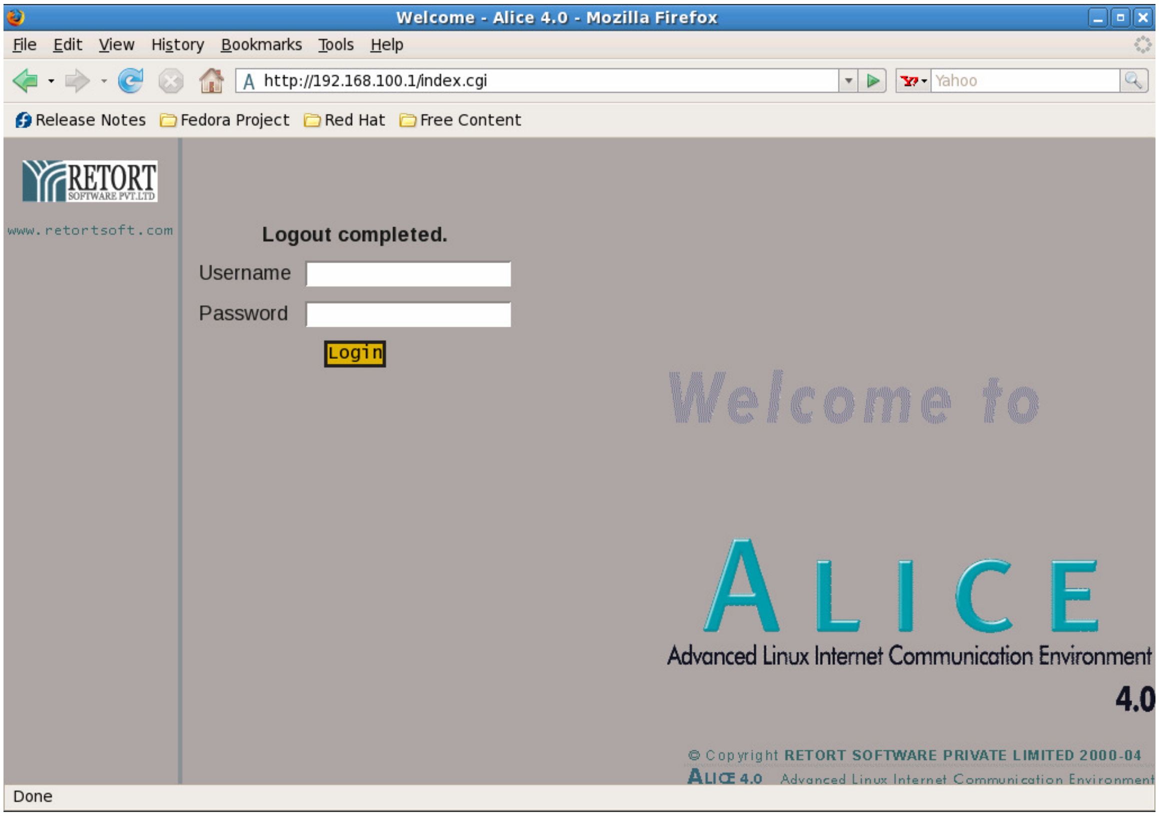
1.2 Administering Alice

Alice provides a simple and convenient way to manage the Internet and email settings for your organization. Alice comes with a number of configurable options which allow for ease-of-use, at the same time providing a secure environment.

Alice presents a graphical user interface (GUI) for administration purposes which can be accessed using any Web browser by the system administrator. To administer Alice in your Web browser configure the proxy settings of your browser with the IP address of Alice and specify port as 8080. Also unselect â€œBypass proxy for local addressesâ€□, then type config or IP address of the Alice machine in the address part of your browser. For example, if the IP address of Alice is 192.168.200.1 then type the URL in the address bar as http://config or â€œhttp://192.168.200.1â€□. This will prompt you for a username and password. To make administrative changes you need to login as 'netadmin', the Alice administrator's login. To make changes to your user profile you can login with your username and password. The administration screen presents you with buttons to access the four main modules of Alice and the logout button.


Welcome - Alice 4.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.100.1/index.cgi
Yahoo
Release Notes
Fedora Project
Red Hat
Free Content
RETORT SOFTWARE PVT.LTD
www.retortsoft.com
Login
Welcome to
ALICE
Advanced Linux Internet Communication Environment
4.0
© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment
Done

Logout completed.

Username

Password

Fig. 1.4 –The Alice Administrator Login Dialogue Box

The Main Controls on the Alice Administrative Console

User Management: For adding users, or editing/removing usersâ€™ profiles on the server who will be part of the LAN.

Proxy Management: To manage Internet access among the users.

Email Management: To configure email and email groups settings for the users.

Advanced Settings: For specifying connectivity interface, providing backup facility and managing date settings.

Server Add-ons: Details on additional utilities that increase office efficiency.

Logout: The logout button is used to exit Alice. If it asks for authentication on logout just

click the 'OK' button. Do not enter any password. A login page should then appear.

Note: Do not click on 'Cancel' as the saved password will not be cleared. Each of these Modules has sub-modules, categorised as per the function. The following pages will provide a step-by-step guide to configure Alice.

1.3 User Management

The administrative tasks you can perform from this module are:

Add: This module can be used to add new users on the server who will be members of the LAN.

Edit / Remove: You can edit usersâ€™ profiles, reset passwords, or remove users' group profiles, schedule timings for access and also remove users' profiles.

Admin profile: The Administrator can make changes to his profile via this option.

User quota: The administrator can set user quotas for individual email IDs.

1.1.1 Adding Users

Users are the people in your company who will be using Alice for their networking needs.By adding a user you create a unique base for each individual within which networking profiles for each of them can be decided.

a) Click on 'Add' under the User Management head to get the 'Add User Screen'.(See fig. 1.5)

b) Fill in the username, full name and password in the form that appears. Re-enter the same password in the next field, else the user will not be added. The username is case insensitive while creating users. Username has to start with an alphabet, and can include numerals, '_'(underscore) and '.' (period). No other special characters are allowed.Username can be a maximum of 32 characters. The password you enter is case-sensitive,as also your full name.

Tip: If you tick the 'Allot same password' option, then for all users where the password fields are left blank, a common system-generated password will be created. Use this option if you are creating multiple users at the same time, since instead of generating (and remembering) different passwords, you only have to remember one randomly generated password. Users can change their passwords later.

c) Once groups are made in the Proxy Management Interface, you will be able to allocate groups to each additional user that you create.

Note: Only groups made in the category User Name will appear in the drop down list.

d) Use the 'More Entries' button if you have more users to add.

e) After filling in all the user details, click on the 'Add' button to add the entered users to the system. To clear the user screen without saving the entered details,click on the 'Clear' button.

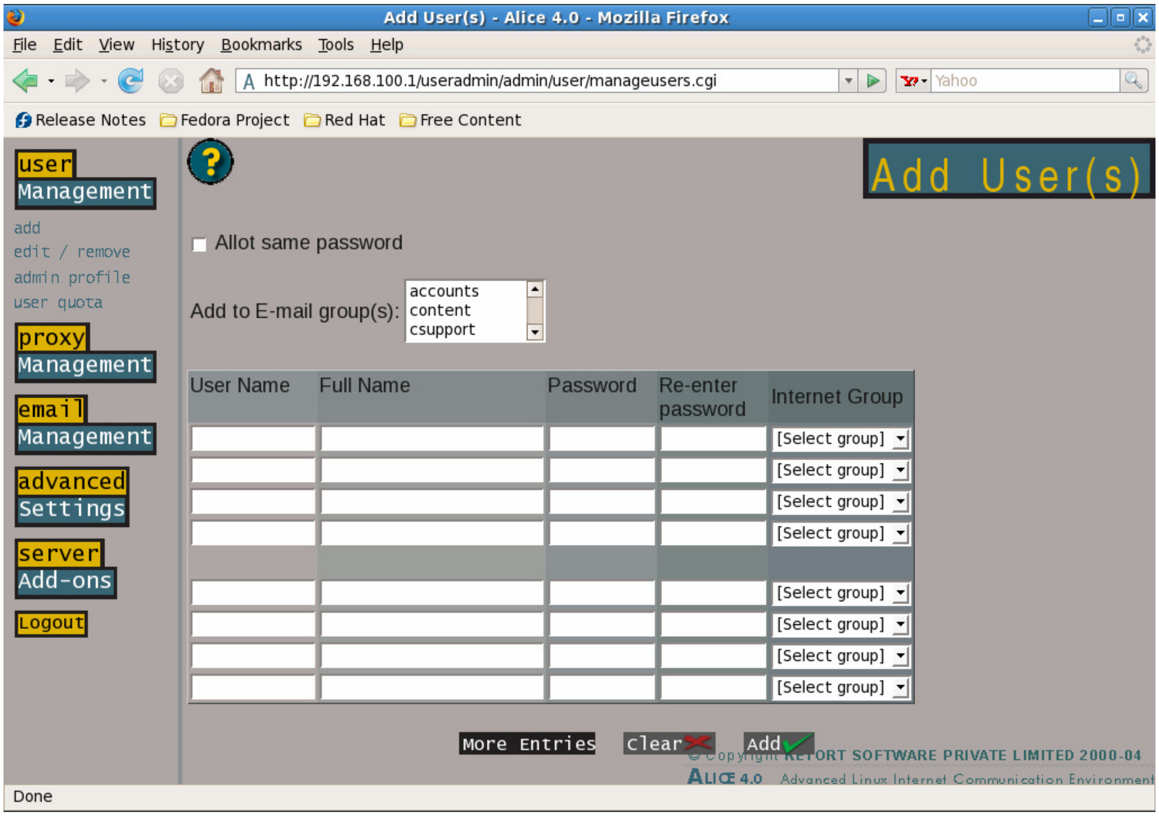


Fig. 1.5 –The â€˜Add Userâ€™ Screen

1.1.2 Editing or removing an existing user's profile

You may need to redo an existing user's profile or completely knock it off from your Alice database. The reasons could be various, say when the user has received a promotion, user has been shifted to a new department within the company or user has resigned from the company.

a) Click on 'Edit/Remove' under User Management.

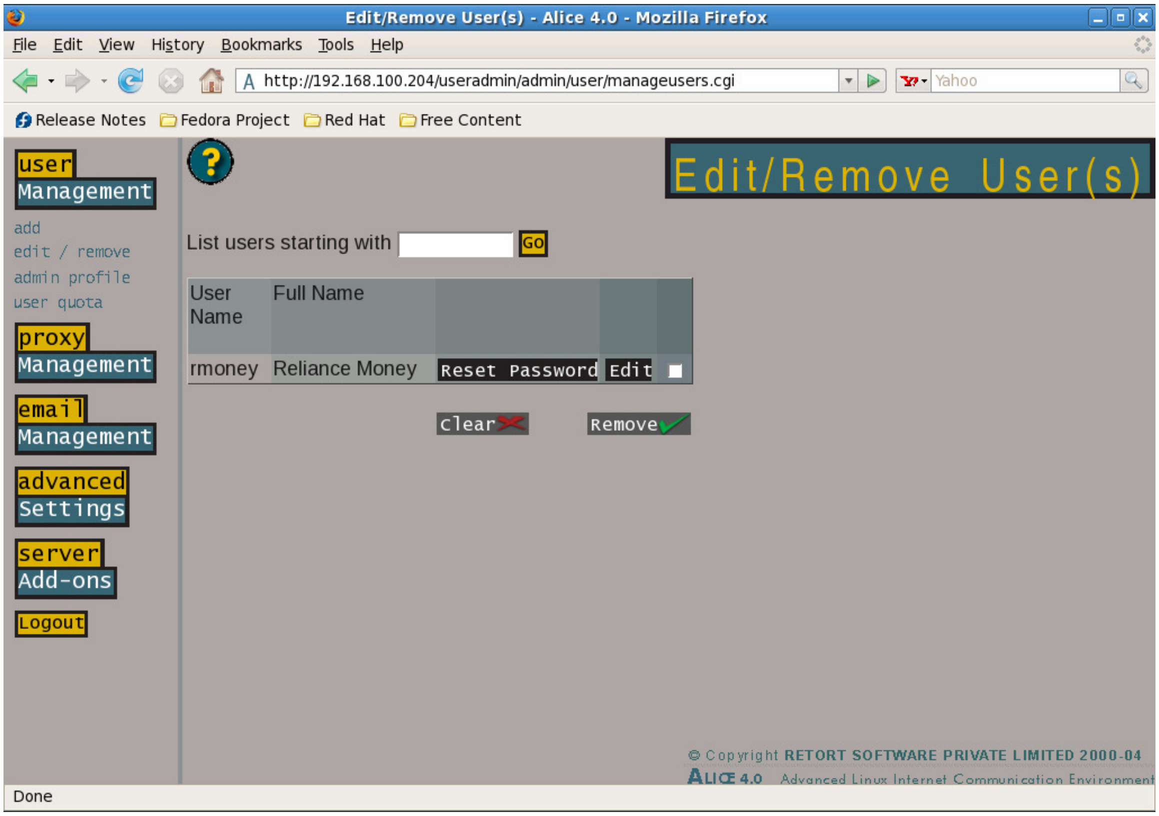
b) A form appears that contains the names of all the users.

