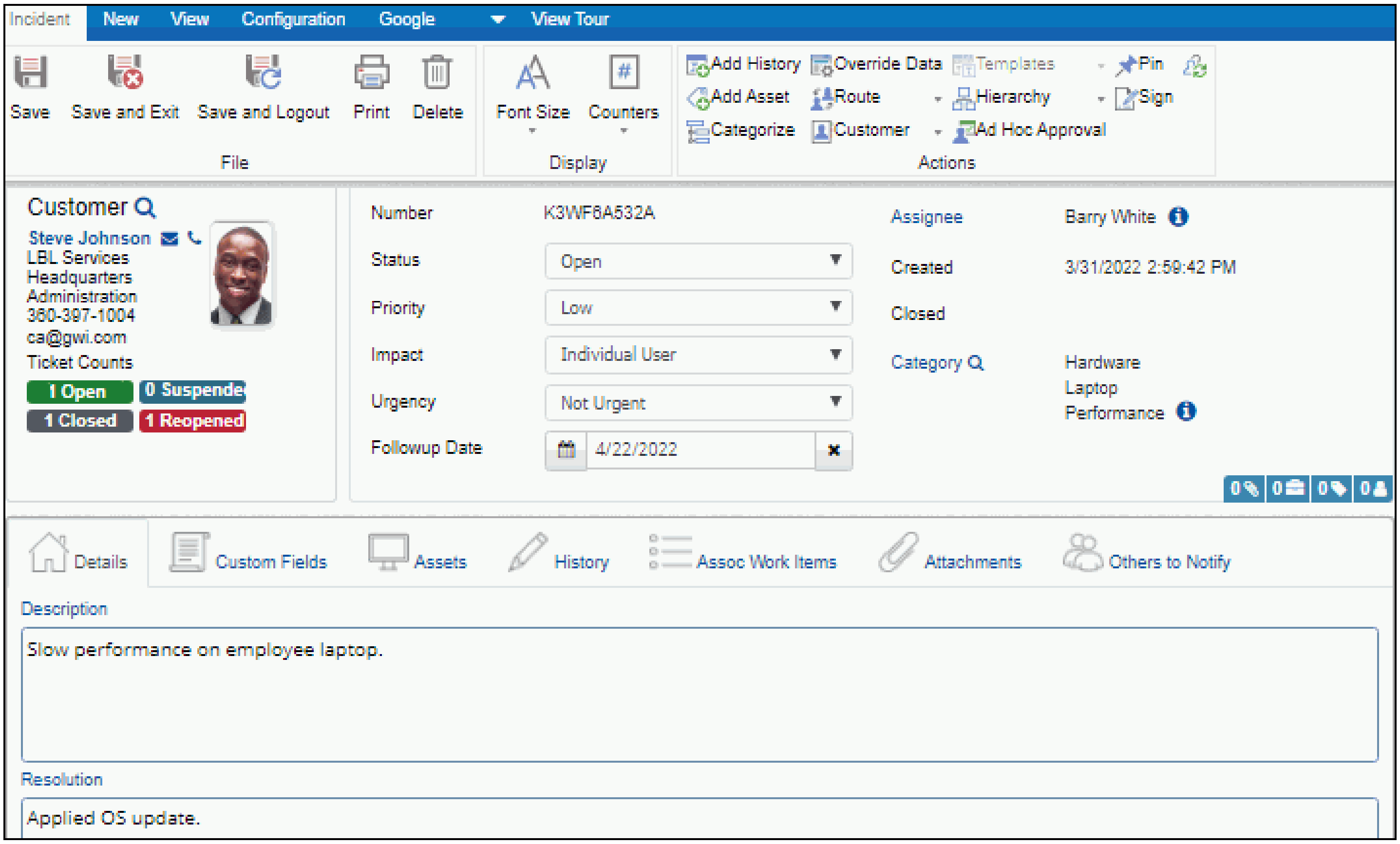
Using the iSupport® Incident Screen

iSupport's Incident functionality can assist in issue tracking and accomplishing quick restoration of service.



The only information required in order for an incident to be saved is the customer, categorization, issue description, a custom number if required, and any required custom fields. The issue resolution is required in order for an incident to be closed. If configured, you may be required to enter time worked in a history entry when you save the incident.

Note: The fields and layout in the Incident screen are set up in the Configuration module. Fields or functionality may not display if disabled or disallowed due to permissions set during configuration. The following sections contain information on **all** incident functionality.

Use the View Tour option at the top of the screen to display a short series of tips on the Incident screen.

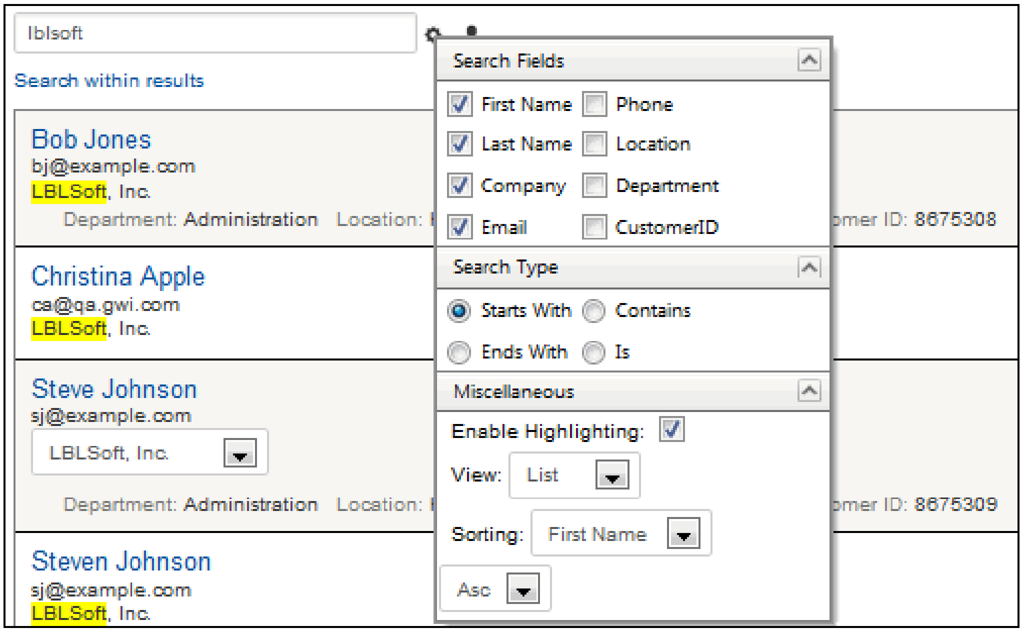
Entering Essential Incident Information

This section includes information on completing the primary fields you'll use to document an issue.

Entering Customer Information

Note: If you are displaying an incident created from an email, the customer's name may not be included on the incident if the customer submitting the email did not have his/her name set up in their email application and did not have an email address that existed in Customer Profiles. To complete the customer's contact information, select View | Customer in the Incident screen, complete the appropriate fields in the customer's profile record, and save the record. Then select the customer in the Incident screen to populate the customer's name in the Name field.

If you are creating a new incident and customer lookups are enabled during configuration, a Select Customer dialog will display for you to select an existing customer or enter information for a new customer. You can search based on last name, first name, phone, location, email, company, department, and customer ID and perform another search on the results if needed. If this dialog is not enabled, select Incident | Actions | Customer | Select Customer or use the Select Customer icon. You can enter the first few characters of the name for faster searching; if only one record results from a type ahead customer search, that record will be automatically selected and added to the work item.



To display or change an existing customer's profile information, select View | Customer. To view information on the customer's company, select View | Company.

A Microsoft® Skype/Lync® status icon can be configured to appear next to the customer's name. If you are using Internet Explorer, the icon will display the Microsoft Skype/Lync status of the selected customer. You can select the icon to access Microsoft Skype/Lync functions.

Entering Information on New Customers

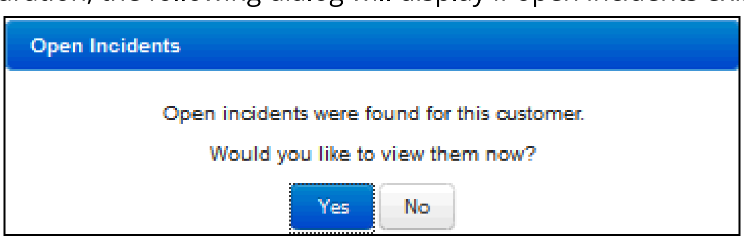
To enter information for a new customer, select the Create New Customer link in the search dialog or select New | Customer and enter the customer's name and contact information. Note: each Customer Profile record must have a unique email address and first and last name combination. The New Customer option may not appear if specified during configuration. After a customer is selected or new customer information is entered, the information appears in the Customer section.

To create a new incident for the same customer and populate the customer information fields, select New | Incident.

Viewing Incidents for Existing Customers

There are a few ways to view a customer's incidents:

- If enabled during configuration, the following dialog will display if open incidents exist for the selected customer.

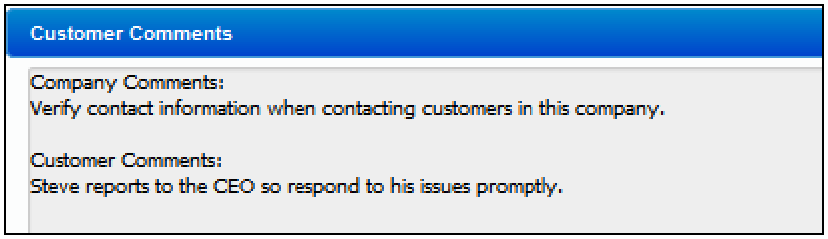


- Use the options on the View | Incidents menu to view a customer's open and/or closed incidents.

- If ticket counts are configured for the Incident screen, select the Ticket Counts 1 Open icon in the Customer section.

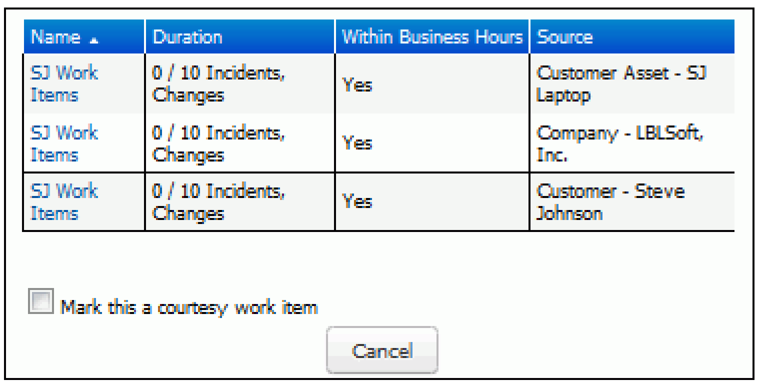
Viewing Customer Comments

Any comments entered in a customer's Profile record and/or a customer's Company record will appear after customer selection will appear as in the example below.



Selecting a Service Contract

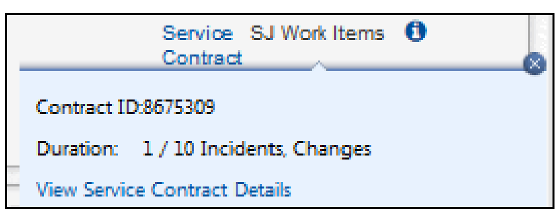
iSupport's Service Contract functionality tracks and restricts incidents and changes for customers, companies, and/or assets. Contracts can be based on work item count (a specified number of incidents and/or changes), hourly count (a specified number of hours), duration (time frame in days), or a combination (limiting the number of incidents and/or changes within a specified daily time frame. If Service Contract functionality is enabled in configuration and a service contract is associated with the selected customer, customer's company, or customer's asset selected for the incident, the Select Service Contract dialog will appear:



Name ▲	Duration	Within Business Hours	Source
SJ Work Items	0 / 10 Incidents, Changes	Yes	Customer Asset - SJ Laptop
SJ Work Items	0 / 10 Incidents, Changes	Yes	Company - LBLSoft, Inc.
SJ Work Items	0 / 10 Incidents, Changes	Yes	Customer - Steve Johnson

The Mark This a Courtesy Work Item checkbox will appear if enabled in configuration. Select the service contract to which the incident should be applied or select the Mark This a Courtesy Work Item checkbox if you do not wish to count the incident against a contract. If you selected a contract, the change will be counted against it when the record is initially saved.

After selecting a contract, the contract name appears in the Service Contract field. You can select Information to display the contract ID and duration. You can select the View Service Contract Details link to display the contract in the Service Contract screen.



Selecting Additional Customers

If there are numerous customers reporting the same issue, you can add customers to the incident by selecting Incident | Customer | Add Additional. The Add Customer dialog appears for you to select the additional customers. The Additional Customers link appears in the customer section once an additional customer has been selected.

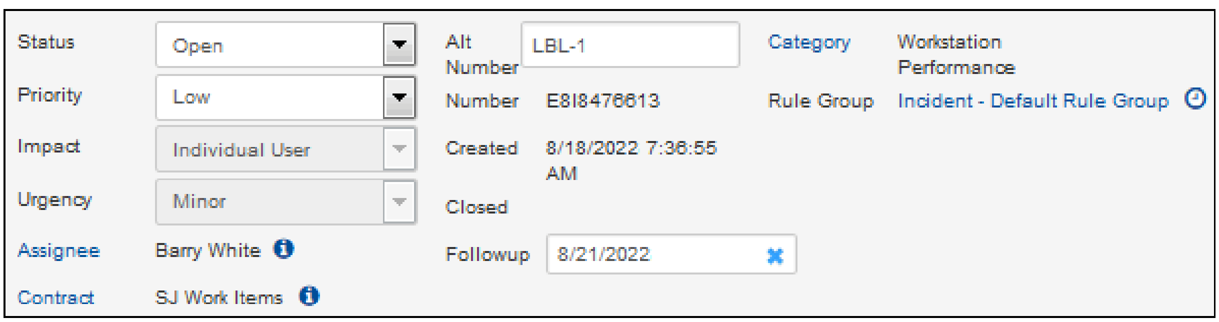
The Customer Profile screen includes an Additional Customer option in the Can View Items For field; this enables the customer to view any incidents for which they are associated as an additional customer in mySupport views and feeds.

To view the additional customers on an incident, select the Additional Customers link and select View or select View | Customers | Additional Customers.

First	Last	Phone	Email	Location
Bob	Jones	360-397-1000	bj@example.com	Headquarters

Selecting the Status, Impact, Urgency, Priority, and Categorization

The Status, Impact, Urgency, and Priority fields describe the state of the incident; the Categorization field describes the incident for use in routing and reporting.



<u>*Setting the Incident Status*</u>

There are four basic status levels: Open, Suspended, Closed, and Reopened; different labels can be set up in the Configuration module for those basic status levels. A status may be assigned via the Scheduling and Approval features if configured. After using the Closed status to close an incident, the Reopen option will appear on the Incident menu for reopening the incident.

<u>*Setting the Incident Priority, Impact, and Urgency*</u>

Priority levels (Low, Medium, High, and Emergency) indicate the severity of the issue. Priority levels can be associated with time frames in rules, so you'll need to consult with your administrator regarding time frames in order to understand how quickly incidents must be resolved.

If enabled in the Configuration module, the Impact (usually the number of users affected) and Urgency (based on the amount of time a resolution is needed) values are defined and associated with the priority levels of Low, Medium, High, and Emergency; these defined values will be available in the Impact and Urgency fields for selection. The mapped priority will appear as default but all priority levels are available if permissions are configured for you to change the priority.

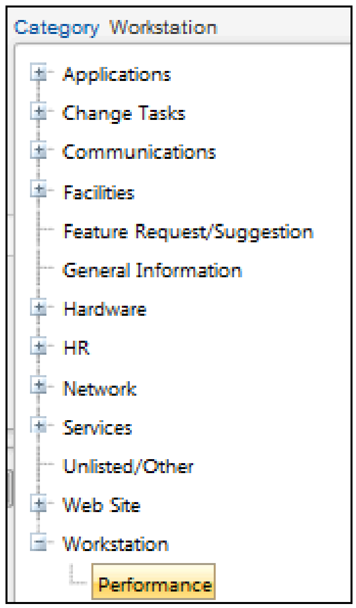
Examples of Impact, Urgency, and Priority mappings include:

Impact	Urgency	Priority
Individual	Minor	Medium
Department	Major	High
Company-wide	Minor	Medium
Company-wide	Critical	Emergency

Selecting the Categorization

Categories are used for routing, reporting, and associating incidents with rules, scripts, and knowledge entries. Categories are enabled in sets of up to five levels; the first level is fairly general and the last level is fairly specific.

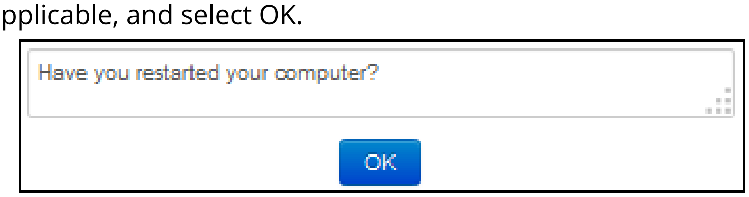
To select a category set for an incident, select Incident | Categorize or select the Category link. A dropdown appears containing predefined categories; expand the entries and select the one that best describes the issue.



If there are other incidents, knowledge entries, headlines, or problems or changes (Service Desk Edition) that have the same categorization, the View Open Work Items for Categorization link appears for you to view these items. You can associate knowledge entries, headlines, problems, and changes with the current record if applicable. **Note:** You can recategorize an incident at any time while the incident is open.

Completing Call Scripts

Call scripts are associated with specific category combinations and can contain instructions on gathering information from a customer, a list of questions to ask the customer, or other related items. If a call script is associated with the selected category set, the script appears in a dialog when the category set is selected. Follow the script, enter responses to questions if applicable, and select OK.



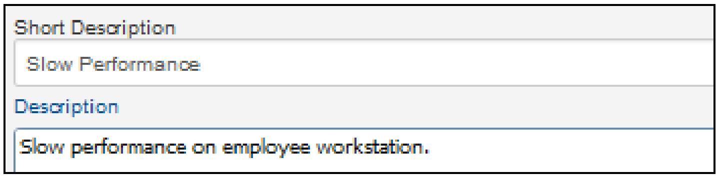
If enabled in configuration, the information will be automatically entered in the Work History field. If you need to display the call script later for reference, select View | Call Script.

Entering a Followup Date

If the Followup Date field is enabled during configuration, select the date on which, if the incident is not closed, a followup reminder email should be sent to the assignee of the incident.

Describing the Incident

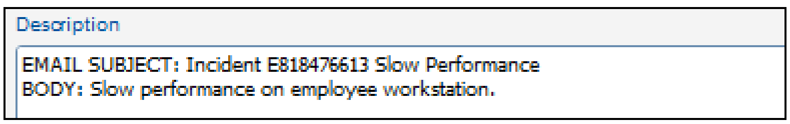
Use the Short Description field to enter an abbreviated description of the incident, and use the Description field to enter a longer description of the incident.



Note: The content in the Description field may be sent to customers in an email notification regarding the incident, depending on options set in the Configuration module.

Working with Email Submissions

If an incident is created from an email submission, the subject line and body of the email are placed in the Description field.

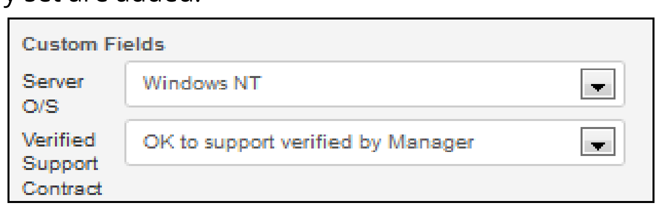


A link to the correspondence is included in the Correspondence History, and attachments are attached to the correspondence. If there is an alternate version of the body of the email (created by the email application), if configured it will be saved as a document and attached to the correspondence.

If an existing incident number is included in the subject or body of the email, depending on configuration settings, an incident may be created or the incident may be updated with a notation and correspondence link in the Audit History field. The link will indicate whether any files were attached to the correspondence. An email may be sent to the sender's email address acknowledging receipt of the email, and email may be sent to the assignee of the updated incident. The email will contain a link to the updated incident.

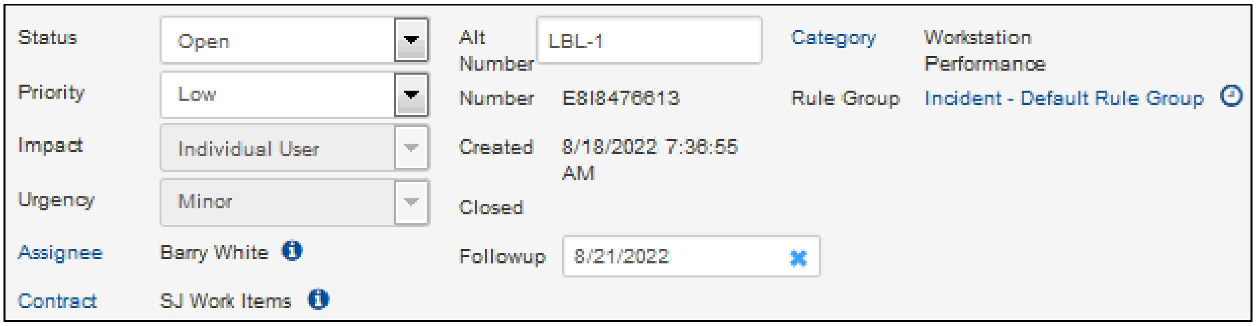
Completing Custom Fields

Custom fields may be configured for entering information specific to your company. Custom fields can be configured to always appear or appear when a certain category is selected. You may be required to enter information in custom fields, and if an incident is recategorized, data saved in custom fields is retained and the custom fields associated with the newly-selected category set are added.



