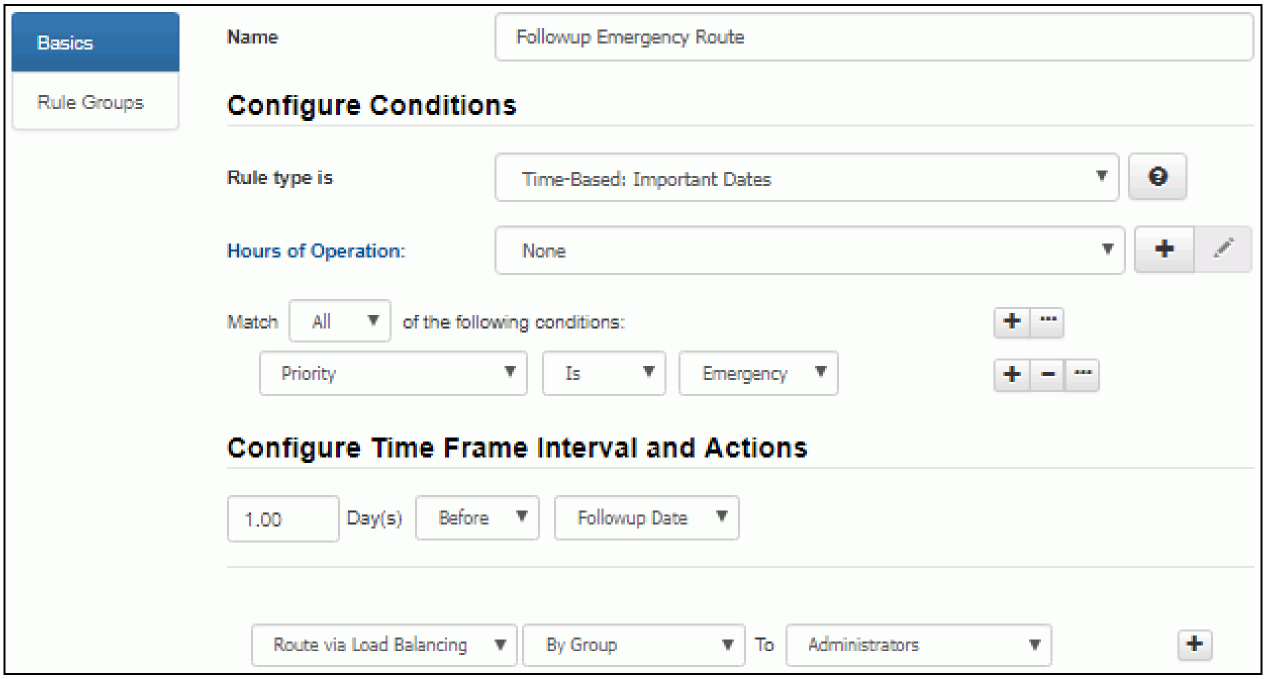


In the Configure Time Frame Intervals and Actions section, use the Intervals field to specify the number of times a time frame should be established and monitored, and use the Time and Minutes/Hours/Day(s) field to specify the amount and unit of time (in minutes, hours, or days) in the time frame. *Note that the Day(s) option is calculated with one day equal to 24 business hours.* Use the dropdowns in the indented actions line to specify the actions to perform if conditions are met for that interval time frame. In the example above, the incident will be monitored for eight hours after initial save; if the priority remains at Emergency for the entire eight hours, the Emergency Priority Warning - Rep notification will be sent to the assignee via email.

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

Time-Based: Important Date Rules

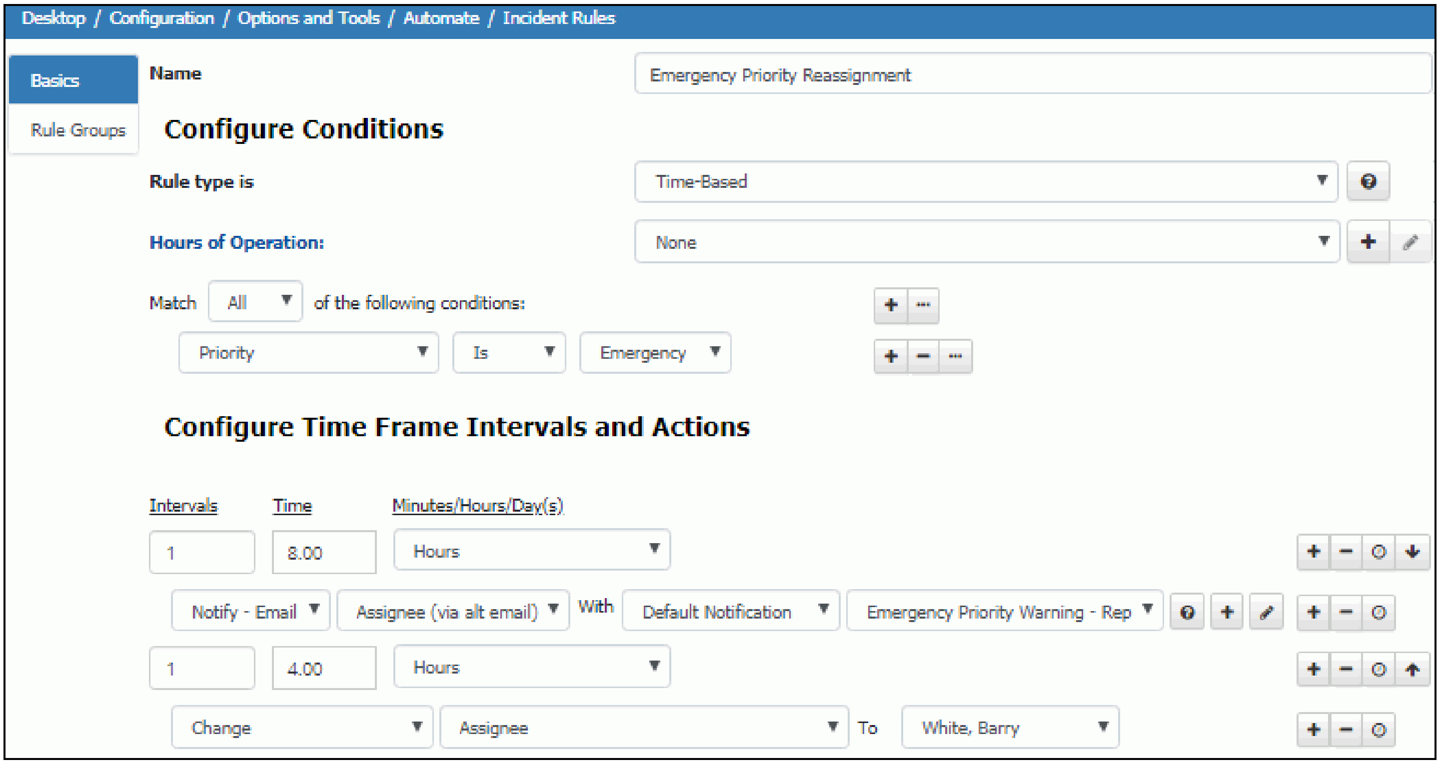
A Time-Based: Followup Date rule will display a field for entering a number of days and a Before/After dropdown; the specified action(s) will be performed when the defined number of days before or after the incident's followup date occurs.



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

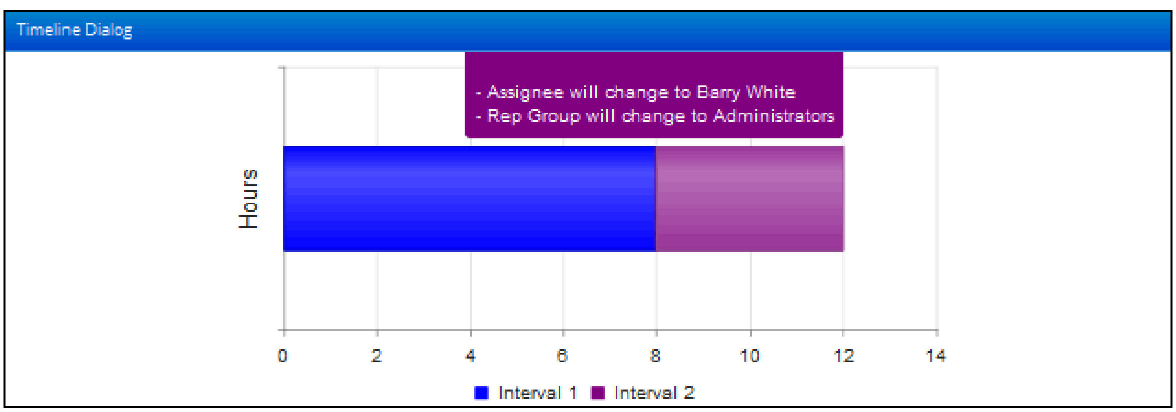
Configuring Multiple Time Frame Intervals

You can use the Add Interval option to add another interval time frame set and actions to perform if conditions are met for that interval time frame. The Move Down and Move Up options will appear for changing the order in which the interval time frames will be evaluated. In the example below, the incident will be monitored for an eight hour time frame and if the priority remains at Emergency for the entire eight hours, the Emergency Priority Warning - Rep notification will be sent to the assignee. The incident will then be monitored for an additional four hour time frame and if the priority remains at Emergency for the entire four hours, the incident will be reassigned to the support representative Barry White.



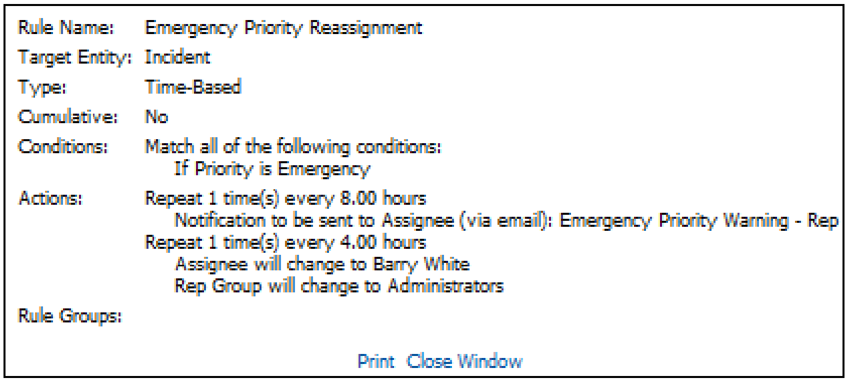
Displaying a Timeline for Configured Time Frame Intervals

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



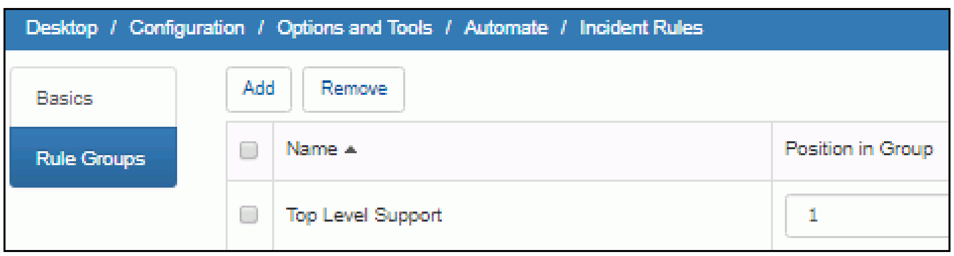
Printing a Rule

Click the Print button to display a summary of your entries; you can click the Print link in the dialog to send the information to the printer.



Associating Rules With Rule Groups

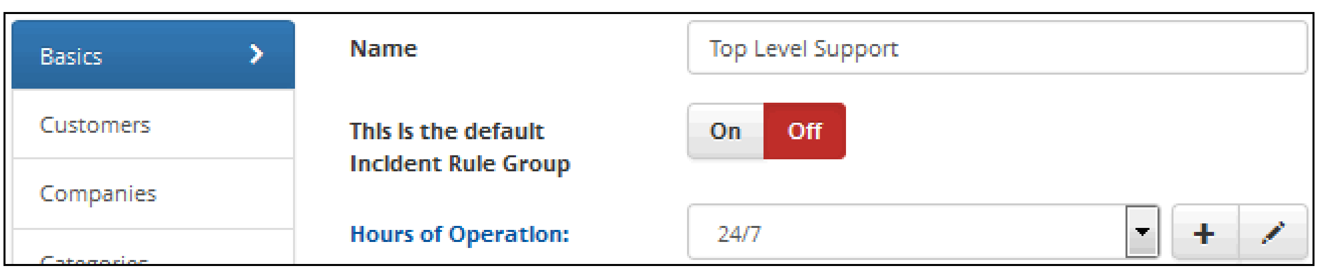
After creating a rule, you'll need to include it in a rule group. You can do this via the Rule Group tab in the Rules screen, or via the Rule Group screen. On the Rule Groups tab, click the Add link. Rule groups configured via the Rule Group screen appear; select the applicable groups and click OK. The rule group displays along with its position as shown below:



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

Creating Rule Groups

Click the Create link in the Incident Rule Groups list screen to create a rule group that can be used as default and/or applied to customers, companies, categories, and incident and hierarchy templates.



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

This is the Default Incident Rule Group - Select this checkbox to designate the rule group as the one to apply if no rule group is associated with the categorization, incident or hierarchy template, or customer associated with an incident.

More than one rule group may apply to an incident; if an incident or hierarchy template selected for the incident has a rule group, it will override any other rule group that may apply. Use the Winner if Both Customer and Category Rule

Groups are Being Used field in the Incident Basics screen to specify what is to take precedence if an incident's customer and categorization both have a rule group.

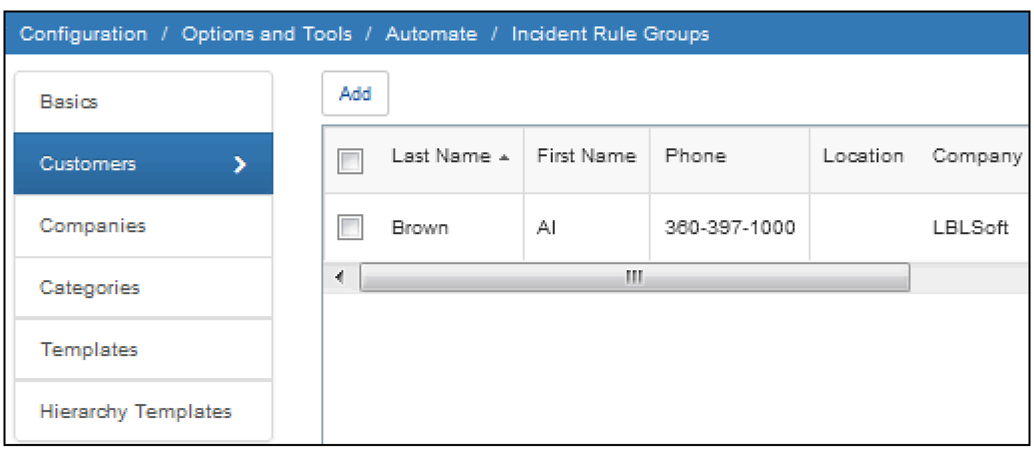
Default Hours of Operation - Select the Hours of Operation definition that will apply if no definition is selected for a time-based rule or for an on-save rule with a condition that includes "Within Business Hours" in the rule group. Use the Create New and View/Edit options to access the Hours of Operation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

Adding Rules

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

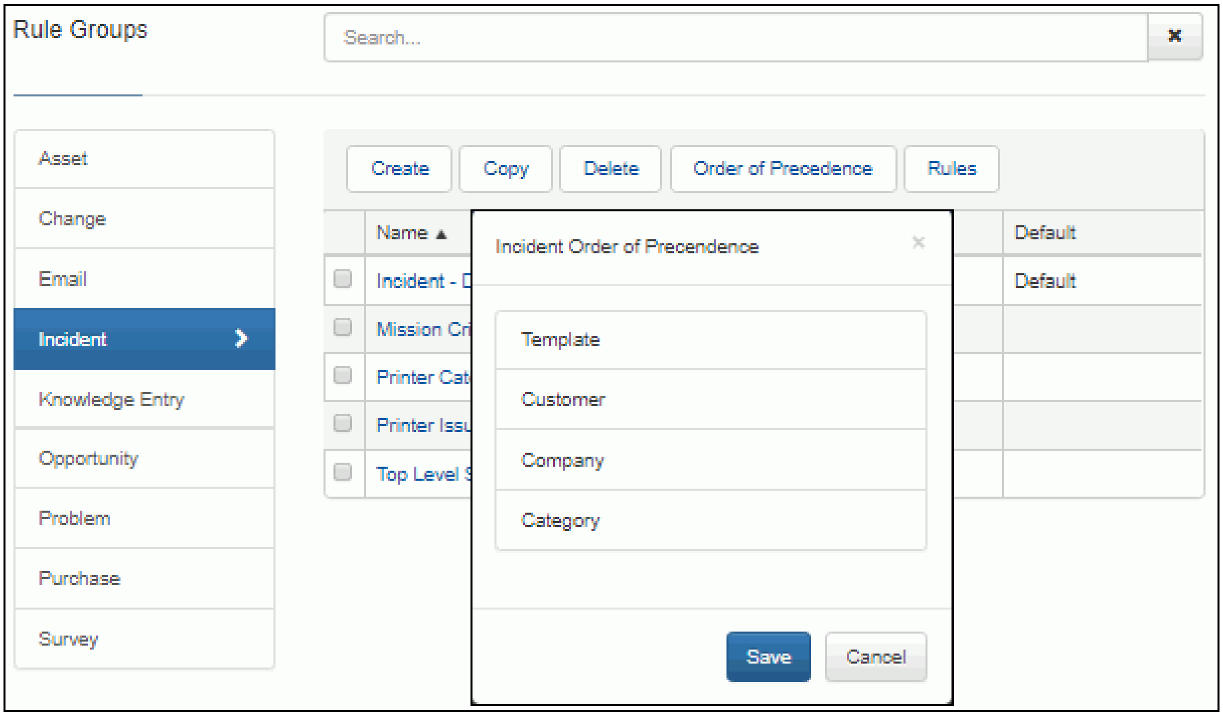
Assigning a Rule Group

Use the Add link on the Customers, Companies, Categories, Templates, and Hierarchy Templates tabs to associate the rule group with one or more customers, companies, categories, templates, and hierarchy templates. You can also do this via the Customer Profile, Company, Category, Incident Template, and Hierarchy Template screens.



Setting the Rule Group Order of Precedence

Use the Order of Precedence button in the Rule Groups list screen to designate which should take precedence if a rule group is associated with a template, customer, company, and/or category in effect for an incident.



Printing the Rule Group Summary

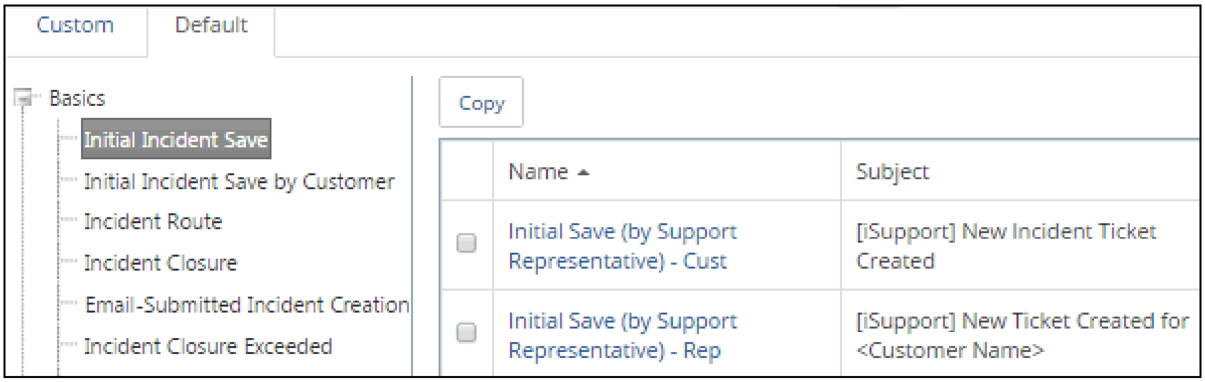
Click the Print button to display a summary of your saved entries; you can click the Print link in the dialog to send the information to the printer.

Customizing and Viewing Event Notification Content

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

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

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



About Recipients

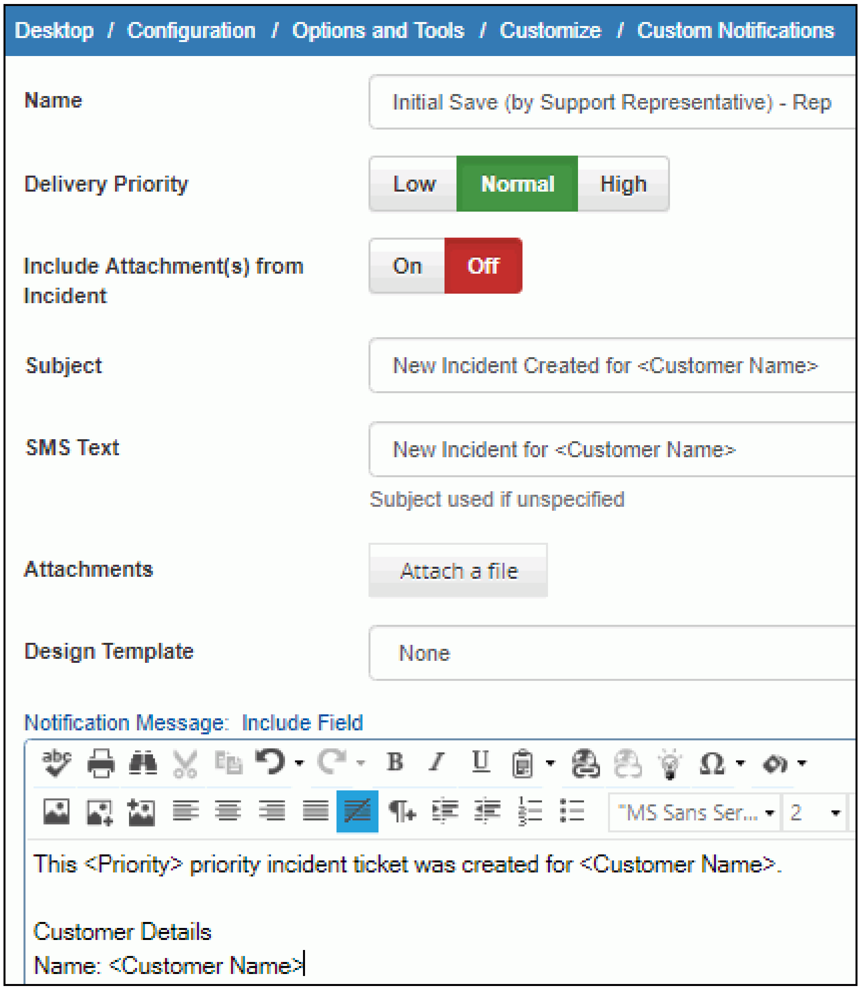
Recipients for default notifications can include both support representatives and customers, and the default notification text is different for each. Support representative notifications (designated as "Rep") typically contain customer details, the priority, the assignee, the URL to Desktop incident,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

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

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

Creating a Custom Notification

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



Name - Enter a name for the custom notification.

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

Design Template - If desired, select the design template with the elements (text and images) to appear around the body of the correspondence template and support representative signature (if applicable). You can select the Create New or View/Edit options to access the Design Template screen; see "Configuring Design Templates" on page 64 for more information.

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

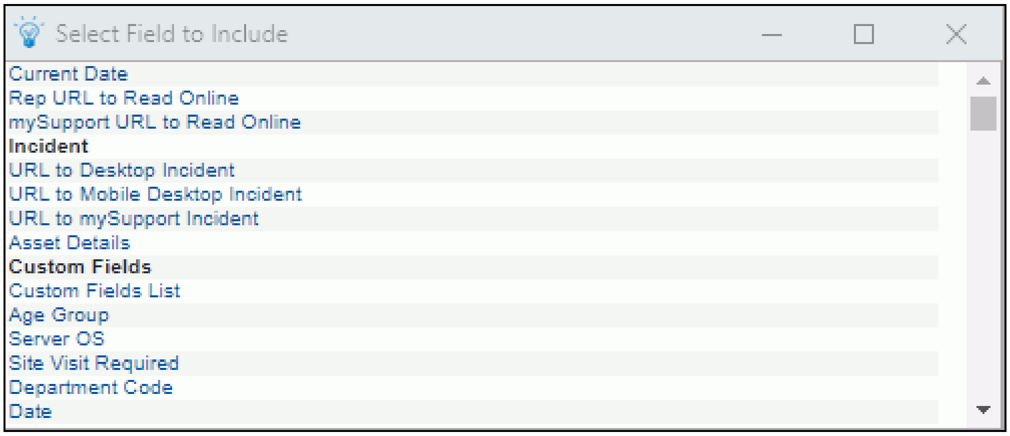
If sending to a support representative, the message will be sent to the following in their Support Representative record: if Twilio integration is configured, the number in the Mobile field; if Twilio is not configured, the address in the Alt Email field; if that is unavailable, the address in the Email field. See "Configuring Twilio Integrations" on page 65 for more information.

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

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

On the Body tab, enter the body of the email notification. You can select the Notification Message link to display a larger window for entry. Use the Include Field link to add field values from the current record. The field will be included in brackets, and the field data will be inserted into the email when it is generated. (If data does not exist for a required field, nothing will be inserted; the field area will be blank.)

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



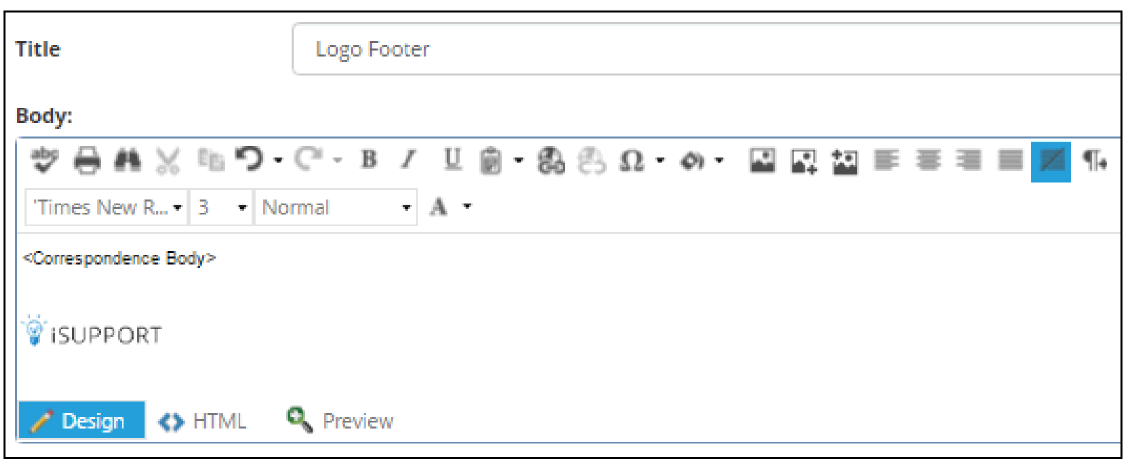
Include Attachment(s) from <record type> - For all modules except Asset, CMDB, Discussion Posts, Security, and Alerts, select this checkbox to associate any attachments from the referenced work item type to the notification when it is sent.

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

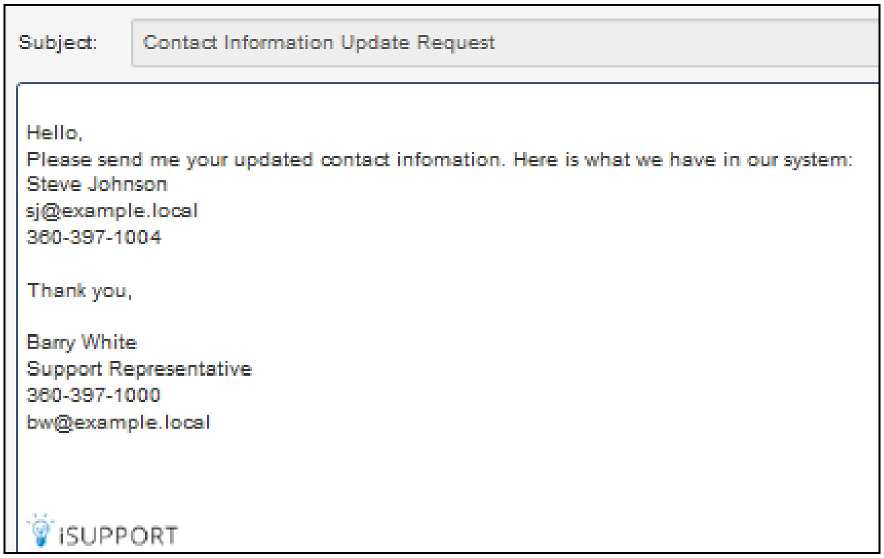
Note: If data does not exist for a required field, nothing will be inserted when the email is generated. The field area will be blank.

Configuring Design Templates

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

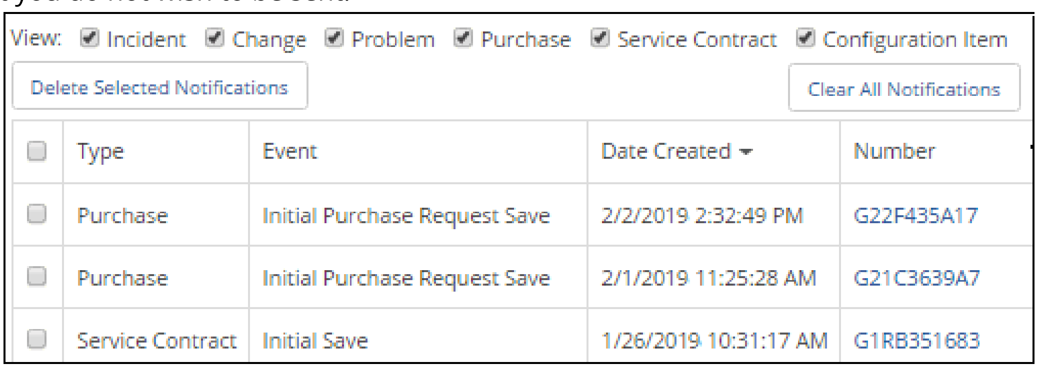


If a support representative sending a correspondence with the design template has a signature block, design elements that are after the <Correspondence Body> tag will appear after it.



