Cornell University
Cornell Information Technologies

Remedy
Local Administrators
Guide

Remedy version 2.5

Guide updated September 2015

For Remedy Support: remedy-admin@cornell.edu

Table of Contents

Interface and Environment Orientations

Production Environment

You and your support providers can access the production server using a web browser with this URL:

http://cornell.onbmc.com

Test Environment

You and your support providers can access the test server using a web browser with this URL:

http://cornell-qa.onbmc.com

Changes made to production configuration data are not automatically moved to test. If you wish to have a current test environment it is necessary to make the changes in both places. Roughly twice a year the support team will schedule a “refresh” of test to ensure it stays usably in sync with production.

Logging in to Remedy ITSM

When you first login to the system you will be presented with your home page. This page provides you with a series of links that take you to different components of the ITSM suite.

Organizational Structure

Remedy uses two parallel hierarchical structures:

Company	Support Company
Organization	Support Organization
Department	Support Group

Company

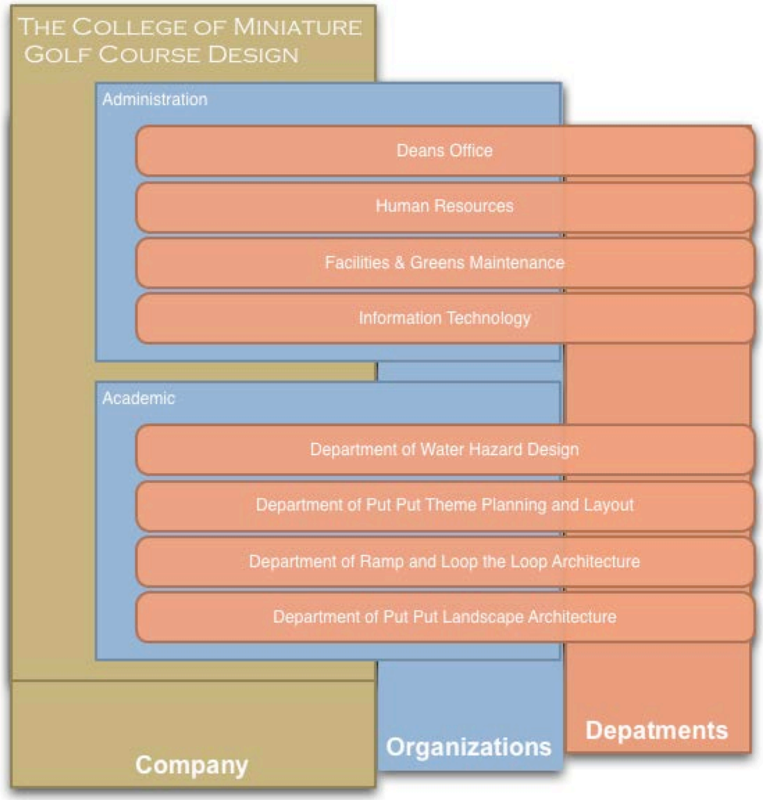
Our Customer Company is “Cornell University.” Our Support Company is “Cornell University – IT.”

There are many settings, filters, and configuration data that are company specific.

Organizations and Departments

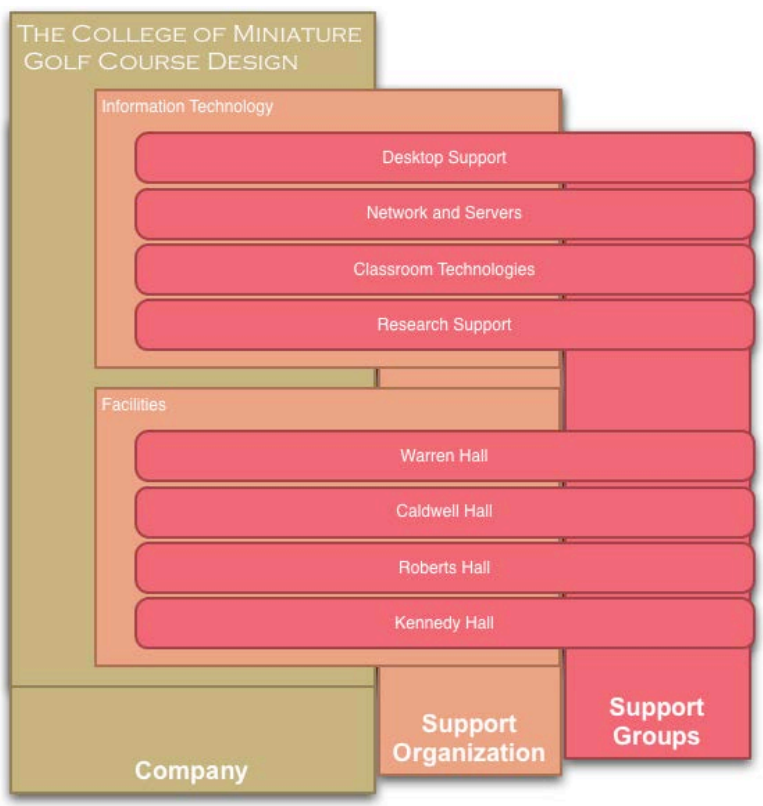
Remedy Organizations and Departments are data used to label customers. The typical organizations in a college would be "Administration" and "Academics." Organizations will be defined centrally.

Within the organization "Administration" you would find departments like Information Technology, Human Resources, Facilities, and other units with administrative functions. Within the "Academic" organization you would find academic departments. Local Remedy administrators will define Departments and Support Groups for their Organization.



Support Organizations and Support Groups

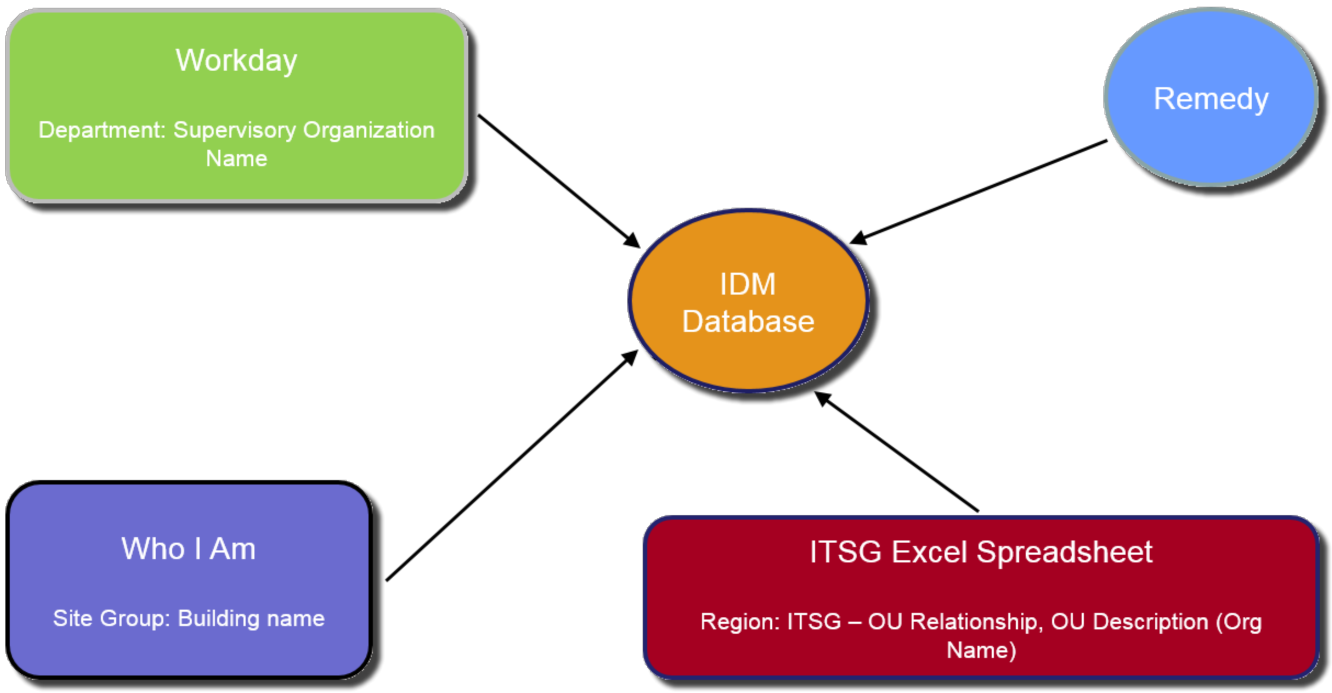
Support Groups play a major role in the definition of your company. Where the Company field and Support Organization fields are organizational containers, Support Groups are the only place where Incidents can be assigned. You cannot assign an incident to a Support Organization or Company.



People

Customer Data

There are two kinds of people in Remedy: support providers and customers. A nightly feed from Cornell's directory servers imports everyone as a customer. Changes made in the directory will be reflected one day later in Remedy. The data comes from different sources as shown below.



The import from the directory will overwrite any changes made to these fields in Remedy except the Corporate Email field.

Remedy People Metadata Data Source Document

In the Remedy Incident Management console, on the left side navigation pane select My Profile. You own profile will be displayed. To search for another user, click on New Search and enter the NetID in the Corporate ID field. You can use other search criteria as well (e.g. name).

Remedy Field	Data Field	Sources	Comments
VIP	Flag Y/N in Remedy	Remedy	A flag set in Remedy. If set to Y, then this individual is designated as a VIP and requires special handling. A process for designating VIPs is being developed and is not yet complete. Generally, Deans, Senior Leadership, and their Admin Assistants are considered VIP. More to follow...
Organization	Workday/PeopleSoft OU Description	AD Group Description for an AD OU Designated for PeopleSoft. Housed in a table owned by Identity Management	This is not the Quest ARS OUs. There is a different structure for Workday/PeopleSoft Data. The OU full name and its relationship to the IT Service Group is kept in a table managed by Identity Management.
Department	Workday Supervisory Organization	Workday	Free form field in Workday (can cause inconsistency in the data) When name is changed or corrected in Workday, it doesn't apply to all existing employee profiles. (Changes are effective only when the profile is updated in Workday).
Region	IT Service Group	Table owned by Identity Management (see Organization field above)	Each service group Director is responsible to claim responsibility for one or more OU above. They can do so by sending an email to remedy-admin. Any data update will be reflected in Remedy only when the employee profile is updated in either Cornell directory or in Workday. For each ITSG one or more AD OU may exist.
Site Group	Building Name	WhoIam	Maintain by the individual in WhoIam. Updated by employee
Manager's Name	Manager's Name/NetID	Workday	Manager in Workday

All the data is being fed to Remedy by a web service provided by Identity Management. The job runs every morning at 5 AM and includes the changes for the last 24 hours.

Implemented July 1, 2014. Tickets before this time may not have this data.

Possible Data issue:

1. **Wrong IT Service Group:** This will happen when an ITSG take over a new OU. When a department does take over a new OU, the ITSG Director should send an email to remedy-admin@cornell.edu and we can work with Identity Management to update the data pull.
2. **Grad Students:** Some Grad students are associated to the graduate school (Example: Engineering, Computer Science) which mean that they have SAS as an ITSG. When this is question look in Help Hero for the student's affiliated college.
3. **Contractor (e.g. Exception with Sponsor):** Contractor are not included in Workday/People soft OU so we don't have an organization and an ITSG for them.

Reporting Data Issues

If you notice problems with the People Metadata in Remedy, create a ticket in Remedy and assign to:

Company: Cornell - IT Support Org: CIT - Support Support Group: BPR & Tools Management

OR

Send and email to Remedy-service@cornell.edu.

