Redmine - Feature #3369
Allowed/Disallowed email domains settings to restrict users' email addresses

2009-05-16 01:12 - Omar Ramos

Status:	Closed	**Start date:**	2009-05-16
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	10.00 hours
Target version:	4.2.0		
Resolution:	Fixed		

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**
Duplicated by Redmine - Feature # 12855: Sometime,we need limit register emai...	**Closed**

Associated revisions

Revision 19735 - 2020-04-30 11:00 - Go MAEDA

Allowed/Disallowed email domains settings to restrict users' email addresses (#3369).

Patch by Yuichi HARADA and Go MAEDA.

Revision 19736 - 2020-04-30 11:02 - Go MAEDA

Update locales (#3369).

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). 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 %>
```

```
+    <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 %>
+    <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."
   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

#9 - 2020-04-27 04:07 - Go MAEDA

- File 3369-restrict-domains-v2.patch added

I have updated the patch:

- Changed the domain name matching to support subdomains. Now **"example.com"** matches "example.com", "foo.example.com", and "bar.example.com". Putting a dot at the beginning of the domain name like **".example.com"** matches "foo.example.com" and "bar.example.com" but "example.com". If you want to only allow email address with "example.com" domain excluding subdomains, set "example.com" to "Allowed email domains" and ".example.com" to "Disallowed email domains"
- Made valid_extension? and extension_in? as class methods like attachment.rb
- Moved some tests from test/unit/user_test.rb to test/unit/email_address_test.rb that has been added in r19661
- Fixed RuboCop offenses that were hidden by .rubocop_todo.yml

#10 - 2020-04-28 05:30 - Ryoh HAMADA

Thank you for creating the patch.

Recent versions of Redmine allow users to register multiple email addresses.
This is a useful feature.

However, on the other hand, there is a possibility that information will be leaked to the email address added or changed by the user via email notification.
If this function is available, it would be very effective in suppressing such risks if email addresses can be restricted.

#11 - 2020-04-28 17:23 - Go MAEDA

- Target version changed from Candidate for next major release to 4.2.0

Let's deliver this feature in Redmine 4.2.0.

#12 - 2020-04-29 08:38 - Go MAEDA

- Subject changed from Ability to Only Allow Users from Certain Domain to Register to Allowed/Disallowed email domains settings to restrict users' email addresses

#13 - 2020-04-29 09:03 - Go MAEDA

- File 3369-restrict-domains-v3.patch added

I have updated the patch again.

- Changed the error message when the domain is not allowed from **"Email contains a domain not allowed (example.com)"** to simpler **"Email is invalid"** because the former detailed error message may give attackers useful hints to avoid restrictions especially on /account/register page
- Moved the Allowed/Disallowed email domains settings to after "Maximum number of additional email addresses" setting in order to put the email related settings together

#14 - 2020-04-30 11:03 - Go MAEDA

- Status changed from New to Closed
- Assignee set to Go MAEDA
- Resolution set to Fixed

Committed the patch.

#15 - 2020-05-21 06:45 - Kuniharu AKAHANE

Maeda-san, Thank you very much for the patch.
Our customer need this feature to keep the information security level.

> *For example, Control the destination of notification e-mail which includes confidential and/or secret information.*

Would be happy if it shipped with Redmine 4.2 release.

Regards,

#16 - 2020-11-06 00:17 - Shankar Vangari

Can you help me to apply this patch

#17 - 2021-06-12 10:18 - Go MAEDA

- Duplicated by Feature #12855: Sometime,we need limit register email address added

Files

setting-restrict-domains.png	96.6 KB	2020-03-12	Yuichi HARADA
3369-restrict-domains.patch	7.32 KB	2020-03-12	Yuichi HARADA
3369-restrict-domains-v2.patch	7.29 KB	2020-04-27	Go MAEDA
3369-restrict-domains-v3.patch	6.76 KB	2020-04-29	Go MAEDA