

ITIL Incident Implementation

Applying ITIL Principles to ServiceNow

ITIL Incident Management

ITIL Incident Management



Note: This article applies to Fuji and earlier releases. For more current information, see Incident 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 **The ServiceNow wiki is no longer being updated.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

The goal of incident management is to restore normal service operation as quickly as possible following an incident, while minimizing impact to business operations and ensuring quality is maintained.

The ServiceNow platform supports the incident management process with the ability to log incidents, classify according to impact and urgency, assign to appropriate groups, escalate, and manage through to resolution and reporting. Any ESS user can log in to ServiceNow to record the incident and track it through the entire incident life cycle until service has been restored and the issue has been completely resolved.

Within the platform, incidents are handled with the task record system. Each incident is generated through a variety of methods as a task record, and populated with the pertinent information in individual fields. These tasks can be assigned to appropriate service desk members, who will deal with the task as appropriate. Once the incident has been properly dealt with, it is closed.

ServiceNow also supports many integrations with outside software. To find out more, visit the integration portal.



Note: The incident alert management application allows you to manage communications around high-priority incidents, and is available starting with the Dublin release.

Incident Management Process

The platform provides a number of tools to enable a service desk to implement the incident management process effectively.

Identifying Incidents

In addition to having users log incidents, it is possible to automatically generate incidents from pre-established conditions. Business rules use JavaScript to generate an incident after a certain series of conditions has been met. It is also possible to generate incidents from outside the platform with SOAP messaging.

Logging Incidents

By default, any user can create an incident within the system. There are a number of ways to do this provided in the base system:

- **Employee Self Service:** ITIL users or administrators can use the **Create New** module in the Incident application, or select **New** from the Incident list. The **Watch list**, **Incident state**, and **Impact** fields are available on the ESS view of the Incident form and the variable formatter is not available. ESS users have write access to the **Watch list** and **Impact** fields.
- **Record Producers:** Using the Create a New Incident record producer in the service catalog. (Note that this record producer sets the **Contact Type** field of the resulting incident to **Self-Service**.)
- **Inbound Email Actions:** An email addressed to the instance mailbox can create an incident according to inbound email actions.

Categorizing Incidents

Incident forms have fields for category and subcategory, which allow for easy classification of incidents. These categories can be used by the system to create automatic assignment rules or notifications. For instance, with a certain assignment rule, an incident with a category of **Database** could automatically be assigned to a Database group that always handles database issues.

Another important category for incidents is the incident state. This allows the service desk to track how much work has been done and what the next step in the process might be.

For more information, see Categorizing Incidents.

Prioritization of Incidents

ITIL uses three metrics for determining the order in which incidents are processed. All three are supported by Incident forms:

- **Impact:** The effect an incident has on business.
- **Urgency:** The extent to which the incident's resolution can bear delay.
- **Priority:** How quickly the service desk should address the incident.

ITIL suggests that priority be made dependent on impact and urgency. In the base system, this is true on Incident forms. Priority is generated from urgency and impact according to the following data lookup rules:

Impact	Urgency	Priority
1 - High	1 - High	1 - Critical
1 - High	2 - Medium	2 - High
1 - High	3 - Low	3 - Moderate
2 - Medium	1 - High	2 - High
2 - Medium	2 - Medium	3 - Moderate
2 - Medium	3 - Low	4 - Low
3 - Low	1 - High	3 - Moderate
3 - Low	2 - Medium	4 - Low
3 - Low	3 - Low	5 - Planning

By default, the **Priority** field is read-only and must be set by selecting **Impact** and **Urgency** values. To change how priority is calculated, administrators can either alter the priority lookup rules or disable the **Priority is managed by Data Lookup - set as read-only** UI policy and create their own business logic.

Initial Diagnosis of Incidents

Initial diagnosis of incidents is largely a human process, wherein the service desk looks at the information within the incident and communicates with the user to diagnose the problem in the incident.

To aid in the process, the service desk can consult the configuration management database, which contains information on hardware and software within a network and the relationships between them. CMDB can be populated in two ways: Discovery and Help the Help Desk. Discovery is available as a separate product, but Help the Help Desk is available with the base system.

Escalation of Incidents

The platform has a built-in system of escalation rules which can ensure that incidents are handled speedily. Two escalators are available in the system:

- **Service Level Agreements:** SLAs monitor the progress of the incident according to defined rules. As time passes, the SLA will dial up the priority of the incident, and leave a marker as to its progress. SLAs can also be used as a performance indicator for the service desk.
- **Inactivity Monitors:** The inactivity monitors prevent incidents from slipping through the cracks by generating an event, which in turn can create an email notification or trigger a script, when an incident has gone a certain amount of time without being updated.

Investigation and Diagnosis of Incidents

Like the initial diagnosis and investigation, investigation and diagnosis are largely human processes. The service desk can continue to use the information provided within by the Incident form and the CMDB to solve the problem. Work notes can be appended to the incident as it is being evaluated, which facilitates communication between all of the concerned parties. These work notes and other updates can be communicated to the concerned parties through email notifications.

Resolution and Recovery of Incidents

After the incident is considered resolved, the incident state should be set to **Resolved** by the service desk. The escalators will be stopped and the service desk may review the information within the incident. After a sufficient period of time has passed, assuming that the user who opened the incident is satisfied, the incident state may be set to closed.

If an incident's cause is understood but cannot be fixed, the service desk can easily generate a problem from the incident, which will be evaluated through the problem management process. If the incident creates the need for a change in IT services, the service desk can easily generate a change from the incident, which will be evaluated through the change management process.

In addition to the base system incident management workflow, a Best Practice - Incident Resolution Workflow Plugin is available to bring the incident management workflow into better alignment with ITIL v3.

Closure of Incidents

Closed incidents will be filtered out of view, but will remain in the system for reference purposes. Closed incidents can be reopened if the user or service desk believes that it needs to be reopened.

Incidents that are on the **Related Incidents** list of a problem can be configured to close automatically when the problem is closed through business rules.

If the knowledge check box is selected, a business rule is triggered by closing the incident, and a knowledge article is generated with the information from the incident. This is useful for knowledge management, and knowledge-centered support, reducing the number of repeat incidents by distributing the information related to the incident.

It is also possible to generate customer satisfaction surveys upon closure of incidents. This allows the service desk to gather information about their quality of service directly from the user.

Continual Service Improvements to Incident Management

The service desk can improve the incident management process using information gathered within the platform. Much of the data is already stored within the incident record. More information can be gathered by enabling auditing, which allows for an accurate review of the history of the problem.

The following plugins allow you to gather additional incident information:

- **Metric Definition:** Define the key performance indicators to monitor within the system. With these metrics, and the information within the database, it is possible to generate reports that can then be added to homepages or automatically generated and distributed.
- **Database Views:** Join tables for reporting purposes.
- **Vendor Ticketing:** Add vendor data to incidents and integrate with Vendor Performance (starting with the Dublin release).

Using this information, it is possible to refine automatic rules such as the assignment rules, service level agreements, or inactivity monitors to better suit the service desk's unique environment.

Unnecessary incidents can be avoided by encouraging users to consult the knowledge base before creating an incident. For more information, see Knowledge Management with KCS.

References

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

Logging Incidents

Creating a Template



Note: This article applies to Fuji. For more current information, see *Create an Incident Template* ^[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.

	Functionality described here requires the Admin role.
--	--

Overview

Templates store populated versions of form for reuse, and can help save time by reducing the amount of time spent filling in forms. By defining common incidents as templates, an administrator can save time for service desk members later, allowing them to focus on solving the incidents at hand.

Once a template is defined, it can be used on a form, from a record producer, from a module, or in a script.

The example below creates a template for users who can't access the bond trading service.

Creating an Incident Template

To create an incident template:

1. Navigate to **System Definition > Templates** and click **New**.
2. Populate the form as follows:
 - **Name** - Bond Trading Access Denied
 - **Table** - Incident
 - **Global** - True. This allows any user to deploy the template, rather than simply the template's creator.
 - **Short Description** - Bond Trading Access Denied
 - **Template** - Category is Inquiry / Help, Configuration Item is Bond Trading, Description is The user was denied access to the Bond Trading application, Impact is 2 - Medium, and Urgency is 3 - Low. This defines the fields that will be filled in by the template.
3. Click **Submit**.

Using a Template from a Form

To use a template from a form, right click the form header bar, and select **Template > Apply Template**

Using the Template from a Record Producer

To use a template with a record producer, see [Creating a Record Producer](#).

Using the Template from a Module

The following example demonstrates how to place the Bond Trade Access Denied template in a module in the **Self-Service** application, allowing end-users to directly file the incident with the template.

To use a template from a Module:

1. Right click the Application **Self-Service** and click **Edit Application**.
2. Scroll to the **Modules** related list and click **New**.
3. Populate the form as follows:
 - **Title** - Bond Trading Access Denied

- **Table** - Incident [incident]
- **Order** - 473. This order places the new module after **Requested Items** in the **Self-Service** application. Order can be found when looking at the Module related list on the Application form.
- **Link Type** - New Record
- **Hint** - File an incident about the Bond Trade application.
- **Image** - /images/newpage.gif
- **Arguments** - incident.do?sys_id=-1&sysparm_template=Bond Trading Access Denied . This deploys the template in the new incident record.

4. Submit.

Module | Required field | Update | Delete | [Icons]

Title: Bond Trading Access D | Link type: New Record

Table: Incident [incident] | View name:

Order: 473 | Roles:

Application: itil_self_service | [Icons]

Hint: File an Incident about the Bond Trade ap

Active: ☒

Image: [Icon]

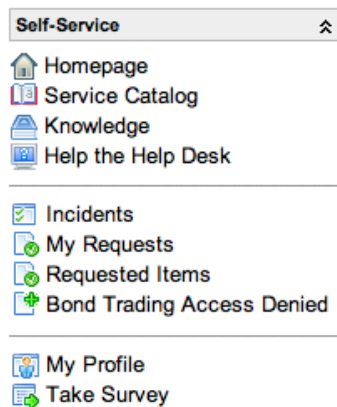
Filter: [Icons]

-- choose field -- | -- oper -- | -- value --

Arguments: incident.do?sys_id=-1&sysparm_template=Bond Trading Access Denied

Update | Delete

The new Module should appear in the **Self-Service** application:



Using the Template in a Script

For information on using the template in a script, see [Applying a Template in a Script](#).

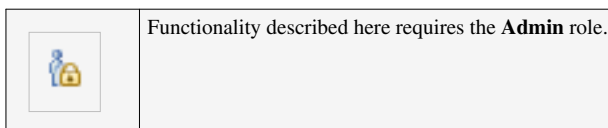
References

[1] https://docs.servicenow.com/bundle/jakarta-it-service-management/page/product/incident-management/task/t_CreateAnIncidentTemplate.html#t_CreateAnIncidentTemplate

Creating a Record Producer



Note: This article applies to Fuji. For more current information, see [Create a Record Producer to Log Incidents](#)^[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.



Functionality described here requires the **Admin** role.

Overview

The Service Catalog provides front-end for service requests, but it can also be used as a front-end for incident management. An administrator can set up record producers that create records on the incident table, allowing the end-user to log incidents directly from the Service Catalog. This can be useful in giving end-users one front-end from which they can make all of their requests to their IT Department.

An out-of-box example of this is the Service Catalog category **Can We Help You?** which features record producers such as **Report an Incident** to allow end-users to directly log incidents from the catalog homepage.

Creating a Record Producer

The first step in using the Service Catalog as a front end is to create a record producer. Record producers appear in the Service Catalog like catalog items, but instead of creating a service request, they create a record on any record in the system, populating the record as defined in the record producer.

This example will show how to create a record producer to request a wireless router reset.

To define a record producer:

1. Navigate to **Service Catalog > Record Producers**.
2. Click **New**.
3. Populate the form as follows:
 - **Name** - Request to Reset Router.
 - **Table Name** - Incident [incident].
 - **Category** - Can We Help You?

Record Producer [Update] [Delete]

Name: Request to Reset Router Category: Can We Help You?

Order: 0 Active: ☒

Table name: Incident [incident] Preview Link: [Preview Item](#)

Template: [add] Click to add...

View: [add] Click to add...

Roles: [add] Click to add...

Short description: Reset Router Request

Description: Please reset the building's router.

Format: Arial 1 (8 pt) Heading 1 [B] [I] [U] [List] [Link] [Image] [Table] [Code]

4. Right click the form and select **Save**. The related lists **Variables** and **Variable Sets** will now appear at the end of the form.
5. Scroll down to the **Variables** related list and click **New**.
6. Populate the **New Variable** form as follows:
 - **Type** - Reference.
 - **Name** - Router.
 - **Reference** - IP Router [cmdb_ci_ip_router]
 - **Question:** - Which router needs to be reset?

