IT Support Tracking with Request Tracker (RT)

Archibald Steiner

AfNOG 2013

LUSAKA

Overview

- What is RT?
- A bit of terminology
- Demonstration of the RT web interface
- Behind the scenes – configuration options
- Requirements and technical details

RT is …

- A Trouble Ticket system
  - Lets a group of people manage tasks and requests
  - Full-featured web, e-mail or command line interface
- Under development since 1996
- Written in object-oriented Perl
  - Open source and fully customizable

RT Terminology

- *Ticket* – request for action
- *Queue* – collection of tickets belonging together
- *Requestor* – person requesting an action
- *Creator* – person creating the ticket
- *Owner* – person responsible for ticket

RT Demonstration

- The life of an email-generated ticket
- Directly creating tickets
- Searching
  - Can update all tickets matching criteria at once
  - Can bookmark a search

RT Configuration - General

- Users created with password and privileges
  - Or auto-created with first email
- Groups defined for varying access rights
  - Pseudo-groups reflect certain roles
- Create queues for different purposes
- Rights can be assigned globally or per queue for both groups or users

RT Configuration - Queues

- Scrips control actions on different events
- Templates format correspondence
- Keywords can be added
- Queue watchers can be defined
- Rights assigned to individuals or groups

Technical Requirements

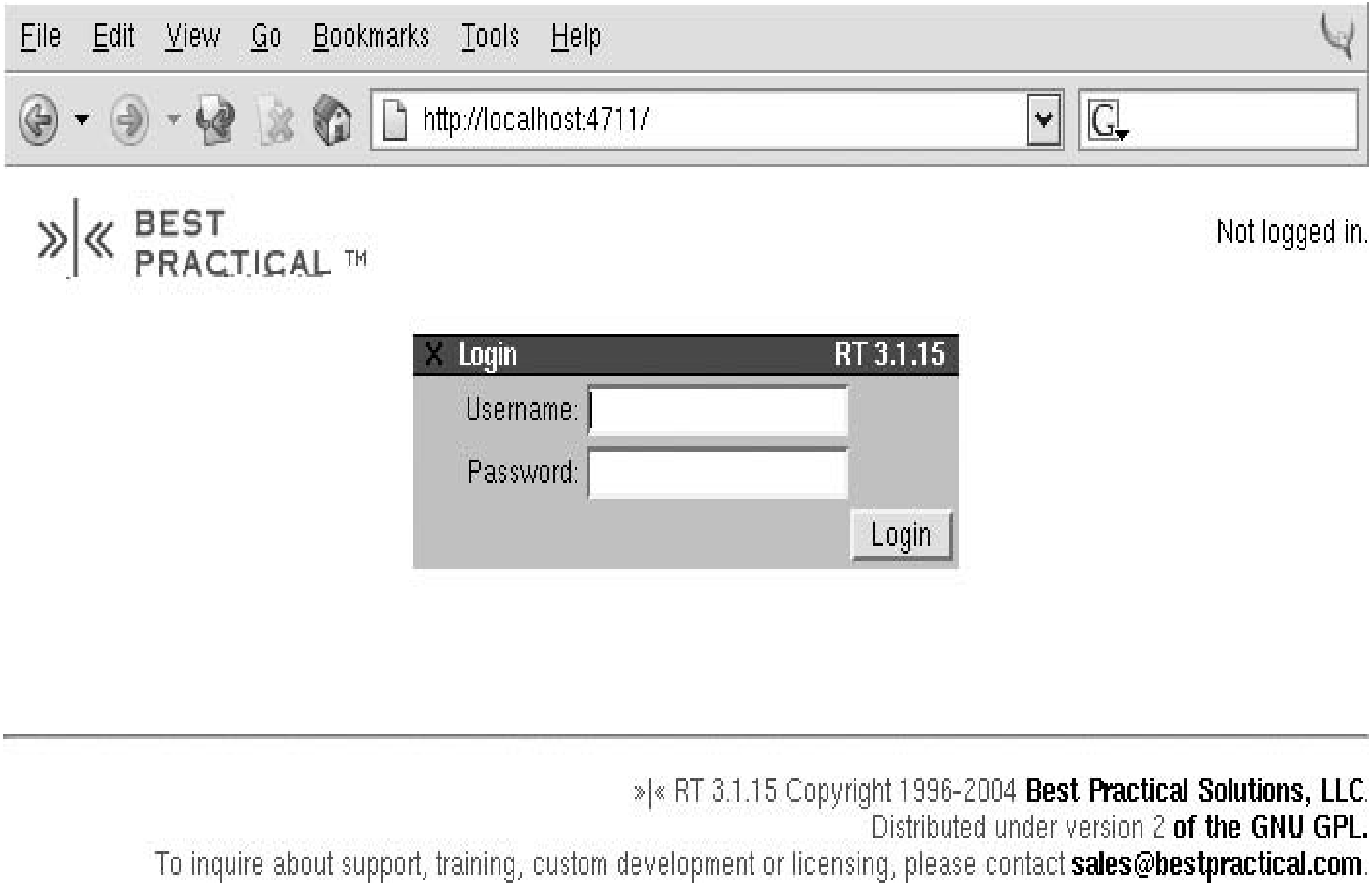
- Free download from www.bestpractical.com/rt/
  - Basic set-up requires ½ - 1 day
- *RT server* - Linux, FreeBSD, Solaris, Mac OS X
  - End user ports to Windows 2000 and XP available
- *SQL database* - MySQL 4 or PostgreSQL 7.3
  - Plans for commercial database support
- *Web server* - RT uses FastCGI protocol or Apache's mod_perl interpreter
- *Mail Transfer Agent*

More Technical Details

- Email interface
  - PGP signatures required for full functionality
- Command line interface
  - Requires a shell interface to the RT server
- Escalations
  - Need to run a cron script
- Changing RT
  - Perl and HTML
  - Online manual available
    - Version 2: fsck.com/rtfm/
    - Version 3: www.bestpractical.com/rt/docs.html

RT in action

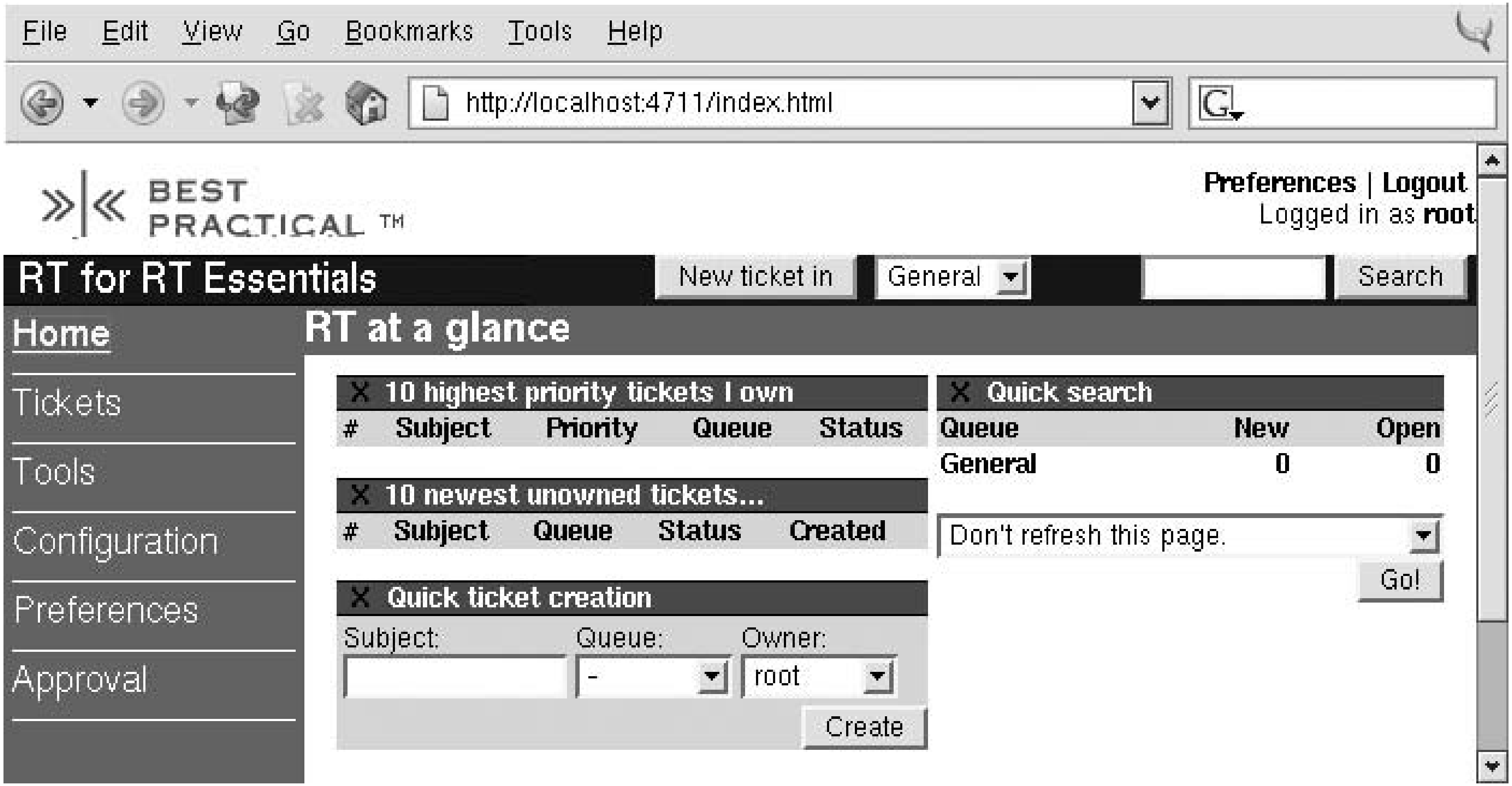
If you are working in an environment where there is an existing RT installation, your RT administrator most likely will give you a **username** and **password** as well as instructions on where the RT **login URL** is. When you first connect, you will see a login box, something like :