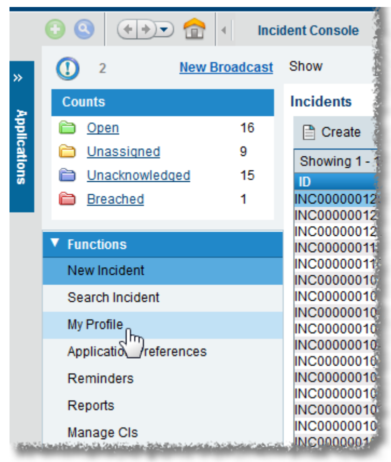
Support Provider Data

Adding and Removing Staff to a Support Groups

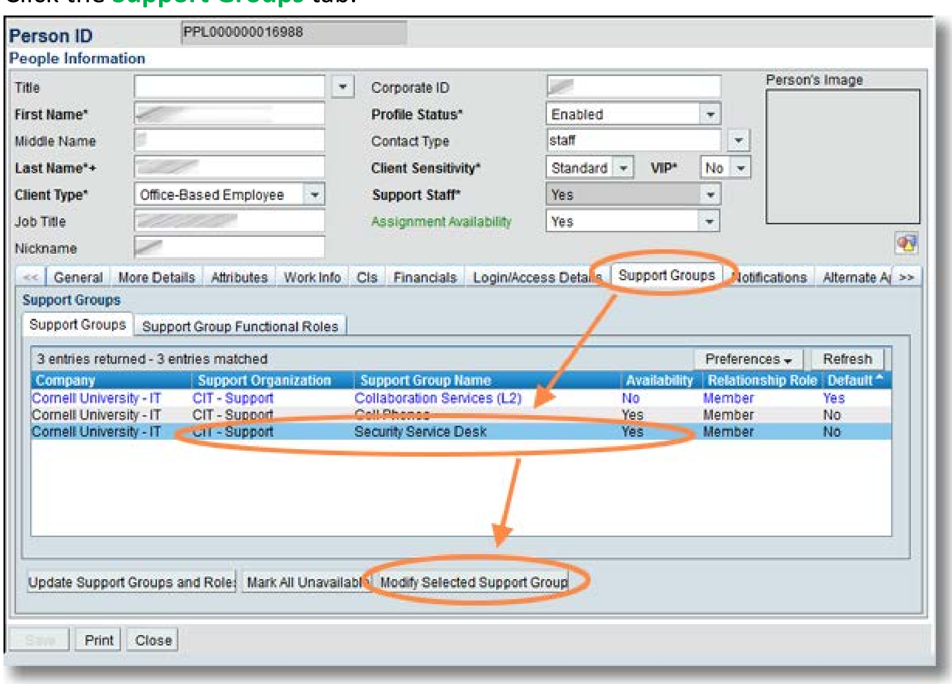
Before you can add a staff member to your support group, the user must have a support staff designation in Remedy. To designate a support staff member, send an email to remedy-admin@cornell.edu requesting the user be granted support staff permissions (support staff designation). You need to provide one support group to add the user to.

Once a user has been assigned a support staff designation then Local Remedy Administrators will have the ability to add that user to support groups.

1. Log into Remedy.
2. From the **Applications** tab, select **Incident Management**, then **Incident Management Console**.
3. On the left, under **Functions**, click **My Profile**.

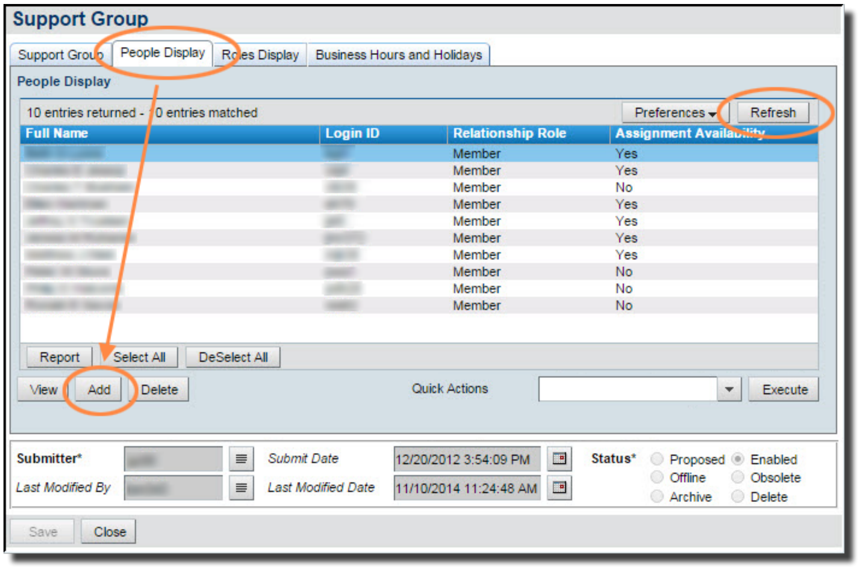


4. Click the **Support Groups** tab.

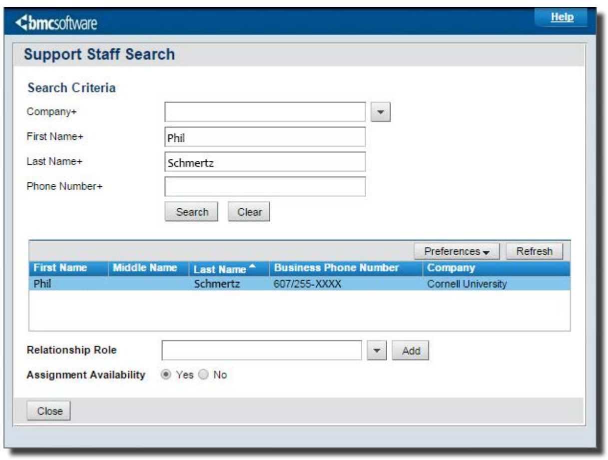


5. Select the support group to which you want to add support staff.

6. Click **Modify Selected Support Group**. A **Support Group** window will open.



7. Click on the **People** tab (you may need to click **refresh** to see the people entries).
8. To add a user,
   a. Click **Add**. A **Support Staff Search** window will open.



   b. Type in the first and last name of the staff, then click **Search**.
   If the user has a support staff designation they will show up.
   If the user doesn't show up, they do not have a support staff designation. Email remedy-admin@cornell.edu to have the user setup with a support staff designation.
   c. Highlight the user in the search results, click the **Relationship Role** field, select **Member**, then click **Add**.
9. To delete a user from your support group,
   a. Click the user's name on the **People** tab, then select **Delete**.
   b. The application will confirm if you want to delete the user from the support group. Click **Yes.**
   c. If the user is leaving your organization, please send an email to remedy-admin@cornell.edu requesting to revoke the user's support staff permissions.

Configuring Notifications to Customers

Customers submit incidents. The settings described here determine whether the customer receives an automated email message when the incident is created and/or when the incident is resolved.

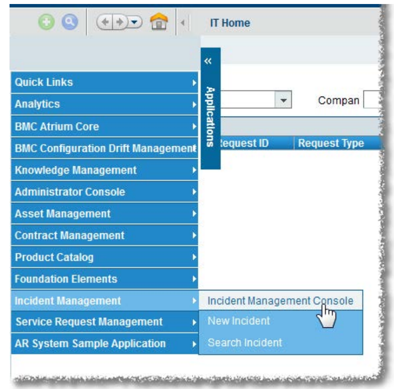
By default, both notifications are sent to customers.

Most of the text in those messages is standardized across all units within the Cornell University "Company," but following information on the notifications can be customized for each Support Group:

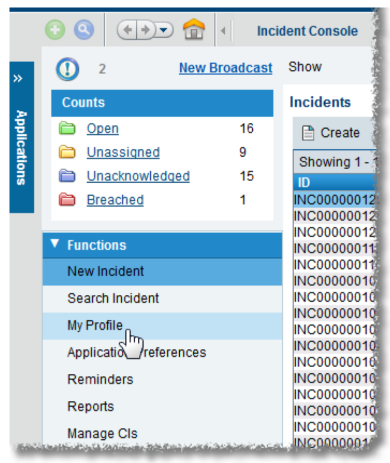
Field in Remedy	Usage in the Notification Emails
Exchange Group Account	The "From" address
Exchange Group Account Name	The descriptive text next to the "From" address
Group Web Address	The Support Group's web address
Group Phone Number	The Support Group's phone number
Special Notes (available on incident creation message only)	A block of text, which is added to the standard incident creation email

Configuring Notifications

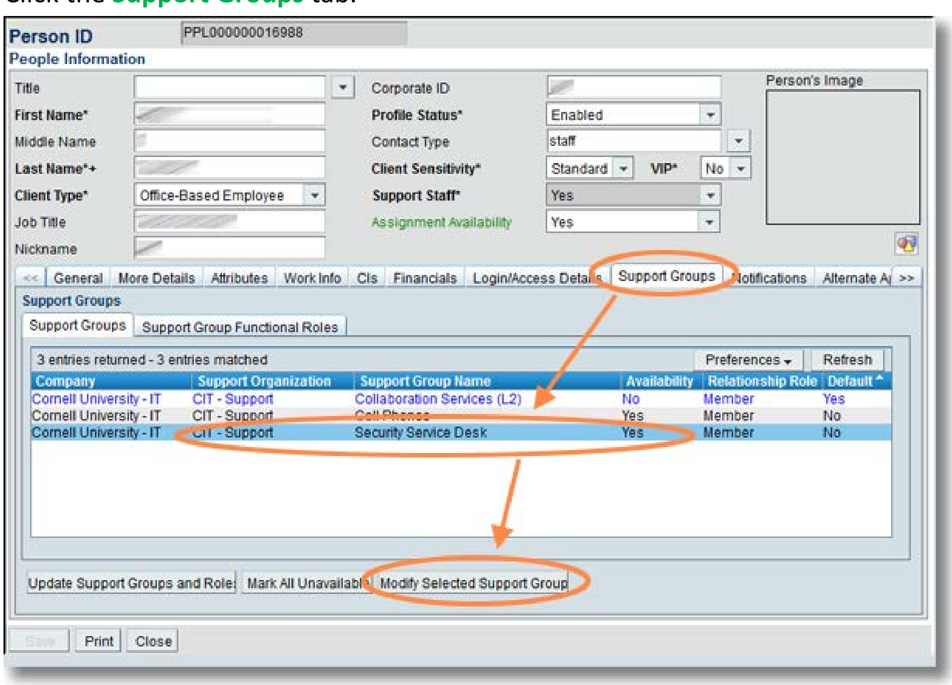
1. Log into Remedy.
2. From the **Applications** tab,
   select **Incident Management**,
   then **Incident Management Console**.



3. On the left, under **Functions**, click **My Profile**.

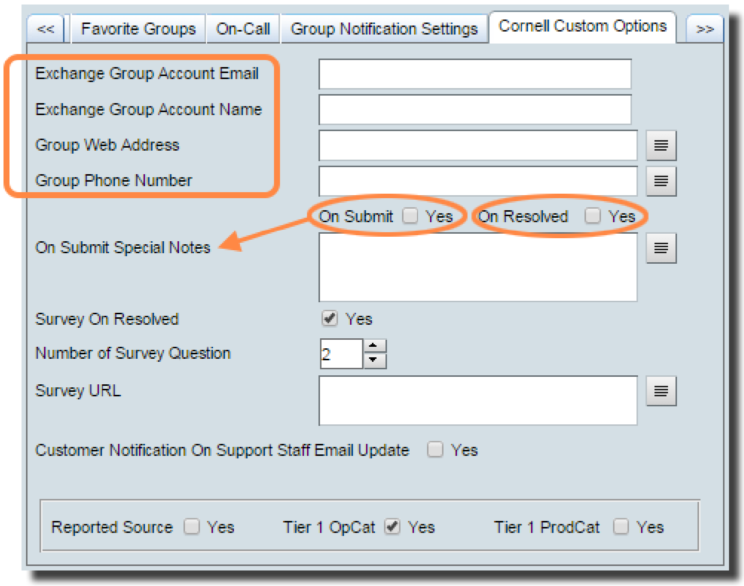


4. Click the **Support Groups** tab.



5. Select the support group for which you want to set group notifications.
6. Click **Modify Selected Support Group**.

7. Click the **Cornell Custom Options** tab. Modify the fields on this tab as desired. If your text is longer than about 30 characters, click the page icon next to the field to see an expanded text entry box. The entries in the first four fields will appear in notification emails.
    a. **Exchange Group Account Email**
    b. **Exchange Group Account Name**
    c. **Group Web Address**
    d. **Group Phone Number**



8. Check **On Submit** if you want the notification message sent to the customer on incident creation
9. Check **On Resolve** if you want the notification message sent to the customer on incident resolution.
10. **On Submit Special Notes**: If you have checked **Customer Notification On Submit**, the text you enter here will appear in the message the customer receives.)
11. Click **Save**.

In Qualtrics surveys, the following embedded fields can be defined:

INC	Incident Number
Bserv	Business Services
Prod	Product Name
Owngr	Incident Owner Support Group
Ownorg	Incident Owner Organization
Sptgroup	Assigned Support Group
Sptor	Assigned Support Organization
Assignee	Assignee
Opcat	Tier 1 Operational Category
Subdate	Submit Date
Resdate	Resolution Date
Reportsrc	Reported Source

Standard Notification Templates

Shaded items are the ones you can modify using the preceding procedure.