Variable [Update] [Copy] [Delete]

Type: Reference Mandatory: ☐

Name: Router Global: ☐

Order: [add] Click to add...

Cat item: Request to Reset Router Visible on Bundles: ☒

Reference: IP Router [cmdb_ci_ip_router] Visible on Guides: ☒

Reference qual: [add] Click to add...

Visible Elsewhere: ☒

Visible on Summaries: ☒

Pricing implications: ☐

Question: Which router needs to be reset?

Show help: ☐

Default value: [add] Click to add...

7. Click **Update**.

To see how the new record producer appears to the end user, click the **Preview Item** link:

Catalog Item - Request to Reset Router

Reset Router Request

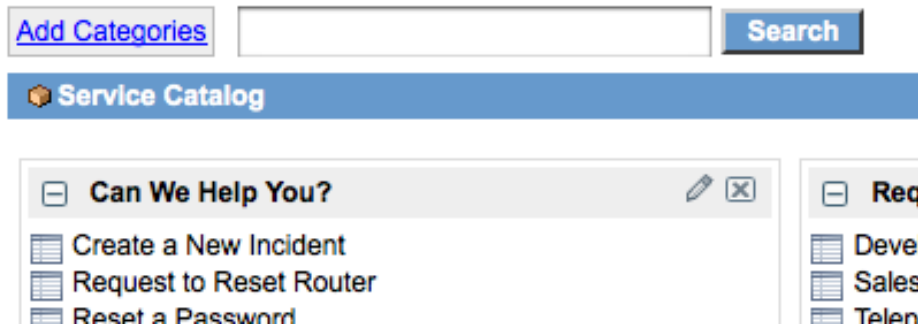
Please reset the building's router.

Which router needs to be reset?

[Input field with search icon]

Submit

Now, when a user would like to request that IT reset a router, they can navigate to the Service Catalog and select the **Request to Reset Router** link:



Creating a Record Producer with a Template

If a pre-defined template for an incident exists, it can be used with the record producer to fill in standard information for the Record Producer. The following example uses the sample template used in Creating an Incident Template.

To define a record producer with a template:

1. Navigate to **Service Catalog > Record Producers**.
2. Click **New**.
3. Populate the form as follows:
 - **Name** - Bond Trade Access Request.
 - **Table Name** - Incident [incident].
 - **Template** - Bond Trade Access Denied
 - **Category** - Can We Help You?

4. Right click the form and select **Save**. The related lists **Variables** and **Variable Sets** will now appear at the end of the form.
5. Scroll down to the **Variables** related list and click **New**.
6. Populate the **New Variable** form as follows:
 - **Type** - Multi-Line Text.
 - **Name** - Comments.
 - **Question:** - Comments

7. Submit.

The screenshot shows a 'Variable' configuration form. At the top, there is a blue header bar with a back arrow, the title 'Variable', and three buttons: 'Update', 'Copy', and 'Delete'. Below the header, the form is divided into two columns. The left column contains fields for 'Type' (set to 'Multi Line Text'), 'Name' (set to 'Comments'), 'Order' (empty), and 'Cat item' (set to 'Bond Trade Access Request' with a search icon). The right column contains a series of checkboxes: 'Mandatory' (unchecked), 'Global' (unchecked), 'Visible on Bundles' (checked), 'Visible on Guides' (checked), 'Visible Elsewhere' (checked), and 'Visible on Summaries' (checked). Below these columns, there is a 'Question' field (set to 'Comments'), a 'Show help' checkbox (unchecked), and a 'Default value' field (empty). At the bottom of the form, there are three buttons: 'Update', 'Copy', and 'Delete'.

8. Click **Update**.

The record producer will appear to the end user as such:

The screenshot shows the 'Catalog Item - Bond Trade Access Request' form. At the top, there is a blue header bar with a back arrow, the title 'Catalog Item - Bond Trade Access Request', and a search icon. Below the header, the form has a title 'Bond Trade Access Request' followed by a description: 'This request is for users who have been cleared for access to the Bond Trade application, but cannot log in. If you see a "403 - Access Denied Error" and feel that this was an error, please fill in this request.' Below the description, there is a 'Comments' section with a text area and a '+' icon. At the bottom of the form, there is a blue 'Submit' button.

Once filled and submitted, it will create the incident with the information from the template, and with the comments supplied on the record producer form, if any.

References

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

Defining an Inbound Email Action

Overview

Inbound Email Actions allow users to log or update incidents on an instance via email. The Inbound Email Action parses the email and responds using a script. Out-of-box, an email received by the instance creates a new incident, sets the Contact type field to Email, and adds the body of the email to the Additional Comments field. More refined Inbound Email Actions can create incident tickets with more data, thus saving the incident management team valuable time.

Defining an Inbound Email Action for Replies

The following Inbound Email Action applies to email replies. Normally, when a user responds to an email sent by the instance, the inbound email action will match the watermark to an existing incident, and update the incident rather than creating a new record. However, if the watermark is missing, this Inbound Email Action will attempt to match a reply to the original incident.

To define an inbound email action for replies:

1. Navigate to **System Policy > Inbound Actions** and click **New**.
2. Populate the Form as follows:
 - **Name:** *Update Incident*
 - **Type:** *Reply*
 - **Target Table:** *Incident [incident]*
 - **Script:** Insert the following:

```
gs.include('validators');

if (current.getTable_name() == "incident") {
    current.comments = "reply from: " + email.origemail + "\n\n" +
email.body_text;

    if (email.body.assign != undefined)
        current.assigned_to = email.body.assign;

    if (email.body.priority != undefined &&
isNumeric(email.body.priority))
        current.priority = email.body.priority;

    if (email.body.category != undefined)
        current.category = email.body.category;

    if (email.body.short_description != undefined)
        current.short_description = email.body.short_description;
```

```
current.update();  
}
```

Categorizing Incidents

Categorizing



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

Overview

Assigning incident tickets to categories and subcategories can greatly improve the clarity and granularity of report data. For example, without good categorization of incidents, you'd never know how many network-related versus telephone-related incidents you had from week to week.

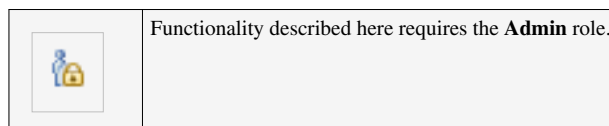
The platform can also use an incident's category/subcategory to automatically assign it to a specific fulfillment group to work on it (i.e., "Network" tickets should automatically go to the Network group, without anyone having to do anything more than assign the category. For more information, see *Defining an Assignment Rule for Incidents*.

Out-of-Box Incident Categories and Subcategories

Category	Subcategory
Request	Password Reset
	Password Expired
	Account Locked
Inquiry / Help	Anti-Virus
	Email
	Internal Application
Software	Email
	Operating System
Hardware	CPU
	Disk
	Keyboard
	Memory
	Monitor
Network	Mouse
	DHCP
	DNS
	IP Address
	VPN

	Wireless
Database	DB2
	MS SLQ Server
	Oracle

Adding or Removing Incident Categories or Subcategories



To add or remove Incident categories or subcategories:

1. Navigate to **Incident > Create New**.
2. Right-click the **Category** or **Subcategory** field and select **Configure Choices** (**Personalize Choices** in versions prior to Fuji). The **Subcategory** field is not on the form by default, and may need to be added.
3. To add new categories, click **New**, specify a Label and Value, and click **Submit**.
4. To add existing categories, highlight the desired category and click **Add**.
5. To remove existing categories, highlight the unwanted category and click **Remove**.

References

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

Defining an Assignment Rule for Incidents



Note: This article applies to Fuji. For more current information, see *Define an Assignment Rule for Incidents*^[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

To ensure that incidents are promptly dealt with by the appropriate IT service members, administrators can define Assignment Rules to automate the process.

Defining an Assignment Rule for Incidents

To define an assignment rule for incidents:

- 1. Navigate to **System Policy > Assignment** and click **New**.
- 2. Populate the form as follows:
 - **Name:** *New York Database Issues*
 - **Table:** *Incident [incident]*
 - **Execution Order:** *50*
 - **Group:** *NY DB*
 - **Conditions:** "Location is New York" and "Category is Database".

← Assignment Rule

UpdateDelete🔍📄⬆️⬆️

Name:

New York Database

Execution Order:

100

Table:

Incident [incident]

User:

Match conditions:

All

Group:

NY DB

Conditions:

and

or

Location is New York

and

Category is Database

Script:

UpdateDelete

To test the assignment rule, navigate to **Incidents > Create New** and populate the form with the following:

- **Location:** *New York*
- **Category:** *Database*

Incident		Submit	Close Incident
Number:	INC10009	Opened:	2009-10-01 13:36:23
Caller:		Opened by:	System Administrator
Location:	New York	Incident state:	New
Configuration item:		Category:	Database
Impact:	3 - Low	Escalation:	Normal
Urgency:	3 - Low	Assignment group:	
Priority:	4 - Low	Assigned to:	
Knowledge:	<input type="checkbox"/>		
Short description:			
Additional comments:			
Work notes:			

When you save the incident, the proper assignment group is added:

Incident		Update	Close Incident	Delete
Number:	INC10009	Opened:	2009-10-01 13:36:23	
Caller:		Opened by:	System Administrator	
Location:	New York	Incident state:	New	
Configuration item:		Category:	Database	
Impact:	3 - Low	Escalation:	Normal	
Urgency:	3 - Low	Assignment group:	NY DB	
Priority:	4 - Low	Assigned to:		
Knowledge:	<input type="checkbox"/>			
Short description:				

References

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

Diagnosis

Attaching Configuration Items

Overview

To aid in the incident management process, attach as much information as possible to the incident. The service desk often deals with an incident related to one or more specific configuration items (CIs). If the configuration management team has populated the CMDB, the CI records may hold valuable information for the incident management team. You can associate configuration items to an incident to see how the incident affects other CIs with dependent relationships.

Associating Configuration Items to Incidents

To associate configuration items to incidents from the Incident form, use either:

- The **Configuration Item** reference field.
- The **Affected CI's** related list.

Use the **Configuration Item** field when there is a single, primary CI that is the cause of the incident, and the **Affected CI's** related list when multiple CIs are affected by the incident. For example, suppose a load-balancer in a datacenter is no longer operational. The **Configuration Item** field might have the specific server which has run out of memory, while the **Affected CI** related list contains the load-balancer, the datacenter, the servers which depend on that load-balancer, and business services that are impacted by the missing server.

These CIs can be associated manually using the fields, or can be attached using the business service management (BSM) map.

Using the BSM Map to Locate Affected CIs

If the incident management team knows which configuration item is behind an incident, but does not know what other CIs might be affected, they can use the BSM map to identify dependent CIs.



Note: The BSM map shown in this procedure is available starting with the Eureka release. For information about adding affected CIs in versions prior to Eureka, expand the procedure at the end of this section.