File Edit View Go Bookmarks Tools Help
http://localhost:4711/
BEST PRACTICAL TM
Not logged in.
Login RT 3.1.15
Username:
Password:
Login
»|« RT 3.1.15 Copyright 1996-2004 Best Practical Solutions, LLC.
Distributed under version 2 of the GNU GPL.
To inquire about support, training, custom development or licensing, please contact sales@bestpractical.com.

If you have a brand new RT instance, you can log in with the default username ***root*** and password ***password***.

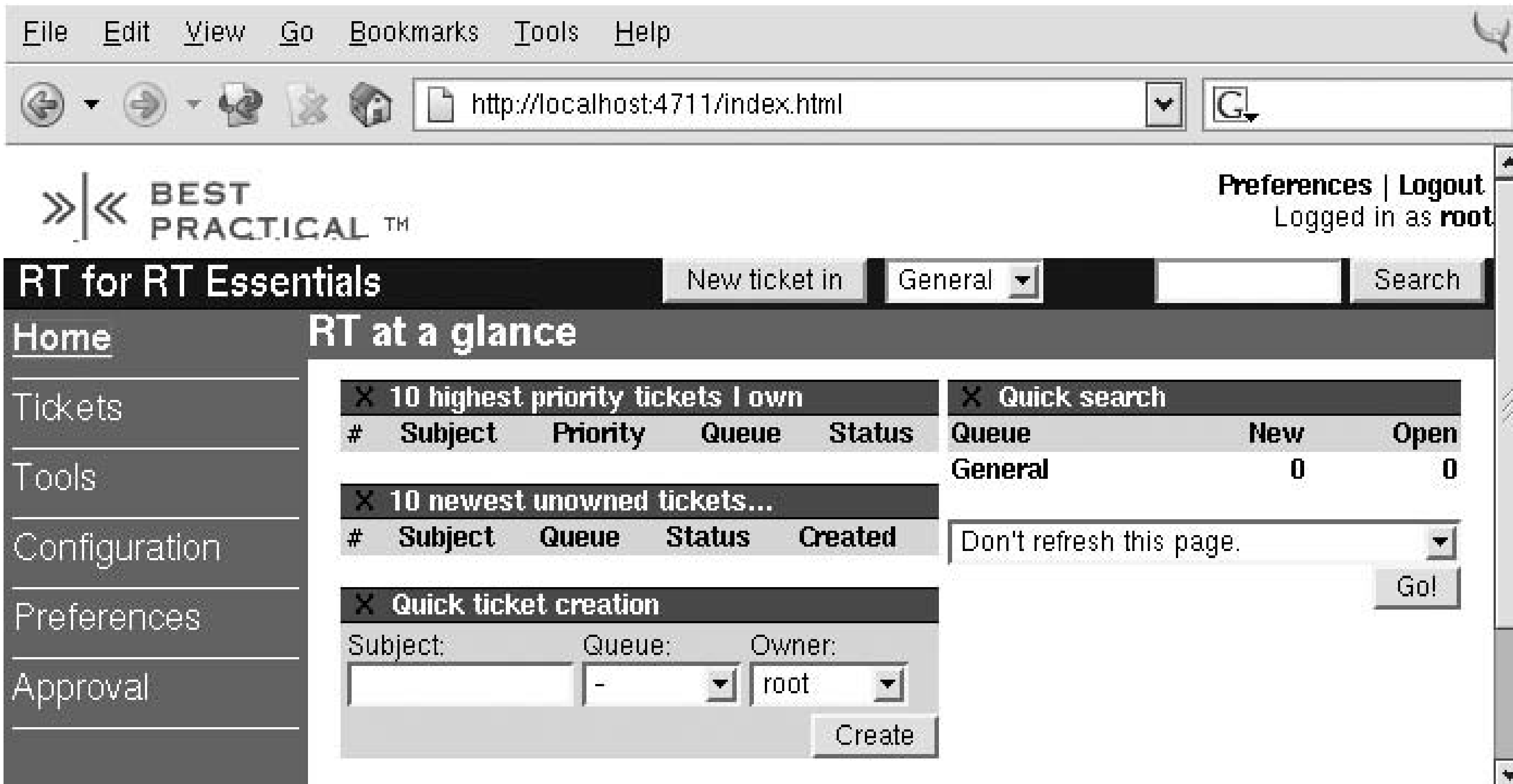
Once you've successfully authenticated yourself to RT, you will see the home page with the title

"**RT at a glance.**"



This screen/page gives you easy access to the tickets you own, tickets you've requested, tickets in the queues you watch, and interfaces for finding existing tickets and creating new ones.

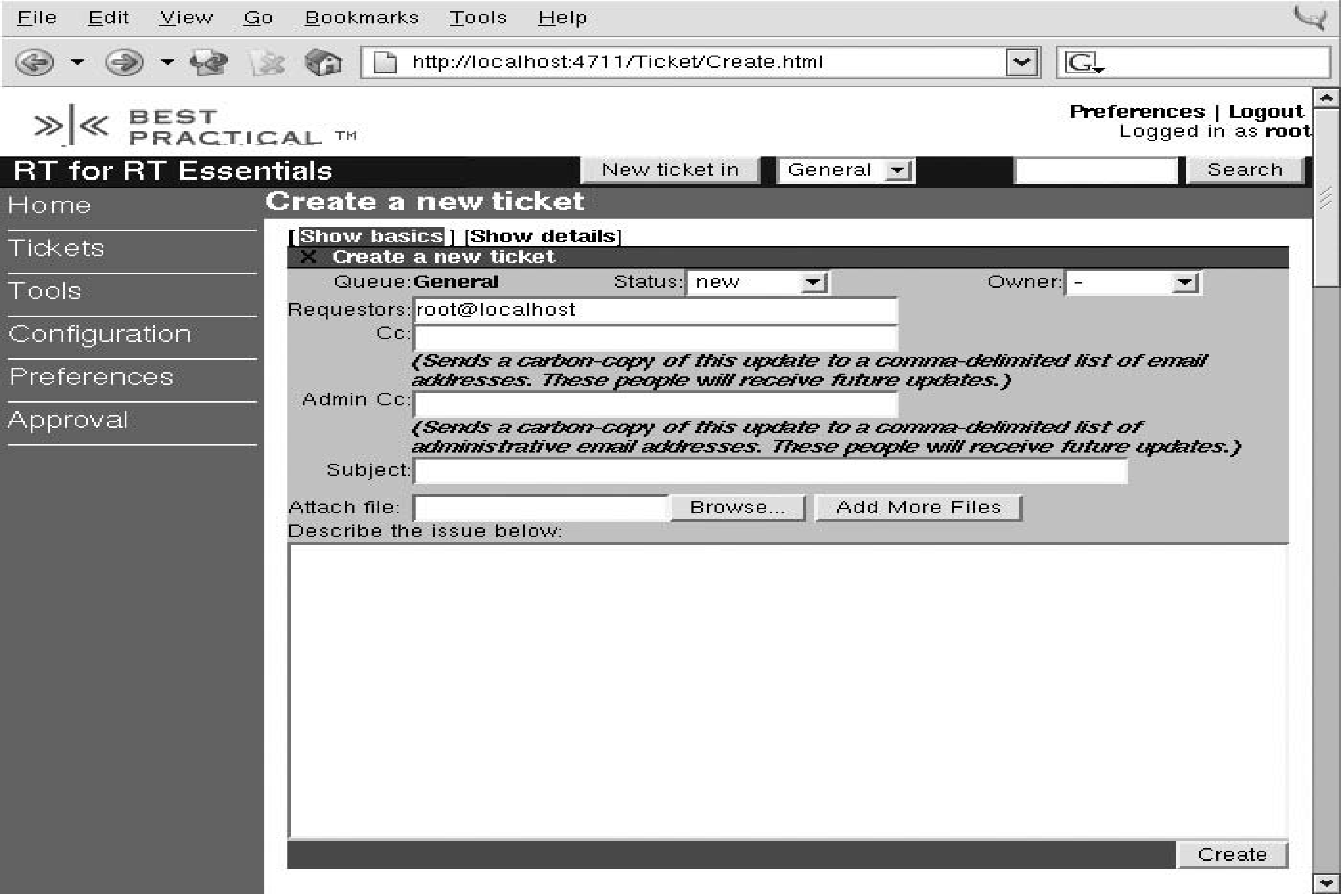
Along the left side of the page is the main site menu. This menu has links to all of the major things you can do with RT like, search for tickets, configure RT, change your references, and so on.