Tip: To avoid scrolling down the list for a particular user, enter the first few letters of the username in the textbox provided and click on 'Go'. You will get a list of all users whose user names begin with those letters.

c) In case a particular user has forgotten the password, you can reset the password to a system generated password using the 'Reset Password' option.

d) To remove users from the system, check the box against the user's name and then click on 'Remove'. You will be prompted to confirm the deletion, on the acceptance of which the user will be deleted.

Caution: Deleting a user permanently erases all his records and this cannot be recovered.Be sure before you delete any user.



Edit/Remove User(s)

List users starting with

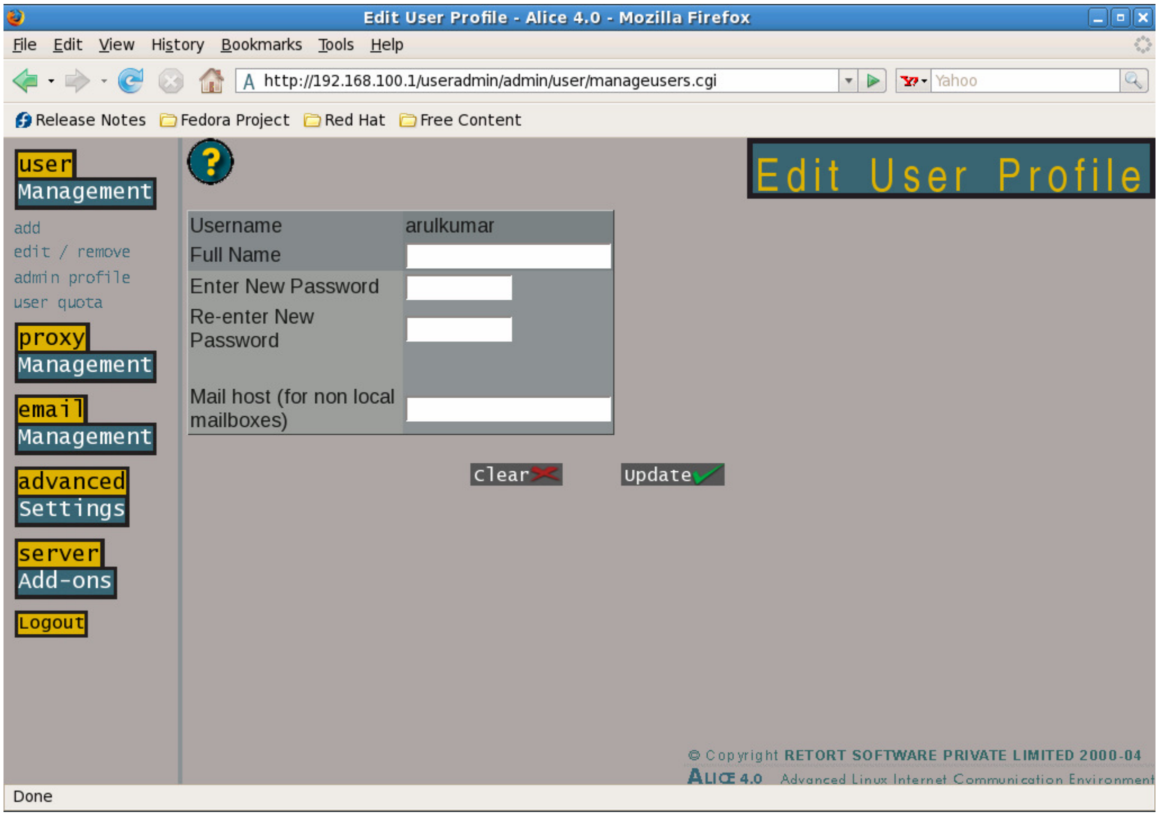
User Name	Full Name			
rmoney	Reliance Money	Reset Password	Edit	□

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04

ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.6 –The â€˜Edit / Remove Userâ€™ Screen

e) Clicking on the â€œEditâ€□ option will allow you to change the full name of the user or change his password. To assign a new password to the user, enter the password in the relevant text field.Confirm by entering the same password again in the 'Re-enter New Password' box.



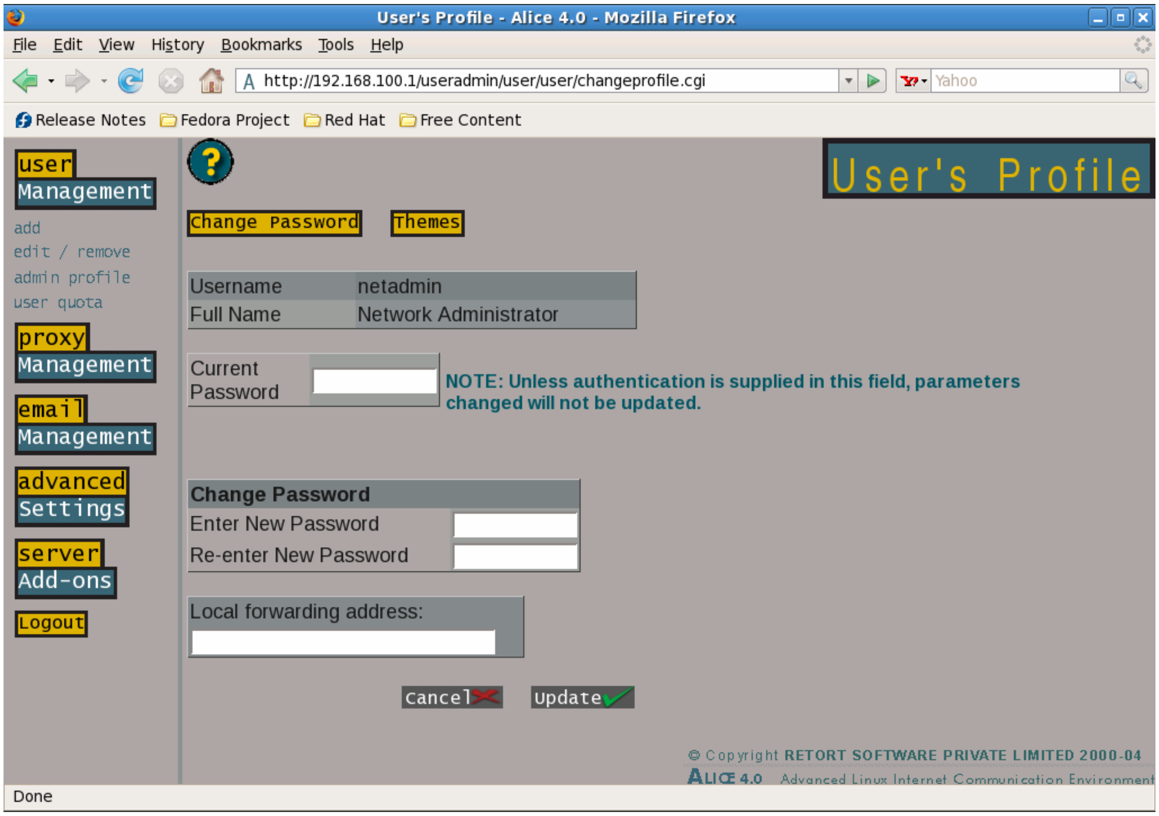
Username	arulkumar
Full Name	
Enter New Password	
Re-enter New Password	
Mail host (for non local mailboxes)	

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.7 –The â€˜Edit Userâ€™ Screen

1.1.3 Admin profile

This screen allows the Administrator to change his password and change the forwarding address to which all non-delivered/ incorrect mail will be delivered.Enter Current Password in the field provided and enter the new password in the relevant field. Make sure the new password is also re-entered. Clicking on the â€˜Updateâ€™ button will now change the password.Similarly, the local forwarding email can also be changed.


User's Profile - Alice 4.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.100.1/useradmin/user/user/changeprofile.cgi
Yahoo
Release Notes
Fedora Project
Red Hat
Free Content
user Management
add
edit / remove
admin profile
user quota
proxy Management
email Management
advanced Settings
server Add-ons
Logout
User's Profile
change Password
Themes
Cancel
Update
© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment
Done

Username	netadmin
Full Name	Network Administrator

Current Password

NOTE: Unless authentication is supplied in this field, parameters changed will not be updated.

Change Password	
Enter New Password	
Re-enter New Password	

Local forwarding address:

Fig. 1.8 –The â€˜Administratorâ€™s Profileâ€™ Screen

1.1.4 User Quota

This screen allows the network administrator to specify the mailbox parameters for each user on the system.

Tip: To avoid scrolling down the list for a particular user, enter the first few letters of the username in the textbox provided and click on 'Go'. You will get a list of all users whose user names beginning with those letters.

Block Quota: Defines the storage limit of a userâ€™s mailbox. This however is a soft limit and the system will continue to receive emails in the userâ€™s inbox even if this limit is exceeded but will send warnings to the user.

Block Limit : defines the upper storage limit for the user after which emails to the user will start bouncing back.

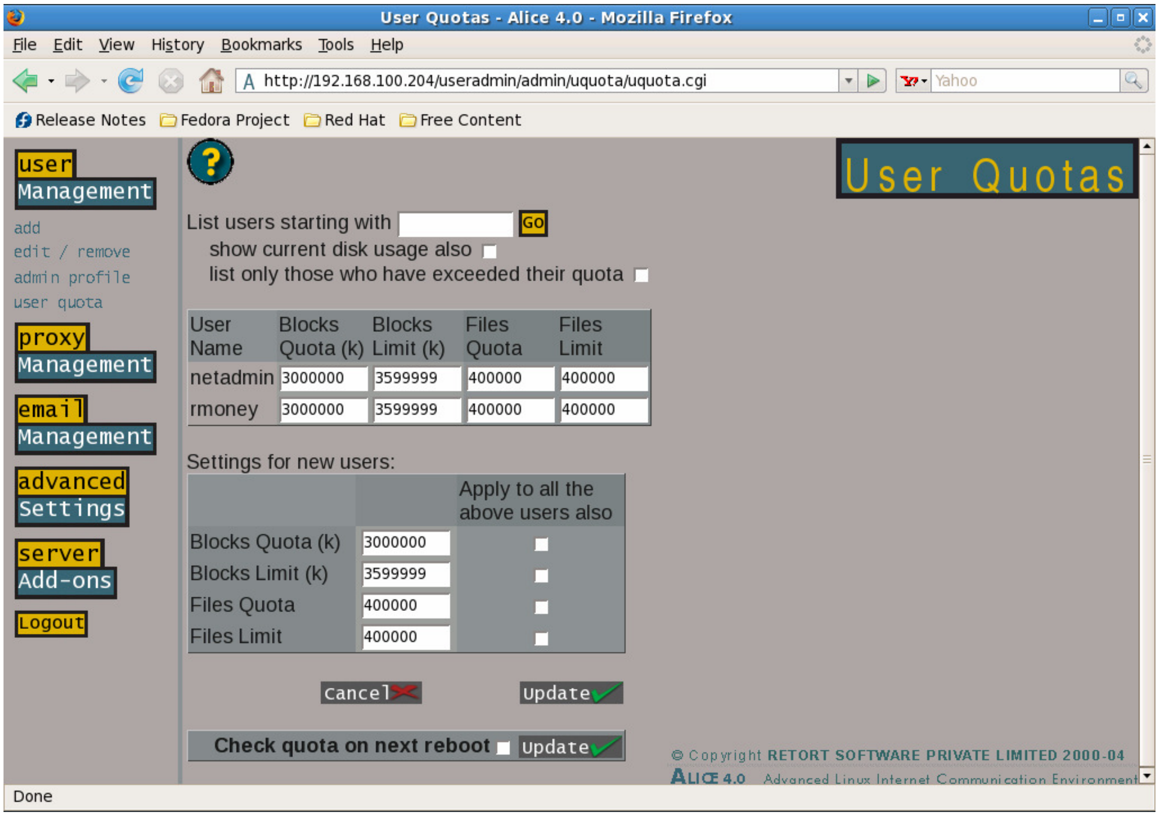
Files Quota : defines the number of emails that a user is allowed to have on the server. If backups of all emails are being kept on the server, care should be taken to ensure that this number is very big. This however is a soft limit and the system will continue to send files /receive files in the userâ€™s inbox even if this limit is exceeded but will send warnings to the user.

Files Limit: defines the upper storage limit for the user after which the system will bar access.

The limits can be changed in the field itself. Clicking on â€˜Updateâ€™ will write the necessary changes to the system.

