Incident Alert Management Guide

PDF generated using the open source mwlib toolkit. See http://code.pediapress.com/ for more information.
PDF generated at: Wed, 29 Nov 2017 20:43:48 PST

Incident Alert Management

Note: *This article applies to Fuji and earlier releases. For more current information, see Incident Alert Management* [1] *at* http://docs.servicenow.com **The ServiceNow Wiki is no longer being updated. Visit** http://docs.servicenow.com **for the latest product documentation.**'

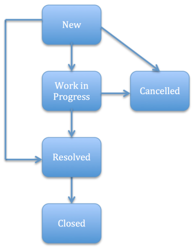
Overview

Incident alert management enables organizations to create and manage communications related to major business issues or incidents. This allows incident alert administrators to bring together all involved users during these events and establish quick and easy communication within this group.

For example, a major issue occurs in an organization's server room, leading to a high-priority incident being raised. The incident could potentially impact all users, so it is important to bring together key representatives and communicate quickly and effectively. An incident alert can facilitate this communication process and help resolve the source incident.

Incident alert management is available starting with the Dublin release.

Incident Alert Life Cycle



Incident alerts are created with a **New** state.

They follow a process that finishes with the **Closed** or **Cancelled** state.

A series of rules ensure that the alert progression is controlled and standardized.

- From **New**, the state can be changed to **Work in progress**, **Cancelled**, or **Resolved**.

  The state automatically changes from **New** to **Work in Progress** if the **Actions Taken** field is updated.
- From **Work in Progress**, the state can be changed to **Resolved** or **Cancelled**.

  Only the alert creator or a user with the admin role can cancel an incident alert.
- From **Resolved**, the state can be changed to **Closed**.

For more information, see Processing Incident Alerts.

Example Scenario

An example of how incident alerts can be used in an incident management process is:

1. An ITIL user creates a high-priority incident regarding a serious issue with the server room.
2. The incident alert administrator creates a new incident alert for this source incident.
3. As a result of a conference call discussion, a problem is identified based on the incident. This problem is assigned to the problem management team, which agrees to investigate further and identify tasks to improve service and prevent similar incidents from occurring.
4. The incident management team resolves the source incident. The source incident may also be closed at this point.
5. The incident alert administrator resolves the incident alert.
6. The incident alert administrator convenes a post incident review meeting to ensure that all identified tasks are logged and tracked to completion.
7. The incident alert administrator can now close the incident alert.

Incident Alert Management Features

You can use the Incident Alert Management application to:

- Create an incident alert when a crisis occurs.
- Set up contact responsibilities to identify the individuals who receive automatic notifications when incident alerts are created. Self-service users can subscribe to incident alerts if they want to receive notifications.
- Manage incident alerts to improve communication while dealing with the crisis.
- Use the optional Notify feature to send notifications by SMS messages and voicemails, and to set up conference calls.
- Monitor events and results with the incident alert dashboard and reports.

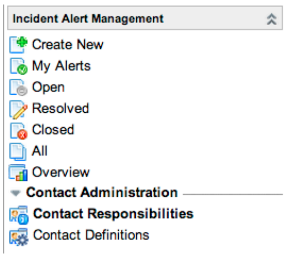
Roles

Role Title [Name]	Description
ITIL user [itil]	Can view the dashboard and incident alerts. Can subscribe to incident alerts.
Incident alert administrator [ia_admin]	Can create and edit incident alerts and contact records.

See User Roles for more details.

Menus and Modules

Administrators and incident alert administrators can use all these modules. ITIL users can only use the **Open**, **Resolved** and **Overview** modules.



The Incident Alert Management application contains these modules:

- **Create New:** Create a new incident alert.
- **My Alerts:** View and edit incident alerts where the current user is the incident creator.
- **Open:** View and edit active incident alerts, which are not resolved or closed.
- **Resolved:** View and edit resolved incident alerts.
- **Closed:** View closed incident alerts.
- **All:** View and edit all incident alerts.
- **Overview:** View a dashboard providing information on all incident alerts.
- **Contact Responsibilities:** View and edit contact responsibilities.
- **Contact Definitions:** View and edit contact definitions.

Activating Incident Alert Management

Administrators can activate the **Incident Alert Management** plugin.

Click the plus to expand instructions for activating a plugin.

If you have the admin role, use the following steps to activate the plugin.

1. Navigate to **System Definition > Plugins**.
2. Right-click the plugin name on the list and select **Activate/Upgrade**.

   If the plugin depends on other plugins, these plugins are listed along with their activation status.
3. [Optional] If available, select the **Load demo data** check box.

   Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance. You can load demo data after the plugin is activated by repeating this process and selecting the check box.
4. Click **Activate**.

References

[1] https://docs.servicenow.com/bundle/jakarta-it-service-management/page/product/incident-alert-management/concept/c_IncidentAlertManagement.html

Installed with Incident Alert Management

Overview

Activating the Incident Alert Management plugin adds or modifies tables, user roles, script includes, and other components.

Demo data is included with incident alert management.

Tables

Incident alert management adds or modifies the following tables.

Display Name [Table Name]	Description
Impacted CI [impacted_ci]	The CIs which have been impacted by the incident alert's source CI.
Incident Alert [incident_alert]	The base table for incident alerts.

Plugins

The following additional plugins are activated with incident alert management.

Plugin Name	Plugin ID	Description
Contact Management	com.snc.contact_management	Provides contact functionality and enables contact administration for incident alerts.

The following additional plugins can optionally be installed to provide additional functionality.

Plugin Name	Plugin ID	Description
Notify	com.snc.notifynow	Provides functionality to send SMS notifications and set up ad-hoc conference calls for an incident alert.

Properties

Incident alert management adds the following system properties.

Name	Description
com.snc.iam.log_level	Logging level for the business rule **MapUpstreamImpactedCI**. Debug is the most detailed option with full trace of how the Impacted CI List is calculated. Error is the minimal logging option with only severe errors being logged • **Type:** String • **Default value:** info • **Possible Values:** debug,info,error • **Location:** System Properties [sys_properties] table
glide.ui.incident_alert_activity.fields	Incident alert activity formatter fields. This is the list of fields tracked from the incident alert form in the activity formatter. • **Type:** String • **Default value:** opened_by, work_notes, comments, severity, estd_distruption_time, actual_disruption_time • **Location:** System Properties [sys_properties] table
com.snc.iam.on_call_escalation_level	Escalation level shown in the selection screen for conference call participants. By default the primary and secondary on-call persons are in the recommended list. The behavior can be changed by adding this property to the system with a different value. • **Type:** String • **Default value:** 2 (primary and secondary on-call) • **Possible Values:** 0, 1, 2, 3, etc. Set to -1 to include everybody in the escalation plan. • **Location:** System Properties [sys_properties] table

User Roles

Incident alert management adds the following user roles.

Role	Contains Roles	Description
ia_admin	notifynow_admin, contact_admin	Can create and edit incident alerts, and manage contact information. This role is only contained in ia_admin if Notify is active.
contact_admin	contact_user	[Requires ia_admin role] Can create and edit contact definitions and contact responsibilities.
contact_user		[Requires ia_admin role] Can view contacts, contact definitions, contact responsibilities and default overrides.

Note: *Typically, incident alert administrators may need to have both ia_admin and itil roles, to have full access to incident alert functionality. For example, the itil and ia_admin role are both needed to be able to create incident alerts from within an incident form.*

UI Actions

Incident alert management adds the following UI actions.

UI Action	Tables	Description
Create new incident alert	incident [incident]	Creates new incident alert from an existing incident record.
Show Live Feed (1)	Incident Alert [incident_alert]	Displays live feed for the document on a list.
Show Live Feed (2)	Incident Alert [incident_alert]	Displays live feed for the document.
Follow on Live Feed (1)	Incident Alert [incident_alert]	Adds user to the live feed for this document. If no feed exists, it is created. This is for lists, forms have the redirect.
Follow on Live Feed (2)	Incident Alert [incident_alert]	Adds user to the live feed for this document. If no feed exists, it is created. This is for forms using the redirect.
View PIR Report	Incident Alert [incident_alert]	Shows the post incident review report.

The following UI actions are also installed if Notify is activated:

UI Action	Tables	Description
Initiate Conference Call	Incident Alert [incident_alert]	Initiate a conference call for a incident alert.

UI Policies

Incident alert management adds the following UI policies.

UI Policy	Table
Make PIR section source incident fields read only	Incident Alert [incident_alert]
Closure info	Incident Alert [incident_alert]
Resolution Info	Incident Alert [incident_alert]
Capturing open / closed / resolved info	Incident Alert [incident_alert]

Script Includes

Incident alert management adds the following script includes.

Script Include	Description
IncidentAlertAjax	AJAX methods for incident alert.

The following script includes are also installed if Notify is activated.

Script Include	Description
IncidentAlertConferenceCall	Returns a list of frequent participants that have joined Notify conference calls.

Client Scripts

Incident alert management adds the following client scripts.

Script	Table	Description
PIR visibility	Incident Alert [incident_alert]	Show PIR section if state is resolved or closed.
Adding info from Source Incident	Incident Alert [incident_alert]	Bring in information from source incident.

Business Rules

Incident alert management adds the following business rules.

Business Rule Name	Table	Description
Incident Alert insertion limitation	Incident Alert [incident_alert]	Only allow one active incident alert to be associated with an incident.
MapUpstreamImpactedCI	Incident Alert [incident_alert]	Populate impacted CIs related list.
Insert in state "New" only	Incident Alert [incident_alert]	Make sure an incident alert can only be created with in a **New** state.
Opened, Resolved and Closed capturing	Incident Alert [incident_alert]	Capture who did what and when.
Automatically WIP if actions taken	Incident Alert [incident_alert]	Automatically change the incident alert state to **Work In Progress** when comments are added.
Check role is ia_admin	Contact [contact]	Make sure that the logged in user is an incident alert administrator.
Map upstream impacted CI	Incident Alert [incident_alert]	Map all impacted configuration items based on source CI.

The following business rules are also installed if Notify is activated.

Business Rule Name	Table	Description
SMS on new Incident Alert	Incident Alert [incident_alert]	Send an SMS notification when an incident alert is created.
Conference Call Allowed	Incident Alert [incident_alert]	Check if a conference call can be initiated.
Update Conference Call Finished IA Activity	NotifyNow Conference Call [notifynow_conference_call]	Extend the Incident Alert activity log when a conference call finishes.
Update Conference Call Started IA Activity	NotifyNow Conference Call [notifynow_conference_call]	Extend the Incident Alert activity log when a conference call is initiated.