1. In the Incident record form, populate the **Configuration Item** field.
-

<

≡

Incident

Number

INC0010019

Caller

Q

Location

Q

Activity due

UNKNOWN

Category

Inquiry / Help

⌵

Subcategory

-- None --


⌵

test_column

test_column_2

Configuration item

Q

2. Click the BSM map icon () that appears beside the **Configuration** field.

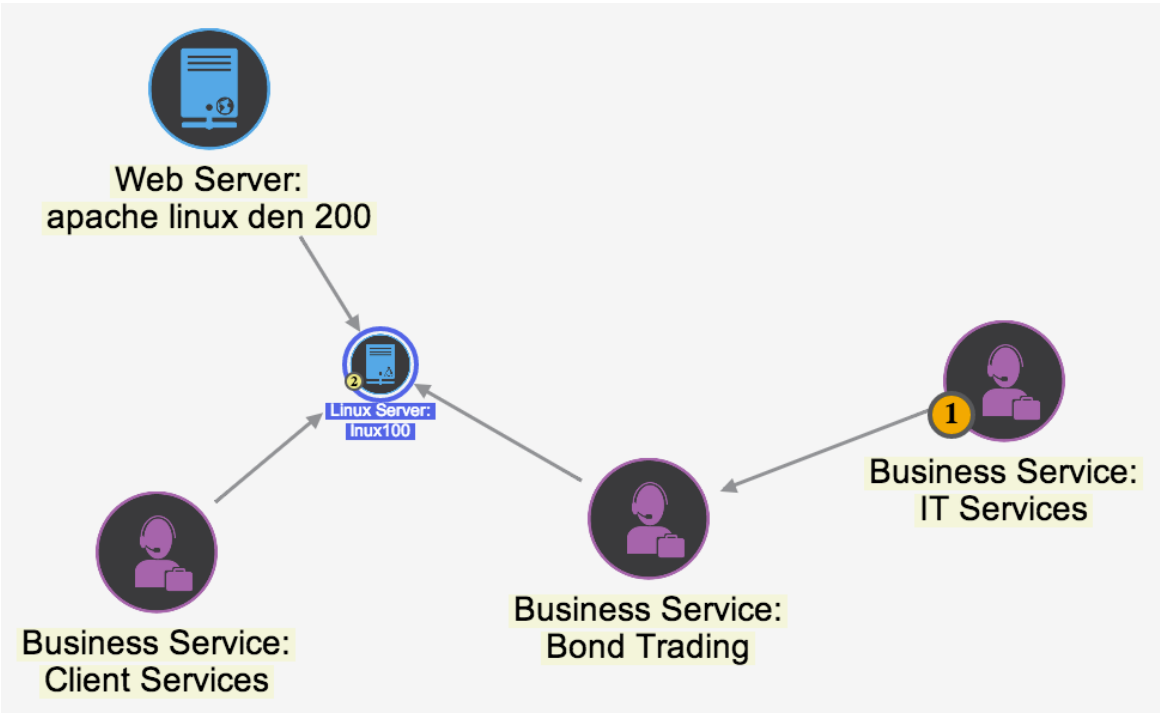
Configuration item

linux100

Q

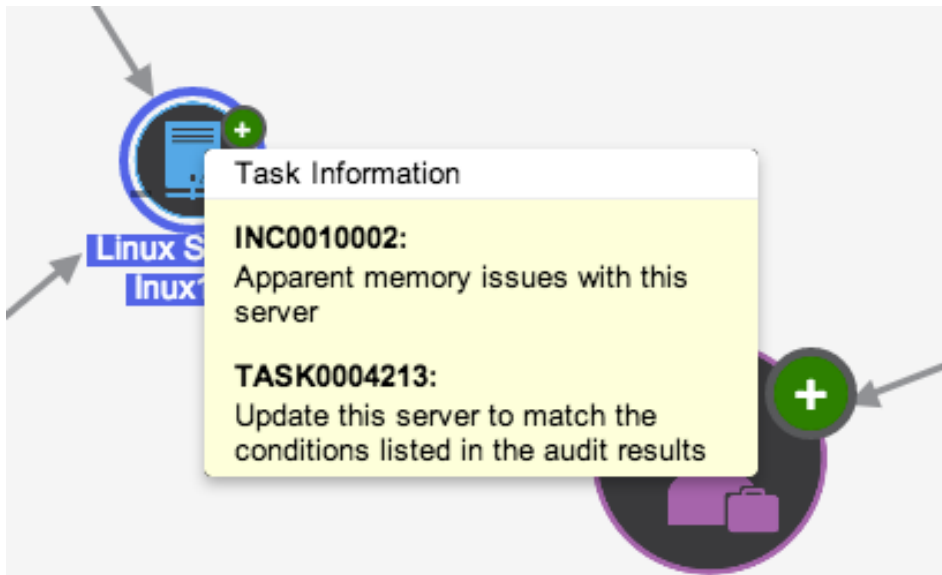


The system displays the configuration item and all its dependent CIs in the map. In this example, the BSM map has a blinking glyph in the lower left corner of the Linux server **linux100**, which indicates that the CI has an some issues associated with it. Also included on the map are the business services that rely on this Linux server and the software it is running, **apache linux den 200**.



3. Point to the glyph to display a list of tasks and issues with the CI.

This Linux server has one memory incident and a follow-on task from a desired state audit, which seems to indicate that the server is out of compliance, possibly resulting in the memory issue.



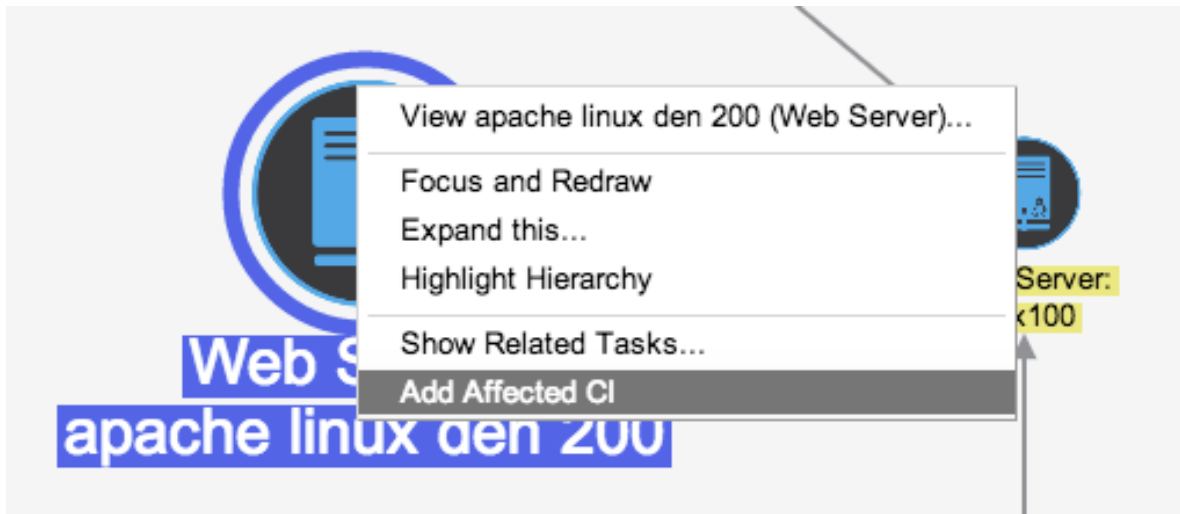
4. Click either task number to display the complete list of active tasks attached to this configuration item.

The list displays the users who are assigned to each line item in the list. Open each record for more information. Attaching the configuration item to the incident gives everyone working on the CI a more complete view of all the relevant information about that CI.

5. To arrange the map in different configurations, select a format from the **Layout** field at the top of the map, or click **Filter Panel** to filter the map for easier viewing.

The BSM map highlights the affected CIs, all of which are dependent on the Linux Server.

6. To add an affected CI to the incident for the Linux server, right-click a highlighted node and select **Add Affected CI** from the context menu.



7. Return to the incident record, and look at the **Affected CI's** related list.

If the list is not visible, configure the form to display it.

Task SLAs

Affected CIs (2)

Affected CIs

Edit...

Go to

Configuration Item

Task = INC0010002


Configuration Item

apache linux den 200

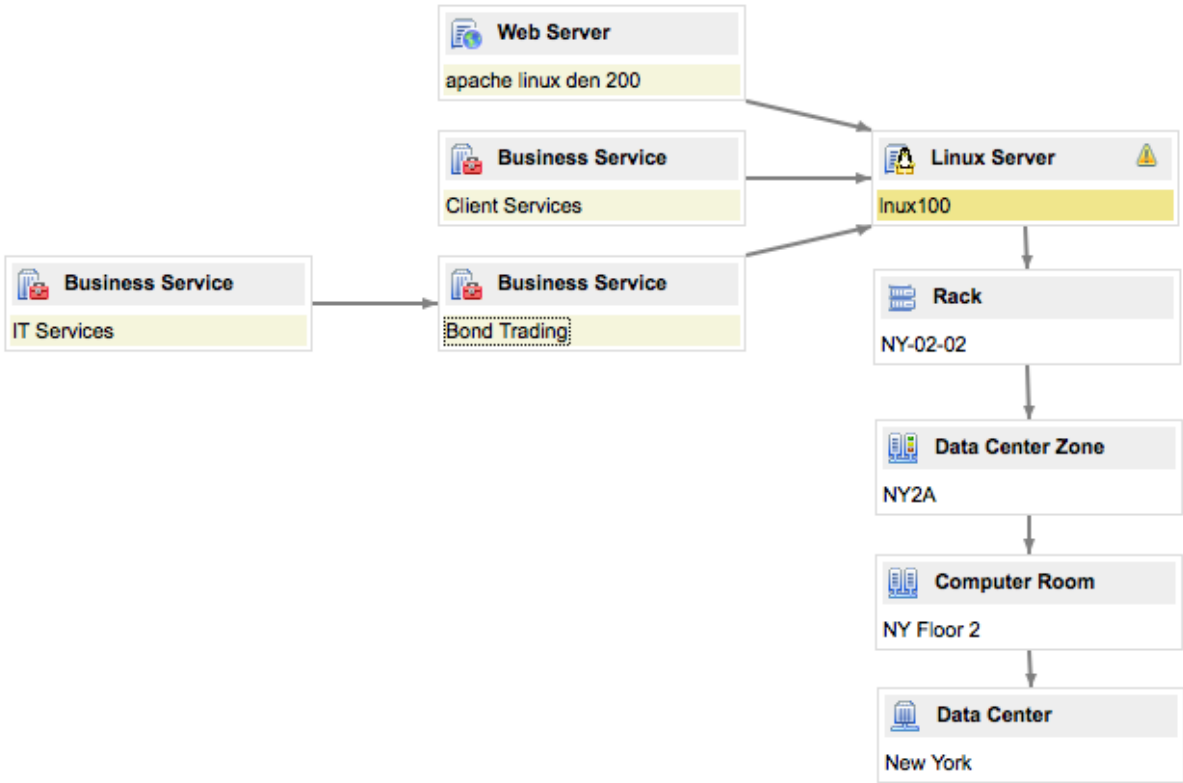
linux100

Actions on selected rows...

Click the plus to view the procedure for versions prior to Eureka

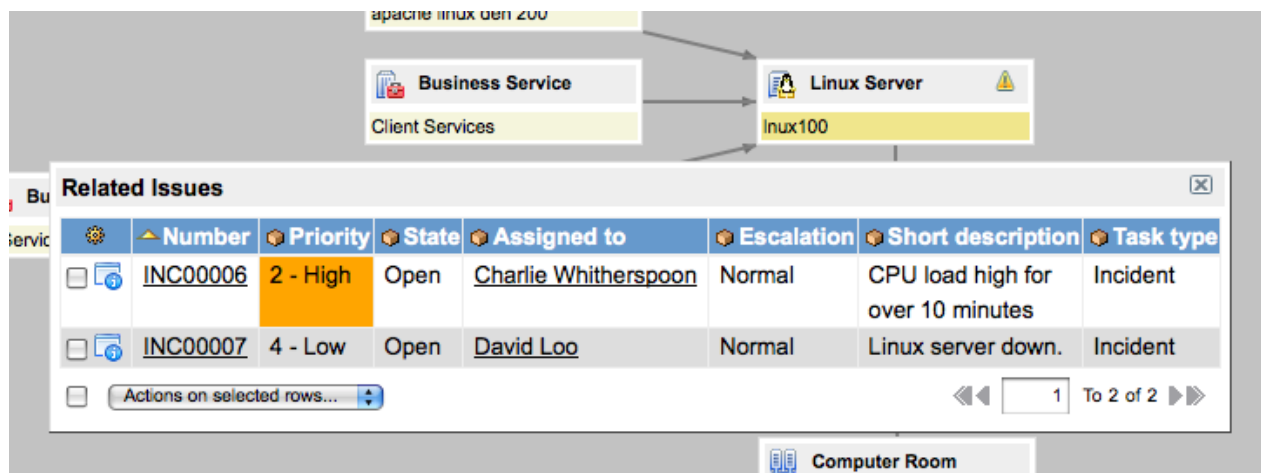
If the incident management team knows which configuration item is behind an incident, but does not know the affected CI, it is possible to look this up using the Business Service Management (BSM) map. Once the **Configuration Item** reference field is populated, click the BSM map icon () and the configuration item will appear with all of its dependent CIs.