Entering a Custom Number

A unique number is automatically assigned to each incident. A custom incident number field may also be configured; an entry may be required. In the example below, the custom number field is labeled "Alt Number".



Using Incident Templates

Incident templates populate the following fields in the Incident screen with information set up during configuration: Categorization, Short Description, Issue Description, Issue Resolution, Priority, Assignee, Followup Date (if configured), and Time Worked (if configured). A script will appear if associated with the categorization. A template can also be configured to automatically close; if you select an auto-close template, the status of the incident will change to Closed and the incident window will close (unless required fields are blank).

To use an incident template, select Incident | Templates | Use Incident Template. A dialog appears containing a list of predefined template names; select one and select OK.

Name	Type
Login to Website - Access Request	Auto-Close
Need Insurance Forms	Auto-Close
Send Documentation	Auto-Close
Submit a Product Suggestion	Auto-Close
Password Reset	Auto-Fill
Print Assistance	Auto-Fill

The template fills in the Categorization, Short Description, Issue Description, and Issue Resolution, Assignee, Priority, and Followup Date fields. Templates can be configured to append or replace the text in the Short Description, Description, and/or Resolution fields.

If you selected an auto-close template, the incident status changes to Closed and the window closes automatically. If configured, the time spent on the incident is recorded in the Time Worked field.

If you selected an auto-fill template (one that does not auto-close), the incident will remain open. A script will display if associated with the categorization.

Hierarchy templates can also be used to populate incident fields; for more information, see "Using Hierarchy Templates" on page 37.

Scheduling Incidents

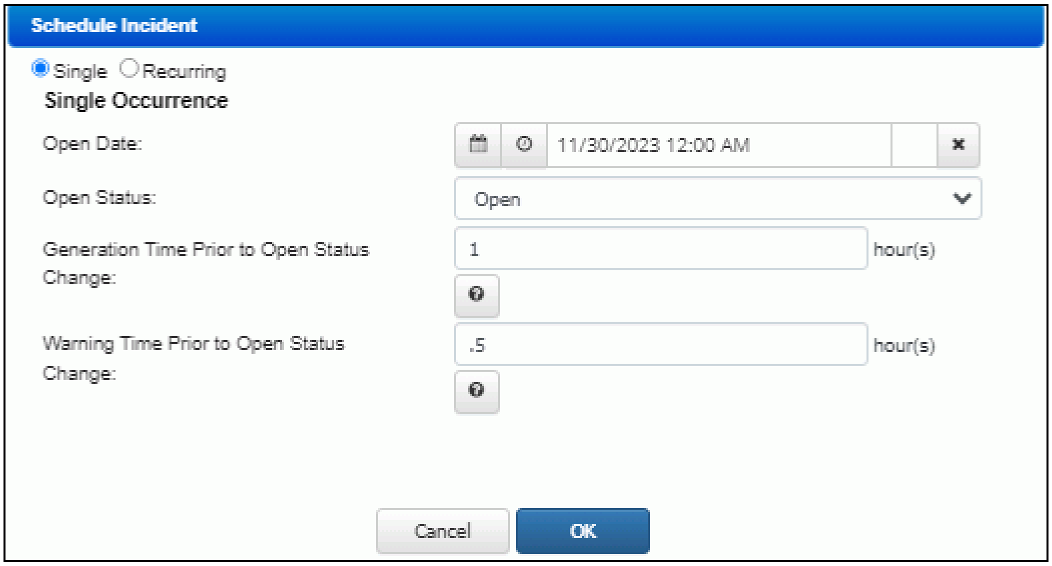
You can schedule one or more incidents to be created with an open status at a future date/time. You can schedule a single occurrence incident or, if configured, a recurring set of incidents. Scheduled incidents are assigned the open status by the Ticket Scheduling agent. You must complete the scheduling dialog before the incident has been saved.

You can generate scheduled incidents prior to the time at which the status changes; when this occurs, the scheduled incidents have a Scheduled status and all fields can be updated except the Status field. Administrators can use the Scheduled status to stop notifications. When the specified open date/time is reached on a scheduled incident, the status will change to the specified open status and the rule group will go into effect using the open date/time.

In the Incident screen, select Incident | Schedule to display the Scheduling dialog.

Scheduling a Single Occurrence Incident

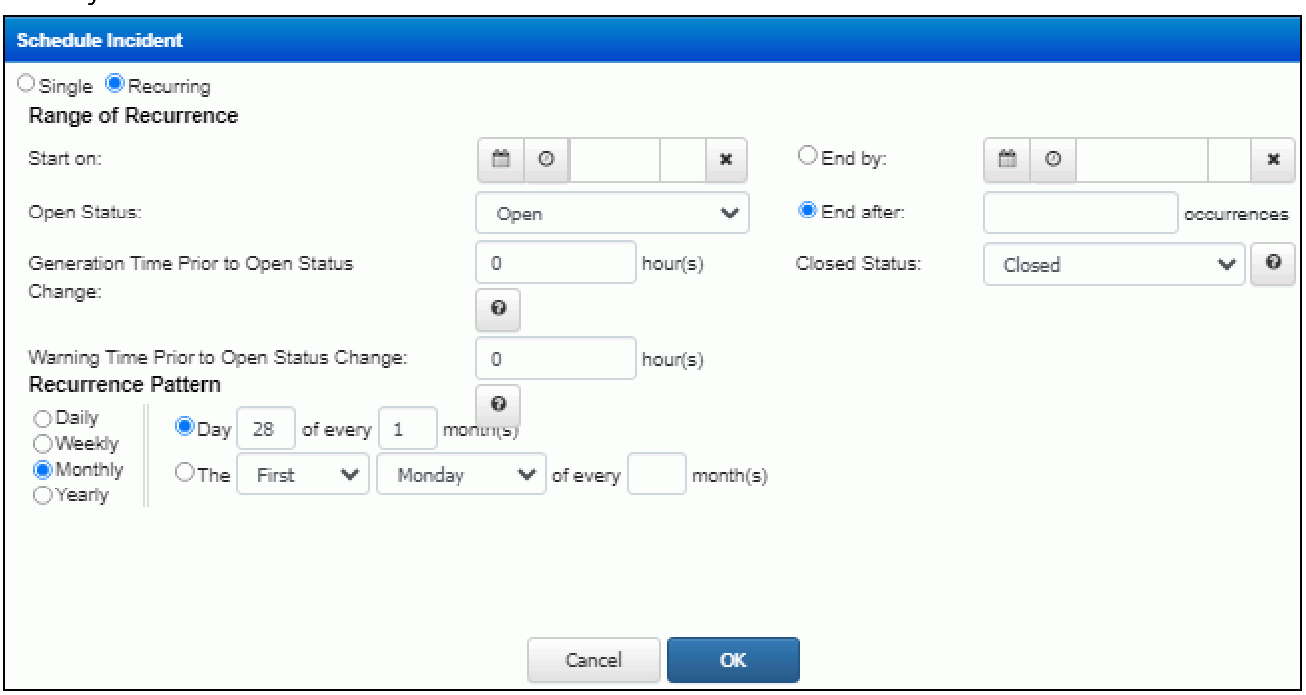
In the Open Date and Start Time field, enter the date and time at which the status should be changed to an Open status, and use the Open Status field to select the status. When the open date/start time is reached, the scheduled incident will become a normal open incident and the rule group will go into effect. No new incidents are created for a single occurrence schedule.



If you wish to create the incident prior to the open status change, select the amount of time in the Generation Time Prior to Open Status Change field. The incident will have a status of Scheduled until the date and time in the Open Date and Start Time fields. To send a warning notification a specified amount of time before the open status change, select the time in the Warning Interval Prior to Open Status Change field.

Scheduling Recurring Incidents

If configured, you can select Recurring to create a new incident on a repeated basis at a specified date/time. When each new incident is created, it will be initially saved in the Scheduled status and only notification rule actions will be executed. When incidents are created on a recurring basis, the incident on which you set the schedule will close automatically when the final incident is created from it.



In the Start Time field, enter the time at which the status should be changed to an Open status, and use the Open Status field to select the status. If you wish to create the incidents prior to the open status change, select the incident creation time in the Generation Time Prior to Open Status Change field. Notifications may be configured to be sent at that time. The incidents will have a status of Scheduled until the date and time in the Open Date and Start Time fields.

To send a warning notification a specified amount of time before the open status change, select the time in the Warning Interval Prior to Open Status Change field.

Selecting the Date Range and Close Status

In the Start Date field, select the date on which the first incident should be created. Use the End After field if you wish to create a specified number of tickets; use the End By field if you wish to end the incident creation schedule on a specified date. When the final incident is created, the incident on which you set the schedule will close; use the Closed Status field to select the Closed status to assign to it.

Notations are included in the History field on all incidents created from the schedule. Once the originating schedule is closed, you can view it via one of these notations in an incident created from the schedule.

Selecting the Recurrence Pattern

Use the Recurrence Pattern section to specify how tickets should be created on a repetitive basis:

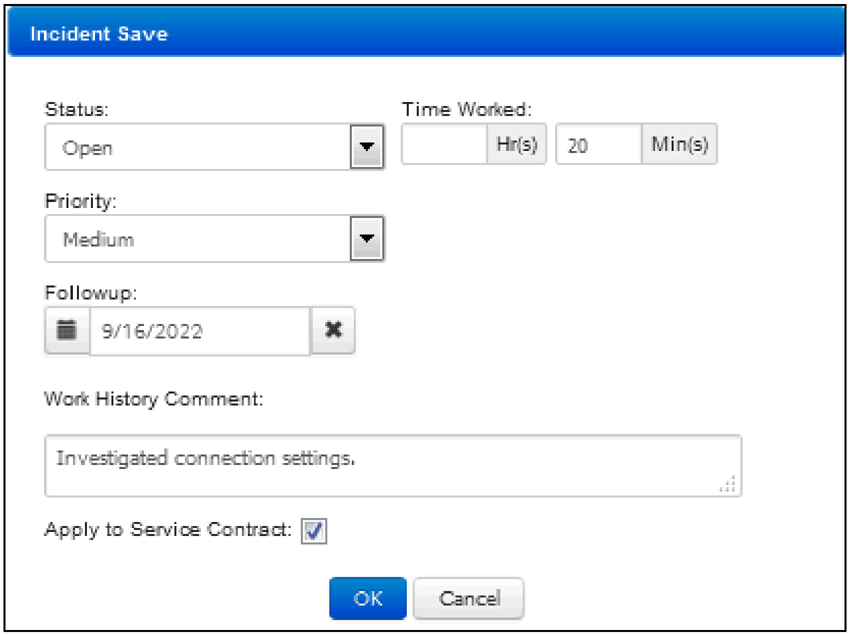
- Select Daily to create an incident every weekday or specified number of days.
- Select Weekly to create an incident on a specified weekday (Sunday-Saturday) for an interval of a specified number of weeks.
- Select Monthly to create an incident for an interval of a specified number of months. Then select the day of the month on which each incident should be created.
- Select Yearly to create an incident yearly on a specified month and date or specified day of the week on a specified month.

Saving the Incident

Do one of the following:

- To save an incident without closing the window, select Incident | Save.
- To save an incident and close the window automatically after completing the Incident Save dialog, select Incident | Save and Exit.
- To save an incident and close the current session, select Incident | Save and Logout. This option is enabled in configuration and is typically used when accessing an incident via a link in an email.

If configured, the Incident Save dialog appears:



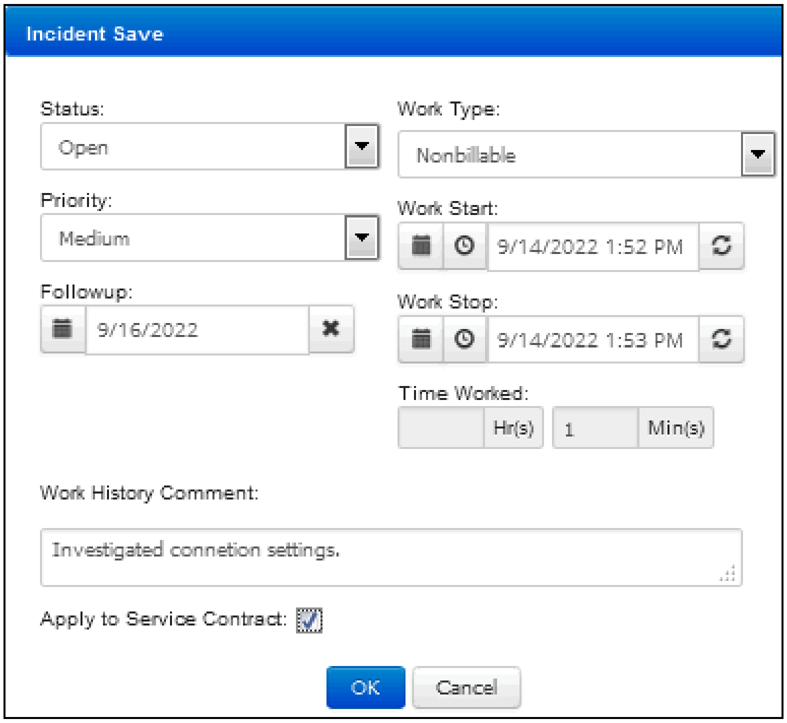
Do the following:

- Select the status of the incident in the Status field. If the issue is resolved, select Closed. If configured, a prompt will appear for creating a knowledge entry using the categorization, issue description, and issue resolution. The knowledge entry will have a status of Pending Approval.
- Select the priority for the severity of the issue in the Priority field.
- Enter the hours and minutes you worked on the incident in the Time Worked field. (You can also enter this information in the History field.) If enabled during configuration, you may be required to complete this field.
- If the Followup Date field is enabled during configuration, select the date on which, if the incident is not closed, a followup reminder email should be sent to the assignee of the incident.
- If an hours-based service contract is in effect for the incident, select the Apply to Service Contract checkbox to apply the amount entered in the Time Worked field to the contract.

If configured, Work Type and/or Work Start and Work Stop fields may be included in the Save dialog. Options in the Work Type field are specified in configuration.

The Work Start field defaults to the date and time when you load the work item. For example, if you open a new incident at 1:00 PM, work with the customer for 30 minutes, and then select the Add Work history option or save and display 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.

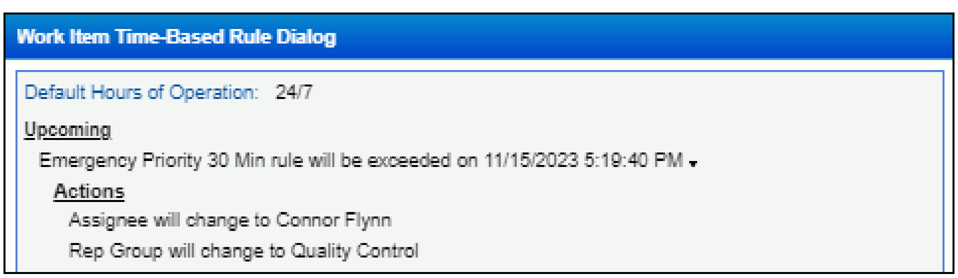
The Work Stop field defaults to the current time, but there will be at least a one minute gap between the Start and Stop times. You can type directly in the Work Start and Work Stop fields or calendar and clock to select the date and time; the difference will populate automatically. Select refresh to 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).



Viewing Rule Information

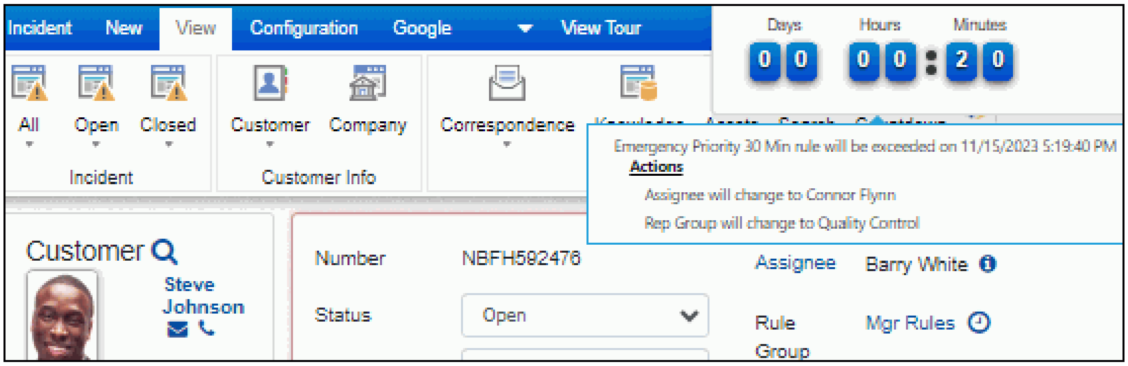
Rules can be configured to automatically perform actions when conditions are met upon save of a record or after a certain time interval. Actions can include changing incident field values, routing via load balancing or the round robin method, sending notifications, initiating an approval cycle, and posting data to a web application. Rules are included in rule groups that are applied to incidents through customers, companies, category combinations, and incident and hierarchy templates; a default rule group will apply if none are applicable. When an incident is saved, the matching rule group is first determined and then all rules in that matching rule group are evaluated. If a rule's conditions are met, its actions are performed. The online help contains more information on rules.

Select the name of the rule group in the Rule Group field to display the Time-Based Rule dialog with actions that will be and have been taken by any time-based rules in the current rule group. The Hours of Operation link displays the time frames in which the rule group is in effect. Note that entries will include the term "fulfilled" if a rule is invalidated or reset due to a change in rule configuration. Time frames reflect the assignee's support center time zone; the actual action dates and times will depend on execution of the Time-Based Rule agent.



Select View | Countdown to display a dialog containing a countdown clock in the upper right corner with the time remaining until the next action. If a pending time-based rule has not been exceeded, a blue countdown clock will appear; if the time-based rule has been exceeded, a red countdown clock will and the numbers will increment to display the amount of time that has passed since the time at which the rule was last exceeded. You can use the Show

Seconds on Countdown field in the Desktop Preferences screen to control display of the Seconds portion of the countdown clock.



To display all actions that have been performed by rules, use the Rule option in the History field.

Assigning and Routing

To route an incident, you can either select Route or the Assignee link. (Note that you can also route one or more incidents via the Desktop.) There are several methods of routing; some or all of these methods of routing may be available to you depending upon configuration settings.

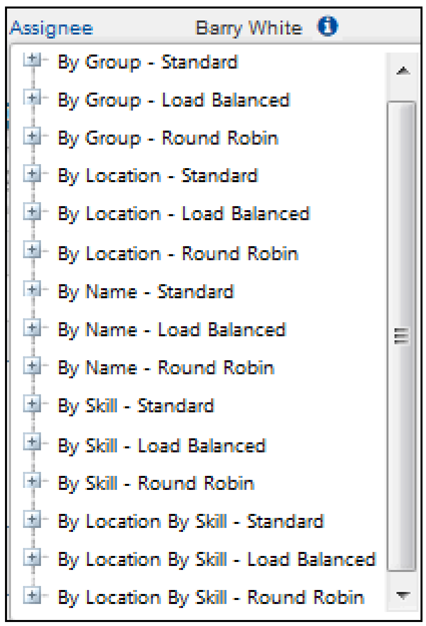
- **Group Based/Standard:** A list of groups appears; when you select a group, a list of support representatives in the group appears for selection. (These groups are set up in Support Representative records.)
- **Group Based/Load Balanced:** The available support representative within the selected group with the lightest overall workload will be selected.
- **Group Based/Round Robin**: The support representative in the group who was assigned an incident using the round robin method on the oldest date and time is selected.
- **Location Based/Standard:** A list of all available support representatives in a selected location appears.
- **Location Based/Load Balanced:** The support representative with the lightest workload within a location is selected.
- **Location Based/Round Robin:** The support representative in a selected location who was assigned an incident using the round robin method on the oldest date and time is selected.
- **Name Based/Standard:** A list of all available support representatives appears.
- **Name Based/Load Balanced:** The support representative with the lightest workload is selected.
- **Name Based/Round Robin:** The support representative who was assigned an incident using the round robin method on the oldest date and time is selected.
- **Skill Based/Standard:** The category levels selected for the incident will appear; select the level of categorization that exactly matches the categorization for which support representative skills should be searched. The support representative(s) with those skills will appear for selection.
- **Skill Based/Load Balanced:** After you select the level of categorization for which support representative skills should be searched, 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.
- **Skill Based/Round Robin**: After you 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 using the round robin method on the oldest date and time is selected.
- **Location by Skill/Standard:** Support representative locations will appear; after selecting a location, the category levels selected for the incident will appear. Select 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 listed for selection.