Creating Incident Alerts

Overview

Incident alerts are typically created to help manage and track communications around a high-priority incident or other issue.

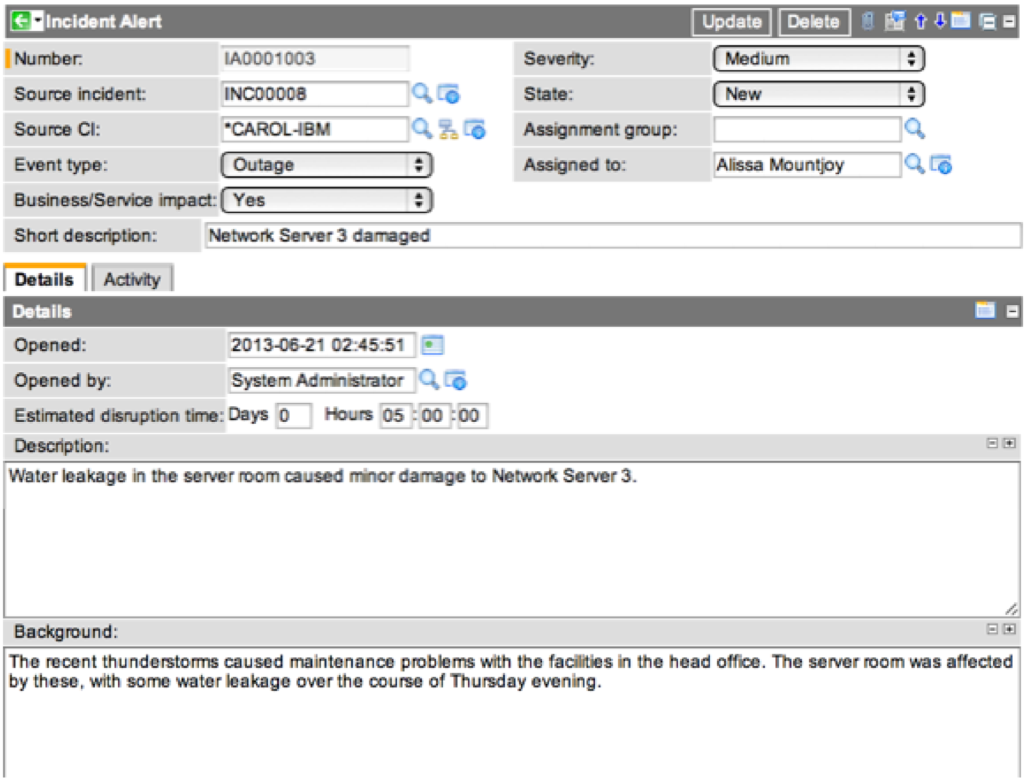
Incident alerts can be created:

- Directly as standalone alerts.
- From an existing active incident. Only one incident alert can be created for each incident.

Creating Alerts Directly

Create an incident alert directly if the original issue that caused the alert was not logged as an incident. For example, a significant facilities problem may not be logged as an incident in ServiceNow, but may still require an incident alert to be created.

1. Navigate to **Incident Alert Management > Create New**.
2. Fill in the fields (see table).



Number:	IA0001003	Severity:	Medium
Source incident:	INC00008	State:	New
Source CI:	*CAROL-IBM	Assignment group:	
Event type:	Outage	Assigned to:	Alissa Mountjoy
Business/Service impact:	Yes		
Short description:	Network Server 3 damaged		

Details

Opened:	2013-06-21 02:45:51
Opened by:	System Administrator
Estimated disruption time:	Days 0 Hours 05 : 00 : 00

Description:

Water leakage in the server room caused minor damage to Network Server 3.

Background:

The recent thunderstorms caused maintenance problems with the facilities in the head office. The server room was affected by these, with some water leakage over the course of Thursday evening.

3. Click **Submit**.

Field	Description
Number	Automatically generated incident alert ID, in the format IAxxxxxxxx.
Severity	The severity for the incident alert. Values are **Major**, **High**, **Medium**, or **Low**.
Source incident	The source incident for this alert, if any. If you select a source incident, the **Source CI**, **Short description**, and **Background** fields are populated with data from this incident, unless there is existing data in those fields.
State	The state of the alert. Values are **New**, **Work In Progress**, **Resolved**, **Cancelled**, or **Closed**.
Source CI	The source CI for this alert, if any. If there is a source incident selected, this field is populated with the source CI attached to that incident. If there is no source incident selected, select the source CI manually, if applicable. If the source CI has related CIs, these are automatically listed in the **Impacted CIs** related list.
Assignment group	The assignment group, if any, for that incident alert. For example, there might be a group that represents a crisis management team, including a number of Incident Managers, Duty Directors and Duty Managers.
Event type	The type of event. Values are: **Outage**, **Degradation**, **Capacity**, **SLA/Delay**, or **Fail-Over**.
Assigned to	The assigned user for the alert. This can be an ITIL user or an incident alert administrator, and defaults to the user who creates the alert.
Business/Service impact	**Yes** or **No** to indicate whether the business or a service is impacted.
Short description	A brief summary of the alert.
***Details** section*	
Opened	When the alert was created.
Opened by	The creator of the alert. This defaults to the user who creates the alert.
Estimated disruption time	The estimated duration of the disruption.
Description	More detailed information for the alert.
Background	Background information about the alert.
***Activity** section*	
Actions taken	The details of all actions taken while working on the alert.
Work notes	Any separate work notes relevant to the alert that might help in communications.

Creating Alerts from an Incident

Creating an incident alert from within an existing incident record populates the alert with information from that incident.

1. Open an existing incident
2. Select the **Create new incident alert** related link.
3. A new incident alert record is created and populated with data from the incident.

   The original incident becomes the source incident of this alert.

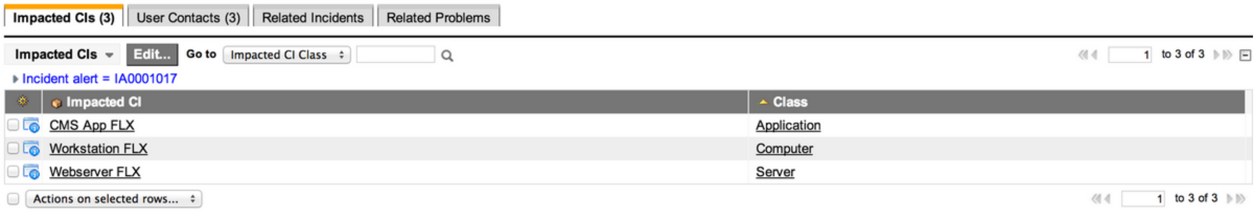
   Other fields populated with data from the source incident are: **Source CI**, **Short description**, **Background**.
4. Fill in other fields as required, as described for creating alerts directly.
5. Click **Submit**.

Viewing Related Lists

After you create an incident alert, several related lists are added to the form: Impacted CIs, User Contacts, Related Incidents and Related Problems.

Impacted CIs

The **Impacted CIs** related list shows all the CIs that the CMDB shows as related to the source CI for this alert.



Impacted CI	Class
CMS App FLX	Application
Workstation FLX	Computer
Webserver FLX	Server

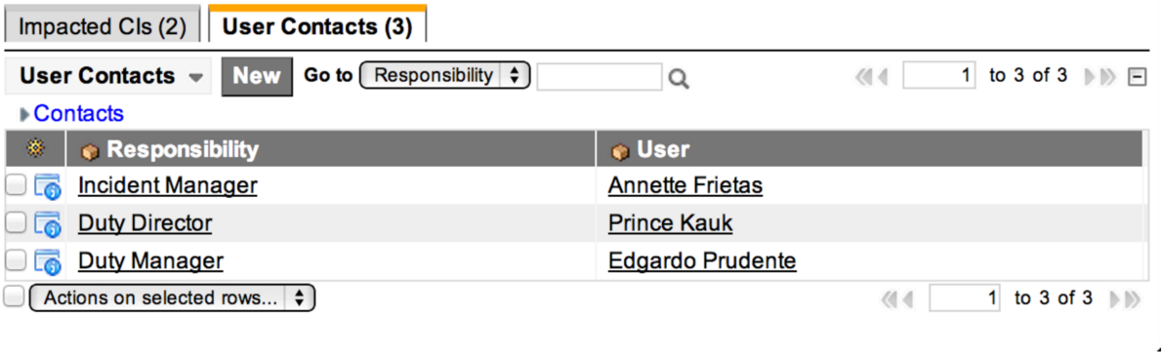
Administrators and incident alert administrators can modify this list. Click the **Edit** button, then add and remove CIs, as appropriate.

Note: *Administrators can adjust the com.snc.iam.log_level property to view more log information for how this list is determined. By default the value is* ***info****. Set this to* ***debug*** *to see more detailed log information.*

User Contacts

After an incident alert is created, the following default user responsibilities are added to the **User Contacts** related list:

- Duty Manager
- Duty Director
- Incident Manager



Responsibility	User
Incident Manager	Annette Frietas
Duty Director	Prince Kauk
Duty Manager	Edgardo Prudente

From this list:

- Click **New** to add a new contact.
- Click the lookup icon beside the responsibility entry to edit the details for that responsibility.
- Select the check box for the entry, then select **Actions on selected rows..** and click **Delete**, to delete that entry from the user contacts list.

For more information, see Using Contacts with Incident Alerts.

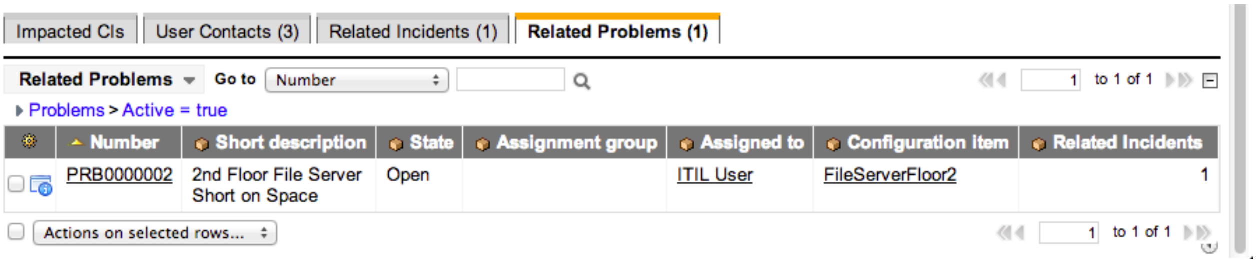
Group Contacts

There are currently no default group contacts defined for incident alert management. However, you can define group responsibilities for your organization, then personalize the form layout to add the **Group Contacts** related list.