Displaying the Notification Queue

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



	Type	Event	Date Created	Number
	Purchase	Initial Purchase Request Save	2/2/2019 2:32:49 PM	G22F435A17
	Purchase	Initial Purchase Request Save	2/1/2019 11:25:28 AM	G21C3639A7
	Service Contract	Initial Save	1/26/2019 10:31:17 AM	G1RB351683

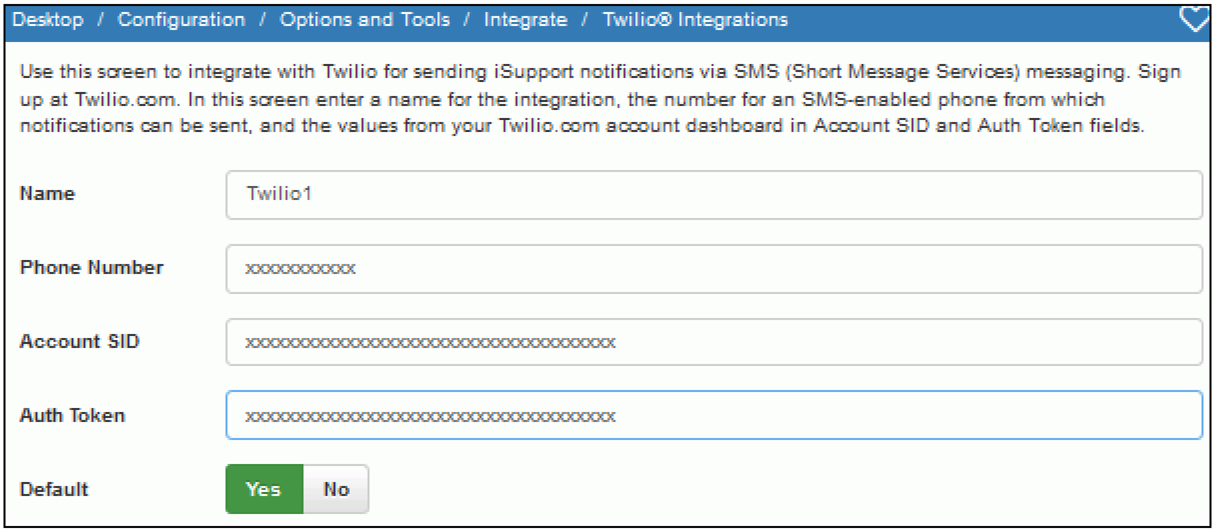
Configuring Twilio Integrations

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

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

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

After signing up at Twilio.com, use the Options and Tools | Integrate | Twilio Integrations screen to set up a number from which iSupport SMS notifications can be sent.



Name - Enter a name for the Twilio integration.

Phone Number - Enter the number for an SMS-enabled mobile phone from which iSupport SMS notifications can be sent.

Account SID - Enter the value for the Account SID from your Twilio.com account dashboard.

Auth Token - Enter the value for the Auth Token from your Twilio.com account dashboard.

Default - Select Yes to use this Twilio integration phone number for all work items that have not been assigned a Twilio integration phone number via a rule.

Configuring Auto-Close and Auto-Fill Incident Templates

Incident templates initially populate fields in Incident records; they are used for incidents that occur frequently. There are two types: auto-close and auto-fill. An auto-fill template will populate fields and the Incident screen will remain open; an auto-close template will, when selected, populate the fields, change the status to a Closed status, and close the Incident screen automatically. However, the auto-close feature will be disabled if:

- The template is used on the mySupport portal.
- Any custom fields are marked as required. Instead, the support representative will be required to enter information in all required custom fields before the incident can be closed.
- Any required fields on the incident have not been completed (customer name, categorization, and description).

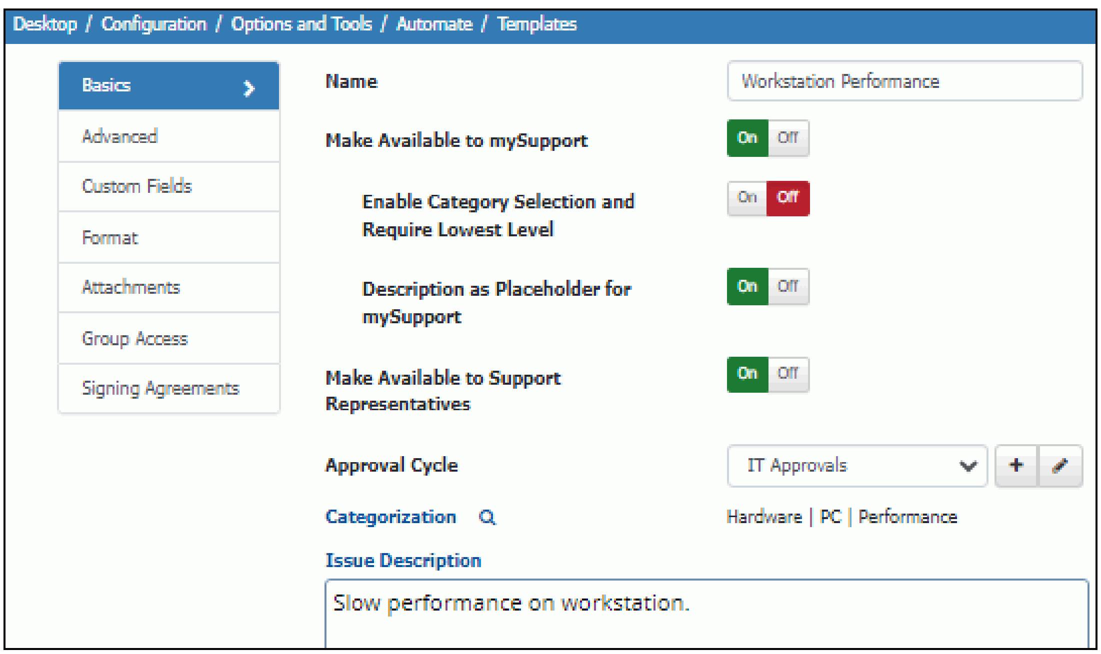
If an inbound email rule uses an auto-close incident template and a required custom field does not have a default value, the required custom field will not have a value in the closed incident.

You can assign a rule group to a template. When the template is selected in the Incident screen, the rule group assigned to the template will replace any existing rule group that may be in effect (for the category or customer). When the template is selected from the mySupport portal, it takes effect based on the creation date and time.

Note that if a template has a field that is blank, the corresponding field in the incident will not be overwritten with a blank value.=

Setting Basic Options

To access the Incident Template screen, select Incident Templates and then click the New link.



Name - Enter a name for the incident template. This name will display for selection in the Incident screen.

Make Available to mySupport - Select Yes to allow the template to be used on a mySupport portal. You can create a link to the template using the mySupport Navigator screen.

Enable Category Selection and Require Lowest Level - This field appears if Yes is selected in the Make Available to mySupport field. Select Yes to enable the category picker when the template is used on a mySupport portal. The user will be prompted to select the lowest level category if they have not already done so.

Description as Placeholder for mySupport - Select On to remove the configured text in the Issue Description field when the user clicks in the field in the Incident screen on mySupport.

Make Available to Support Representatives - Select Yes to include the template in the list of templates for selection in the Incident screen. See "Restricting Access" on page 72 for information on restricting access to members of support representative groups.

Approval Cycle - If approvals are enabled, select the approval cycle to associate with the template. The rule group in effect for the incident can control whether approvals are required and how approval cycles are applied.

Categorization - Click the Categorization link to select a category combination describing the issue. This category combination will populate the Categorization field in the Incident screen.

Display the Call Script for This Category Set - This field is enabled if a script is associated with the selected category combination. Select Yes to display the script when the template is selected in the Incident screen. To view the call script associated with the categorization, click the View Call Script link.

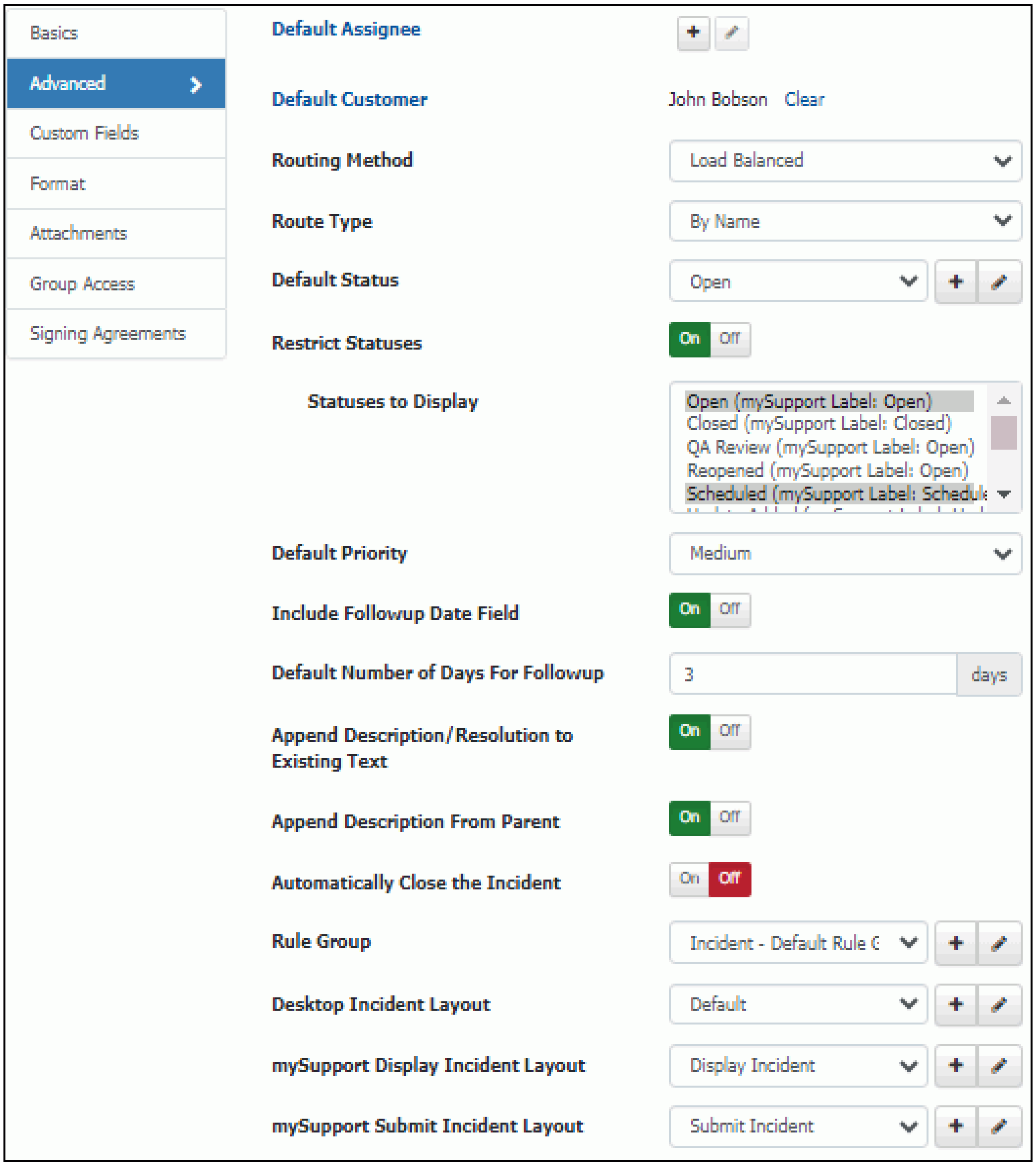
Short Description - This field appears if the Short Description field is enabled on the Incident Fields tab in the Incident Basics screen. Enter the text to populate the Short Description field in the Incident screen.

Issue Description - Enter the text to populate the Description field in the Incident screen. If On is selected in the Description as Placeholder field, the text will disappear when the user clicks in the field in the Incident screen.

Issue Resolution - Enter the text to populate the Resolution field in the Incident screen.

Setting Advanced Template Options

Use the Advanced tab to set miscellaneous template options and enter defaults.



Default Assignee - Select the support representative to populate the Assignee field in the Incident screen. If this field is left blank and the template is applied, the incident source is considered:

- If the incident was manually created by a rep and has not been routed, the default assignee selected in the Incident Basics screen will be used when the template is applied.
- If the incident had been routed previously, the original author of the incident will be the new assignee.
- If the incident was created from a child incident in a hierarchy, the author of the parent incident is used.
- If the incident was created via mySupport, the default customer request owner specified for the portal options set will be used.
- If the incident was created via email processing, the email account's default assignee will be used.

Use the Create New and View/Edit options to access the Rep Profile screen.

Default Customer - This field will apply if a customer has not been added to an incident. Select the customer to populate the Customer field in the Incident screen.

Routing Method - Select one of the following for assignment of incidents created by the template:

- None to only assign to the support representative specified in the Default Assignee field.
- Load Balanced to select an assignee based on current open incident statistics, including weights based on priority. The available support representative with the lightest overall workload will be selected.
- Round Robin to select an assignee based on the oldest date and time.

If Load Balanced or Round Robin is selected, the Route Type field will appear; select By Name to select among all available representatives, By Group to select among a specified group, By Location to select among those in a specified location, By Skill to use the categorization to select qualified support representatives, and By Location By Skill to select among those in a specified location with qualified skills. See "Enabling Routing Methods" on page 10 for more information.

If there is no support representative available for a selected method, an incident will be assigned to the support representative in the Default Assignee field. If none, the incident will be assigned to the support representative in the Default Incident Assignee field on the Basics tab in the Incident Management Basics screen.

Route Type - If Load Balanced is selected as the routing method,

Default Status - If the template is not an auto-close template, select the open status level to populate the Status field in the Incident screen. Use the + Create New and View/Edit options to access the Custom Status Labels screen.

Restrict Statuses/Statuses to Display - To designate the status labels that will be available for selection in incidents created by the template, select Yes and then select the labels.

Default Mapping - This field appears if Impact Urgency Mapping is enabled on the Basics tab in the Incident Basics screen. Click this link to select the Impact, Urgency, and Priority to assign to the Impact, Urgency, and Priority fields on incidents created from the template. These mappings are configured in the Impact and Urgency screen. Use the + Create New and View/Edit options to access the Impact and Urgency screen.

Default Priority - This field appears if Impact Urgency Mapping is not enabled. Select the priority level to populate the Priority field on the Incident screen.

Include Followup Date Field - This field appears if Select Yes to display a Followup Date field in the Incident screen; if a followup reminder email is configured, the email will be sent to the incident assignee when the date in the field is reached. Use the Default Number of Days for Followup field to enter the number of days (after the incident open date) to be used in the calculation of the date to display by default in the Followup Date field.

Default Number of Days for Followup - If including a followup date on the Incident screen, enter the number of days (after the incident open date) to be used in the calculation of the date to display by default in the Followup field. When the followup date is reached, a followup reminder email will be sent to the assignee of the incident. Once the email is sent, the date is recalculated based on the number of days entered in this field.

Append Short Description/Description/Resolution to Existing Text - Select Yes to add a blank line and the text from the Short Description, Description, and/or Resolution field to existing text when the template is applied to a saved incident.

Append Description From Parent - Select Yes to enable the description from a parent (originating) incident in a hierarchy to be appended to the description in a child incident created from it. This will also apply to child incidents created via rules or when the template is applied to an incident that is already part of a hierarchy. Note that if this option is set to Yes for templates on all levels of a multi-tier hierarchy, the lowest level work items could have descriptions built up from many other higher level work items.

The text entered in the work item's description via email or direct entry will be retained when the template's configured description and resolution are applied. If the Append Description/Resolution to Existing Text option is also enabled for a template, an incident description would include the text from the template, the text entered via the email, rep, or mySupport customer, and the description from the parent (originating) incident.

This setting will be ignored if the template is applied to an incident that has no parent level incident (it's not part of a hierarchy).

Automatically Close the Incident - Select Yes to enable the auto-close option for the template. When the template is selected for an incident, the incident status will change to Closed and the incident window will close.

If you do not enable this option, the template will be labeled "Auto-Fill" in the template selection dialog in the Incident screen. If you enable this feature, "Auto-Close" will appear next to the template name.

Note: The auto-close feature will be disabled if:

- The template is used on the mySupport portal.
- Any custom fields are required. Instead, the support representative will be required to enter information in all required custom fields before the incident can be closed.
- Any required fields on the incident have not been completed (customer name, categorization, and description).

Default Closed Status - If automatically closing the incident, select the Closed status to populate the Status field in the incident. Use the ✚ Create New and ✎ View/Edit options to access the Custom Status Labels screen.

When an Incident is Auto-Closed, Record Time Worked - If automatically closing the incident, select Yes to record a specified amount of time in the Time Worked field on the incident.

Time Value - If automatically closing the incident and recording the time worked, enter the amount of time to record.

Rule Group - If applicable, select the rule group to apply when the template is selected in the Incident screen. The rule group assigned to the template will replace any existing rule groups that may be in effect (for the category or customer). Use the ✚ Create New and ✎ View/Edit options to access the Incident Rule Group screen; see "Configuring Rules and Rule Groups for Incidents" on page 46 for more information.

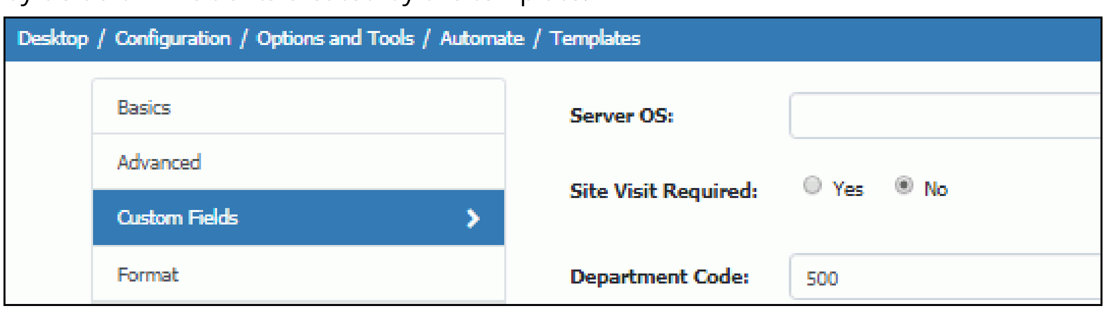
Desktop Incident Layout - Select the layout containing the fields and tabs that will display when the template is selected for an incident via the Incident screen or a rule. You can use the ✚ Create New and ✎ View/Edit options to access the Incident Layouts configuration screen. Layouts can also be associated with a category, customer group, support rep group, or incident hierarchy template; the Order of Precedence field in the Incident Layouts screen determines which layout to use when more than one reference is applicable (for example, if the logged in rep's primary group has a layout as does the selected category). For categories, the layout found with the lowest level will be used; if a layout is not found at the lowest level the next level up will be checked, and so on up to the top level. If no layout is associated at the top level, the default layout specified in the Layouts screen will be used.

mySupport Display Incident Layout - Select the mySupport incident display layout (configured via the mySupport Layouts screen) to apply when incidents created by the template are displayed on a mySupport portal. You can use the ✚ Create New and ✎ View/Edit options to access the mySupport Layouts configuration screen.

mySupport Submit Incident Layout - Select the mySupport incident submit layout (configured via the mySupport Layouts screen) to apply when the template is used on a mySupport portal. You can use the ✚ Create New and ✎ View/Edit options to access the mySupport Layouts configuration screen.

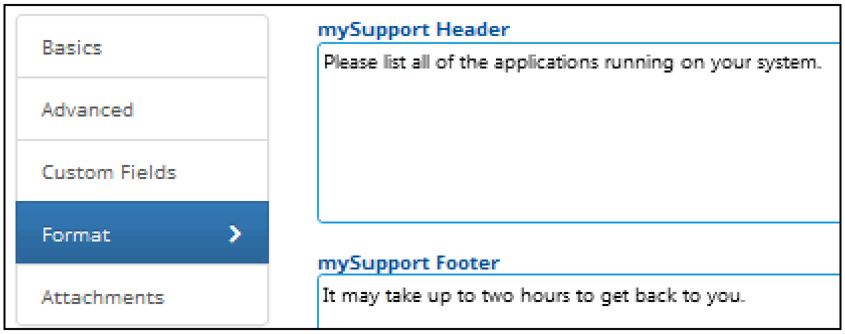
Configuring Custom Fields

The Custom Fields tab contains custom fields configured via the Custom Fields screen; select the values to populate custom fields by default in incidents created by the template.



Formatting the mySupport Incident Template Submit Screen

If Yes is selected in the Make Available to mySupport field on the Advanced tab, use the Format tab to add formatted text and images to appear at the top (header) and bottom (footer) of the mySupport Submit screen.

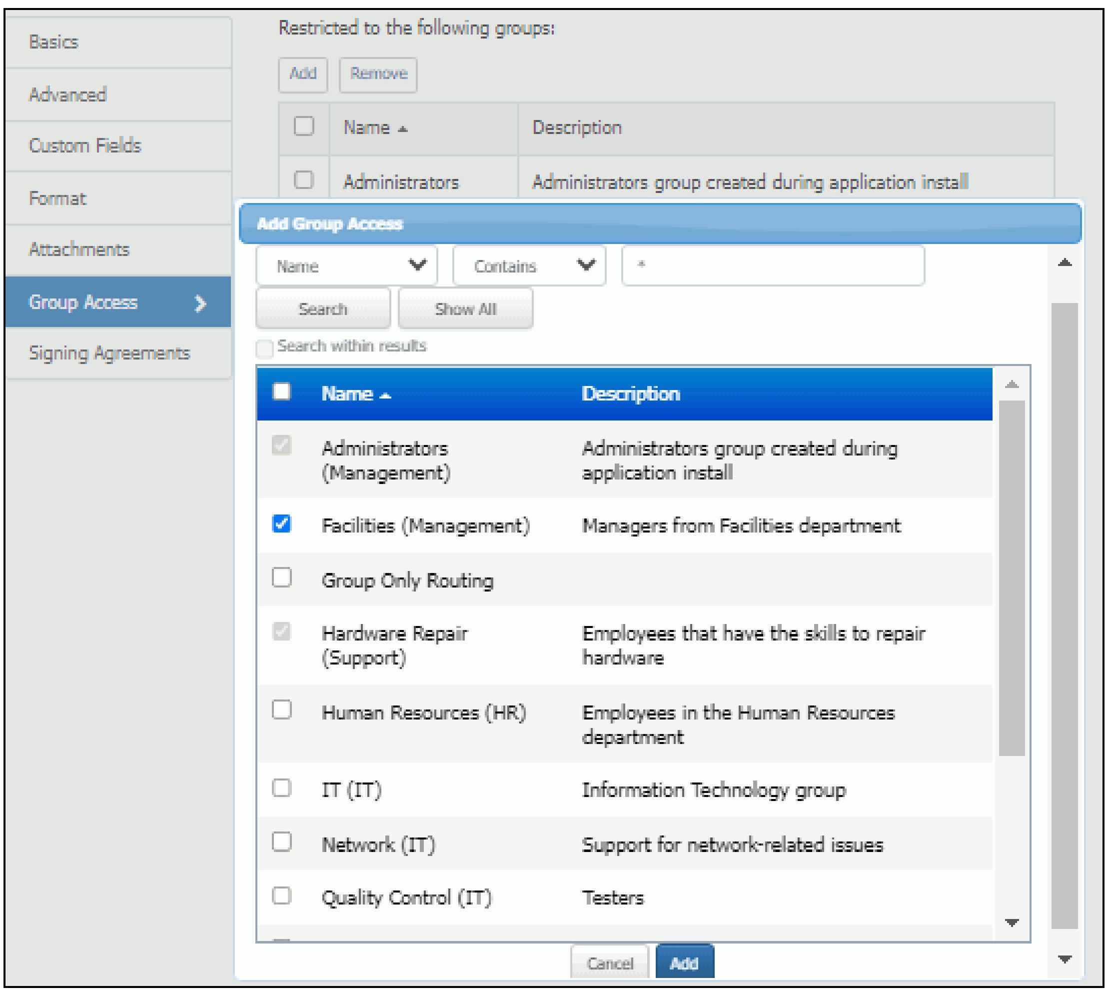


Attaching Files

Use the Attachments tab to attach any files to the template.

Restricting Access

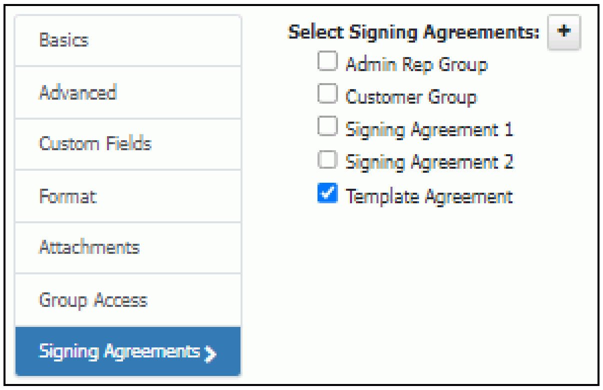
Use the Group Access tab to restrict display of the template to members of support representative groups. Click the Add link to display the following dialog for selecting the groups. ***After you add one or more groups and save, the template will display only to members of the selected groups.***



Associating Signing Agreements

Use a signing agreement to display details in the Sign dialog in the Incident and Change work item screens. Signing agreements can be associated with customer and support representative groups, categories, and incident and change templates. If an incident or change involves more than one associated signing agreement (group, category, or template), all will be included in the Sign dialog in a dropdown for selection. (Note that "Blank" is also included for displaying no text above the signing line.)

On the Signing Agreements tab, select the agreements to appear for selection in the dropdown when the incident or change involves the associated template. Use the plus sign icon to create an agreement via the Signing Agreements configuration screen.



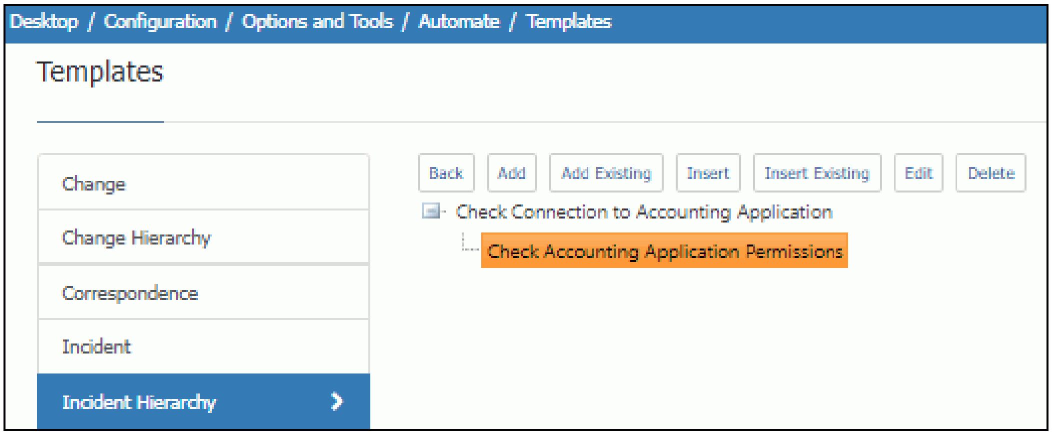
Deleting Templates

You cannot delete a template that has been used to create incidents until the associated incidents have been closed and archived or deleted and removed via the Database Maintenance agent. You can create a view with the Template Name attribute in the Incidents data source to display the name of templates used to create incidents.

Configuring Incident Hierarchy Templates

Like incident templates, incident hierarchy templates initially populate fields in Incident records. Use hierarchy templates to track and manage issues, incidents, and service requests that have multiple activities; you can use a template as an incident model that predefines steps to handle a process. Existing incident functionality such as escalation, routing, and followup dates apply to incidents created from hierarchy templates. Note that if a template has a field that is blank, the corresponding field in the incident will not be overwritten with a blank value.

Hierarchy templates are especially useful for accountability purposes if there is more than one person involved; for example, you could create a hierarchy template for checking an application connection with someone in IT as the default assignee, and create a template for checking permissions with someone in Accounting as the default assignee.

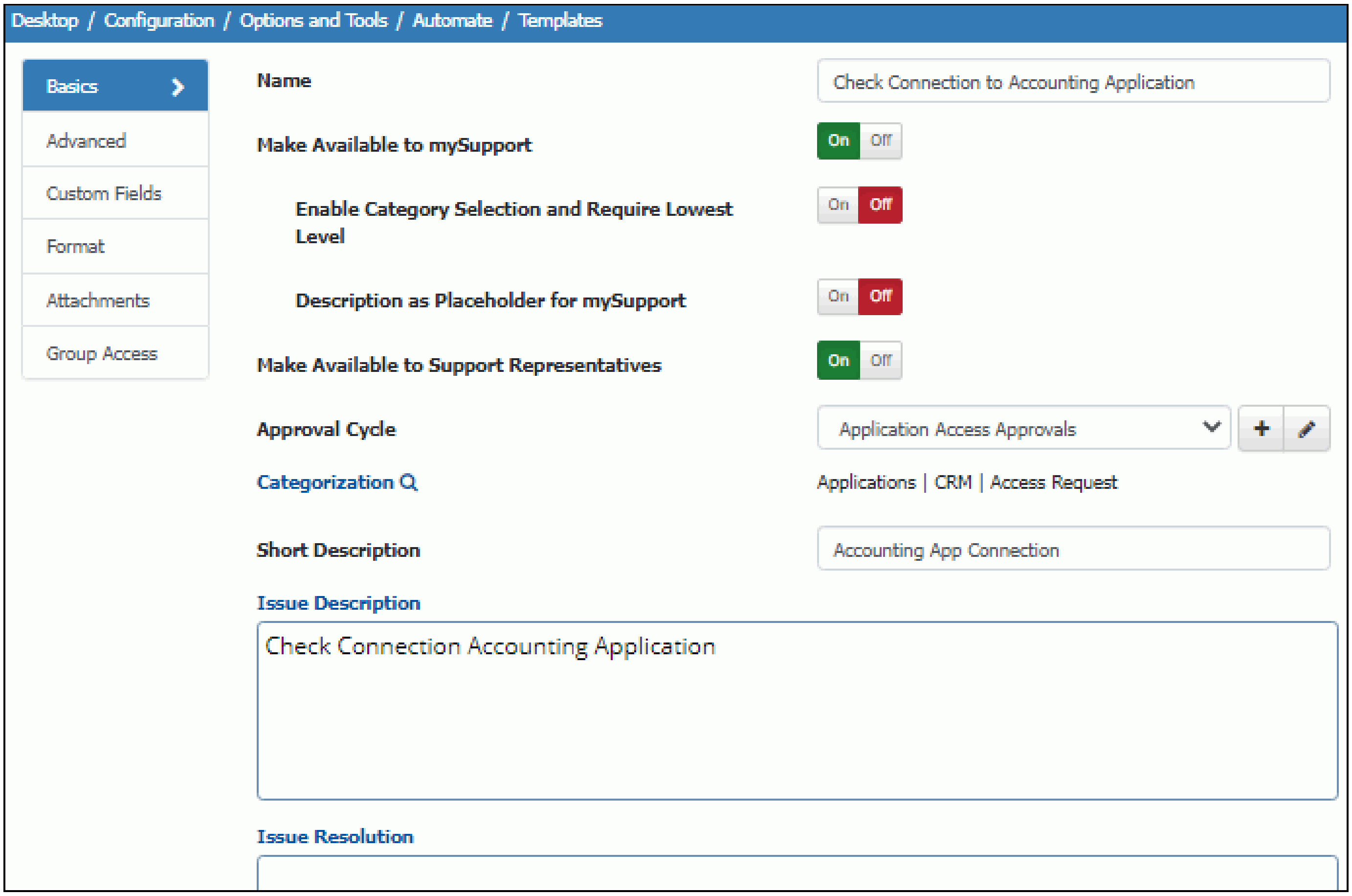


In the example above, when the Check Connection to Accounting Application template is selected in the Incident screen, an incident is created from the Check Connection to Accounting Application template as well as the Check Accounting Application Permissions template.