- **Location by Skill/Load Balanced**: Support representative locations will appear; after selecting a location, the category levels selected for the incident will appear. Select the level of categorization that exactly matches the categorization for which support representative skills should be searched. The support representative in the selected location with matching skills and the lightest workload is selected.
- **Location by Skill/Round Robin**: Support representative locations will appear; after selecting a location, the category levels selected for the incident will appear. Select 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 using the round robin method on the oldest date and time is selected.

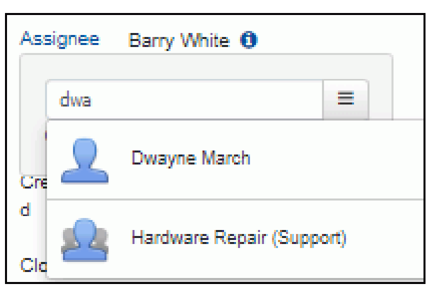
Load balanced routing involves weights based on incident priority; these weights are set up in configuration. If a support representative has worked with an incident and the incident is reassigned, he/she will be bypassed until all available support representatives with the skill or in the group or location (depending on the method selected) have worked with the incident.

If you select **skill based standard routing**, you'll select the level for which associated support representative skills should be searched. Support representatives with skills/categories in their Support Representative records that *exactly match that categorization level* will appear for selection. If you selected a method with load balanced routing, the name of the person calculated to have the lightest workload will appear.

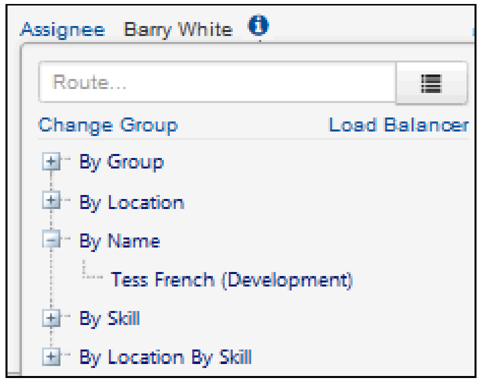
If you select Route or the Assignee link with the Tree Selector, all of the configured routing methods and options will appear.



If you use the Assignee link and name-based routing is enabled, you can perform a standard name-based route by entering the first few letters of a support representative's name:



You can also select the Load Balancer link to display the name of the support representative calculated to have the lightest workload for each routing method.



To view the assignee's contact information, skills, and groups, select the View Rep Details link after selecting information next to the Assignee field.

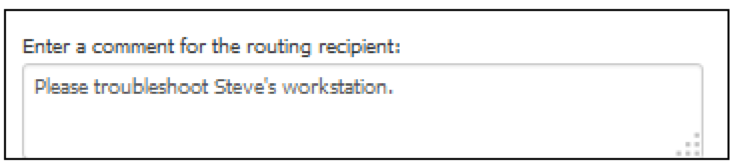
A permission can enable you to route to unavailable support representatives; if you have this permission, support representatives who are unavailable for routing will be included with an asterisk.

Routing to Yourself

To route an incident to yourself (for example, if incidents are first routed to a queue), select Incident | Actions | Route and select Route to Self. Your primary group will be used. If you wish to change your group, you'll need to use the Change Assignee's Group option or the routing dialogs (via the Route icon or Assignee link).

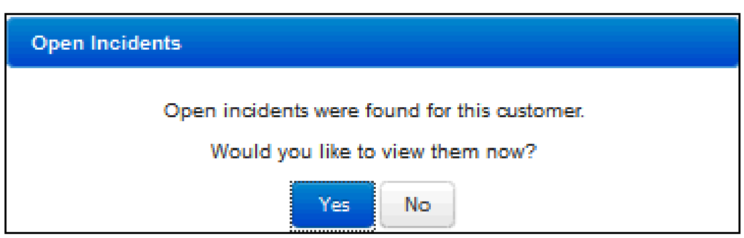
Entering Routing Comments

A routing comment dialog may be configured for entering a note to be included in a routing notification.



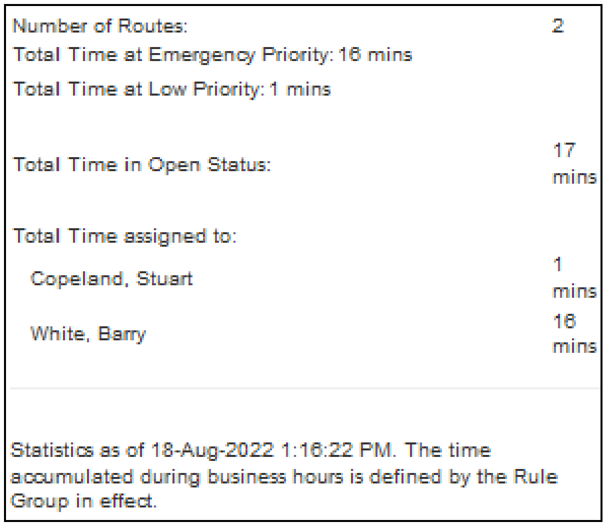
Routing Multiple Incidents via the Desktop

You can route incidents with an Open or Suspended status from views on the Desktop. Select the incidents to route and then select the Route view action. The routing dialogs will appear, but the skill-based routing and location by skill based routing methods will not be available. If load balanced routing is used, the selected incidents will be distributed evenly to the available support representatives in the selected group, location, or all (if using name-based routing). The same comment will be applied to all routed incidents. Note that incidents that are closed or pending approval cannot be routed.

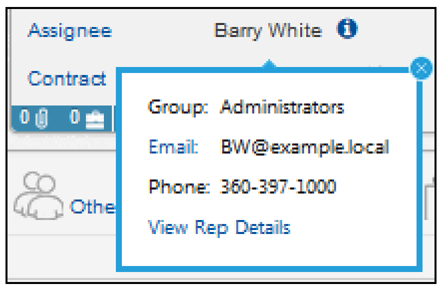


Viewing Routing Information

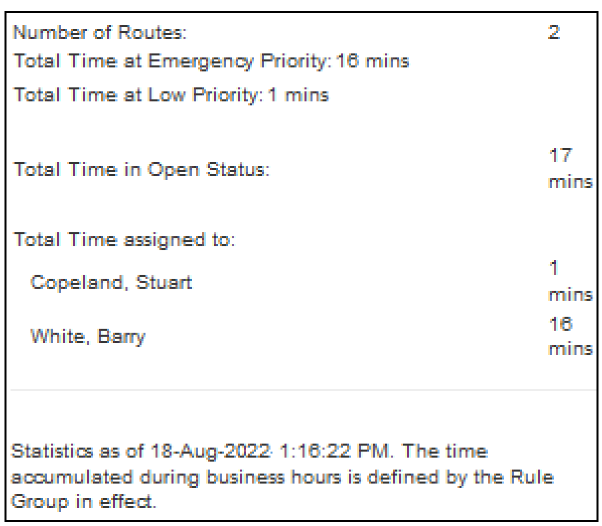
The News Feed and Audit History entries in the History field include routing details. To view the number of times the incident has been routed, total time by status and priority, and the amount of time the incident has been assigned to each assignee, select View | Routing/Time Statistics.



Select information next to the Assignee field to display the assignee's group, email address, and phone. You can select the Email link to send an email to the assignee.



To view the assignee's contact information, skills, and groups, select the View Rep Details link. You can send an email or page from this dialog.

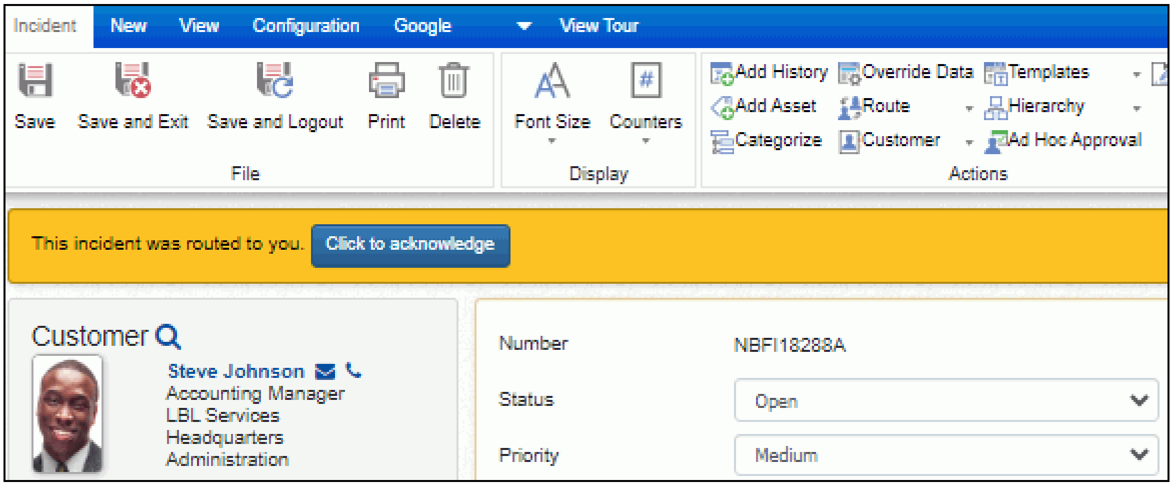


Changing an Assignee's Group

If an assignee is a member of more than one group, you can select Incident | Actions | Change Assignee's Group to change the assignee's group membership for an incident. Select the appropriate group in the Select Group dialog.

Acknowledging a Routed Ticket

If ticket acknowledgments are enabled in configuration, the following alert bar will appear at the top of the Incident screen to the new assignee:

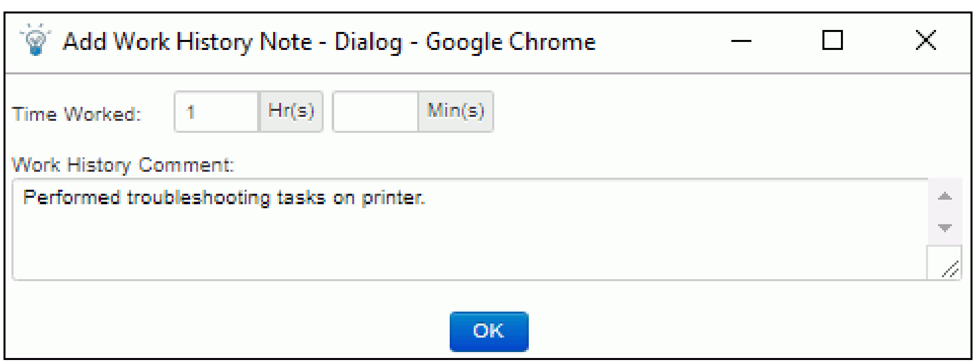


When the assignee selects the Click To Acknowledge button, an entry will be recorded in the Audit History field and an acknowledgment notification will be sent if configured.

Adding Work History and Viewing Historical Information

Entering Work and Customer Work History

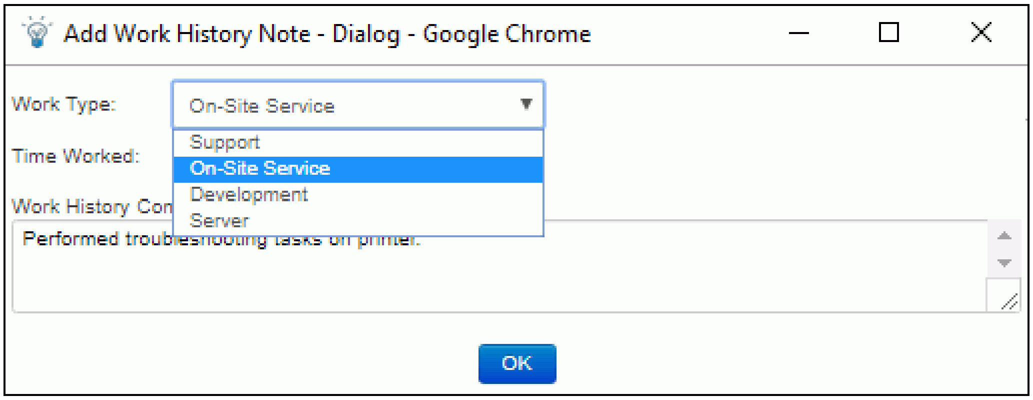
Use the History field to enter and view information on any activities related to resolving the incident. You can use this field to document customer contacts or conversations with customers or support staff. Call scripts may be configured to be included. This field is useful when routing an incident to another support representative because it allows them to see the work that has been performed. To enter information on any activities related to a change**,** select Add History on the ribbon bar or Add Work History in the History field. For example, you can document customer contacts or conversations with customers or support staff. This field is useful when routing a Change record to another support representative because it allows them to see the work that has been performed. If configured, you may be required to make an entry in the Time Worked field after entering work history.



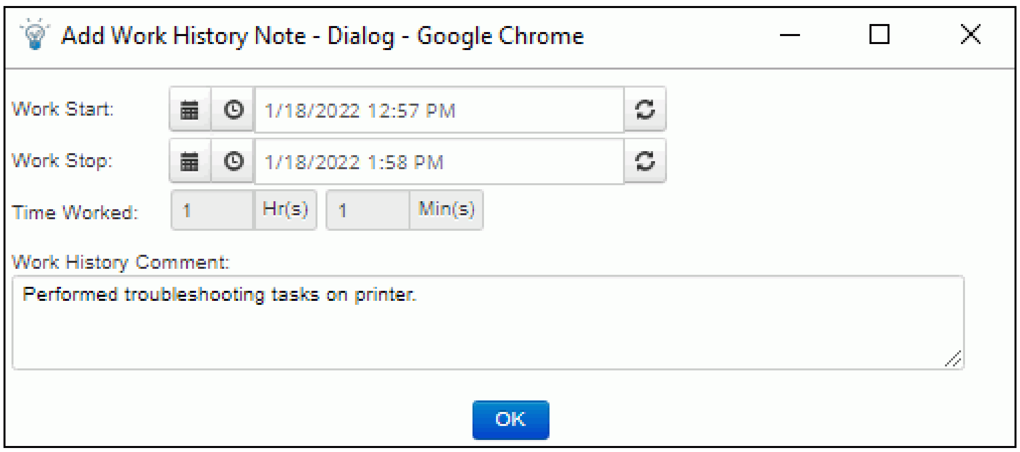
If an hours-based service contract is in effect, you can select the Apply to Service Contract checkbox to apply the amount entered in the Time Worked field to the contract.

The following options may be configured:

- A Work Type field may be included with options for describing the type of worked performed.



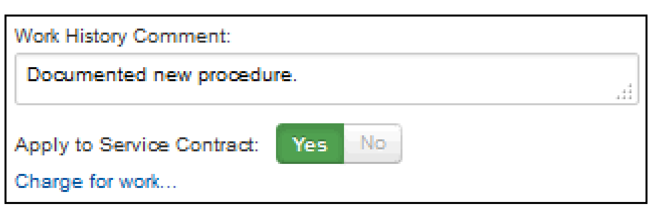
- Work Start and Work Stop fields may be included.



The Work Start field defaults to the date and time when you load the work item. For example, if you open a new request at 1:00 PM, work with the customer for 30 minutes, and then select the Add Work history option or save and display 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.

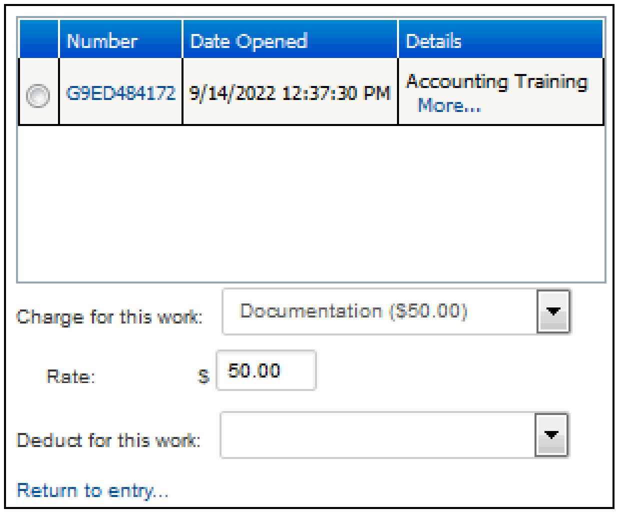
The Work Stop field defaults to the current time, but there will be at least a one minute gap between the Start and Stop times. You can type directly in the Work Start and Work Stop fields or select calendar and clock to select the date and time; the difference will populate automatically. The refresh 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).

- If Purchasing functionality is enabled and you are designated as a vendor in your Support Representative Profile record, you can add a charge (an amount of time worked multiplied by a rate) as a separate line item or use a charge to decrement an existing line item on an associated purchase order.After entering the time worked, select the Charge for Work link.

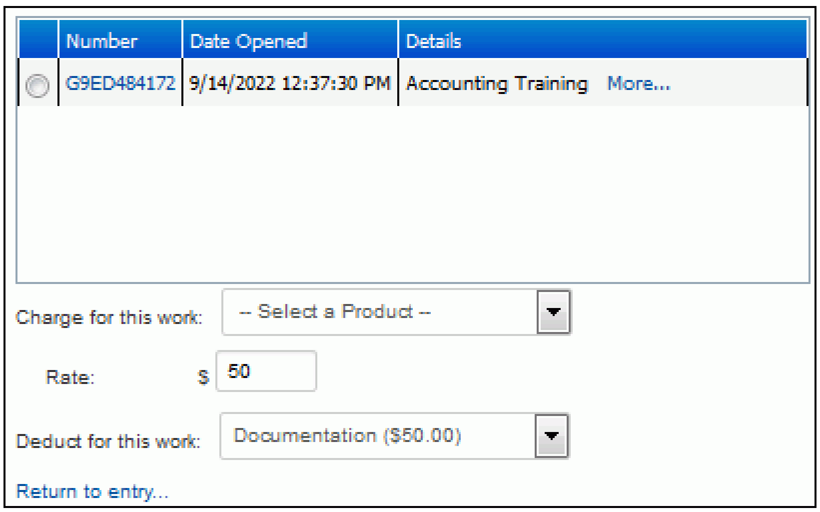


The purchase orders associated with the change appear; select the purchase order for which the charge should be applied. Then:

- **Add a separate line item charge** to the purchase order (increasing the total amount). Choose the product from the selected purchase order in the Charge For This Work field. (Only decimal-enabled products will appear in this list.) In the Rate field, enter the amount to be multiplied by the entry in the Time Worked field in the previous dialog.

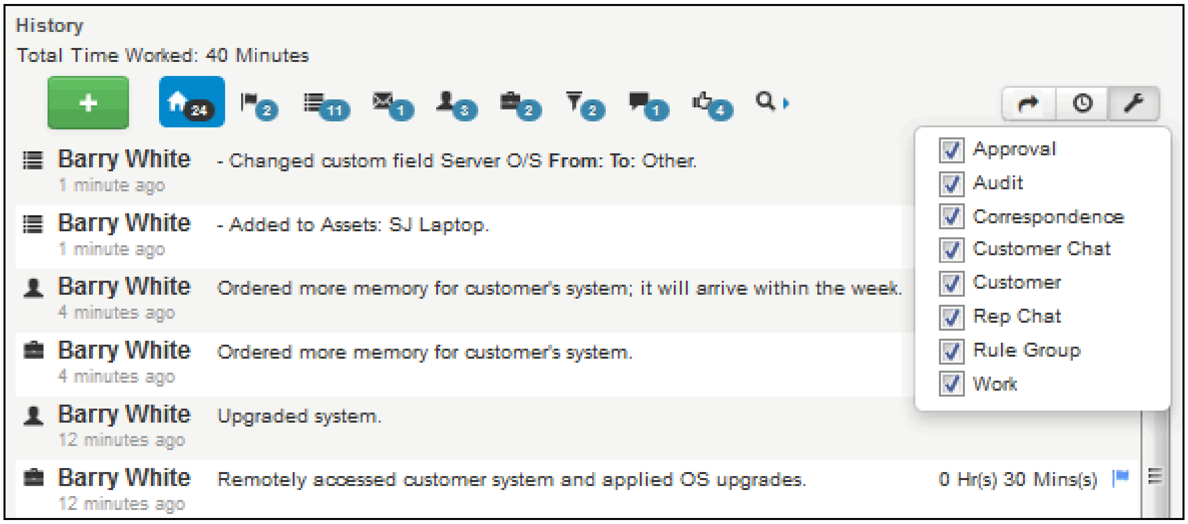


- **Use the time worked as an amount received on** an existing line item quantity on a purchase order, in the Deduct For This Work field, choose the line item from the selected purchase order. (Only decimal-enabled products will appear in this list.)