You can then edit and modify this list, as for the user contacts.

Related Incidents and Related Problems

The **Related Incidents** and **Related Problems** related lists show incidents and problems affected, based on the source incident for the alert.



Impacted CIs | User Contacts (3) | Related Incidents (1) | **Related Problems (1)**

Related Problems ▾ Go to Number ⇕ 1 to 1 of 1

▸ Problems > Active = true

	Number	Short description	State	Assignment group	Assigned to	Configuration item	Related Incidents
□	PRB0000002	2nd Floor File Server Short on Space	Open		ITIL User	FileServerFloor2	1

□ Actions on selected rows... ⇕ 1 to 1 of 1

This information is read-only. To make changes to this information, update the source incident.

Notify

If Notify is active, two additional related lists appear on the Incident Alert form.

The **SMS Messages** related list gives information about the SMS notifications sent to users identified as contacts on the incident alert. For example, by default, SMS notifications are sent to users who are assigned to responsibilities when an incident alert is created.

The SMS message content depends on the fields that were filled in when the alert is created, but is generally in the following format:

IA0000001: a <*severity*> severity <*event type*> incident alert for '<*CI name*>' has been opened

Note: *The CI name may be truncated to keep the content within 160 characters.*

The **Conference Calls** related list shows details of any conference calls that have been launched for the incident alert.

For more information, see Using Notify with Incident Alert Management.

Processing Incident Alerts

Overview

After creating an incident alert, the incident alert administrator can process it through a set of predefined states to ensure efficient and consistent handling. The incident alert administrator may also be assigned the contact responsibility of Duty Manager.

When an incident alert is resolved, the incident alert administrator can run a post incident review, and can generate a report for that review from within the incident alert.

The incident alert administrator can also view the dashboard and run reports on incident alerts.

Resolving an Alert

Typically, when the event that initiated the incident alert is resolved, the incident alert can also be marked as resolved.

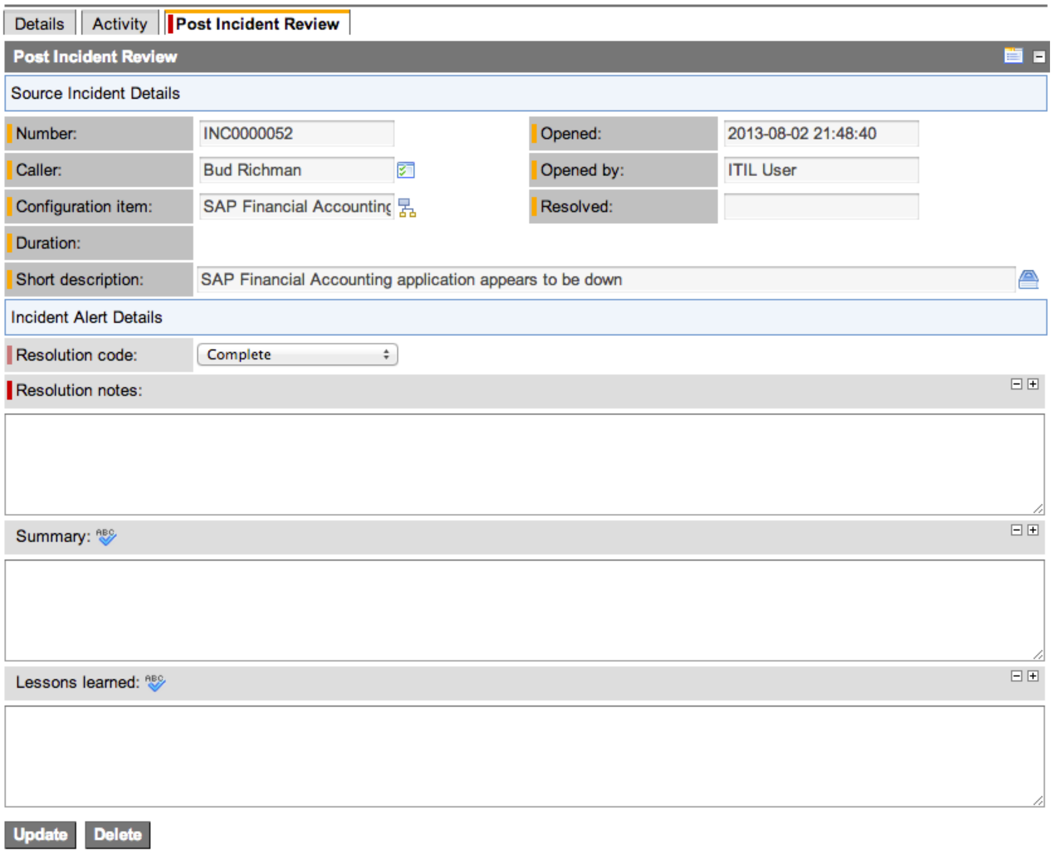
When an alert is resolved, the following fields are added to the Incident Alert form:

Field	Description
Resolved	The date and time when the alert was resolved. Automatically set when the form is saved, but can be changed later.
Resolved by	The user who resolved the alert. Automatically set when the form is saved, but can be changed later.
Actual disruption time	The amount of disruption time recorded, based on the time between when the incident alert was created and the time it was marked as resolved.
Post Incident Review section	Information for discussion and review. For more information, see Running a Post Incident Review.

Running a Post Incident Review

After an incident alert has been marked as resolved, the **Post Incident Review** section appears on the Incident Alert form, This allows the incident alert administrator to initiate a post incident review (PIR) meeting to review and learn from the issues that arose from the source event.

Fill in this section as appropriate, then use the **View PIR Report** related link to create the PIR report. This report can be circulated or printed for the PIR meeting.



Post Incident Review

Source Incident Details

Number:	INC0000052	Opened:	2013-08-02 21:48:40
Caller:	Bud Richman	Opened by:	ITIL User
Configuration item:	SAP Financial Accounting	Resolved:	
Duration:			
Short description:	SAP Financial Accounting application appears to be down		

Incident Alert Details

Resolution code: Complete

Resolution notes:

Summary:

Lessons learned:

The **Source Incident Details** section contains read-only information, taken from the source incident

Fill in the **Incident Alert Details** fields as follows:

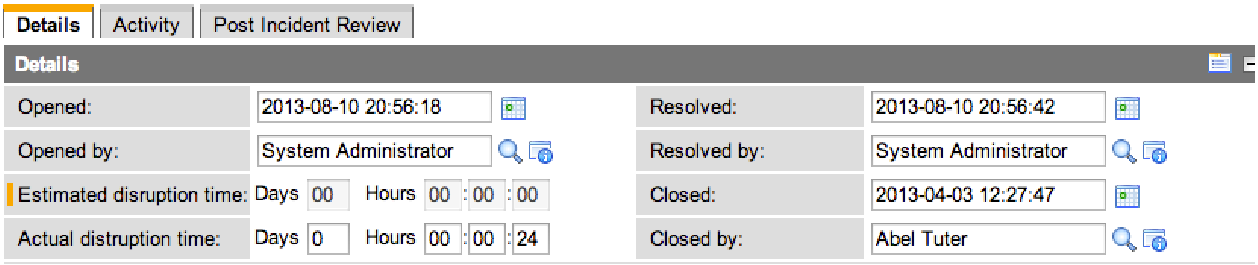
Field	Description
Resolution code	[Required] Whether the incident alert has been completed. Values can be **Complete**, **Complete with Actions**, or **Not complete**.
Resolution notes	[Required] Any notes about the resolution of the incident alert. After a user enters information in the resolution notes and saves the record, both the **Resolution notes** and **Resolution code** are set to read-only.
Summary	A summary of the incident alert.
Lessons learned	Any lessons learned from the review process.

Use the **View PIR Report** related link to create a report that can be circulated or printed for the post incident review meeting.

Closing an Alert

Typically, when the post incident review is complete, the incident alert can be closed.

To close an alert, mark the state as **Closed**.



Details

Opened:	2013-08-10 20:56:18	Resolved:	2013-08-10 20:56:42
Opened by:	System Administrator	Resolved by:	System Administrator
Estimated disruption time:	Days 00 Hours 00 : 00 : 00	Closed:	2013-04-03 12:27:47
Actual distruption time:	Days 0 Hours 00 : 00 : 24	Closed by:	Abel Tuter

The following values are then set in the **Details** section of the alert.

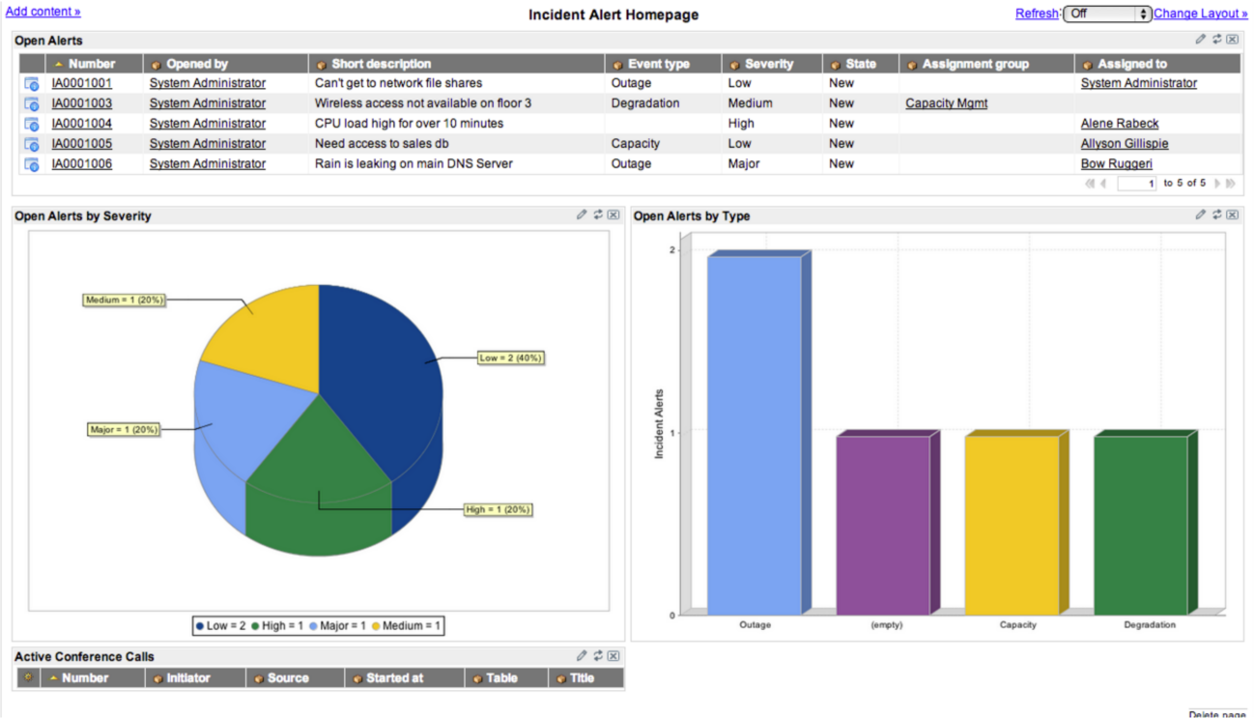
Field	Description
Closed	The date and time when the alert was closed.
Closed by	The user who closed the alert.