Notifications regarding hierarchy events can be configured via incident rules; for example, you can send a notification to the assignee of the top (root) level incident or to the assignees of lower level incidents.

Creating a Top Level Template

Complete the following fields on the Basics tab in the Hierarchy Templates screen.



Name - Enter a name for the hierarchy template. This name will display for selection in the Incident screen.

Make Available to mySupport - This field is only available on a top-level hierarchy template. Select Yes to allow the template to be used on the mySupport portal. You can create a link to the template using the mySupport Navigator screen.

Enable Category Selection and Require Lowest Level - This field appears if Yes is selected in the Make Available to mySupport field. Select Yes to enable the category picker when the template is used on a mySupport portal. The user will be prompted to select the lowest level category if they have not already done so.

Description as Placeholder for mySupport - Select On to remove the configured text in the Issue Description field when the user clicks in the field in the Incident screen on mySupport.

Make Available to Support Representatives - This field is only available on a top-level hierarchy template. Select Yes to include the template in the list of templates for selection in the Incident screen. See "Restricting Access" on page 80 for information on restricting access to members of support representative groups.

Approval Cycle - If approvals are enabled, select the approval cycle to associate with the template. The rule group in effect for the incident can control whether approvals are required and how approval cycles are applied.

Categorization - Click the Categorization link to select a category combination describing the issue. This category combination will populate the Categorization field in the Incident screen.

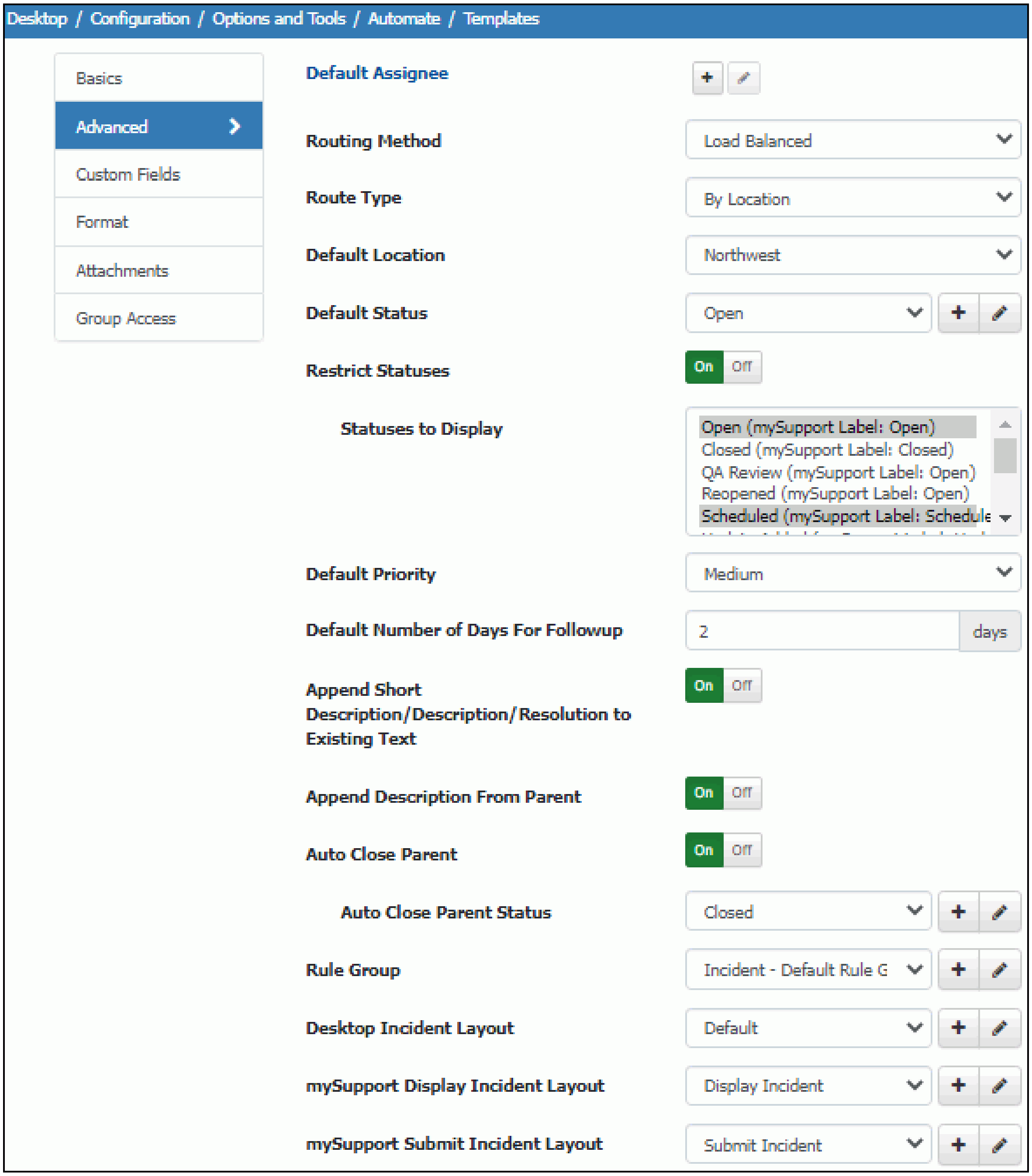
Display the Call Script for This Category Set - This field is enabled if a script is associated with the selected category combination. Select Yes to display the script when the template is selected in the Incident screen. To view the call script associated with the categorization, click the View Call Script link.

Short Description - This field appears if the Short Description field is enabled on the Incident Fields tab in the Incident Basics screen. Enter the text to populate the Short Description field in the Incident screen.

Issue Description - Enter the issue description to populate the Description field in the Incident screen.

Issue Resolution - Enter the issue resolution to populate the Resolution field in the Incident screen.

Use the Advanced tab on the Hierarchy Template screen to set miscellaneous template options and enter defaults for the assignee and priority fields.



Default Assignee - Select the support representative to populate the Assignee field in the Incident screen. Use the + Create New and View/Edit options to access the Rep Profile screen.

Routing Method - Select one of the following for assignment of incidents created by the template:

- None to only assign to the support representative specified in the Default Assignee field.
- Load Balanced to select an assignee based on current open incident statistics, including weights based on priority. The available support representative with the lightest overall workload will be selected.
- Round Robin to select an assignee based on the oldest date and time.

If Load Balanced or Round Robin is selected, the Route Type field will appear; select By Name to select among all available representatives, By Group to select among a specified group, By Location to select among those in a specified location, By Skill to use the categorization to select qualified support representatives, and By Location By Skill to select among those in a specified location with qualified skills. See "Enabling Routing Methods" on page 10 for more information.

If there is no support representative available for a selected method, an incident will be assigned to the support representative in the Default Assignee field. If none, the incident will be assigned to the support representative in the Default Incident Assignee field on the Basics tab in the Incident Management Basics screen.

Default Status - Select the status level to populate the Status field in the Incident screen. Use the + Create New and View/Edit options to access the Custom Status Labels screen.

Restrict Statuses/Statuses to Display - To designate the status labels that will be available for selection in incidents created by the template, select On and then select the labels. Note: Use the Order of Precedence link in the Custom Status Labels screen to set which will prevail if both a template and a support representative group have a restricted status.

Default Mapping - This field appears if Impact Urgency Mapping is enabled on the Basics tab in the Incident Basics screen. Click this link to select the Impact, Urgency, and Priority to assign to the Impact, Urgency, and Priority fields on incidents created from the template. Use the + Create New and View/Edit options to access the Impact and Urgency screen.

Default Priority - This field appears if Impact Urgency Mapping is not enabled in the Incident Basics screen. Select the priority level to populate the Priority field on the Incident screen.

Default Number of Days for Followup - If including a followup date on the Incident screen, enter the number of days (after the incident open date) to be used in the calculation of the date to display by default in the Followup field. When the followup date is reached, a followup reminder email will be sent to the assignee of the incident. Once the email is sent, the date is recalculated based on the number of days entered in this field.

Append Short Description/Description/Resolution to Existing Text - Select On to add a blank line and the text from the Short Description, Description, and/or Resolution field to existing text when the template is applied to a saved incident.

Append Description From Parent - Select On to enable the description from a parent (originating) incident in a hierarchy to be appended to the description in a child incident created from it. This will also apply to child incidents created via rules or when the template is applied to an incident that is already part of a hierarchy. Note that if this option is set to Yes for templates on all levels of a multi-tier hierarchy, the lowest level work items could have descriptions built up from many other higher level work items.

The text entered in the work item's description via email or direct entry will be retained when the template's configured description and resolution are applied. If the Append Description/Resolution to Existing Text option is also enabled for a template, an incident description would include the text from the template, the text entered via the email, rep, or mySupport customer, and the description from the parent (originating) incident.

This setting will be ignored if the template is applied to an incident that has no parent level incident (it's not part of a hierarchy).

Auto Close Parent - Select Yes to automatically close the top level work item if all lower level work items in the hierarchy are closed. The following text will be included in the resolution field: "Automatically closed after closure of all work items in the hierarchy".

Auto Close Parent Status - If automatically closing a top level work item when all lower level work items in the hierarchy are closed, select or create a Closed status label to assign to the top level incident that is automatically closed. Use the + Create New and View/Edit options to access the Custom Status Labels screen.

Rule Group - If applicable, select the rule group to apply when the template is selected in the Incident screen. The rule group assigned to the template will replace any existing rule groups that may be in effect (for the category or customer). Use the + Create New and View/Edit options to access the Incident Rule Group screen; see "Configuring Rules and Rule Groups for Incidents" on page 46 for more information.

Desktop Incident Layout - Select the layout containing the fields and tabs that will display when the hierarchy template is selected for an incident via the Incident screen or a rule. You can use the + Create New and View/

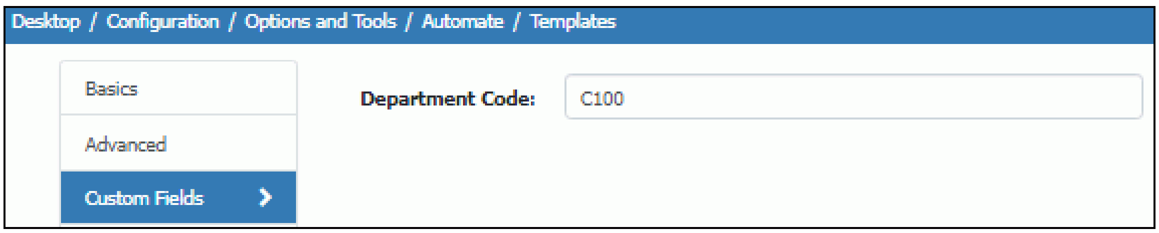
Edit options to access the Incident Layouts configuration screen. Layouts can also be associated with a category, customer group, support rep group, or incident template; the Order of Precedence field in the Incident Layouts screen determines which layout to use when more than one reference is applicable (for example, if the logged in rep's primary group has a layout as does the selected category). For categories, the layout found with the lowest level will be used; if a layout is not found at the lowest level the next level up will be checked, and so on up to the top level. If no layout is associated at the top level, the default layout specified in the Layouts screen will be used.

mySupport Display Incident Layout - Select the mySupport incident display layout (configured via the mySupport Layouts screen) to apply when incidents created by the template are displayed on a mySupport portal.

mySupport Submit Incident Layout - Select the mySupport incident submit layout (configured via the mySupport Layouts screen) to apply when the template is used on a mySupport portal.

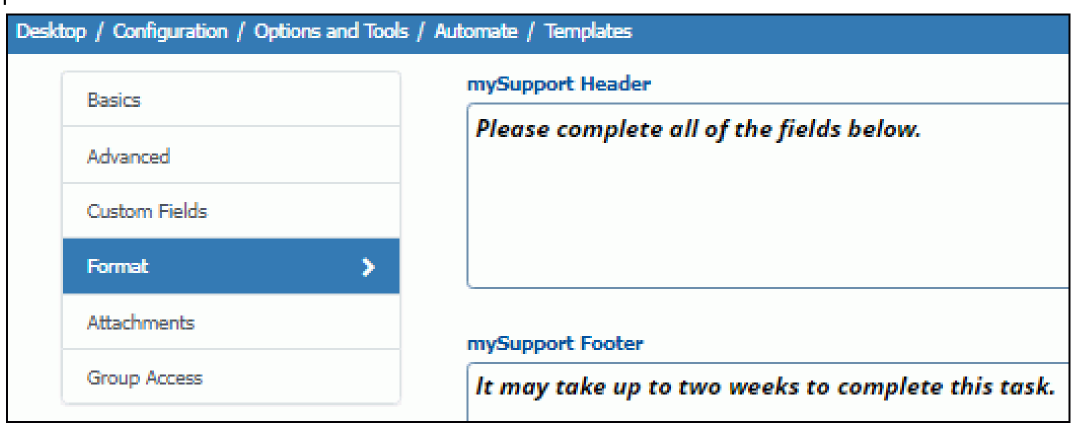
Configuring Custom Fields

The third tab contains custom fields configured via the Custom Fields screen; select the values to populate custom fields by default in incidents created by the template.

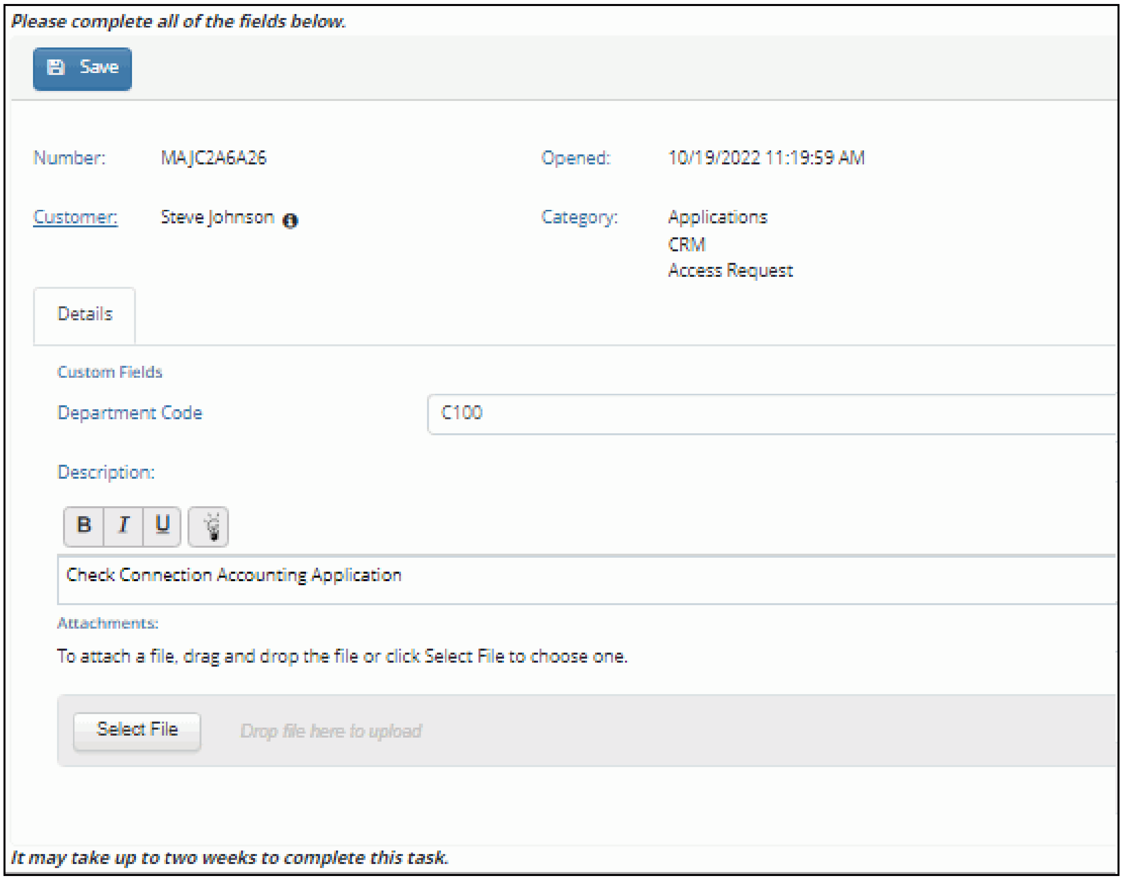


Formatting the mySupport Incident Hierarchy Template Submit Screen

The Format tab will appear if Make Available to mySupport is selected on the Advanced tab. Use the Format tab to add formatted text and images to appear at the top (header) and bottom (footer) of the mySupport Incident Hierarchy Template Submit screen.



The text will appear as shown in the example below.

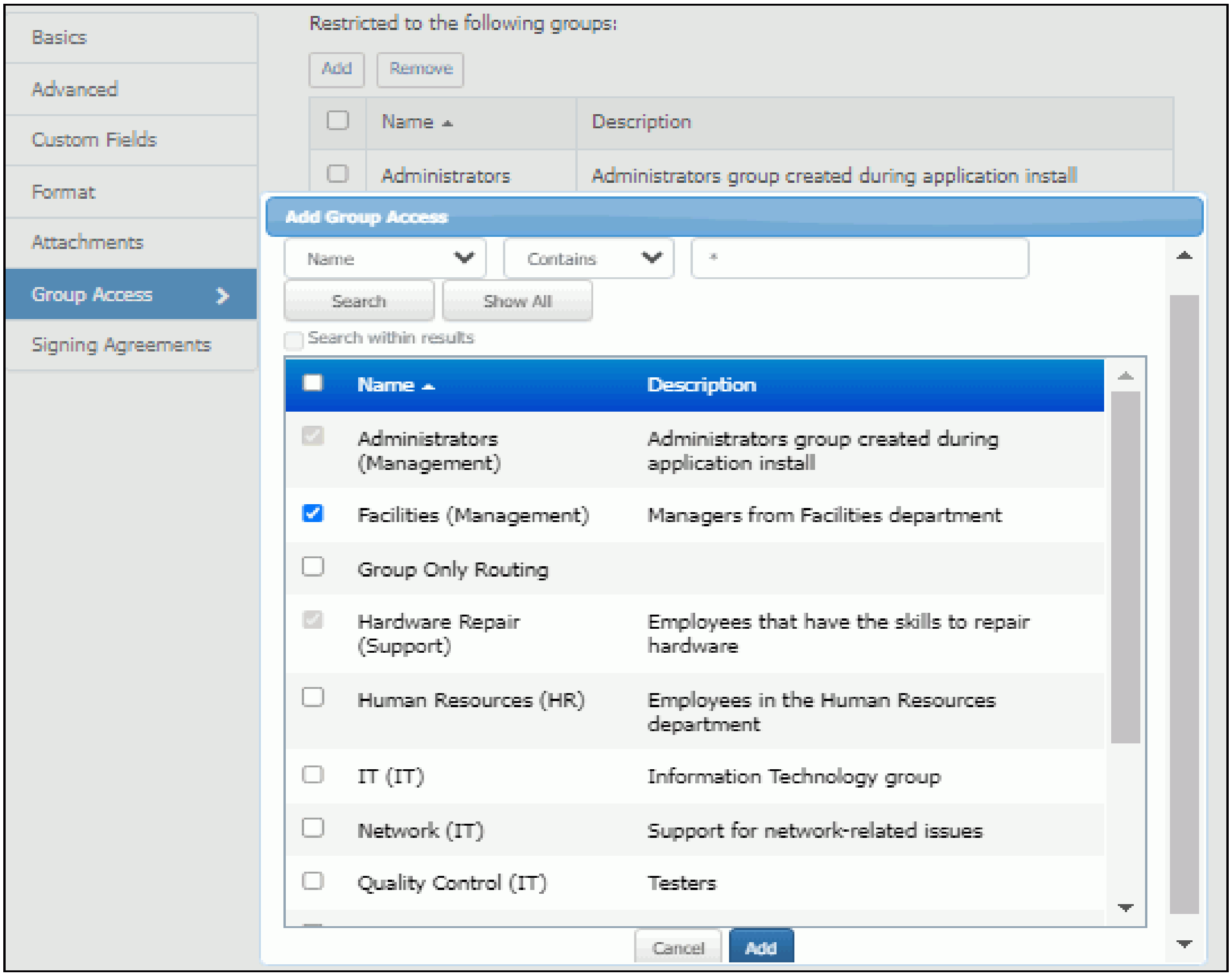


Attaching Files

Use the Attachments tab to attach any files to the template.

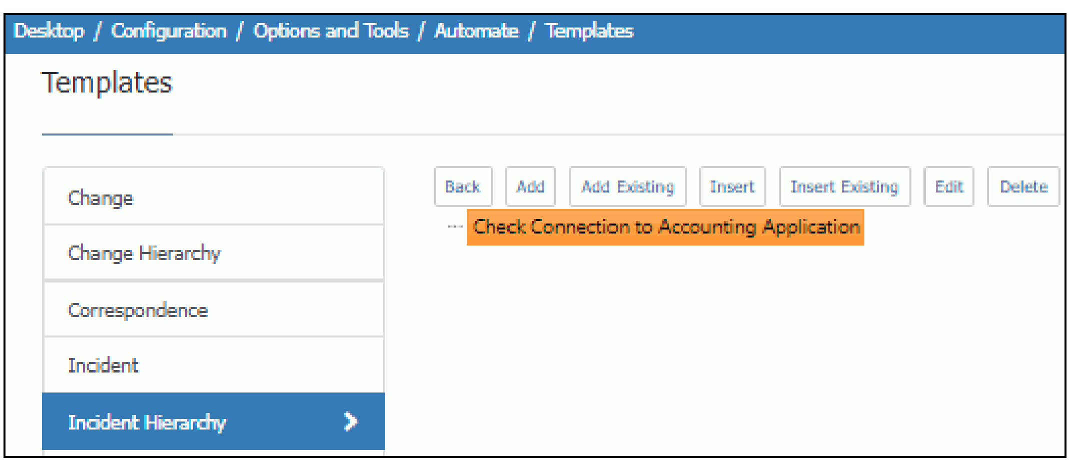
Restricting Access

Use the Group Access tab to restrict display of the template to members of support representative groups. Click the Add link to display the following dialog for selecting the groups. ***After you add one or more groups and save, the template will display only to members of the selected groups.***



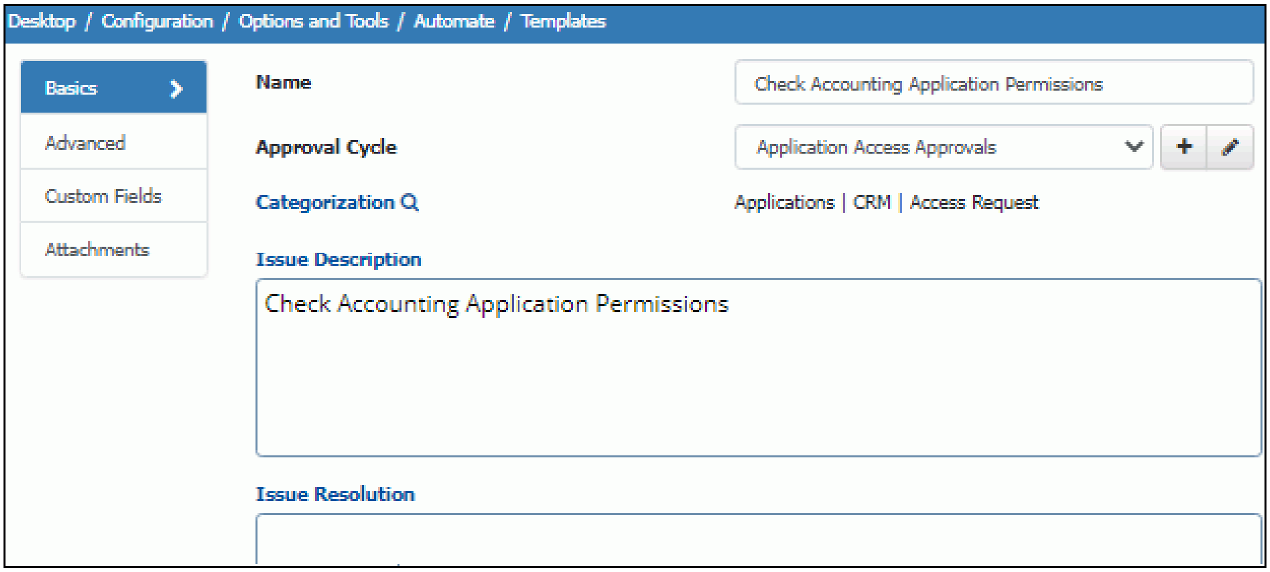
Creating a Lower Level Template

After you create and save a template, the following links appear in the View Hierarchy Templates screen:

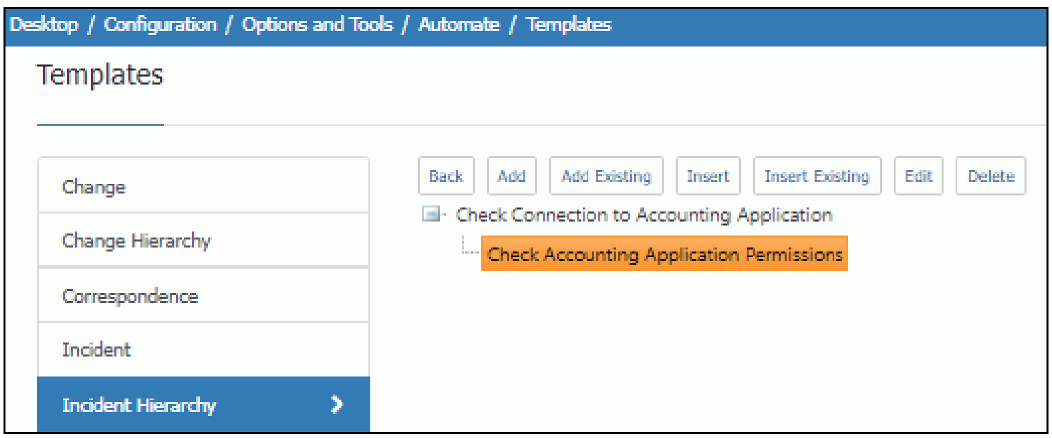


To create a template that will be one level below an existing template, select the existing template and click the Add link.

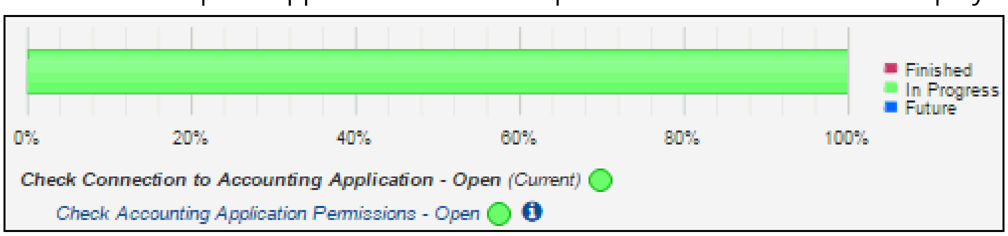
The Hierarchy Template screen appears. On a lower-level template, the Basics tab does not contain the Make Available to mySupport and Make Available to Support Representatives fields because only top-level templates are available for selection in the mySupport portal and Incident screens. (However, the layouts will apply to incidents created by the template.)



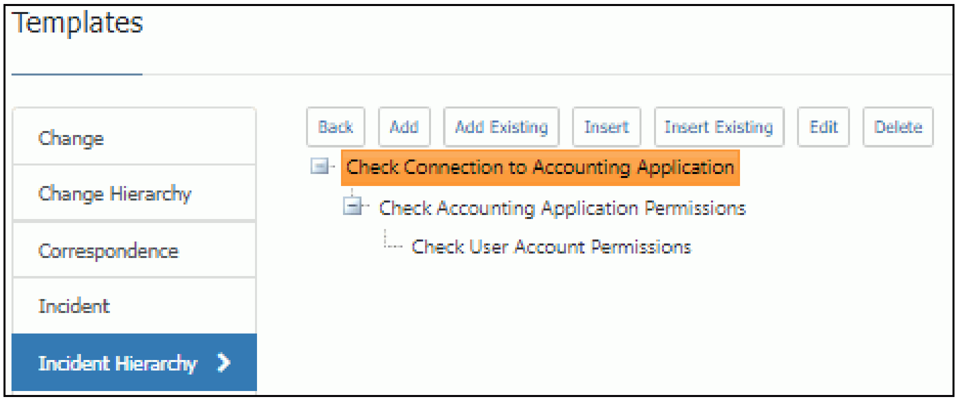
When you add a lower level template to a top-level template, the lower level template is indented in the View Hierarchy Templates screen.