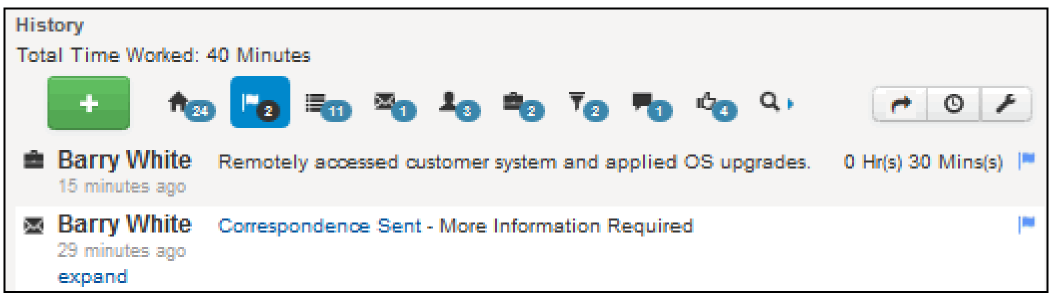


Viewing History

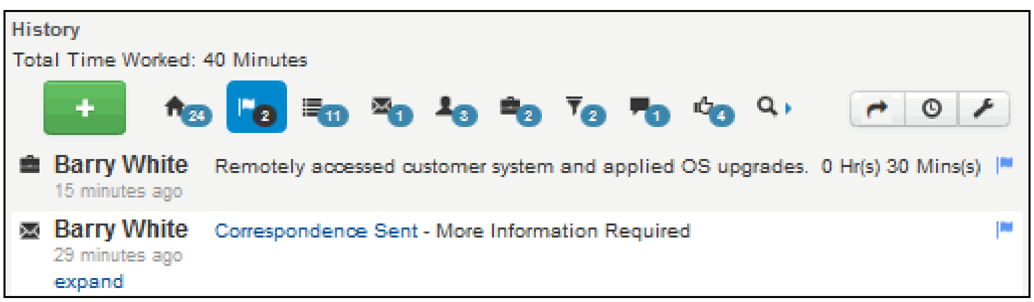
Use the History field to view notations on all incident actions. You can flag work history and correspondence entries via Mark as Important that appears when you hover over those entries with your cursor. Once marked, it changes to Unmark as Important for removing the flag. Note that the Ref ID that appears on expanded correspondence entries is included for reference; it is used by iSupport's email processing engine.



- Feed displays a list of all actions performed on the record; you can filter the content via Settings.
- Important displays work history and correspondence entries that have been flagged as important via Mark as Important; it appears when you hover over work history and correspondence entries with your cursor.

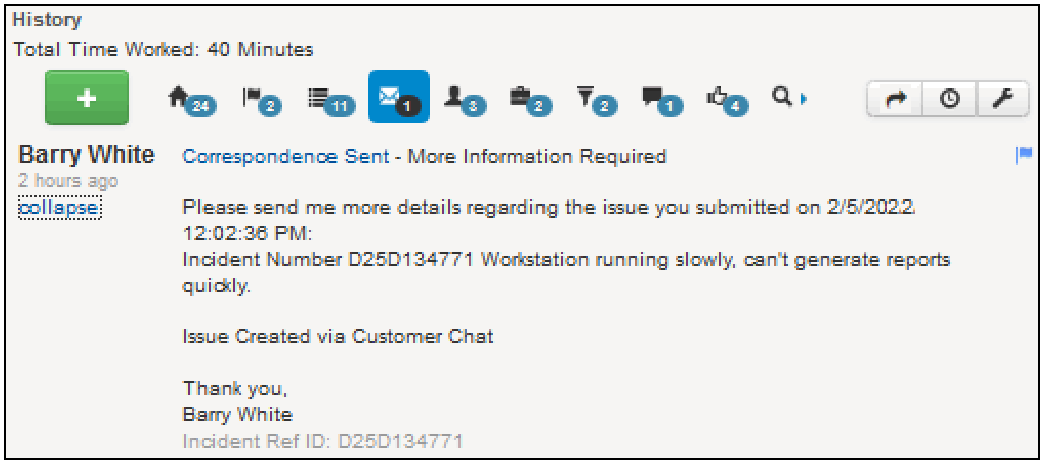


- Audit includes entries on functions performed by the system and support representatives (for example, field changes), as well as correspondence entries. Work history, chat, and approval entries are not included.

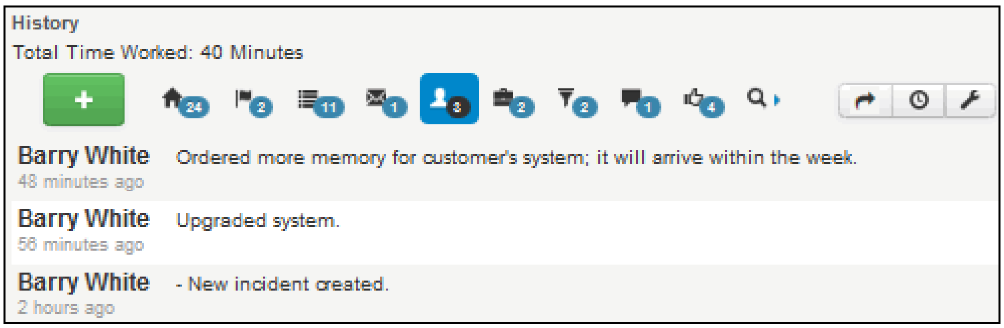


- Correspondence displays entries for sent and received correspondence, including the subject line and body of the correspondence. The Correspondence Received and Correspondence Sent links display the

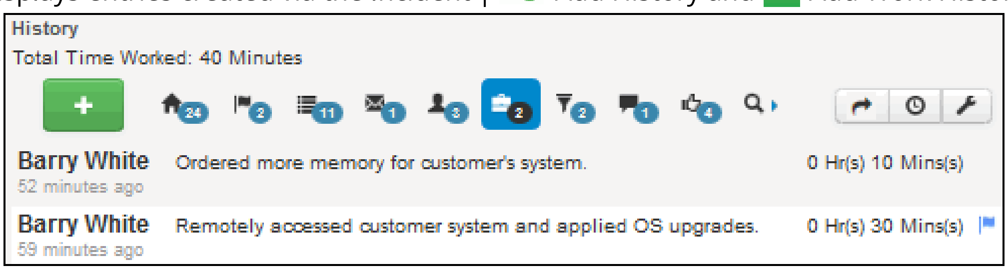
Correspondence screen. Note that the Ref ID that appears on expanded correspondence entries is included for reference; it is used by iSupport's email processing engine.



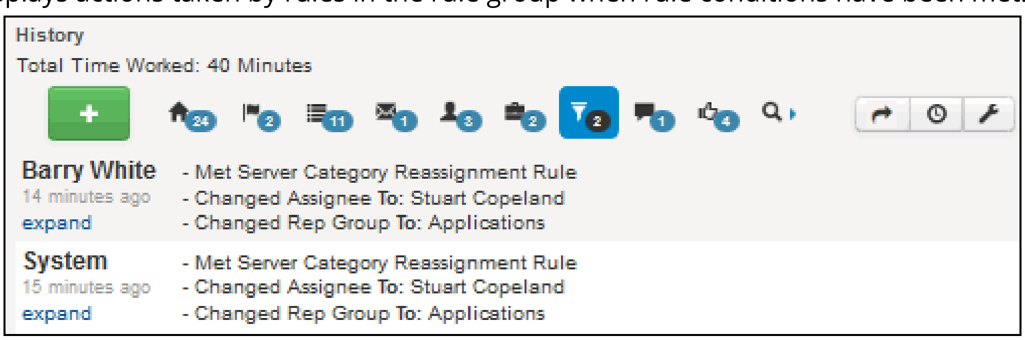
- Customer displays customer work history entries (from the Customer Work History dialog that can be configured to appear after the Work History dialog) as well as generic customer audit history entries.



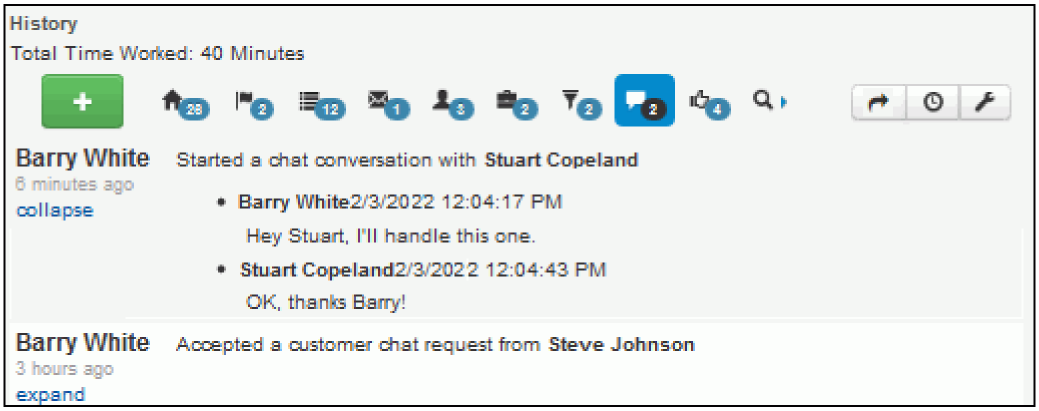
- Work displays entries created via the Incident | Add History and Add Work History icons.



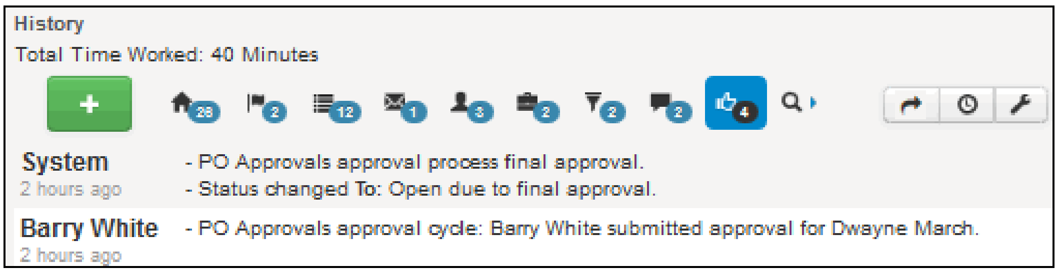
- Rule displays actions taken by rules in the rule group when rule conditions have been met.



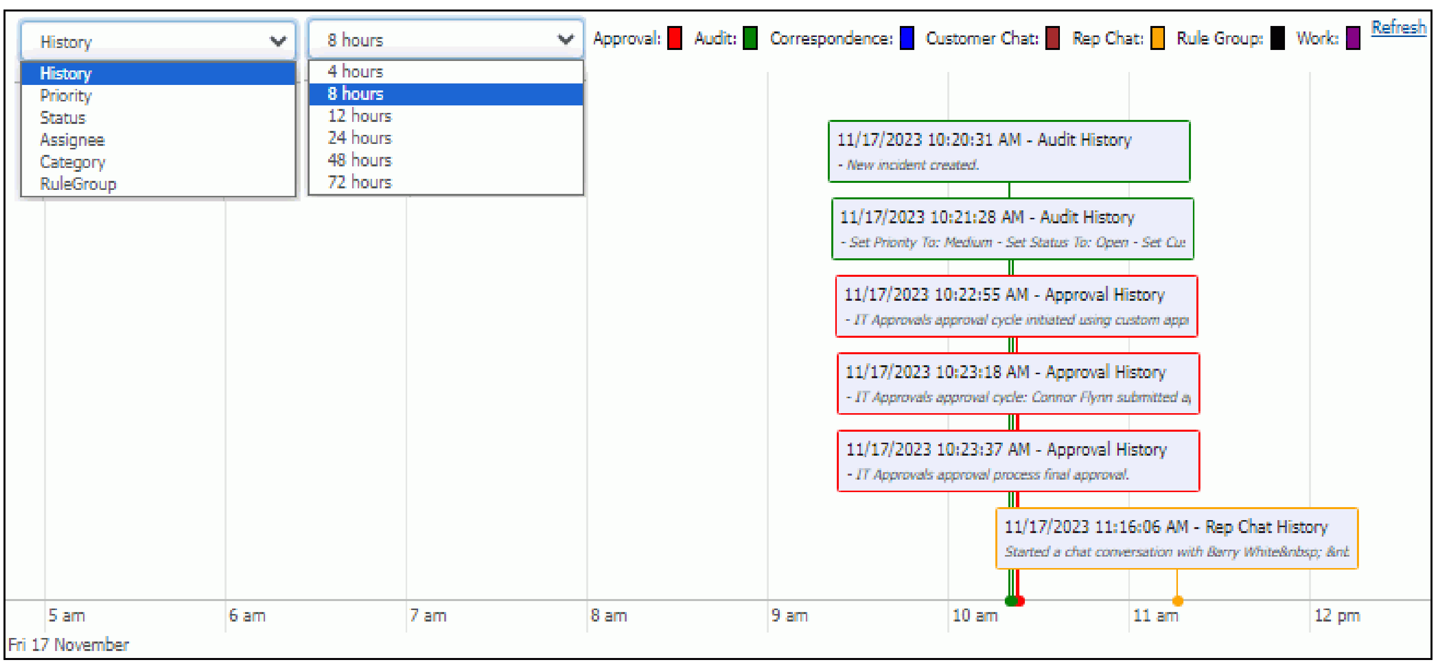
- Chat displays information on a customer chat that created the incident, as well as chats initiated via the Awareness feature for the current incident. For more information, see "Using Awareness and Chat Functionality" on page 44.



- Approvals displays entries for any approval actions. For more information on incident approvals, see "Working With Approval Cycles" on page 24.



- Search enables you to enter a search string for searching history entries.
- Open in New Window displays a filterable feed of history entries in a new browser window.
- Select View Timeline at the top right of the history entries to display historical incident events on a timeline. Use the dropdown fields to select the types of entries to display and the timeline increments. You can use your mouse to scroll the green hour bar and red month bar at the bottom of the screen.

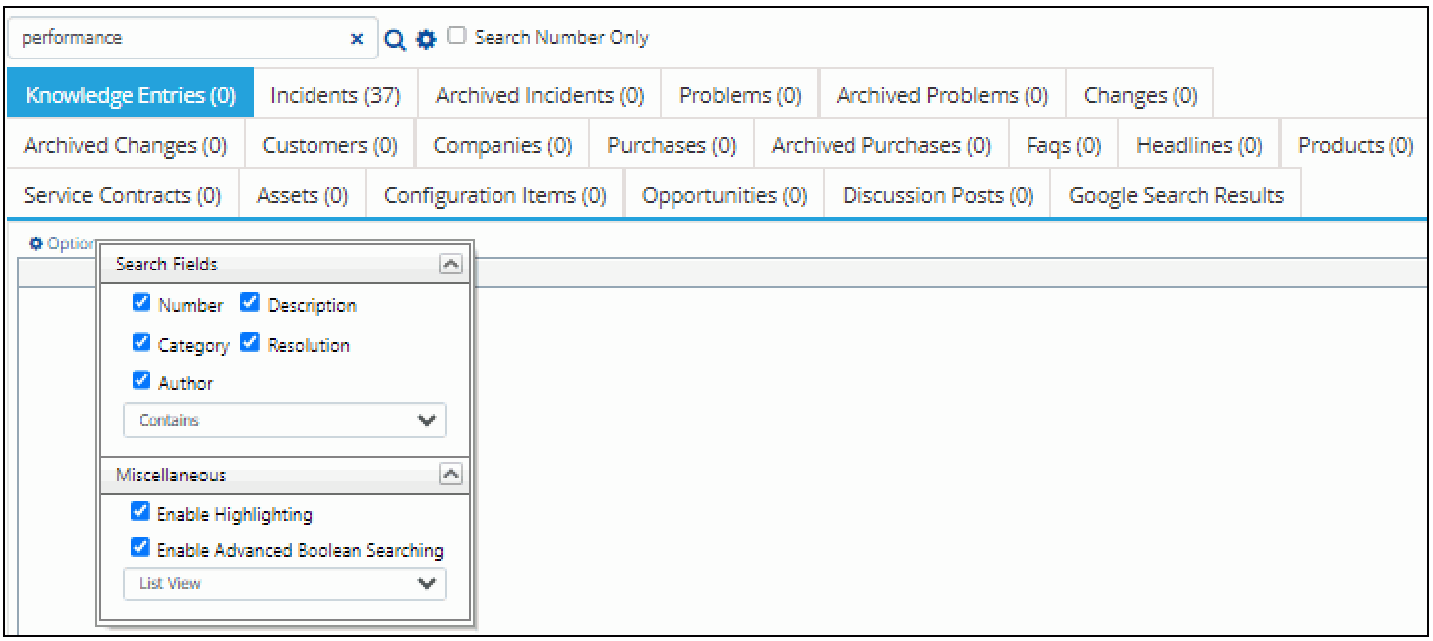


Using the View Menu

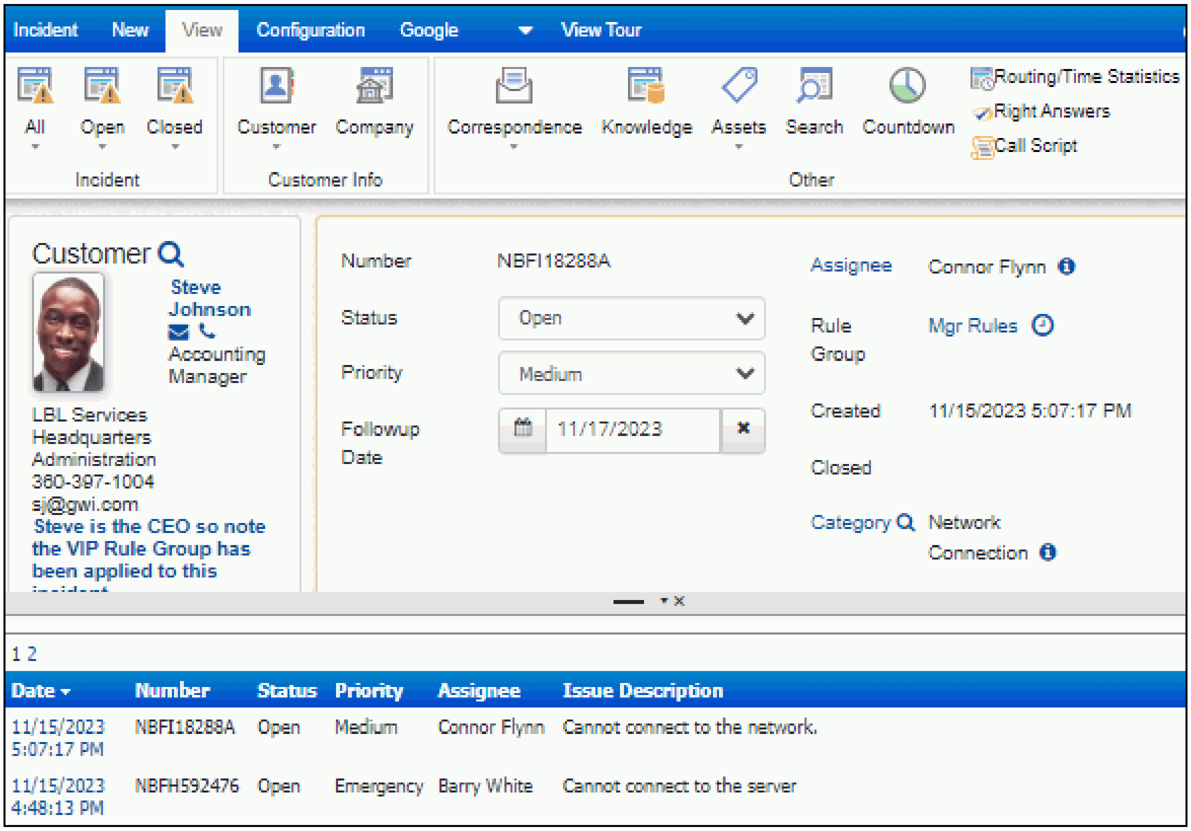
Use options on the View menu to display the following:

- Open, closed, or all **incidents** for the asset, category, customer, or the customer's company, location, or department.
- The selected **customer**'s profile record and the profiles of additional customers.
- The **company** profile associated with the selected customer.
- All **correspondence** associated with the current incident, associated with the customer selected for the incident, and associated with the configuration associated with the change.
- **Knowledge** entries that have same categorization as the current incident.
- The **assets** selected for the incident or all of the customer's assets.
- **Routing/time statistics**, including the number of times the incident has been routed, total time by status and priority, and the amount of time the incident has been assigned to each assignee.
- The **call script** associated with the category selected for the incident.