For instance, suppose the Linux server **linux100** is impacted. Here is the BSM:



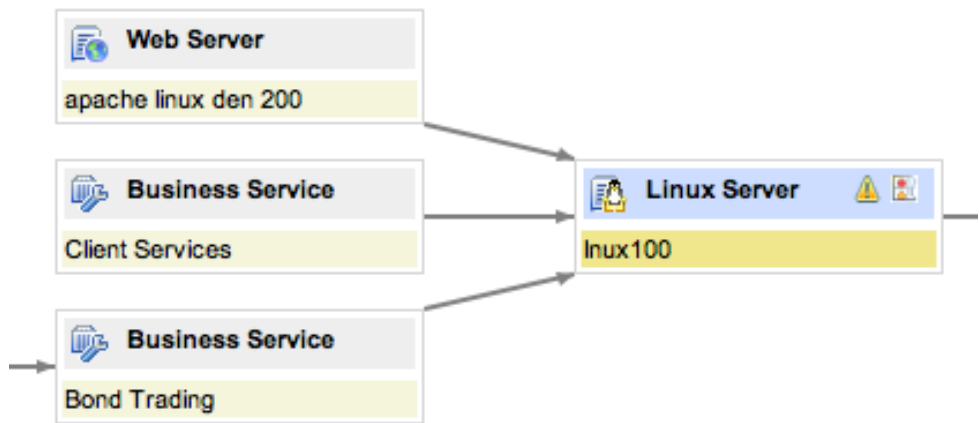
At the center is the Linux server in question. Included on the map are the business services which rely on it, the software it is running (**apache linux den 200**), and where in the data center it is.

The BSM shows a warning icon in the top right hand corner of the Linux server. This indicates that there is an incident attached to it. When clicked, it will display a list of the incidents attached to it.



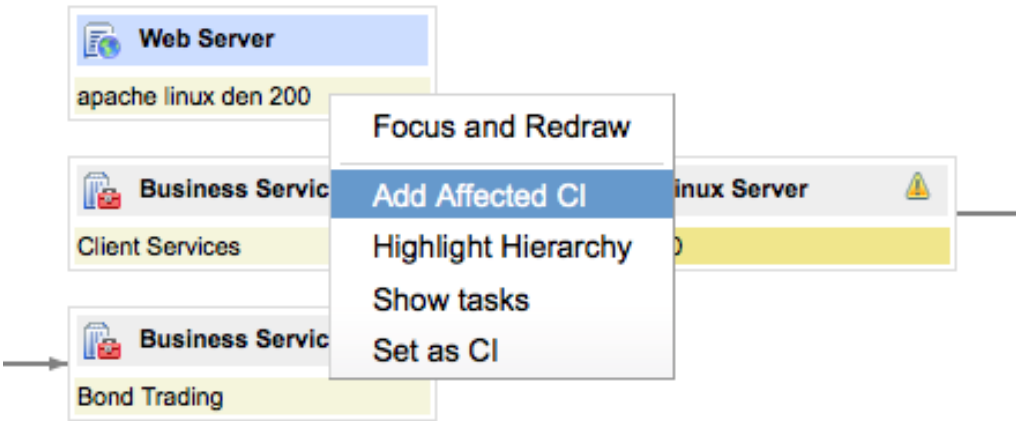
This Linux server has two incidents on it, which have been assigned to two different service desk employees. Now the two employees will be aware that another employee is working on a similar issue. The configuration management team will also be aware.

The BSM also lightly colors the affected CIs, all of which are dependent on the Linux Server. If the affected CI record is viewed, its dependencies are displayed in hierarchy form:

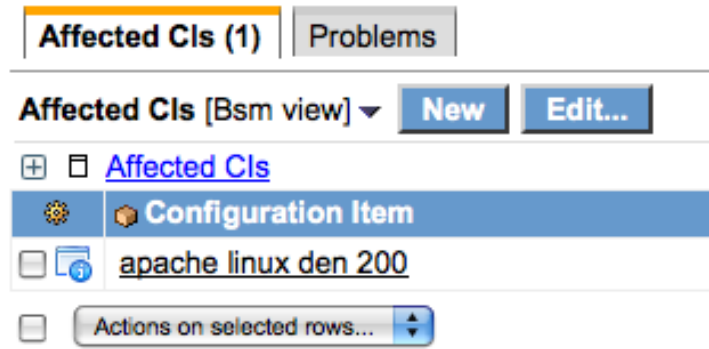


Note the yellow triangular exclamation mark icon next to **Inux100**. This too indicates that the dependent CI has an incident recorded for it, and when clicked will display the incidents. The icon to the right links to the **Affected CI's** related list.

From the BSM, it is possible to add the affected CI to the incidents attached to a CI. Right click the affected CI, and select **Add Affected CI**.



Now return to the incident record, and look at the **Affected CI's** related list.



The related list is now populated with the affected CI.


Checking Related Incidents




Note: This article applies to Fuji. For more current information, see *Configure Related Incidents* ^[1] at <http://docs.servicenow.com>. The Wiki page is no longer being updated. Please refer to <http://docs.servicenow.com> for the latest product documentation.

Overview



You have have these options to discover related incidents from the Incident form:

- The Show Related Incidents icon ()
- The **Related Incidents** related list
- The Business Services Map.

Using the Show Related Incidents Icon

You can view related incidents by clicking the Show Related Incidents icon (). It is a reference icon that appears beside the "Caller" field on the default incident form, when the field is populated. When you click the icon, it displays a list of other incidents for same caller.

Displaying the Show Related Incidents Icon

The **Show Related Incidents** icon ( in UI15,  in previous UIs) displays other incidents related to the referenced record. Administrators can add this icon to any reference field by modifying the dictionary and adding the `ref_contributions=user_show_incidents` dictionary attribute. The icon appears only for users who have read or write access to this field.




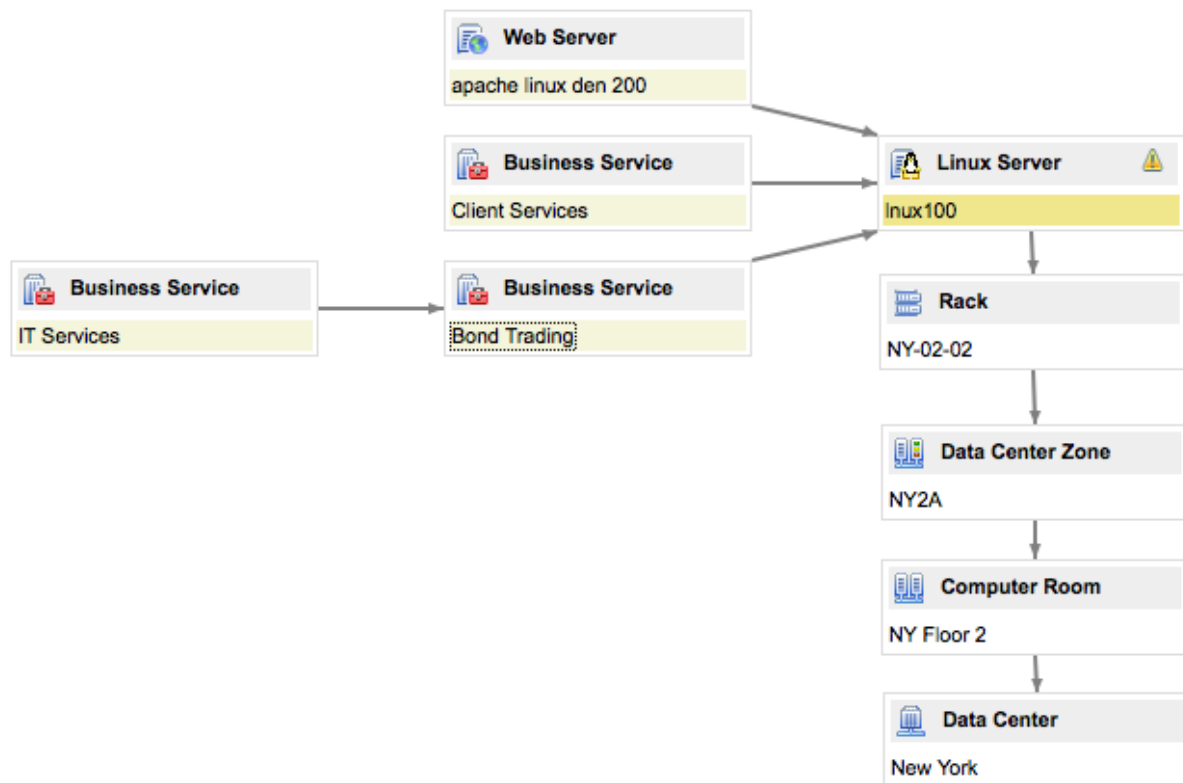
Note: The icon's behavior is defined by a UI Macro named `user_show_incidents`. If this UI Macro is not active in your instance, this reference field decoration will not be displayed.

Using the Related List

Other incidents by the same caller can also be found using the **Incidents by Same Caller** related list. You may need to add the related list to the form.

Using the Business Service Map

The methods above locate related incidents based on the caller. The Business Service Map can help find related incidents based on Configuration Item. If a Configuration Item is attached to an incident, clicking on the BSM Icon() will display the Business Service map. For example, this is the BSM for a server named **linux100**:



The Caution symbol in the CI's top right-hand corner indicates that there are tasks attached to it. Clicking on that icon displays a list of related issues:

	Number	Priority	State	Assigned to	Escalation	Short description	Task type
<input type="checkbox"/>	INC00006	2 - High	Open	Charlie Whitherspoon	Normal	CPU load high for over 10 minutes	Incident
<input type="checkbox"/>	INC00007	4 - Low	Open	David Loo	Normal	Linux server down.	Incident

Actions on selected rows... 1 To 2 of 2

In this way, the service desk can find related issues using the information gathered by the CMDB.

References

- [1] https://docs.servicenow.com/bundle/istanbul-servicenow-platform/page/administer/field-administration/task/t_ConfigureRelatedIncidentsIcon.html

Copying Attachment Contents into a KB Field

Overview

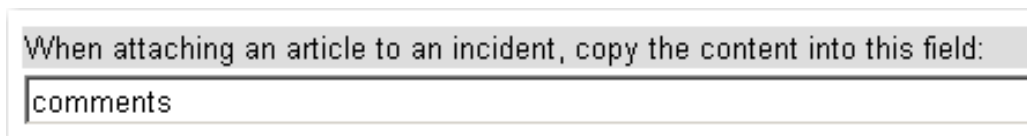
When a user searches for a knowledge base article from an incident, problem, or change request, the displayed article includes an **Attach to Task** button at the top right. The word *task* is replaced by the name of the form where the search was initiated.

Clicking this button copies the article number and contents into the **Comments** or **Description** field of the incident or problem record by default. Administrators can control the field where this information is placed.

Controlling the Attach to Task Button

Administrators can customize the copying behavior with a property.

1. Navigate to **Knowledge Base > Properties**.
2. In the **Other Knowledge Properties** section, locate **When attaching an article to an incident, copy the content into this field:**



The screenshot shows a configuration interface for a knowledge base property. It features a label "When attaching an article to an incident, copy the content into this field:" followed by a text input field containing the word "comments".

3. Specify a field into which to copy knowledge article content. This must be the **Element** name for the field, which is found by right-clicking the field name and selecting **Configure Label** (**Personalize Label** in versions prior to Fuji).

By default, this property is set to **comment**, meaning that content will be copied into the **Additional comments** field. If you change the value to **work_notes**, the article content would be copied into the **Work notes** field.

The copy behavior is based on the data type of the destination field. If the destination field is a *reference* field to kb_knowledge, ServiceNow creates a reference link to the existing article rather than copying the article contents into the record.

Notes/Limitations

- The target field must be on the form to receive the data.
- You can (optionally) specify more than one target field, separated by commas. In this case, ServiceNow looks for each field in order and copies the contents into the first one it finds on the form. It does *not* copy the data into multiple fields.
- If the selected field does not exist on the form, ServiceNow checks for **Comments** and **Description** automatically.

Resolving Incidents

Promoting Incidents



Note: This article applies to Fuji and earlier releases. For more current information, see *Promote an Incident* ^[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

When the incident management team has determined that the cause of an incident is an error or widespread problem, the team should initiate the problem management process. When the issue requires a change to be resolved, the team should initiate the change management process.

You can use a menu item on the Incident form to create a problem or change record and associate the incident with the new record. In this way, incidents can be used to easily create problems or changes.

You cannot promote an incident to a problem or change if the incident already has an associated record of that type.

Promoting an Incident

To promote an incident to a problem or change:

1. Open the Incident form for the incident to promote.
2. Right-click the form header bar.
3. Select **Create Problem** or **Create Change**.

Promoting an incident to a problem

The form for the new record appears. At this point, the new record is created. You do not need to manually save this record.

The screenshot shows the 'Problem' form in ServiceNow. At the top, it says 'Problem PRB40001 created'. The form has several fields: 'Number' (PRB40001), 'Problem state' (Open), 'Escalation' (Normal), 'RFC' (empty), 'Configuration item' (empty), 'Created by' (admin), 'Assigned to' (empty), 'Knowledge' (checkbox), 'Created' (2009-10-12 05:35:07), 'Short description' (Wireless access not available on floor 3), and 'Description' (empty). There are 'Update' and 'Delete' buttons at the bottom. Below the form, there is a table of incidents related to this problem.