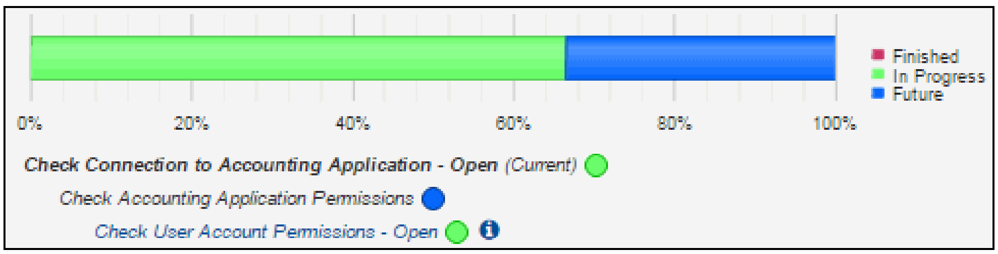
After using a hierarchy template in the Incident screen, use either the Related Hierarchy field (if configured) or the View Related option (which displays a dialog as shown below) to display the incidents created by the template hierarchy. A Click for Details option appears next to each open and closed incident for displaying incident details.



When a third level template is added to the hierarchy, a dependency is created. An incident will not be automatically created from the middle-level template until the incident created from the template below it is closed. In the example below, when the Check Connection to Accounting Application template is selected in the Incident screen, it is applied to the current incident and an incident is created with the Check User Account Permissions template. An incident will be created with the Check Accounting Application Permissions template when the Check User Account Permissions incident is closed.

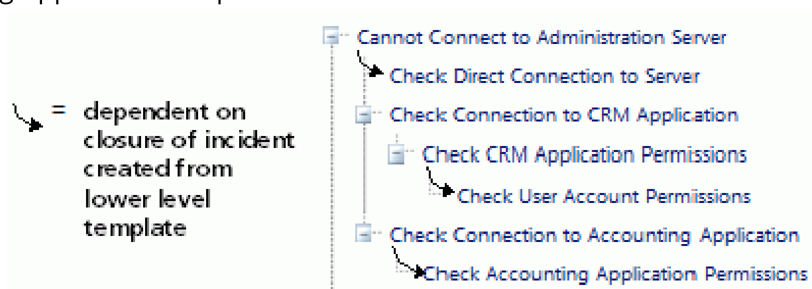


This is shown in the Incident screen when you view the hierarchy.

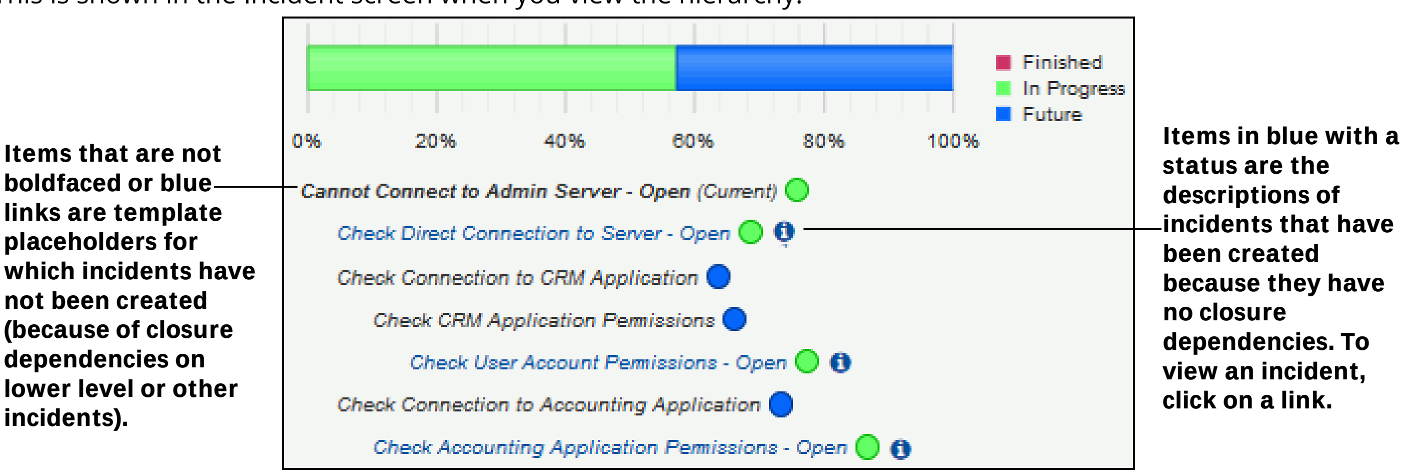


In iSupport, template components that have not created incidents due to dependencies are called *placeholders*.

Dependencies are created as you add more levels. In the example below, an incident created from the Check Accounting Application Permissions template must be closed before an incident will be created from the Check Connection to Accounting Application template.

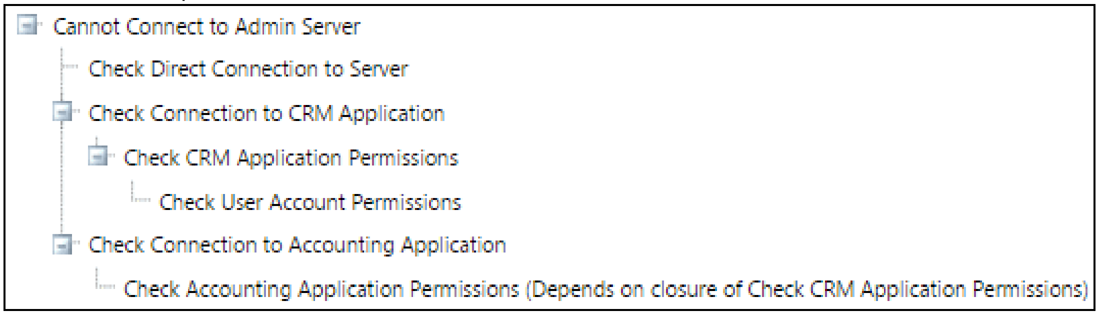


This is shown in the Incident screen when you view the hierarchy.

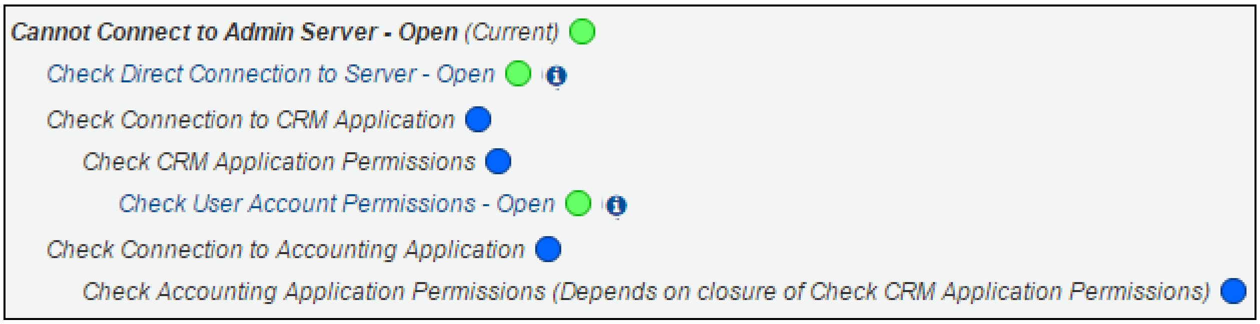


In addition to the dependency that exists when a template is directly below (a lower level template to) another template in a hierarchy, you can define a separate dependency. In the following example, the Check Accounting

Application Permissions template is defined to be dependent on closure of an incident created from the Check CRM Application Permissions template.



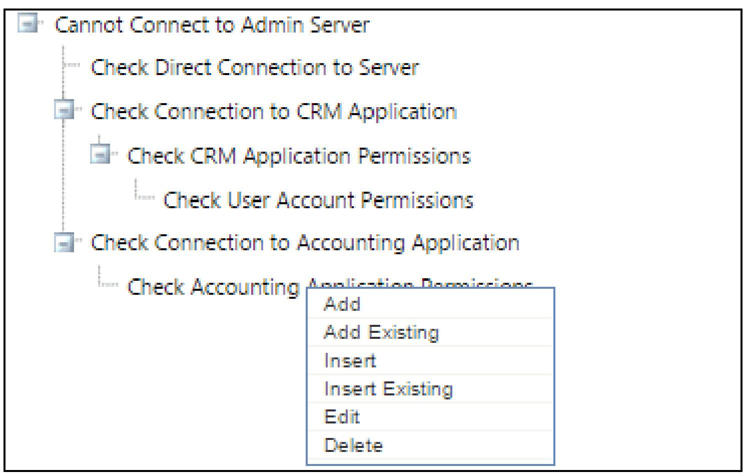
The defined dependency is shown in the Incident screen when you view the hierarchy.



For information on defining the separate dependency, see "Adding Other Dependencies" on page 84.

Example - Building a Workflow Hierarchy

You can use the Add, Add Existing, Insert, and Insert Existing options on the right-click menu to create a large hierarchy as shown in the example below. It is useful to chart your template structure using a white board to ensure that it is logical and complete.



You would use the following steps to create the workflow:

1 Use the New link to create and save the Cannot Connect to Admin Server template.

2 Select the Cannot Connect to Admin Server template and click the Add link.

3 Create and save the Check Direct Connection to Server template.

4 Select the Cannot Connect to Admin Server template and click the Add link. Create and save the Check Connection to CRM Application template.

5 Select the Check Connection to CRM Application template and click the Add link.

6 Create and save the Check CRM Application Permissions template.

7 Select the Check CRM Application Permissions template and click the Add link.

8 Create and save the Check User Account Permissions template.

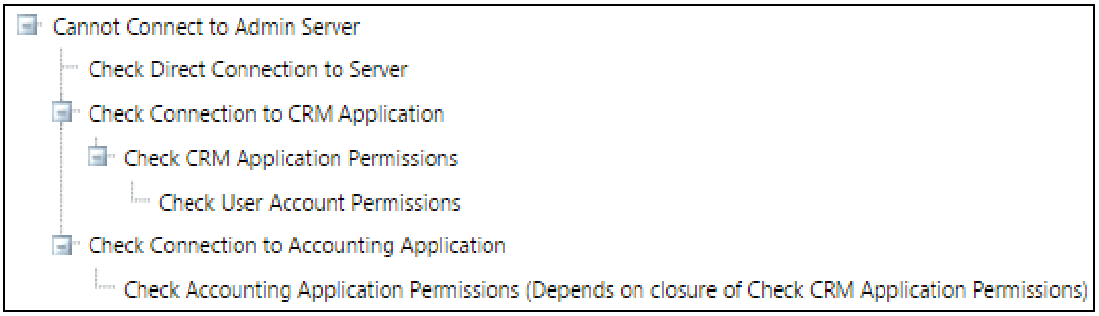
9 Select the Cannot Connect to Admin Server template and click the Add link. Create and save the Check Connection to Accounting Application template.

10 Select the Check Connection to Accounting Application template and click the Add link.

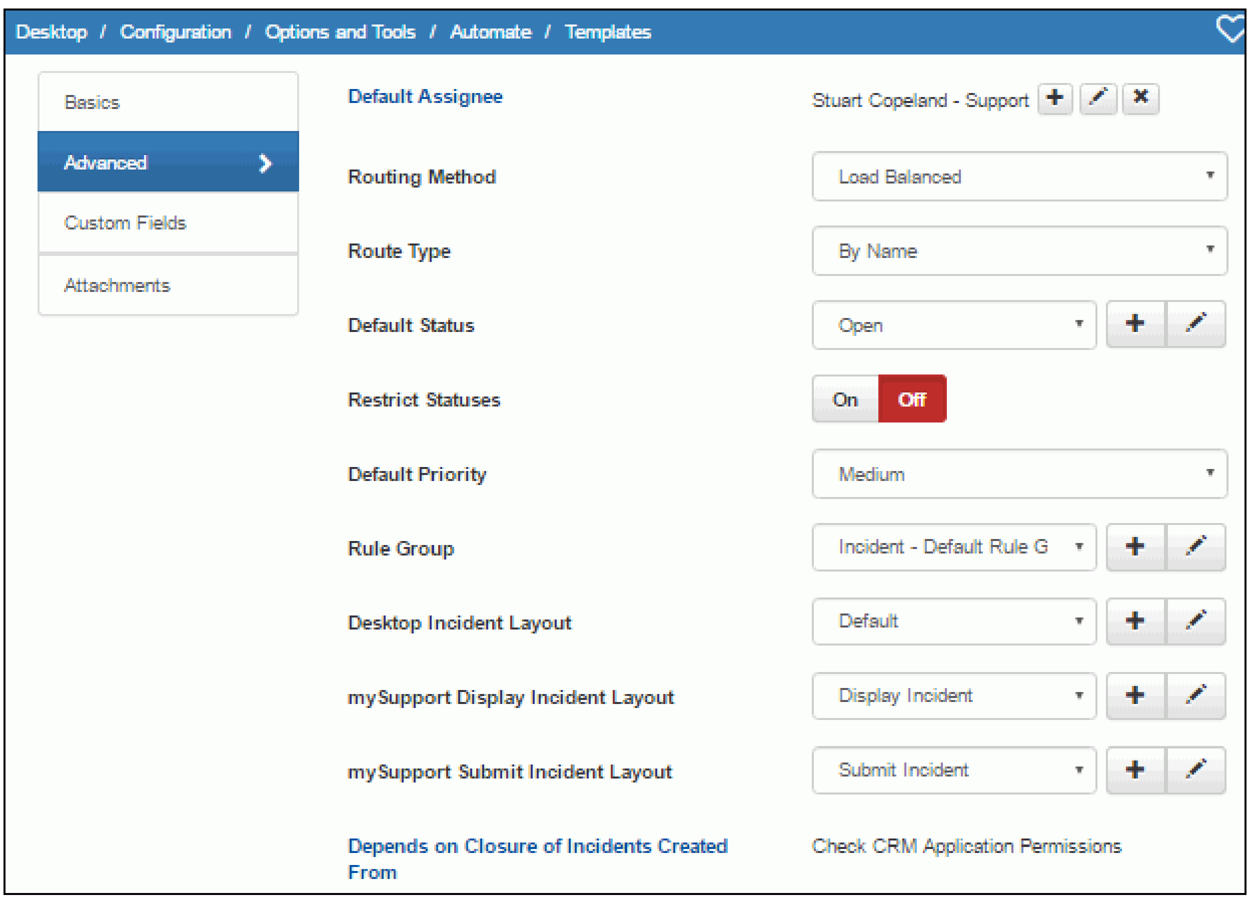
11 Create and save the Check Accounting Application Permissions template.

Adding Other Dependencies

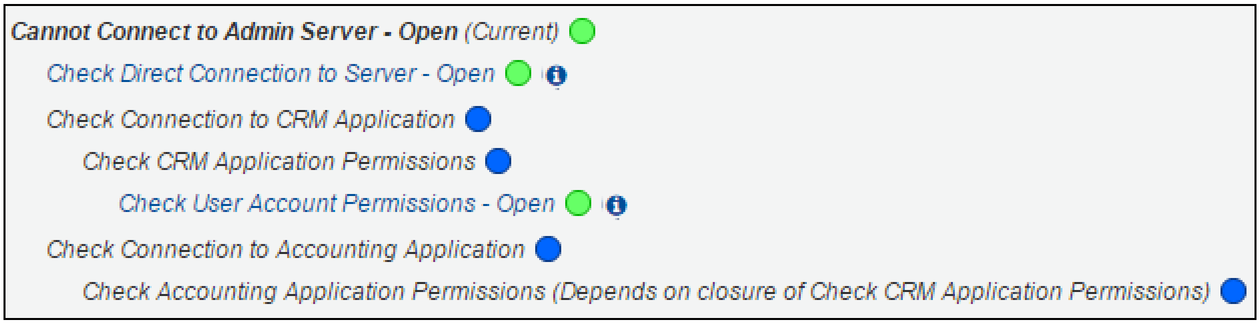
In addition to the dependency created when you add or insert a template, you can define a dependency on a template that is not on a level directly below the specified template. In the following example, a dependency can be defined for the Check Accounting Application Permissions template so that an incident will not be created from it until an incident created from the Check CRM Application Permissions template is closed.



To define this type of dependency, you would first select the template (Check Accounting Application Permissions in this example) and click the Edit link. In the Hierarchy Template screen, click the Depends on Closure of Incidents Created From link on the Advanced tab. Select the template from which an incident must be closed before an incident will be created from current template. Continuing with the example, you would select the Check CRM Application Permissions template.



The defined dependency is shown in the Incident screen when you view the hierarchy.



Note: When you use the Edit link to change a template, the change will not be reflected in any other hierarchies that use the template. Incidents already created from the template are not affected; however, future incidents created from the template will reflect the change.

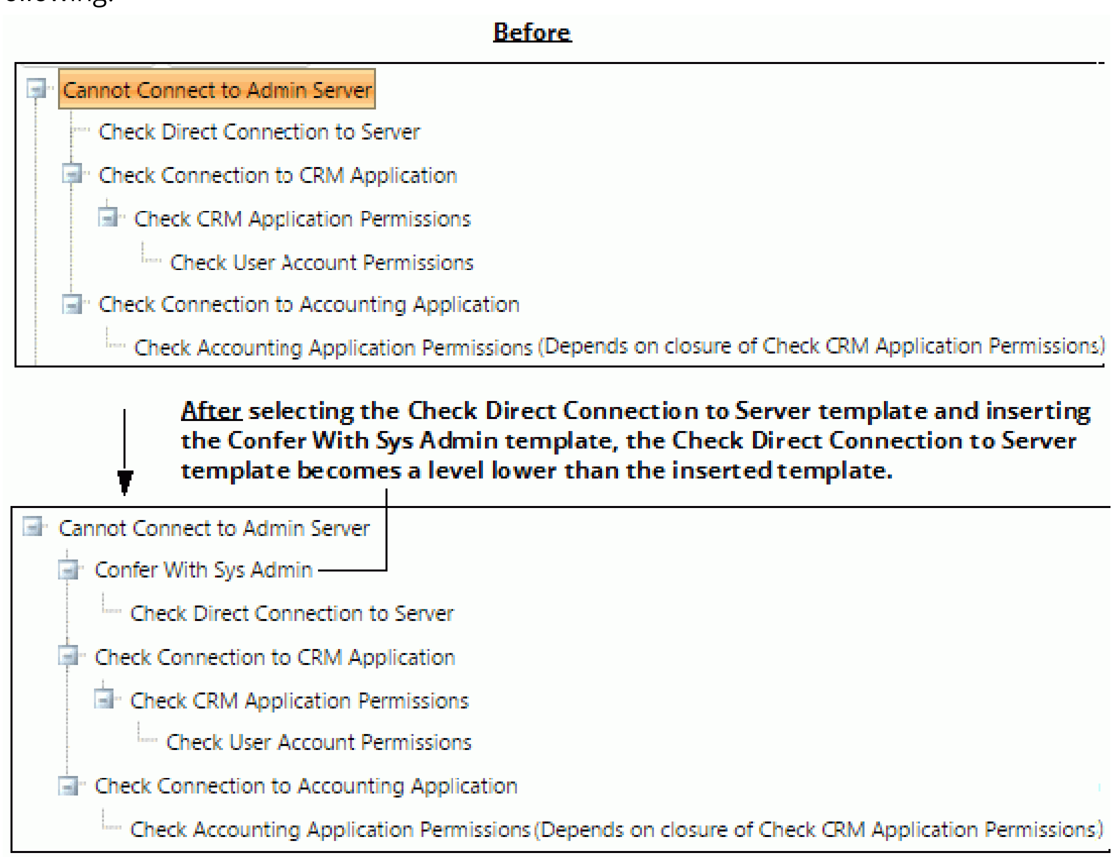
Adding Existing Templates

When you use the Add Existing link to add an existing template to a hierarchy, a copy of the existing template is placed a level *under* the selected template and changes can be made if necessary. If the template that is copied includes lower level templates, those templates are also copied.

Inserting Templates Into a Hierarchy

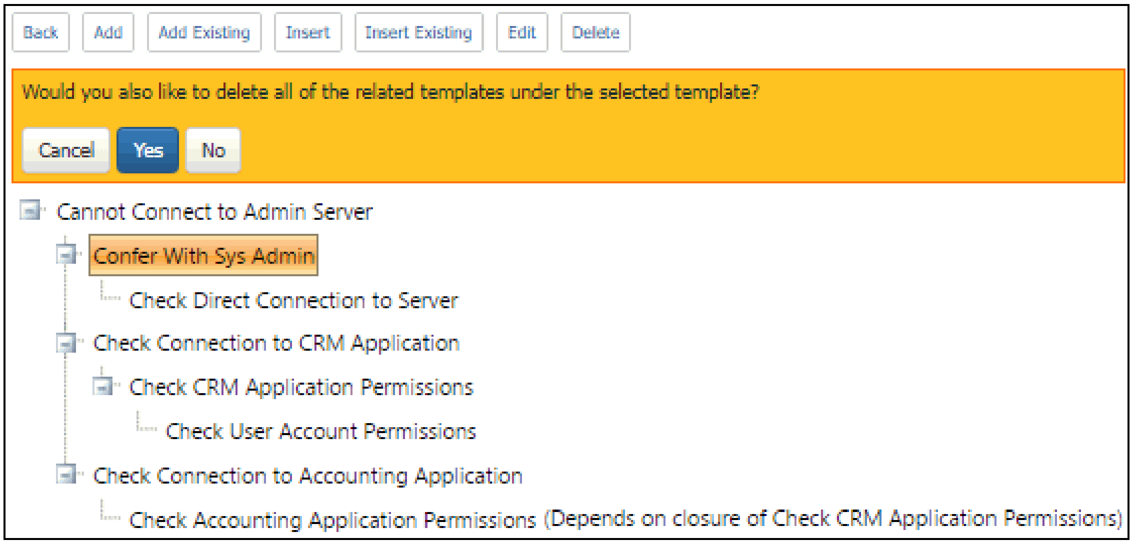
Once you have created a workflow hierarchy, you can use the Insert and Insert Existing links to insert a copy of a template into it. The inserted template will be placed *above* (as a parent to) the selected template, pushing the selected template down a level. If the template to be inserted includes lower level templates, those templates are also copied.

In the example below, if you were to select the Check Direct Connection to Server template, click the Insert link, and create and save a different template (Confer With Sys Admin in the example below), the template hierarchy would look like the following.

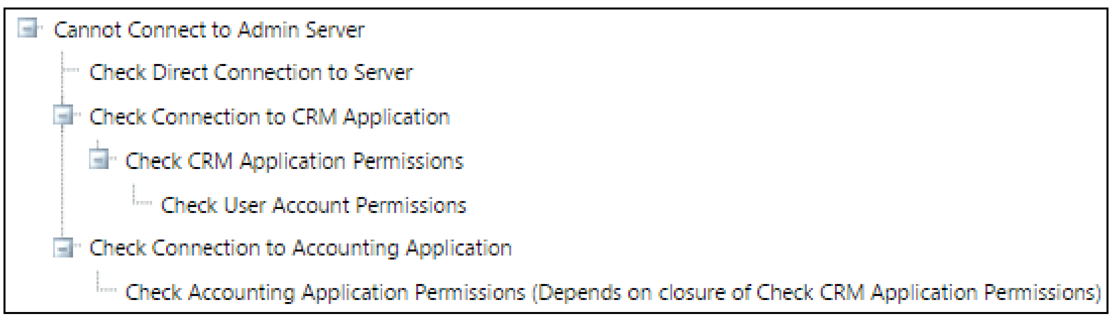


Deleting Templates in a Hierarchy

If you need to delete a template that has lower level templates, you can choose to delete the lower level templates or move them under the upper level of the template to be deleted. In the example below, if you select the Confer With Sys Admin template and click the Delete link or press the Delete key, the following prompt will appear after a verification prompt:



If you answer No, the lower level template (Check Direct Connection to Server in the example below) will move up one level in the hierarchy, becoming a lower level of the Cannot Connect to Admin Server template.



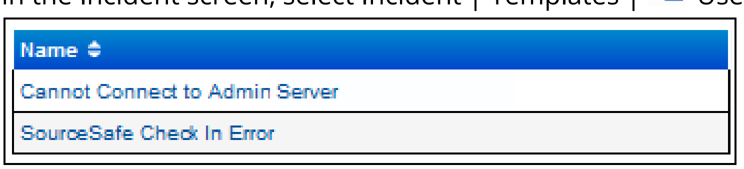
If you delete a top level template, the next level of templates below it will each become top-level templates. Any templates below those will retain their lower level templates.

If you delete a template with no lower level templates, the template will be deleted after a confirmation message. You cannot delete a template that has been used to create incidents until the associated incidents have been closed and archived or deleted and removed via the Database Maintenance agent. You can create a view with the Template Name attribute in the Incidents data source to display the name of templates used to create incidents.

Note: There is no limit to the number of templates in a hierarchy.

Using Hierarchy Templates in the Incident Screen

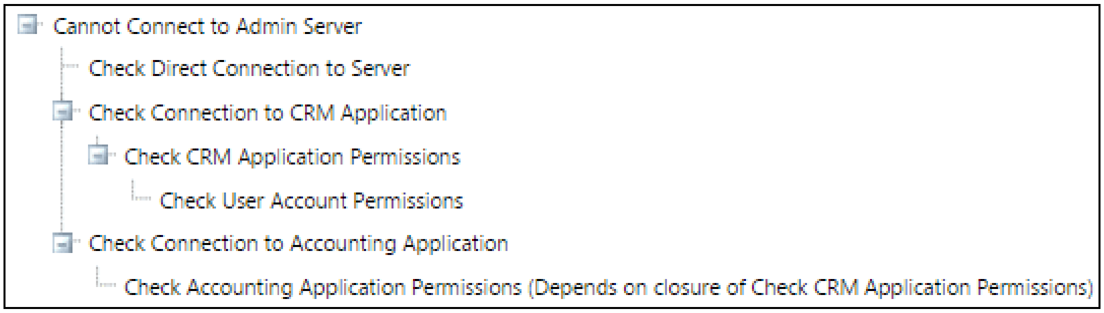
To use a hierarchy template in the Incident screen, select Incident | Templates | Use Hierarchy Template.



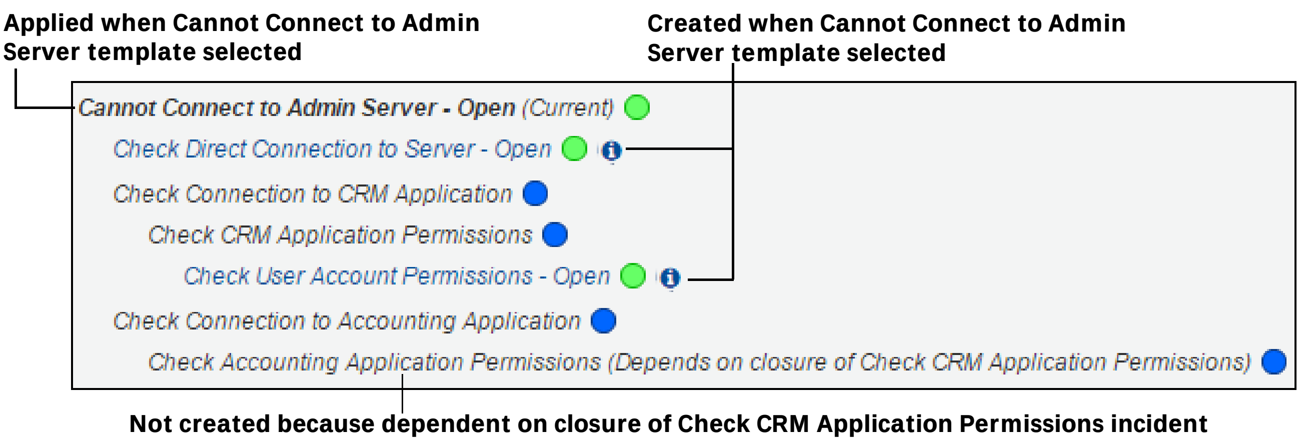
Only top-level templates appear for selection in the Incident screen and mySupport portal (if configured to be available to support representatives and customers).

When a hierarchy template is selected for an incident, the template structure is copied to the incident. The top-level template is applied to the incident and incidents are created for any templates without lower-level templates or other dependencies. If a template contains a dependency, an incident is *not* created from it until the dependent incidents are closed.

Template Hierarchy



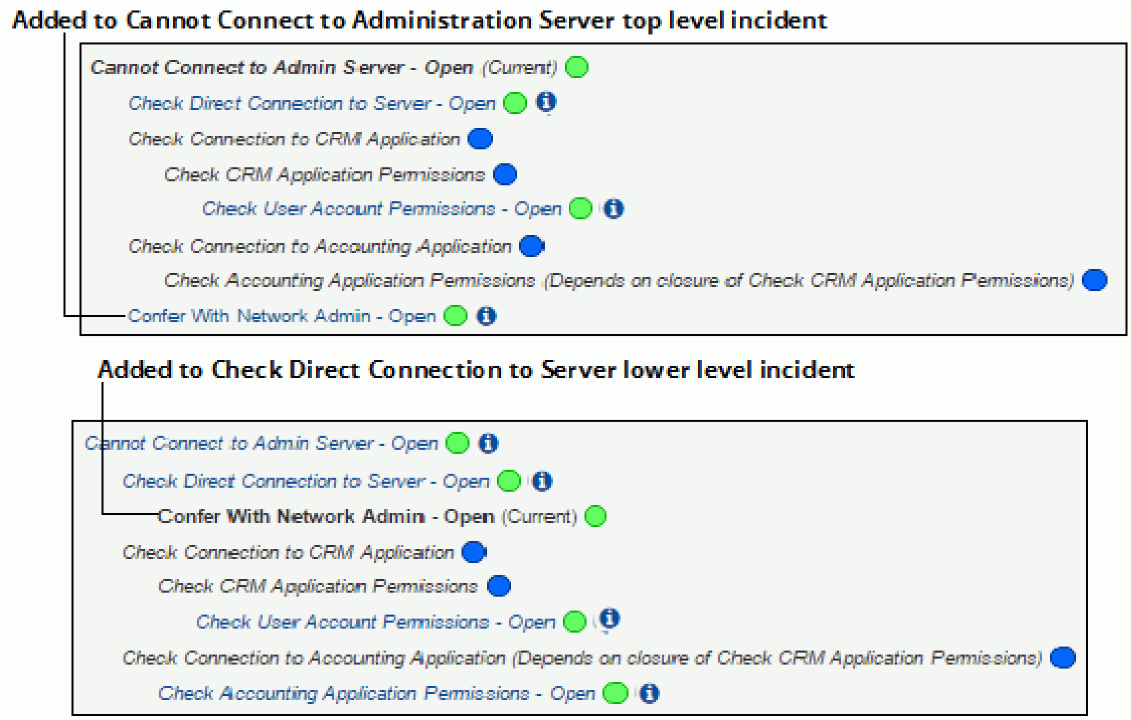
When Template is Selected in Incident Screen



Note: If a top level incident is a scheduled incident, any lower level incidents will not be created (and the Related Hierarchy link will be inactive) until the top level incident has an Open status.