Creating a New Ticket

You can create a ticket from anywhere in RT; the top of every page has a small form with a button labeled ***New Ticket in and a drop-down menu listing the queues you*** can access.

Select the queue in which you want to create a new ticket, and click the New Ticket button. It will take you to the new ticket form.


File Edit View Go Bookmarks Tools Help
http://localhost:4711/Ticket/Create.html
BEST PRACTICAL ™
Preferences | Logout
Logged in as root
RT for RT Essentials
New ticket in
General
Search
Home
Tickets
Tools
Configuration
Preferences
Approval
Create a new ticket
[Show basics] [Show details]
Create a new ticket
Queue: General
Status: new
Owner: -
Requestors: root@localhost
Cc:
(Sends a carbon-copy of this update to a comma-delimited list of email addresses. These people will receive future updates.)
Admin Cc:
(Sends a carbon-copy of this update to a comma-delimited list of administrative email addresses. These people will receive future updates.)
Subject:
Attach file:
Browse...
Add More Files
Describe the issue below:
Create

The two most important fields in this basic form are the **<u>subject</u>** of the ticket and an **<u>entry box for a description</u>**; *these are the first items that people see when they look at your ticket*.

NB! *Tickets created in an Emergency queue outside of business hours might send a message to the on-call operator's SMS device*.

Tickets are identified by number. On a fresh install, the first ticket you create is numbered 1. Every new ticket after that gets a number one higher than the previous ticket.
If your RT instance is configured to send mail when a ticket is created (as it is by default), then you should get an email message shortly with a summary of the ticket **you** created.

When a new ticket is created, RT may run some user-defined actions—called ***scrips***. These scrips can do almost anything, but the most common type of scrip sends mail to the queue's watchers informing them of the new ticket.

Other scrips might send a notification to an alphanumeric pager, or even print the ticket's info to a local line printer.

Ticket Display Page

The important part of handling a request is doing the work, but once you've completed the task, you need to update the ticket to reflect your work.

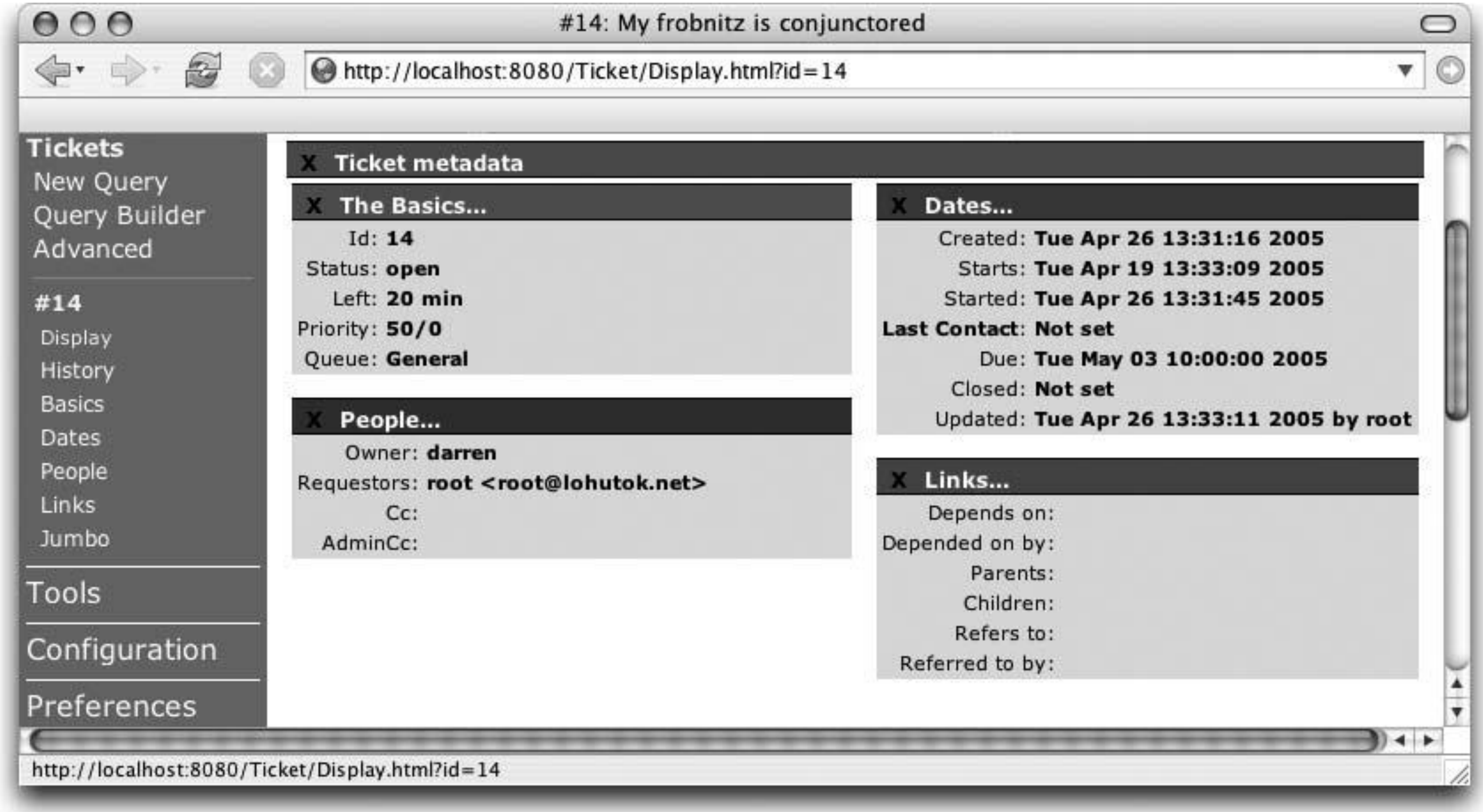
So how do you update a ticket?

•First, you need to go the main display page for that ticket. Clicking on a ticket's ID or Subject from the home page is one way to get there.

•If you click on the name of a queue in the Quick Search box on the right of the home page, you can preview all the tickets in that queue and select your ticket from the list.

•You also can enter a ticket number in the search box on the top right of every page, and click Search to get there, etc,

Below is a Ticket Display Page



The metadata associated with a ticket is divided into four main categories—Basics, Dates, People, and Links—each of which tracks a different aspect of the ticket

