Redmine - Feature #3369
Ability to Only Allow Users from Certain Domain to Register
2009-05-16 01:12 - Omar Ramos

Status: New
Priority: Normal
Assignee: 
Category: Accounts / authentication
Target version: Candidate for next major release
Resolution: 
Start date: 2009-05-16
Due date: 
% Done: 0%
Estimated time: 10.00 hours

Description
For using Redmine in an internal company situation it would be nice if we could do one or two of the following (some of this may require enhancements slated for v0.9 and the improved permissions):

1. Set in Redmine's backend the domain that we would like to allow registrations from (in our case it would be our school's domain name which employees have emails addresses from). This would allow us to make our Redmine site public but not have to worry about random robots or visitors coming to the site and signing up for an account.

2. In addition to being able to choose the email domain, it would be nice to be able to set the permissions of these registrants automatically. For example, it would be nice if any of the users from our domain would automatically be placed into Redmine with permissions that would allow them to create their own projects (I believe this type of permission will be available in 0.9 so that registered users can create their own projects). This would be extremely useful if we wanted to use Redmine generically for Project Management at the college, as it is also useful for things besides coding project management :-).

Related issues:
Related to Redmine - Feature # 14341: Ability to self-register only from cera... Closed
Related to Redmine - Feature # 33216: /my/account: Prevent users from changin... New

History
#1 - 2009-05-16 06:37 - Adam Piotr Żochowski

Why don't you just setup yourself against the LDAP?

#2 - 2009-05-16 23:19 - Omar Ramos

Because our college is a little behind-the-times in that respect, we have an Active Directory server, but it is poorly organized, though I guess in this case permissions wouldn't matter, just logging in (though I do know that LDAP auth systems usually have trouble with AD, for example Joomla.).

And I'm sure that not every organization has an Active Directory server so they may not have that option available to them.

#3 - 2009-05-17 05:19 - Adam Piotr Żochowski

Thomas Löber wrote a year ago documentation on setting up Redmine with Apache and SSPI ( see [http://www.redmine.org/boards/2/topics/127](http://www.redmine.org/boards/2/topics/127)). This removes problems with AD/LDAP authentications. Only problem is maintaining users (adding them). The only thing you will need is to copy NTLogins information into Redmine (I do it nightly).

None of my users request for accounts (typically by the time they need redmine, they are already there).
None of my users have to deal with passwords (since it piggybacks through ntlm/sspi authentication).

If I can add a something to Thomas's docs, then it would be:

    SSPIOfferBasic Off
    ErrorDocument 401 “Sorry, your NT authentication is not recognized.”
SSPIOfferBasic controls what to do with browsers that do not support NTLM based authentication (password is sent cleartext). ErrorDocument 401 is special document / text you want to present to users that are not part of your windows domain.

All other options already enforce domain user requirement

Kind regards

#4 - 2017-05-03 13:25 - Go MAEDA
- Related to Feature #14341: Ability to self-register only from ceratain domains added

#5 - 2020-01-09 06:30 - Go MAEDA
- Category changed from Permissions and roles to Accounts / authentication

+1
This feature can prevent potential information leakage.

If an employee has changed the email address of their Redmine account from the organization's email address to their personal email address, notifications are delivered to their home. It is problematic for some organizations.

We can avoid or reduce the problem if Redmine has "Allowed email domains" and "Disallowed email domains" settings that limit email addresses that can be set for accounts. For attachments, we already have similar settings "Allowed extensions" and "Disallowed extensions" (#20008).

#6 - 2020-03-12 06:33 - Yuichi HARADA
- File setting-restrict-domains.png added
- File 3369-restrict-domains.patch added

Go MAEDA wrote:

We can avoid or reduce the problem if Redmine has "Allowed email domains" and "Disallowed email domains" settings that limit email addresses that can be set for accounts. For attachments, we already have similar settings "Allowed extensions" and "Disallowed extensions" (#20008).