Adding Incidents to a Template Hierarchy

To add an incident or an incident and its hierarchy to an incident in a hierarchy template structure, you can select New | Incident | Related Incident or use the Add options under Incident | Hierarchy to add an existing incident.

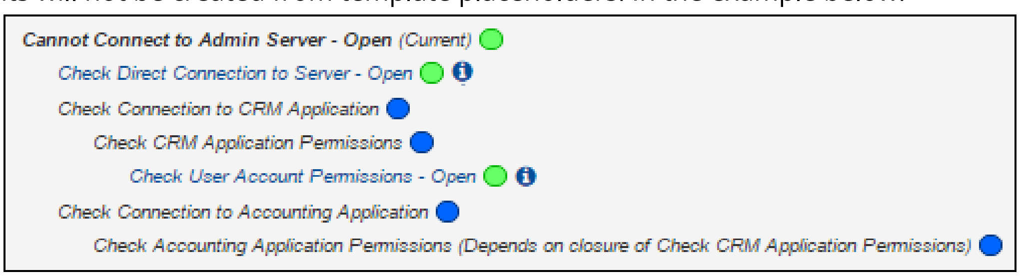


If the added existing incident contains lower level incidents, the structure is also added.

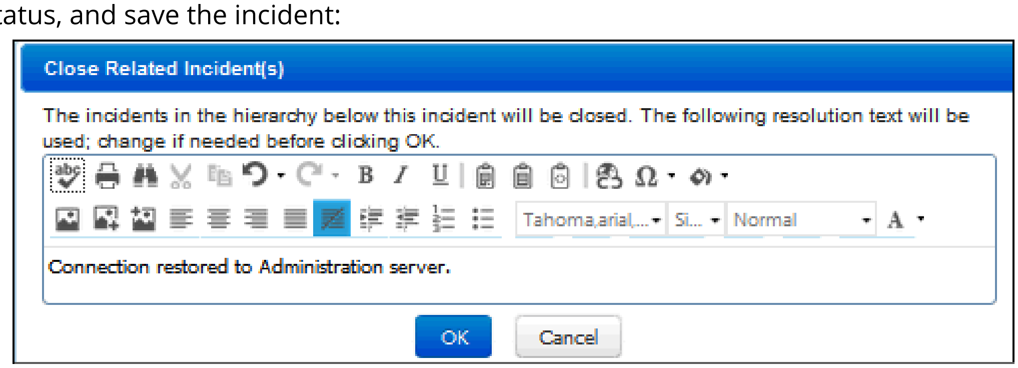
Closing Incidents in a Hierarchy Template Structure

Closing a Top Level Incident in a Hierarchy Template

If you close the top level incident in a hierarchy template structure, incidents in all levels underneath it must also close and incidents will not be created from template placeholders. In the example below:

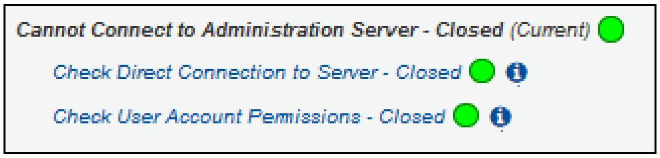


In the Cannot Connect to Administration Server incident, the following dialog appears when you enter a resolution, select a closed status, and save the incident:



You can change the resolution that will be applied to the open lower level incidents before closure. If you select Cancel in this dialog, the top level incident will remain open.

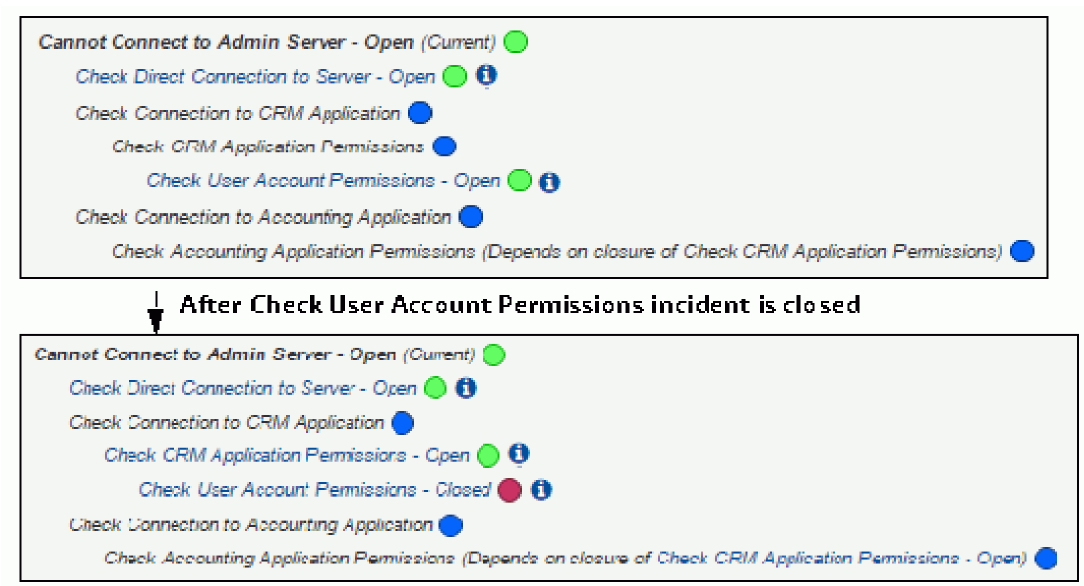
After you select OK, the hierarchy is as follows:



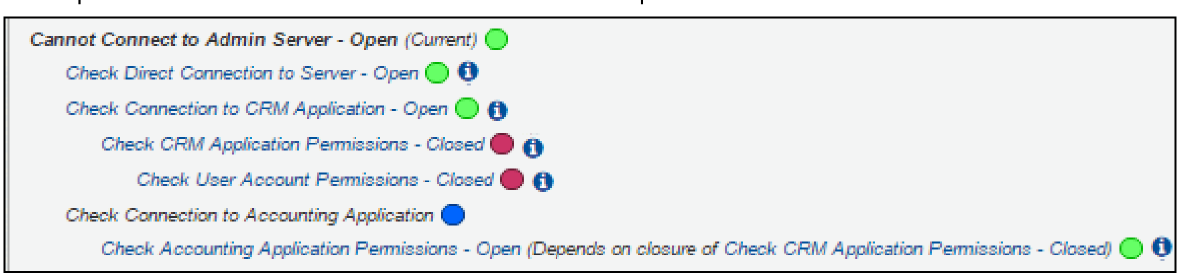
A configuration option can be set (on the Advanced tab in the Hierarchy Template screen) for a top level template to automatically close the top level incident in a hierarchy if all lower level incidents in the hierarchy are closed. The following text will be included in the resolution field: “Automatically closed after closure of all work items in the hierarchy".

Closing Lower Level Incidents in a Hierarchy

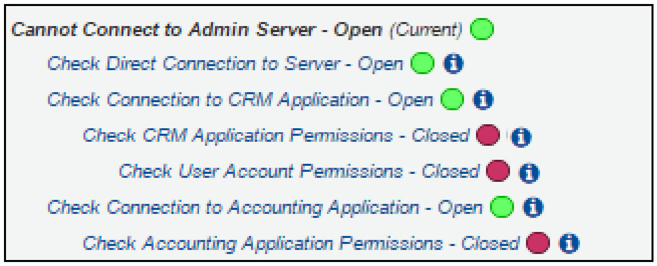
When a lower level incident in a hierarchy template structure is closed, incidents are created from templates that were dependent on closure of that incident. In the following example, after the Check User Account Permissions incident is closed, the Check CRM Application Permissions incident is created.



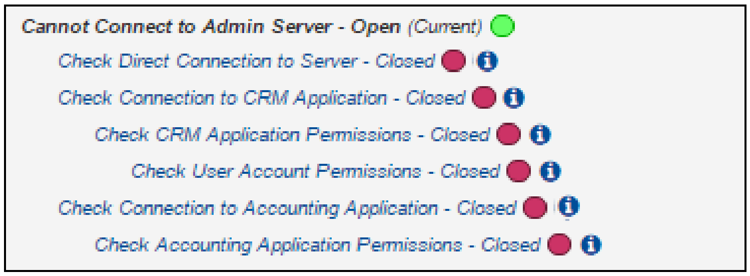
When the Check CRM Application Permissions incident is closed, an incident will be created from the Check Connection to CRM Application template. An incident will also be created from the Check Accounting Application Permissions template because the incident on which it was dependent is closed.



When the Check Accounting Application Permissions incident is closed, the Check Connection to Accounting Application incident is created.

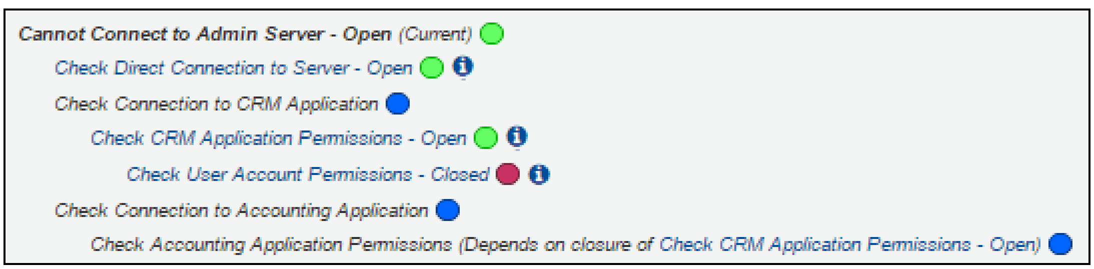


When the Check Direct Connection to Server, Check Connection to CRM Application, and Check Connection to Accounting Application incidents are closed, the Cannot Connect to Admin Server incident w be closed.

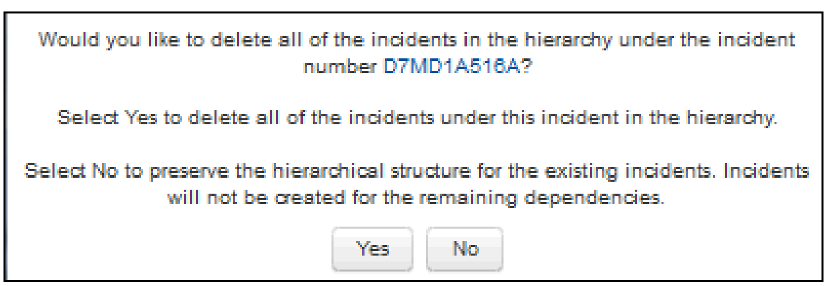


Deleting Lower Level Incidents Hierarchy Template Structure

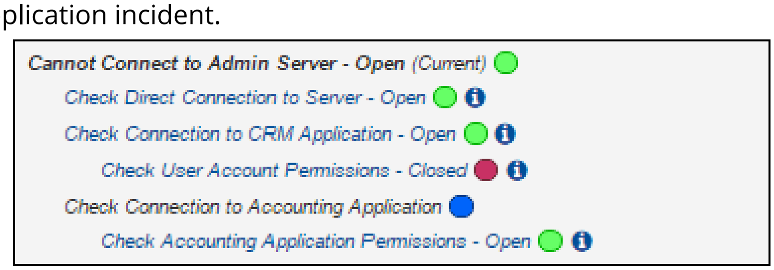
If you delete an incident in a lower level of a hierarchy template structure, you have the option of deleting the incident's lower level incidents. Incidents will be created from template placeholders above it if dependencies are met. In the following example:



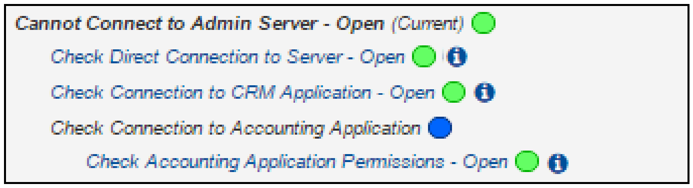
If you delete the Check CRM Application Permissions incident, the following appears:



- If you select No (you wish to retain its lower level incidents), the lower level incidents will go up a level. The structure will appear as follows; note that the Check User Account Permissions incident is now below the Check Connection to CRM Application incident.

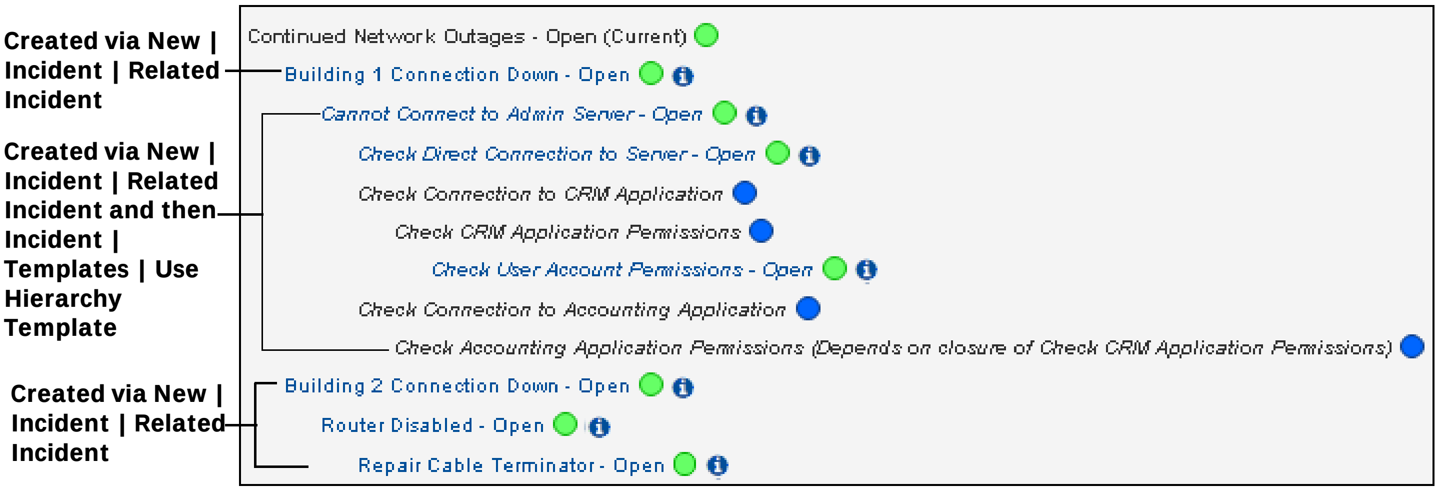


- If you select Yes (you wish to delete its lower level incidents), the lower level incidents will be deleted. The structure will appear as follows.

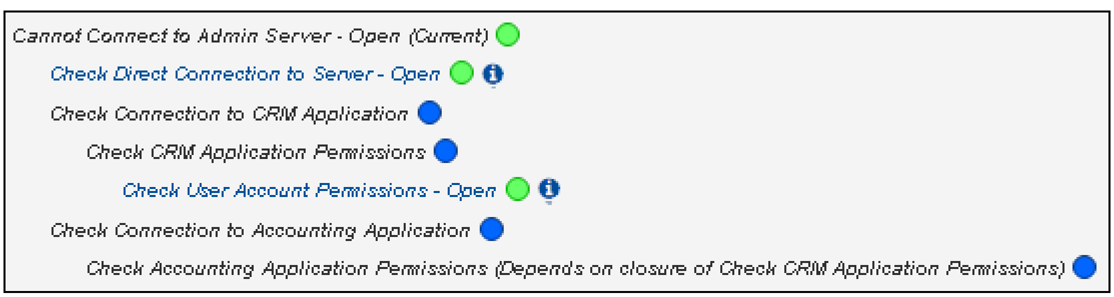


In both cases, an incident was created from the Check Connection to CRM Application template placeholder, which was above the deleted incident.

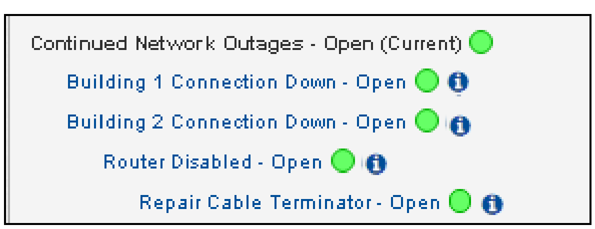
You can remove a top level incident in a hierarchy structure. In the following example:



In the top level incident in the incident created from a hierarchy template, the Cannot Connect to Admin Server incident, you can select Incident | Hierarchy | Remove Incident and Dependent Hierarchy to remove it from the larger hierarchy structure. The Cannot Connect to Administration Server incident and its lower levels will become a standalone structure as shown below:

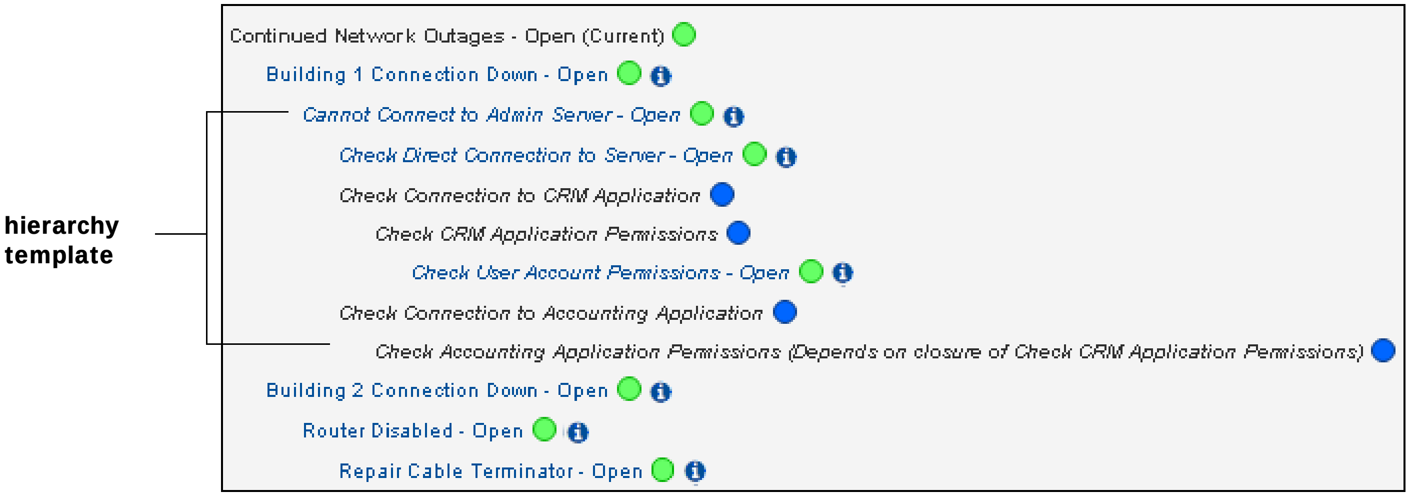


The rest of the structure would appear as follows:

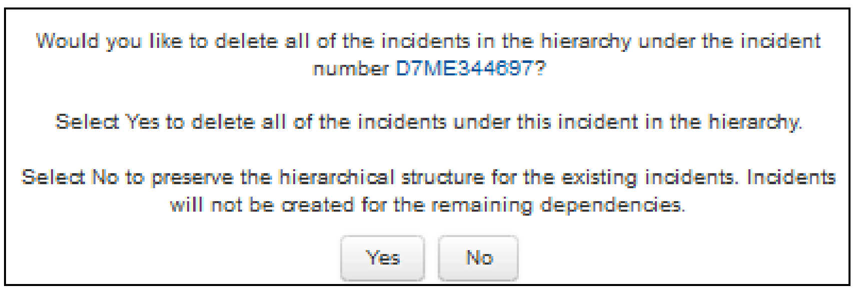


Deleting a Top-Level Incident in a Hierarchy Template Structure

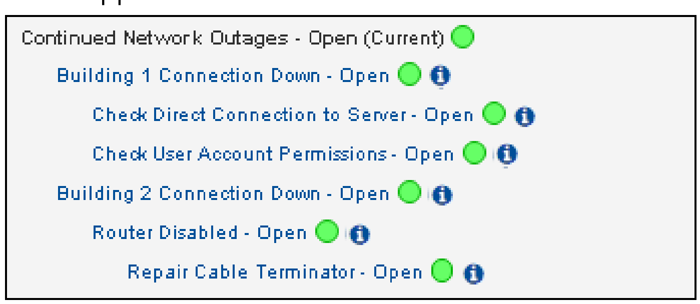
When you delete a top level incident in a hierarchy template, you'll have the option of retaining its lower level incidents. In the example below:



If you delete the Cannot Connect to Administration Server incident, the following prompt appears:



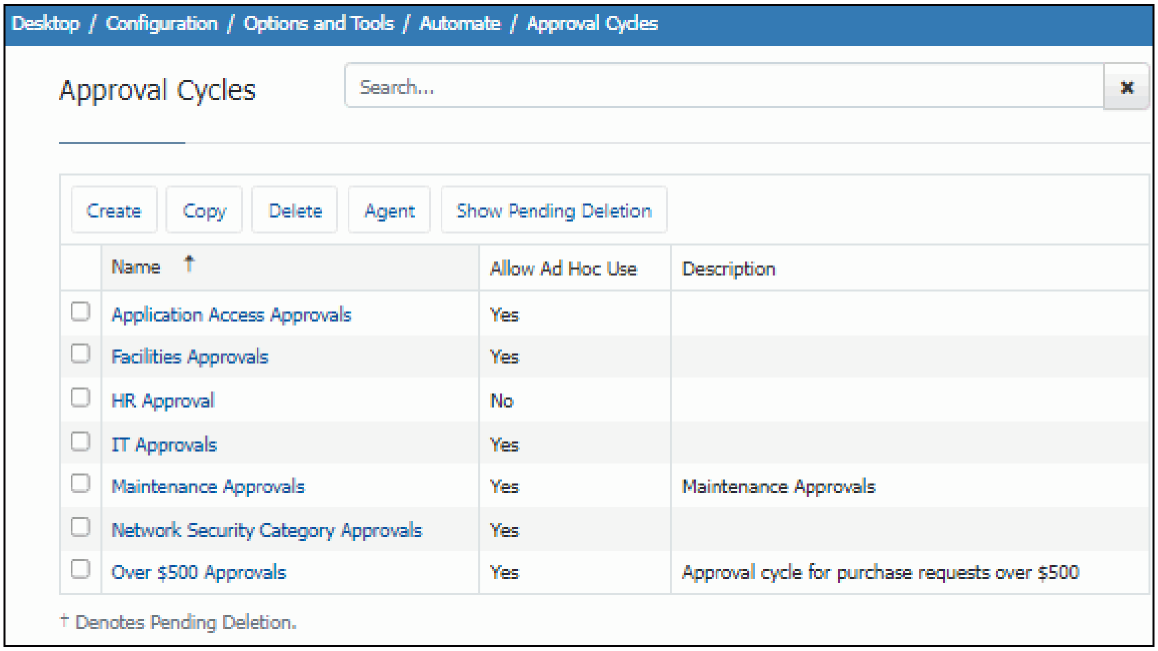
If you select No, the structure would appear as follows.



When an incident structure contains both a dynamic hierarchy (created via the New | Incident | Related Incident and Incident | Templates | Use Hierarchy Template functions) and a hierarchy template structure, actions of the incidents in the dynamic hierarchy do not affect the incidents in the hierarchy template structure above it.

Configuring Approval Cycles

The Approval feature requires work items to be approved by designated approvers before most functions can be performed. (You can, however, enable modifications via a setting in the Incident, Change, and Purchasing Basics screens.)

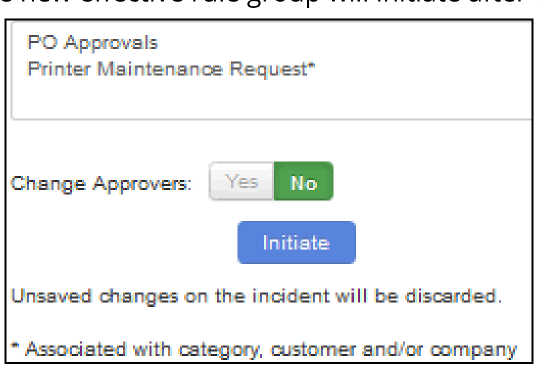


You can use the Show Pending Deletion link to display records that have been deleted by an iSupport user but are retained in the system because of references to other records (incidents, correspondence, etc.) The Database Maintenance agent ultimately removes these records. When the Show Pending Deletion link is selected, records that are pending deletion will display with a cross symbol.

Approvers can be support representatives or customers, and delegates can be set. See "Specifying Approvers" on page 97 for more information.

Approval cycles are applied to incidents, changes, and purchase requests as follows:

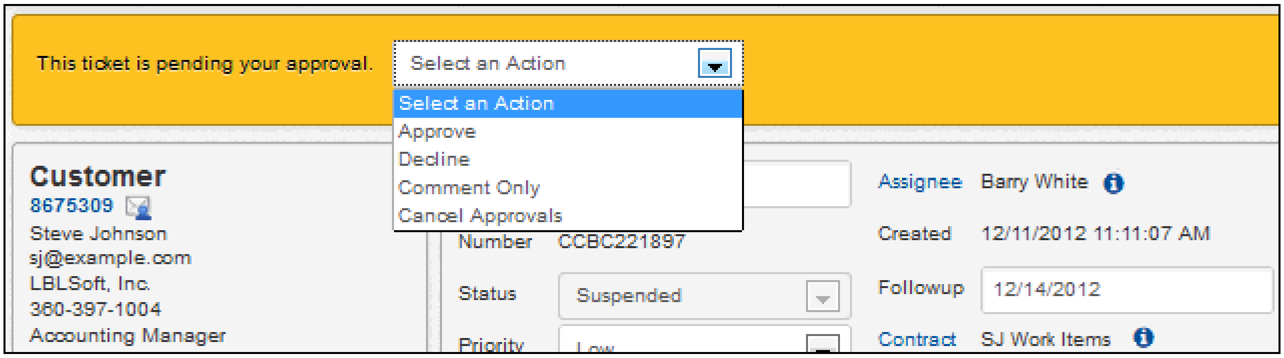
- The customer, company, selected category (for incidents and changes), or template has an associated approval cycle.
- A rule that initiates an approval cycle is in effect for an incident, change, or purchase that meets configured conditions. Multiple cycles can be specified for a rule group but only one cycle can be active at a time, and approval functionality is not affected by the business hours configured for a rule group. If a canceled or completed cycle needs to be run again, the rule it is linked to will need a condition that can be set on the work item or the support representative can initiate an ad hoc approval. If the cycle associated with a category is specified, the lowest level category is checked and if no cycle is associated, the next (higher) level is checked, and so on up the category hierarchy.
- An ad hoc approval cycle is selected by the assignee via the Ad Hoc Approval option. Note that an active ad hoc approval cycle for an incident or change will not be cancelled when the effective rule group changes; any approvals that are defined by the new effective rule group will initiate after the ad hoc cycle is approved.



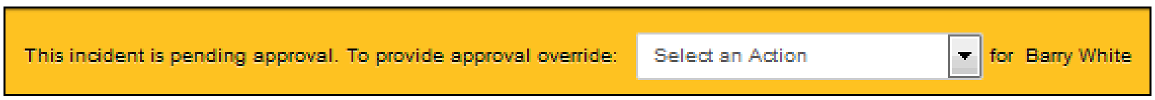
The status of the work item will change throughout the process as configured for the initial status, final approval, final decline, and cancellation. Notifications can be sent for approval events and verdicts.

Specifying a Verdict

When an approval cycle is in effect, an alert bar will appear with an action dropdown for specifying a verdict and/or comments for the next approver(s) in the current approval cycle or support representatives with approval override.



The following will appear if a support representative is not the current approver but has approval override:



The alert bar will only include a message stating "This <*work item type*> is pending approval" for support representatives who do not have approval override or are not the next approvers for the current cycle.

The following can be selected:

- **Approve** - If it is a concurrent cycle, the approval cycle will stop if the number of Approve verdicts specified for the cycle is reached. All approvers must specify an approval for a serial cycle.
- **Decline** - A Decline verdict requires an entry in the Comments field. In a serial cycle, the cycle reaches final decline if one of the approvers sets a verdict of Decline. In a concurrent cycle, the approval cycle will stop if the number of Decline verdicts specified for the cycle is reached. If any approval cycle results in a Decline verdict, no further cycles will apply.
- **Comments Only** - When a Comments Only verdict is specified, the comments will be included in notifications sent to designated recipients.
- **Cancel Approvals** - A Cancel Approvals verdict requires an entry in the Comments field, and the comment will be included in the Approval Audit History entry. If the Cancellation Status configured for the approval cycle is a Closed status, the comment is appended to the text in the Resolution field (for incidents), Results field (for changes), or Comments field (for purchase requests). An approval cycle can be cancelled by the customer or any support representative with Edit permission (whether or not they are an approver or have approval override).

A reminder notification can be configured to be sent a specified number of hours after the initial approval request is sent; it can be configured to be sent repeatedly until a verdict is specified.

If the status is changed to Closed via data override, the cycle will be cancelled and notifications will not be sent. Note that if an incident or change is reopened, approvals do not automatically restart.

If a rule group-required cycle is completed or canceled, the Initiate Ad Hoc Approval option will be available for initiating another approval cycle.

Configuration Overview

Do the following to configure approvals:

- Enable approval functionality via the Global Settings screen.