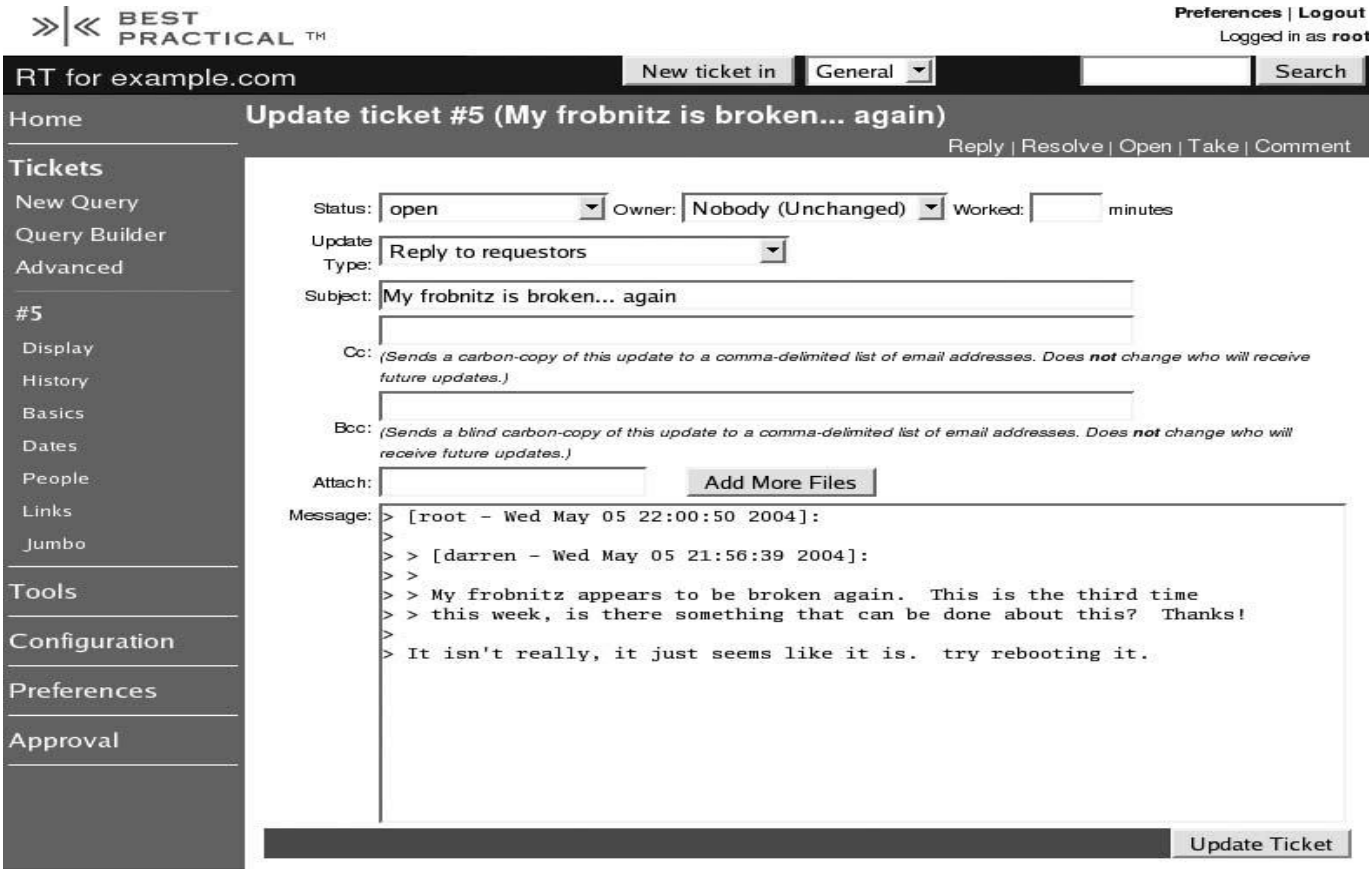
The **Basics category** includes obvious things, like the subject, status, priority, and queue of a ticket. It also includes elements like the estimated amount of time to complete the work, the amount of time worked on the ticket—which can be very useful for tracking the scale of requests—and the amount of time left before the initial estimated completion date passes. This area displays any custom fields attached to the ticket as well.

The **Dates category** includes the start date of the ticket, the date the actual work started, when the requestor was last contacted about the request, and the date by which the work must be completed. If you and other users maintain these dates accurately, they can be used to generate reports on how long requests take to be fulfilled. Dates can be entered in a variety of formats, and, as long as the format is unambiguous, RT will figure it out.

The **People category** lists watchers, requestors, and the ticket's owner. Long-lived tickets have a tendency to accumulate many watchers over time, as more man-power is added to fulfilling a request and managers of various sorts start getting interested in why the request is taking so long to be finished. The form to edit a ticket's People data functions as a search form as well as a modification form. It can find users and groups in RT based on simple searches, remove watchers from the ticket, and change the owner of the ticket by changing the value in the Owner drop-down menu.

The **Links category** contains all the links between the current ticket, other tickets, and the outside world. You can merge tickets and link them with other tickets through this form. We will soon talk about “Merging Duplicate Tickets” and “Associating Related Tickets”.

Replying to (and Commenting on) a Ticket "UPDATE"



Replying to (and Commenting on) a Ticket

You reply to a ticket by clicking the **Reply** link at the top right of the ticket display page or beside an individual item in the ticket's history. The same form creates either replies or comments, depending on what you select for Update Type. From this form, it's simple to reply to an **end user**, mark down how much time you spent composing your response, and close the ticket.

Escalating a Ticket

- Each ticket has a priority.

- Priority is a way to indicate relative importance. It can be any integer. Most organizations use the range 0-100.

- Every queue has a default priority for new tickets if you don't explicitly set one.

- To escalate the priority of a ticket, set the priority of a ticket to a higher number.

NB!!. The priority field is in the Basics category.

*Queues can be configured to automatically adjust the priority of tickets over time. Based on the current priority of the ticket, the priority escalates every day so that it reaches its final priority on a given due date.**

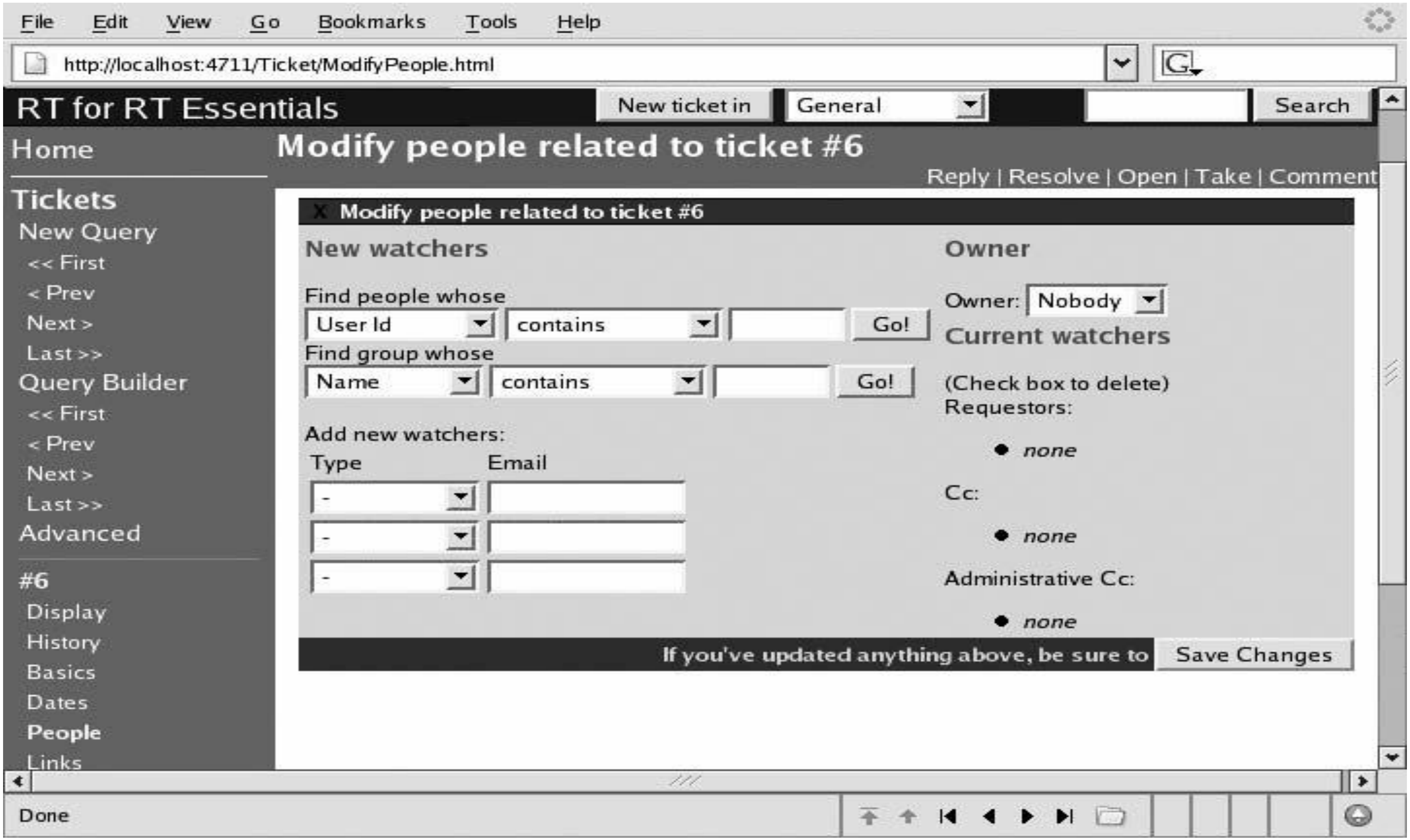
Assigning a Ticket

Tickets can have an **owner**; the user responsible for working on the ticket or for coordinating the work.
To assign a ticket to someone, go to the People form from the ticket display page, and select the user from the Owner drop-down list. This list contains the usernames of all the users allowed to own tickets in the ticket's **current queue**.