These fields can be changed later, if required.

Viewing the Dashboard

The incident alert dashboard is a homepage that contains gauges and reports showing open incident alerts with a status of **New** or **Work in Progress**.

To open the dashboard, navigate to **Incident Alert Management > Overview** or point to the homepage icon (🏠) in the banner and select **Incident Alert Homepage**.



Incident Alert Homepage

Open Alerts

	Number	Opened by	Short description	Event type	Severity	State	Assignment group	Assigned to
	IA0001001	System Administrator	Can't get to network file shares	Outage	Low	New		System Administrator
	IA0001003	System Administrator	Wireless access not available on floor 3	Degradation	Medium	New	Capacity Mgmt	
	IA0001004	System Administrator	CPU load high for over 10 minutes		High	New		Alene Rabeck
	IA0001005	System Administrator	Need access to sales db	Capacity	Low	New		Allyson Gillispie
	IA0001006	System Administrator	Rain is leaking on main DNS Server	Outage	Major	New		Bow Ruggeri

Refresh: Off

Open Alerts by Severity

Open Alerts by Type

Active Conference Calls

	Number	Initiator	Source	Started at	Table	Title

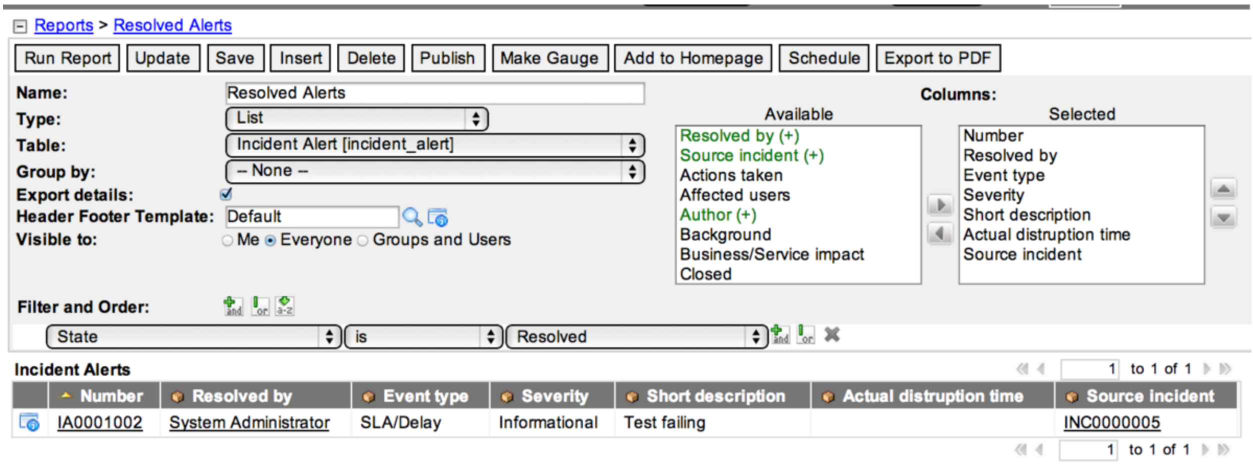
- **Open Alerts:** displays all open alerts. Click an alert number to open the details for that alert.
- **Open Alerts By Severity:** groups open alerts by severity levels, as defined in the Incident Alert form.
- **Open Alerts by Type:** groups open alerts by event type, as defined in the Incident Alert form.
- **Active Conference Calls:** displays any active conference calls. This appears only if Notify is active.

Running Incident Alert Reports

Administrators and incident alert administrators can run incident alert reports to view the current status of alerts, track them and intervene where required, and improve overall efficiency and effectiveness.

To run a report:

1. Navigate to **Reports > View / Run**.
2. Locate the **Incident Alert** heading.
3. Click a report name and view the results (see table).



Reports > Resolved Alerts

Name: Resolved Alerts
Type: List
Table: Incident Alert [incident_alert]
Group by: -- None --
Export details: ☑
Header Footer Template: Default
Visible to: ○ Me ● Everyone ○ Groups and Users

Columns:

Available	Selected
Resolved by (+)	Number
Source incident (+)	Resolved by
Actions taken	Event type
Affected users	Severity
Author (+)	Short description
Background	Actual distruption time
Business/Service impact	Source incident
Closed	

Filter and Order:
State is Resolved

Incident Alerts 1 to 1 of 1

	Number	Resolved by	Event type	Severity	Short description	Actual distruption time	Source incident
	IA0001002	System Administrator	SLA/Delay	Informational	Test failing		INC0000005

1 to 1 of 1

4. Alter parameters, as required, and click **Run Report** to run the revised report.

Report Name	Description	Contains
IAs opened in the last 72 hours	All alerts, of any state, which have been opened in the last 72 hours.	Number, Created by, Event Type, Severity, Title, Open time, Estimated Disruption time, Related Record, Assignee.
Open Alerts	Displays all open alerts. Click an alert number to open the details for that alert. Displayed on the dashboard by default.	Number, Severity, Short description, Source incident, State, Business/Service impact, Assigned to.
Open Alerts By Severity	Groups open alerts by severity levels, as defined in the Incident Alert form. Displayed as a pie chart on the dashboard by default.	Severity.
Open Alerts by Type	Groups open alerts by alert type, as defined in the Incident Alert form. Displayed as a bar chart on the dashboard by default.	Event type.
Open IA's this week	All open alerts which have been created in the current week.	Number, Created by, Event Type, Severity, Title, Time Created, Estimated Disruption time, Related Record number, Incident Manager.
Resolved Alerts	All alerts which have been resolved. This does not include closed alerts.	Number, Resolved by, Event Type, Severity, Title, Actual Disruption time, Source Incident number, Source Incident status.
Resolved IA's this Week	All alerts which have been resolved in the current week, including any alerts closed this week.	Number, Resolved by, Event Type, Severity, Title, Actual Disruption time, Related Record, Assignee.

Using Notify with Incident Alert Management

Note: *This article applies to Fuji and earlier releases. For more current information, see Notify with Incident Alert*[1] *at* http://docs.servicenow.com **The ServiceNow Wiki is no longer being updated. Visit** http://docs.servicenow.com **for the latest product documentation.**

Overview

Within incident alert management, Notify functions can be used to launch a conference call for involved users to discuss the relevant issue. This allows all users involved in the issue to quickly communicate with each other and helps in the fast turnaround and resolution of the issue.

Note: *Notify is available as a separate subscription from the ServiceNow platform. To purchase a subscription, contact your ServiceNow account manager.*

Sending SMS Notifications

When you create a new incident alert, Notify sends an SMS notification to the users defined as default contact responsibilities for the alert. This text message is sent to the mobile phone number on each user's record and takes this form:

IA<number>: a <Severity> severity <Event Type> incident alert for <CI Name> has been opened.

Administrators can modify the content of this message by editing the **SMS on new Incident Alert** business rule.

Note: *The message is limited to 160 characters. So if a long CI name is included in the message, this may be truncated in the message.*

Launching a Conference Call

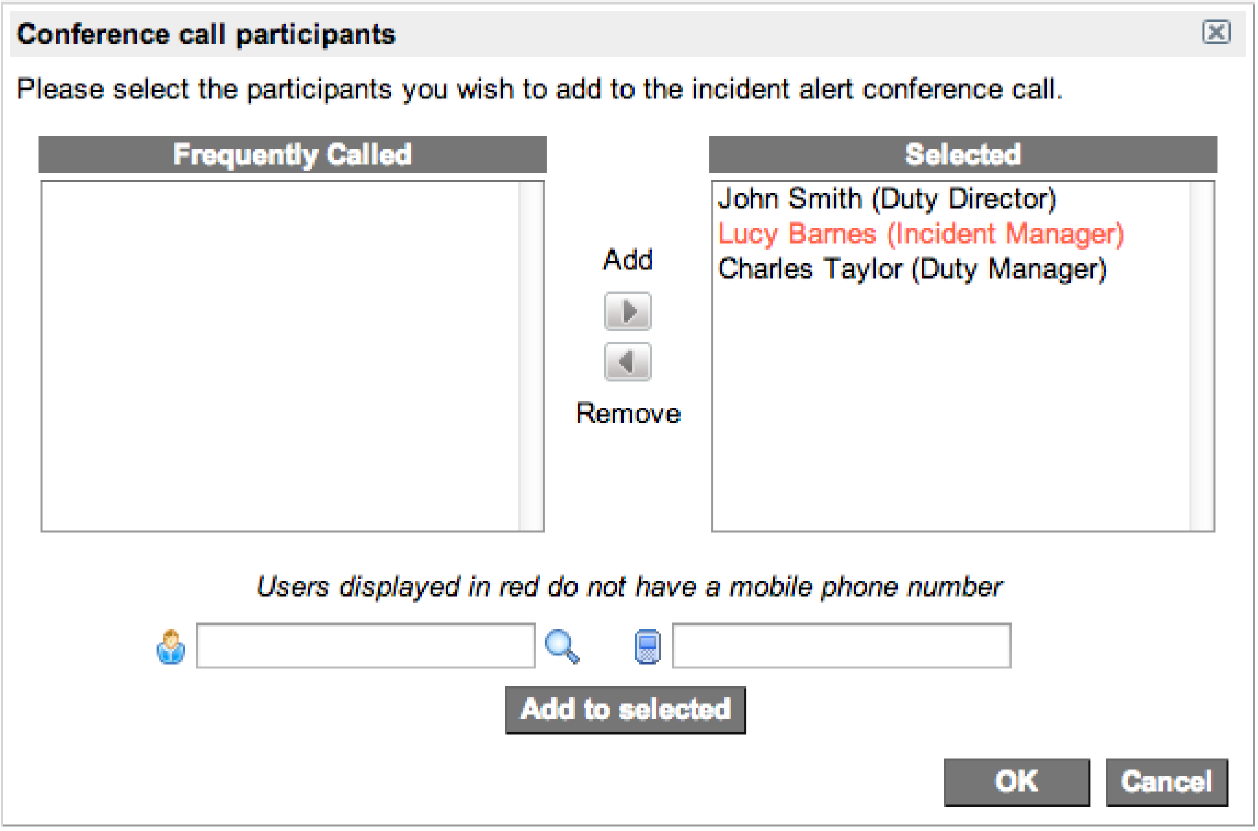
As part of processing an incident alert, a conference call can be created between involved users. Call participants can include:

- Those users who have been assigned specific responsibilities.
- Any required ad-hoc user contacts.
- Other involved parties who are not recorded as users, such as third-party contacts.