Incidents	New	Edit...	Go to	Number	Category	Priority	Incident state	Escalation	Short description	Assigned to
INC00003				Network	4 - Low	New	Normal	Wireless access not available on floor 3	Beth Anglin	

A newly created problem with its related incident

Customizing Incident Promotion Behavior

Administrators can customize incident promotion behavior. The menu items **Create Problem** and **Create Change** are UI actions with that name. You can edit the UI action to customize the behavior of the menu item.

The **Create Problem** script carries over these fields from the Incident form:

- short_description
- cmdb_ci

- priority

The syntax for carrying a field from the Incident form to the Problem form is:

```
prob.[fieldname] = current.[fieldname]
```

The **Create Change** script carries over these fields from the Incident form:

- short_description
- description
- cmdb_ci
- priority

The syntax for carrying a field from the Incident form to the Change form is:

```
change.[fieldname] = current.[fieldname]
```

Promoting to Other Processes

If there is another process that incidents may be promoted to, such as if an incident should really be handled by Facilities Management, you can create a new UI action modeled after the **Create Change** and **Create Problem** UI actions to promote the incident to that table.

References

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

Best Practice Resolution Workflow Plugin



Note: This article applies to Fuji. For more current information, see *Best Practice - Incident Resolution Workflow*^[1] at <http://docs.servicenow.com>. The Wiki page is no longer being updated. Please refer to <http://docs.servicenow.com> for the latest product documentation.

Overview

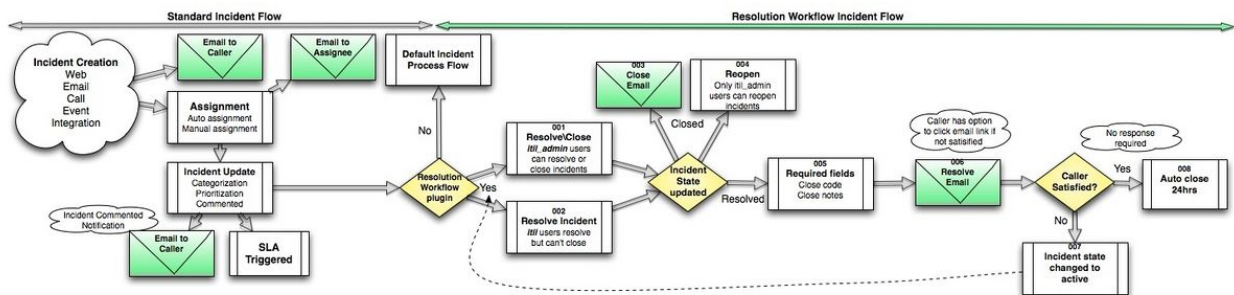
The **Best Practice - Incident Resolution Workflow** provides an ITIL-based best practice workflow to power the resolution of incidents.

Best practices for incident resolution dictate that rather than closing the incident, the incident should have a state of **Resolved**. This state gives the service desk a mechanism to verify that caller is satisfied with the resolution, and that the customer agrees with closing the incident. This workflow is automatically enabled on instances.



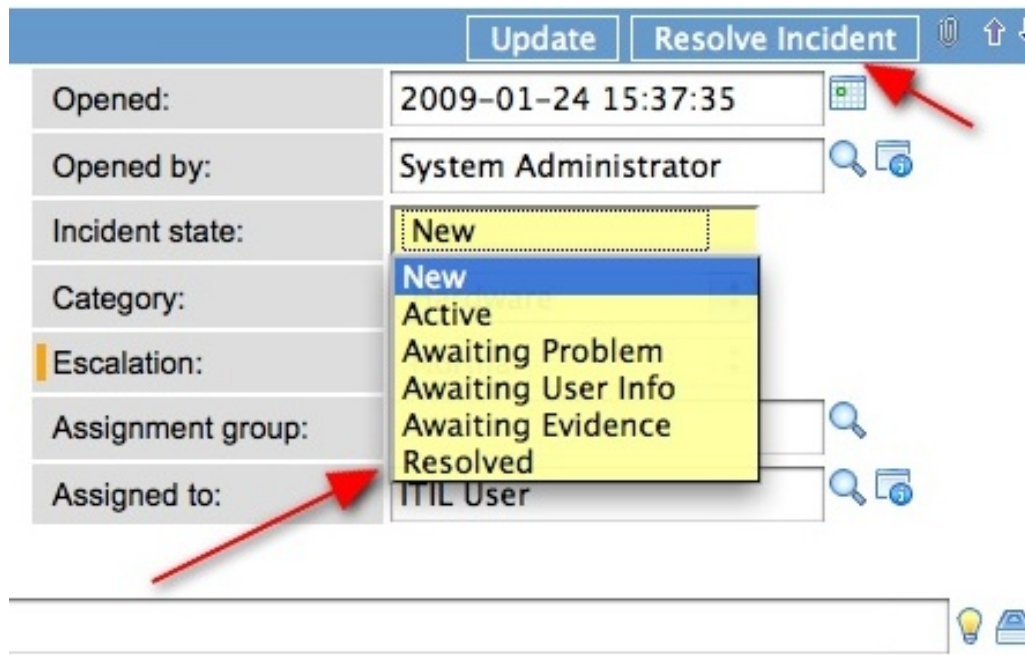
Note: Use this plugin to build a workflow (it does not install a workflow).

Incident Resolution Workflow



Resolve Incident

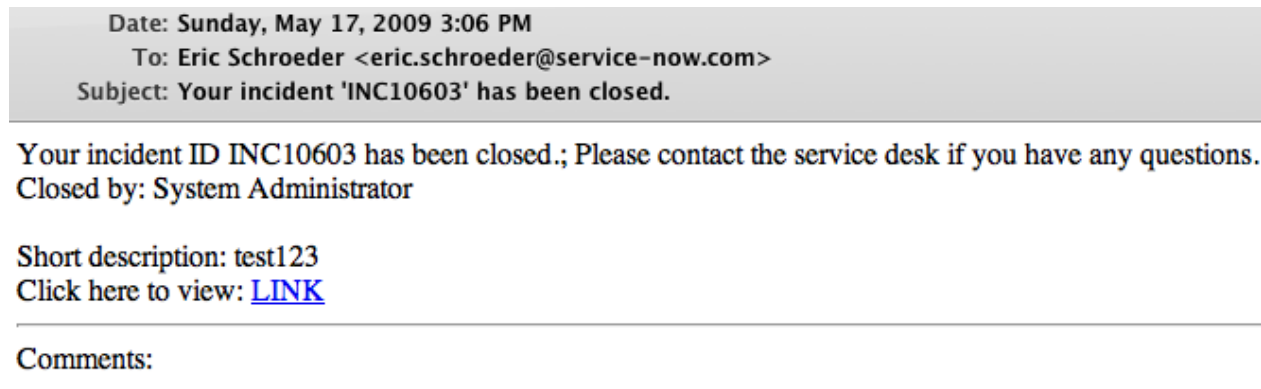
Users with the **itil** role or the **itil_admin** role have the capability to **Resolve** incidents with no option to close. Users with these roles will see a **Resolve Incident** button toward the top of the form as well have the option to select **Resolved** from the **Incident State** drop down list (see image for **itil_admin** options):



The screenshot shows the top of an incident form. At the top right, there are two buttons: 'Update' and 'Resolve Incident'. Below these are several form fields: 'Opened:' with the value '2009-01-24 15:37:35', 'Opened by:' with the value 'System Administrator', 'Incident state:' with a dropdown menu open showing options: 'New', 'Active', 'Awaiting Problem', 'Awaiting User Info', 'Awaiting Evidence', 'Resolved', and 'ITIL User'. The 'Resolved' option is highlighted. There are also search and info icons next to the 'Opened by' and 'Assigned to' fields. A red arrow points to the 'Resolve Incident' button, and another red arrow points to the 'Resolved' option in the dropdown menu.

Incident Closed Email

If an incident is closed, an email is sent to the end user.



The screenshot shows an email template for a closed incident. The header section contains the following text: 'Date: Sunday, May 17, 2009 3:06 PM', 'To: Eric Schroeder <eric.schroeder@service-now.com>', and 'Subject: Your incident 'INC10603' has been closed.' Below this, the main body of the email contains the text: 'Your incident ID INC10603 has been closed.; Please contact the service desk if you have any questions. Closed by: System Administrator'. There is a section for 'Short description: test123' and a link 'Click here to view: LINK'. At the bottom, there is a section for 'Comments:'.

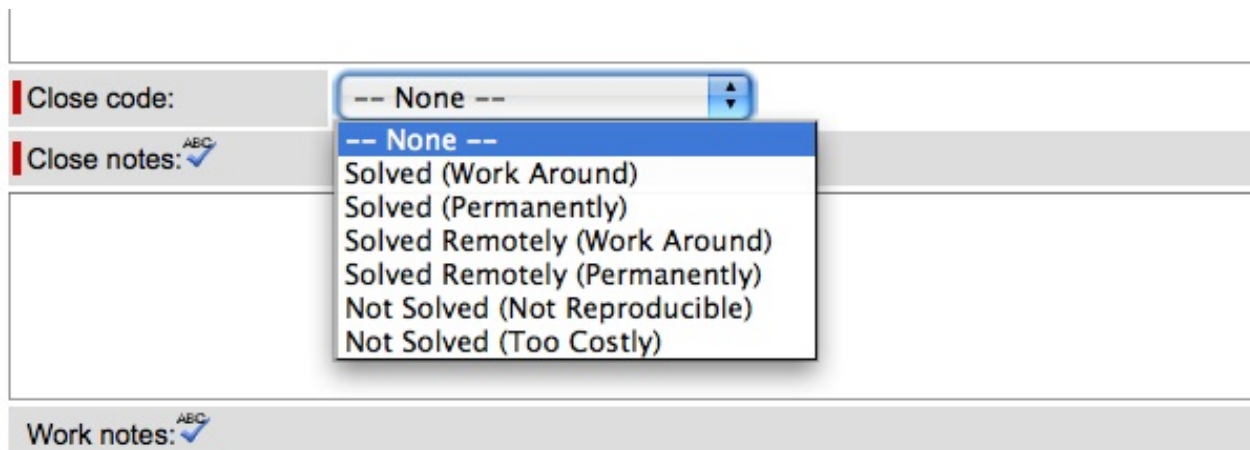
Reopen

- Closed incidents are read-only for non-administrators.
- Incidents can only be reopened by users with the admin role.
- Users with the **itil** role cannot reopen closed incidents.
- ESS users have a **Reopen Incident** button on resolved Incidents.

Required fields

Close code and **Close notes** fields are mandatory whenever an incident is **Resolved** or **Closed**. When an **Incident state** is set to resolved, two fields display on the incident form: **Close code** and **Close notes**. These fields require the help desk to select a **Closed code** and enter **Closed notes** detailing how the incident was resolved.

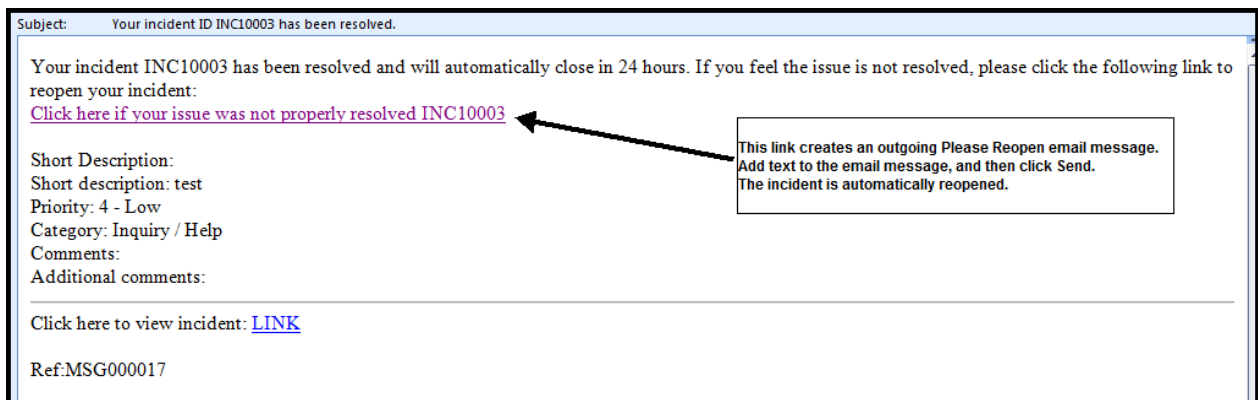
If custom incident forms have been created, the Close code and Close notes fields may need to be added manually.