You can assign only tickets that you own or that are unowned. If you need to reassign a ticket that you do not own, you can **steal** the ticket and then assign it to someone else.

Tickets you can steal will display a Steal link next to Reply and Comment in the upper right corner of the ticket display page. Not all users have access to steal tickets.

Assigning a ticket



Resolving a Ticket

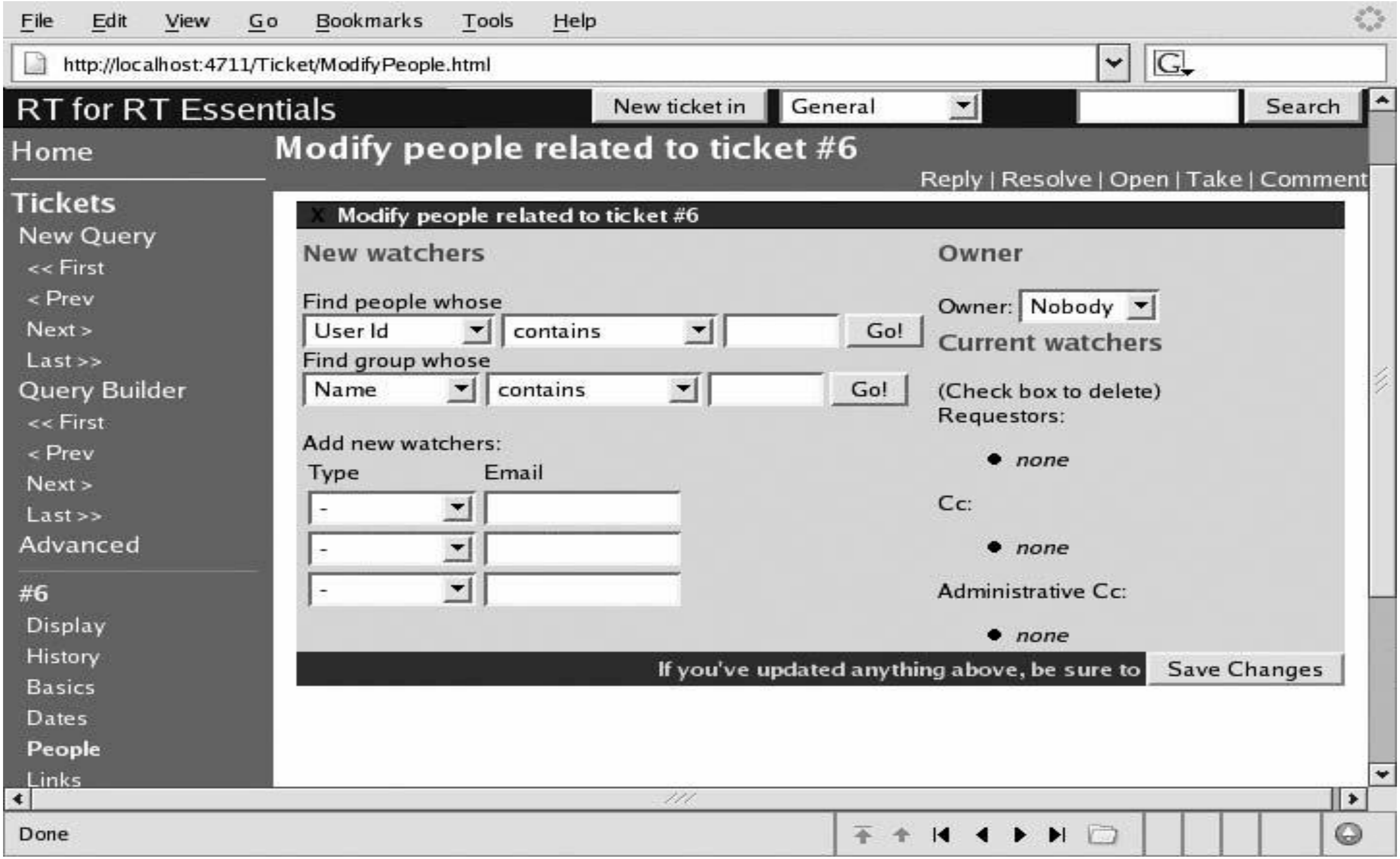
When you are satisfied that the ticket you are working on is finished, you can change its status to **resolved**, so other users know it doesn't need any more work. *This process is known as resolving the ticket*.
To modify a ticket's status, just click *Resolve in* the upper right hand corner of any ticket page.
The form used for resolving a ticket allows you to send a reply to the ticket's requestor and watchers.

Certain scrips run when a ticket is resolved. The default scrips send mail to the ticket's watchers.

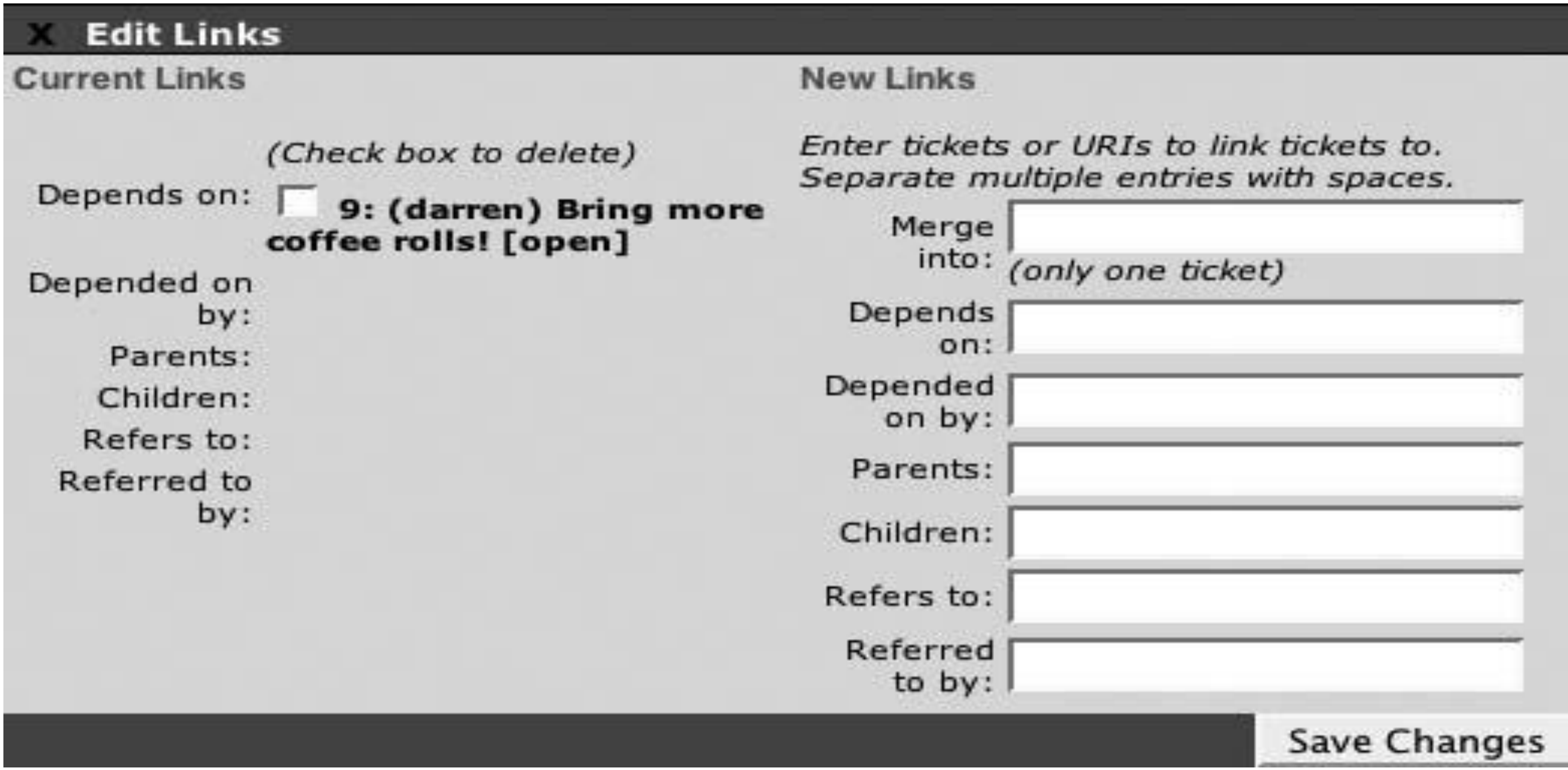
Merging Duplicate Tickets

Sometimes, multiple people submit reports for the same problem. This is especially likely if you've got a big problem in a busy environment. When it happens, you need a way to tell RT that the multiple tickets are actually the same request. RT lets you collapse tickets together in a process called *Merging.*