Items in {{double curly brackets}} are filled in based on the incident elements.

On Submit notification

From	Exchange Group Account Name <Exchange Group Account>
Subject	{{Incident Number}} – {{Summary}}
Body	Hello Customer {{Firstname}} {{Lastname}}, We have received your request for service. A support person will respond to you as soon as possible. Your request has been assigned a case number: {{Incident Number}} Request date: {{Incident creation Date/Time}} Original request:{{ Incident Summary}} Updates and additional questions regarding this incident are welcome. For faster service, always include your case number (Incident number) in the subject line of any related follow-up emails. Special notes Exchange Group Account Name Group Web Address Group Phone number

On Resolve notification without survey

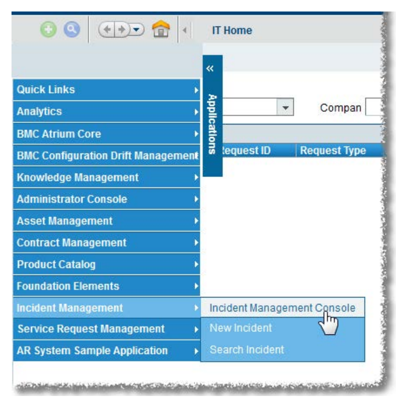
From	Exchange Group Account Name <Exchange Group Account>
Subject	{{Incident Number}} – {{Summary}}
Body	The following case has been marked as resolved. Case number: {{Incident Number}} Request date: {{Incident creation Date/Time}} Original request: {{Incident Summary}} Resolution: {{Incident Resolution}} Please reply if you have any further questions, or if your case remains unresolved. For faster service, always include your case number (Incident Number) in the subject line of any related follow-up emails. Thank you, Exchange Group Account Name Group Web Address Group Phone Number

On Resolve notification with survey URL

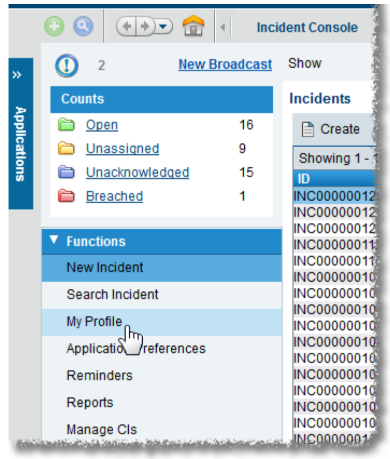
From	Exchange Group Account Name <Exchange Group Account>
Subject	{{Incident Number}} – {{Summary}}
Body	The following case has been marked as resolved. Case number: {{Incident Number}} Request date: {{Incident creation Date/Time}} Original request: {{Incident Summary}} Resolution: {{Incident Resolution}} *Please give us feedback with a* <Number of survey question> *question survey by clicking the link below. Please do not send it to anyone else, because this URL links the survey to your individual case information.* <Survey Link Here> *We value your input and will use it to improve our service to you and to measure customer satisfaction.* Thank you, Exchange Group Account Name Group Web Address Group Phone Number

Configuring Surveys

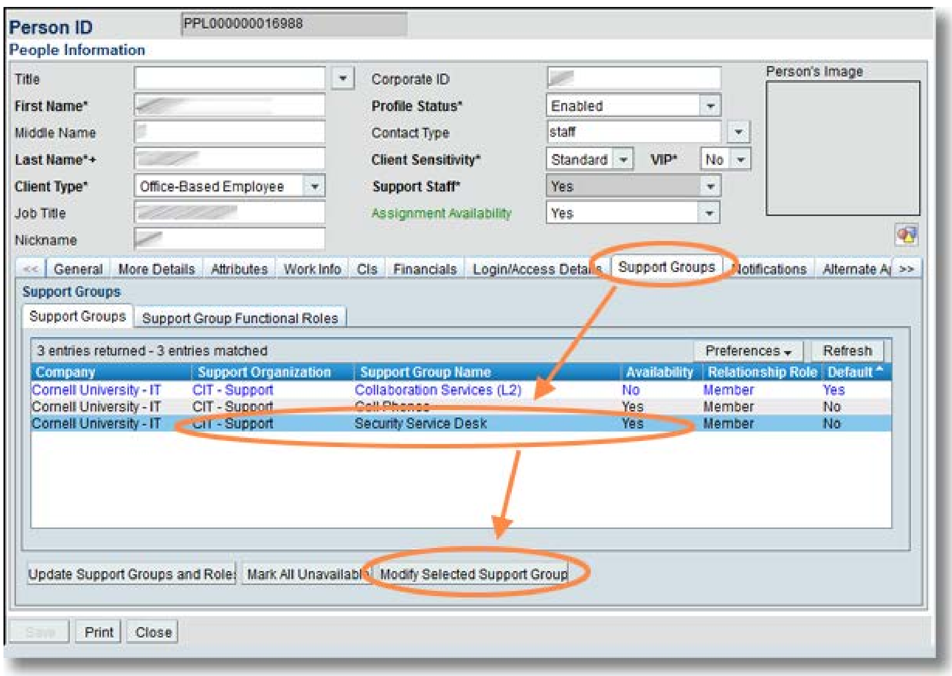
1. Log into Remedy.
2. From the **Applications** tab, select **Incident Management**, then **Incident Management Console**.



3. On the left, under **Functions**, click **My Profile**.



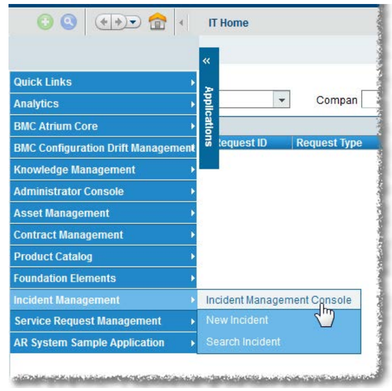
4. Click the **Support Groups** tab.



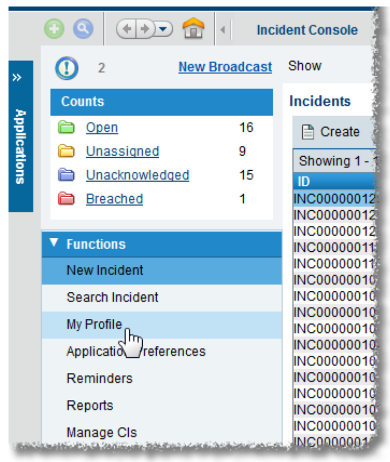
5. Select the support group for which you want to set group notifications.
6. Click **Modify Selected Support Group**.
7. **Survey On Resolved**: If you have checked **Customer Notification On Resolved** AND you check **Survey On Resolved**, a link to a short feedback survey will be added to the message the customer receives.)
8. If you have checked **Survey On Resolved**, enter the **Number of Survey Questions**.
9. If you have checked **Survey On Resolved**, enter the **Survey URL** (the URL will begin with `cornell.qualtrics.edu`)
10. Click **Save**.

Configuring Required Fields “On Resolve”

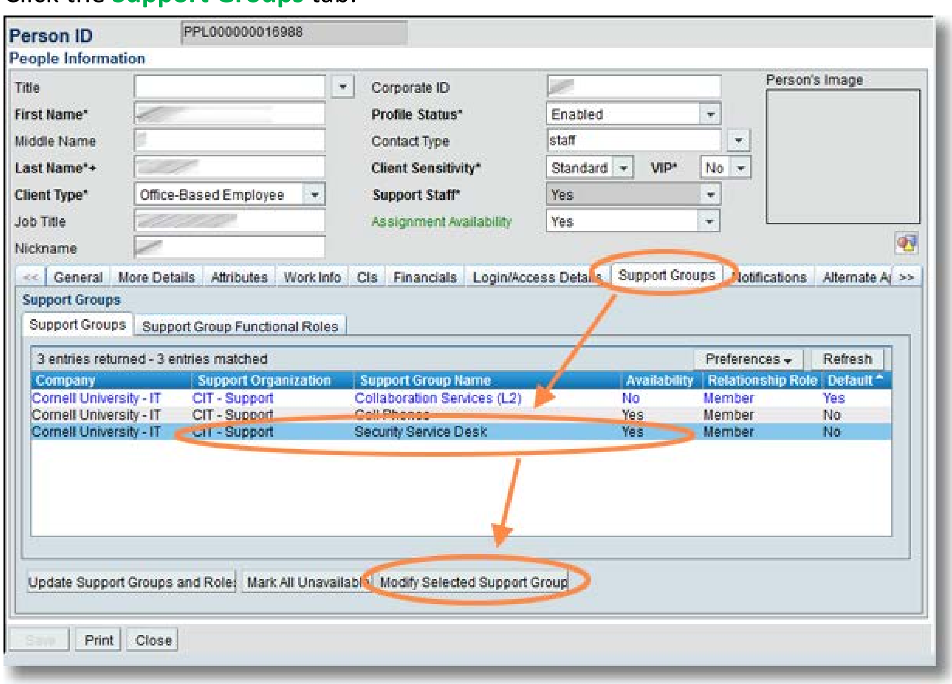
1. Log into Remedy.
2. From the **Applications** tab,
   select **Incident Management**,
   then **Incident Management Console**.



3. On the left, under **Functions**, click **My Profile**.

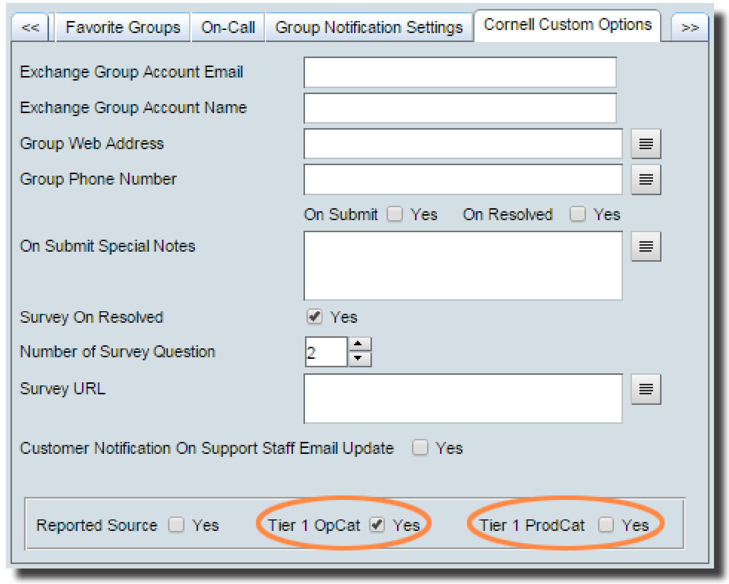


4. Click the **Support Groups** tab.



5. Select the support group for which you want to set group notifications.
6. Click **Modify Selected Support Group**.

7. Click the **Cornell Custom Options** tab.
8. Check **Tier 1 OpCat** if a Tier 1 Operational Category is required when resolving an incident.
9. Check **Tier 1 ProdCat** if a Tier 1 Product Category is required when resolving an incident.
10. Click **Save**.



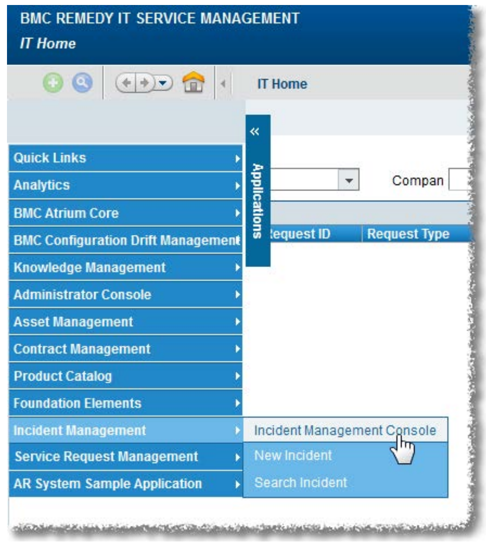
Setting Up Incident Creation Notifications to Support Providers

By default, when an incident is created, Remedy sends notifications to all members of the appropriate Support Group. An alternative is to use group notifications to send these messages to an Exchange Group Account (EGA) or e-list address instead.