The screenshot shows a form with three main sections: 'Close code:', 'Close notes:', and 'Work notes:'. The 'Close code:' dropdown menu is open, displaying a list of options: '-- None --', 'Solved (Work Around)', 'Solved (Permanently)', 'Solved Remotely (Work Around)', 'Solved Remotely (Permanently)', 'Not Solved (Not Reproducible)', and 'Not Solved (Too Costly)'. The 'Close notes:' field has a small 'ABC' icon and a checkmark. The 'Work notes:' field also has a small 'ABC' icon and a checkmark.

Resolve Email

When an incident is set to a 'Resolved' incident state an email notification is sent to the caller. If the caller is satisfied with the resolution, no action is required on the caller's behalf. ServiceNow automatically closes the incident after 24 hours. If the caller is not satisfied, s/he can reopen the incident by clicking on the link within the email notification. This creates an outgoing Please Reopen email message. The user can add text to the outgoing email if they want to add any additional remarks. The Resolved incident is automatically reactivated and displays an Active status.



The screenshot shows an email notification with the following content:

Subject: Your incident ID INC10003 has been resolved.

Your incident INC10003 has been resolved and will automatically close in 24 hours. If you feel the issue is not resolved, please click the following link to reopen your incident:
[Click here if your issue was not properly resolved INC10003](#)

Short Description:
 Short description: test
 Priority: 4 - Low
 Category: Inquiry / Help
 Comments:
 Additional comments:

Click here to view incident: [LINK](#)

Ref:MSG000017

A callout box points to the link with the text: "This link creates an outgoing Please Reopen email message. Add text to the email message, and then click Send. The incident is automatically reopened."

Auto Close 24hrs

If the incident state is **Resolved**, and the caller has not emailed any feedback within 24-hours, the incident is auto-closed (with no entry in the **Closed by** field) by a scheduled job.

The duration of the auto-close function can be modified.

To change the duration of the incident auto-close function:

1. From the left navigation pane, select **System Properties > UI Properties**.
2. Scroll to locate the field below:

Number of days (integer) after which Resolved incidents are automatically closed. Zero (0) disables this feature.

1

3. Change the number of days (integer only).
4. Click **Save**.

The property updates the number of days after which the Resolved incident is closed. Make sure to update the resolved incident email notification text to reflect the new duration.

To update the resolved incident notification template:

1. From the left navigation pane, select **System Policy > Templates**.
2. Scroll to the *incident.ess.resolve* template, and then click the **Name** (the template displays)
3. Manually update the template's text.
4. Click **Update**. (Your incident resolved notification template is updated.)

Caller Closes Incident

When a caller closes their incident:

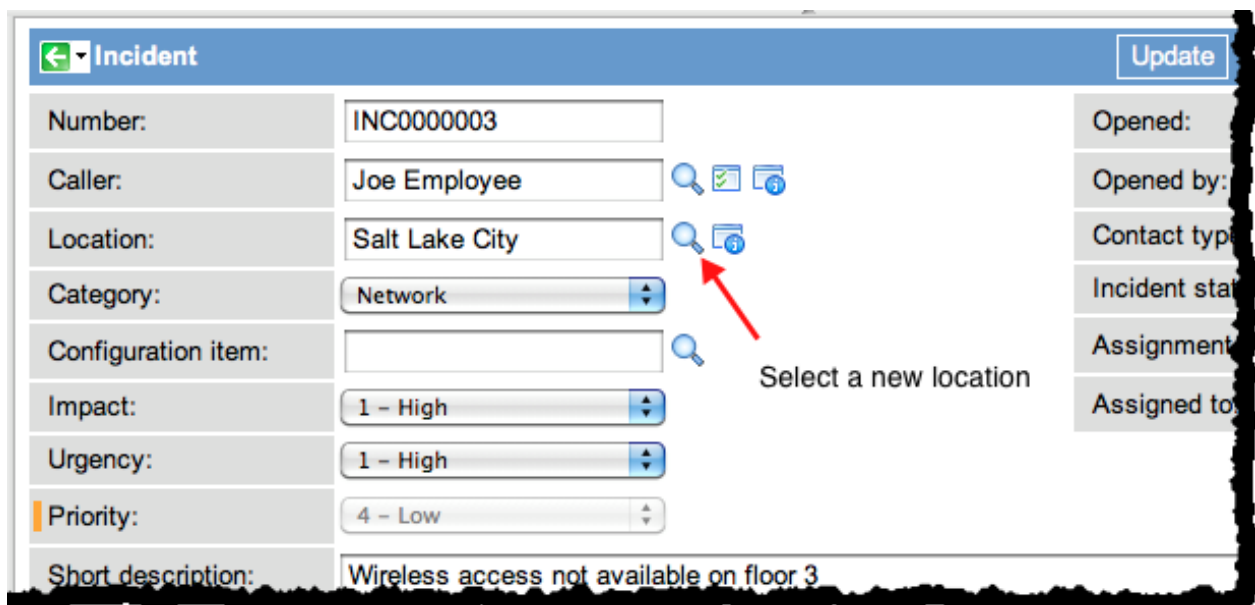
- An info message with a link to the incident displays.
- Close notes and the close code are automatically set by a business rule.

Automatically Populating the Caller's Location

With the Best Practice - Incident Resolution Workflow plugin, when the **Caller (user)** is added to the Incident form, the caller's **Location** is automatically populated in the incident form. This best practice plugin adds functionality that autofills the **Location** field whenever the **Caller** information is entered or changed. However, the option remains to manually replace the auto-filled location.

To manually replace the caller's (autofilled) location:

1. Click the magnifying list icon next to the **Location** field, and select another location from the list.



The screenshot shows the 'Incident' form with the following fields and values:

Field	Value
Number:	INC0000003
Caller:	Joe Employee
Location:	Salt Lake City
Category:	Network
Configuration item:	
Impact:	1 - High
Urgency:	1 - High
Priority:	4 - Low
Short description:	Wireless access not available on floor 3

A red arrow points to the magnifying list icon next to the Location field, with the text 'Select a new location' next to it.

Flagging VIPs

Organizations commonly designate VIP status in the user record for some of their VIP customers. If the incident forms have been customized, the VIP field may need to be added to the user record form. Checking the VIP box on the user record sets the VIP value to **true** for the user. By default, users are automatically checked for VIP status. Therefore, whenever a VIP caller opens an incident, the Caller's name displays in red.

Incident form details:

- Number: INC0000050
- Caller: Jerrod Bennett (VIP status indicated by red text and icon)
- Location: San Diego
- Category: Hardware
- Configuration item: EXCH-SD-05
- Impact: 1 - High
- Urgency: 1 - High
- Priority: 1 - Critical
- Short description: Exchange server appears to be down...lots of users impacted
- Opened: 2013-05-31 14:58:24
- Opened by:
- Contact type: Phone
- Incident state: Active
- Assignment group: Hardware
- Assigned to: Beth Anglin

The **Caller** name column does not display by default in the **Incident > Open** module.

To add the Caller column:

1. Right-click the **Incident** table header.
2. Select the appropriate option for your version:
 - **Fuji or later:** Configure > List Layout
 - **Eureka or earlier:** Personalize > List Layout
3. Add the **Caller** column to the **Selected** list.
4. Click **Save**.

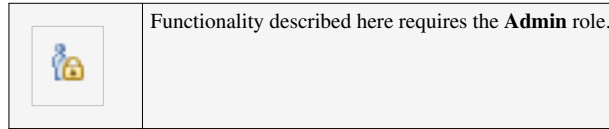
Number	Caller	Short description	Category	Priority	Incident status
INC0000002	Jerrod Bennett	Can't get to network file shares	Software	4 - Low	Awaiting Problem
INC0000003	Joe Employee	Wireless access not available on floor 3	Network	4 - Low	Active
INC0000005		CPU load high for over 10 minutes	Software	2 - High	Active
INC0000007	Joe Employee	Need access to sales db for the west	Database	4 - Low	Active
INC0000014	Bow Ruggeri	missing my home directory	Hardware	4 - Low	New
INC0000015	Fred Luddy	I can't launch my game anymore	Software	4 - Low	New
INC0000016	Bow Ruggeri	Rain is leaking on main DNS Server	Software	4 - Low	New
INC0000017	Joe Employee	How do I create a sub-folder	Hardware	4 - Low	New
INC0000018	Taylor Vreeland	Sales forecast spreadsheet is READ ONLY	Hardware	1 - Critical	New

References

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

Closing Incidents

Closing Resolved Incidents Automatically



Note: This article applies to Fuji. For more current information, see *Configure Incidents to Close Automatically*^[1] at <http://docs.servicenow.com>. The Wiki page is no longer being updated. Please refer to <http://docs.servicenow.com> for the latest product documentation.

Overview

You can configure ServiceNow to automatically close tickets that have been in an Incident State of "Resolved" a specified number of days. For example, if you set the property to 3 days, then 3 days after an incident is Resolved it will be automatically closed. Any update to the incident, for example an added comment from a Self Service user, would restart this 3-day clock.

If you set this property to zero days (the default), Incidents will not auto-close. To set the property, navigate to **System Properties > System**, and then look for the following property:

<p>The number of days after which a Resolved, un-updated incident will be automatically closed by a scheduled business rule. The default, 0, means incidents will not be automatically closed.</p> <input type="text" value="0"/>



Note: If you have an inactivity monitor firing on your incident, it will reset this auto-close clock each time it fires, preventing your incident from being closed. To prevent this, put a Reset Condition on your inactivity monitor of **Incident state is not Resolved**.

Assigning a User Name to Incidents Closed Automatically

A scheduled job called Autoclose Incidents runs the Incident Autoclose business rule to close incidents as described above. By default, it assigns the name of the administrator who is logged in when the Autoclose Incidents job runs.



Note: The Incident Autoclose rule (**System Definition > Business Rules > Incident autoclose**) should be set on the Incident [incident] table, not the Global [global] table, to avoid potential performance issues.

You can set a specific user name to show in the incident record as the Updated By user when the incident is closed automatically. Go to **System Scheduler > Scheduled Jobs > Autoclose Incidents** and add `fcRunAs=<user_name>` to the Scheduled Job record. The following example places System Administrator into the Updated By field when an incident is closed automatically:

```
fcRunAs=admin
fcScriptName=incident autoclose
```

References

- [1] <https://docs.servicenow.com/bundle/istanbul-it-service-management/page/product/incident-management/task/configure-incident-auto-close.html>

Closing Multiple Incidents



Note: This article applies to Fuji. For more current information, see *Closing Multiple Incidents from a List* ^[1] at <http://docs.servicenow.com>. The Wiki page is no longer being updated. Please refer to <http://docs.servicenow.com> for the latest product documentation.

Overview

Service desk technicians with the `list_updater` role can close multiple incidents from an incident list and attach the same close notes to all of them. In addition to the default method for closing multiple incidents, an administrator can create a UI action and make the feature available to users without the `list_updater` role.

Closing Incidents from a List

In the base system, users with the `list_updater` role can use the list view to close multiple incidents with the same close notes:

1. Select the check box beside each incident to be closed.
2. Right-click the list header and select **Update Selected**.
3. Set the **State** to **Closed** and enter close notes in the **Additional comments** field.
4. Click **Update**.

Closing Incidents with a UI Action

To simplify the process of closing multiple incidents with the same close notes, you can create a UI action called **CloseNotes** to close these incidents from the list view. This also requires a business rule for the UI action to reference and a form view.

Creating the Business Rule

To create a business rule for the UI action to close multiple incidents:

1. Navigate to **System Definition > Business Rules**.
2. Create a business rule like the one in this screenshot.

(Versions prior to Eureka only) If needed, personalize the Business Rule form to add the fields **Action label** and **Action name**.

Business Rule [Submit]

Name: When:

Table: Insert: ☐

Order: Update: ☐

Client callable: ☐ Delete: ☐

Active: ☒ Query: ☐

Action label:

Action name:

Condition:

Script:

```
current.active = 'false';
current.short_description = "TEST CLOSE NOTES";
current.incident_state = '7';
gs.addInfoMessage("Closing");
current.update();
```

Select variables: ☐ ☐

- ☐ Fields
- ☐ GlideRecord
- ☐ GlideElement
- ☐ System
- ☐ GlideAggregate

[Submit]

Following is a copy of the script that you can copy and paste as the basis for the new rule:

```
current.active = 'false';
current.short_description = "TEST CLOSE NOTES";
current.incident_state = '7';
gs.addInfoMessage("Closing");
current.update();
```

Creating a UI Action

To create the UI action for closing multiple incidents with the same close notes:

1. Navigate to **System UI > UI Actions**.
2. Create a UI action like the one in this screenshot.
3. Click **Submit**.

The new UI action appears in the **Action** choice list at the bottom of lists associated with the selected table.