Note: *Only one conference call at a time can be active for each issue.*

To launch a conference call for an incident alert:

1. Navigate to **Incident Alert Management > Open**.
2. Open the relevant incident alert.
3. Click the **Initiate Conference Call** related link.
4. Within the dialog box that appears, select the participants for the conference.



Conference call participants

Please select the participants you wish to add to the incident alert conference call.

Selected:

John Smith (Duty Director)
Lucy Barnes (Incident Manager)
Charles Taylor (Duty Manager)

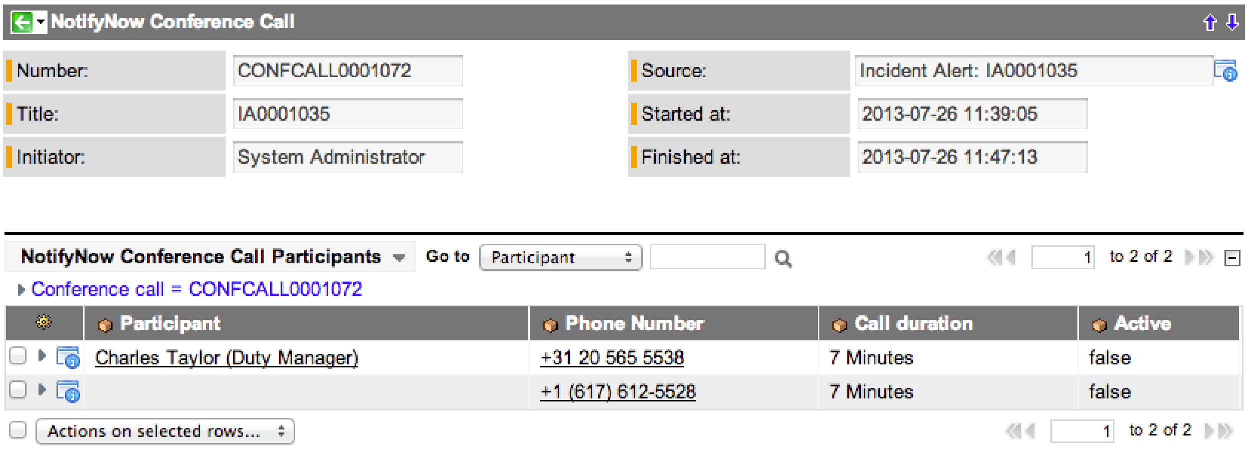
Users displayed in red do not have a mobile phone number

The dialog box displays the recommended and selected participants for the conference. All users from the **User Contacts** list in the incident alert are selected by default. If a rotation schedule exists for the **Group Contacts**, the primary and secondary on-call resources are shown in the **Recommended** list. This way, the current on-call persons can quickly be invited to join the conference call.

Calls are placed to the number in the **Mobile phone** field on the user record. If that information is blank, the user cannot be contacted through Notify. The mobile phone number has to be an E.164 [2] compliant phone number. If the phone number is a local number, without the + prefix, the number will be retrieved based on the user's location and, if possible, converted into a valid E.164 number.

5. To select ad-hoc participants, do one of the following:
   - Click the reference lookup icon, select the relevant user, and click **Add to selected**.
   - Enter the participant's phone number in the field beside the telephone icon, and click **Add to selected**.
6. After the participant list is finalized, click **OK**
7. The conference call starts and a **Conference call initiated** message is displayed at the top of the Incident Alert form. Each user is called and can accept the call to join the conference.

   Note: Several response types are possible from users invited to join the conference call, apart from **Accepted**.
8. Click the **Conference call initiated** message to see details of that conference call.



NotifyNow Conference Call

Number:	CONFCALL0001072	Source:	Incident Alert: IA0001035
Title:	IA0001035	Started at:	2013-07-26 11:39:05
Initiator:	System Administrator	Finished at:	2013-07-26 11:47:13

NotifyNow Conference Call Participants ▾ Go to Participant ⬍ 1 to 2 of 2

▸ Conference call = CONFCALL0001072

	Participant	Phone Number	Call duration	Active
□	Charles Taylor (Duty Manager)	+31 20 565 5538	7 Minutes	false
□		+1 (617) 612-5528	7 Minutes	false

□ Actions on selected rows... ⬍ 1 to 2 of 2

9. When the final participant leaves the conference, the conference call closes.

Note: *VoIP phone systems, which do not use touch tone phones, may encounter issues with recognizing key presses. To avoid problems, ensure that conference call users use touch tone phones, or configure your VoIP system settings to recognize key presses, as described in your VoIP system documentation.*

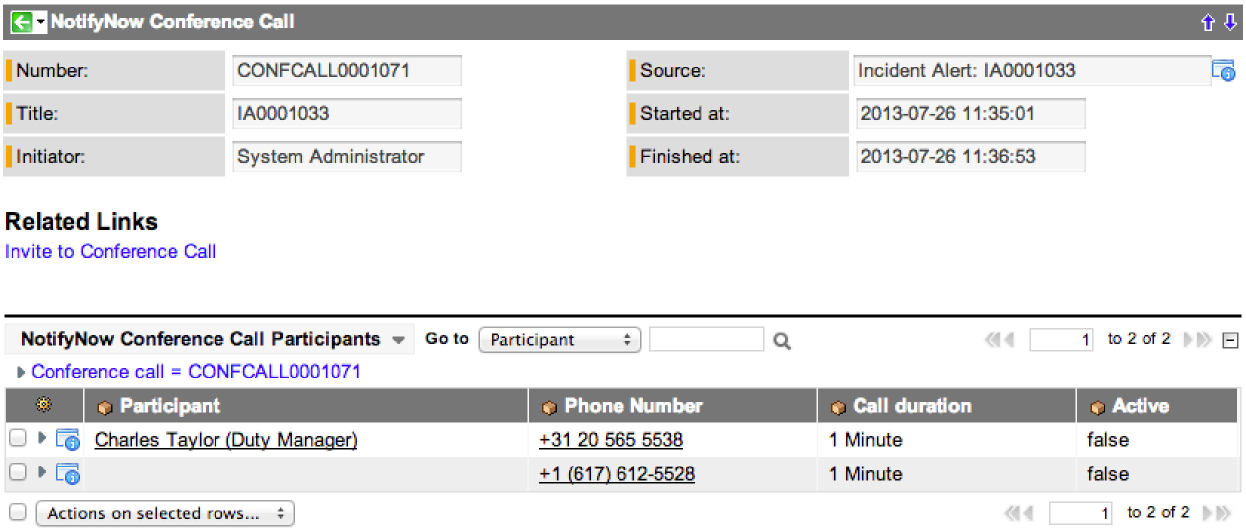
Adding Participants

If the conference participants decide that another user's input is required, that user can be invited to join the current conference call.

Participants who may have involuntarily dropped out of the conference can also contact the conference call initiator, who can add them to the conference call.

To add an ad-hoc participant to an active conference call:

1. Open the form for the relevant active conference call.
2. Click the **Invite to Conference Call** related link.



NotifyNow Conference Call

Number:	CONFCALL0001071	Source:	Incident Alert: IA0001033
Title:	IA0001033	Started at:	2013-07-26 11:35:01
Initiator:	System Administrator	Finished at:	2013-07-26 11:36:53

Related Links

Invite to Conference Call

NotifyNow Conference Call Participants ▾ Go to Participant ⬍ 1 to 2 of 2

▸ Conference call = CONFCALL0001071

	Participant	Phone Number	Call duration	Active
□	Charles Taylor (Duty Manager)	+31 20 565 5538	1 Minute	false
□		+1 (617) 612-5528	1 Minute	false

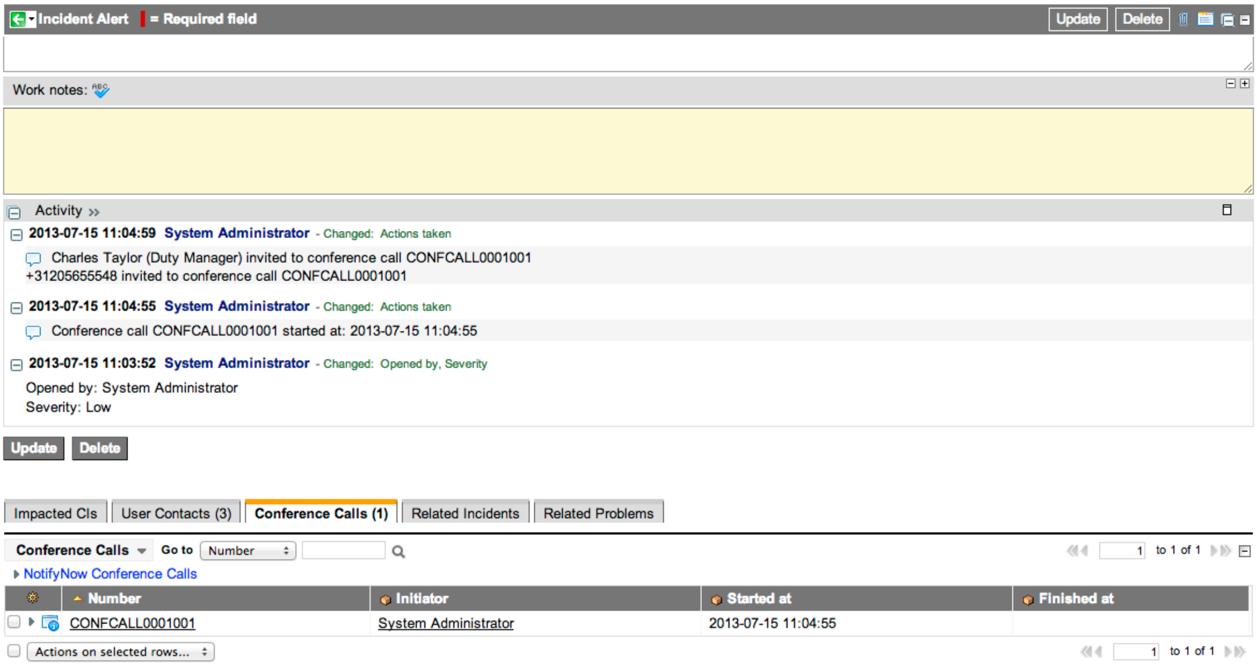
□ Actions on selected rows... ⬍ 1 to 2 of 2

3. Select participants as described for launching a conference call.
4. The selected participant is called directly and can join the conference.