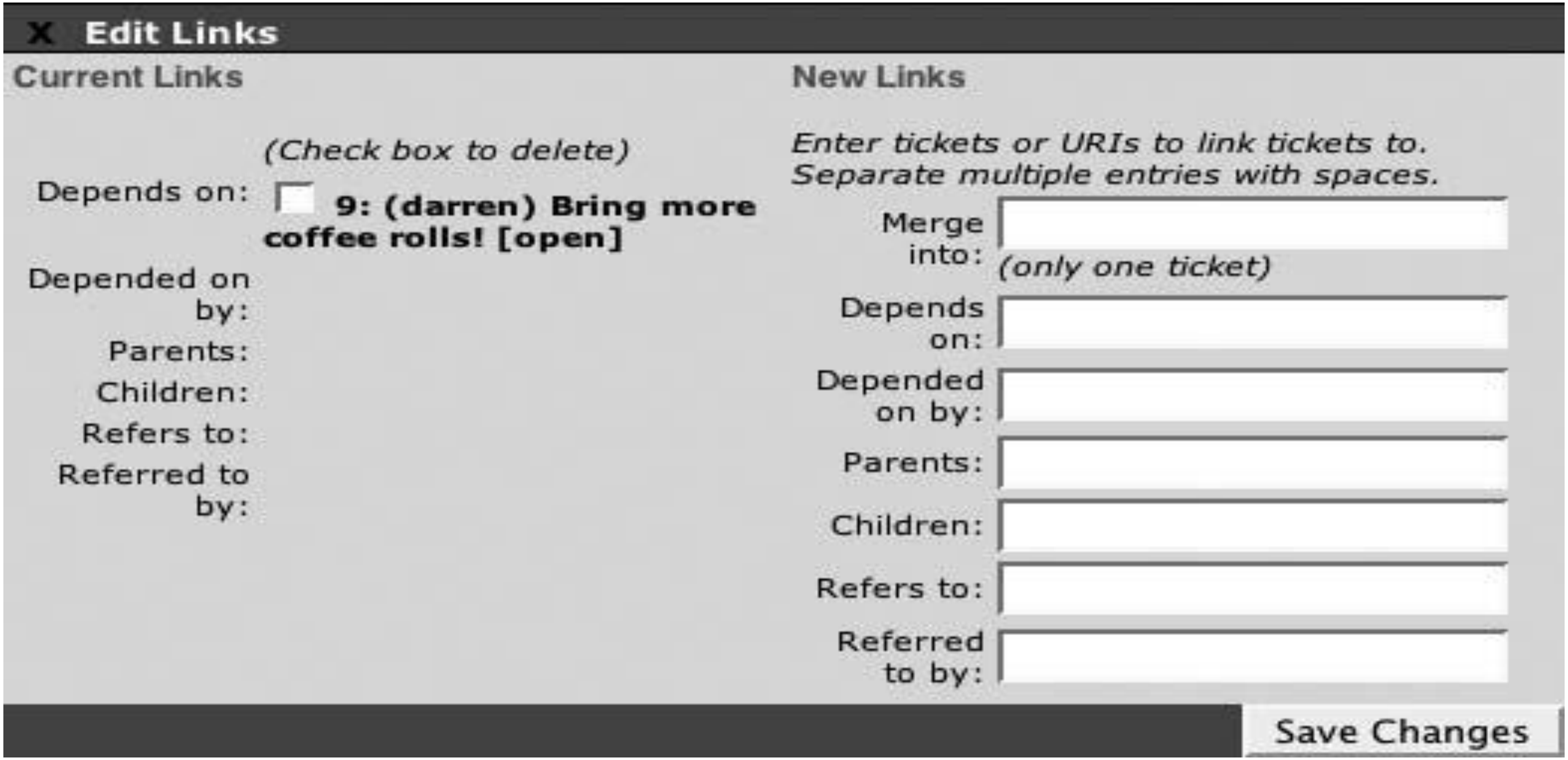
To do a merge go to the Links form for the ticket you want to merge. *Left down*



This form has two major sections, **Current Links** and **New Links**.
The Current Links section describes any existing relationships that the ticket has and provides a simple editing interface.
The New Links section allows you to define new relationships.



To merge one ticket into another, enter the number of the target ticket in the Merge Into Field, and submit the form. You can merge any number of tickets this way.



Associating Related Tickets

Sometimes a ticket represents a complex issue or difficult request, and you may need to break it down into smaller, more manageable pieces. When this happens, it makes sense to create tickets for these smaller tasks, and associate them with the original ticket.

RT provides a *Depends On/Depended On By relationship for these cases.*

From the Links form of the new ticket, enter the original ticket's number in the *Depended On By field, and save your changes.*

Associating Related Tickets

You can create this relationship from the other direction as well: on the Links form for the original ticket you can enter the new ticket's number in the Depends On field.

Once this relationship is established, the parent ticket cannot be resolved until the child ticket is resolved. A ticket can have multiple parents and multiple children, which can be used to create arbitrarily complex and interdependent workflows.

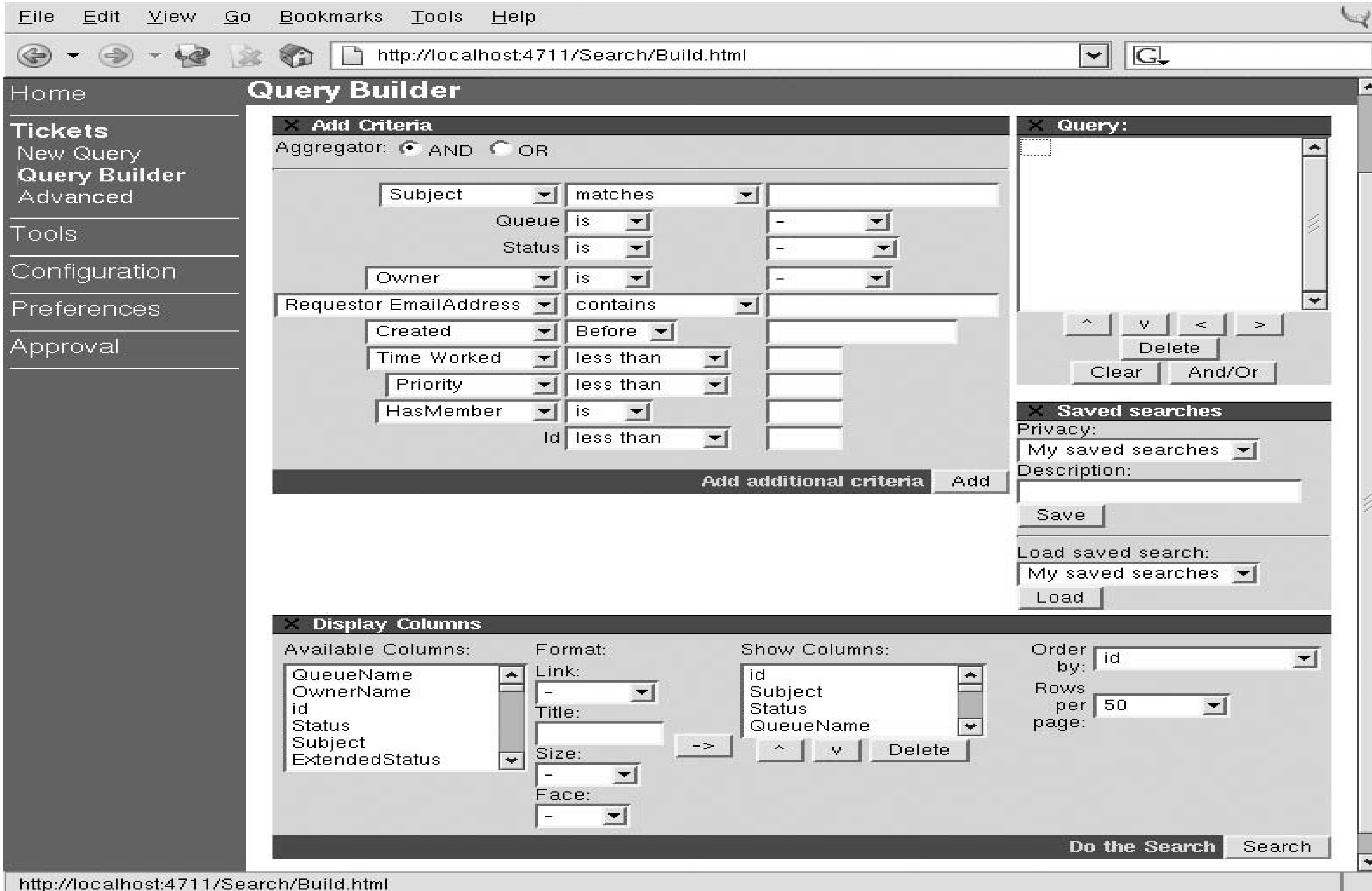
Searching for Tickets

In an active RT instance, with thousands of tickets, finding the ones you are interested in can quickly become a chore. Luckily, all of the ticket metadata we've been harping about is searchable.