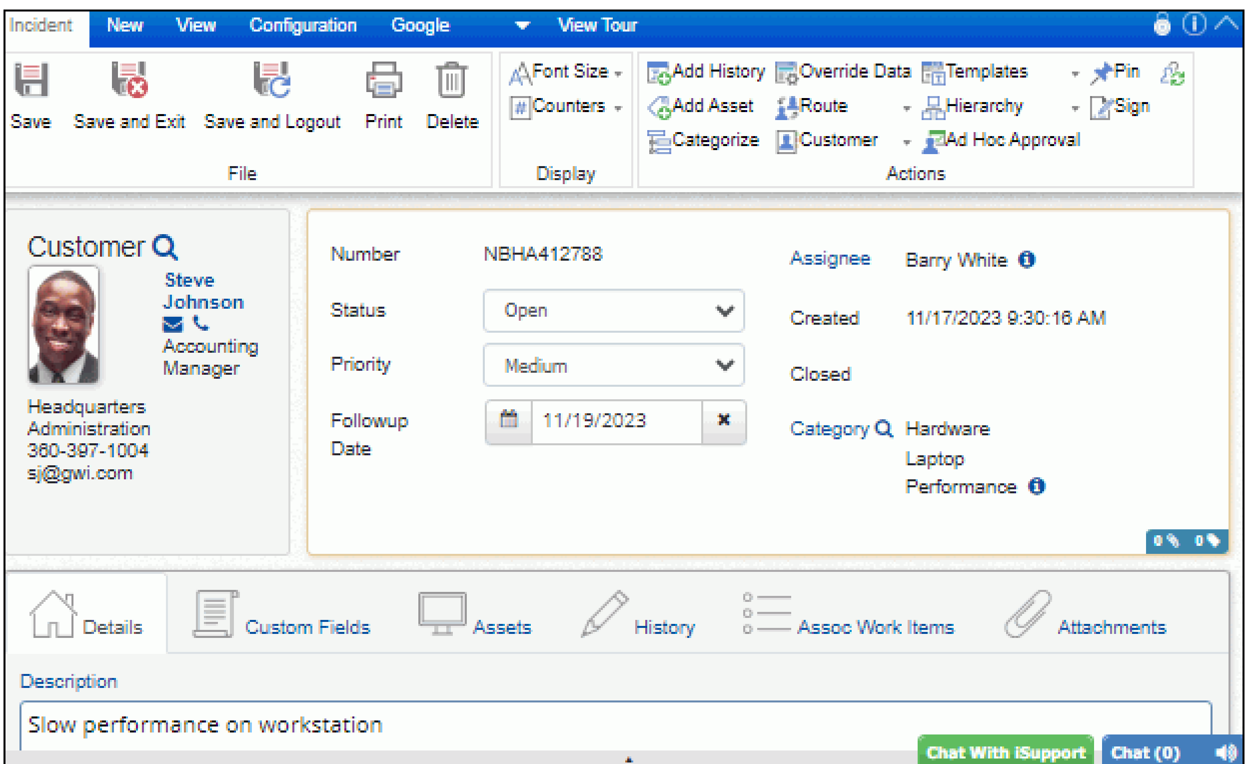
You can also select Search to perform a **global search** on iSupport data using keywords and, if searching knowledge, Boolean operators (And, Or, Not as well as parenthesis to group words and phrases). You can include Google in the search if configured in configuration. In the Global Search dialog, select settings to select incident fields for narrowing the search. Use the Options link on each tab to select the fields to search, the type of search (Starts With, Contains, Ends With and Is), enable text highlighting, select the type of view in which search results are displayed (list or classic), and sort options.



View and ticket count results will display at the bottom of the screen.

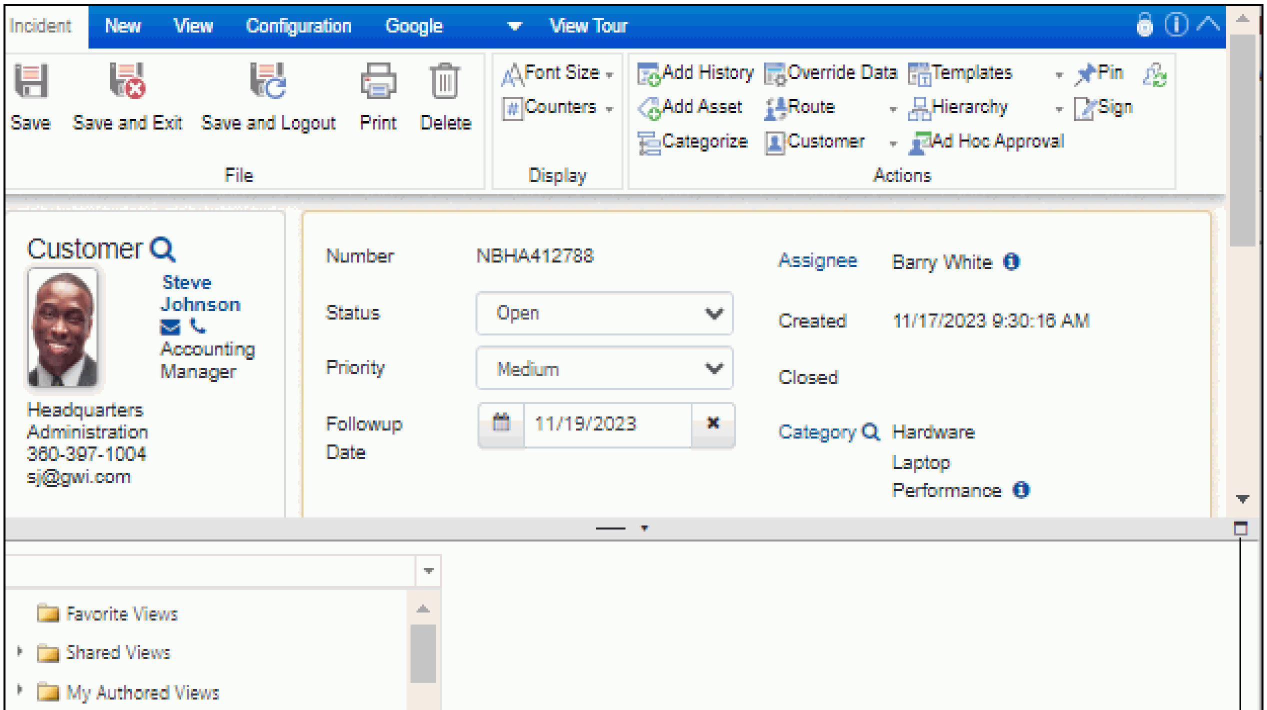


The frame will be minimized by default; select the up arrow icon to expand and collapse the frame.



Select to expand and collapse the frame

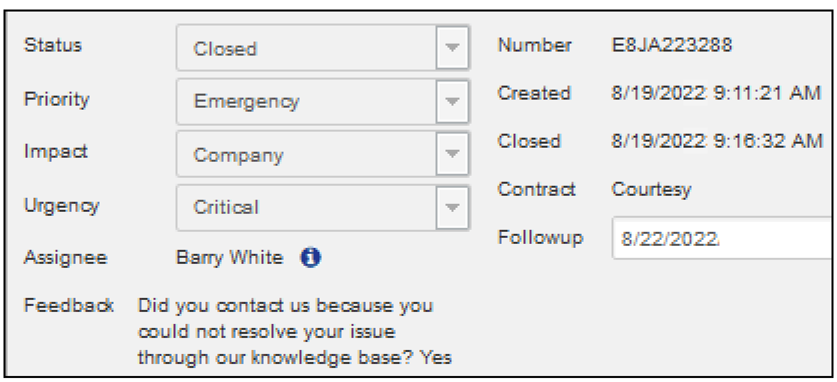
Select Open In New Window to display the view in a new window.



Select to open the view in a new window

Viewing Incident Feedback

If configured, a question with two response choice image links can be included in an incident notification; when a customer receives the email and selects 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.



Working With Approval Cycles

Approval cycles require tickets to be approved by designated approvers before most incident functions can be performed. (However, a configuration setting can allow modifications to incidents under approval.) Approval cycles are set up in the Configuration module, configured with serial or concurrent approvers, notifications, and statuses for each stage of the process. Approvers can be support representatives or customers (who specify a verdict via the mySupport portal), and approver delegates can be designated for support representatives and customers. An approval cycle can be associated with a customer profile, company record, or category.

A rule/rule group can require one or more approval cycles to go into effect:

- The initial approval cycle

- Any cycles associated with a customer profile, company record, or category
- The final approval cycle

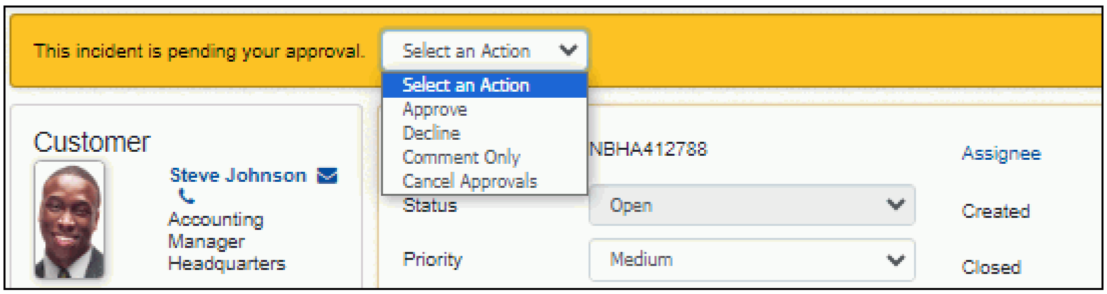
Approval functionality is not affected by the business hours configured for a rule group. When an incident is saved with a rule group that requires approvals, the approval cycle will go into effect automatically. If any approval cycle results in a Decline verdict, no further cycles will apply. If a rule-group-required cycle is completed or canceled, the Incident menu will contain an Incident | Actions | Ad Hoc Approval option for starting another approval process.

Approval cycles can also be designated as available for you to initiate in the Incident screen on an ad hoc basis if the incident is not currently pending approval.

If an approval cycle is in effect, an alert bar will appear at the top of the Incident screen after the incident is saved and most of the ticket fields will be disabled. (However, you can send correspondence and update work history.)

Specifying a Verdict

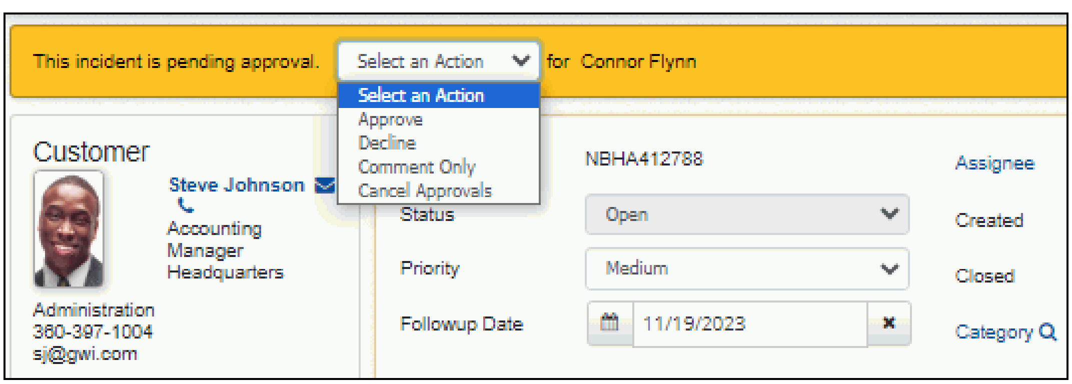
An action dropdown field will appear in the approval alert bar if you are the current approver in the approval cycle or if you have permission to override approvals.



Select one of the following:

- **Approve** to enable the next approver to specify a verdict or, if it is the final approval, complete the cycle.
- **Decline** if you do not wish to enable functionality on the ticket. An entry will be required in the Comments field. One or more Decline verdicts may be needed to stop the cycle.
- **Comments Only** to enter any comments without approving, declining, or canceling the cycle. The comments will be included in notifications sent to recipients configured for the approval cycle.
- If you have permissions, you can specify **Cancel Approvals** to cancel the cycle. An entry will be required in the Comments field; the comment will be appended to the text in the Resolution field. An approval cycle can also be canceled by the customer assigned to the incident.

If you are not the current approver but you have approval override, the following will appear:

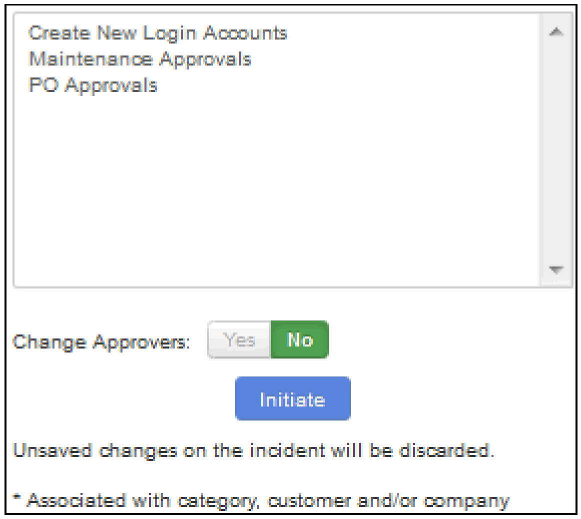


When you specify a verdict, configured notifications will be sent and the incident status changes to the status designated by the approval cycle if it is a cancellation, final approval, or final decline.

If a rule-group-required cycle is completed or canceled, the Incident menu will contain an Initiate Approvals option to restart the approval process.

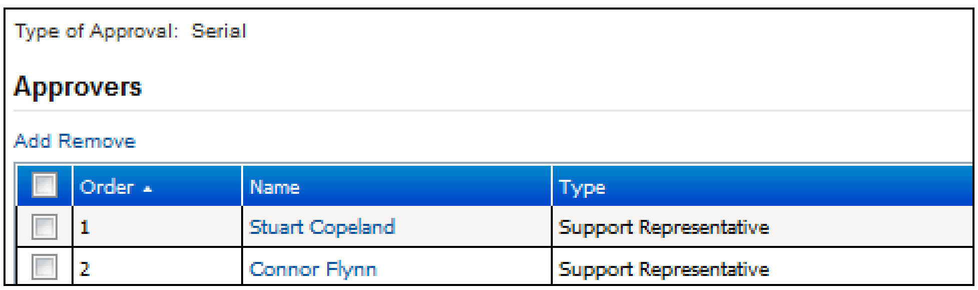
Initiating an Approval Cycle

To initiate an approval cycle in the Incident screen, select Incident | Approvals | Initiate Ad Hoc Approval after an incident has been saved. The following dialog appears with the approval cycles designated as available for ad hoc use. The cycle will be enabled for the incident after the Initiate button is selected.



An active ad hoc approval cycle for an incident will not be canceled 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.

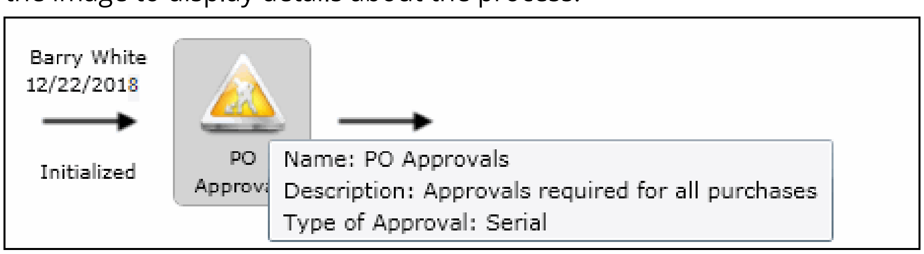
The Change Approvers checkbox will display if permissions are configured; select it to display the following dialog for adding or removing the approvers configured for the selected cycle.



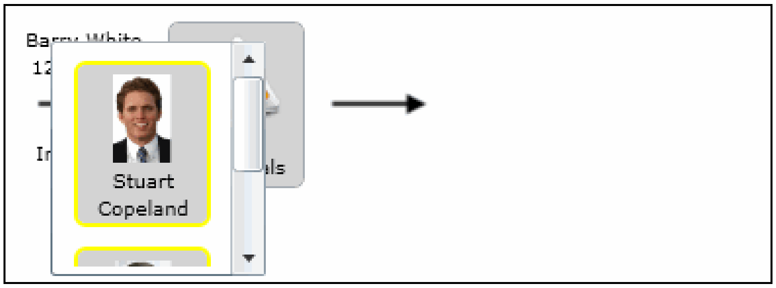
Note that the approver cannot be changed if an approval cycle is configured to be available for ad hoc use and configured to use the approver associated with the selected customer.

Viewing Approval History

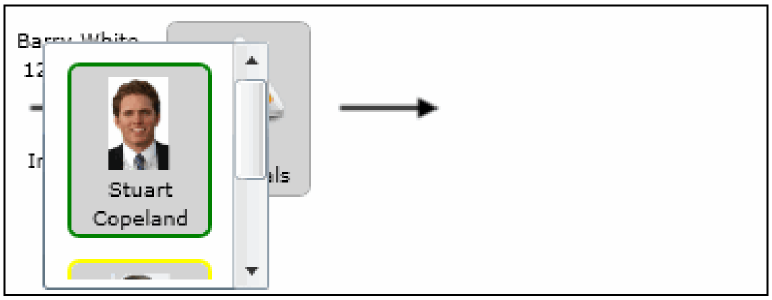
Select View | Approvals to view a graphic display of the approvers and status of each approval in the approval process. Mouse over the image to display details about the process.



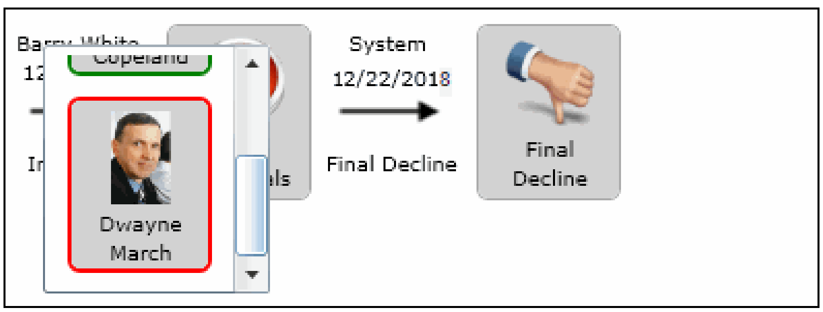
Pictures are associated with support representatives in the Support Representative Profile screen and with customers in the Customer Profile screen; if a support representative is involved in an approval cycle, the associated picture will appear when you select an image as shown below. The picture will be outlined in yellow if the approver is next in the approval process.



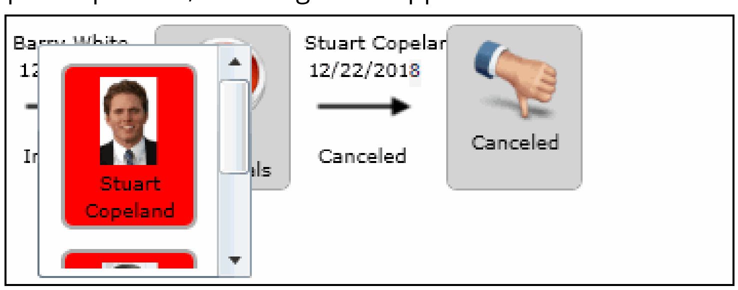
The picture will be outlined in green if the approver specifies an Approve verdict.



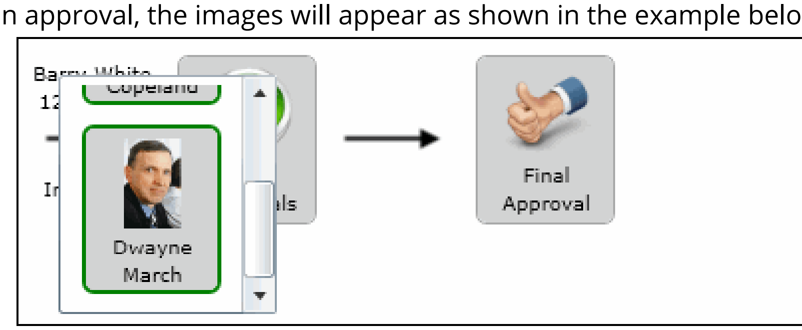
If an approver specifies a Decline verdict, the images will appear as shown in the example below.



If an approver cancels the approval process, the images will appear as shown in the example below.



If the process results in an approval, the images will appear as shown in the example below.

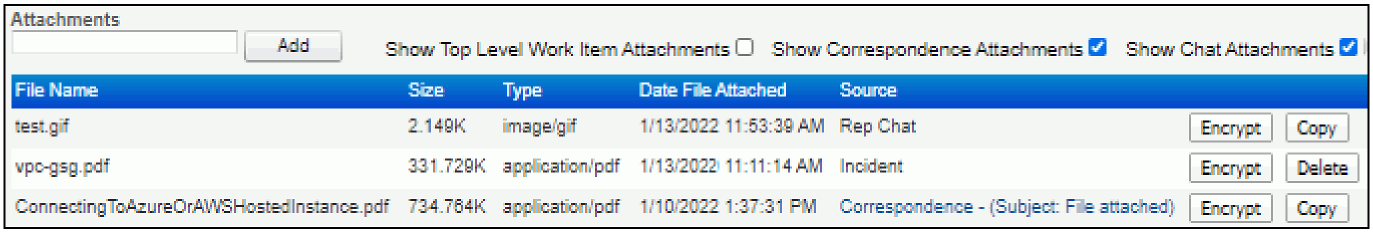


Use the Approvals option in the History field to view approval actions.