Selecting the â€˜Show Current Disk Usage alsoâ€™ checkbox will show the current space being utilized by each user, while the â€œlist only those who have exceeded their quotaâ€□ option will show only the users who have exceeded their quota.

We recommend that you enable the â€œCheck quota on next rebootâ€□ option, as this will prevent any discrepancy in the system.


User Quotas - Alice 4.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.100.204/useradmin/admin/uquota/uquota.cgi
Yahoo
Release Notes
Fedora Project
Red Hat
Free Content
user Management
add
edit / remove
admin profile
user quota
proxy Management
email Management
advanced Settings
server Add-ons
Logout
User Quotas
GO
cancel
Update
Update
© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment
Done

List users starting with ______ GO

show current disk usage also □

list only those who have exceeded their quota □

User Name	Blocks Quota (k)	Blocks Limit (k)	Files Quota	Files Limit
netadmin	3000000	3599999	400000	400000
rmoney	3000000	3599999	400000	400000

Settings for new users:

		Apply to all the above users also
Blocks Quota (k)	3000000	□
Blocks Limit (k)	3599999	□
Files Quota	400000	□
Files Limit	400000	□

Check quota on next reboot □

Fig. 1.9 –The â€˜User Quotasâ€™ Screen

1.4 Proxy Management

This section allows you to specify Internet access privileges for members of the LAN and to view their logs. Internet access can be specified using a number of different parameters, or their combination thereof.

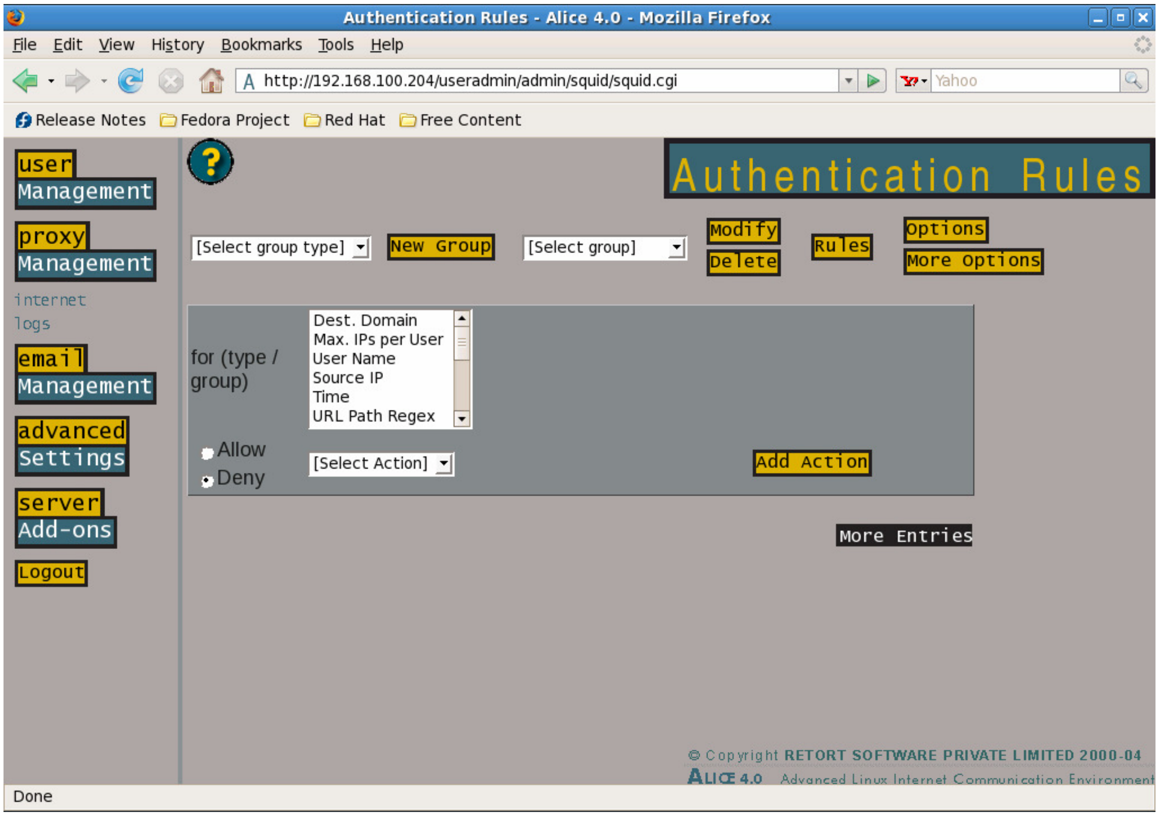


Fig. 1.10 –The â€˜Proxy Managementâ€™ Screen

1.4.1 Internet

Access to the Internet for members of the LAN can be denied or allowed based on user IP address, user name, time, or destination IP. This is done by forming groups, allocating rules for each group and then adding conditions to each rule. All rules and their combinations can result in one of two actions: access or denial of HTTP access. Groups are essentially collections of IP addresses, user names, or time blocks to which a common action will be applicable.

The default categories of possible groups are:

Destination domain: allows you to create a list of domains to which the rules of access or denial can be added. Conditions could further specify the times during which such domains may be accessible or denied, or for users exempt from the rule.

Max IPs per user: Referring to the IP addresses within the LAN, the default number of IP addresses allocated for a particular username and password is 1. Hence a user will be able to access the Internet only from the one IP allocated to him using his unique username and password. For groups such as monitors/system administrators, it will be possible to allow users the ability to access the Internet from multiple IP addresses.

User Name: Allows the administrator to form groups and allow / deny/ selectively allow Internet access on the basis of the username.

Source IP: Allows the administrator to allow/ deny/ selectively allow Internet access on the basis of the userâ€™s IP address.

Time: Allows the administrator to form groups and selectively allow/ deny Internet access on the basis of pre-decided time slots.

The â€˜Modifyâ€™ button on the right of the screen is used to make changes to the settings of an existing group that you may have created at an earlier date. This is done by selecting the group from the drop down list (any group that you create among the different categories explained above will appear in this list) and clicking on â€˜Modifyâ€™. Similarly, a created group can be deleted by selecting the group from the drop down list, and clicking on â€˜Deleteâ€™.

The â€˜Rulesâ€™ button is used to define the rules for a particular group. There are 3 broad categories of rules:

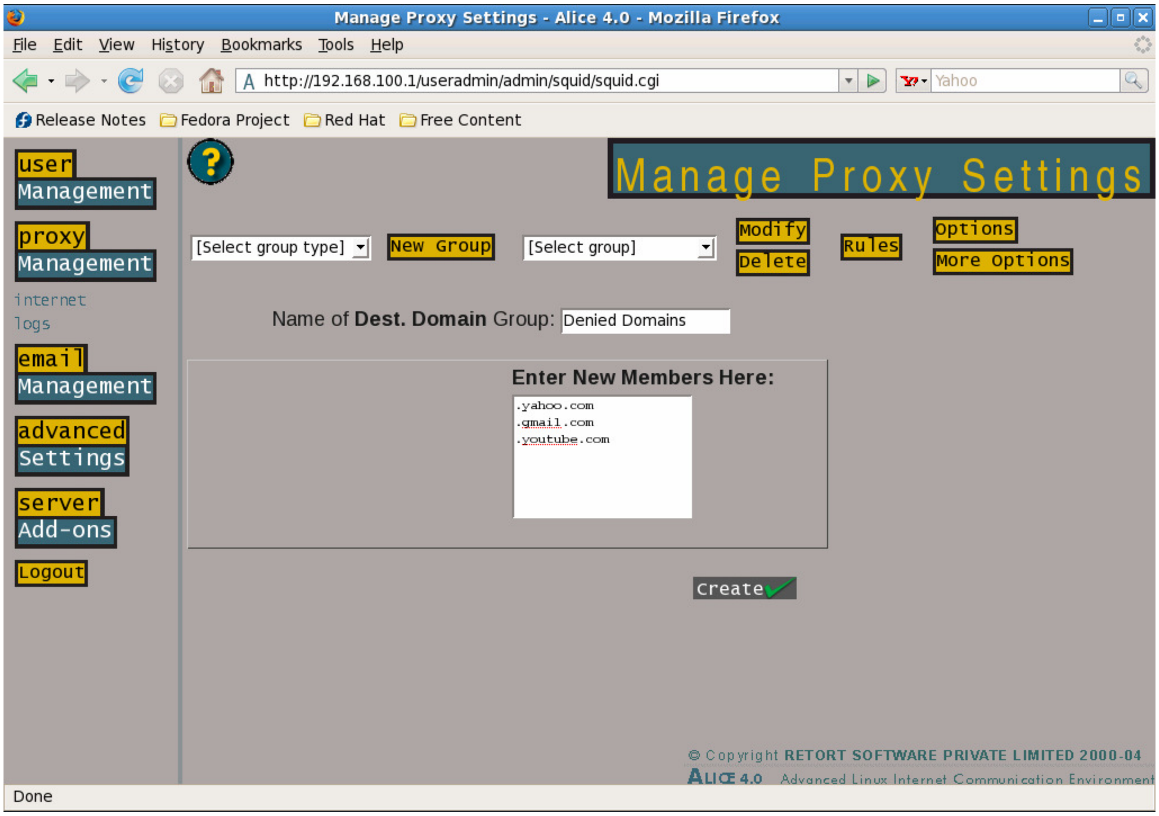
Pre-authentication rules: These are rules based on IP Address/ DNS/ Time, which are applied to a user request to Alice before the authentication of the user is done via his username and password. Since they come into play before the user is authenticated they can apply only to the groups falling in the categories Destination Domain, Source IP and Time.

Authentication rules: These are rules that are carried out after the authentication of the user at the Alice server and allow the administrator to allow or deny HTTP access to users, or a group of users, based on their username or IP addresses at specific times.

Default Rules: These are applied to all groups or users and override all other sets of rules.

Creating Groups

We will initially be creating a group within the category â€œDestination Domainâ€□- this will allow us to collate specific domains (website URLs) to which we can then attach specific rules and conditions, and thus control Internet access.



Name of **Dest. Domain** Group: Denied Domains

Enter New Members Here:

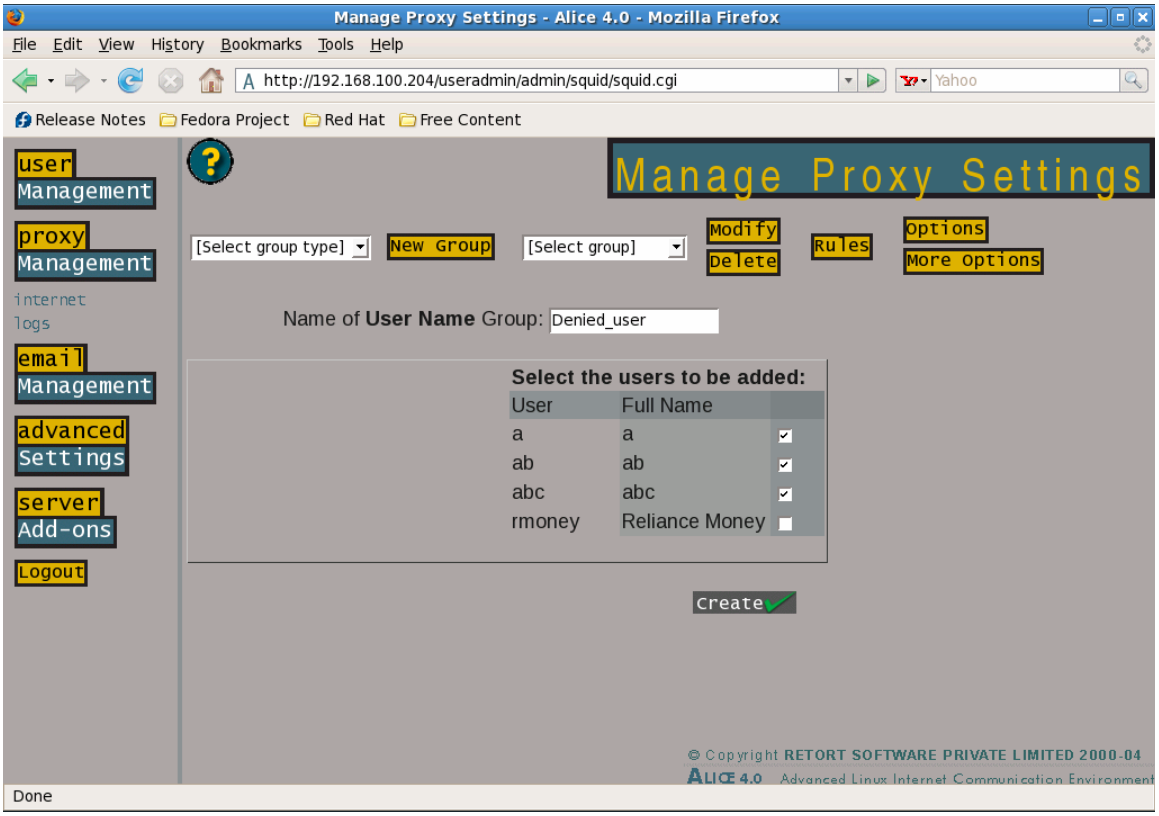
```
.yahoo.com
.gmail.com
.youtube.com
```

Fig. 1.11 –The â€˜Creating Groupsâ€™ Screen

Step 1: From the drop down list, select Dest. Domain and click on â€˜New Groupâ€™.