To start a new search, click on the *Tickets link in the* main menu. This takes you to an empty ticket search form,

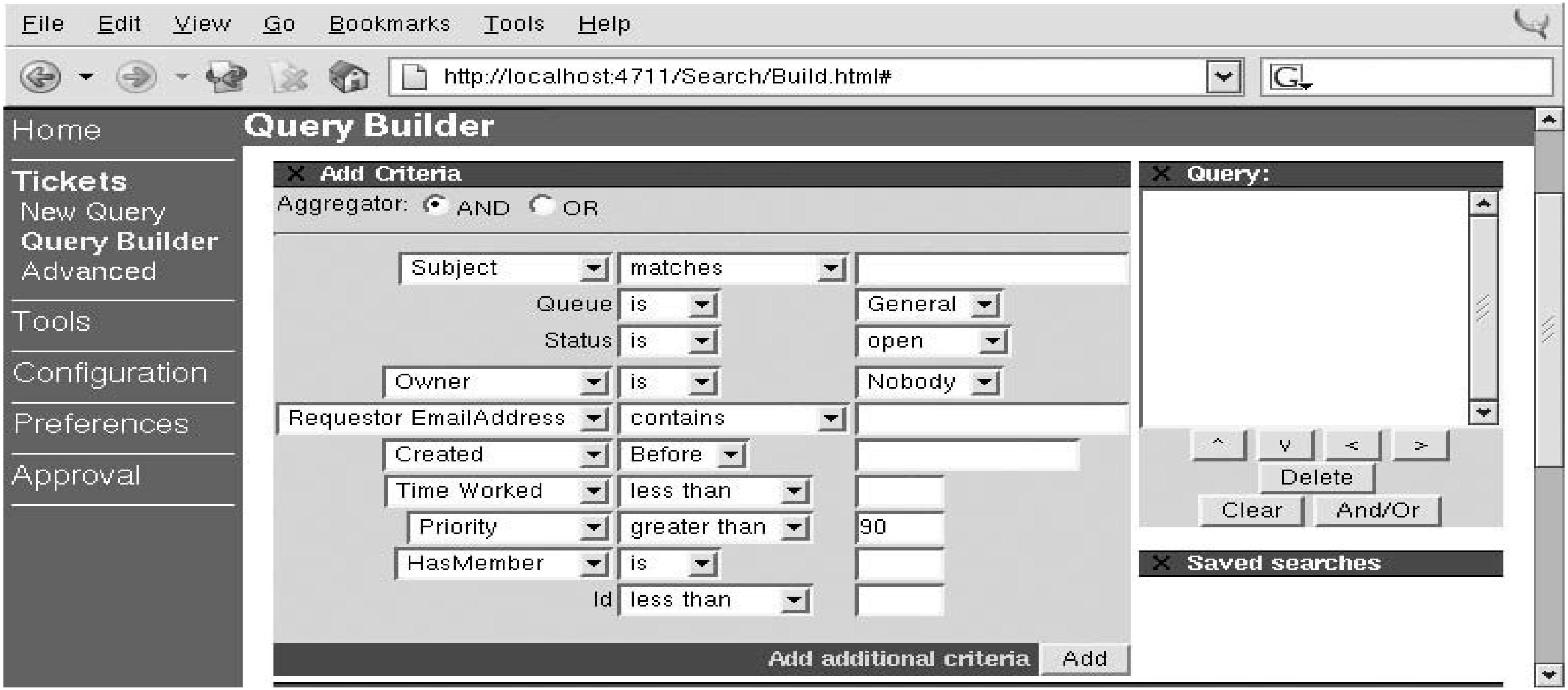
next screen, a very flexible and powerful search tool.

Search form


File Edit View Go Bookmarks Tools Help
http://localhost:4711/Search/Build.html
Home
Tickets
New Query
Query Builder
Advanced
Tools
Configuration
Preferences
Approval
Query Builder
Add Criteria
Aggregator: AND OR
Subject matches
Queue is
Status is
Owner is
Requestor EmailAddress contains
Created Before
Time Worked less than
Priority less than
HasMember is
Id less than
Add additional criteria Add
Query:
Delete
Clear And/Or
Saved searches
Privacy:
My saved searches
Description:
Save
Load saved search:
My saved searches
Load
Display Columns
Available Columns:
QueueName
OwnerName
id
Status
Subject
ExtendedStatus
Format:
Link:
Title:
Size:
Face:
Show Columns:
id
Subject
Status
QueueName
Delete
Order by: id
Rows per page: 50
Do the Search Search
http://localhost:4711/Search/Build.html

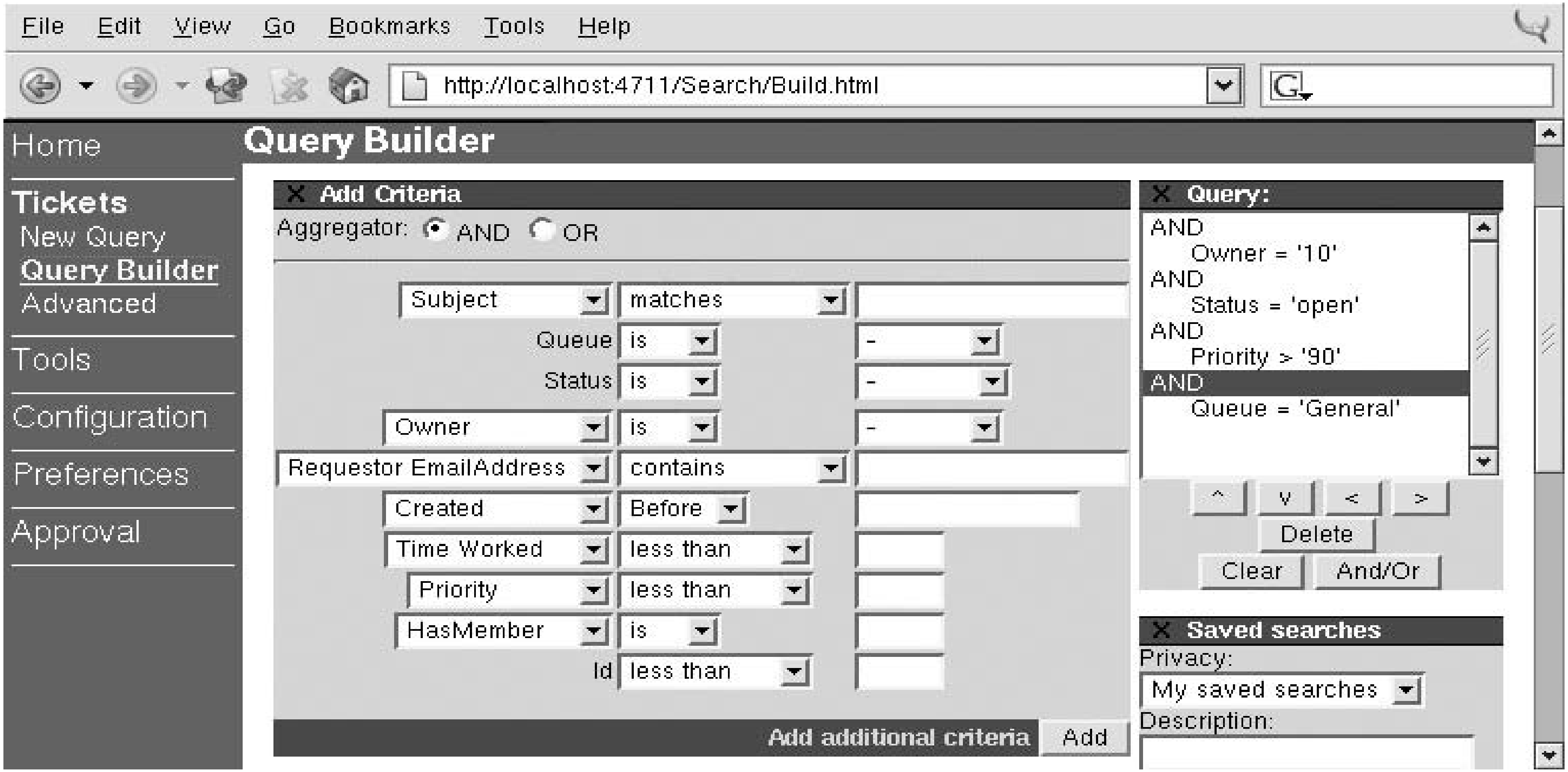
The Add Criteria section is less complicated than it looks. Each criterion you want to add is represented by a row of form elements. For example, the selected options in the figure below search for tickets where the queue is **General, the status is open, the** owner is **Nobody, and the priority is greater than 90.**