Associating Other Work Items and Files

Attaching Files

To attach a file to the incident, select the Add button in the Attachments field and select the file. You can select the Show Correspondence Attachments checkbox to display attachments from all sent or received correspondence (including attachments from an inbound email update) associated with the incident. If the incident was created via a chat or a chat was initiated while the incident was open, use the Show Chat Attachments checkbox to display any files attached during the chat. A Copy button will be included next to correspondence and chat attachments; you can use it to directly associate the attachment to the incident.

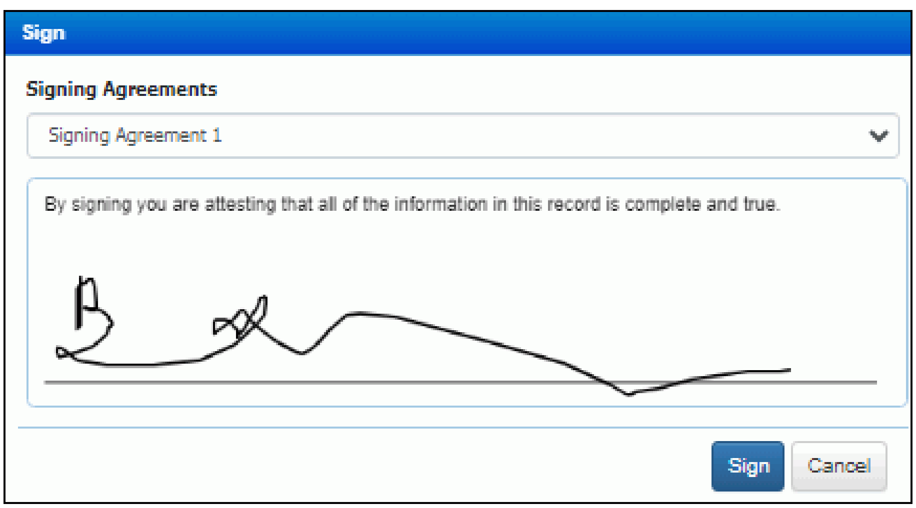


Use the Show Top Level Work Item Attachments field to display any files attached directly to the top level parent incident in a hierarchy; this field is enabled via the Cookie Defaults | Attachments tab in the Support Representative list screen.

If you are working on an incident created from an email submission, a link to the correspondence is included in the History field and attachments are placed in the Attachments field of the correspondence. If there is an alternate version of the body of the email (created by the email application), if configured it will be saved as a document and placed in the Attachments field of the correspondence.

Attaching a Signature

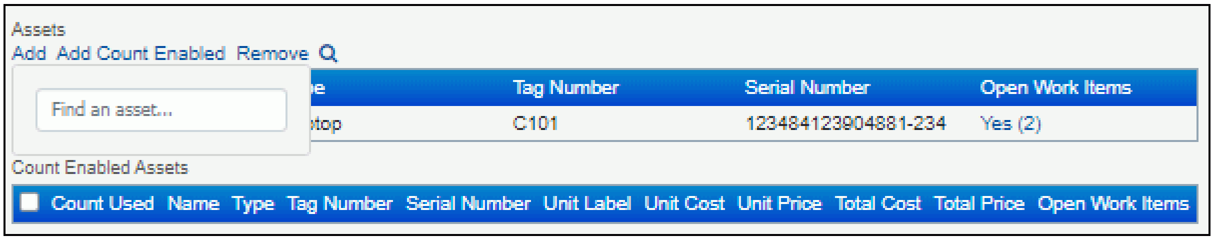
Use the Sign feature to display a dialog for signing using a touch screen or mouse. Select the signing agreement applicable to the incident; this text is set up in configuration and can be associated with customer and support representative groups, categories, and incident and change templates.



The signature image and text will be saved as a .png file and included as an attachment.

Associating Assets and Performing Scans

Use the Asset field to associate Asset records with an Incident record and display any other open incidents, problems, or changes associated with the asset. To search for an asset, select Select Asset and enter a search string. The asset type, name, owner, tag number, location, serial number, model, manufacturer, purchase date, and comments will be searched. If one record results from a type ahead search, that record will be automatically selected and added to the work item.



You can also perform asset scans from the Incident screen. Asset scans collect hardware, software, and service details automatically. You can scan non-Windows SNMP-enabled devices in your network, computers with Windows 98 and above, or any other WMI-compliant machine (WMI must be installed and active).

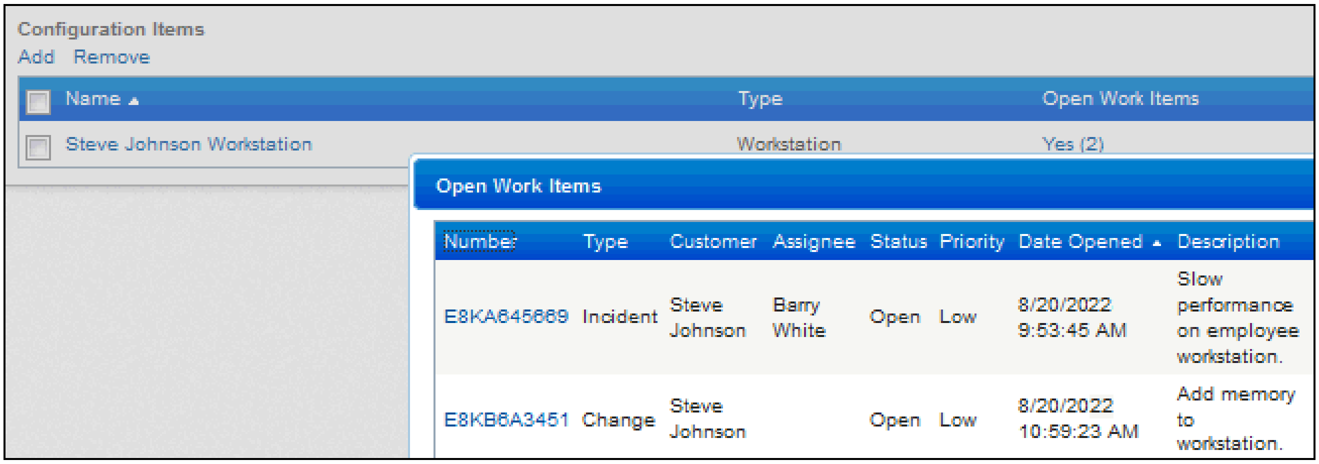
Associating Other Work Items

Use the Add Existing link in the Associated Work Items field to associate an existing knowledge entry, headline, problem, change (if enabled), or purchase request/order with the incident. If configured, notifications regarding incident events can be sent to customers of associated items. (Note that only one Problem record can be associated with an incident.) To associate new work items:

- Select New | Associated Work Item | Problem or Add New Problem in the Associated Work Items field to create a new Problem record that will be associated with the incident. The categorization and description from the incident will be included in the corresponding fields on the record.
- Select New | Associated Work Item | Change or Add New Change in the Associated Work Items field to create a Change record that will be associated with the incident. The categorization and description from the incident will be included in the corresponding fields on the record.
- Select New | Associated Work Item | Purchase or Add New Purchase in the Associated Work Items field to create a new purchase request that will be associated with the incident. The text in the Description field will be included in the Comments field on the purchase request.
- Select Add New Knowledge Entry in the Associated Work Items field to create a new knowledge entry that will be associated with the incident. The description, resolution, and categorization from the incident will be included in the corresponding fields on the knowledge entry. The current incident will be included in the Associated Work Items field on the knowledge entry as well.
- Select Add New Headline in the Associated Work Items field to create a new headline that will be associated with the incident. On the headline, the text in the Short Description field will be included in the Message field and the text in the Description field will be included in the Details field. The current incident will be included in the Associated Work Items field on the knowledge entry as well.

Associating Configuration Items

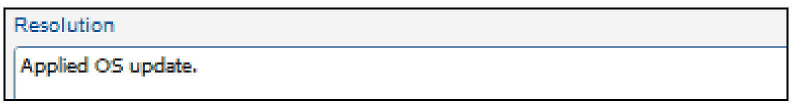
If you have the Service Desk edition and a CMDB has been configured, select the Add link on the Configuration Items field to associate a predefined configuration item with the incident. You can select it to display the Configuration Item screen for viewing the item's relationships with other items, and include information on associated configuration items in views, reports, and correspondence. If the configuration item has other open incidents, problems, or changes associated with it, “Yes” will appear along with the number of open work items. Select the link to display a list of those items.



Resolving Incidents

Entering the Issue Resolution

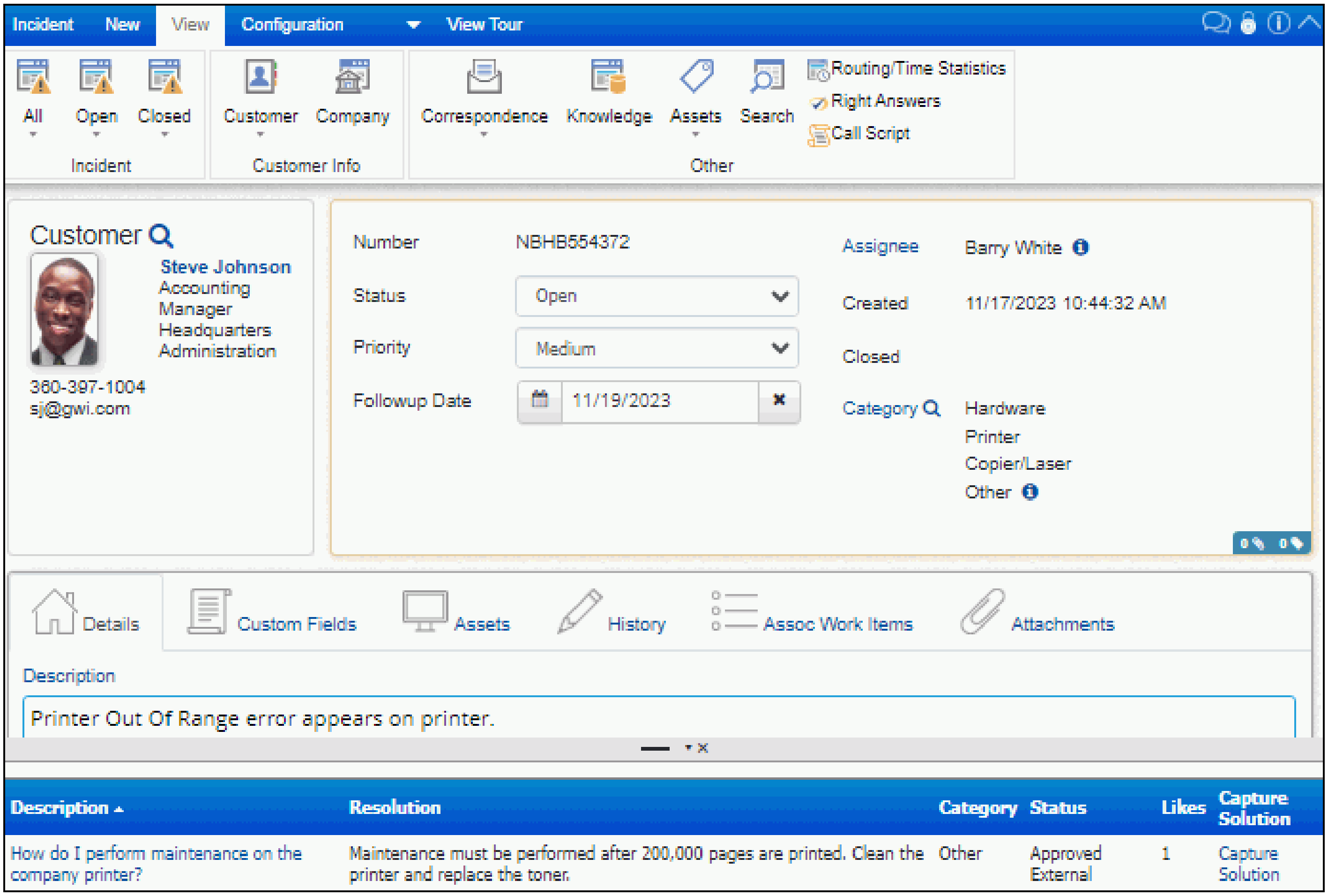
Use the Resolution field for the resolution of the issue. The next sections contain information on including content from knowledge entries and RightAnswers in the Resolution field.



Using Knowledge Functionality

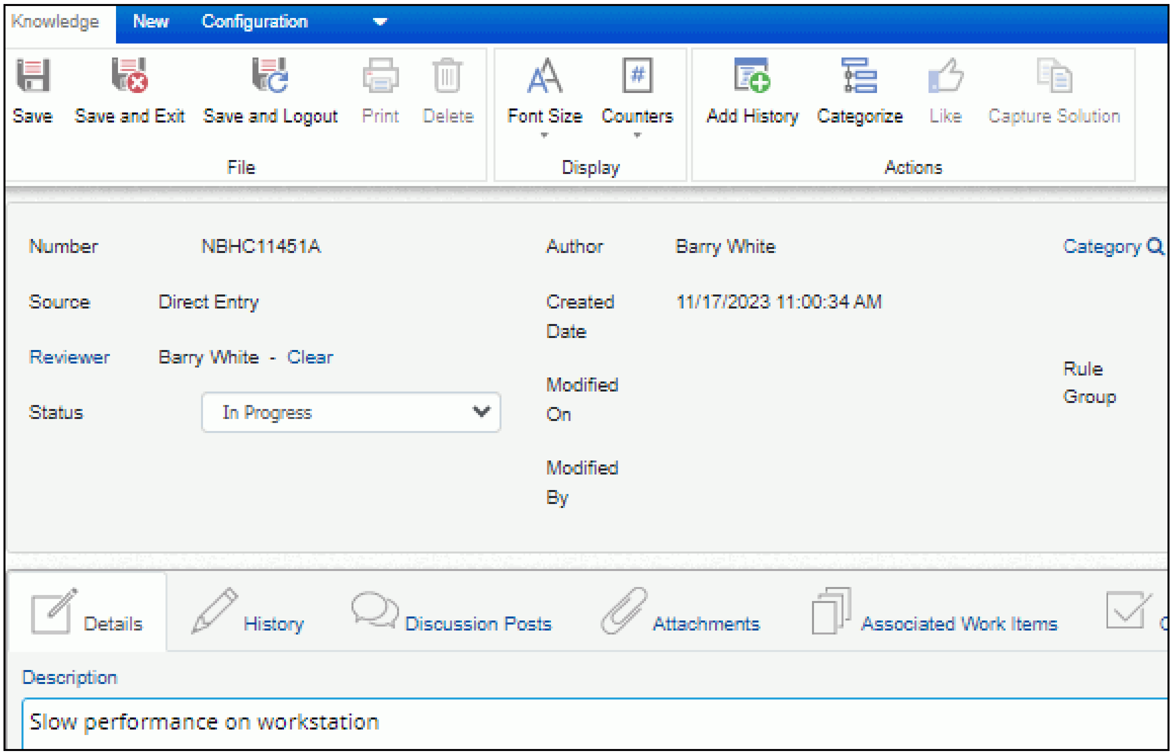
Searching for Knowledge Entries

iSupport's Capture Solution feature enables you to display and copy/paste information from a knowledge entry matching the selected category set into related fields in an incident. If enabled for the category in the Category configuration screen, these entries will appear in the view frame at the bottom of the screen automatically or after you select View | Knowledge in the Incident screen. If you find a knowledge entry that solves the issue, use the Capture Solution link to copy and paste the issue description, resolution, and/or mySupport URL (depending on what is enabled in the Knowledge Management configuration screen) into the incident. If you open a knowledge entry from the view frame you can select Knowledge | Capture Solution  in that entry.



Creating New Knowledge Entries

Knowledge entries contain fields for the category set, issue description and resolution, cause, steps, error messages, and URLs, and attachments. To create a new knowledge entry, select New | Knowledge Entry in the Incident screen.



Searching RightAnswers

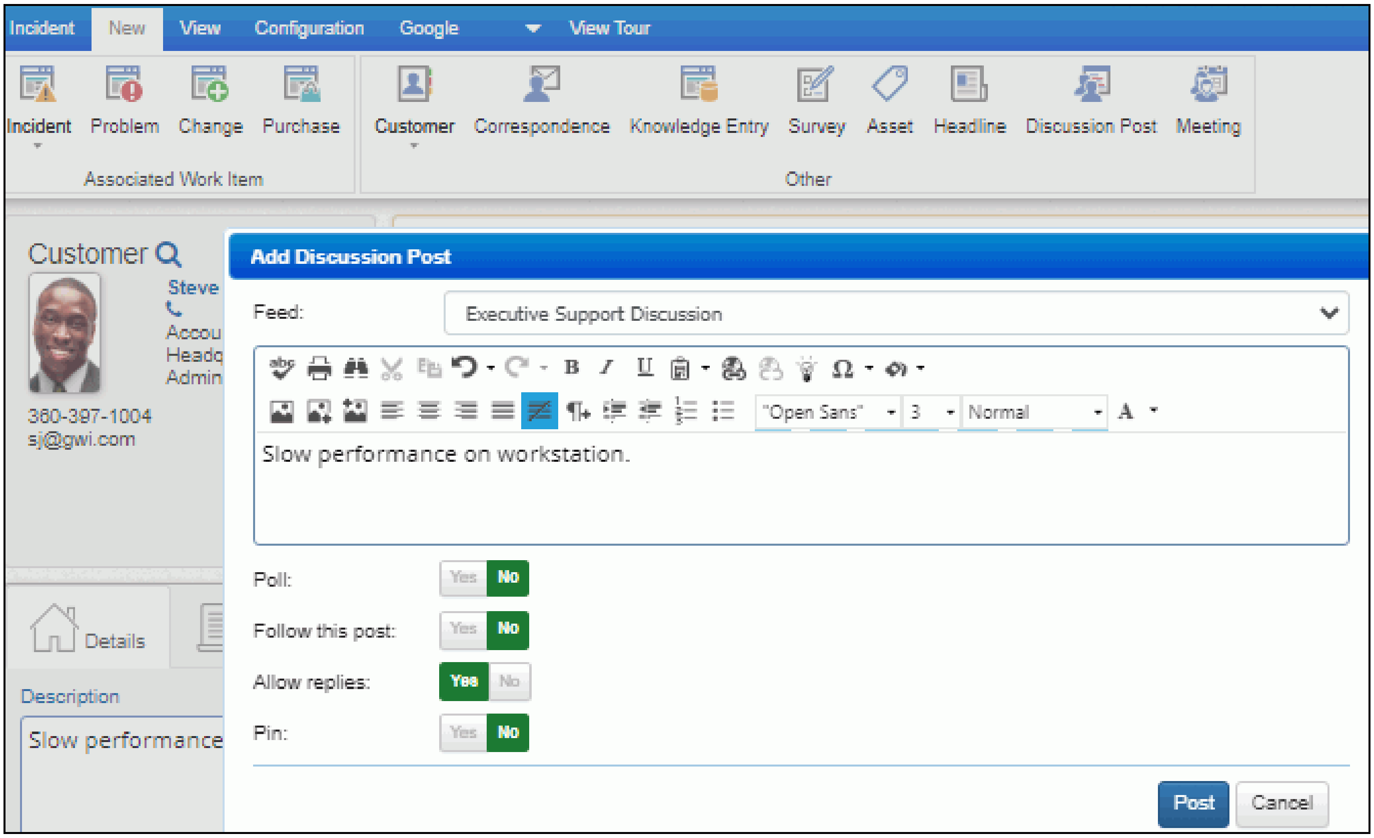
If iSupport's RightAnswers integration is enabled and set up in the Configuration module, you can access subscription-based knowledge content for common PC hardware, software, and network issues. Depending upon options set in the Configuration database, the search may be based on the incident's issue description and/or categorization.

To access RightAnswers, select View | Other | RightAnswers. A screen displays listing all of the knowledge entries that match the search; select the applicable solution. In the screen detailing the entry, select the Yes, Copy Solution to Incident Ticket button to automatically paste in the Issue Resolution field. The solution appears in the Issue Resolution field. A link to the RightAnswers entry will also be included. **Note:** If text exists in the Resolution field, it will be overwritten when the solution is copied from RightAnswers.

Using Communication Features

Creating a Discussion Post

Select New | Discussion Post to add a post to a selected discussion feed. The description and resolution are copied in by default. Select Yes in the Allow Replies field to prevent the Reply link from appearing on the post. Select Yes in the Pin field to retain the post at the top of the feed for the number of days in the Expires In field.



Creating a Headline

Select New | Headline to create a new headline from the Incident screen. The Headline entry screen will appear with text in the Description and Resolution fields by default.

Specifying Others to Notify

If enabled in configuration, you can use the Others to Notify feature to set up a list of customers and support representatives that are not directly involved in the incident process to be sent incident event notifications and other correspondence. For example, notifications could be configured to be sent to a salesperson whenever an incident is created for one of their accounts. An Others to Notify list can be set up for an individual customer, all customers in a company, a category set, and an individual incident, problem, change, or configuration item.