Note: *if you try to add a user that is already in another call to a conference call, the message:* [Name] is already active in a call *is shown. If you try to start a new call with a user that is already in a conference call, two messages are shown, the first stating this is an invalid participant and the second that this person is already in another call.*

Viewing Conference Call Information

Conference calls are listed as system activities in the **Activity** section of the Incident Alert form and also are listed in the **Conference Calls** related list.



2013-07-15 11:04:59 System Administrator - Changed: Actions taken

Charles Taylor (Duty Manager) invited to conference call CONFCALL0001001
+31205655548 invited to conference call CONFCALL0001001

2013-07-15 11:04:55 System Administrator - Changed: Actions taken

Conference call CONFCALL0001001 started at: 2013-07-15 11:04:55

2013-07-15 11:03:52 System Administrator - Changed: Opened by, Severity

Opened by: System Administrator
Severity: Low

Number	Initiator	Started at	Finished at
CONFCALL0001001	System Administrator	2013-07-15 11:04:55	

Note: *Conference call information can also be accessed by navigating to* ***Notify > Conference Calls*** *starting with the Eureka release. In previous versions, navigate to* ***NotifyNow > Conference Calls****.*

Viewing Responses to Conference Call Invitations

When a user is invited to join a conference call, Notify may receive one of several responses. These responses can be viewed in the conference call details.

Response	Description
Accepted	The contact answered the call and accepted the invitation to join the conference.
Busy	A busy signal was received. Either the contact rejected the incoming call or the phone was in use.
Cancelled	The conference call manager canceled the outgoing call.
Completed	The call was finished or the contact hung up.
Failed	The call could not be completed as dialed, possibly because the phone number did not exist.
Ignored	The contact answered the phone, but hung up or disconnected without choosing to accept or reject the incoming call.
Rejected	The contact answered the call and rejected the invitation.
Ringing	The contact is being called.
Unanswered	Any other action, for example, missed call, or the contact took another action.

Note: *Depending on the contact's phone service provider, the information the participant receives may vary. For example, contacts who have switched off their phones may or may not receive a missed call message.*

References

[1] https://docs.servicenow.com/bundle/jakarta-servicenow-platform/page/product/notify2/concept/c_NotifyWithIncidentAlert.html

[2] http://en.wikipedia.org/wiki/E.164

Contact Administration

Note: *This article applies to Fuji. For more current information, see Contact Administration* [1] *at* http://docs.servicenow.com The ServiceNow Wiki is no longer being updated. Please refer to http://docs.servicenow.com for the latest product documentation.

Overview

Contacts allow incident alerts to be associated with users and groups based on conditions defining the reason for association: for example, the ownership of that incident alert. Multiple users and groups can be assigned as contacts.

You can assign users or groups to incident alerts automatically based on the information provided in these records:

- **Contact responsibilities:** these provide a name, such as Incident Duty Manager, for a set of tasks related to incident alerts. The contact responsibility record also indicates whether those tasks are performed by an individual user or a group of users. Contact responsibilities can also be used to manually add contacts to an incident alert.
- **Contact definitions:** identify a set of conditions to determine which specific user or group is assigned to handle particular responsibilities for an incident alert. For example, **All P1 Incidents must have an Incident manager, assigned to US Incident Management group**.

Contact responsibilities and contact definitions allow you to define and modify data-driven contact information for automatic notifications, rather than specifying individual users or groups directly for each incident alert.

You can use group contacts. **Group contacts** are available when you use on-call scheduling, notify and incident alert management. Group contacts include the people that are on-call. The group contacts do not automatically get an SMS notification when an incident alert is created. But they can be included when initiating a conference call that is the result of an incident alert. By default, the primary and secondary on-call persons are available. To modify this behavior, set the system property `com.snc.iam.on_call_escalation_level`

Responsibilities for Incident Alerts

The types of responsibility available for use with incident alerts are:

- **Default Responsibilities:** contacts who are notified by default.
- **Other Responsibilities:** contacts who can be selected for notification.

Use contact definitions to view and modify the rules that determine the specific users associated with contact responsibilities.

Default Responsibilities

By default, contacts with the following responsibilities are notified when an incident alert is created:

- Duty Manager
- Incident Manager
- Duty Director

These roles are involved with resolving the source incident or original event that the incident alert relates to, and so are seen as key contacts for the incident alert.

The following sections describe typical operational roles for these responsibilities.

Title	Description
Duty Manager	The senior point of presence in the monitoring environment at the time an incident occurs. The Duty Manager assesses the incident against standard operating procedures, escalation triggers and personal knowledge and experience, to take corrective actions. To clarify the urgency and impact of an incident, the Duty Manager can contact the Incident Manager for advice.
Incident Manager	A senior technician, accountable for coordinating and managing all technical resources required to resolve incidents. After being notified by the Duty Manager of a serious incident, the Incident Manager assesses the seriousness and associated business impact. Based on this assessment, the Incident Manager decides whether to escalate the incident to the Duty Director. The Incident Manager may escalate to the Duty Director to gain access to resources outside of the department, if necessary.
Duty Director	The escalation point for all issues that affect critical services The Duty Director works in partnership with the business directors in the organization to approve recovery plans developed by the Incident Manager, and to manage the senior level communications for the source incident.

Other Responsibilities

Incident alert management provides the following additional responsibilities that can be added to incident alerts. You can also create contact responsibilities, as needed. The associated users receive notifications about the alert.

Title	Description
Business Director	Director within the business who is identified as a potential contact in the the event of an incident alert.
Communication Manager	Business-facing role in the event communication is required in an incident alert.
Crisis Action Manager	Overall responsibility and accountability for managing incident alerts.
Crisis Action Team Member	Nominated department heads who are involved when an incident alert occurs.
Development	Development personnel involved in the troubleshooting and resolving an incident alert.
Operations	Second or third level operations support involved in troubleshooting and resolving an incident alert.
Service Owner	Service owner or manager who is identified as a potential contact in the the event of an incident alert that relates to one or more of their services.
Technical Support	Second or third level technical support personnel involved in troubleshooting and resolving an incident alert.

References

[1] https://docs.servicenow.com/bundle/jakarta-it-service-management/page/product/incident-alert-management/reference/r_ContactAdministration.html

Using Contacts with Incident Alerts

Overview

Incident alert management uses contacts for notification purposes. Administrators and incident alert administrators can:

- Create and edit contact responsibilities.
- Create and edit contact definitions to automatically assign contacts to alerts.
- Add contacts manually to an incident alert.

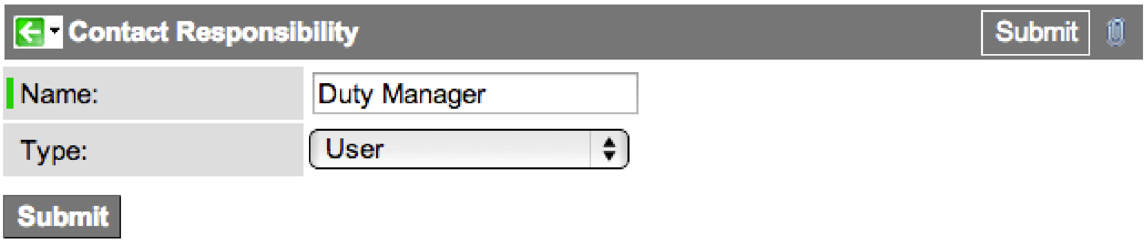
Creating Contact Responsibilities

Contact responsibilities allow contacts to be used in specific alerts. They can be used:

- Within a contact definition, as part of the rules for assigning users or groups as contacts for incident alerts.
- On an ad-hoc basis, to be added within specific incident alerts.

To create a contact responsibility:

1. Navigate to **Incident Alert Management > Contact Administration > Contact Responsibilities**
2. Click **New**.



Name: Duty Manager

Type: User

3. Fill in the fields (see table).
4. Click **Submit**.

Field	Description
Name	The responsibility name.
Type	**User** or **Group** to indicate whether the responsibility appears in the **User Contacts** or **Group Contacts** related list of the Incident Alert form.

Creating Contact Definitions

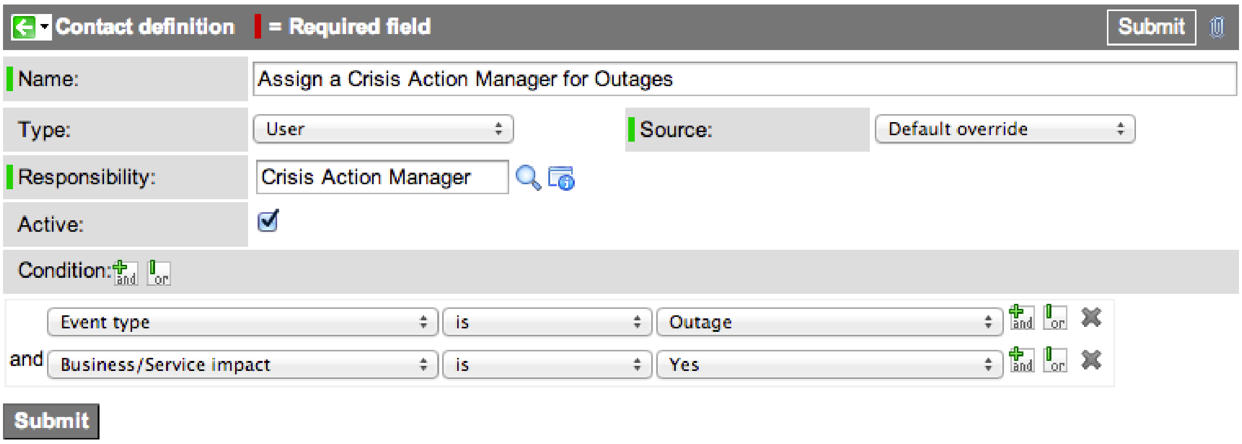
Contact definitions specify:

- The conditions for assigning the associated contact responsibility record to incident alerts.
- The conditions for assigning specific users or groups to those responsibilities.