Step 2: Fill in a name for the group in the field provided (eg. Denied_domains), fill in the domains you want to block in the text field below, and click on â€˜Createâ€™ . You will now get a message saying that the group denied_domains has been created successfully. You can now go back to the previous screen by clicking on â€œInternetâ€□ in the left pane. The newly created group can now be viewed in the drop down box to the right of the interface.

Note: The name of the group cannot have any spaces.


Manage Proxy Settings - Alice 4.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.100.204/useradmin/admin/squid/squid.cgi
Yahoo
Release Notes
Fedora Project
Red Hat
Free Content
user Management
proxy Management
internet logs
email Management
advanced Settings
server Add-ons
Logout
Manage Proxy Settings
[Select group type]
New Group
[Select group]
Modify
Delete
Rules
Options
More Options
Create
© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment
Done

Name of **User Name** Group: Denied_user

Select the users to be added:

User	Full Name	
a	a	☑
ab	ab	☑
abc	abc	☑
rmoney	Reliance Money	□

Fig. 1.12 –The â€˜Denied Userâ€™ Screen

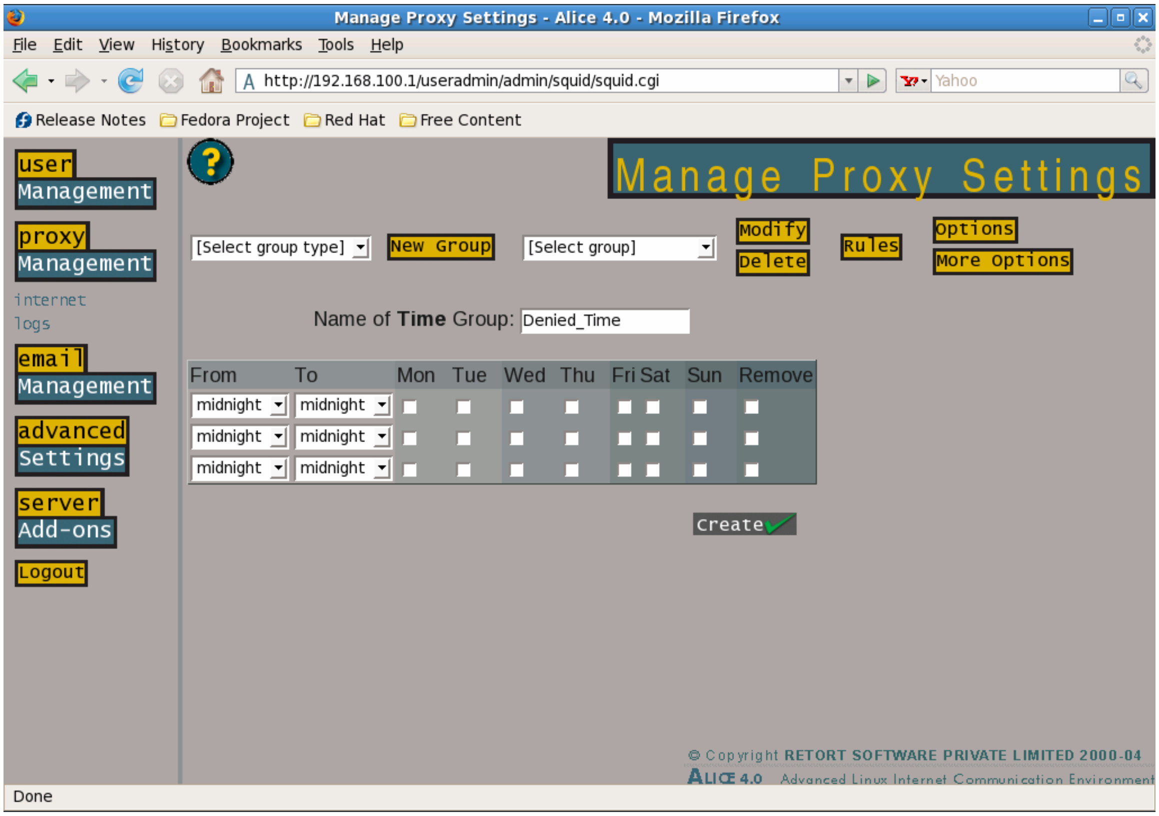
Following the same procedure we can create a group of users (denied_users).

Step 1: From the drop down list, select User Name and click on â€˜New Groupâ€™.

Step 2: Fill in a name for the group in the field provided (eg. denied_users), put a check against the users you want to add to this group, and click â€˜Createâ€™. You will now get a message saying that the group denied_users has been created successfully. You can now go back to the previous screen by clicking on â€œInternetâ€□ in the left pane. The newly created group can now be viewed in the drop down box to the right of the interface.

Note 1: The name of the group cannot have any spaces.

Note 2: All groups created in this category (i.e. users) will now appear in the â€œAdd userâ€□ screen in the section on User Management.



Name of Time Group: Denied_Time

From	To	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Remove
midnight	midnight	□	□	□	□	□	□	□	□
midnight	midnight	□	□	□	□	□	□	□	□
midnight	midnight	□	□	□	□	□	□	□	□

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment

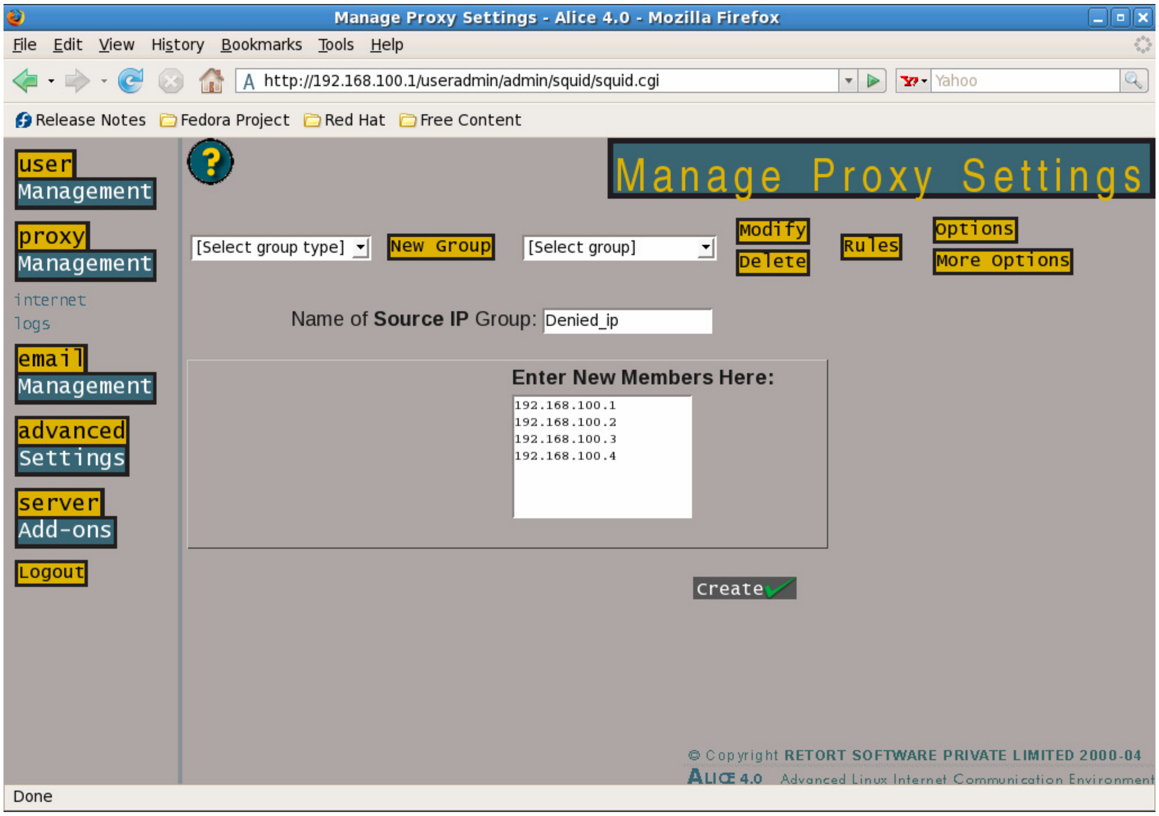
Fig. 1.13 –The â€˜Denied Timeâ€™ Screen

Following the same procedure we can create a time group (denied_time).

Step 1: From the drop down list, select Time and click on â€˜New Groupâ€™.

Step 2: Fill in a name for the group in the field provided (eg. Denied_time), pick the time block desired by selecting it from the drop down list presented in the interface, and select the days of the week when the denial will be applicable. Clicking on â€˜Createâ€™ will give you a message saying that the group denied_time has been created successfully. You can now go back to the previous screen by clicking on â€œInternetâ€□ in the left pane. The newly created group can now be viewed in the drop down box to the right of the interface.

Note: The name of the group cannot have any spaces.


Manage Proxy Settings - Alice 4.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.100.1/useradmin/admin/squid/squid.cgi
Yahoo
Release Notes
Fedora Project
Red Hat
Free Content
user Management
proxy Management
internet
logs
email Management
advanced Settings
server Add-ons
Logout
Manage Proxy Settings
[Select group type]
New Group
[Select group]
Modify
Delete
Rules
Options
More options
Create
© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment
Done

Name of Source IP Group: Denied_ip

Enter New Members Here:

192.168.100.1
192.168.100.2
192.168.100.3
192.168.100.4

Fig. 1.14 –The â€˜Denied ipsâ€™ Screen

Following the same procedure we can create a group of Source IPs (denied_ips).

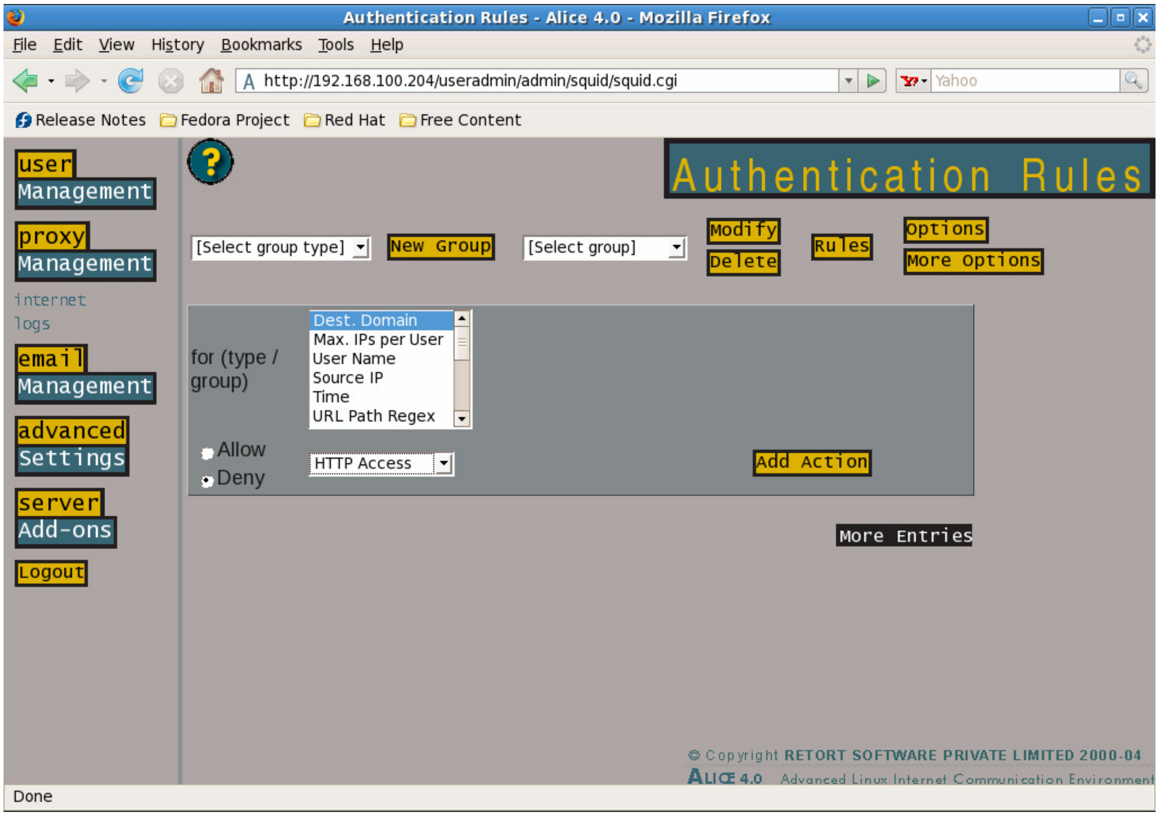
Step 1: From the drop down list, select Source IP and click on â€˜New Groupâ€™.