UI Action [Submit]

Name: Form button: ☐

Table: Form context menu: ☐

Order: Form link: ☐

Action name: List bottom button: ☐

Active: ☒ List context menu: ☐

Show insert: ☒ List choice: ☒

Show update: ☒ List link: ☐

Client: ☒

Comments:

Hint:

Onclick:

Condition:

Script:

```
showQuickForm('CloseNotes','close_it')
```

Select variables: ☐ ☐

- ☐ Fields
- ☐ GlideRecord

[Submit]

Creating a Form View

Create a view of the Incident form, using the following guidelines.

- Make the view **Name** match the first parameter to `showQuickForm()` in the UI action. In this example, the parameter is **CloseNotes**.
- Make sure the view contains the fields to be updated, in this case the **Additional comments** field.

Using the UI Action

To close multiple incidents with the new UI action:

1. Navigate to **Incident > Open**.
2. Select the check box beside each incident to be closed.
3. Go to the **Action** choice list at the bottom of the list and choose **CloseNotes**.
4. Set the **Incident state** to **Closed**, enter close notes in the **Additional comments** field, and fill in any other relevant fields.
5. Click **Update**.



Note: For faster updates, the `showQuickForm` function does not perform validations such as for **UI policies** or mandatory fields.

References

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

Continual Service Improvements

Reporting on Incidents



Note: This article applies to Fuji and earlier releases. For more current information, see [Reporting](http://docs.servicenow.com)^[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

In order to continually improve the Incident Management process, it is possible to gather the information collected by the platform and present the data in reports. Below are instructions on how to create a pair of sample Incident Management reports. The first is a bar chart of Incidents by Caller's Company. The second is a line chart of Incidents Opened per Month. The last is a pivot table of Incidents by Caller and State. The last example also demonstrates how to put the new report on a homepage as a gauge.


Incidents by Caller's Company

This bar chart displays all of the incidents, grouped by the company of the caller, further broken down by the state of the incident. This allows the incident management team to see which companies are generating more or less incidents, and how those incidents are being handled.

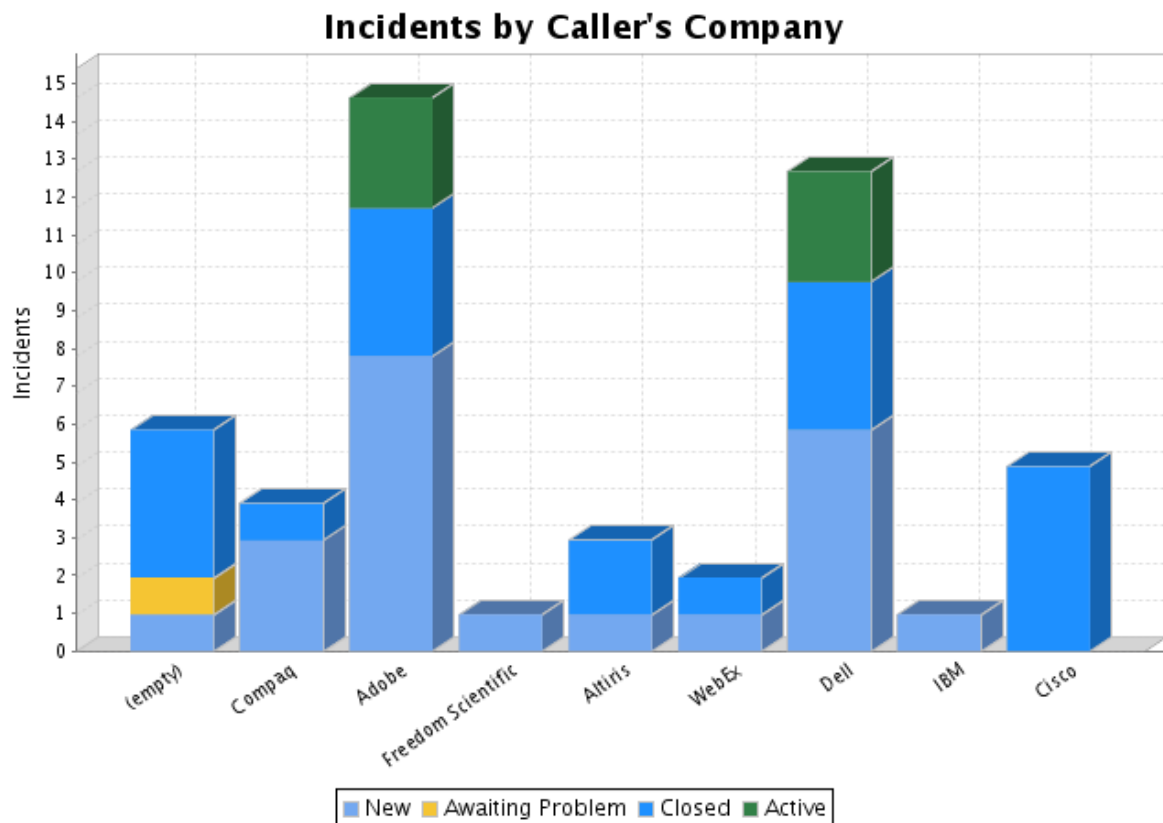
To report on Incidents by Caller's Company:

1. Navigate to **Reports > View / Run** and click **New**.
2. Populate the form as follows:
 - **Name** - Incidents by Caller's Company.
 - **Type** - Bar Chart
 - **Table** - Incident [incident]
 - **Group By** - Dotwalk to Caller.Company
 - **Stacked Field** - Incident State

[Reports](#) > [New report](#)

Run Report	Save	Insert	Delete	Make Gauge	Schedule
Name:	Incidents by Caller's Company			Stacked Field:	State
Visible to:	Me			Aggregation:	Count
Type:	Bar chart			Chart size:	Large
Table:	Incident [incident]			Other threshold:	System Default (12)
Group by:	Company			Display grid:	<input type="checkbox"/>
Filter and Order: 					

3. Select **Run Report**. The bar chart should appear as follows:



4. Click **Save**.

Incidents Opened per Month

The following example is a line chart that tracks the number of Incidents opened per month.

To report on Incidents Opened per Month:

1. Navigate to **Reports > View / Run** and click **New**.
2. Populate the form as follows:
 - **Name** - Incidents Opened per Month.
 - **Type** - Line Chart
 - **Table** - Incident [incident]
 - **Trend Field** - Opened per Month.

Run Report
Save
Insert
Delete
Make Gauge
Schedule

Name:

Visible to:

Type:

Table:

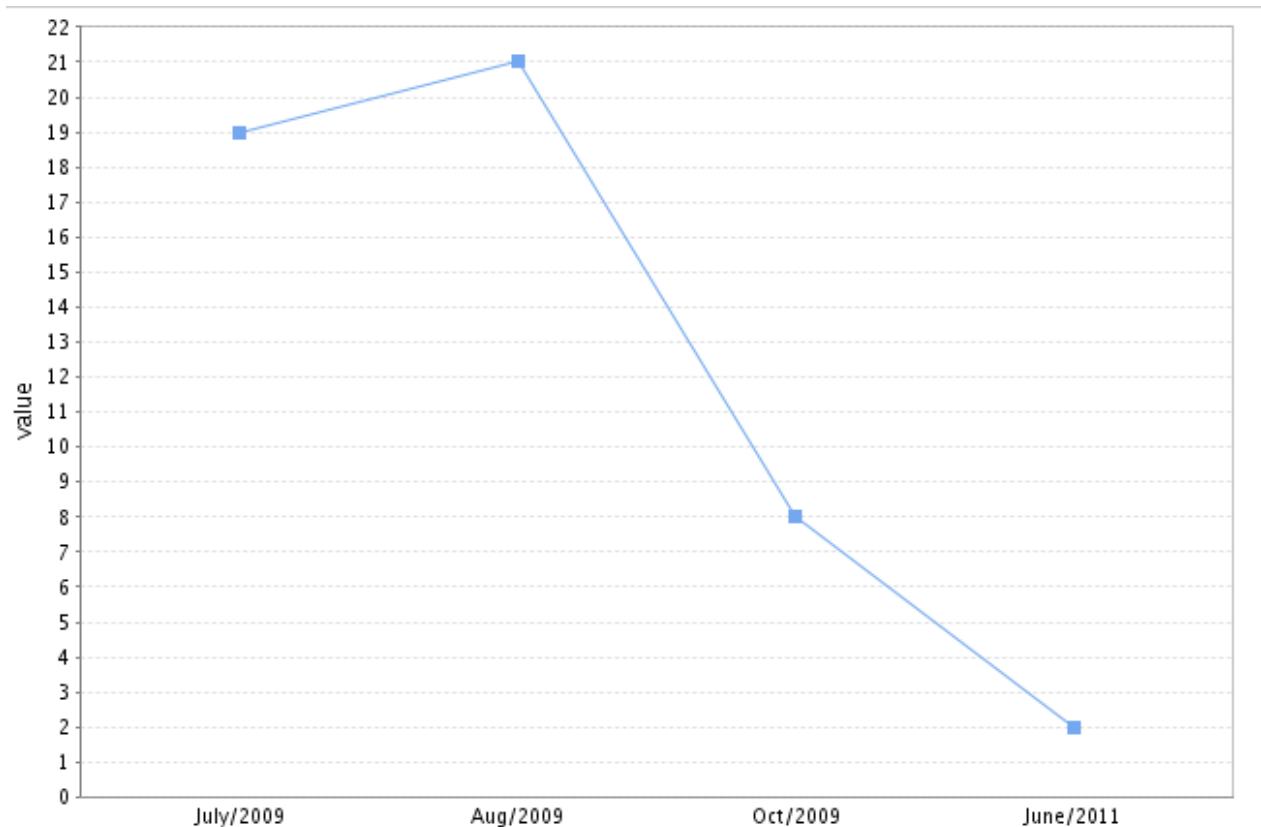
Group by:

Filter and Order: and or a-z

Trend Field: per

Aggregation:

3. Select **Run Report**. The line chart should appear as follows:



4. Click **Save**.

Incidents by Caller and State

To report on Incidents by Caller and State which are assigned to the current user:

1. Navigate to **Reports > View / Run** and click **New**.
2. Populate the form as follows:
 - **Name** - Incidents by Caller and State.
 - **Type** - Pivot Table
 - **Table** - Incident [incident]
 - **Rows** - Caller.
 - **Columns** - Incident State.
 - **Filter and Order** - Assigned To is the name of the current user. In this example, the current user will be ITIL User.

[Reports](#) > [New report](#)

Run Report | **Save** | **Insert** | **Delete** | **Make Gauge**

Name: Incident by Caller and State	Row: Caller
Visible to: Me	Column: Incident state
Type: Pivot Table	Aggregation: Count
Table: Incident [incident]	Other threshold: System Default (12)

Filter: And Or

Assigned to is ITIL User Find And Or ×

3. Select **Run Report**. The table should appear as follows:

Incident by Caller and State

Caller	Incident state			
	Active	Closed	New	Total
(empty)	0	1	1	2
Bow Ruggeri	0	1	2	3
Bud Richman	1	0	0	1
Carol Coughlin	0	0	1	1
Christen Mitchell	0	0	1	1
Don Goodliffe	0	1	1	2
Fred Luddy	0	0	1	1
Joe Employee	0	1	1	2
Luke Wilson	0	0	1	1
Taylor Vreeland	0	0	1	1
Total	1	4	10	15

4. Click **Make Gauge** and then **Add to Homepage**. Select a particular dropzone. The report will now appear on the last homepage viewed.