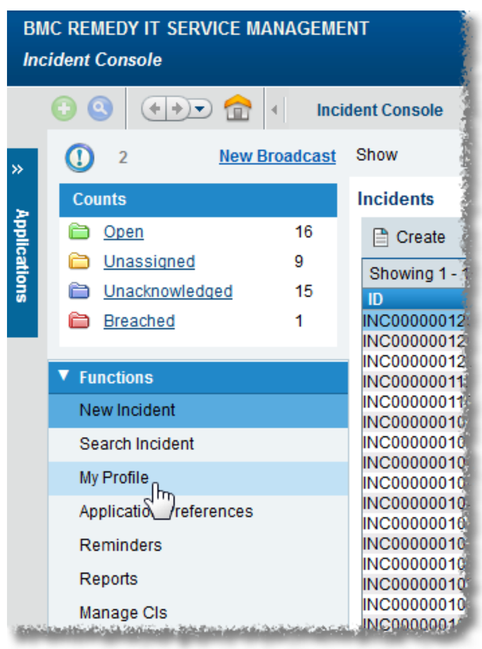
The settings in the following procedure take precedence over any settings on the Notification tab in a user's profile.

To set up group notifications

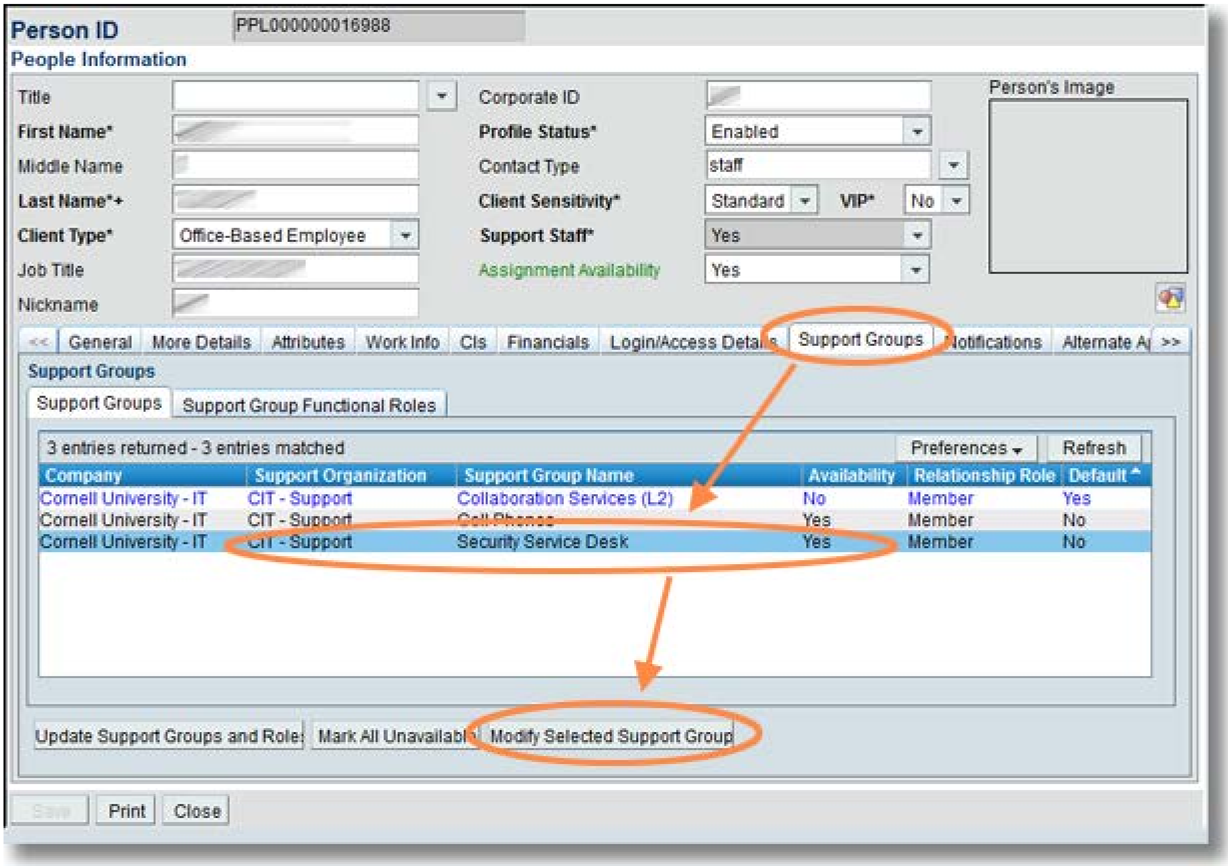
1. Log into Remedy.
2. From the **Applications** tab, select **Incident Management**, then **Incident Management Console**.



3. On the left, under **Functions**, click **My Profile**.

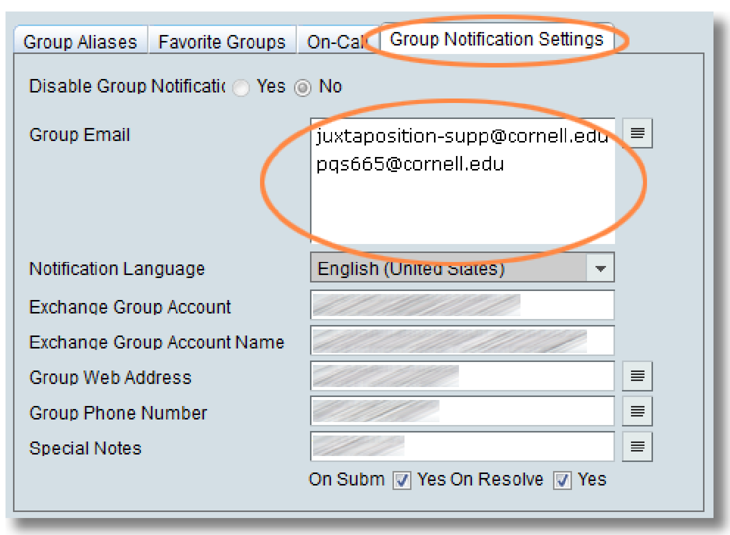


4. Click the **Support Group** tab.



5. Select the support group for which you want to set group notifications.
6. Click **Modify Selected Support Group**.
7. Click the **Group Notification Settings** tab.
8. In the **Group Email** box, enter any combinations of
   - Exchange Group Account (EGA) addresses,
   - e-list addresses, and
   - email addresses.

   If you enter more than one address, separate addresses with a carriage return.
   Leave this field blank to have Remedy use the default, which is to send notifications to all members of this Support Group.
9. Click **Save**.



Note: Leave **Disable Group Notifications** option set to **No**.

Incident Templates

Best Practice

The values that the administrator configures in the template forms are used to add information to the Incident form. This allows support staff to use standard business processes and increase automation and value.

Support staff can select any templates that are available for their support group(s). Templates are useful in a request that follows well-defined methods for specific and repeated requirements. You can create as many templates as you want. But the best practice is creating templates only for standardized processes that your support staffs perform on a frequent basis.

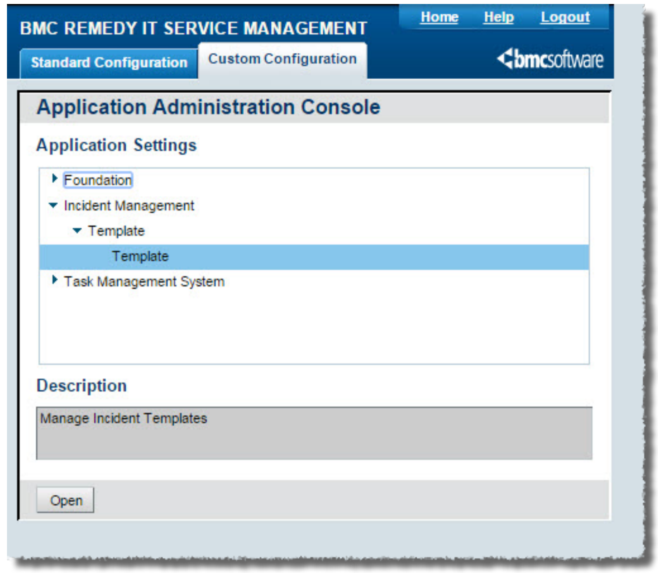
Templates are also used by the pmail process to create incident. An association is made between your Exchange Group Account (EGA) and a template you specify at configuration.

When creating an incident or on existing incident, a Template can be selected using the Incident template field.

Creating/Modifying Incident Management templates

1. Log into Remedy.
2. From the **Applications** tab, select **Administrator Console**, then **Application Administration Console**.

3. On the Application Administration Console, on the **Custom Configuration** Tab, then select **Incident Management** > **Template** > **Template** and click **Open**.



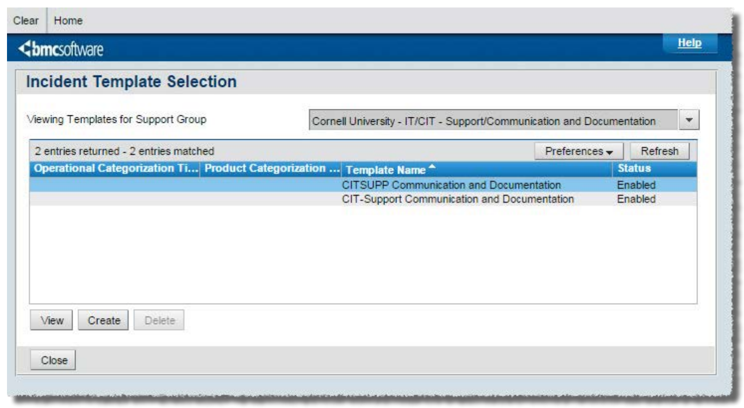
4. From the **Viewing Templates for Support Group** drop-down, select the appropriate support group.

   The list of templates displays the templates for that support group.

5. Click **Create**. The Incident Template form opens

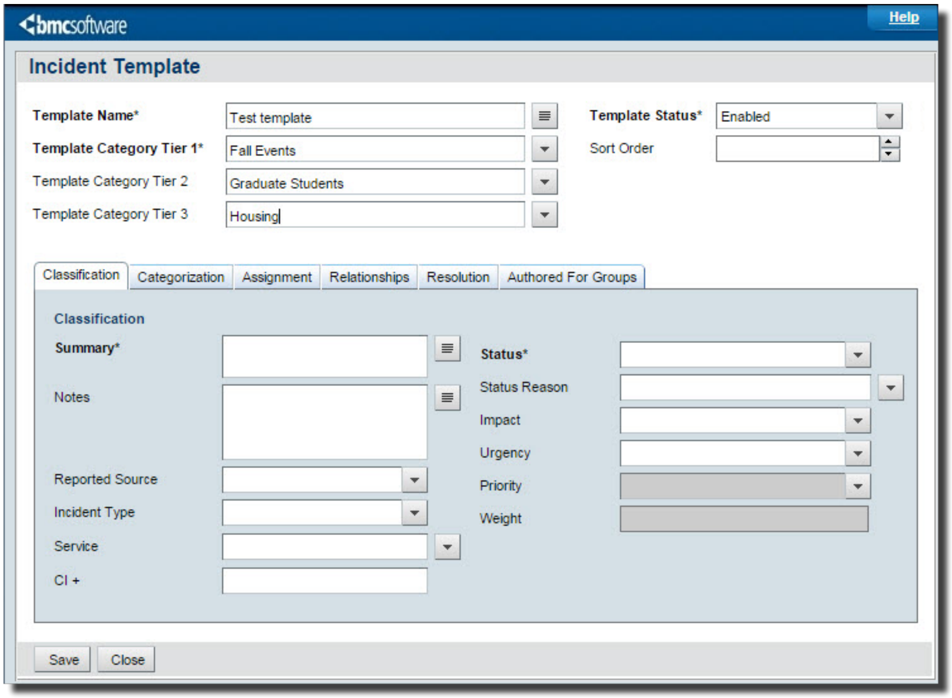
   OR

   Select a template, and click **View** to modify a template.



6. In the **Template Name** field on the Incident Template form, type a brief descriptive name for the **template**.

7. From the **Template Status** drop-down list, select **Enabled**, which indicates that the template is available for use in BMC Remedy Incident Management.



8. Select or create the appropriate template categorizations for **Tier 1, Tier 2, and Tier 3.**

   To create a template categorization, type the category name in the **template category** field. When you save the template, the category name is also saved and added to the field's selection list, where it is available to select when you create the next template.

9. **Configure classification settings**

   a. On the Incident Template form, click the **Classification** tab.

   b. From the **Impact** list, select an impact level for the incident form that is created when the template is used.

   c. From the **Urgency** list, select a level of urgency for the incident form.

   d. The **Priority** value is based on the impact and urgency.

   e. From the **Incident** Type list, select the type of service that is recorded when the template is used.

   f. From the **Service** list, select the related business service CI, for example, **Email Service**.

   g. Click **Save**.