Step 2: Fill in a name for the group in the field provided (eg. denied_ips), fill in the IP addresses of the members you want added to this group, and click â€˜Createâ€™. You will now get a message saying that the group denied_ips has been created successfully. You can now go back to the previous screen by clicking on â€œInternetâ€□ in the left pane. The newly created group can now be viewed in the drop down box to the right of the interface.

Note: The name of the group cannot have any spaces.

Attaching Rules and Conditions to the created groups

Now that the groups have been created we can now attach rules and conditions to the groups that will result in an action. The action will usually result in access or denial of Internet Access if the conditions are met.



for (type / group): Dest. Domain (selected); Max. IPs per User; User Name; Source IP; Time; URL Path Regex

○ Allow
● Deny

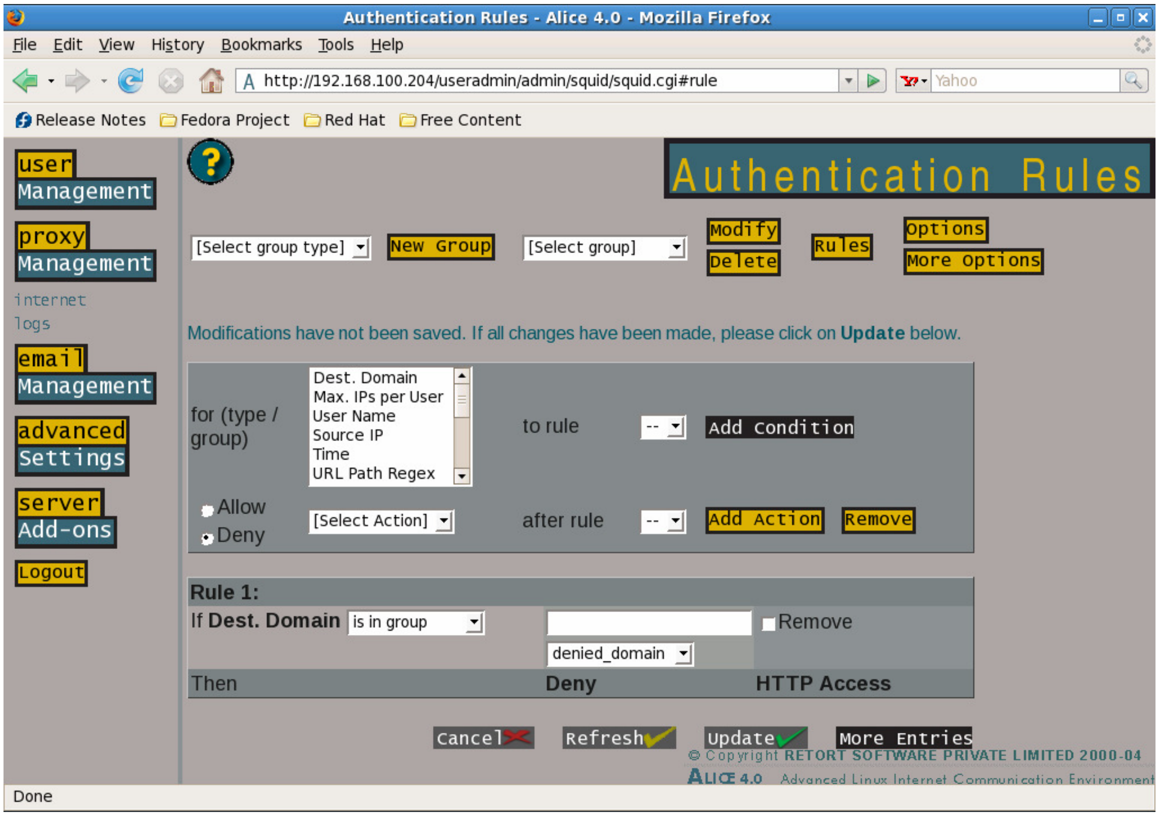
HTTP Access

Fig. 1.15 –The â€˜Attaching Rulesâ€™ Screen

Step 1: Against for (group of type), choose Dest. Domain, click on the radio button against Deny, select HTTP access from the drop down list, and click on â€˜Add Actionâ€™.

Step 2: In the screen provided, fill in the specifications â€œis in groupâ€□, select the newly created group â€œdenied_domainsâ€□ from the list, and click on â€˜Updateâ€™.

Note: Clicking on â€˜Updateâ€™ is essentially to save each change and to move to the next step.



Modifications have not been saved. If all changes have been made, please click on **Update** below.

for (type / group): Dest. Domain, Max. IPs per User, User Name, Source IP, Time, URL Path Regex — to rule: --

○ Allow ● Deny — [Select Action] — after rule: --

Rule 1:

If **Dest. Domain** is in group — denied_domain — □ Remove

Then **Deny** **HTTP Access**

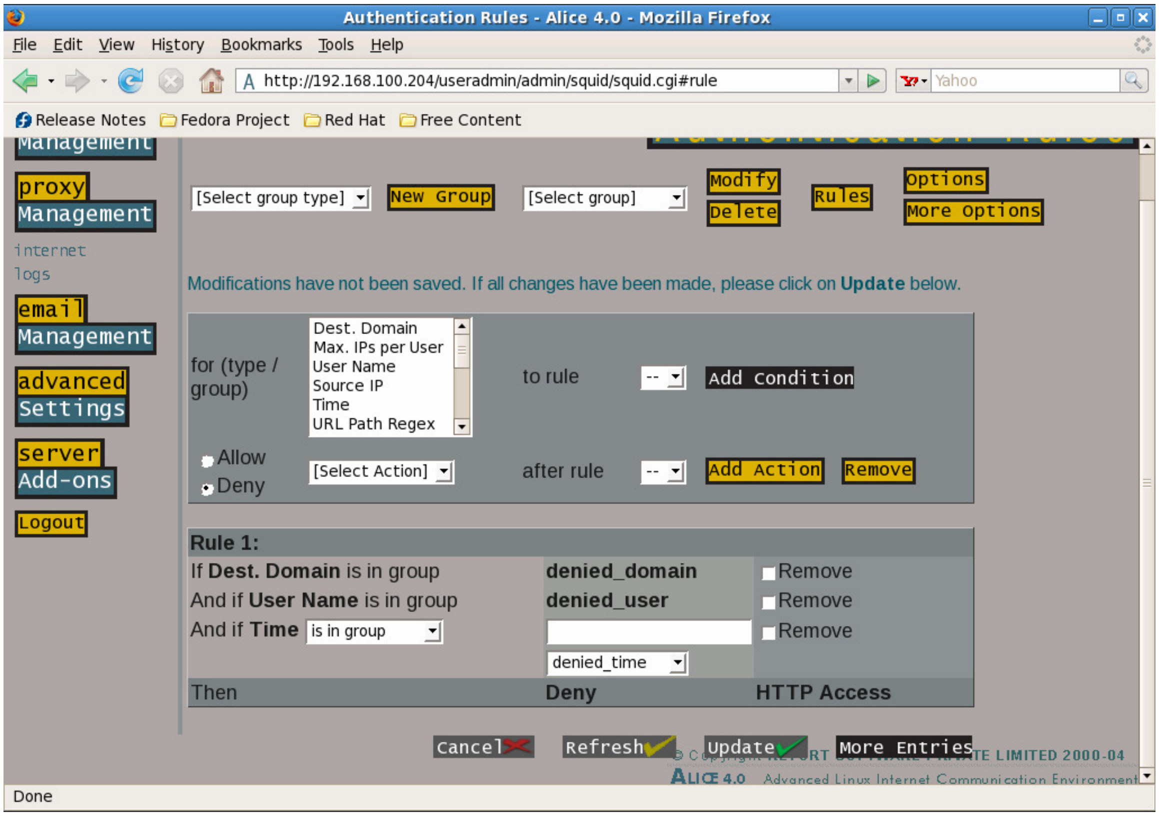
© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04

ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.16 -The â€˜Attaching Rulesâ€™ Screen

Step 3: Now from â€œfor (group of type)â€□ choose User Name, against â€œto ruleâ€□, choose 1 and click on Add Condition.

Step 4: Select â€œis in groupâ€□ and denied_users and click â€˜Updateâ€™. You now see that a condition has been added to your original rule of denying access to the domains in the group denied_domains. This existing rule with the condition will deny access to the selected domains to the members of the user group named denied_users.



Modifications have not been saved. If all changes have been made, please click on **Update** below.

Rule 1:

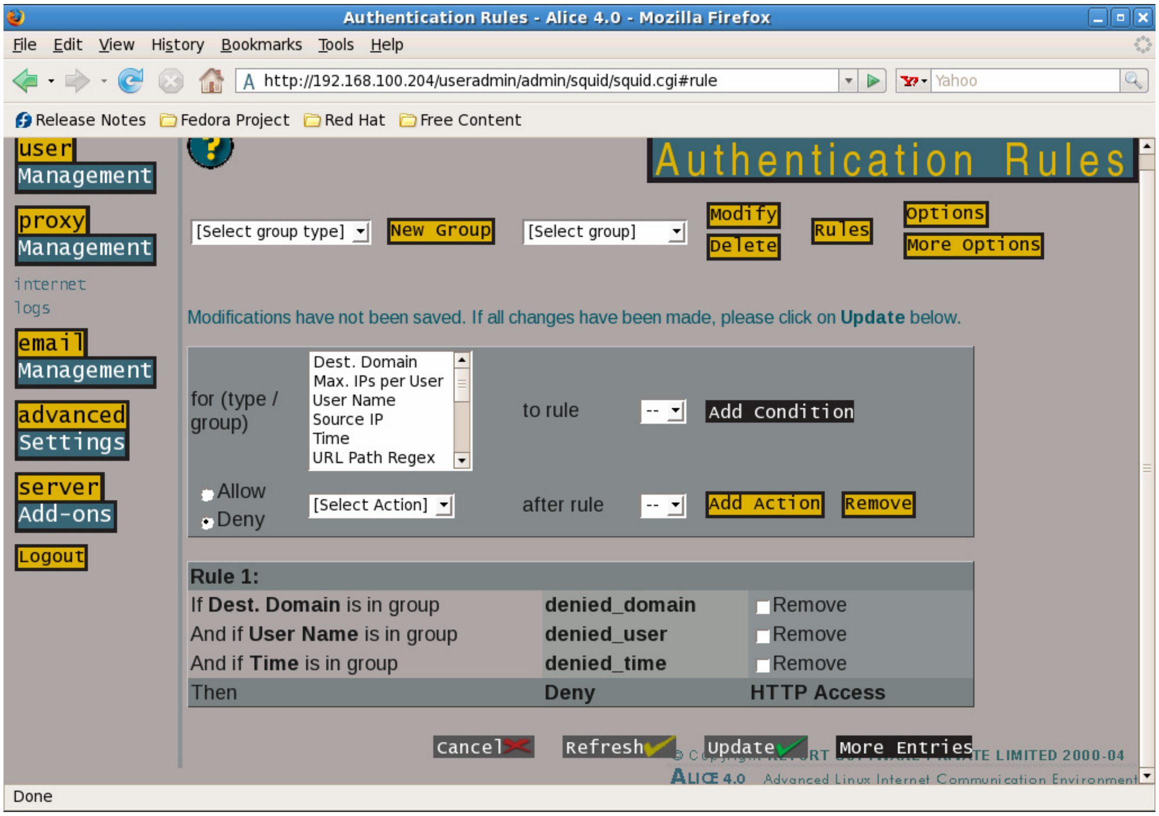
If **Dest. Domain** is in group	**denied_domain**	□ Remove
And if **User Name** is in group	**denied_user**	□ Remove
And if **Time** is in group	denied_time	□ Remove
Then	**Deny**	**HTTP Access**

Fig. 1.17 –The â€˜Attaching Rulesâ€™ Screen

Step 5: Select Time from â€œfor (group of type)â€□, choose 1 against â€œto ruleâ€□, choose 1 and click on Add Condition.

Step 6: Select â€œis in groupâ€□ and denied_time and click â€˜Updateâ€™. You now see that a condition has been added to your original rule. This existing rule with the conditions will deny access to the selected domains to the members of the user group named denied_users only during the time blocks specified in the time group denied_time.

In this manner, more rules can be added with combinations of different groups. A created rule can be removed by selecting the rule number against the â€˜Removeâ€™ button and clicking on â€˜Removeâ€™.