Sending an Email

To send an email from the Incident screen, you can select New | Correspondence or Email in the customer information section (if configured) to populate the To field with the customer's email address. You can select Details next to the Assignee field and then select the Email link to populate the To field with the assignee's email address.

Scheduling Meetings and Tasks

If configured, New Meeting will appear for scheduling a Microsoft Office Outlook calendar and/or Google Calendar meeting. You can view the schedules of meeting attendees, create a meeting, and configure a notification to be sent to meeting attendees. Select View | Meeting to view scheduled meetings.

If configured, options may appear for scheduling meetings: Microsoft Teams, Zoom, Google Meet. When the icon is selected, a Generate Join URL dialog will appear with options for entering the topic, 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. You can also select Planner Task to access Microsoft Planner and create tasks with prefilled references to the iSupport work item number.

Sending a Survey

If iSupport's Survey functionality is configured, you have appropriate permissions, customer, you can send a survey questionnaire to the customers assigned to the incident by selecting New | Other | Survey. The survey will be sent after you select a survey in the Select Survey dialog. Surveys are defined in the Configuration module, and if configured, surveys can be sent automatically on an interval basis. You can also send surveys via the Change and Customer Profile screens, and send surveys to multiple customers via the Desktop. If you have sufficient permissions, you can view survey responses on the Desktop.

Using Awareness and Chat Functionality

If configured, the Awareness feature displays Connected Reps and an alert in the upper right corner if two or more support representatives have the same record open. You can select the icon to display the support representative(s) viewing the work item and initiate a chat by selecting their name.

If a support representative is viewing an incident and another support representative modifies and saves a field on that incident, an Incident Modified dialog will appear with the changes that were made. Note that this dialog will also appear for modifications done via Desktop views.

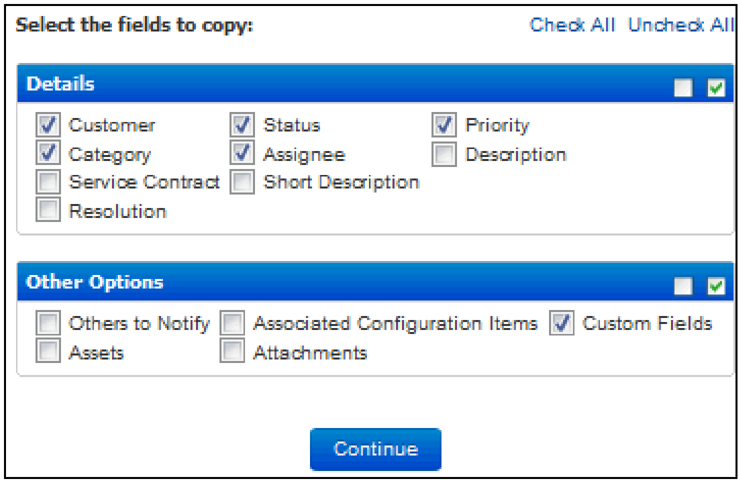
If you are using Google ChromeTM, you can enable Google's Desktop Notification feature to display a small alert at the bottom of the screen (even when the iSupport window is minimized) when you are viewing the same work item as at least one other support representative and a support representative initiates a chat with you. A prompt will appear for you to enable or disable the Desktop Notification feature; after selecting OK, a prompt will appear at the top of the screen to enable or disable desktop notifications. You can later enable or deny desktop notifications via Google Chrome's settings.

Working With Related Incidents

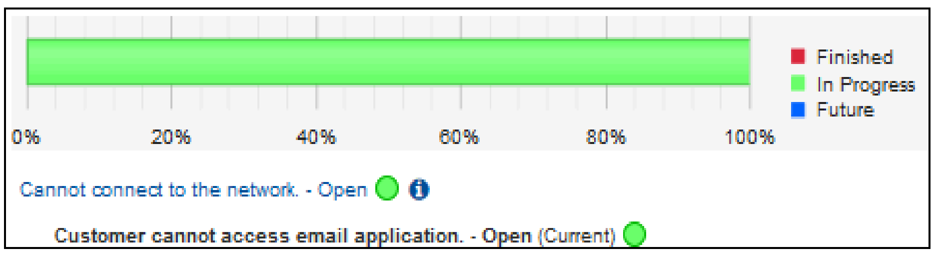
Creating Related Incidents

You can create related incidents to associate and track issues and requests. For example, for an incident regarding a Toner Low notification on a printer, you could create a related incident for ordering more toner for the printer. You can close all related incidents when you close the original incident.

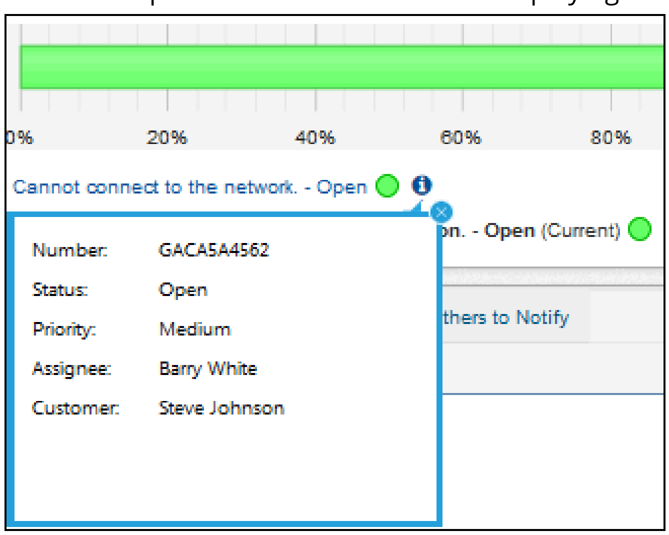
Select New | Related Incident. The following dialog appears; select the fields to populate with data from the original incident.



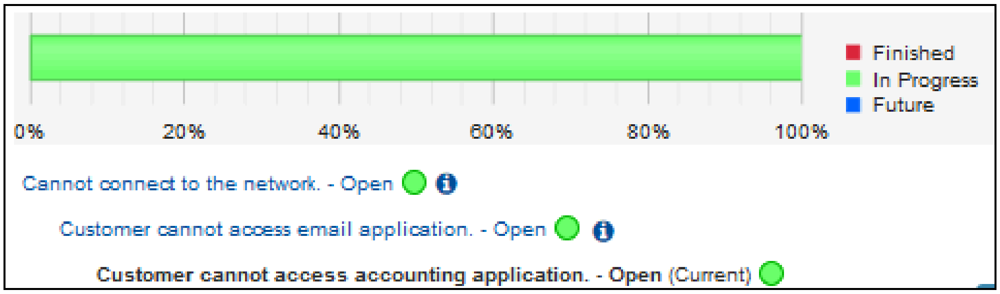
Complete the fields and save the incident. Then save the original incident. Hierarchies can be displayed via either the Related Hierarchy field (if configured) or View Related (which displays a dialog as shown below). Note that the colors that appear on the progress indicator can be set in configuration.



Click for Details appears next to each open and closed incident for displaying incident details.



If you open a related incident and then create and save another related incident, a hierarchy would be created as shown below. In iSupport, a structure created in this manner is called a *dynamic hierarchy* because you can add and remove incidents as needed.

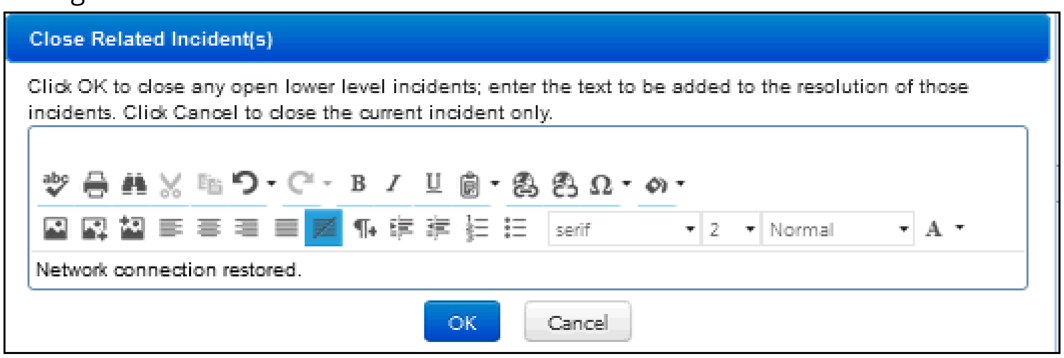


Related incidents can be inserted into the hierarchy. For example, in the hierarchy shown above, you can open the Customer Cannot Access Email Application incident and select New | Related Incident to add an incident under the open incident.

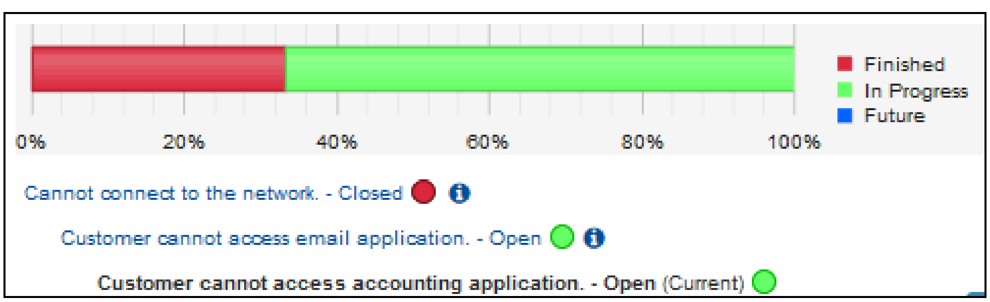
You can also relate multiple incidents via an incident view on the Desktop; select the incident(s) to be related (on a lower level) and then select Relate on the view Actions menu. The Select Upper Level Incident dialog will appear for you to select the incident that will be a level above your previously selected incidents. The Lower Level Incident Options dialog will appear for you to enable custom values to be copied from the selected upper level incident and apply a template to selected lower level incidents if applicable.

Closing Related Incidents

When you enter an issue resolution and close an incident with one or more lower level related incidents, a prompt will appear for closing the related incidents.



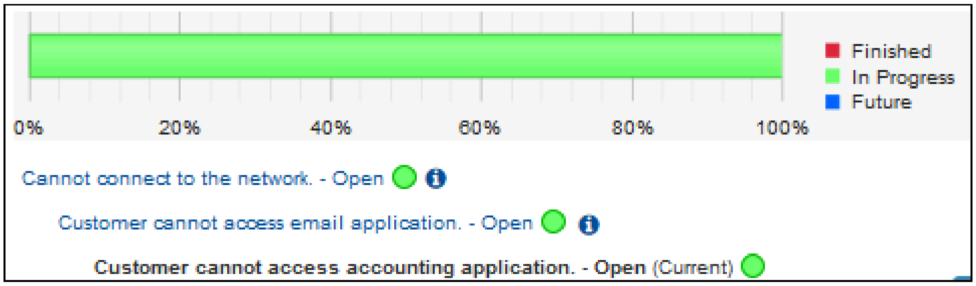
If you select OK, the resolution will be appended to any existing resolution in the lower level incidents and the lower level incidents will be closed. If you select Cancel, the lower level incidents will remain open as shown below.



For information on closing related incidents in a more complex incident structure, see "Closing Incidents in a Hierarchy Template Structure" on page 40.

Removing Incidents in a Dynamic Hierarchy

Select Incident | Hierarchy if you need to remove an incident from a dynamic hierarchy structure such as in the following example.

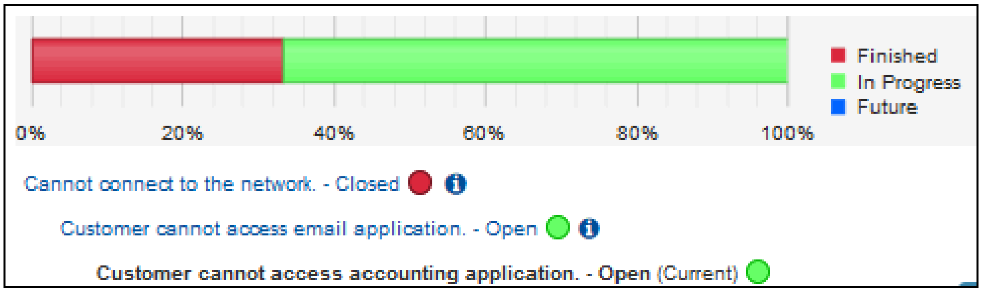


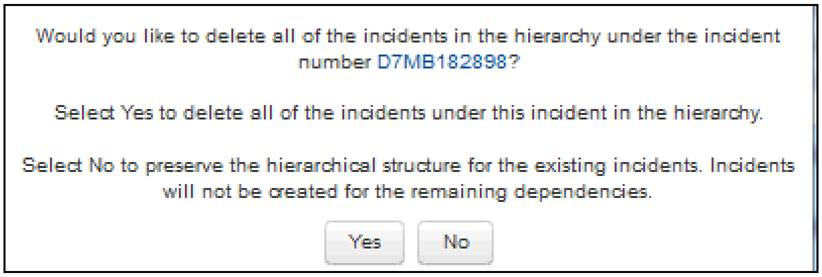
There are three removal options:

- You can remove **the current incident but not its related incidents** via the Remove Incident From Hierarchy option. The current incident will become an independent incident. In the example above, if you remove the Cannot Connect to the Network incident, its lower level incidents will retain their structure.
- You can remove **the current incident and its related incidents** via the Remove Incident and Dependent Hierarchy option. In the example above, you could open the Customer Cannot Access Email Application incident and remove it as well along with its lower level incident (Customer Cannot Access Accounting Application).
- You can remove **the related incidents under the current incident but not the current incident** via the Remove Dependent Hierarchy Below Incident option. The first level being removed will become the top level for its related incidents in a separate dynamic hierarchy. In the example above, the current incident is Cannot Connect to the Network. You could remove the Customer Cannot Access Email Application incident and its lower level incident (Customer Cannot Access Accounting Application), and those incidents would retain their relationship. The Cannot Connect to the Network incident would become a standalone incident.

Deleting Incidents in a Dynamic Hierarchy

When you delete an incident in a dynamic hierarchy, a prompt will appear with the option of deleting its lower level incidents.





In the example above, if you delete the top level Cannot Connect to the Network incident, the prompt appears. If you select No, the lower level incidents will not be deleted and will retain their structure.

Using Hierarchy Templates

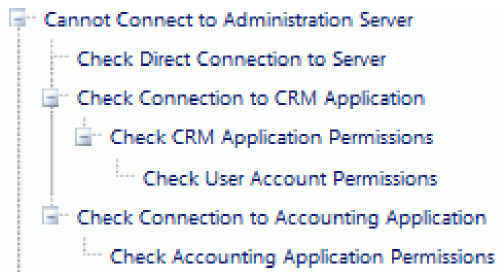
Hierarchy templates function similar to incident templates in that incident fields are populated. However, hierarchy templates consist of a structure with multiple levels and closure dependencies. Existing incident functionality such as routing and followup dates apply to incidents created from a hierarchy template. However, the auto-close option cannot be set for a hierarchy template.

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

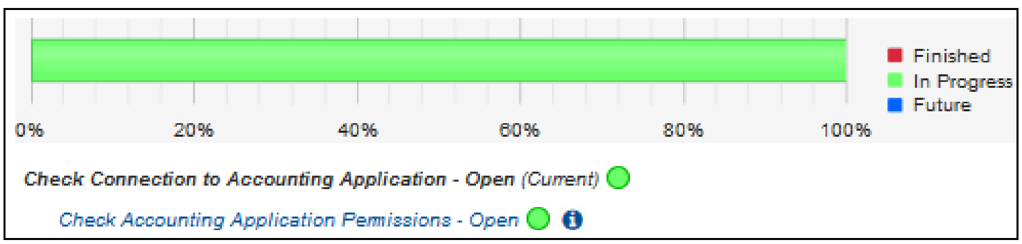
Name
Cannot Connect to Admin Server
SourceSafe Check In Error

Only top-level templates appear in the Incident screen for selection. When you select a hierarchy template, the top-level template is applied to the incident and the template structure is copied to the incident.

A hierarchy template structure can contain any number of templates and levels. Examples are shown below.



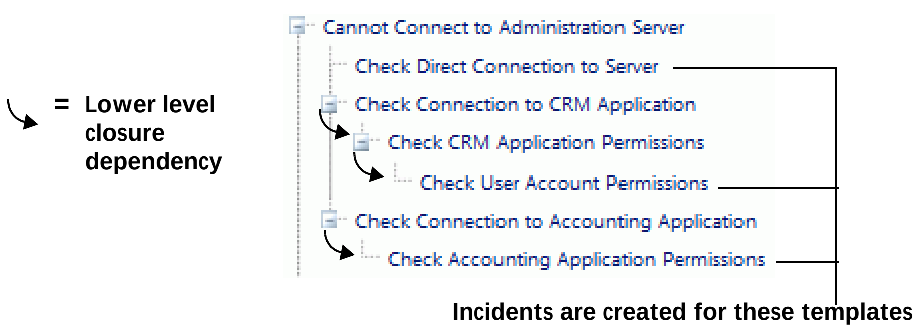
When you select a hierarchy template in the Incident screen and save the incident, you can view the hierarchy via either the Related Hierarchy field (if configured) or the View Related icon (which displays a dialog as shown below). Note that the colors can be changed in configuration.



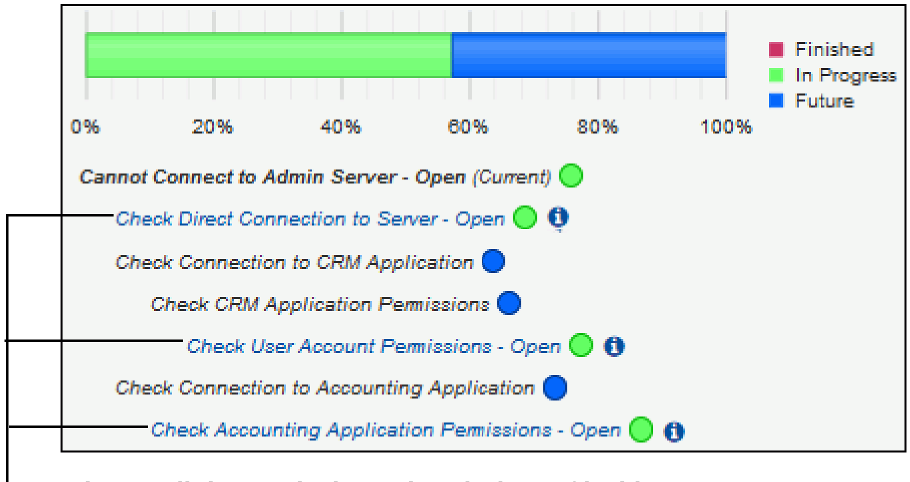
When you select a template with one lower level template, the top level template is applied to the current incident and an incident is created from the lower level template. In the example above, the Check Connection to Accounting Application template was selected in the Incident screen and an incident was also created from the Check Accounting Application Permissions template.

Note: If a top level incident is a scheduled ticket, 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.

When a hierarchy template contains three or more levels, a closure dependency exists for the lowest levels. In addition to the top level template being applied to the current incident, an incident is created for the lowest level incidents.

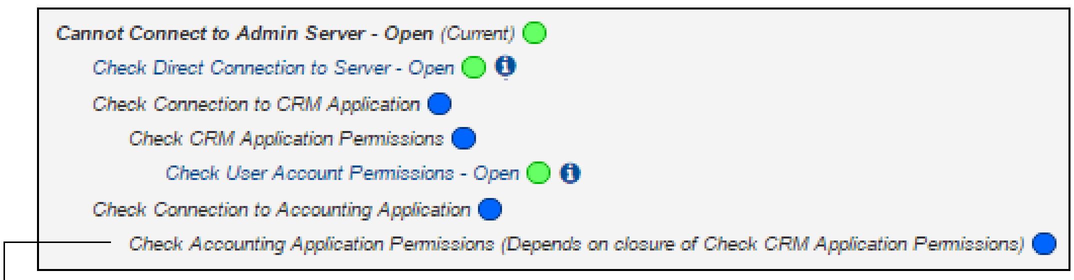


A placeholder will appear for a template with a closure dependency on an open lower level incident. An incident will be created from the template placeholder when the lower level incident is closed. In the example below, the Check Connection to CRM Application, Check CRM Application Permissions, and Check Connection to Accounting Application items are template placeholders that are dependent on closure of their lower level incidents.



Items that are links are the issue descriptions of incidents that have been created because they have no closure

In addition to lower level closure dependencies, a template can also contain a dependency that is defined when the template is configured. In the example below, an incident will not be created for the Check Accounting Application Permissions template until the Check CRM Application Permissions incident is created and closed.