10. **Configure Categorization settings**

    a. On the Incident Template form, click the **Categorization** tab.

    b. Select the appropriate **operational categorizations** for Tier 1, Tier 2, and Tier 3.

    c. Select the appropriate **product categorizations** for Tier 1, Tier 2, Tier 3, Product

    d. Enter **Product Name, and Model/Version**.

11. Configure assignment settings

a. On the Incident Template form, click the **Assignment** tab.

b. To assign the incident to the user creating the incident, in the **Assign To Current User** field, select **Yes**. Otherwise, use the following steps for assignment settings:

  i. In the **Support Company** field, select the **company** that incidents created from the template will be assigned to.

  ii. In the **Support Organization** field, select an **organization**.

  iii. In the **Assigned Group Name** field, select a **group**.

c. Click **Save**.

12. **Configure resolution settings**

Typically, you use this tab only when creating templates for incidents that can be resolved when they are recorded. For example, this might be used for frequently asked questions, such as how to change your password.

Tip: The resolution details can remind support staff of the steps to resolve an issue. For example, the details could list all the places to check for a paper jam on a printer.

a. On the Incident Template form, click the **Resolution** tab.

b. In the **Resolution** field, type the steps that resolve the incident.

c. From the **Resolution Method** list, select **On-Site Support, Service Desk assisted**, **Self-Service**, or **Remote Control**.

d. Click **Save**.

13. Set groups that can use the template

The template authoring group specifies the group that can modify this template. If you have the Support Group Admin functional role or the Incident Config permission, you can assign the template authoring group to any group.

a. On the Incident Template form, click the **Authored For Groups** tab.

b. Click **Update**.

c. The **Template Support Group Association** dialog box appears.

d. To add groups that can use this template, follow these steps:

e. Select the **company**, **support organization**, and **support group**.

f. Click **Add**.

g. Click **Close**, then click **Save**.

Email Templates

Email templates (also referred to as predefined replies or standard emails) are used to respond to a common question or problem. They are also use by the email process to create incident sends to a mailbox.

Regular users can create Individual templates, which they can use when responding to an incident.

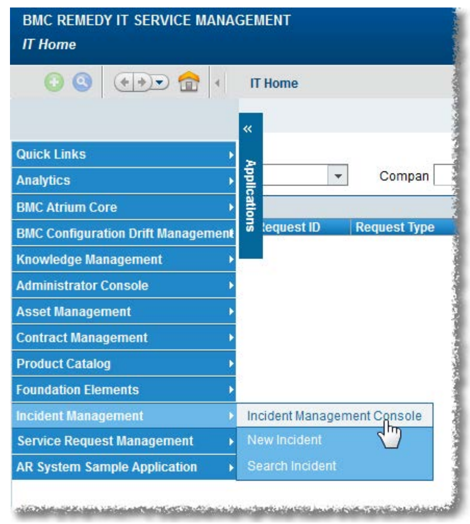
A user with the functional role of Support Group Manager, Support Group Lead, or Support Group Admin can also create Group templates, which will be available to any member of their support group.

Creating Email Templates

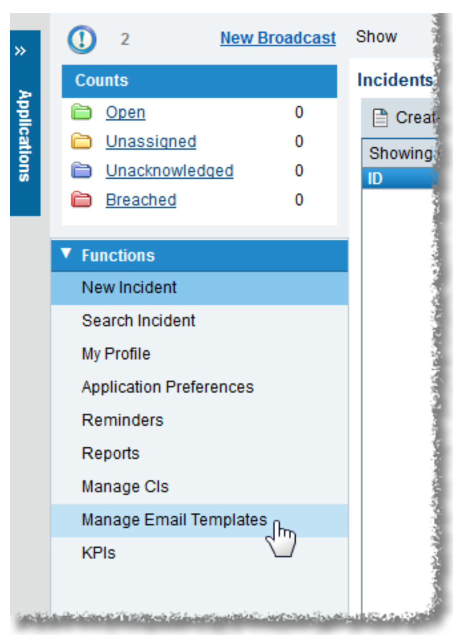
There are two methods for creating an Email Template. The first method involves creating it before you need it. The second method allows you to turn any email response into a template.

Method One: Create a Template Before You Need It

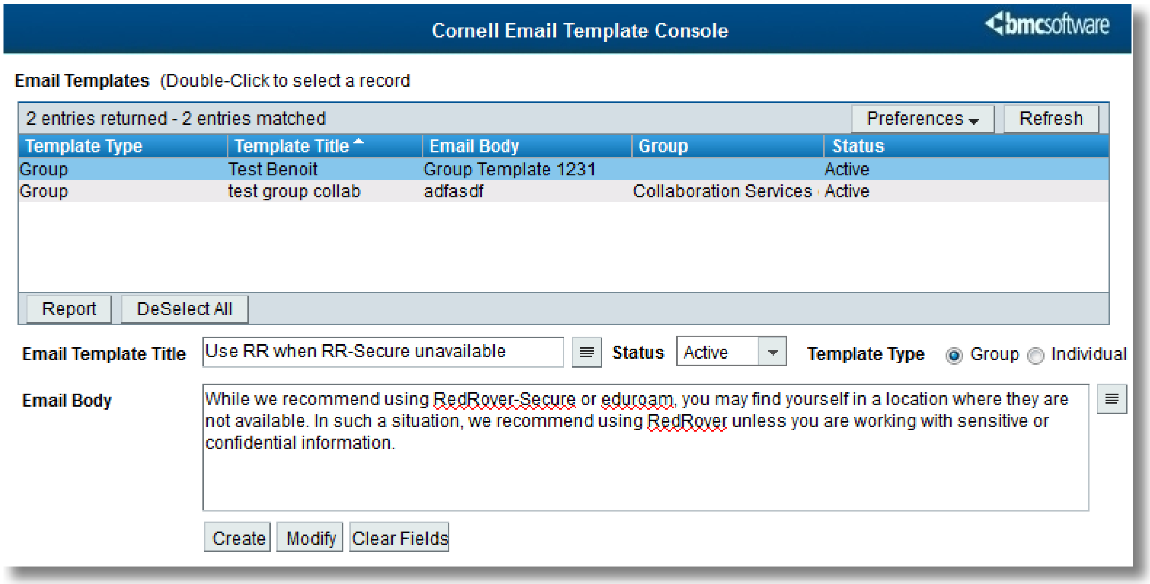
1. Log into Remedy.
2. From the **Applications** tab,
   select **Incident Management**,
   then **Incident Management Console**.



3. On the left, under **Functions**, click **Manage Email Templates**.
   The **Email Template Console** will open.



4. Enter an **Email Template Title** and the **Email Body** text.



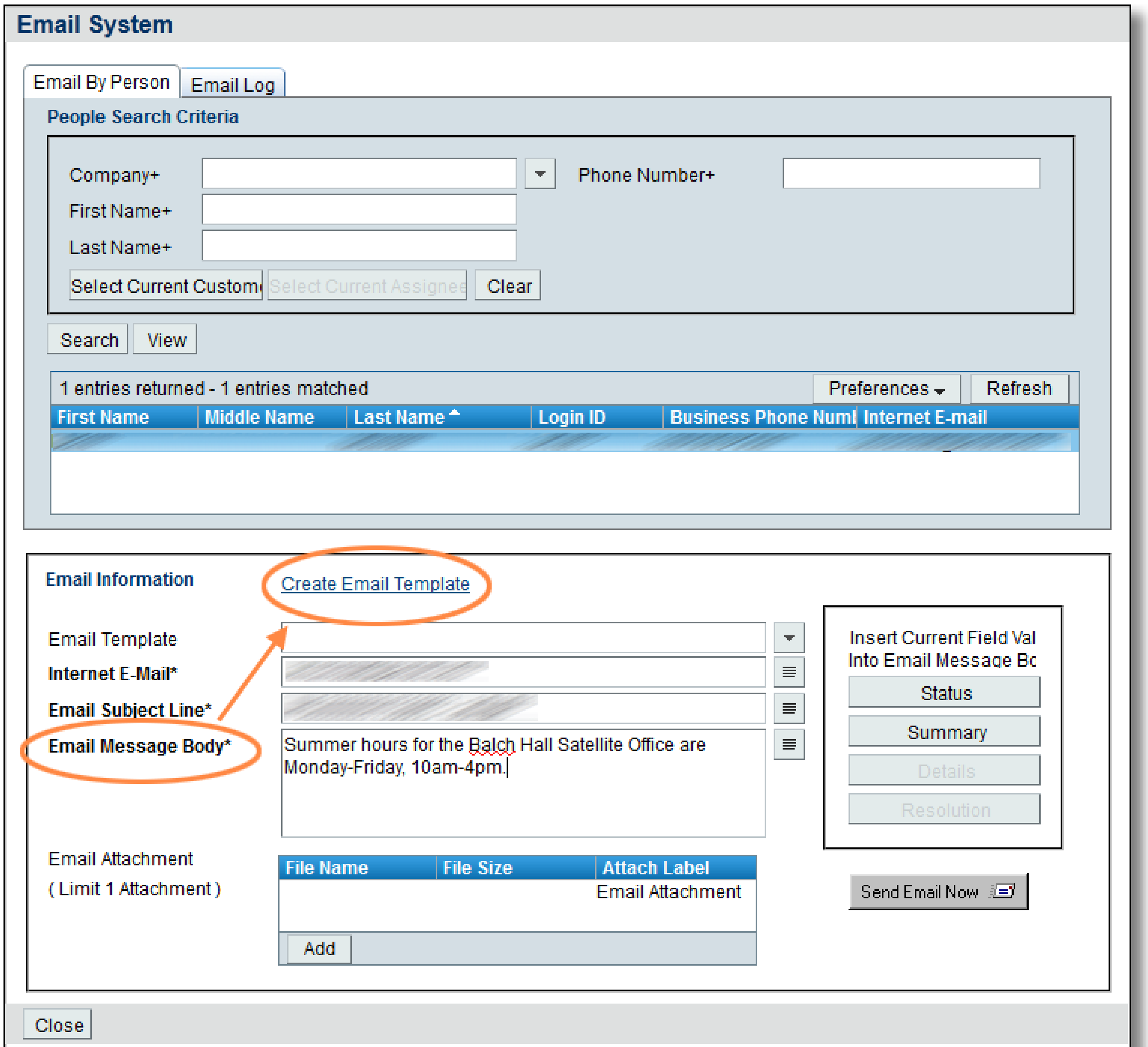
5. From the **Status** drop-down list, select **Active**.
6. For **Template Type**, select **Group** or **Individual**.
   (Only Support Group Managers, Leads, and Admins can select Group.)
7. Click **Create**.

If you selected **Group** and you are the manager, admin, or lead for more than one group, you will need to select the support group for which the template is available.

Method Two: Turn an Email Response Into a Template

You can also create a template while working in the Email form. This is useful when you find yourself creating an individual reply that you can foresee using again.

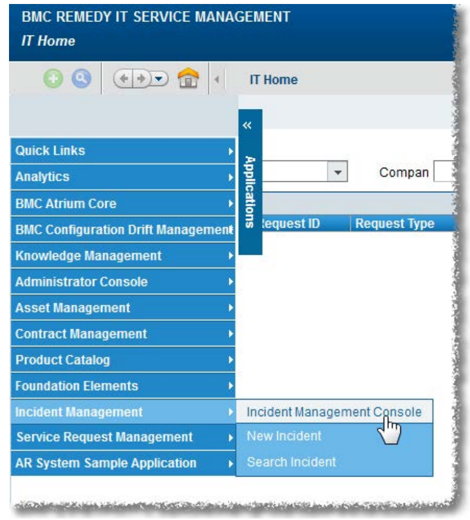
1. Open an incident.
2. Under **Functions** (on the left), click **Email System**. The Email System window will open.