Modifications have not been saved. If all changes have been made, please click on **Update** below.

for (type / group): Dest. Domain, Max. IPs per User, User Name, Source IP, Time, URL Path Regex — to rule: --

○ Allow
● Deny
[Select Action] — after rule: --

Rule 1:		
If **Dest. Domain** is in group	**denied_domain**	□ Remove
And if **User Name** is in group	**denied_user**	□ Remove
And if **Time** is in group	**denied_time**	□ Remove
Then	**Deny**	**HTTP Access**

Fig. 1.18 –The â€˜Attaching Rulesâ€™ Screen

1.4.2 Logs

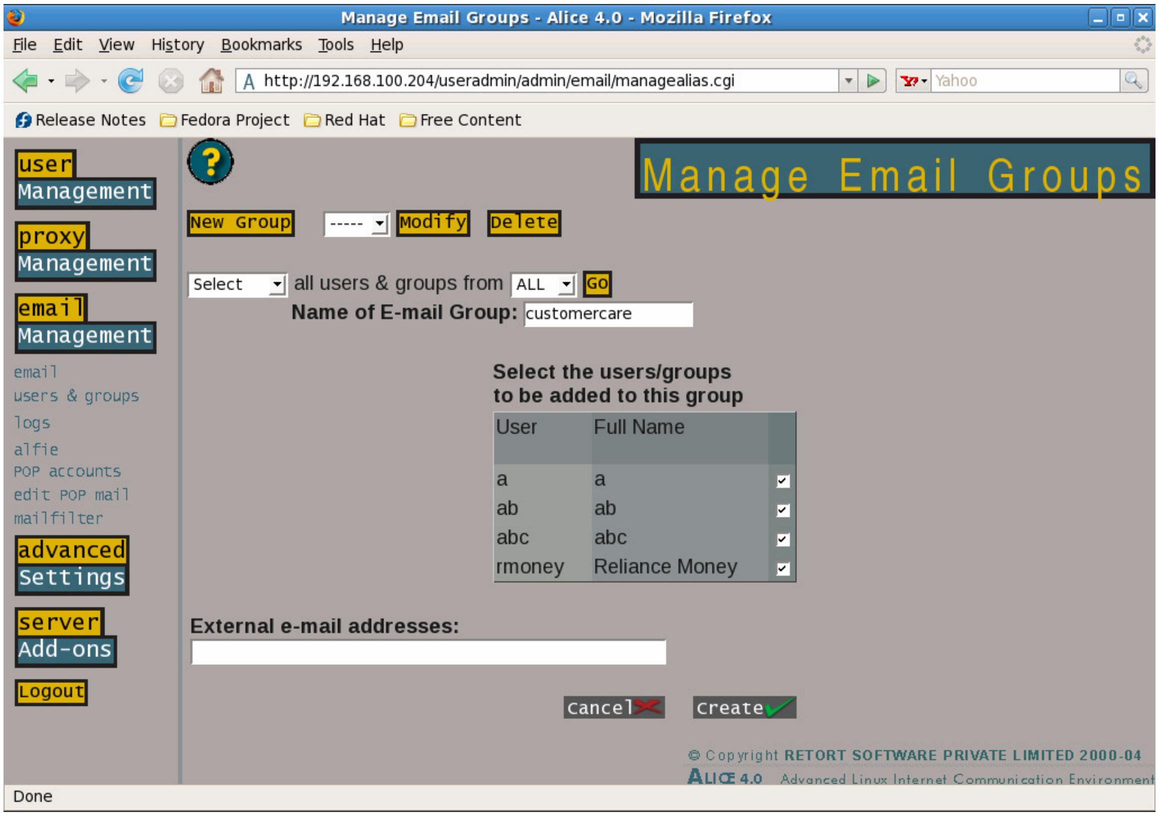
This shows surfing logs date-wise, per user. This can be done by selecting a user from the drop down list against the User Name, or by IP address, or by a combination of both by selecting the relevant IP Address from the drop down list against Machine ID.

Note: The asterisk (*) symbol is read as a wild character by the system and will give you the logs for all the users. The time period for the logs for each particular user/ machine can also be specified.

This data can then be used to specify limits on Internet access for the members of the LAN. This interface also allows you to delete logs older than a particular date and hence keep your system up to date. The date can be entered in any fashion such as dd/mm/yyyy or June 24, 2004 or even in blocks of time, such as 1 month.

1.5 Email Management

This section allows you to form groups for all users specified in the section on User Management. This is useful for the administrator to communicate information as well as for the groups to communicate among themselves.



Name of E-mail Group: customercare

Select the users/groups to be added to this group

User	Full Name	
a	a	☑
ab	ab	☑
abc	abc	☑
rmoney	Reliance Money	☑

External e-mail addresses:

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.19 –The â€˜Email Managementâ€™ Screen

1.5.1 eMail

This interface deals with the formation/ modification or deletion of email groups.

Clicking on â€˜New Groupâ€™ will take you to the interface that allows you to create a New Group. Selecting a group from the drop down list and selecting Modify will take you to the Modify screen. Clicking â€˜Deleteâ€™ will delete the group.

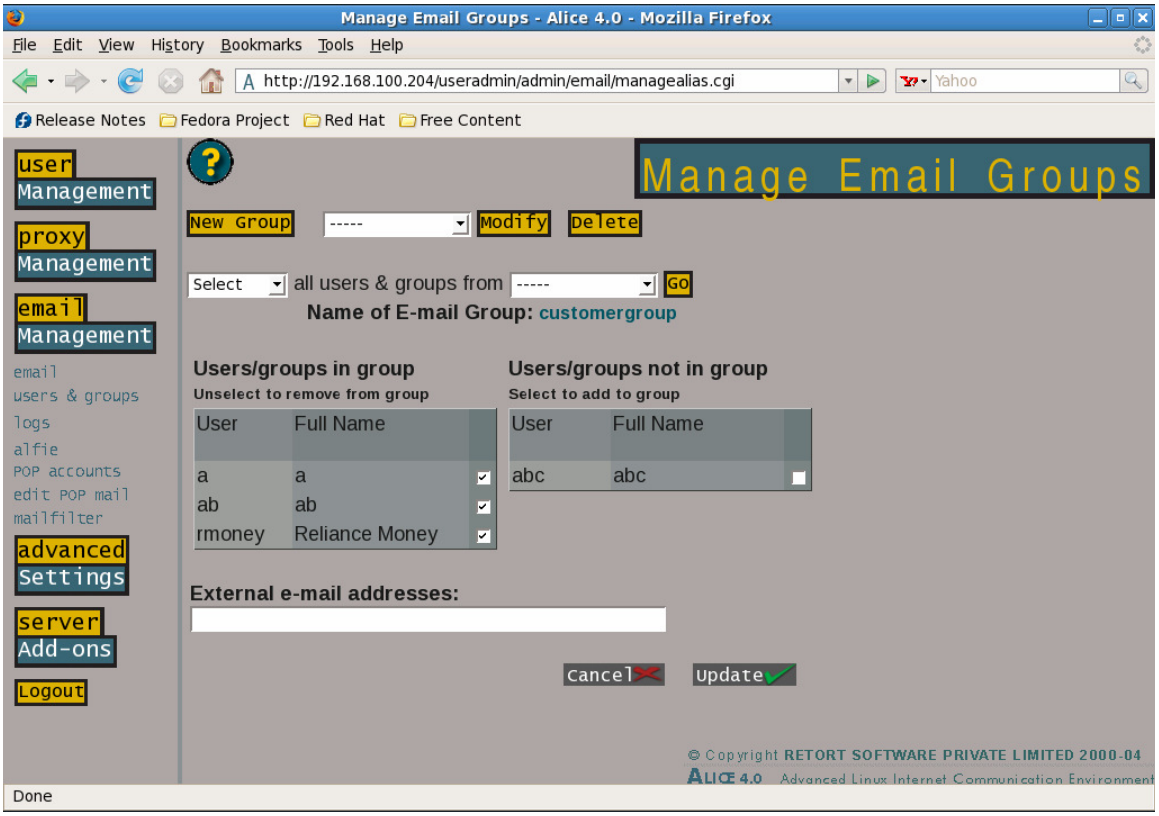
1.5.1.1 New Group

In the interface arrived at by clicking on â€˜New Groupâ€™, choose Select from the first Drop down list. Select will include the users/ groups that you choose subsequently from the group that you are creating. Unselect will exclude them. Next, choose the users and groups that you want to add to the new group and from the last drop down list choose the group from which you want to add. This last drop down list also contains the default group ALL.

Next, enter the name of the email group (eg. customercare_finance1). The email group can be a maximum of 32 alphanumeric characters but has to start with an alphabet. It cannot start with a numeral or other special characters. Special symbols like #, &, *, cannot form part of the email groupname. The groupname has to be unique and is not case-sensitive. By default, an email ID with the name of the groups (of the form groupname@companyname.com) is also created, which can be used as the common email ID for communication among and with the group.

Next, select the users/ groups that you want added from the list given below. This list will contain all users and email groups that are in existence on the system. If you want external members to receive the group email IDs, you can enter their email IDs in the field provided. You can add as many emails as needed, separated by a comma.

Clicking â€˜Createâ€™ will now create the email group customercare_finance, which can also be accessed from the drop down list next to the â€˜Modifyâ€™ button.Selecting the group and clicking on â€˜Modifyâ€™ will allow you to make changes to the settings of the group, while selecting the group, and clicking on â€˜Deleteâ€™ will delete the group.



Name of E-mail Group: customergroup

Users/groups in group

Unselect to remove from group

User	Full Name	
a	a	☑
ab	ab	☑
rmoney	Reliance Money	☑

Users/groups not in group

Select to add to group

User	Full Name	
abc	abc	□

External e-mail addresses:

Fig. 1.20 –The â€˜Email Managementâ€™ Screen

1.5.1.2 Users and Groups

This interface displays a complete list of the users and groups on the server. The administrator can use this interface to send an email to either a user, a group, or multiple users and groups. Clicking on the + sign next to the group/user name shows you the members of the group or the details of the user as the case may be.

1.5.1.3 Logs

This interface shows the details of emails per user as well as by group. The interface also allows you to delete logs so as to keep an updated system.

1.5.1.4 Alfie

This interface is used to create email filter settings which apply to all mailboxes in an organization. It works on a similar principal of Rules, Conditions and Actions as is present in Internet settings in Proxy Management. The number of possible actions in this interface is greater than that possible in Internet settings.

Thus, the administrator specifies a rule to which he can add a number of different conditions, and in the event of all the conditions being met, a specific action will take place.

Clicking on the â€˜Rulesâ€™ button on the top right corner will take you to the screen showing the current rules in existence, while clicking on â€˜Optionsâ€™ will allow you to specify more detailed settings for your email. The list of possible actions can be viewed by clicking on the drop down box, while selecting an action and clicking on â€˜Add Actionâ€™ will add that particular action to the rule that you have chosen from the previous drop down box.

Scenario: Creating a â€˜Ruleâ€™ and setting conditions that allow the server to skip mail processing in case both the sender and the recipient are local.

Step 1: Choose â€œIf Sender is Localâ€ from the drop down box and the Action â€œSkip Mail processingâ€ from the second drop down box and click on â€˜Add Actionâ€™. This will specify the Rule â€œIf Sender is Localâ€ and associate the Action â€œSkip Mail Processingâ€ to the Rule.You can specify a name for the rule that you are creating, in which case it will take the name as its identification in all other drop down boxes in the Interface. The default setting will assign sequential numbers to each rule. In our case, we have taken mailfilter as the name. Spaces are not allowed in the name. The position of the rule in the list defines the priority at which the rule will be processed.

Step 2: Select 1 in the drop down list beside â€˜Add Conditionâ€™ and choose the required condition from the drop down list in the Rule section. In our example the condition would be â€œIf Recipient is Localâ€.

Step 3: Click on â€˜Updateâ€™. You can now see your created rule.

Another set of rules and actions can be created by selecting the rule after which you want to create and clicking on â€˜Add Actionâ€™, while a rule can be deleted by selecting it from the drop down box and clicking â€˜Removeâ€™.
Similarly, a number of rules can be specified. These will be applicable on an organization wide level except in cases where specific users form part of the conditions, which can be done by selecting the condition â€œIf Sender is ..â€ or â€œIf Recipient is â€¦â€ from the drop down list.

1.5.1.5 POP account

Apart from the email IDs created locally, Alice allows the user to receive email from other external accounts which is delivered to his inbox automatically. A user can thus have email from his remote account directly posted to his local email ID in your organization.

To enable such a scenario, the following details will be needed:

Deliver mail to: Enter the username/email group to whom the mail from the external account should be directed. For a multidrop box, enter ALL as the user name.

Note: The field is case sensitive.