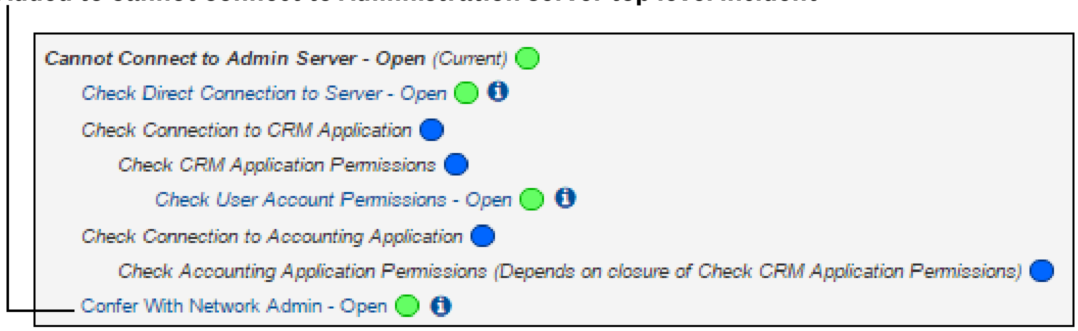


Not created because dependent on closure of Check CRM Application Permissions incident

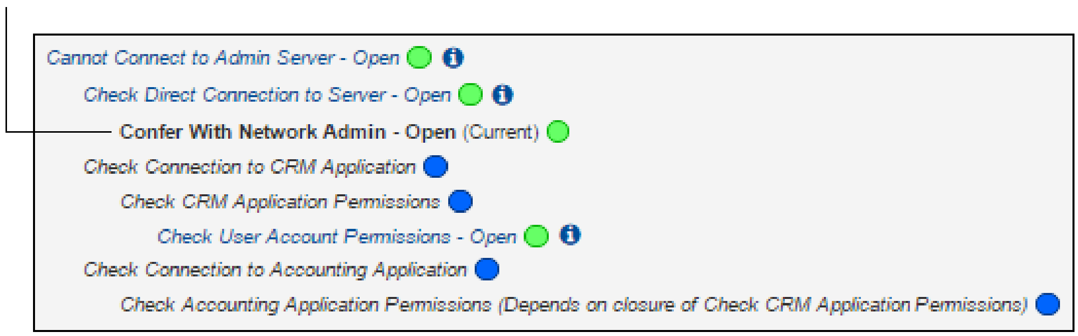
Adding Incidents to a Template Hierarchy

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 | Actions | Hierarchy to add an existing incident.

Added to Cannot Connect to Administration Server top level incident



Added to Check Direct Connection to Server lower level incident

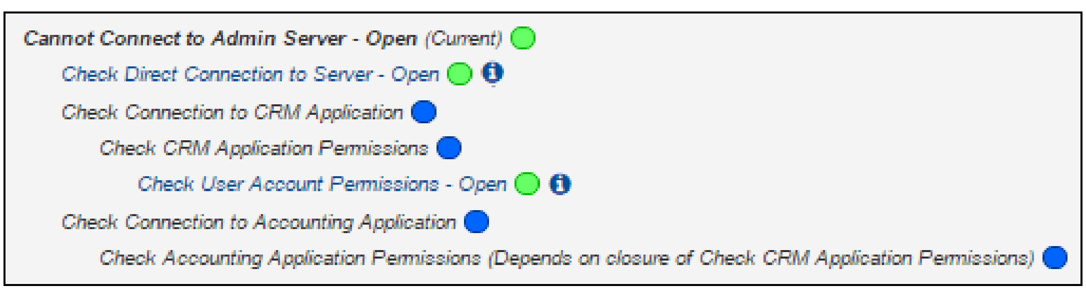


If the added existing incident contains lower level incidents, the structure is also added.

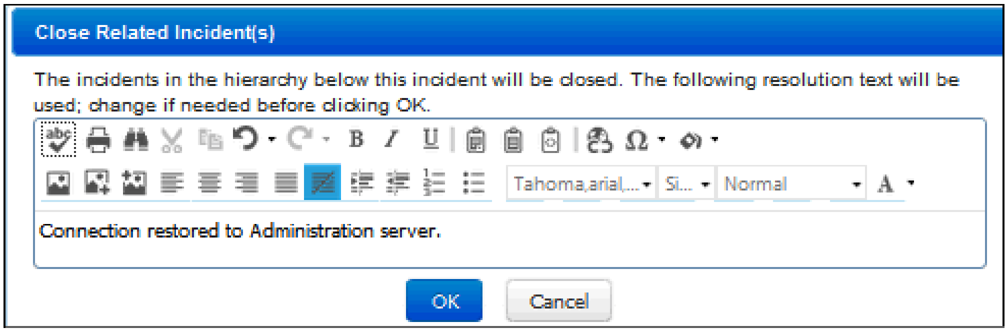
Closing Incidents in a Hierarchy Template Structure

Closing the Top Level Incident

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:



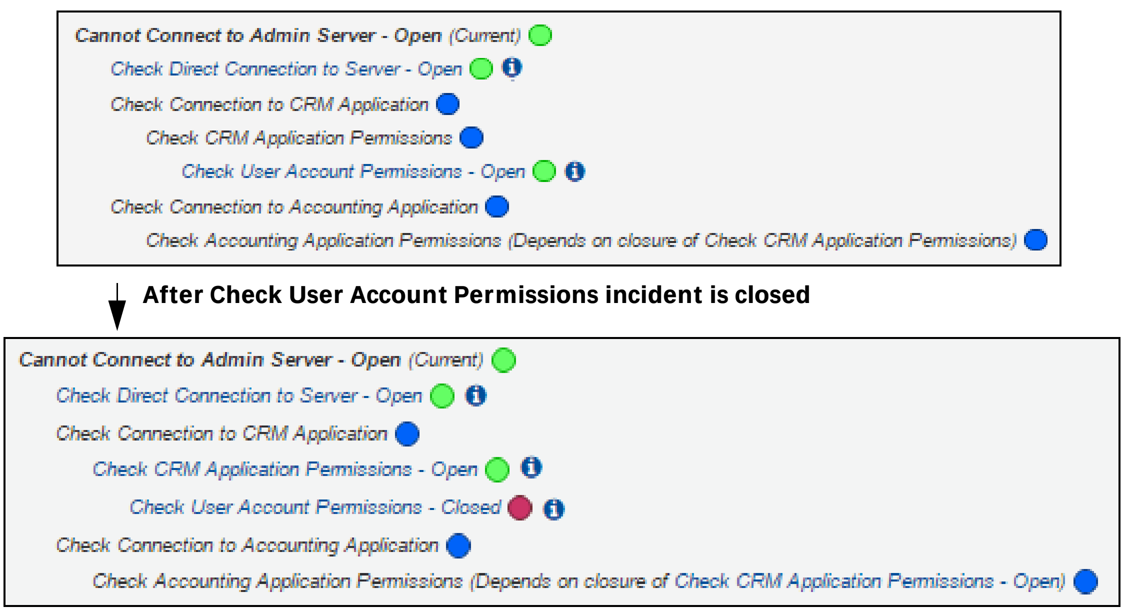
You can change the resolution that will be applied to the open lower level incidents before closure. If you select Cancel in this dialog, the top level incident will remain open.

If you select OK, the hierarchy is as follows:

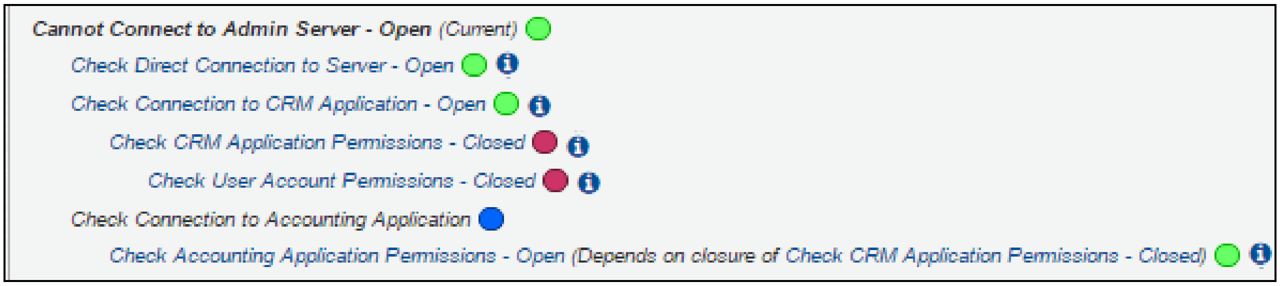
A configuration option may be set to automatically close the top level incident in a hierarchy if all lower level incidents in the hierarchy are closed. The following text will be included in the resolution field: “Automatically closed after closure of all work items in the hierarchy".

Closing Lower Level Incidents

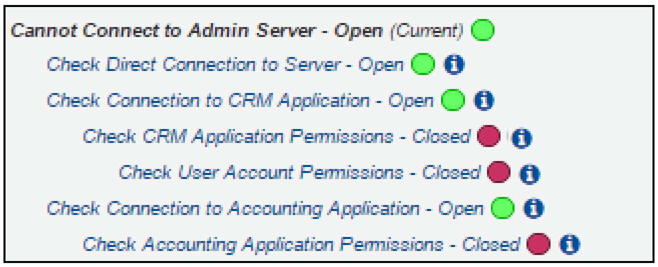
When a lower level incident in a hierarchy template structure is closed, incidents are created from templates that were dependent on closure of that incident. In the following example, after the Check User Account Permissions incident is closed, the Check CRM Application Permissions incident is created.



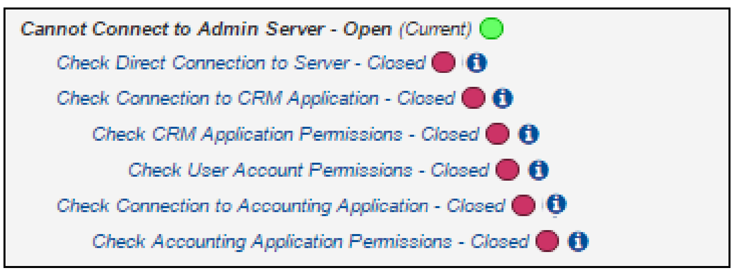
When the Check CRM Application Permissions incident is closed, an incident will be created from the Check Connection to CRM Application template. An incident will also be created from the Check Accounting Application Permissions template because the incident on which it was dependent is closed.



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



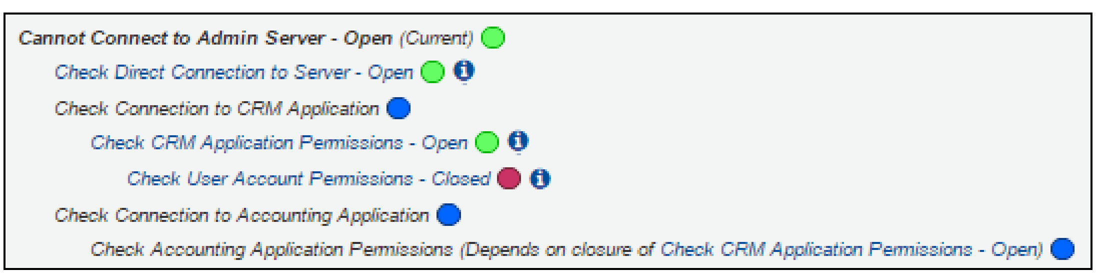
When the Check Direct Connection to Server, Check Connection to CRM Application, and Check Connection to Accounting Application incidents are closed, the Cannot Connect to Administration Server incident can be closed.



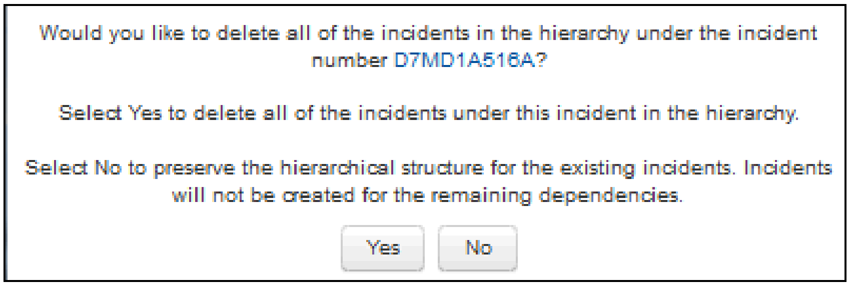
If configured for the hierarchy template, the top level work item will be automatically closed if all lower level work items in the hierarchy are closed. The following text will be included in the resolution field: "Automatically closed after closure of all work items in the hierarchy".

Deleting Lower Level Incidents in a Hierarchy Template Structure

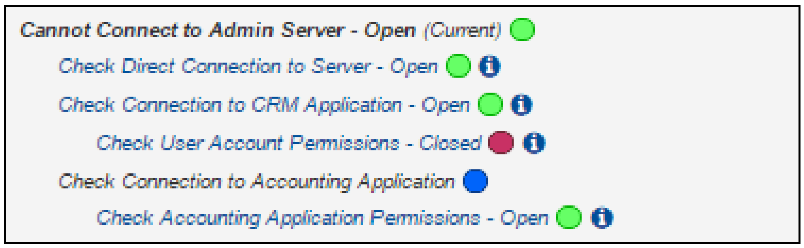
If you delete an incident in a lower level of a hierarchy template structure, you have the option of deleting the incident's lower level incidents. Incidents will be created from template placeholders above it if dependencies are met. In the following example:



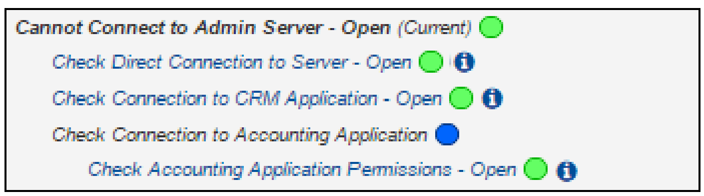
If you delete the Check CRM Application Permissions incident, the following appears:



- 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.



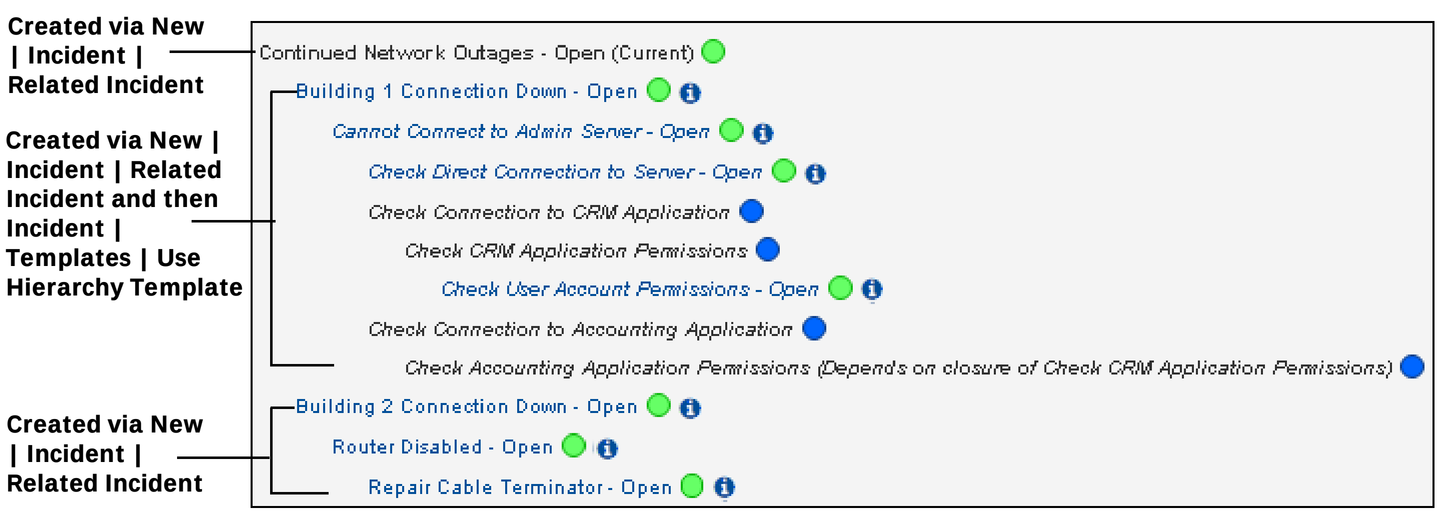
- If you select Yes (you wish to delete its lower level incidents), the lower level incidents will be deleted. The structure will appear as follows.



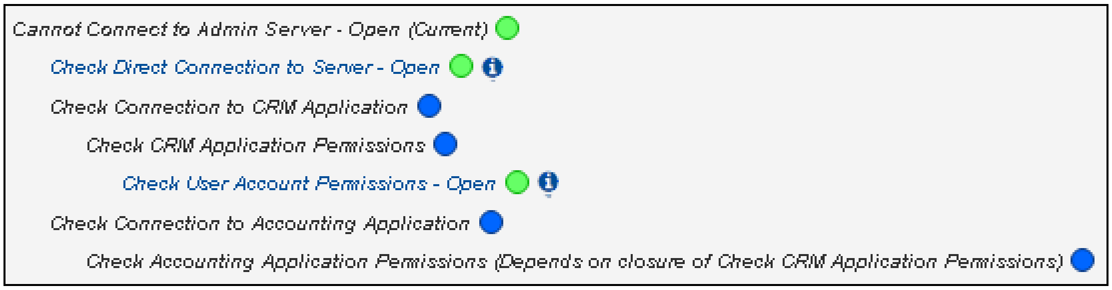
In both cases, an incident was created from the Check Connection to CRM Application template placeholder, which was above the deleted incident.

Removing and Deleting a Top Level Incident in a Hierarchy Template Structure

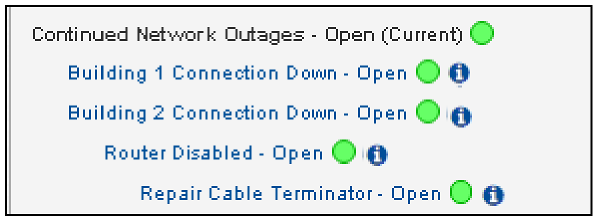
You can remove a top level incident in a hierarchy from a larger hierarchy structure. In the following example:



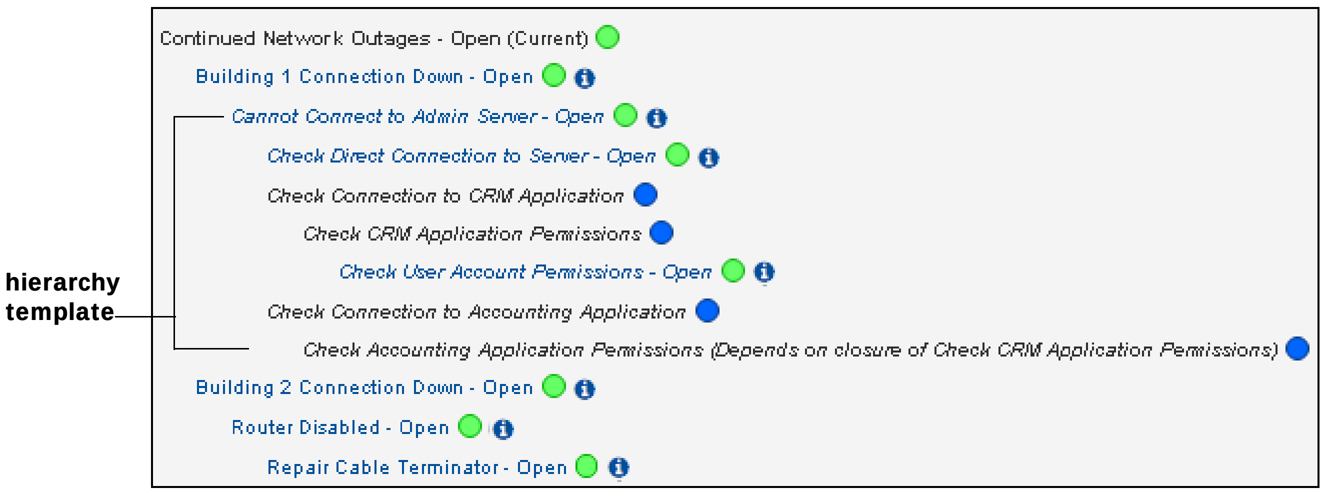
In the top level incident in the incident created from a hierarchy template, the Cannot Connect to Administration Server incident, you can select Incident | Actions | Hierarchy | Remove Incident and Dependent Hierarchy to remove it from the larger hierarchy structure. The Cannot Connect to Administration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



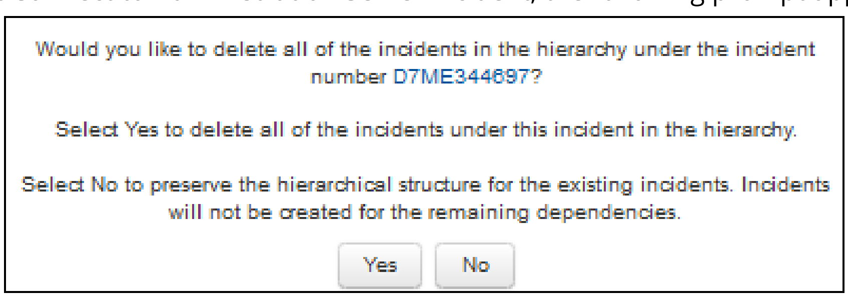
The rest of the structure would appear as follows:



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.