For example, a contact definition may be **Assign a Crisis Action Manager for Outages** with an additional condition of **Business/Service impact** is **True**.

To create a contact definition:

1. Navigate to **Incident Alert Management > Contact Administration > Contact Definitions**.
2. Click **New**.



Contact definition = Required field Submit

Name:	Assign a Crisis Action Manager for Outages		
Type:	User	Source:	Default override
Responsibility:	Crisis Action Manager		
Active:	☑		
Condition:			

	Event type	is	Outage
and	Business/Service impact	is	Yes

Submit

3. Fill in the fields (see table).
4. Click **Submit**.

Field	Description
Name	The name that indicates the conditions defined for this contact definition.
Type	The type of contacts this definition can be associated with. Can be **User** or **Group**.
Source	The method to determine the user or group to associate with this definition. Can be set to: • **None:** Use no association. The incident alert administrator should associate users or groups manually, editing that responsibility entry within the Incident Alert form. • **Default Override:** Use a default override to associate users or groups based on conditions. • **Form Field:** Use information used from a specified field on the incident alert, as defined by the **Source field** value.
Source field	The field on the Incident Alert form that identifies the contact associated with the selected contact responsibility. Appears only when **Form field** is selected as the value for **Source**. • For user contact types, values can be **Assigned to**, **Closed by**, **Opened by**, or **Resolved by**. • For group contact types, the value is **Assignment group**.
Responsibility	The contact responsibility associated with this definition.
Quantity	The maximum number of contacts that can be associated with the selected **Responsibility** per incident alert record. This field appears only when **None** is selected as the value for **Source**.
Active	A check box to indicate whether the definition is active or not.
Condition	The conditions that must be met to associate this contact definition to a particular user or group. For example, **]Affected users] + [is] + [0-25]**. If multiple conditions are defined, each condition is evaluated in the order listed.

Creating a Default Override

Default overrides specify the user value for each contact the definition adds to an incident alert. The **Default overrides** related list is available if the **Source** for the contact definition is set to **Default override**.

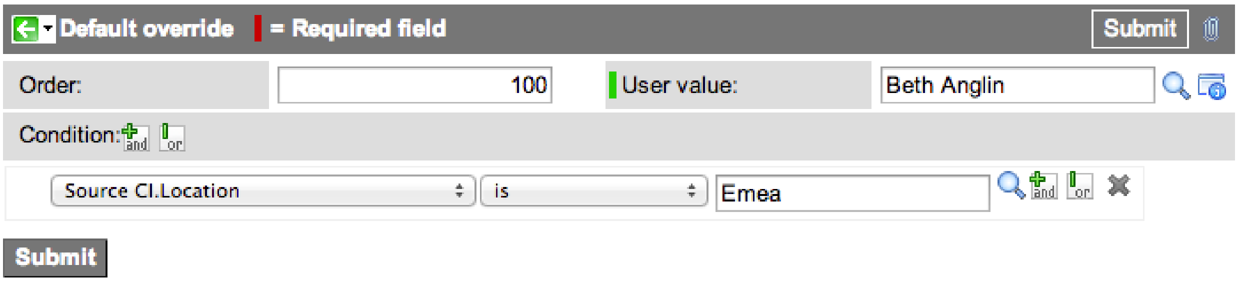
For example, you could define two default overrides for a contact definition:

- **If Source CI's location is EMEA then user is Beth Anglin**, with an evaluation order of 100.
- **If Source CI's location is APAC then user is Abel Tuter**, with an evaluation order of 200.

If an incident alert is created that matches the conditions of the contact definition, ServiceNow then compares the alert's source CI to these override conditions and assigns the appropriate user as the contact.

To create a new default override:

1. Click **New** in the **Default overrides** related list.
2. Fill in the fields, as appropriate (see table).
3. Click **Submit**.



Order: 100

User value: Beth Anglin

Condition:

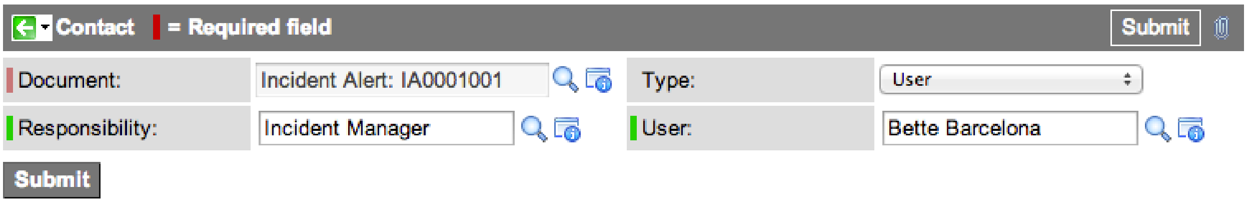
Source CI.Location | is | Emea

Field	Description
Order	The order in which the condition is to be evaluated.
User value	The user to assign as that contact if the condition matches. If the definition type is set to **Group**, this field is labelled **Group value** and defines the group to assign as that contact.
Condition	The conditions defining whether the default override is to be applied. If multiple conditions are defined, each condition is evaluated in the order listed. If no conditions match, this default override is not applied.

Adding Contacts Manually

Contact entries can be added to an incident alert manually, within an incident alert:

1. Open the incident alert record.
2. Select the **User Contacts** related list.
3. Do one of the following:
   - Click **New** to create a new ad-hoc entry.
   - Select an entry created by a contact definition which has the **Source** field set to **None**.



Document: Incident Alert: IA0001001

Type: User

Responsibility: Incident Manager

User: Bette Barcelona

4. Select a **Responsibility** and the **User** to have this responsibility for this incident alert. That contact information is now listed in the incident alert's **User Contacts** related list.

Note: *If you delete an incident alert, all contacts associated with that incident alert are also deleted.*

Subscribing to Incident Alerts

Overview

Any self-service user can subscribe to incident alerts, to be notified when:

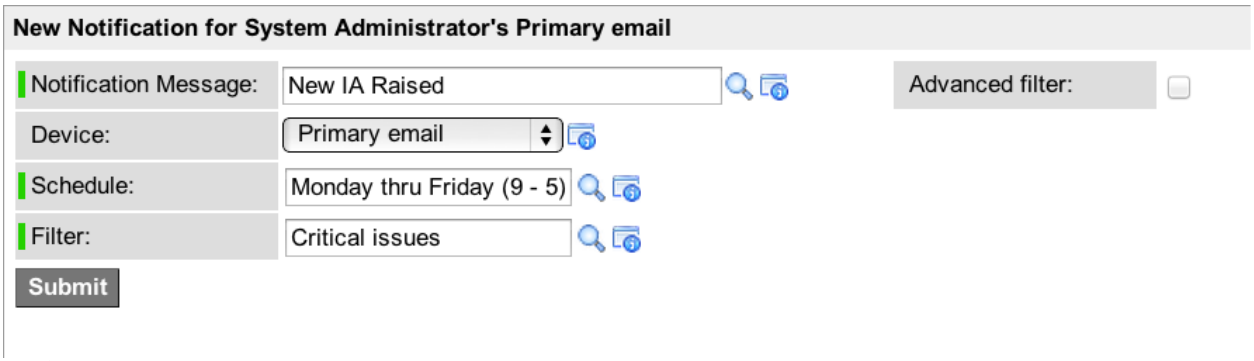
- A new incident alert is created.
- An incident alert is resolved or closed.
- An incident alert is canceled.
- The **Actions Taken** field on an incident alert is updated.

Notifications are sent by email. If Notify is active, notifications can also be sent by SMS message or voicemail.

For example, a business manager does not log in to the system on daily basis, but needs to know when a new incident alert is created. The business manager can subscribe to receive notifications whenever a new incident alert is raised.

Subscribing to Notifications

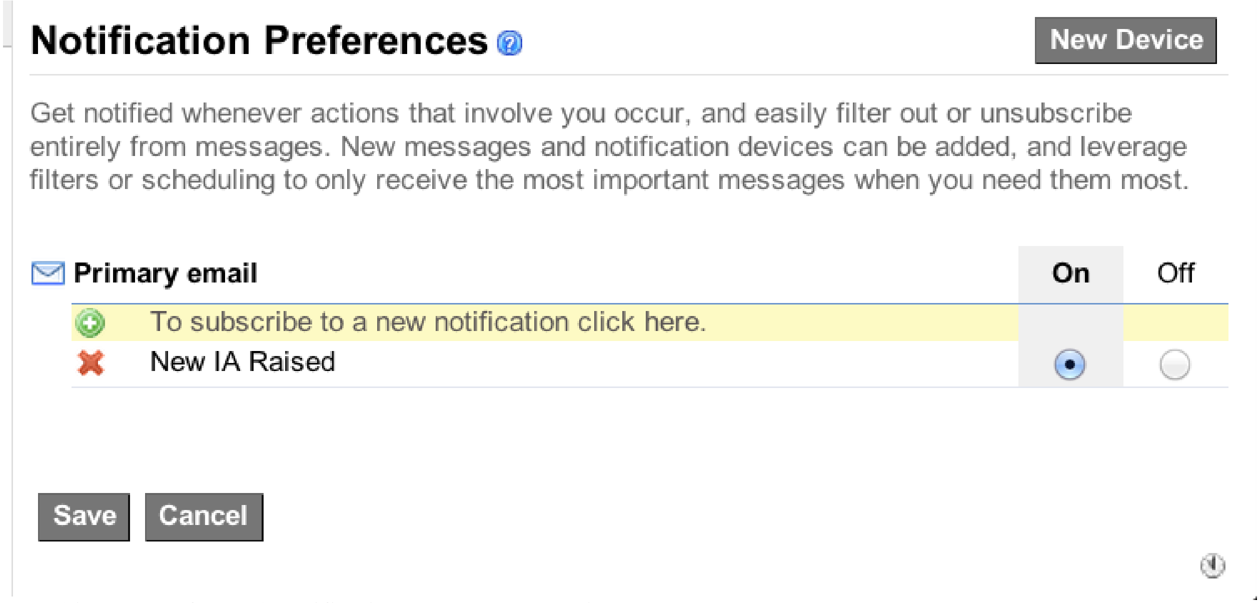
1. Navigate to **Self-Service > My Profile**.
2. Select **Notification Preferences** under **Related Links**.
3. Under the device to receive notifications, click in the area labeled **To subscribe to a new notification click here.**
4. Click the lookup icon beside **Notification Message** to display a list of available notifications.
5. Select one of the following notifications:
   - New IA Raised
   - IA Actions Taken
   - IA Resolved Or Closed
   - IA Cancelled
6. Fill in the details for the selected notification.