- Configure approval cycles via the Options and Tools | Automate | Approval Cycles screen. You can designate approvers, assign default status levels, and create customized notifications for approval events.
- Approval cycles are automatically initiated via rules in the rule group that is in effect for a work item. Use the Rules and Rule Groups screens to configure the rules that will trigger either an initial approval cycle or a cycle associated with a category, customer, template, or company.
- Configure additional approver options:
  - Enable support representatives to override an approval. Use the Support Representative Profile screen to enable a support representative to specify a verdict if not designated as an approver for the cycle in effect.
  - In the Support Representative Profile and Customer Profile screens, you can select an approver delegate who can specify a verdict in place of the approver(s) designated for an approval cycle.
  - Use the Allow Approvers to Edit During Approval Cycle field in the Incident, Change, and Purchasing Feature Basics configuration screen to enable support representatives designated as approvers (or those with Approval Override) to have access to all functionality except Status in records in an approval cycle. Use the Recipient Notification Mappings field to select the recipients and notifications to be sent to others in the cycle that have previously approved the record.
  - If using the customer's approver for a cycle, designate approvers via the Customer Profile screen.
- If applicable, associate approval cycles with categories (for incidents and changes), customers, companies, and templates.
- If customers will be approving, add the Approval button to the applicable display page via the mySupport | mySupport Options screen.

Creating an Approval Cycle

Use the Approval Cycle screen to configure approval cycles consisting of serial or concurrent approvers, notifications, and statuses to assign while the cycle is in effect, final approval/decline, and cancellation. The same approval cycles are used with incidents, changes, and purchase requests; however, you can designate statuses and notifications that are specific to each type of work item.

Name - Enter a name for the approval cycle.

Description - Enter a description of the approval cycle.

Available for Ad Hoc Use - Select Yes to enable the approval cycle to be available in the Incident, Change, and Purchase Request screens for support representatives to initiate on saved records.

Type of Approval - Select:

- Serial to enable approvers to specify a verdict one at a time in a designated order. All approvers must approve the incident or change (if enabled), and the cycle will stop if an approver specifies a Decline verdict.
- Concurrent to enable all approvers to specify a verdict at the same time. The cycle will complete after the number of Approve verdicts is equal to the number in the Number of Verdicts Required for Final Approval field. The cycle

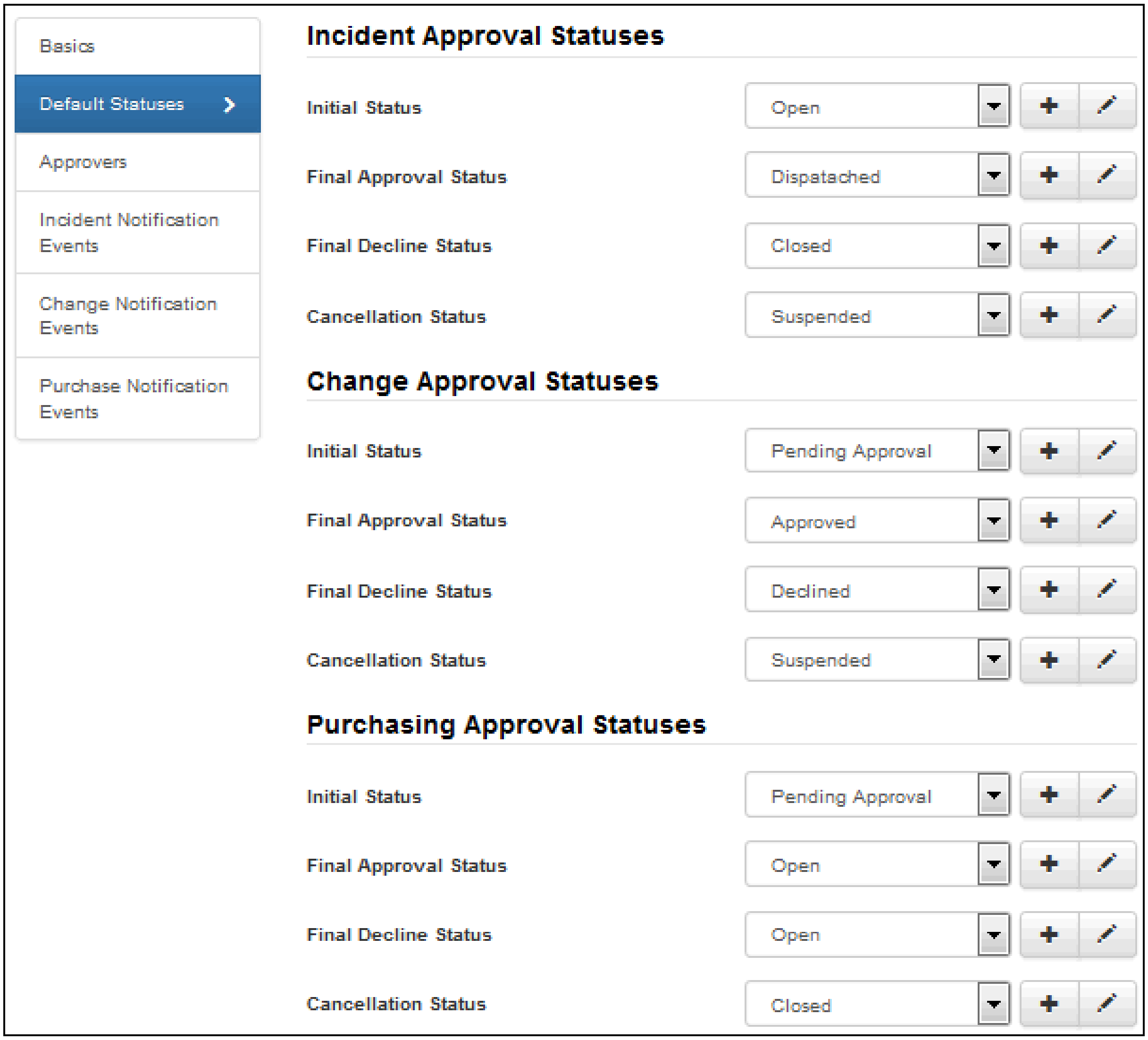
will stop after the number of Decline verdicts is equal to the amount specified in the Number of Verdicts Required For field.

Number of Verdicts Required for/Final Approval/Final Decline - This field appears if Concurrent is selected in the Type of Approval field.

- In the Final Approval field, select the number of Approve verdicts needed to complete the cycle.
- In the Final Decline field, select the number of Decline verdicts needed to stop the cycle.

Default Statuses

Use the Default Statuses tab to assign a status to each stage of the approval cycle.



Default Approval Incident/Change/Purchase Statuses - Select the status to assign at each stage of the approval cycle. Use the Create New and View/Edit options to access the applicable Custom Status Label screen.

- In the **Initial Status** field, select the status to assign when an incident with the rule group is initially saved.
- In the **Final Approval Status** field, select the status to assign when:
  - For a serial cycle, all approvers have specified an Approve verdict.
  - For a concurrent cycle, the number of Approve verdicts is equal to the number in the Number of Verdicts Required for Final Approval field.
- In the **Final Decline Status** field, select the status to assign when:
  - For a serial cycle, an approver specifies a Decline verdict.

- For a concurrent cycle, the number of Decline verdicts is equal to the number in the Number of Verdicts Required for Final Decline field.
- In the **Cancellation Status** field, select the status to assign when a support representative with Incident Edit permission or customer assigned to an incident specifies a **Cancel Approvals** verdict.

Specifying Approvers

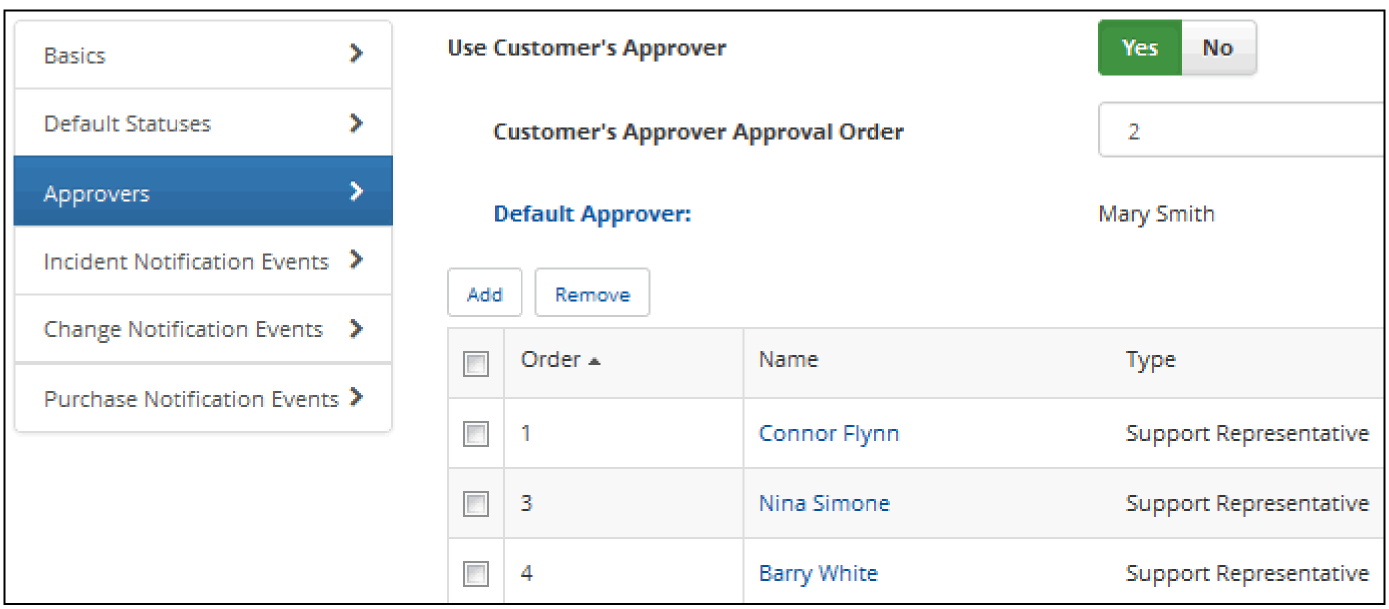
Use the Approvers tab to specify the approvers for the approval cycle. Note that a support representative can change the approvers if an ad hoc approval cycle is initiated.

A customer can be assigned an approver (support representative or another customer) in their Customer Profile record; if using Active Directory integration as a customer data source and a record in Active Directory has a value in the Manager field, the AD manager will be populated in that field. An approver delegate can be set for a customer in their Customer Profile record; if enabled in the mySupport Portal Options screen, a customer can designate their own approver delegate via the mySupport Portal Account Settings screen.

Approver delegates can specify a verdict on work items pending approval for the specific customer or support representative to which they are a delegate.

If a support representative is designated as an approver, any lower level permissions are overridden (for example, if the representative does not have permission to edit but is designated as an approver, a verdict can still be submitted). Approver override can be enabled for a support representative in their profile; this allows them to specify a verdict on any work item pending approval that they can access. Another support representative can be designated as a delegate for a support representative via their profile, and a support representative can designate their own delegate via the Preferences screen on the Desktop.

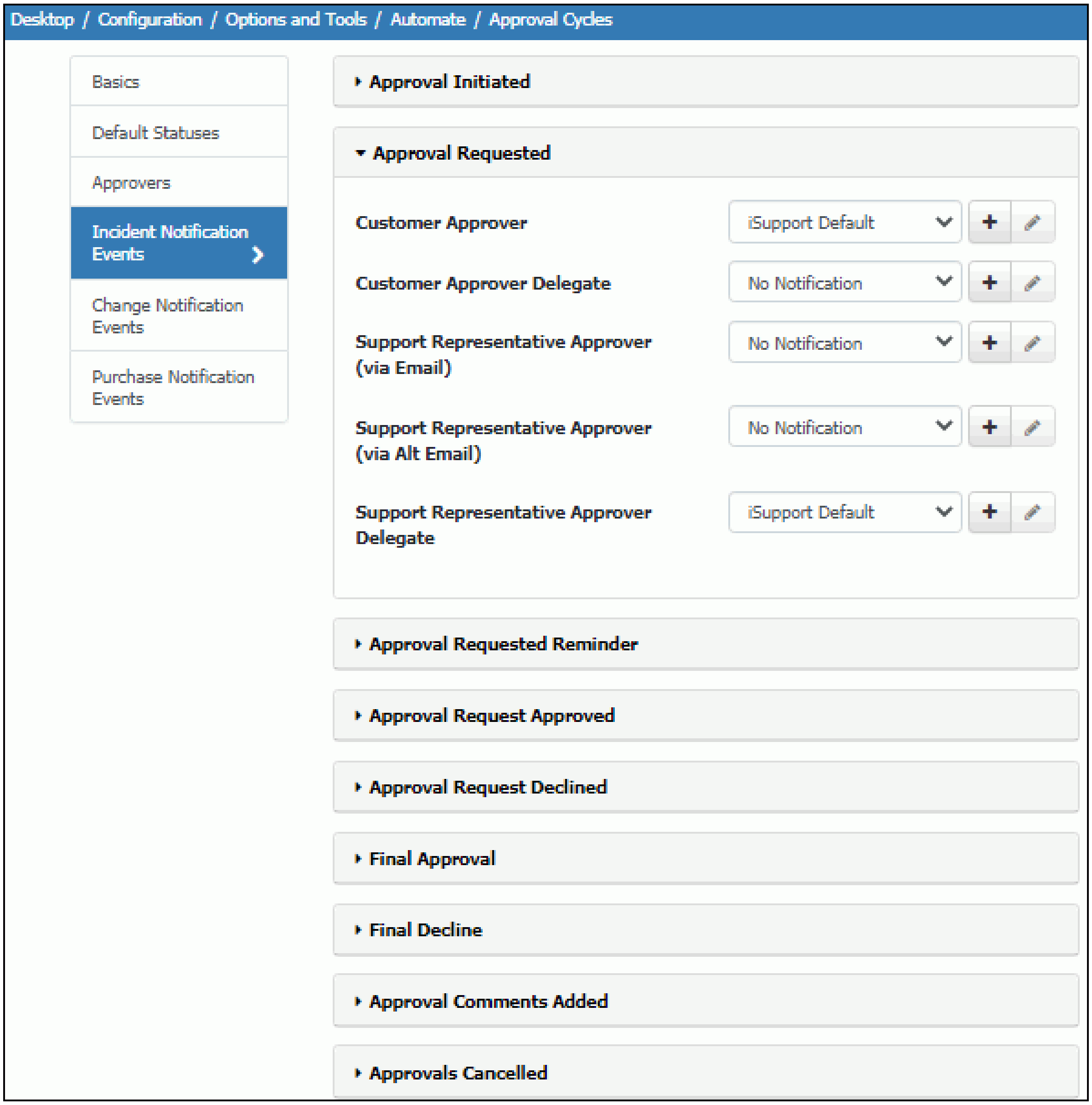
In the Use Customer's Approver field on the Approvers tab in the Approval Cycle configuration screen, select Yes if you wish to use the approver specified in the Approver field in the Customer Profile screen. If it is a serial cycle, use the Customer Approver Approval Order field to specify the position of the customer's approver in the order for the cycle. Use the Default Approver field to specify an approver to use if the Approver field is blank in the Customer Profile screen. Click the Add link to select support representative or customer approvers. Be sure to click the Add button at the bottom of the screen when finished. The selected approvers appear in a list; if it is a serial cycle, you can change the order in which approvers will specify a verdict by clicking the approver's name to display a numeric dropdown field in the Order column.



Configuring Approval Notifications

Use the Notifications tab to configure notifications to be sent for all approval events. For each event and recipient you can select iSupport's default notification, a predefined custom notification, or you can select Create New Custom

Notification to access the Custom Notifications screen to create one or view default notification text. Notification recipients can include both support representatives and customers, and the default text is different for each.



Approval Initiated - Select the recipients and notifications to be sent when the <*Incident/Change/Purchase*> is saved with an associated approval cycle.

Approval Requested - Select the recipients and notifications to be sent when the applicable work item requires approval. You can select Customer Approver, Support Rep Approver (via email), and/or Support Rep Approver (via alternate email).

If a concurrent cycle is in effect, the notification will be sent to all designated approvers in the cycle. For example, if both Customer Approver and Support Rep Approver are selected, the notification will be sent to all of the customer approvers and support representative approvers for the cycle.

If a serial cycle is in effect, the notification will be sent to the next approver in the cycle.

Approval Reminder - This section appears when the Approval Requested Reminder Event is selected. Select Yes to enable a reminder notification to be sent on an interval basis if the approvers have not submitted a verdict after the approval request is sent.

Approval Requested Reminder - This section appears when the Approval Requested event is selected. Select Yes to enable a reminder notification to be sent if the approvers have not submitted a verdict after the approval request is sent.

Use the **Send Reminder <x> Hour(s) After Approval Request Sent** field to specify the number of hours after the approval request is sent in which to send the reminder notification. Use the Maximum Number of Reminders field to enter the maximum number of times in which the notification should be sent.

Select the recipients and notifications to be sent a reminder notification on an interval basis if the approvers have not submitted a verdict after the approval request is sent.

Notifications are sent on the schedule of the Approval Reminder agent on the Agents tab; be sure to enable and set the interval for this agent.

Request Approved - Select the recipients and notifications to be sent when an approver or support representative with approval override submits a verdict of Approved.

Request Declined - Select the recipients and notifications to be sent when an approver or support representative with approval override submits a verdict of Declined.

Final Approval - Select the recipients and notifications to be sent when an approver or support representative with Approval Override submits a verdict of Approved **and**:

- If a concurrent cycle is in effect, the number of approval verdicts is equal to the number specified in the Number of Verdicts Required for Final Approval field on the Basics tab.
- If a serial cycle is in effect, the approver is the last in the cycle.

Final Decline - Select the recipients and notifications to be sent when an approver or support representative with Approval Override submits a verdict of Declined:

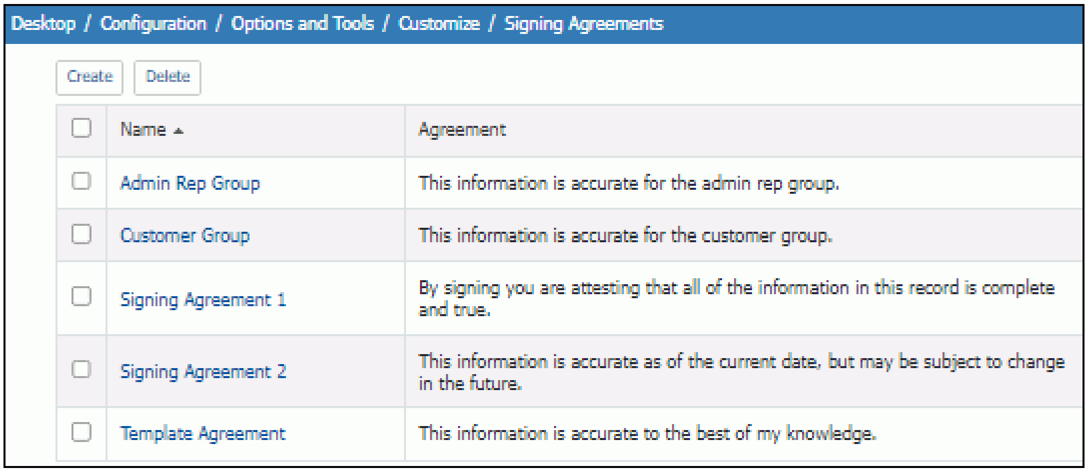
- If a concurrent cycle is in effect, the notification is sent when the number of Decline verdicts is equal to the number specified in the Number of Verdicts Required for Final Decline field on the Basics tab.
- If a serial cycle is in effect, the notification is sent whenever a Decline verdict is submitted.

Comments Added - Select the recipients and notifications to be sent when an approver or support representative with Approval Override submits a comment.

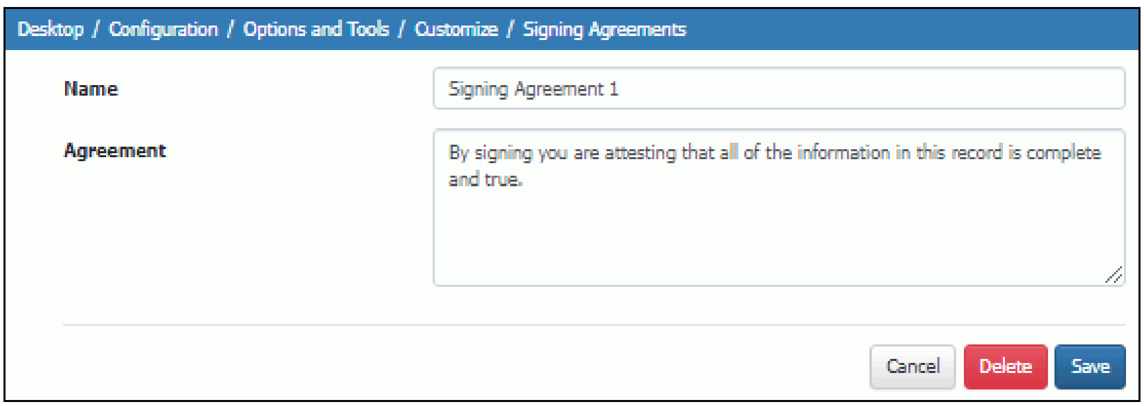
Approval Canceled - Select the recipients and notifications to be sent when the approval cycle is canceled by the customer or a support representative with <*Incident/Change/Purchase*> Edit permission.

Configuring Signing Agreements

Signing agreements display details in the Sign dialog in the Incident and Change work item screens. Signing agreements can be associated with customer and support representative groups, categories, and incident and change templates.



Use the Configuration | Options and Tools | Customize | Signing Agreement configuration screen to create a signing agreement.



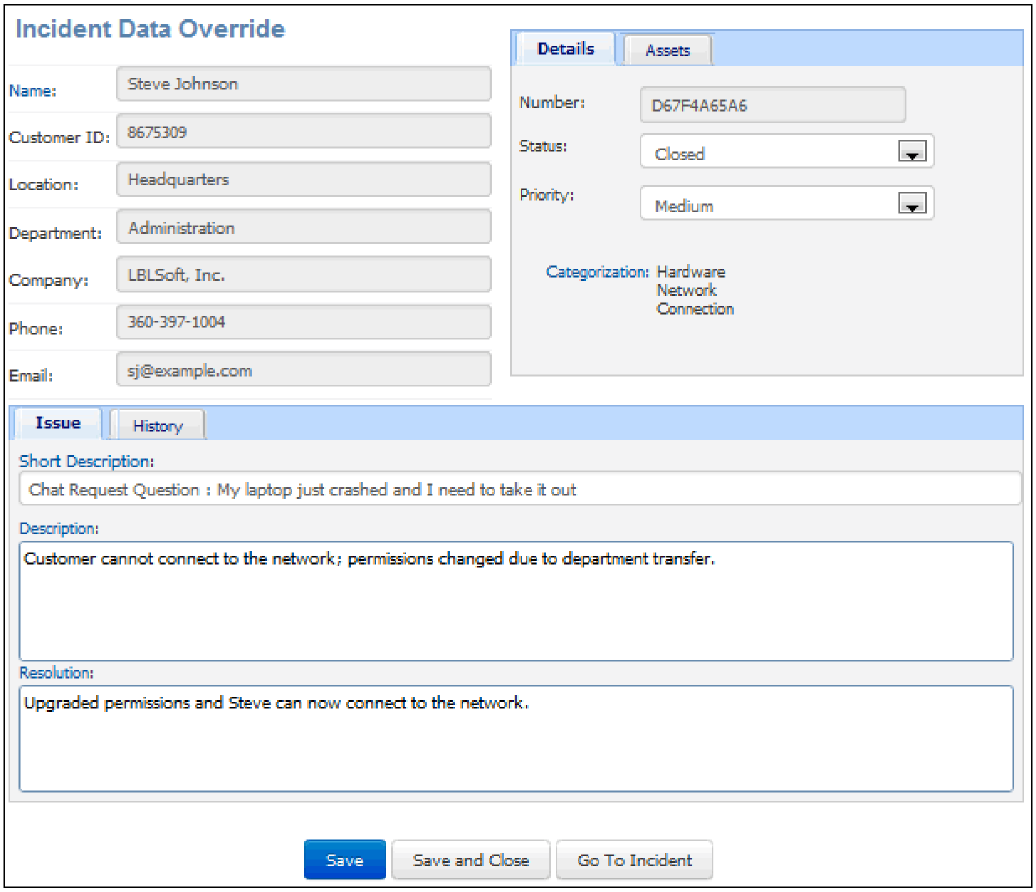
If an incident or change involves more than one associated signing agreement (associated with the group, category, or template), all will be included in the Sign dialog in a dropdown for selection. Note that “Blank” is also included for displaying no text above the signing line.

When the Sign dialog has been completed by the user, the text and signature are saved as an image in an attachment and a notation with the name of the signature agreement is included in the History field. Note that this feature is not available for mySupport.

Using the Data Override Feature for Incidents, Problems, and Changes

Use the Options and Tools | Administer | Data Override feature to overwrite fields on any saved incident, problem, or change. When a change is made using this feature, it will be logged in the Audit History field and notifications will be suppressed. If an approval cycle is in effect and the status is changed to Closed via data override, the cycle will be canceled and notifications will not be sent.

To access this feature, use the Override Data option on the applicable menu. It is available if the Allow Data Override field is enabled in your Rep Profile record.



Configuring Calendar and Meeting Integrations

You can configure integration with Google Calendar, Google Meet, Microsoft Outlook, Microsoft 365 Teams and Planner, and Zoom to display an option in the Incident, Problem, Change, and Customer Profile screens for initiating a meeting.

Note: iSupport utilizes or integrates with a number of third party applications and resources; changes in these external applications and resources may have a negative impact on functionality in iSupport. Depending on the nature and degree of the change, iSupport will, at its discretion, revise the current version of iSupport or make a corrective change in a future release of iSupport.

Google Calendar/Meet

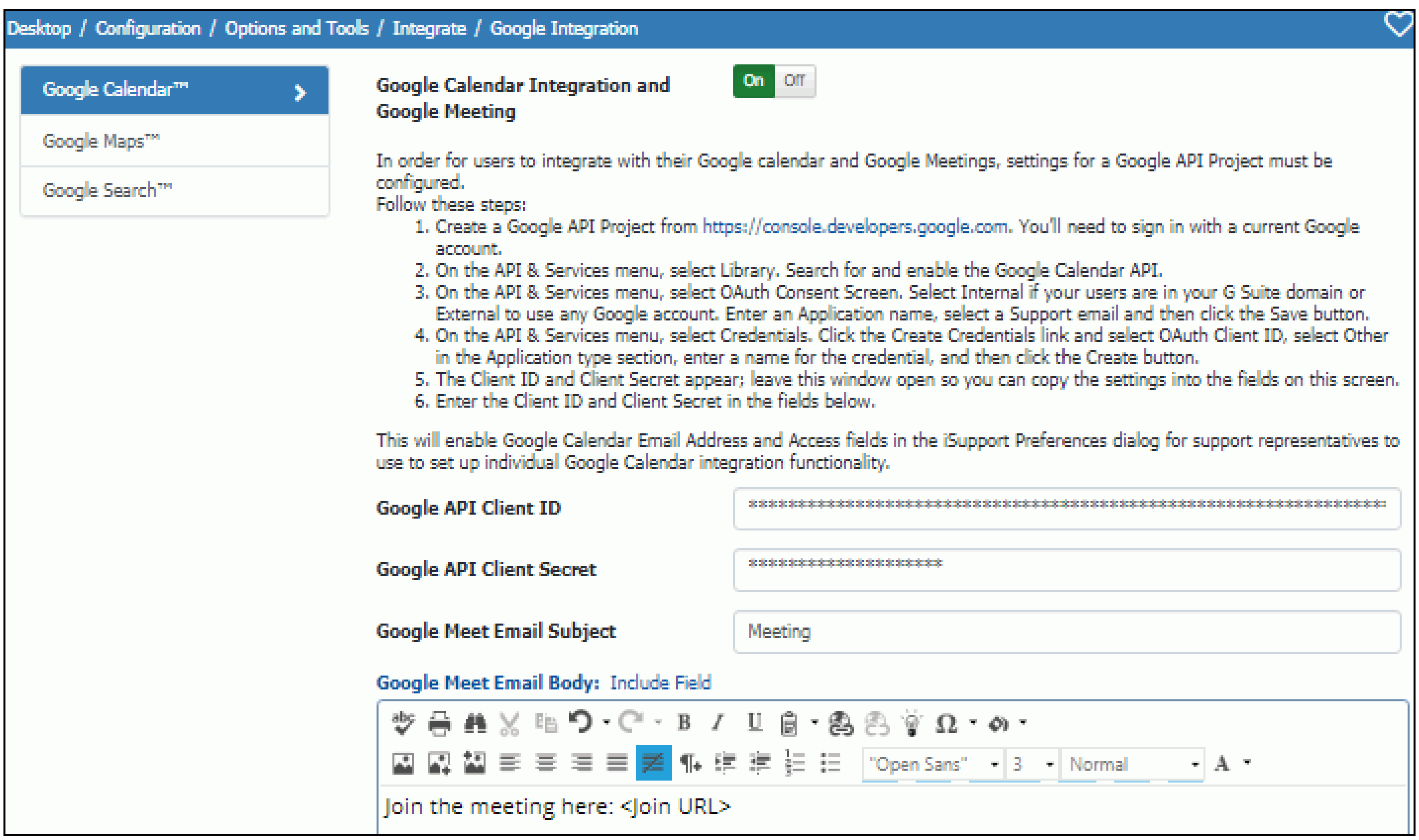
Set up Google Calendar integration in the Options and Tools | Integration | Google Integration screen to enable users to access their Google Calendar for the Calendar option on the Desktop and mySupport portals, a New Meeting option in iSupport entry screens for scheduling a Google Calendar meeting, and a Google Meet option to appear in work item screens for starting a meeting.

With Google Calendar, support representatives can view the schedules of meeting attendees, create a meeting to be added to their calendar, and configure a notification to be sent to the meeting attendees.