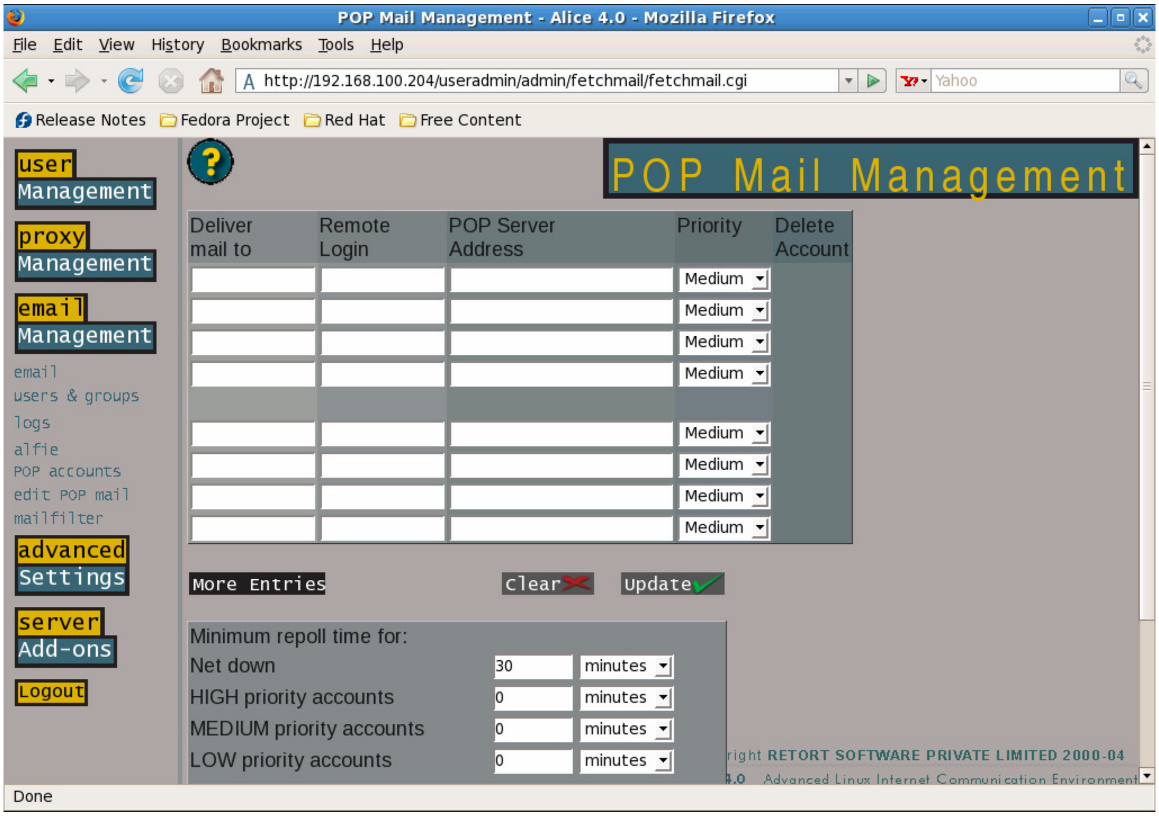
Remote Login: Specify the username/login name for the remote email account. For example, the login name for the external Yahoo! Account.

POP Server address: The IP address or the name of the POP server where the user has an external account. It can be POP server address like mail.yahoo.com.

Priority: You will need to specify the priority that the server should attribute to the specific POP account. The polling time for High priority/ Medium Priority/ Low Priority accounts can be specified in the settings below. The timings specified are the maximum time limits. If a mailbox receives mail frequently it will be rechecked for mail earlier.

Delete Account: This option allows you to delete a POP account.

Note: You will need to click on â€˜Updateâ€™ to enable any changes that you may have made.


POP Mail Management - Alice 4.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.100.204/useradmin/admin/fetchmail/fetchmail.cgi
Yahoo
Release Notes
Fedora Project
Red Hat
Free Content
user Management
proxy Management
email Management
email
users & groups
logs
alfie
POP accounts
edit POP mail
mailfilter
advanced Settings
server Add-ons
Logout
?
POP Mail Management

Deliver mail to	Remote Login	POP Server Address	Priority	Delete Account
			Medium	
			Medium	
			Medium	
			Medium	
			Medium	
			Medium	
			Medium	
			Medium	

More Entries
Clear
Update

Minimum repoll time for:

Net down	30	minutes
HIGH priority accounts	0	minutes
MEDIUM priority accounts	0	minutes
LOW priority accounts	0	minutes

right RETORT SOFTWARE PRIVATE LIMITED 2000-04
4.0 Advanced Linux Internet Communication Environment
Done

Fig. 1.21 –The â€˜POP Mail managementâ€™ Screen

The Net Down option controls the timing when polling is forcefully started when the Internet connection is down. This will also connect to the Internet if demand dialling has been enabled.The Poll from / to settings govern the timings when the system will poll the POP server for emails. Thus, the administrator can allow users POP access to their external email accounts only after office hours. If the fields are left blank, polling will occur whenever an Internet connection is available.

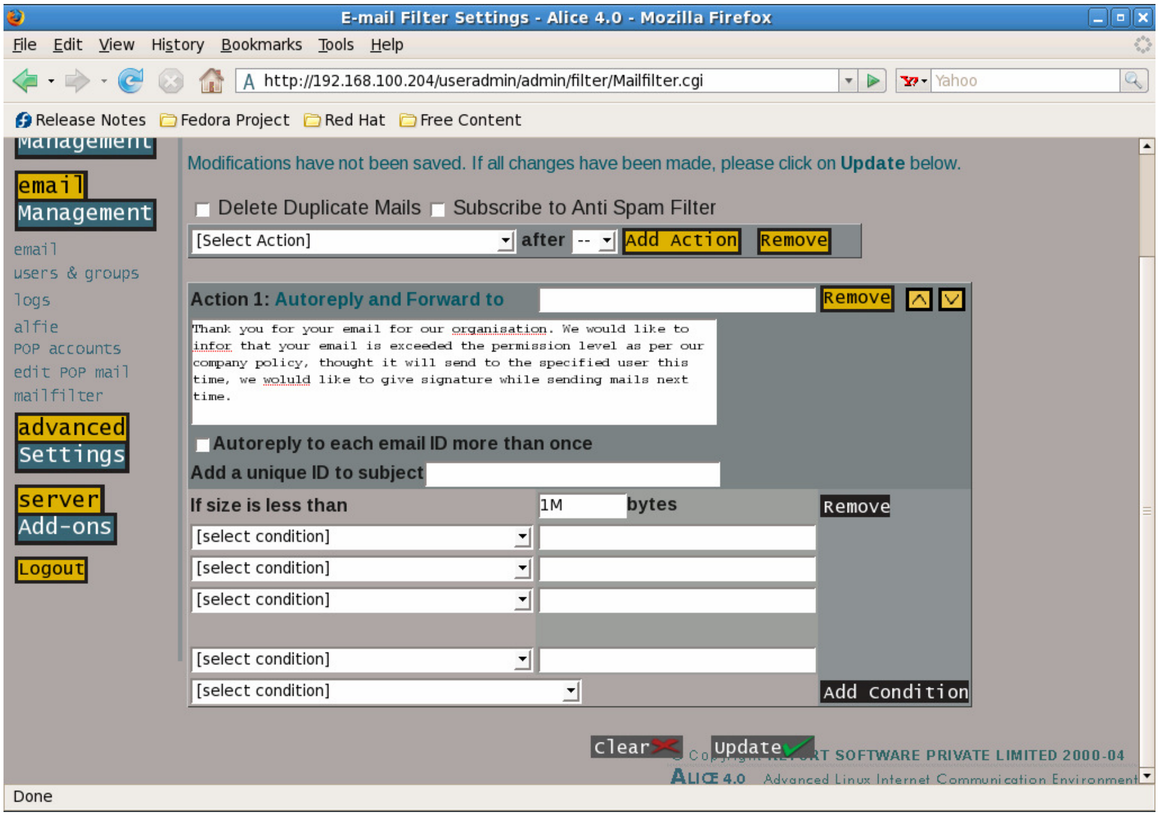
The Use Separate settings for ALL settings allow the administrator to allocate different timings for polling for the Group ALL, which serves as the name for a multi-drop box.

1.5.1.6 Edit POP mail

This screen allows the administrator/ user to specify settings for the POP account which pertain more to the settings required by the external mail server. The administrator has access only to the ALL (or the multi drop box) account, while an individual user will need to log in with his network username and password to access this feature and apply his individual settings.

1.5.1.7 Mailfilter

From this interface the administrator can add specific settings to each user mailbox on the server, or settings that will apply to every user, by selecting â€˜ALLâ€™. Any setting made under â€˜ALLâ€™ will get priority and individual users will not be able to either view or modify them. Hence for monitoring purposes, the administrator can set the condition that a copy of every email exceeding 10 MB sent by any user should also be sent to the administrator.This setting will not be accessible by a user.



Modifications have not been saved. If all changes have been made, please click on **Update** below.

□ Delete Duplicate Mails □ Subscribe to Anti Spam Filter

[Select Action] after --

Action 1: Autoreply and Forward to

Thank you for your email for our organisation. We would like to infor that your email is exceeded the permission level as per our company policy, thought it will send to the specified user this time, we woluld like to give signature while sending mails next time.

□ Autoreply to each email ID more than once

Add a unique ID to subject

If size is less than 1M bytes

[select condition]

[select condition]

[select condition]

[select condition]

[select condition]

Fig. 1.22 –The â€˜Mail Filter Settingsâ€™ Screen

Scenario: Setting a filter for â€˜ALLâ€™ users which will Autoreply, send a copy to the userâ€™s Inbox, AND forward every mail above 10 MB to the system administrator.

Step 1: From the list of users viewed from the Mailfilter screen, click the â€˜Editâ€™ button against ALL.

Step 2: From the drop down list select â€œAutoreply and INBOX and forward to â€¦â€□ and click on â€˜Add Actionâ€™.

Step 3: Fill in the email ID of the System administrator in the space provided and a customized autoreply in the relevant field. Optionally, add a â€œUnique ID to the subjectâ€□ of the email to add a subtle reminder to the recipient. Spaces are not allowed in this ID and it is recommended that the ID be enclosed in brackets to avoid confusion. In our example,this will appear as [Large_size] in the subject of the email. Choose the string â€œIs Larger thanâ€□ from the drop down box and fill in the required size in the relevant field. The number can be suffixed by k for kilobytes and M for megabytes.

Step 4: Clicking on â€˜Updateâ€™ will now finalize the settings.

Similarly, relevant settings can be allocated for individual users or to all users.

1.5.1.8 Address book

This refers to the Address Book settings that a system administrator can make which will be of frequent use to the members of the LAN. A system administrator can hence make a group of email IDs from an external LDAP database which will then be available to the members of the LAN from their Webmail interface.

1.6 Advanced Settings

This section allows you to:

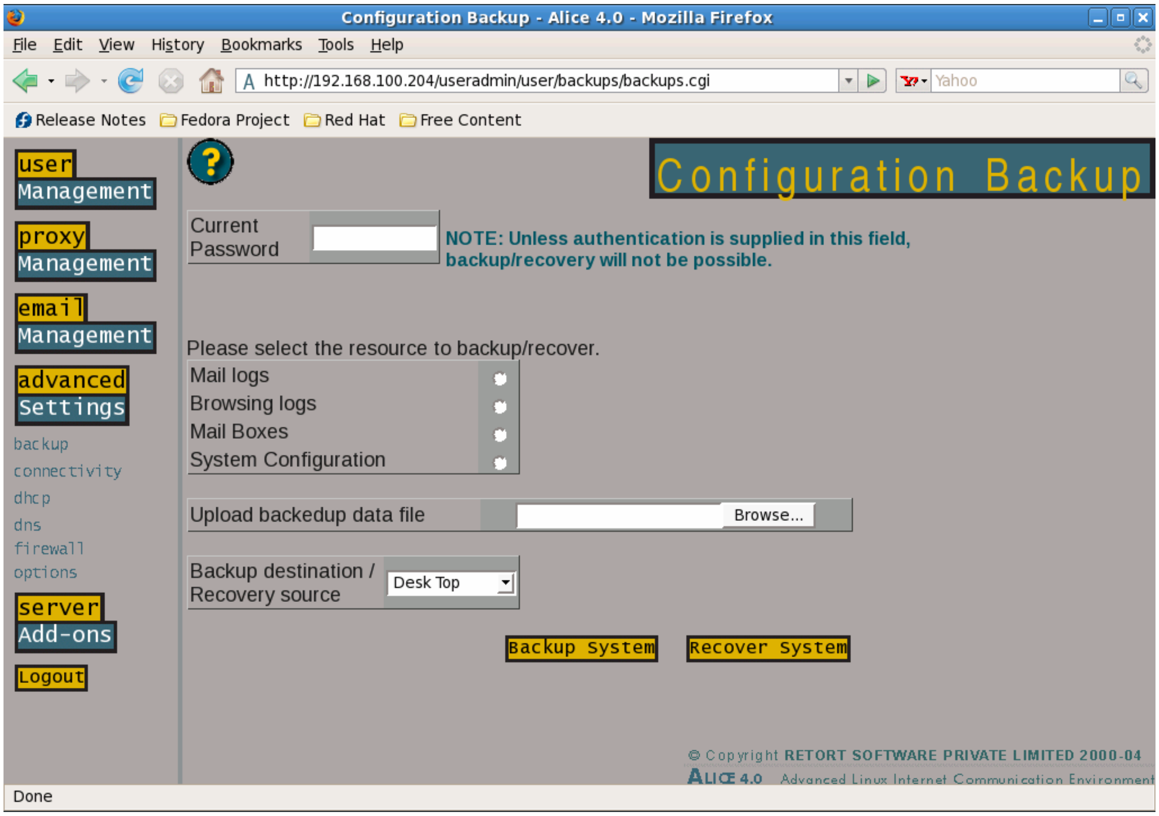
(a) Backup your system and restore it

(b) Provide and configure connectivity options to connect to other networks

(c) Change the â€œDateâ€□ on the system

1.6.1 Backup

This interface allows you to backup your entire Alice settings and to enable a recovery in case of some problem like hard disk failure. The same settings can also be restored on another machine in case you want to transport Alice to some other machine.