New Notification for System Administrator's Primary email

Notification Message:	New IA Raised	Advanced filter:	☐
Device:	Primary email		
Schedule:	Monday thru Friday (9 - 5)		
Filter:	Critical issues		

7. Click **Submit**.
8. The notification is then listed in the **Notification Preferences** list.



Notification Preferences

Get notified whenever actions that involve you occur, and easily filter out or unsubscribe entirely from messages. New messages and notification devices can be added, and leverage filters or scheduling to only receive the most important messages when you need them most.

Primary email	On	Off
To subscribe to a new notification click here.		
New IA Raised	●	○

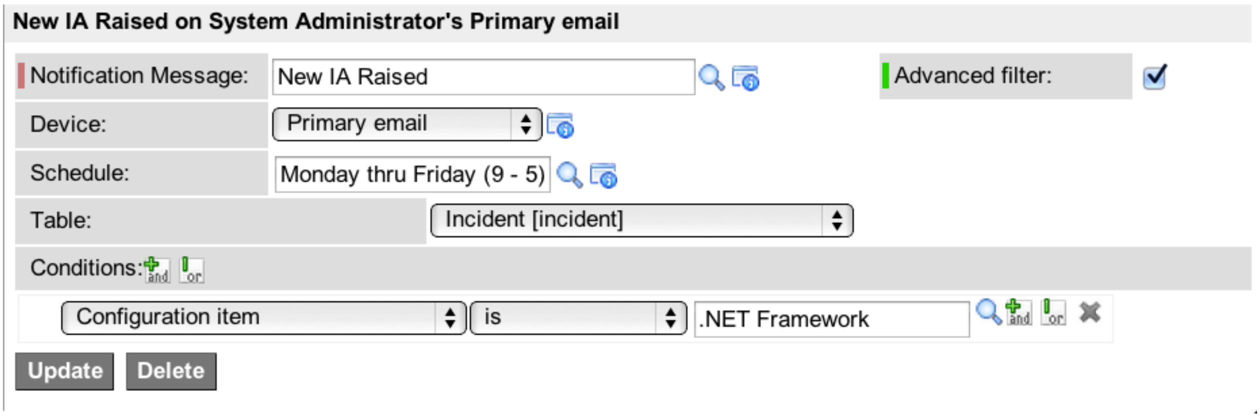
9. Repeat this process for each notification you want to receive.

Filtering Notifications

If no filtering is applied to a subscription, then a subscribed user receives all notifications for that subscription. For example, a user subscribed to **New IA Raised**, with no filtering, receives notifications every time any incident alert is created.

To make the notifications more relevant, select **Advanced filter**, then use the condition builder to create an appropriate filter.

For example, you can choose to be notified only when an incident alert is created for a specific CI.



New IA Raised on System Administrator's Primary email

Notification Message: New IA Raised

Advanced filter: ☑

Device: Primary email

Schedule: Monday thru Friday (9 - 5)

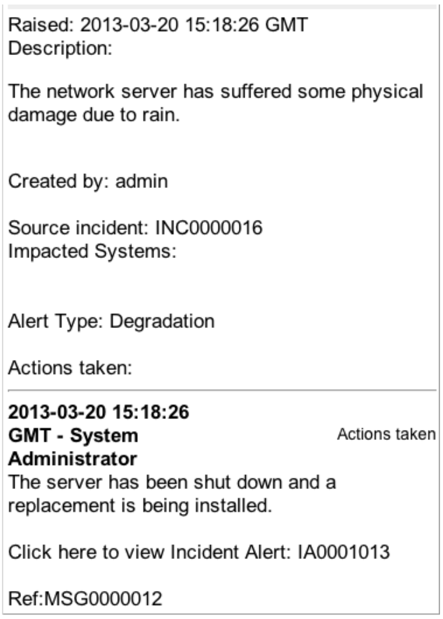
Table: Incident [incident]

Conditions:

Configuration item | is | .NET Framework

Notification Message Content

When a relevant notification event happens, a notification message is generated and sent to all subscribed users. This message will give the notification type, the alert number, and details of the event.



Raised: 2013-03-20 15:18:26 GMT
Description:

The network server has suffered some physical damage due to rain.

Created by: admin

Source incident: INC0000016
Impacted Systems:

Alert Type: Degradation

Actions taken:

2013-03-20 15:18:26 GMT - System Administrator Actions taken
The server has been shut down and a replacement is being installed.

Click here to view Incident Alert: IA0001013

Ref:MSG0000012

Article Sources and Contributors

Incident Alert Management *Source*: http://wiki.servicenow.com/index.php?oldid=250637 *Contributors*: David.Bailey, John.ramos, Ludwig.adriaansen, Maneesha.Nanda, Rachel.sienko

Installed with Incident Alert Management *Source*: http://wiki.servicenow.com/index.php?oldid=226064 *Contributors*: David.Bailey, Ludwig.adriaansen

Creating Incident Alerts *Source*: http://wiki.servicenow.com/index.php?oldid=190925 *Contributors*: David.Bailey, Ludwig.adriaansen

Processing Incident Alerts *Source*: http://wiki.servicenow.com/index.php?oldid=190937 *Contributors*: David.Bailey

Using Notify with Incident Alert Management *Source*: http://wiki.servicenow.com/index.php?oldid=251002 *Contributors*: Cheryl.dolan, David.Bailey, John.ramos, Joseph.messerschmidt, Ludwig.adriaansen

Contact Administration *Source*: http://wiki.servicenow.com/index.php?oldid=250186 *Contributors*: David.Bailey, John.ramos, Ludwig.adriaansen

Using Contacts with Incident Alerts *Source*: http://wiki.servicenow.com/index.php?oldid=189415 *Contributors*: David.Bailey

Subscribing to Incident Alerts *Source*: http://wiki.servicenow.com/index.php?oldid=189417 *Contributors*: David.Bailey

Image Sources, Licenses and Contributors

Image:Warning.gif *Source*: http://wiki.servicenow.com/index.php?title=File:Warning.gif *License*: unknown *Contributors*: CapaJC

Image:Incident_Alert_State.png *Source*: http://wiki.servicenow.com/index.php?title=File:Incident_Alert_State.png *License*: unknown *Contributors*: David.Bailey

File:IAM_application.png *Source*: http://wiki.servicenow.com/index.php?title=File:IAM_application.png *License*: unknown *Contributors*: David.Bailey, Georgi.ivanov

Image:New Incident Alert.png *Source*: http://wiki.servicenow.com/index.php?title=File:New_Incident_Alert.png *License*: unknown *Contributors*: David.Bailey

Image:Incident_Alert_Impacted_CIs.png *Source*: http://wiki.servicenow.com/index.php?title=File:Incident_Alert_Impacted_CIs.png *License*: unknown *Contributors*: Bushra.akhtar, David.Bailey

Image:Incident_Alert_Contacts.png *Source*: http://wiki.servicenow.com/index.php?title=File:Incident_Alert_Contacts.png *License*: unknown *Contributors*: David.Bailey

Image:Incident_Alert_Related_Problems.png *Source*: http://wiki.servicenow.com/index.php?title=File:Incident_Alert_Related_Problems.png *License*: unknown *Contributors*: David.Bailey

Image:Post_Incident_Review.png *Source*: http://wiki.servicenow.com/index.php?title=File:Post_Incident_Review.png *License*: unknown *Contributors*: David.Bailey

Image:Incident_Alert_Closed.png *Source*: http://wiki.servicenow.com/index.php?title=File:Incident_Alert_Closed.png *License*: unknown *Contributors*: David.Bailey

file:Icon-home.png *Source*: http://wiki.servicenow.com/index.php?title=File:Icon-home.png *License*: unknown *Contributors*: Guy.yedwab

Image:Incident_Alert_Dashboard.png *Source*: http://wiki.servicenow.com/index.php?title=File:Incident_Alert_Dashboard.png *License*: unknown *Contributors*: Aat.rutten, David.Bailey

Image:IA_report_resolved.png *Source*: http://wiki.servicenow.com/index.php?title=File:IA_report_resolved.png *License*: unknown *Contributors*: David.Bailey

Image:NotifyNow-Bridge.png *Source*: http://wiki.servicenow.com/index.php?title=File:NotifyNow-Bridge.png *License*: unknown *Contributors*: David.Bailey, Georgi.ivanov, Paul.palse

Image:NotifyNow-Bridge-Details.png *Source*: http://wiki.servicenow.com/index.php?title=File:NotifyNow-Bridge-Details.png *License*: unknown *Contributors*: David.Bailey, Georgi.ivanov

Image:Invite_to_Bridge.png *Source*: http://wiki.servicenow.com/index.php?title=File:Invite_to_Bridge.png *License*: unknown *Contributors*: David.Bailey, Georgi.ivanov

Image:Conference-Bridge-History.png *Source*: http://wiki.servicenow.com/index.php?title=File:Conference-Bridge-History.png *License*: unknown *Contributors*: Aat.rutten, David.Bailey

Image:New_Contact_Responsibility.png *Source*: http://wiki.servicenow.com/index.php?title=File:New_Contact_Responsibility.png *License*: unknown *Contributors*: Bushra.akhtar, David.Bailey

Image:Create_Contact_Definition.png *Source*: http://wiki.servicenow.com/index.php?title=File:Create_Contact_Definition.png *License*: unknown *Contributors*: David.Bailey

Image:New_Default_Override.png *Source*: http://wiki.servicenow.com/index.php?title=File:New_Default_Override.png *License*: unknown *Contributors*: David.Bailey

Image:New_Contact_Ad_hoc.png *Source*: http://wiki.servicenow.com/index.php?title=File:New_Contact_Ad_hoc.png *License*: unknown *Contributors*: David.Bailey

Image:New_IA_Raised_Notification.png *Source*: http://wiki.servicenow.com/index.php?title=File:New_IA_Raised_Notification.png *License*: unknown *Contributors*: David.Bailey

Image:Notification_preferences_New_IA.png *Source*: http://wiki.servicenow.com/index.php?title=File:Notification_preferences_New_IA.png *License*: unknown *Contributors*: David.Bailey

Image: New_IA_Raised_Filter.png *Source*: http://wiki.servicenow.com/index.php?title=File:New_IA_Raised_Filter.png *License*: unknown *Contributors*: David.Bailey

Image:IA_notification_Message.png *Source*: http://wiki.servicenow.com/index.php?title=File:IA_notification_Message.png *License*: unknown *Contributors*: David.Bailey