When the Google Meet option is selected, the Generate Join URL dialog will appear for you to enter the topic, share the Join URL, and email a link to the meeting. The Share Join URL option will display a dialog with the URL and an option to start the meeting; the Email Link option will display the Correspondence dialog.

The timeframe (work hours) during which support representatives are available to be scheduled via iSupport can be set via the Desktop or Support Representative Profile screen. On the Desktop, a support representative can view their calendar via the Calendar component and work item-specific calendars can be viewed from action menu. Administrators can view support representative calendars via the Support Representative Profile screen.

On the Google Calendar tab, follow the steps on the screen and copy the Google API Client ID and Secret into the applicable fields. Enter the subject body of the email to be sent for the scheduled meeting; use the Include Field link to add field values regarding the meeting.

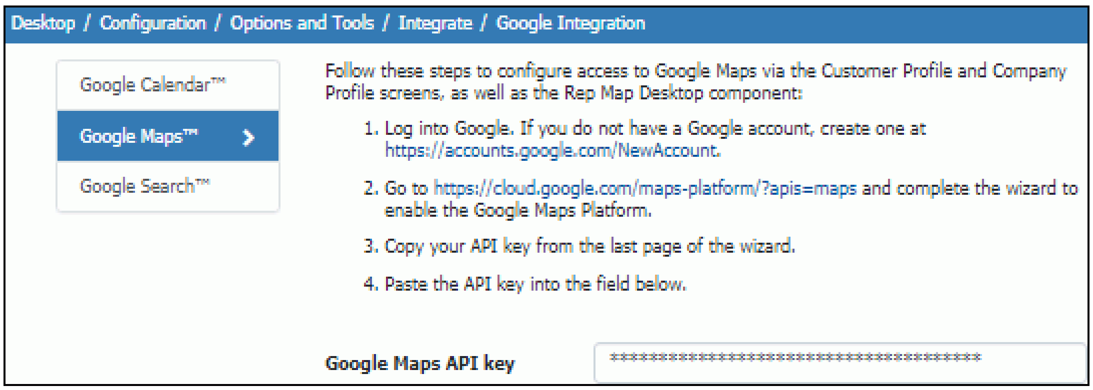


Note: Support representatives will need to use the Google Calendar Email Address and Google Calendar Access fields on the Details screen in the Preferences dialog to enable access to their calendar(s) and set the work day hours during which they are available to be scheduled via iSupport. (The dates/times outside of work day hours are designated as "Unavailable" in the calendars displayed via iSupport.) After clicking the Grant Access link, a Google dialog will appear for the support representative to allow iSupport access to their calendar and a code will be provided. The Grant Access to Your Google Calendar dialog will appear in the Preferences screen with an Auth Code field for pasting the code. After clicking Continue, “Access Granted” will appear in the Google Calendar Access field.

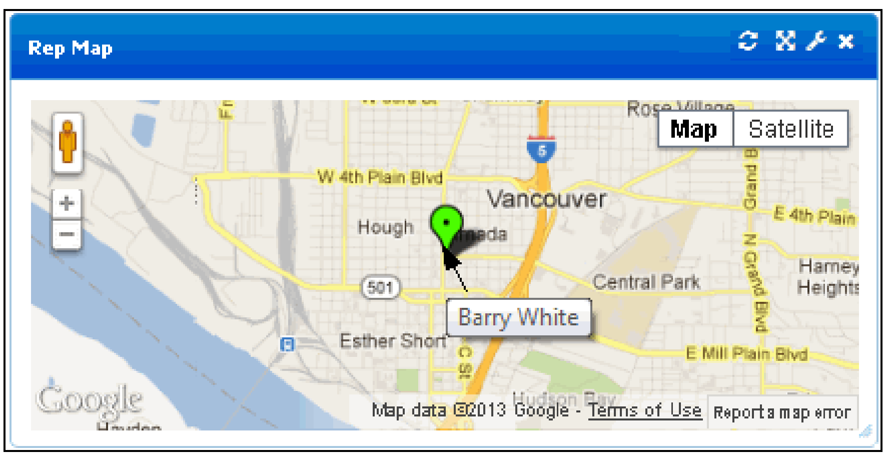
Google Meet meetings can be included in work item screens; add the Google Meetings field to a work item screen layout via the Layouts configuration screen.

Google Maps

Use the Google Maps tab in the Options and Tools | Integration | Google Integration screen to enable access to Google Maps via the Customer Profile and Company Profile screens, as well as the Rep Map Desktop component. Follow the steps on the screen and enter the Google Maps API key.

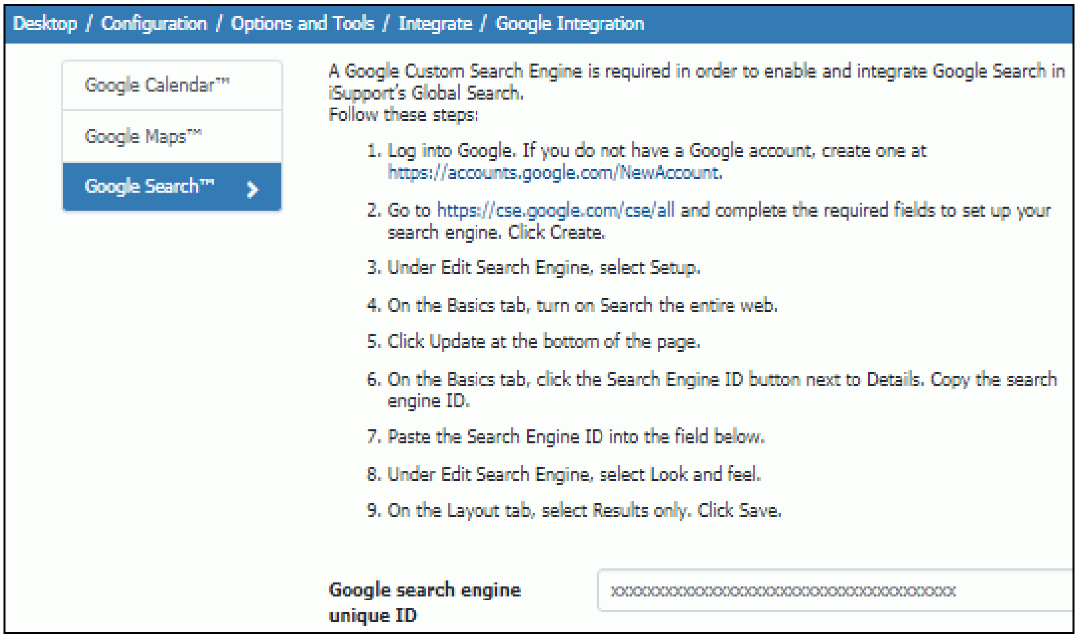


Maps will appear as shown in the example below.

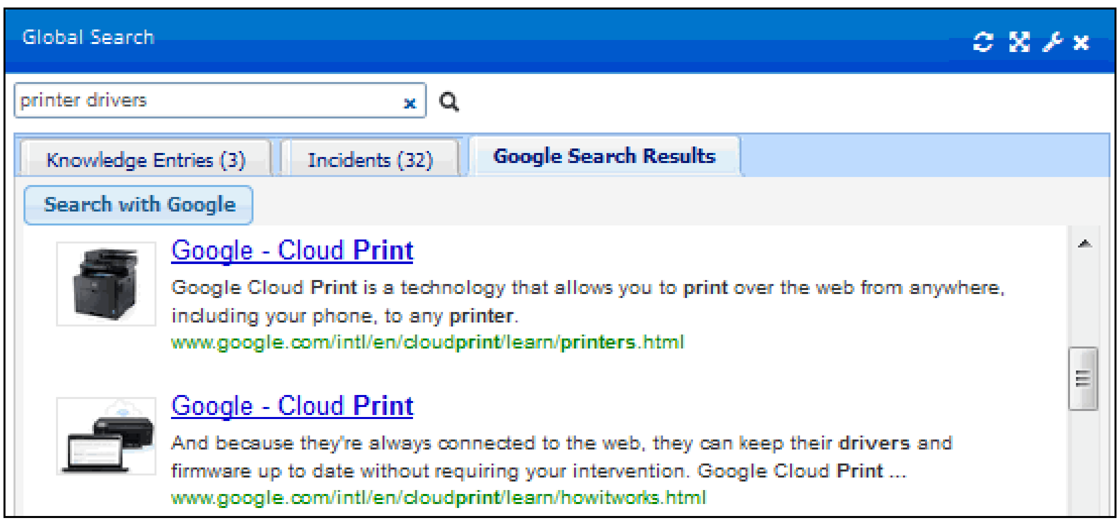


Google Search

Use the Google Search tab in the Options and Tools | Integration | Google Integration screen to enable access to Google Search throughout the application. Follow the steps on the screen to create a Google Custom Search Engine, copy the unique ID from the Google Custom Search Engine screen, and enter it in the Google Search Engine Unique ID field.



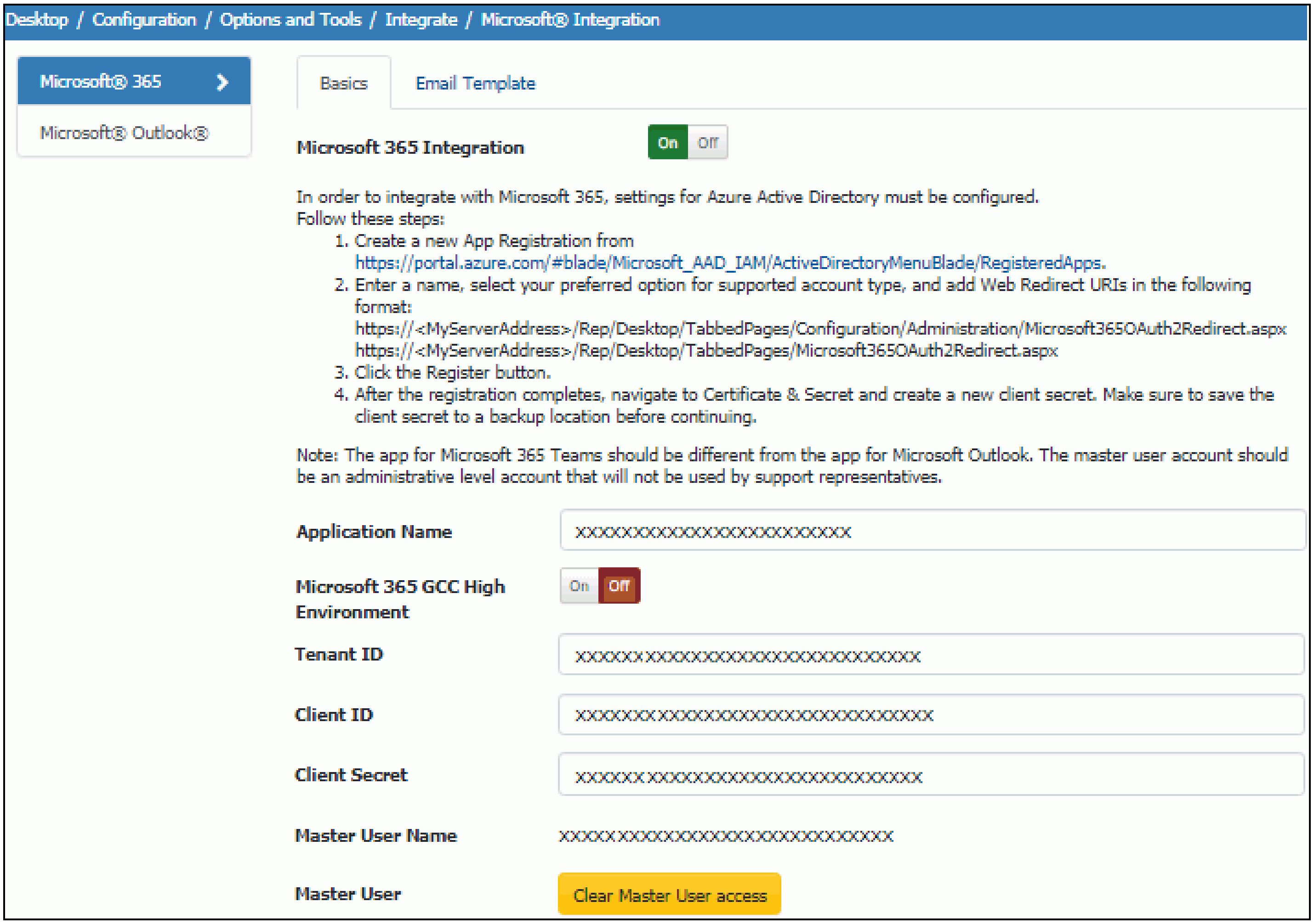
The Google Search tab will appear in the Global Search component as shown in this example.



Microsoft 365 Integration

Use the Microsoft 365 tab in the Options and Tools | Integration | Microsoft Integration screen to enable the Microsoft Teams Planner component on the iSupport Desktop for viewing and accessing scheduled and unscheduled

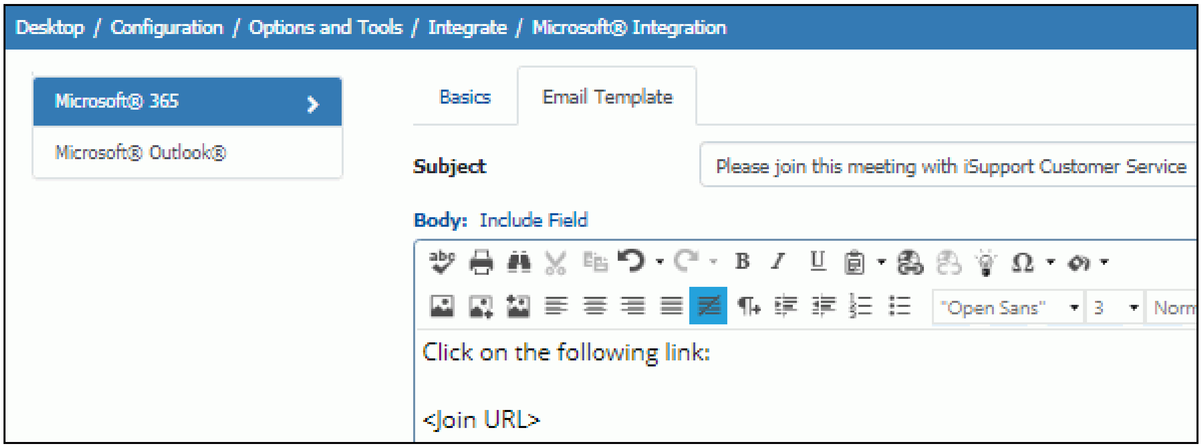
Microsoft Teams tasks, and enabling Microsoft Teams Meeting and Planner Task option to appear in work item screens for creating meetings and tasks with prefilled references to the iSupport work item number.



Follow the steps on the screen and complete the fields. Note that this requires administrator level access in Microsoft. The app for Microsoft 365 Teams should be different from the app for Microsoft Outlook. The master user account should be an administrative level account that will not be used by support representatives. Enable the Microsoft GCC High Environment setting if your Microsoft account was created under the .US domain in a Government Community Cloud High environment.

If you wish to allow support representatives to enable access to Teams and a group calendar in the Preferences screen without Microsoft administrator level access, ensure that you select the Consent On Behalf of Your Organization checkbox while requesting permissions in this screen. The Master User account is used for Team channel posts via rules and Outlook calendar groups available for display on dashboards.

Use the Email Template tab in the Microsoft 365 Integration screen to enter defaults for the subject and body of the email to be sent with a link to the meeting.



Note: Support representatives will need to use the Microsoft 365 Access field on the Details screen in the Preferences dialog to enable access to their calendar(s).

To add list fields of Microsoft Teams meetings and Planner tasks in work item screens, add the Microsoft Teams Meetings and Microsoft Planner Tasks fields to a work item screen layout via the Layouts configuration screen.

You can utilize the MS Teams Channel recipient with the Notify - Email action in work item rules.

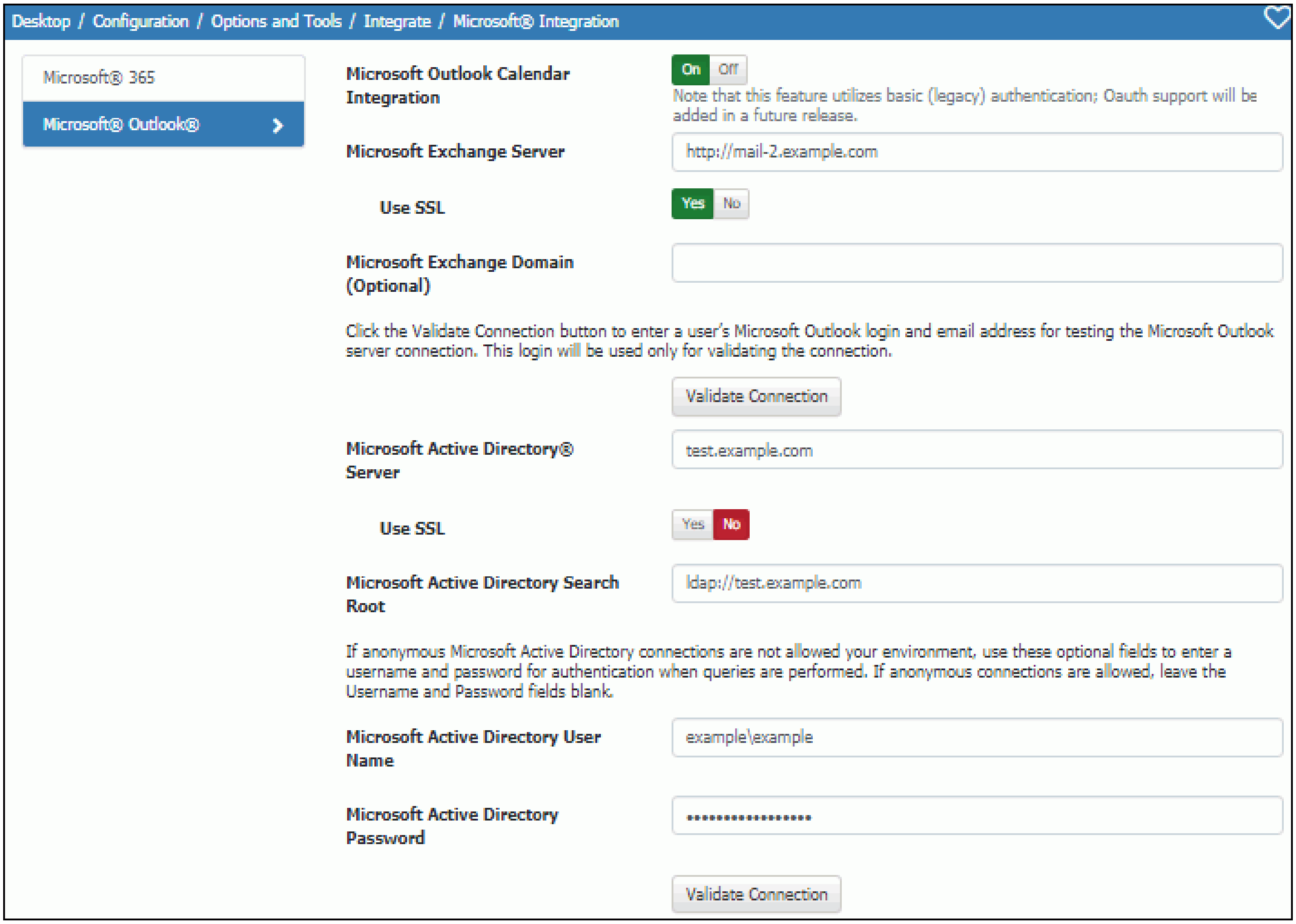
Microsoft Outlook Calendar Integration

Use the Microsoft Outlook tab in the Options and Tools | Integrations | Microsoft Integration screen to enable:

A New Meeting option to appear in iSupport entry screens after a record is saved for scheduling a Microsoft® Office Outlook® calendar meeting.

A support representative to view their calendar via the Desktop Calendar component and work item-specific calendars via the Action menu. Administrators can view support representative calendars via the Support

Representative Profile screen. Support representatives can view the schedules of meeting attendees, create a meeting to be added to their calendar, and configure a notification to be sent to the meeting attendees.



Microsoft Outlook Calendar Integration - Select On to enable the Microsoft Outlook Calendar Integration feature.

Microsoft Exchange Server - Enter the web address of the installation location of the Microsoft Exchange Server. If using SSL, the format must be: https://<*server*>

Use SSL - SSL is an encryption method that overlays the connection between the iSupport server and the Microsoft Active Directory server. Select Yes if SSL encryption is enabled on the Microsoft Active Directory server.

Microsoft Exchange Domain (Optional) - Enter the domain for accessing the Microsoft Exchange server. An entry in this field may be needed for a successful test connection.

A valid connection to the Microsoft Outlook server is required; click the Validate Connection button to enter a Microsoft Outlook login and email address to test the connection. Note that this information will be used only for validating the connection.

Microsoft Active Directory Server - Enter the installation location of the Microsoft Active Directory Server.

Use SSL - SSL is an encryption method that overlays the connection between the iSupport server and the Microsoft Active Directory server. Select Yes if SSL encryption is enabled on the Microsoft Active Directory server.

Microsoft Active Directory Search Root - Enter the complete search root URL for querying user information in Active Directory® entries. The search root can point to anywhere in the Active Directory® hierarchy, but the entry must be preceded by: ldap://

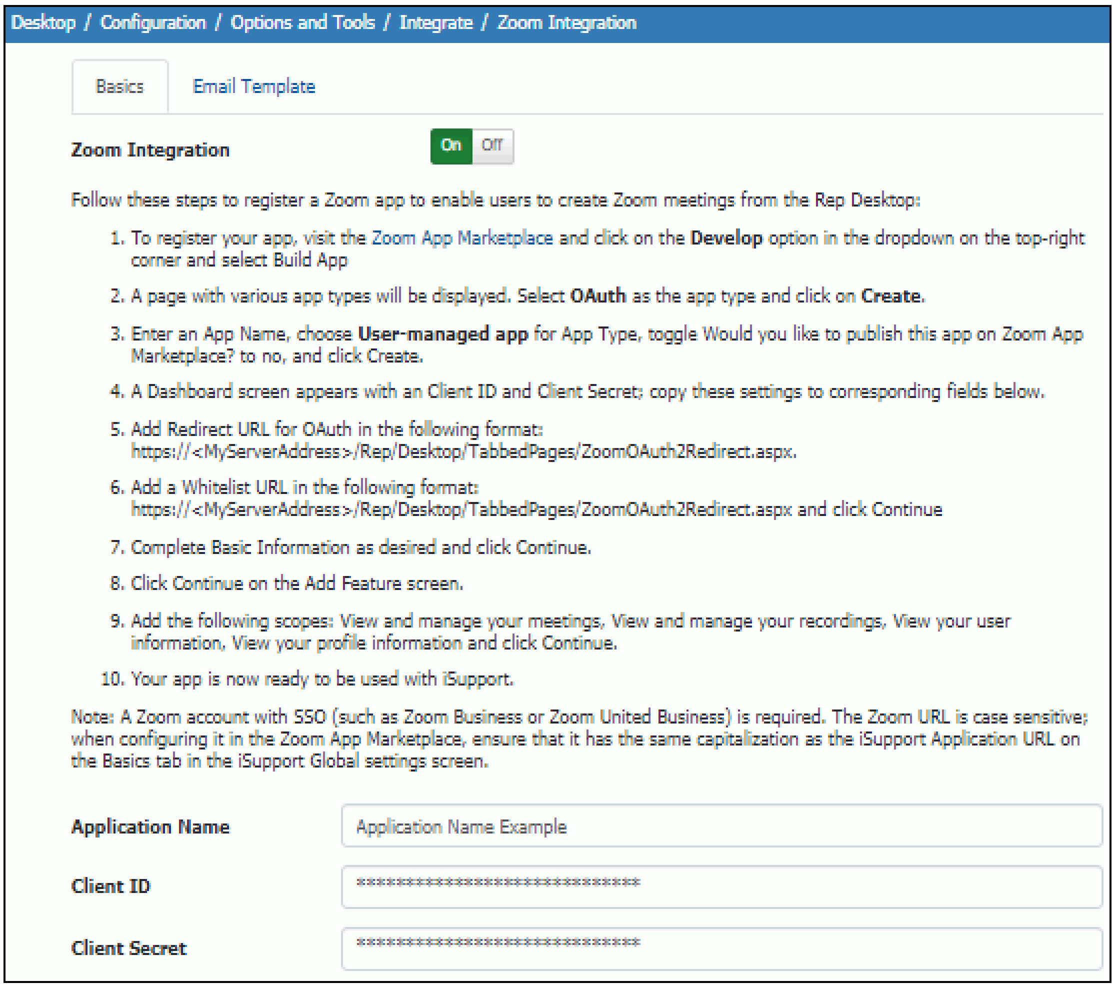
Microsoft Active Directory User Name/Microsoft Active Directory Password - If anonymous Active Directory® connections are not allowed in your environment, use these optional fields to enter a login for authentication when queries are performed. The username should be in the following format: DOMAINNAME\usernameIf anonymous connections are allowed, leave these fields blank.

Note: Support representatives will need to use the Microsoft Exchange User Name and Microsoft Exchange Password fields on the Details tab in the Preferences dialog and set the work day hours during which they are available to be scheduled via iSupport. The timeframe (work hours) during which support representatives are available to be scheduled via iSupport can be set via the Desktop or Support Representative Profile screen. (The dates/times outside of work day hours are designated as "Unavailable" in the calendars displayed via iSupport.)

Zoom Integration

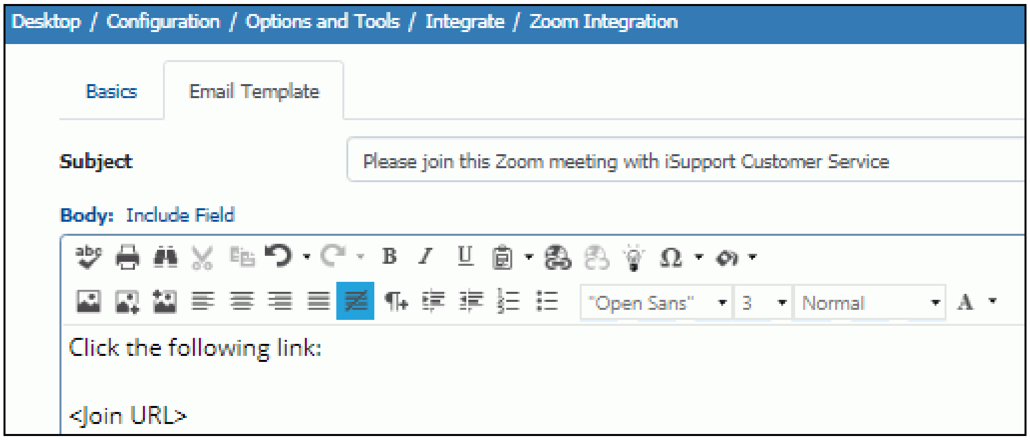
Use the Options and Tools | Integrations | Zoom Integration configuration screen to enable a Zoom Meeting option to appear in the Incident, Change, Problem, and Customer screens for scheduling an on-demand Zoom meeting. When the option is selected, a Generate Join URL dialog will appear for you to enter the topic and options for sharing the Join URL, and emailing a link to the meeting. The Share Join URL option will display a dialog with the URL and an option to start the meeting; the Email Link option will display the Correspondence dialog.

Follow the steps on the screen, enter an application name, and then enter the Client ID and Client Secret in the applicable fields.



Note: A Zoom account with SSO (such as Zoom Business or Zoom United Business) is required. The Zoom URL is case sensitive; when configuring it in the Zoom App Marketplace, ensure that it has the same capitalization as the iSupport Application URL on the Basics tab in the iSupport Global settings screen.

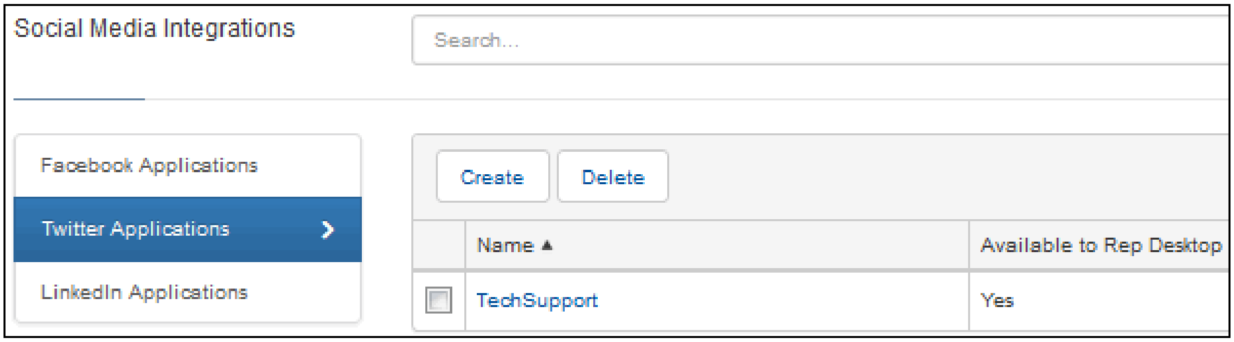
Use the Email Template tab in the Zoom Integration screen to enter the subject and body of the email to be sent with a link to the meeting.



Zoom meetings can be included in work item screens; add the Zoom Meetings field to a work item screen layout via the Layouts configuration screen.

Configuring Social Media Integration

Use the Options and Tools | Integrate | Social Media Integration screen to configure settings that work in conjunction with Twitter notifications as well as the LinkedIn and Facebook linked account functionality on the mySupport portal.