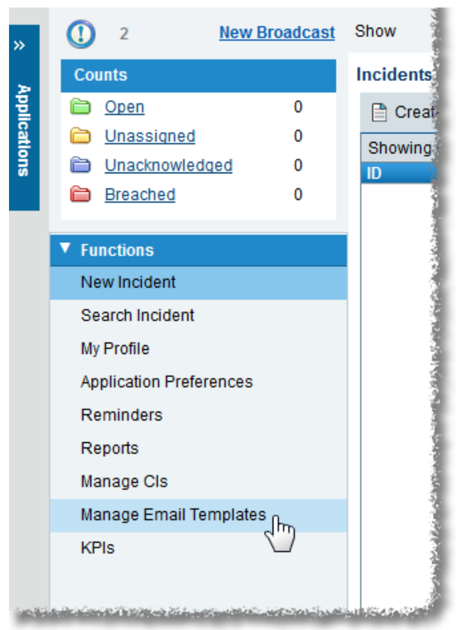
3. In the **Email Information** section, enter the **Email Message Body** text.
4. Click **Create Email Template**. An **Email Template** form will open with the **Email Body** field filled in with the text from your email message.
5. Enter an **Email Template Title**.
6. From the **Status** drop-down list, select **Active**.
7. For **Template Type**, select **Group** or **Individual**.
   (Only Support Group Managers, Leads, and Admins can select Group.)
8. Click **Save** (at the upper left corner of the form).

Modifying Email Templates

1. Log into Remedy.
2. From the **Applications** tab,
   select **Incident Management**,
   then **Incident Management Console**.



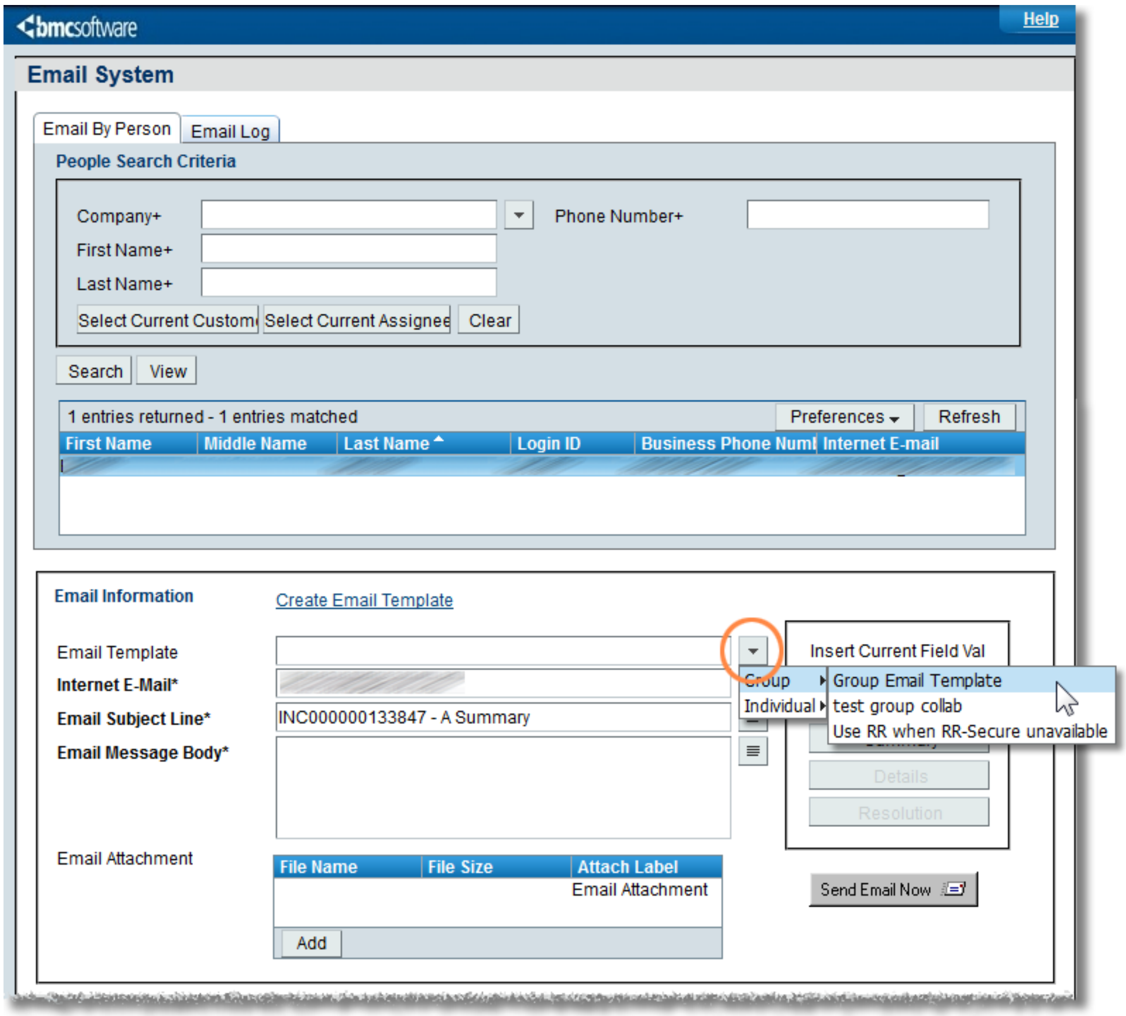
3. On the left, under **Functions**, click **Manage Email Templates**. The **Email Template Console** will open.



4. In the **Email Templates** table at the top of the screen, click on the template you want to edit. The fields on the lower part of the screen will show you the information for that template.
5. Edit the **Title**, **Body**, **Status**, and/or **Type** information as desired.
6. Click **Save**.

Using Email Templates

1. Open an incident.
2. Under **Functions** (on the left), click **Email System**. The **Email System** window will open.



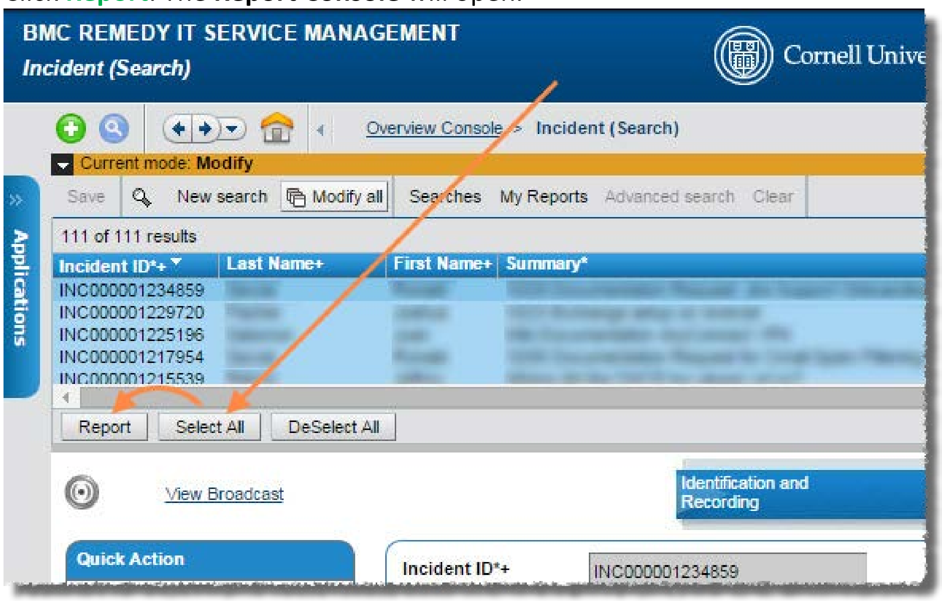
3. In the **Email Information** section, click the arrow at the right end of the **Email Template** field.
4. From the menu that appears, select **Group** or **Individual**, then select the desired template. The body text for that template will be pasted into the **Email Message Body** field, after any text already in the body.

You can select more than one template by repeating the step 4. Each time, the body text for the selected template will be added to the **end** of the text already captured in the **Email Message Body** (regardless of where you have placed the insertion point).

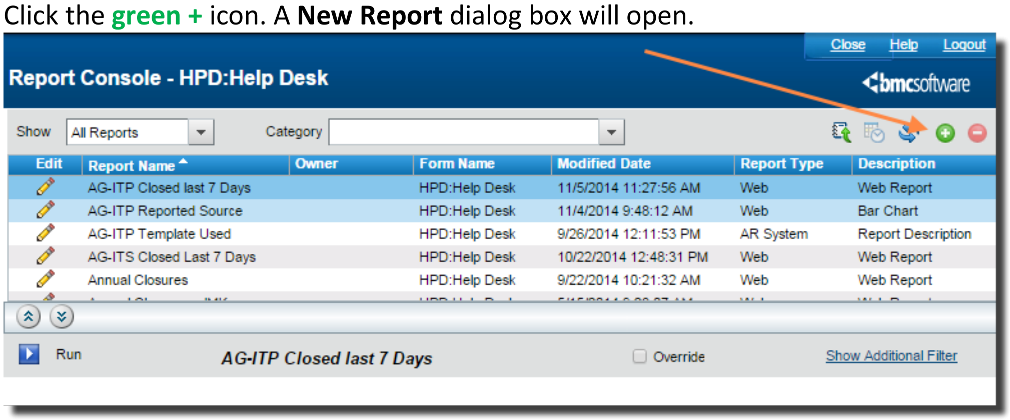
Reporting

Creating Reports via Search

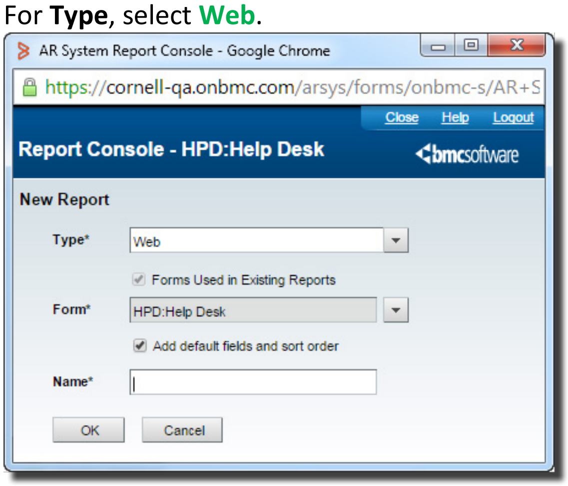
1. Run a Search to display the data you wish to report on
2. Click **Select All**.
3. Click **Report**. The **Report Console** will open.



4. Click the **green +** icon. A **New Report** dialog box will open.



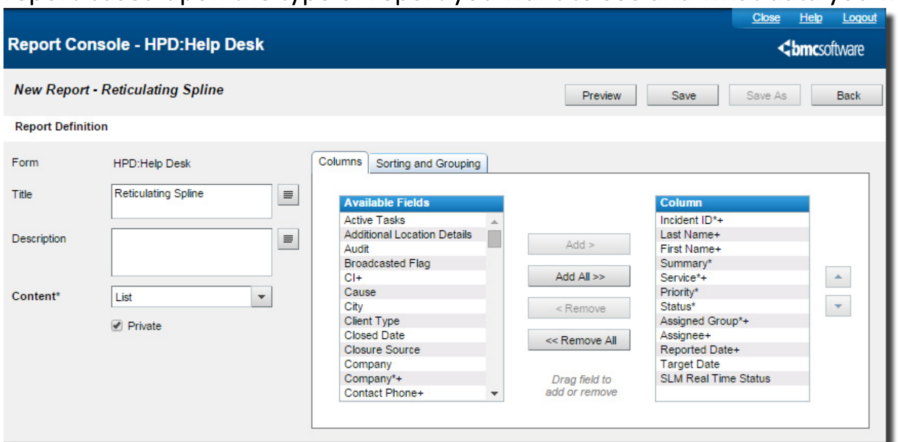
5. For **Type**, select **Web**.



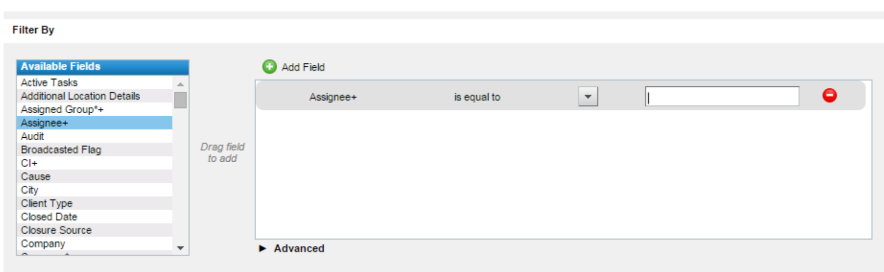
6. Select the appropriate **Form** based on your situation.

HPD:Help Desk	Incident Report
HPD:WorkLog	Incident Work Details Report
PBM:Problem Investigation	Problem Report
PBM:Investigation Worklog	Problem Work Details Report
CHG:Infrastructure Change	Change Request Report
CHG:WorkLog	Change Request Work Detail Report

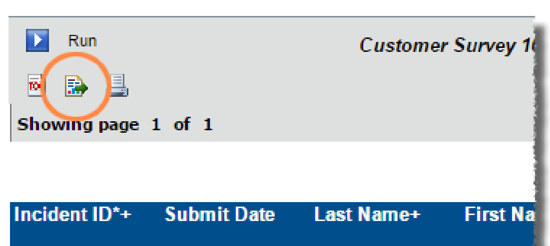
7. Give your report a name, then click OK. The New Report Console will open. Here you can configure the report based upon the type of report you want to see and what data you want displayed.