Added settings for "Allowed email domains" and "Disallowed email domains" to "Administration > Settings > Users".

setting-restrict-domains.png

I created a patch that restricts domains.

diff --git a/app/models/email_address.rb b/app/models/email_address.rb
index 4cd9c5dfd..85b77fc3a 100644
--- a/app/models/email_address.rb
+++ b/app/models/email_address.rb
@@ -36,6 +36,7 @@ class EmailAddress < ActiveRecord::Base
  validates_length_of :address, :maximum => User::MAIL_LENGTH_LIMIT, :allow_nil => true
  validates_uniqueness_of :address, :case_sensitive => false,
  :if => Proc.new { |email| email.address_changed? && email.address.present?}
+  validate :validate_domain, :if => Proc.new(email) email.errors[:address].blank? && email.address.present?

   safe_attributes 'address'
@@ -117,4 +118,29 @@ class EmailAddress < ActiveRecord::Base
     Token.where(:user_id => user_id, :action => tokens).delete_all
   end
 end
+
+  def validate_domain
+    denied, allowed = 
+      [:email_domains_denied, :email_domains_allowed].map do |setting|
+        Setting.__send__ (setting)
+      end
+    invalid = false
+    domain = address.sub(/\A.*@/ , "
+    if denied.present? && domain_in? (domain, denied)
+      invalid = true
+    end
+    if allowed.present? && !domain_in? (domain, allowed)
+      invalid = true
+    end
+    errors.add (:address, l (:error_domain_not_allowed, :domain => domain)) if invalid
+  end
+
+  def domain_in? (addr, domains)
+    domain = addr.downcase.sub(/\A.*@/ , '')
+    unless domains.is_a? (Array)
+      domains = domains.to_s.split (/\s+/, )
+    end
+    domains = domains.map{|s| s.downcase.sub(/\A.*@/ , '')}.reject(& :blank?)
+    domains.include? (domain)
+  end
end

diff --git a/app/views/settings/_users.html.erb b/app/views/settings/_users.html.erb
index ab61d7c21..8d446317a 100644
--- a/app/views/settings/_users.html.erb
+++ b/app/views/settings/_users.html.erb
@@ -4,6 +4,12 @@
 <p>
 <%= setting_text_field :max_additional_emails, :size => 6 %></p>

 <p>
 <%= setting_check_box :unsubscribe %></p>
+
+  <p><%= setting_text_area :email_domains_allowed %></p>
+  <em class="info">%= l(:text_comma_separated) %:<%= l(:label_example) %>: foo.example.com, bar.example.org</em></p>
+
+  <p><%= setting_text_area :email_domains_denied %></p>
+  <em class="info">%= l(:text_comma_separated) %:<%= l(:label_example) %>: baz.example.net, qux.example.biz</em></p>
 <div>

 <fieldset class="box tabular settings">

diff --git a/config/locales/en.yml b/config/locales/en.yml
index 7bb506c57..7d1c793e5 100644
--- a/config/locales/en.yml
+++ b/config/locales/en.yml
@@ -232,6 +232,7 @@
 en:
   error_can_not_delete_auth_source: "This authentication mode is in use and cannot be deleted."

2020-04-06 3/4
error_spent_on_future_date: "Cannot log time on a future date"
error_not_allowed_to_log_time_for_other_users: "You are not allowed to log time for other users"
+ error_domain_not_allowed: "Domain %{domain} is not allowed"

mail_subject_lost_password: "Your %{value} password"
mail_body_lost_password: "To change your password, click on the following link:"
@@ -476,6 +477,8 @@ en:
    setting_force_default_language_for_loggedin: Force default language for logged-in users
    setting_link_copied_issue: Link issues on copy
    setting_max_additional_emails: Maximum number of additional email addresses
+ setting_email_domains_allowed: Allowed email domains
+ setting_email_domains_denied: Disallowed email domains
    setting_search_results_per_page: Search results per page
    setting_attachment_extensions_allowed: Allowed extensions
    setting_attachment_extensions_denied: Disallowed extensions
diff --git a/config/settings.yml b/config/settings.yml
index d33523aeb..4dee88b26 100644
--- a/config/settings.yml
+++ b/config/settings.yml
@@ -53,6 +53,10 @@ password_max_age:
  max_additional_emails:
  format: int
  default: 5
+email_domains_allowed:
+ default:
+email_domains_denied:
+ default:
  # Maximum lifetime of user sessions in minutes
  session_lifetime:
  format: int

#7 - 2020-03-19 15:44 - Go MAEDA
- Target version set to Candidate for next major release

#8 - 2020-03-31 09:07 - Go MAEDA
- Related to Feature #33216: /my/account: Prevent users from changing their Email [redmine 4.1.0 stable] added

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>setting-restrict-domains.png</td>
<td>96.6 KB</td>
<td>2020-03-12</td>
<td>Yuichi HARADA</td>
</tr>
<tr>
<td>3369-restrict-domains.patch</td>
<td>7.32 KB</td>
<td>2020-03-12</td>
<td>Yuichi HARADA</td>
</tr>
</tbody>
</table>

2020-04-06 4/4