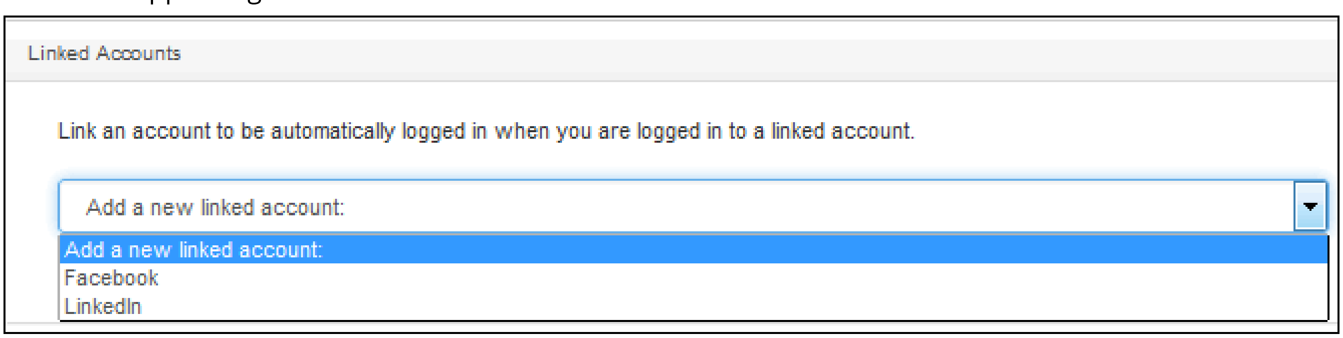
- **Facebook Applications** - Customers can link to and authenticate to the mySupport portal via a Facebook account; use the Facebook Applications tab to configure an application for this functionality. See “Facebook Applications” on page 110.
- **Twitter Applications** - A Twitter account and application must be configured in iSupport in order to use the Twitter and Twitter Monitor Desktop components, publish headlines and problems to Twitter, and send customer notifications regarding work item updates via Twitter. See “Twitter Applications” on page 112.
- **Linked In Applications** - Customers can link to and authenticate to the mySupport portal via a LinkedIn account; use the LinkedIn Applications tab to configure an application for this functionality. See “LinkedIn Applications” on page 114.

Note: iSupport utilizes or integrates with a number of third party applications and resources; changes in these external applications and resources may have a negative impact on functionality in iSupport. Depending on the nature and degree of the change, iSupport will, at its discretion, revise the current version of iSupport or make a corrective change in a future release of iSupport.

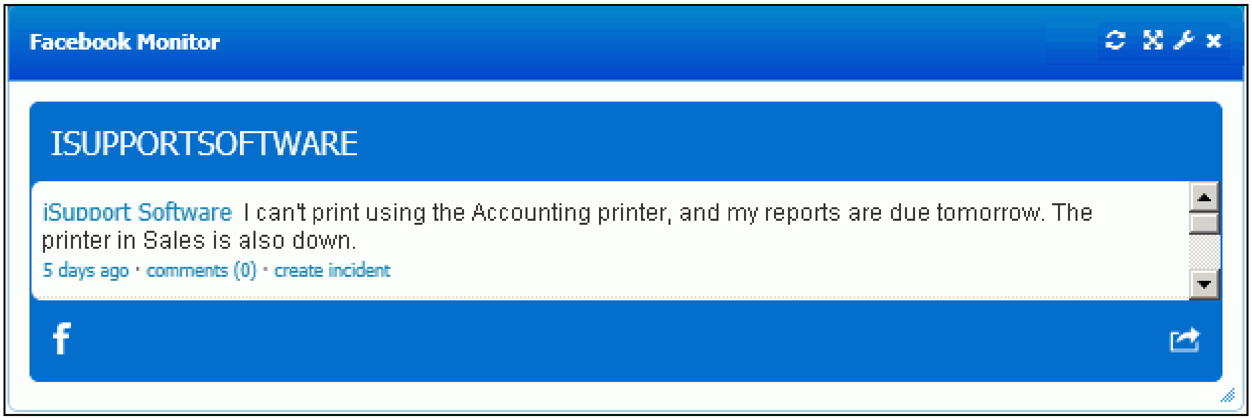
Facebook Applications

Configure a Facebook application to enable:

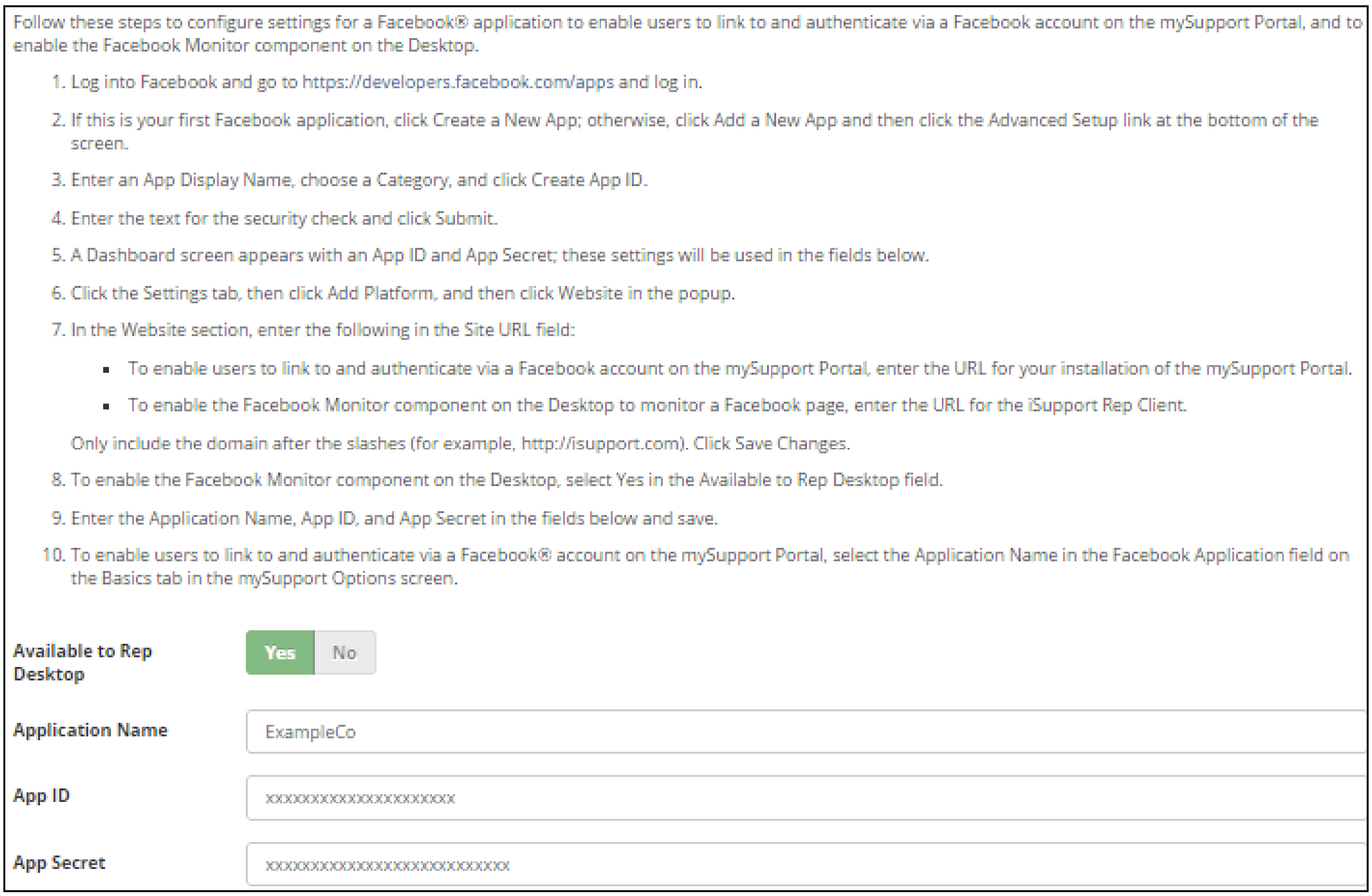
- Customers can use the Linked Accounts section in the mySupport Account Settings dialog to link an account for authenticating automatically via Facebook; if the customer is logged into Facebook, the customer will not need to enter an iSupport login.



- The Facebook Monitor component on the Desktop to monitor a Facebook page and display posts and comments from it. It includes an option to create an incident from a listed post or reply. If the customer's Facebook email address exists for a customer in Customer Profiles, the matching Customer Profile record will be used; otherwise, a new Customer Profile record will be created with the customer's email address in the format of <*Facebook username*>@facebook.com. A reply will be posted to Facebook with the incident number and a link to the incident; if the Facebook application doesn't have permission to do this, an email will be sent to the customer's Facebook email account.



Follow the steps on the Facebook Applications tab in the Options and Tools | Integrate | Social Media Integration screen to configure a Facebook application.


Follow these steps to configure settings for a Facebook® application to enable users to link to and authenticate via a Facebook account on the mySupport Portal, and to enable the Facebook Monitor component on the Desktop.

1. Log into Facebook and go to https://developers.facebook.com/apps and log in.
2. If this is your first Facebook application, click Create a New App; otherwise, click Add a New App and then click the Advanced Setup link at the bottom of the screen.
3. Enter an App Display Name, choose a Category, and click Create App ID.
4. Enter the text for the security check and click Submit.
5. A Dashboard screen appears with an App ID and App Secret; these settings will be used in the fields below.
6. Click the Settings tab, then click Add Platform, and then click Website in the popup.
7. In the Website section, enter the following in the Site URL field:
   - To enable users to link to and authenticate via a Facebook account on the mySupport Portal, enter the URL for your installation of the mySupport Portal.
   - To enable the Facebook Monitor component on the Desktop to monitor a Facebook page, enter the URL for the iSupport Rep Client.

   Only include the domain after the slashes (for example, http://isupport.com). Click Save Changes.
8. To enable the Facebook Monitor component on the Desktop, select Yes in the Available to Rep Desktop field.
9. Enter the Application Name, App ID, and App Secret in the fields below and save.
10. To enable users to link to and authenticate via a Facebook® account on the mySupport Portal, select the Application Name in the Facebook Application field on the Basics tab in the mySupport Options screen.

Available to Rep Desktop	Yes No
Application Name	ExampleCo
App ID	xxxxxxxxxxxxxxxxxxxxx
App Secret	xxxxxxxxxxxxxxxxxxxxxxxxxxx

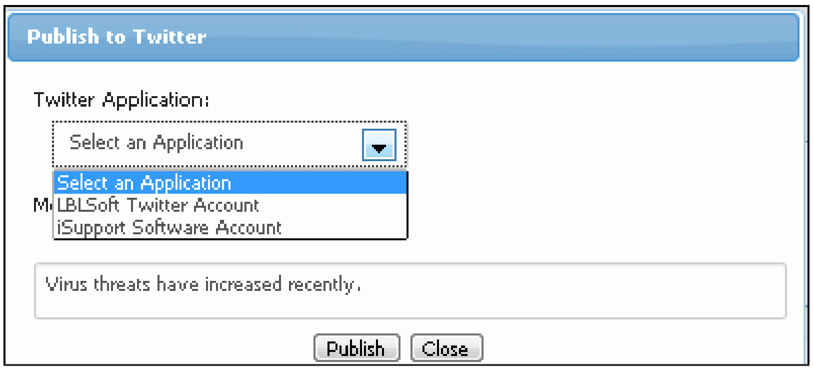
After completing the Application Name, App ID, and App Secret fields:

- To enable the Facebook Monitor component on the Desktop to monitor a Facebook page, select Yes in the Available to Rep Desktop field.
- To enable "Facebook" to display in the Add a New Linked Account dropdown in the Linked Accounts section in the mySupport Account Settings dialog, select the application name in the Core Settings | mySupport | mySupport Portals | Options screen.

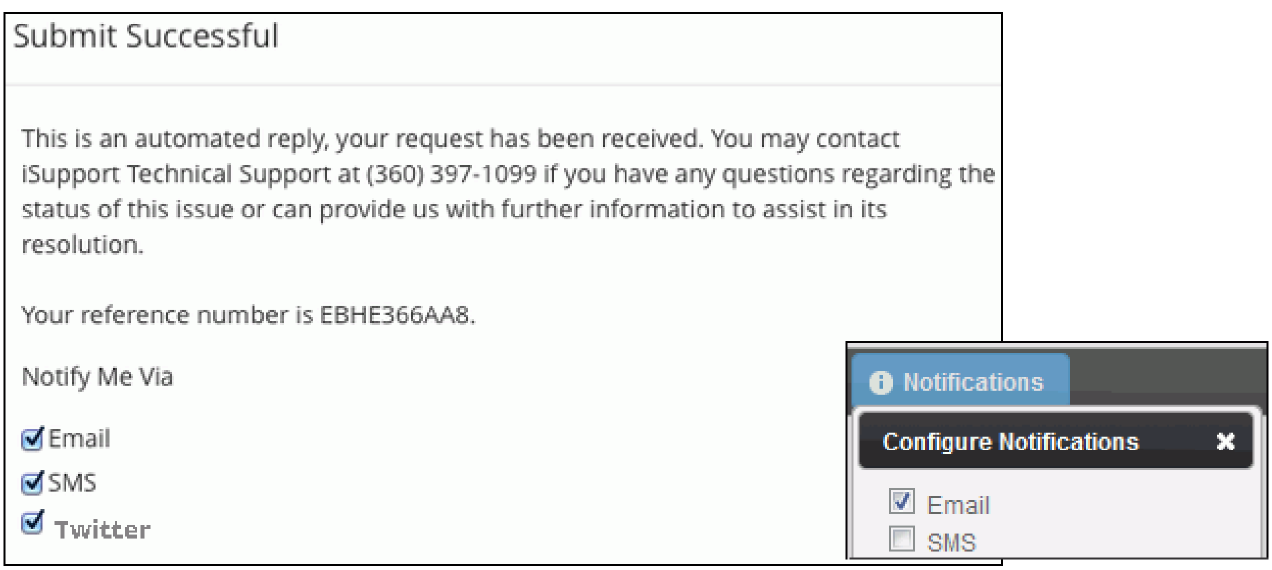
Twitter Applications

A Twitter account and application must be configured in iSupport in order to use the following features. To get started with creating a Twitter application, see "Configuring a Twitter Application" on page 113.

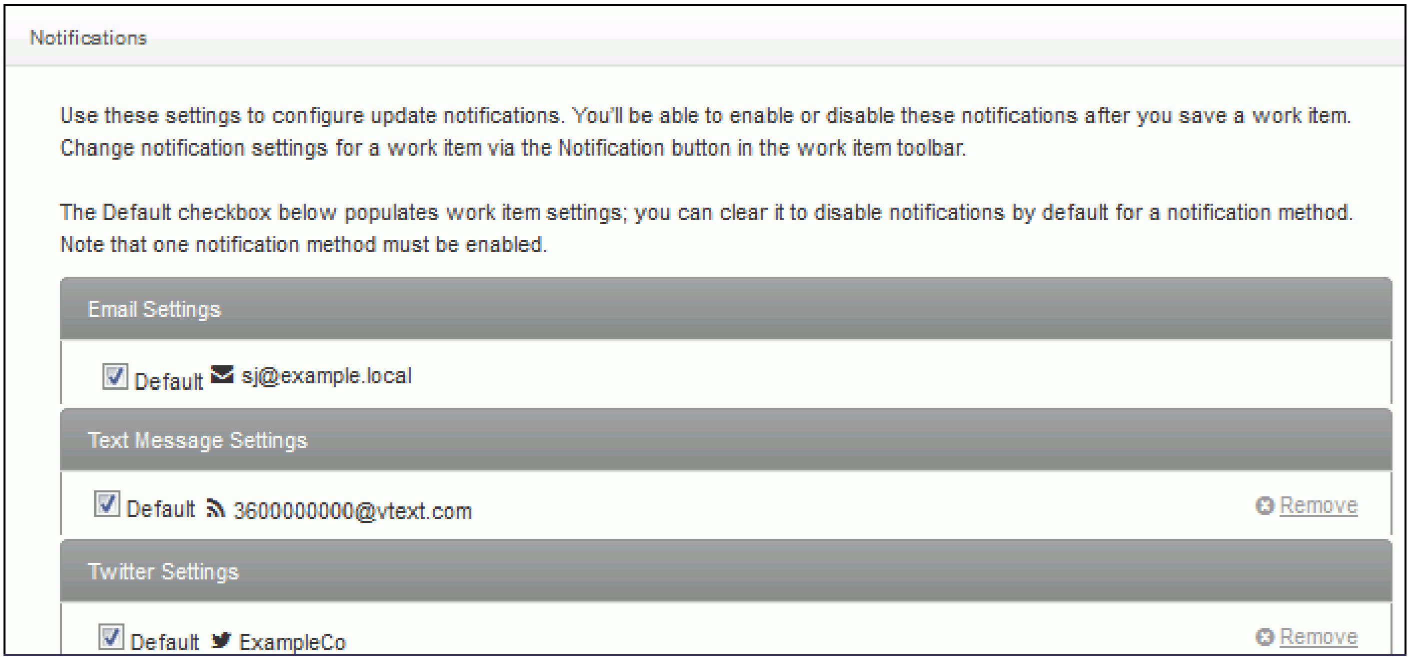
- Use the Twitter component display a Twitter feed for a specified Twitter username.
- Use the Twitter Monitor component to search Twitter feeds and display tweets that include a specified search term. You can use the Reply link to reply to tweets directly from iSupport, or use the Create Incident link to create an incident and send a reply to the Twitter user (via a Twitter direct message) with their incident number included. The tweet will be included in the Description field in the incident, and if the Twitter username exists for a customer in Customer Profiles, the matching Customer Profile record will be used. If the Twitter username does not exist for a customer, a new Customer Profile record will be created in the format of <*Twitter username*>@twitter.com.
- Support representatives can publish headlines and problems via Twitter. The Twitter option will appear in the Headline and Problem screens if the support representative has the Publish to Twitter permission; when clicked, the Publish to Twitter dialog will appear with the contents of the message and details (for headlines) or the short description (for problems). If multiple Twitter applications have been created, the user can select the account to which the headline or problem should be published.



- Customers can use the Notifications section in the mySupport Account Settings dialog to enable a notification to be sent via Twitter direct message whenever when a rule results in any notification to the customer regarding work items (incidents, problems, changes, purchase requests). As shown in the dialogs below, customers can enable or disable notifications for a work item after saving, and change notification settings for an existing work item via the Notification button in the work item toolbar.

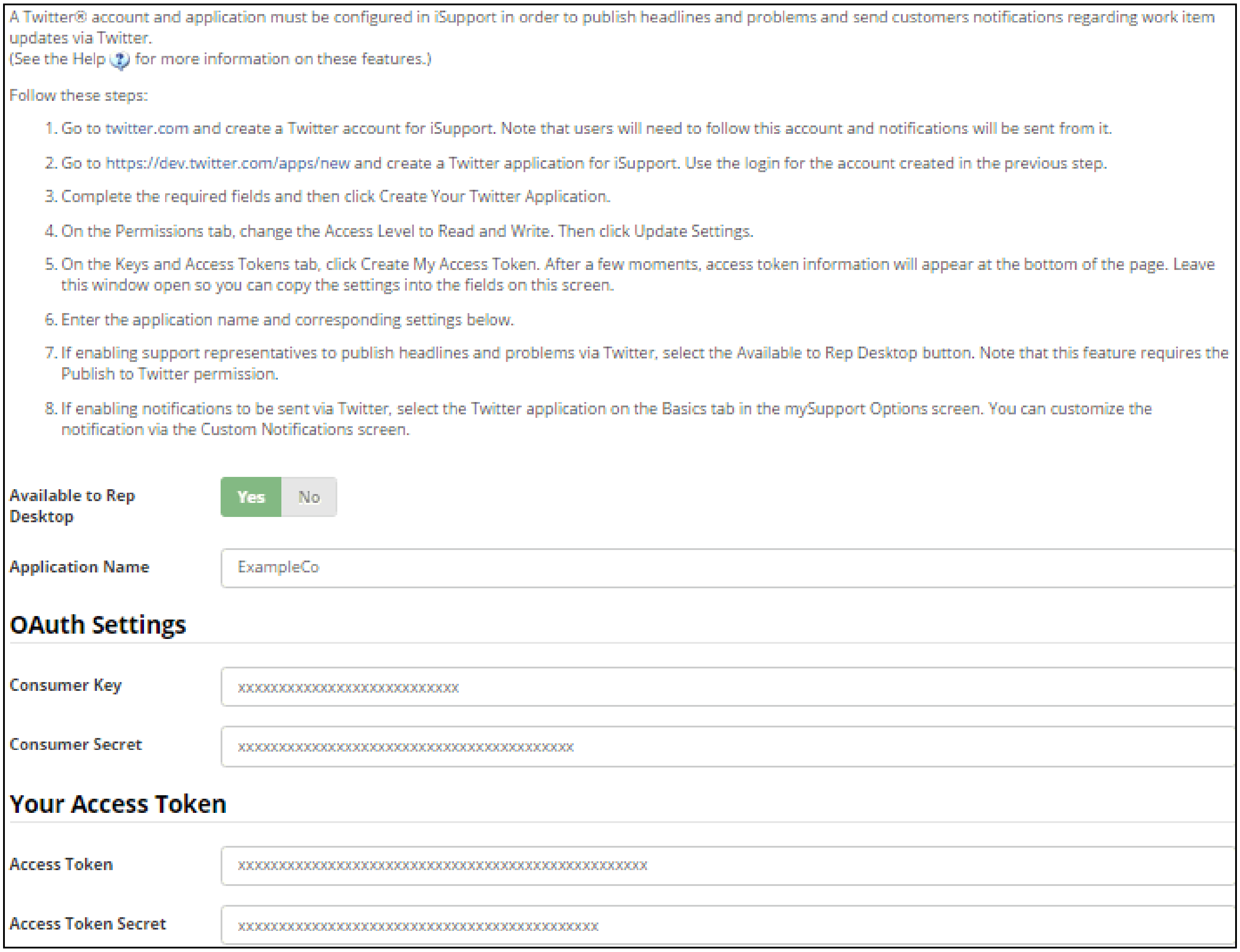


Customers configure the Twitter account to which the notification should be sent in the Notifications settings. The user needs to be following the account associated with the Twitter application specified in configuration; this account will be listed in the dialog prompting for the activation code.



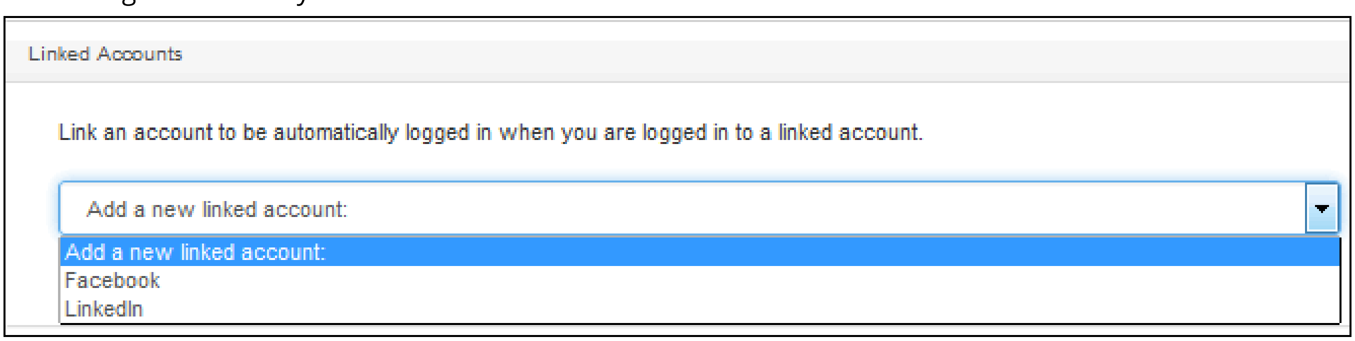
Configuring a Twitter Application

Follow the steps on the Twitter Applications tab in the Options and Tools | Integrate | Social Media Integration screen to create a Twitter account and application; use the Available to Rep Desktop button to enable an account to be published to Twitter. To enable the application to be used for update notifications sent to customers via the mySupport portal, select the application name in the Core Settings | mySupport | mySupport Portals | Options screen.

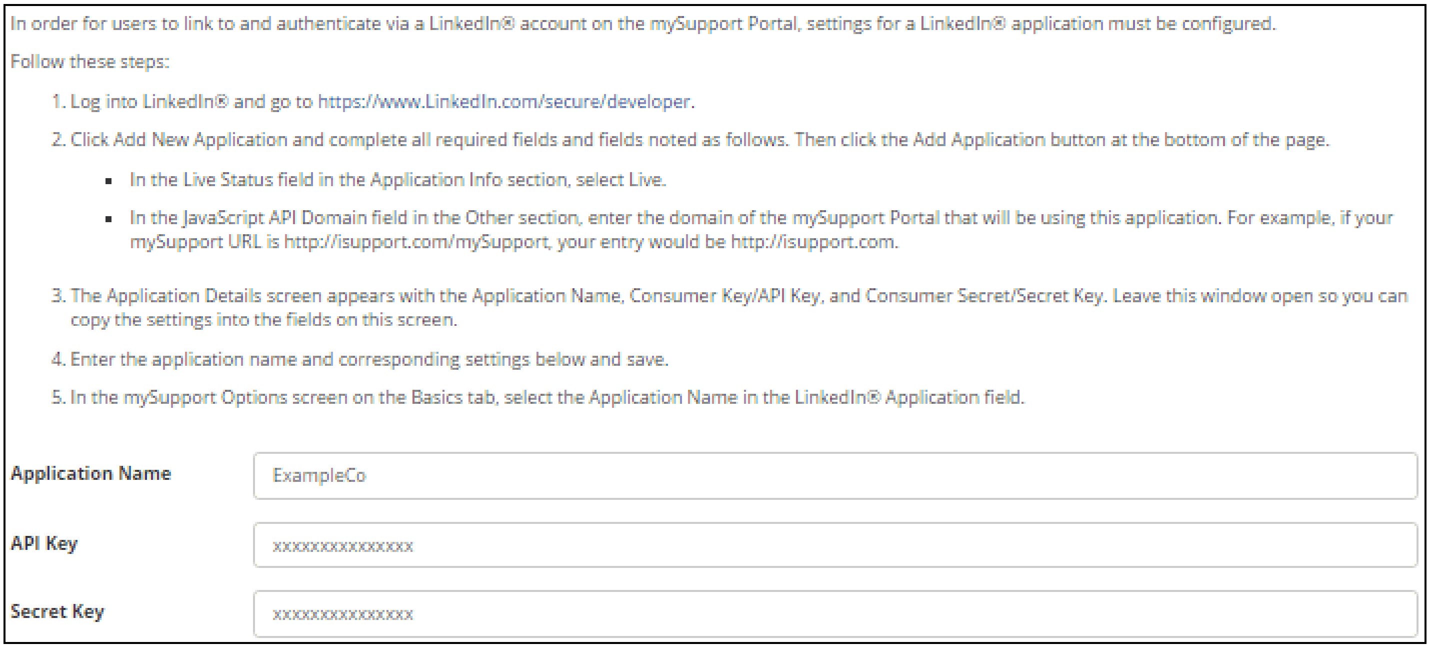


LinkedIn Applications

Customers can use the Linked Accounts section in the mySupport Account Settings dialog to link an account for authenticating automatically via LinkedIn.



Follow the steps in the screen to configure a LinkedIn application, and then select the application name in the Core Settings | mySupport | mySupport Portals | Options screen to enable "LinkedIn" to display in the Add a New Linked Account dropdown in the Linked Accounts section in the mySupport Account Settings dialog.



In order for users to link to and authenticate via a LinkedIn® account on the mySupport Portal, settings for a LinkedIn® application must be configured.

Follow these steps:

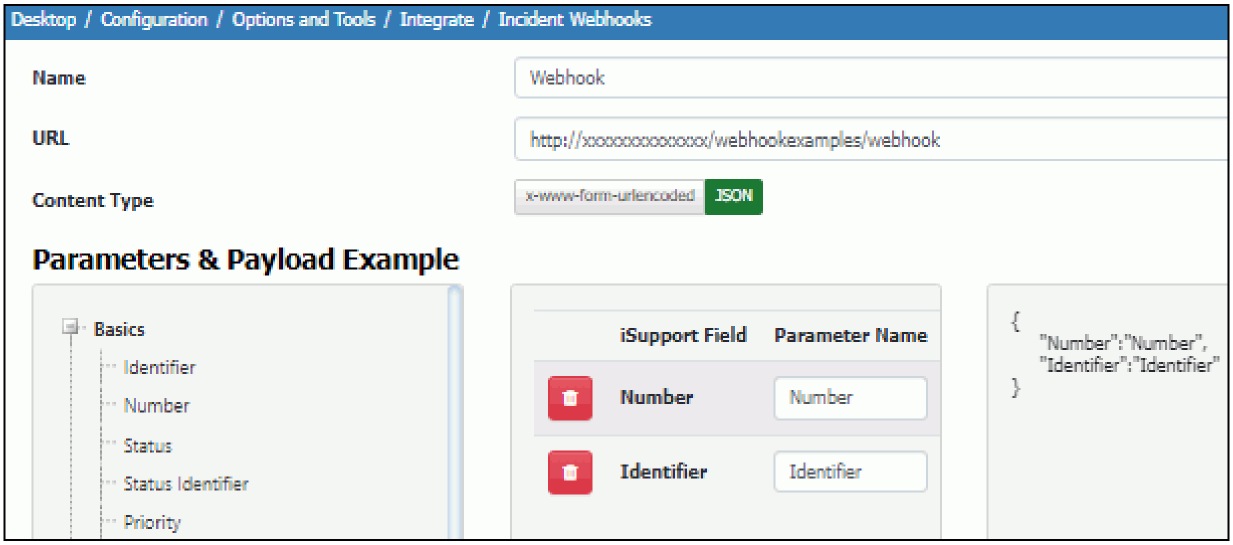
1. Log into LinkedIn® and go to https://www.LinkedIn.com/secure/developer.
2. Click Add New Application and complete all required fields and fields noted as follows. Then click the Add Application button at the bottom of the page.
   - In the Live Status field in the Application Info section, select Live.
   - In the JavaScript API Domain field in the Other section, enter the domain of the mySupport Portal that will be using this application. For example, if your mySupport URL is http://isupport.com/mySupport, your entry would be http://isupport.com.
3. The Application Details screen appears with the Application Name, Consumer Key/API Key, and Consumer Secret/Secret Key. Leave this window open so you can copy the settings into the fields on this screen.
4. Enter the application name and corresponding settings below and save.
5. In the mySupport Options screen on the Basics tab, select the Application Name in the LinkedIn® Application field.

Application Name	ExampleCo
API Key	xxxxxxxxxxxxxxx
Secret Key	xxxxxxxxxxxxxxx

Configuring Webhooks

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

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



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.