[Add content »](#) **My ITIL Homepage** [Refresh:](#) [Switch to page...](#)

Incident by Caller and State

Caller	Incident state			
	Active	Closed	New	Total
(empty)	0	1	1	2
Bow Ruggeri	0	1	2	3
Bud Richman	1	0	0	1
Carol Coughlin	0	0	1	1
Christen Mitchell	0	0	1	1
Don Goodliffe	0	1	1	2
Fred Luddy	0	0	1	1
Joe Employee	0	1	1	2
Luke Wilson	0	0	1	1
Taylor Vreeland	0	0	1	1
Total	1	4	10	15

Users by Location

(empty) = 2 (4%)
Denver = 3 (6%)

News

Windows XP How-To 2011-03-04

References

- [1] <https://docs.servicenow.com/bundle/jakarta-performance-analytics-and-reporting/page/use/reporting/reference/reporting-landing-page.html>

Article Sources and Contributors

ITIL Incident Management *Source:* <http://wiki.servicenow.com/index.php?oldid=189616> *Contributors:* Amy.bowman, CapaJC, Cheryl.dolan, David.Bailey, Davida.hughes, Emily.partridge, G.yedwab, Guy.yedwab, Ishrath.razvi, John.ramos, Joseph.messerschmidt, Ludwig.adriaansen, Mike.malcangio, Neola, Pat.Casey, Phillip.salzman, Rob.woodbyrne, Steven.wood, Suzanne.smith, Vaughn.romero, Vhearne

Creating a Template *Source:* <http://wiki.servicenow.com/index.php?oldid=250426> *Contributors:* Guy.yedwab, John.ramos, Jonathan.sparks, Joseph.messerschmidt, Julie.phaviseth, Neola, Steven.wood

Creating a Record Producer *Source:* <http://wiki.servicenow.com/index.php?oldid=250161> *Contributors:* Guy.yedwab, John.ramos, Joseph.messerschmidt, Neola, Publishing.user, Virginia.kelley

Defining an Inbound Email Action *Source:* <http://wiki.servicenow.com/index.php?oldid=100668> *Contributors:* G.yedwab, Guy.yedwab, Joseph.messerschmidt, Neola, Rachel.sienko, Steven.wood, Suzanne.smith

Categorizing *Source:* <http://wiki.servicenow.com/index.php?oldid=250069> *Contributors:* CapaJC, Emily.partridge, Fuji.publishing.user, Guy.yedwab, John.ramos, Joseph.messerschmidt, Neola, Vhearne

Defining an Assignment Rule for Incidents *Source:* <http://wiki.servicenow.com/index.php?oldid=250265> *Contributors:* Emily.partridge, Guy.yedwab, Jessi.graves, John.ramos, Joseph.messerschmidt, Neola

Attaching Configuration Items *Source:* <http://wiki.servicenow.com/index.php?oldid=239846> *Contributors:* Cheryl.dolan, Dawn.bunting, Emily.partridge, Fuji.publishing.user, Guy.yedwab, Joseph.messerschmidt, Neola, Steven.wood, Suzanne.smith

Checking Related Incidents *Source:* <http://wiki.servicenow.com/index.php?oldid=250094> *Contributors:* CapaJC, Cheryl.dolan, Emily.partridge, Fuji.publishing.user, Guy.yedwab, John.ramos, Joseph.messerschmidt, Julie.phaviseth, Neola, Rob.woodbyrne, Vhearne

Copying Attachment Contents into a KB Field *Source:* <http://wiki.servicenow.com/index.php?oldid=240120> *Contributors:* CapaJC, Cheryl.dolan, David.Bailey, Emily.partridge, Fuji.publishing.user, Guy.yedwab, Joseph.messerschmidt, Neola, Pat.Casey, Steven.wood, Vhearne

Promoting Incidents *Source:* <http://wiki.servicenow.com/index.php?oldid=250797> *Contributors:* Emily.partridge, Guy.yedwab, Jennifer.harvey, John.ramos, Joseph.messerschmidt, Neola, Phillip.salzman, Publishing.user, Steven.wood, Suzanne.smith

Best Practice Resolution Workflow Plugin *Source:* <http://wiki.servicenow.com/index.php?oldid=250010> *Contributors:* CapaJC, David.Bailey, Emily.partridge, Eric.schroeder, Fuji.publishing.user, G.yedwab, Guy.yedwab, Joe.Westrich, John.ramos, Joseph.messerschmidt, Michael.randall, Neola, Phillip.salzman, Rachel.sienko, Steven.wood, Suzanne.smith, Vhearne, Wallymarx

Closing Resolved Incidents Automatically *Source:* <http://wiki.servicenow.com/index.php?oldid=250138> *Contributors:* CapaJC, Cheryl.dolan, Guy.yedwab, John.ramos, Joseph.messerschmidt, Neola, Steven.wood, Vhearne

Closing Multiple Incidents *Source:* <http://wiki.servicenow.com/index.php?oldid=250137> *Contributors:* Amy.bowman, Anat.kerry, Cheryl.dolan, Guy.yedwab, John.ramos, Joseph.messerschmidt, Neola, Phillip.salzman, Steven.wood

Reporting on Incidents *Source:* <http://wiki.servicenow.com/index.php?oldid=250815> *Contributors:* Davida.hughes, Guy.yedwab, John.ramos, Joseph.messerschmidt, Michael.randall, Neola

Image Sources, Licenses and Contributors

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

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

Image:IncTemplate.png Source: <http://wiki.servicenow.com/index.php?title=File:IncTemplate.png> License: unknown Contributors: Guy.yedwab

Image:IncTemplateA.png Source: <http://wiki.servicenow.com/index.php?title=File:IncTemplateA.png> License: unknown Contributors: Guy.yedwab

Image:IncTemplate2.png Source: <http://wiki.servicenow.com/index.php?title=File:IncTemplate2.png> License: unknown Contributors: Guy.yedwab

Image:IncTemplateMod.png Source: <http://wiki.servicenow.com/index.php?title=File:IncTemplateMod.png> License: unknown Contributors: Guy.yedwab

Image:RecordProducer1.png Source: <http://wiki.servicenow.com/index.php?title=File:RecordProducer1.png> License: unknown Contributors: Guy.yedwab

Image:RecordProducer2.png Source: <http://wiki.servicenow.com/index.php?title=File:RecordProducer2.png> License: unknown Contributors: Guy.yedwab

Image:RecordProducer3.png Source: <http://wiki.servicenow.com/index.php?title=File:RecordProducer3.png> License: unknown Contributors: Guy.yedwab

Image:RecordProducer4.png Source: <http://wiki.servicenow.com/index.php?title=File:RecordProducer4.png> License: unknown Contributors: Guy.yedwab

Image:RecordProducer5.png Source: <http://wiki.servicenow.com/index.php?title=File:RecordProducer5.png> License: unknown Contributors: Guy.yedwab

Image:RecordProducer6.png Source: <http://wiki.servicenow.com/index.php?title=File:RecordProducer6.png> License: unknown Contributors: Guy.yedwab

Image:RecordProducer7.png Source: <http://wiki.servicenow.com/index.php?title=File:RecordProducer7.png> License: unknown Contributors: Guy.yedwab

Image:NYDB.png Source: <http://wiki.servicenow.com/index.php?title=File:NYDB.png> License: unknown Contributors: Guy.yedwab

Image:NYDB2.png Source: <http://wiki.servicenow.com/index.php?title=File:NYDB2.png> License: unknown Contributors: Guy.yedwab

Image:NYDB3.png Source: <http://wiki.servicenow.com/index.php?title=File:NYDB3.png> License: unknown Contributors: Guy.yedwab

Image:bsm_incident_config_field.png Source: http://wiki.servicenow.com/index.php?title=File:Bsm_incident_config_field.png License: unknown Contributors: Dawn.bunting

Image:BSMicon.png Source: <http://wiki.servicenow.com/index.php?title=File:BSMicon.png> License: unknown Contributors: Guy.yedwab

Image:bsm_incident_config_field02.png Source: http://wiki.servicenow.com/index.php?title=File:Bsm_incident_config_field02.png License: unknown Contributors: Dawn.bunting

Image:BSM_Affected_CI_Map.png Source: http://wiki.servicenow.com/index.php?title=File:BSM_Affected_CI_Map.png License: unknown Contributors: Dawn.bunting

Image:BSM_Affected_CI_Tasks.png Source: http://wiki.servicenow.com/index.php?title=File:BSM_Affected_CI_Tasks.png License: unknown Contributors: Dawn.bunting

Image:BSM_Affected_CI_Option.png Source: http://wiki.servicenow.com/index.php?title=File:BSM_Affected_CI_Option.png License: unknown Contributors: Dawn.bunting

Image:BSM_Affected_CI_List.png Source: http://wiki.servicenow.com/index.php?title=File:BSM_Affected_CI_List.png License: unknown Contributors: Dawn.bunting

Image:BSMinux.png Source: <http://wiki.servicenow.com/index.php?title=File:BSMinux.png> License: unknown Contributors: Guy.yedwab

Image:BSMinux2.png Source: <http://wiki.servicenow.com/index.php?title=File:BSMinux2.png> License: unknown Contributors: Guy.yedwab

Image:BSMinux5.png Source: <http://wiki.servicenow.com/index.php?title=File:BSMinux5.png> License: unknown Contributors: Guy.yedwab

Image:BSMinux3.png Source: <http://wiki.servicenow.com/index.php?title=File:BSMinux3.png> License: unknown Contributors: Guy.yedwab

Image:BSMinux4.png Source: <http://wiki.servicenow.com/index.php?title=File:BSMinux4.png> License: unknown Contributors: Guy.yedwab

Image:Tasks.png Source: <http://wiki.servicenow.com/index.php?title=File:Tasks.png> License: unknown Contributors: Guy.yedwab

Image:Icon-relatedincidentsUI15.png Source: <http://wiki.servicenow.com/index.php?title=File:Icon-relatedincidentsUI15.png> License: unknown Contributors: Fuji.publishing.user

Image:Kb_attach.png Source: http://wiki.servicenow.com/index.php?title=File:Kb_attach.png License: unknown Contributors: CapaJC, Pat.Casey, Steven.wood

Image:IncidenttoProblem.png Source: <http://wiki.servicenow.com/index.php?title=File:IncidenttoProblem.png> License: unknown Contributors: Guy.yedwab

Image:NewProblemForm.png Source: <http://wiki.servicenow.com/index.php?title=File:NewProblemForm.png> License: unknown Contributors: Guy.yedwab

Image:Resolution_Diagram.jpg Source: http://wiki.servicenow.com/index.php?title=File:Resolution_Diagram.jpg License: unknown Contributors: Eric.schroeder

Image:Itil_resolve1.jpg Source: http://wiki.servicenow.com/index.php?title=File:Itil_resolve1.jpg License: unknown Contributors: Eric.schroeder

Image:Close_email.png Source: http://wiki.servicenow.com/index.php?title=File:Close_email.png License: unknown Contributors: Eric.schroeder

Image:Itil_resolve4.jpg Source: http://wiki.servicenow.com/index.php?title=File:Itil_resolve4.jpg License: unknown Contributors: Eric.schroeder

Image:Notification.gif Source: <http://wiki.servicenow.com/index.php?title=File:Notification.gif> License: unknown Contributors: Vhearne

Image:Itil_resolve5.jpg Source: http://wiki.servicenow.com/index.php?title=File:Itil_resolve5.jpg License: unknown Contributors: Eric.schroeder

Image:Itil_resolve6.png Source: http://wiki.servicenow.com/index.php?title=File:Itil_resolve6.png License: unknown Contributors: Steven.wood

Image:ITIL_resolve7.png Source: http://wiki.servicenow.com/index.php?title=File:ITIL_resolve7.png License: unknown Contributors: Steven.wood

Image:VIP Callers.png Source: http://wiki.servicenow.com/index.php?title=File:VIP_Callers.png License: unknown Contributors: Steven.wood

Image:AutoClose1.png Source: <http://wiki.servicenow.com/index.php?title=File:AutoClose1.png> License: unknown Contributors: CapaJC

Image:ClosingBR.png Source: <http://wiki.servicenow.com/index.php?title=File:ClosingBR.png> License: unknown Contributors: Cheryl.dolan, Guy.yedwab

Image:ClosingUI.png Source: <http://wiki.servicenow.com/index.php?title=File:ClosingUI.png> License: unknown Contributors: Cheryl.dolan, Guy.yedwab

Image:IncReport1.png Source: <http://wiki.servicenow.com/index.php?title=File:IncReport1.png> License: unknown Contributors: Guy.yedwab

Image:IncReport2.png Source: <http://wiki.servicenow.com/index.php?title=File:IncReport2.png> License: unknown Contributors: Guy.yedwab

Image:IncReport4.png Source: <http://wiki.servicenow.com/index.php?title=File:IncReport4.png> License: unknown Contributors: Guy.yedwab

Image:IncReport5.png Source: <http://wiki.servicenow.com/index.php?title=File:IncReport5.png> License: unknown Contributors: Guy.yedwab

Image:INCRReport7.png Source: <http://wiki.servicenow.com/index.php?title=File:INCRReport7.png> License: unknown Contributors: Guy.yedwab

Image:INCRReport8.png Source: <http://wiki.servicenow.com/index.php?title=File:INCRReport8.png> License: unknown Contributors: Guy.yedwab

Image:INCHomepage.png Source: <http://wiki.servicenow.com/index.php?title=File:INCHomepage.png> License: unknown Contributors: Guy.yedwab