8. Under **Report Definition**, from the **Content** dropdown, select **List**, **Chart** or **Chart + List**.
9. If your selection in step 8 included "Chart," use the fields on the **Chart Options** tab to control the design of your chart.
   If your selection in step 8 included "List," use the fields on the **Columns** and **Sorting and Grouping** tabs to control the design of your report.
10. (optional) In the **Filter By** section, drag and drop the field(s) on which you'll be filtering, then specify the criteria.

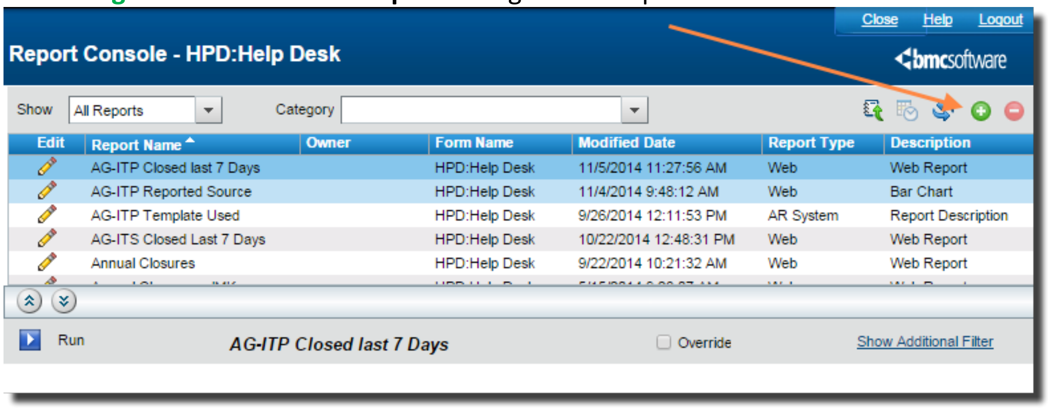


11. (optional) Click **Preview** to see how your report will look. You can modify the report definition and filters as needed before saving your report.
12. After you have created your report, click **Save**.
13. After you have saved the report, you can run the report and then export the data into multiple formats (Excel, PDF, etc.) by clicking on **Export Report**.

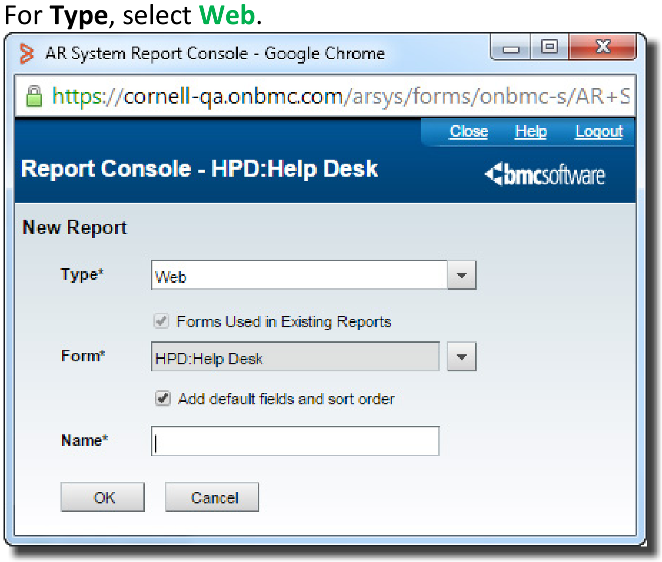


Creating Ad-hoc Reports

1. From the **Functions** menu (on the left side of the screen while in **Incident Management**), click **Reports**. The **Report Console** will open.
2. Click the **green +** icon. A **New Report** dialog box will open.



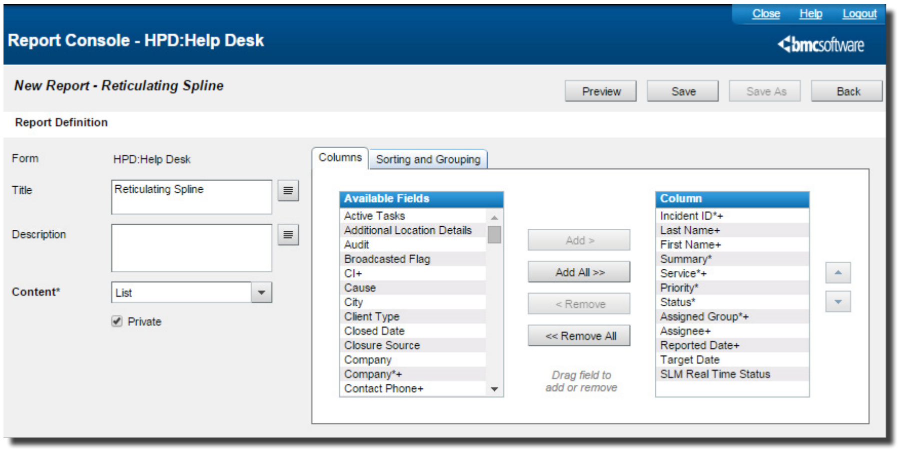
3. For **Type**, select **Web**.



4. Select the appropriate **Form** based on your situation.

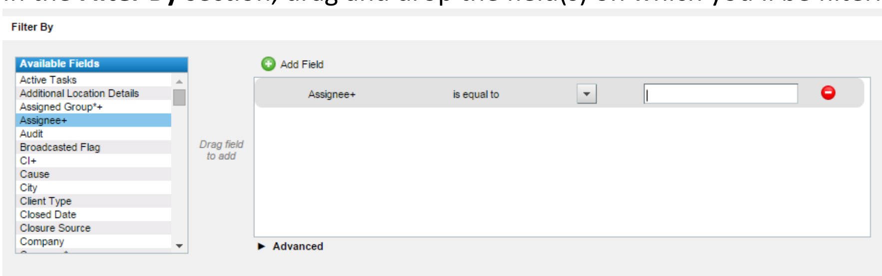
HPD:Help Desk	Incident Report
HPD:WorkLog	Incident Work Details Report
PBM:Problem Investigation	Problem Report
PBM:Investigation Worklog	Problem Work Details Report
CHG:Infrastructure Change	Change Request Report
CHG:WorkLog	Change Request Work Detail Report

5. Give your report a name, then click **OK**. The **New Report Console** will open. Here you can configure the report based upon the type of report you want to see and what data you want displayed.

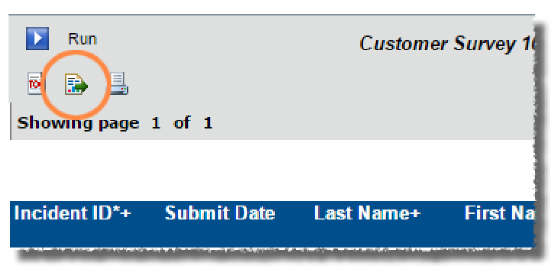


6. Under **Report Definition**, from the **Content** dropdown, select **List**, **Chart** or **Chart + List**.
7. If your selection in step 8 included "Chart," use the fields on the **Chart Options** tab to control the design of your chart.

   If your selection in step 8 included "List," use the fields on the **Columns** and **Sorting and Grouping** tabs to control the design of your report.
8. In the **Filter By** section, drag and drop the field(s) on which you'll be filtering, then specify the criteria.



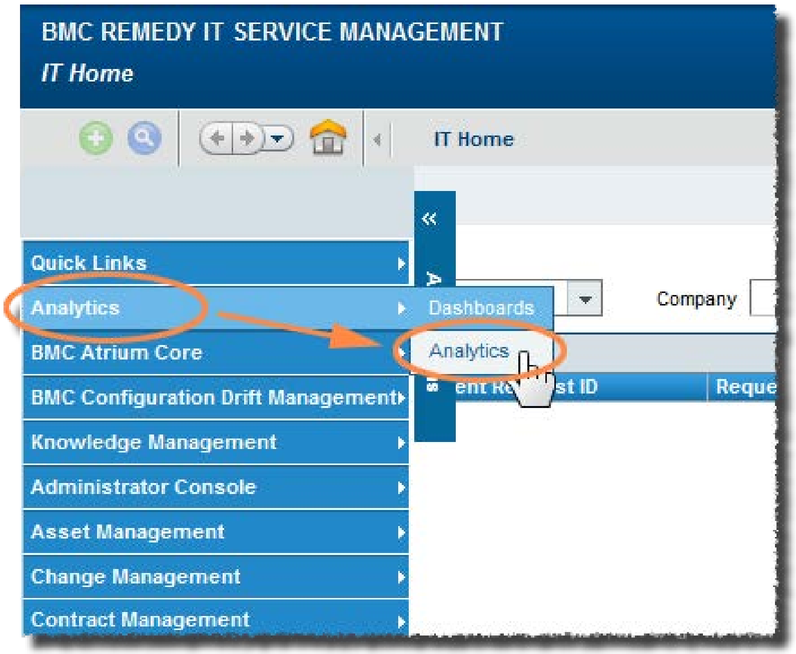
9. (optional) Click **Preview** to see how your report will look. You can modify the report definition and filters as needed before saving your report.
10. After you have created your report, click **Save**.
11. After you have saved the report, you can run the report and then export the data into multiple formats (Excel, PDF, etc.) by clicking on **Export Report**.



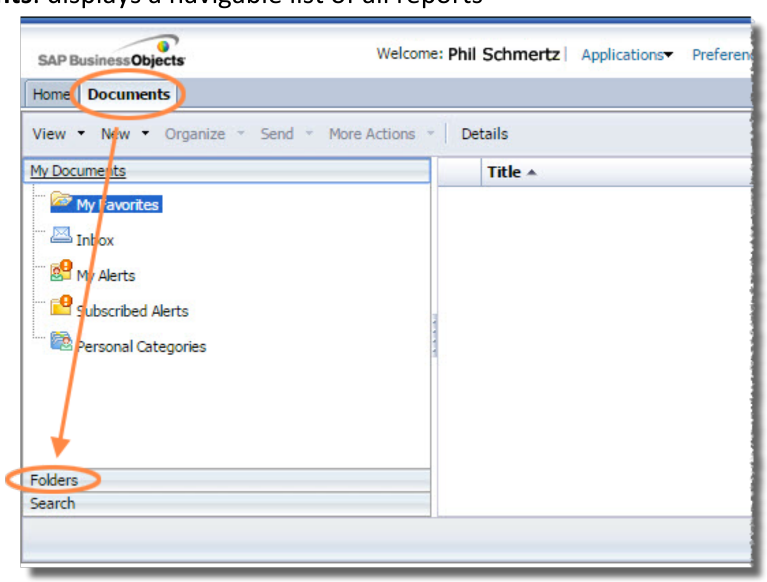
Using Analytics

CIT provides several standard reports that we have developed based upon the feedback and needs of the user community. There are also a number of reports designed by the vendor

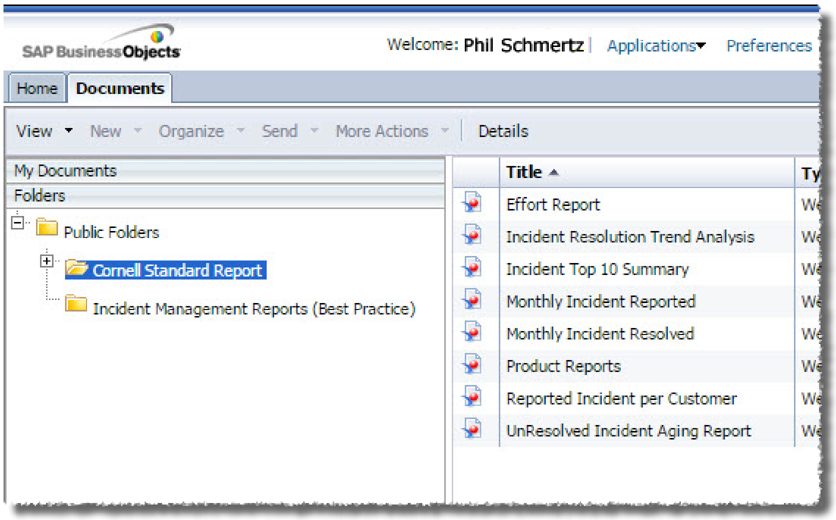
1. Log into Remedy.