Search for tickets



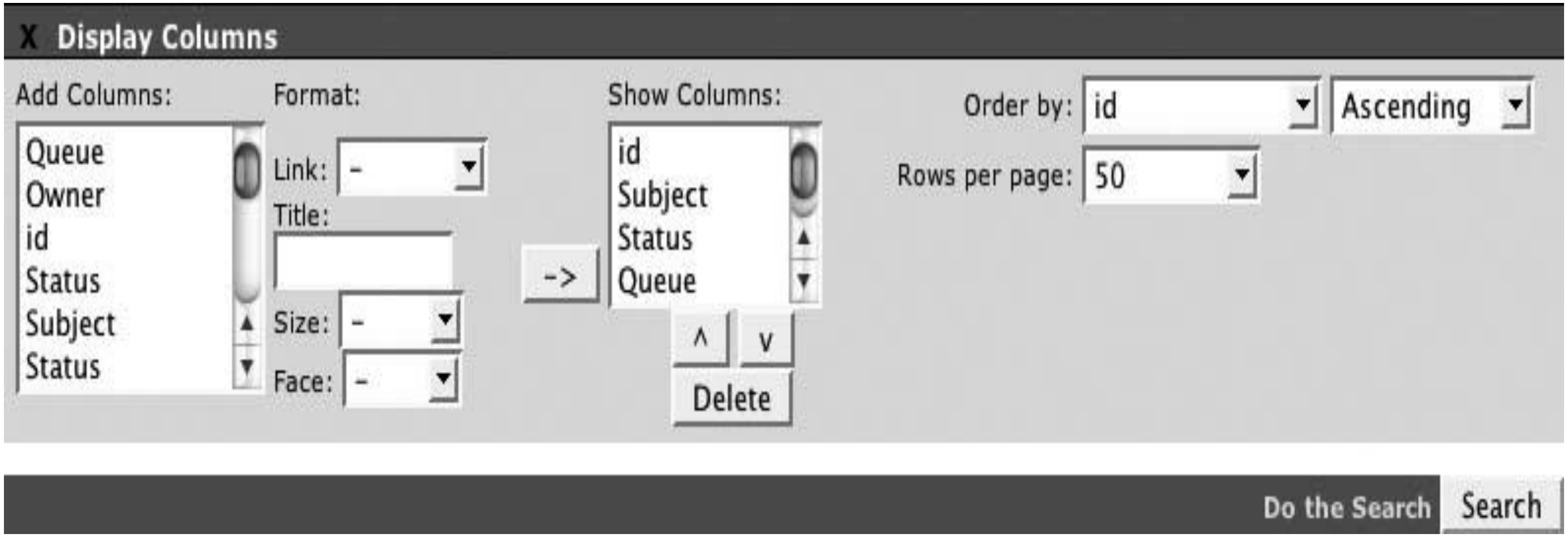
When you click the *Add button, it adds all the criteria to the query at* once. The next screen clears the Add Criteria section, but it lists the criteria in the Query section toward the upper right of the page.

Constructed query



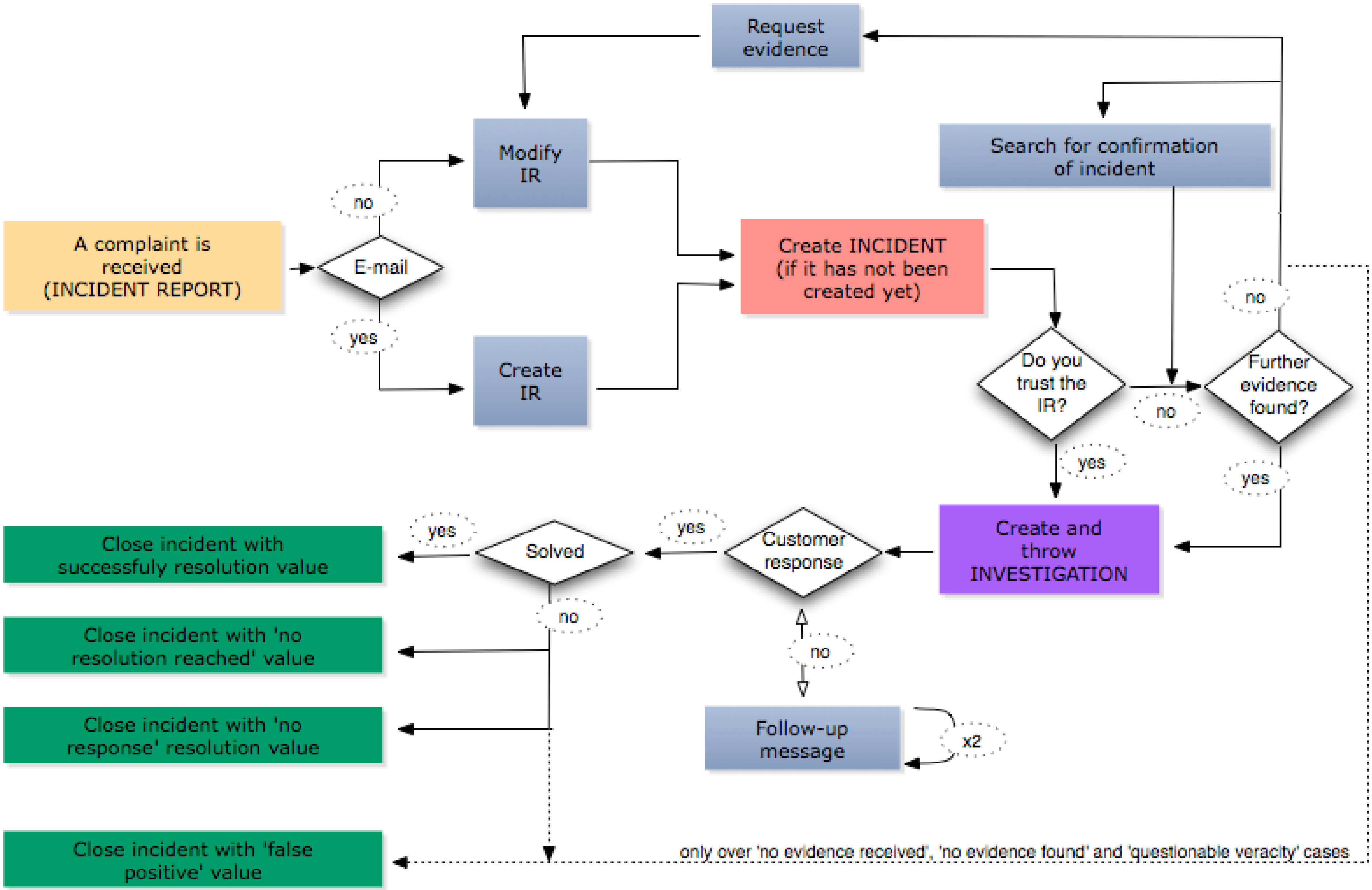
The query builder also allows you to choose the fields you want to display when listing your search results. The default display shows many fields, but you can limit the display to only those fields you want in the Display Columns box at the bottom of the search form page, shown below.

Display Columns



Once you've created your query and chosen the fields you want to display, execute the search by clicking the Search button at the bottom of the form.

SLA compliance can be measured by response times to Incident Reports. The software allows for the configuration of SLA timers which are customized by the RTIR administrator. This should be configured according to existing CSIRT procedures and policies.


Request evidence
Modify IR
Search for confirmation of incident
no
A complaint is received (INCIDENT REPORT)
E-mail
Create INCIDENT (if it has not been created yet)
yes
no
Create IR
Do you trust the IR?
no
Further evidence found?
yes
yes
Close incident with successfuly resolution value
yes
Solved
yes
Customer response
Create and throw INVESTIGATION
no
Close incident with 'no resolution reached' value
no
Close incident with 'no response' resolution value
Follow-up message
x2
Close incident with 'false positive' value
only over 'no evidence received', 'no evidence found' and 'questionable veracity' cases