2. From the **Applications** menu tab (on the left edge of your browser window), select **Analytics**, then, on the sub-menu that appears, select **Analytics** again. At the top of the browser window you will see two tabs:
   - **Home**: displays a list of recently viewed reports
   - **Documents**: displays a navigable list of all reports

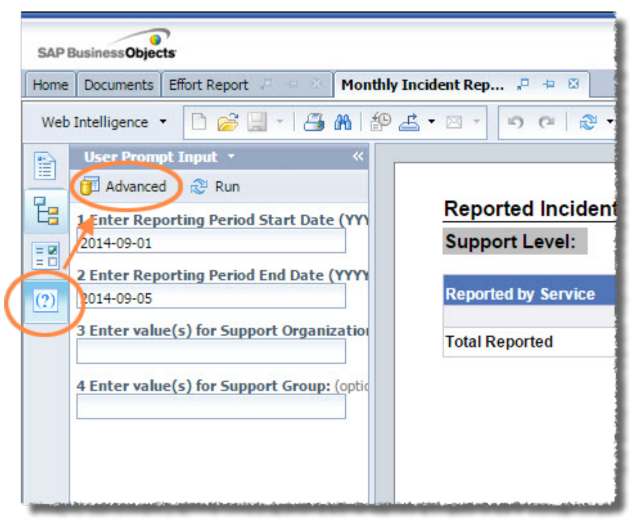


3. Click **Documents**. In the left navigation are three sections: **My Documents**, **Folders**, and **Search**. The section you select expands; the other two sections show just their title bar.
4. Click **Folders**.
5. In the folder hierarchy on the left, open **Public Folders**, then click on **Cornell Standard Reports**. The main section of the browser window will display the available reports.



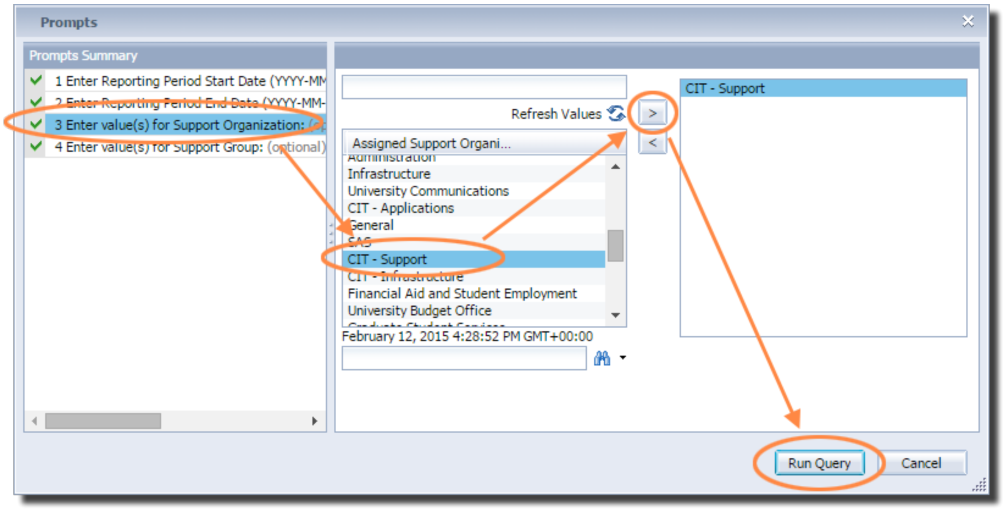
Optional: You can have Remedy display the Cornell Standard Report folder immediately by setting your Start Page preference. (See the section below.)

6. Double-click the name of the desired report. A results screen will be displayed, but ignore this, as it shows the results for the default set of criteria.

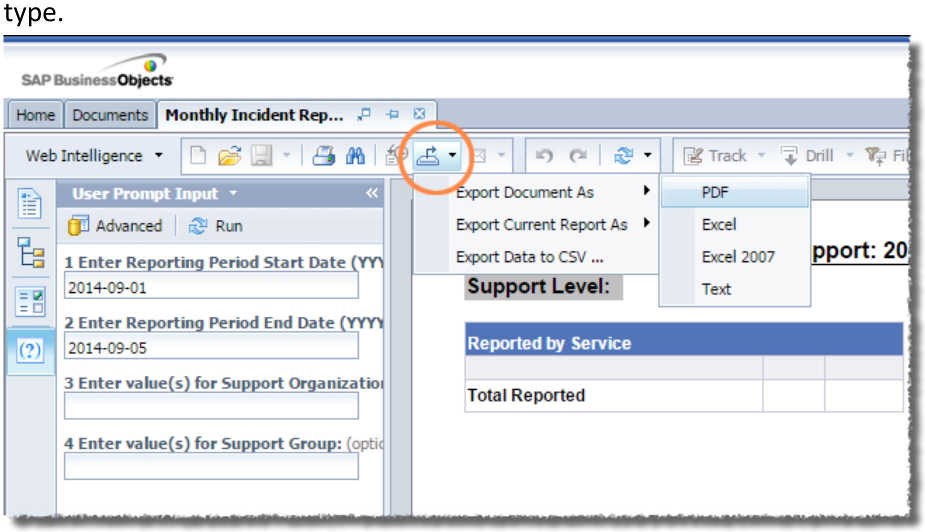


7. On the left edge of the window you'll see four icons. Click the fourth, which is **User Prompt Input** (it shows a question mark in parentheses). Next to the four icons, in a section titled **User Prompt Input**, you'll see a list of the search criteria available for this report.
8. At the top of the **User Prompt Input** section, click **Advanced**. A **Prompts** dialog box will open (it may take a minute or so) where you can modify the search criteria. The exact list of criteria shown will depend on the report you've selected.
9. To change **Start Date** or **End Date** parameters, click it in the numbered list at the left of the **Prompts** window, then enter the value in YYYY-MM-DD format.

10. If your report has additional fields such as product, support group or support organization, click on the numbered prompt on the left to see a list of available options. Select the desired data from the list and then click the right-facing arrow to move that value to the box on the right.



11. When you have finished specifying the report criteria, click **Run Query**. You will be returned to the results window (it may take a few moments), which now displays the results for your criteria. With some reports you will see more than one tab at the bottom of the browser window, offering different views of the data.
12. With some reports, you may further filter the results by Group within your Support Organization. Click the **Input Controls** icon (the third in the column of four icons on the left edge of the window), select one or more groups, then click **OK**.
    Please note that the Groups filter is only applied to the tab (at the bottom of the browser window) you were viewing when you clicked OK. That is, if you filter by group on one tab, then click to a different tab, the results shown will still be for all groups.
13. To save your results, click the **Export** icon, select **Export Document As**, then select the desired document type.

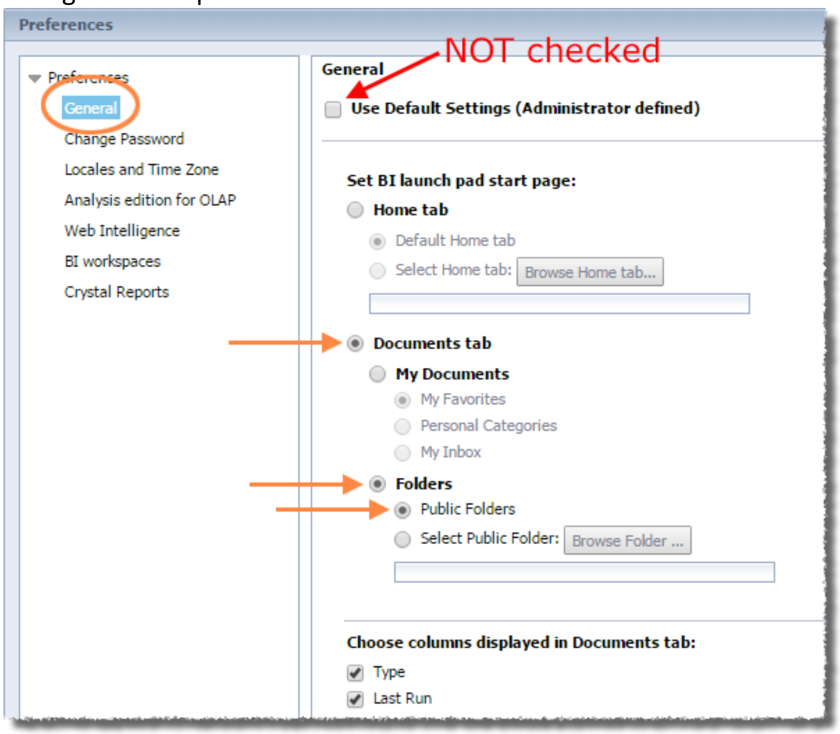


Reports can also be configured so that a copy is automatically emailed to specified users when the report is run. If you are interested in this feature, please contact remedy-admin@cornell.edu.

Set Start Page

You can save yourself a few clicks by telling Analytics to display the Cornell Standard Report folder when you log on.

1. While in Analytics, in the toolbar at the top of the browser window, click **Preferences**. A **Preferences** dialog box will open.

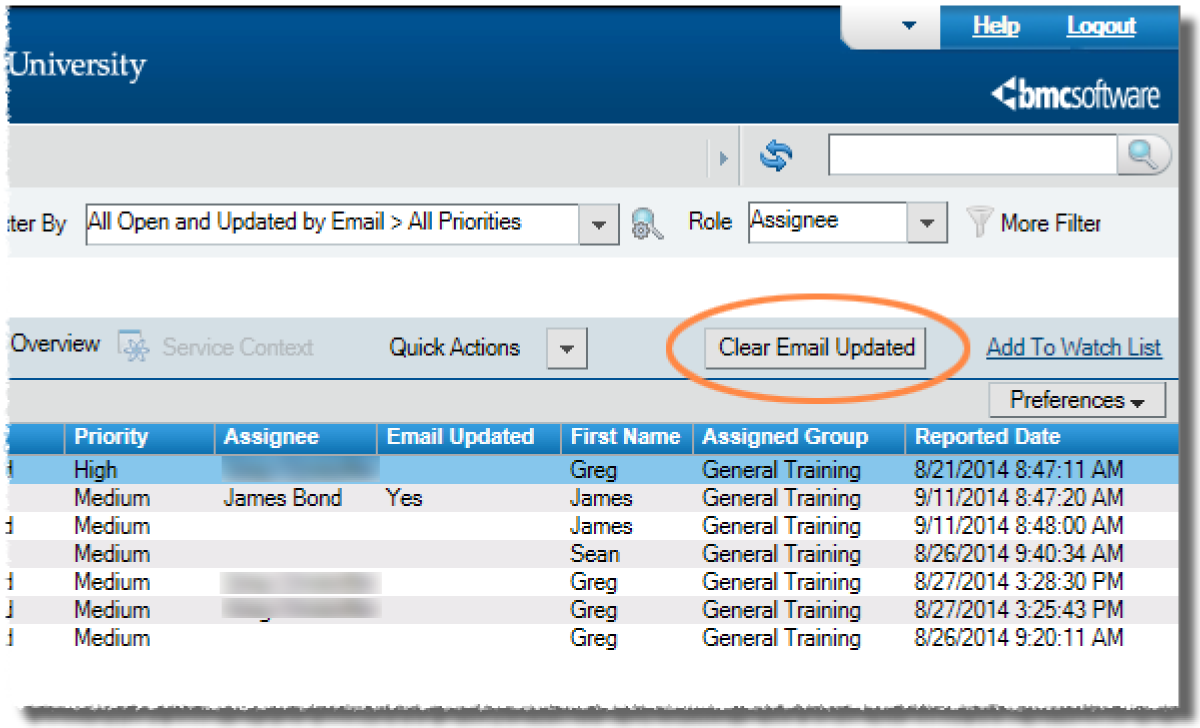


2. On the left, click **General**.
3. In the main section of the dialog box, make sure **Use Default Settings (Administrator defined)** is NOT checked.
4. Under **Set BI launch pad start page**, click **Documents tab**.
5. Under **Documents tab**, click **Folders**.
6. Under **Folders**, click **Public Folders**.
7. Click **Save & Close**.

Updating Closed & Canceled Tickets

Update by Email Flag

As an admin you can clear the flags on Closed or Cancelled tickets. Just highlight the closed or cancelled incident, then click **Clear Email Updated**.



Reopening a Closed or Canceled Ticket

To reopen a closed or canceled ticket, open the ticket and change the status to **Assigned**, then click **Save**.