Current Password

NOTE: Unless authentication is supplied in this field, backup/recovery will not be possible.

Please select the resource to backup/recover.

Mail logs ○
Browsing logs ○
Mail Boxes ○
System Configuration ○

Upload backedup data file

Backup destination / Recovery source: Desk Top

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.23 –The â€˜Backup Settingsâ€™ Screen

The following fields are presented on the screen:

Before backing up you will need to enter your administrator password. This is to ensure foolproof security.

Next, select the Resource to be backed up by clicking on the â€˜Radioâ€™ button next to the various options provided (mail logs, browsing logs, mailboxes, system configuration).

The â€œBackup destination / Recovery sourceâ€□ option defines the destination of the file to be saved. Ensure that there is adequate space on the destination for backups.

Clicking on â€˜Backup Systemâ€™ will backup all the files to the destination specified. The â€œUpload backed up data fileâ€□ option is to be used to define the destination of an existing data file to enable a system restore.

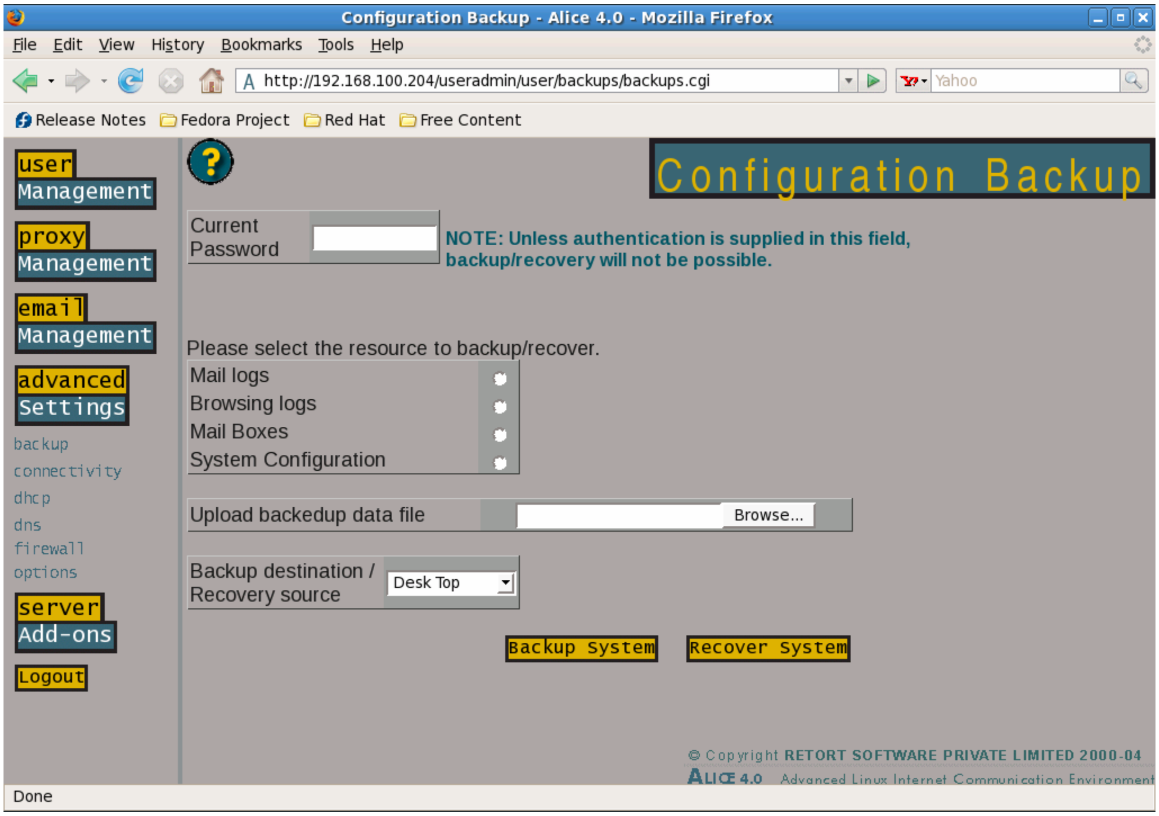
Clicking on â€˜Recover systemâ€™ will enable the system to return to its previous settings. This is recommended only in the case of a system crash.

1.6.2 Connectivity

These settings allow you to create, modify, delete, activate or de-activate profiles for the different types of connectivity specified in the drop down list.

1.6.2.1 New Account

Creating a new account for any of the connectivity options provided in the drop down box.



http://192.168.100.204/useradmin/user/backups/backups.cgi

Current Password

NOTE: Unless authentication is supplied in this field, backup/recovery will not be possible.

Please select the resource to backup/recover.

Mail logs ○
Browsing logs ○
Mail Boxes ○
System Configuration ○

Upload backedup data file

Backup destination / Recovery source: Desk Top

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.24 –The â€˜Dialoutâ€™ Screen

1.6.2.1.1 Dialout

Select Dialout from the drop down list and click on â€˜New Accountâ€™. This interface allows you to specify settings which allow you to connect to the Internet or to a sub network.

Dialout Name: Specify a name for the profile. Use a simple name that can be easily identifiable. You may give the phone number as the profile name or the name of the ISP. For example, 4404444 or VSNL.

Trusted Remote: Low (Direct Internet) - Used when Alice connects to the Internet. High(Internal Networks) - Allows Alice to work with multi subnets within the LAN.

Set Default Gateway: This option allows you to select the default gateway for the particular network.

Remote host login: Specify the username/login name to be used to dial-in to any remote server.

Remote host dial-in numbers: Enter the numbers used to dial-in to the remote server. If there is more than one number, separate them with a comma.

Connection Port: Specify the port to which the communication device (modem or ISDN) is connected. Select the right port ranging from COM1 to COM4 from the drop-down list. If an ISDN card is used then select the ISDN channel accordingly in the drop-down list that is ISDN CH1 or ISDN Ch2.

Select dialing mode: If the exchange provides for Tone dialing, select that. Else, set it to Pulse dialing.

Authentication method: Select the authentication method to connect to your remote server from the drop-down list (Options are PAP, CHAP, Interactive or None). For example, VSNL uses Interactive and PAP authentica0tion while MTNL uses PAP. Optionally NONE can also be selected from the drop-down list.

Password: Enter the Password for authentication on the remote server.

Re-enter password: To confirm that the password entered is correct, re-enter the password in this field.

Prefix(PBX) for outside numbers: If dialing from an EPABX then enter the number to be dialed to get the dial tone. The number might be 0 or 9 depending on the type of PBX dialing system used in the organization. A comma or few commas can be added to get the dial tone before dialing, for example '0,' or '0,,'.

Modem initialization string: Enter certain modem strings additionally required. The string may be something like ATX3 (if the modem cannot detect the dial tone) or Atl3 (for increasing the volume). Check the modem manual for additional settings.

Interactive ISP remote command: Enter the Interactive Remote server remote command such as 'ppp' if using an interactive type of authentication. This is however optional and depends on the type of authentication methods used by the remote server.

Clear: Clears all data and does not save it. A new form will be presented to enter the data again.

Create: It creates a connection profile with specified settings and saves the settings.

1.6.2.1.2 Local Net

This option allows the administrator to configure alternate IP addresses for dialout/dialin.

Local Net Name: Specify a name for the profile. Use a simple name that can be easily identifiable. The profile name can be only alphabets or alphanumeric (it should start with a character).

Trusted Remote: Low (Direct Internet) – Used when Alice connects to the internet. High (Internal Networks) – Allows Alice to work with multi subnets within the LAN.

Set Default Route: This option allows you to select the default gateway for the particular network.

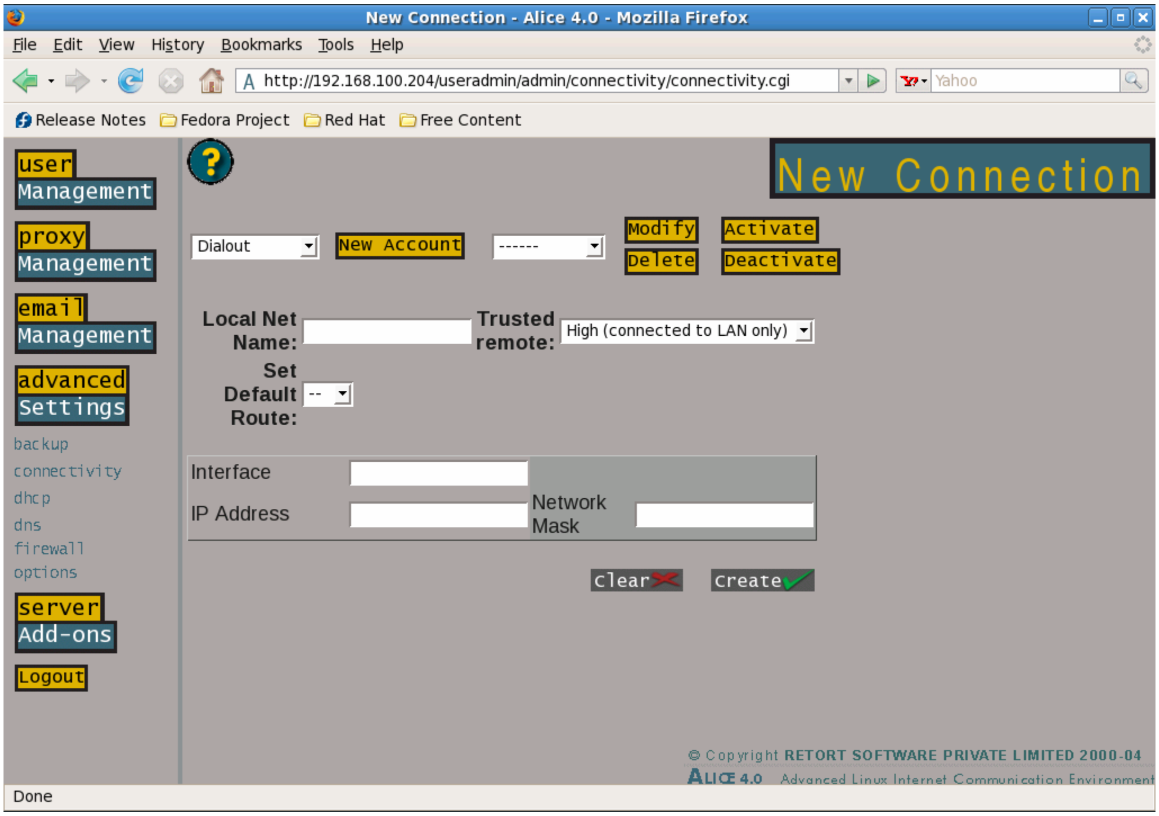
Interface: Enter the interface name for the virtual interface to be created on the available physical interface. For example eth0:0,eth0:1 where 0 and 1 are two virtual interfaces to be created on eth0.

IP Address: Specify the IP address in this field but this IP address should not be a part of the LAN IP addressing Scheme. It is recommended that the third number should be different from the IP address of the Alice server.

Network Mask: Depending upon the IP address specify the corresponding network mask.

Clear: Clears all data and does not save it. A new form will be presented to enter the data again.

Create: It creates a connection profile with specified Local Net settings and saves the settings.



Dialout

Local Net Name:

Trusted remote: High (connected to LAN only)

Set Default Route: --

Interface

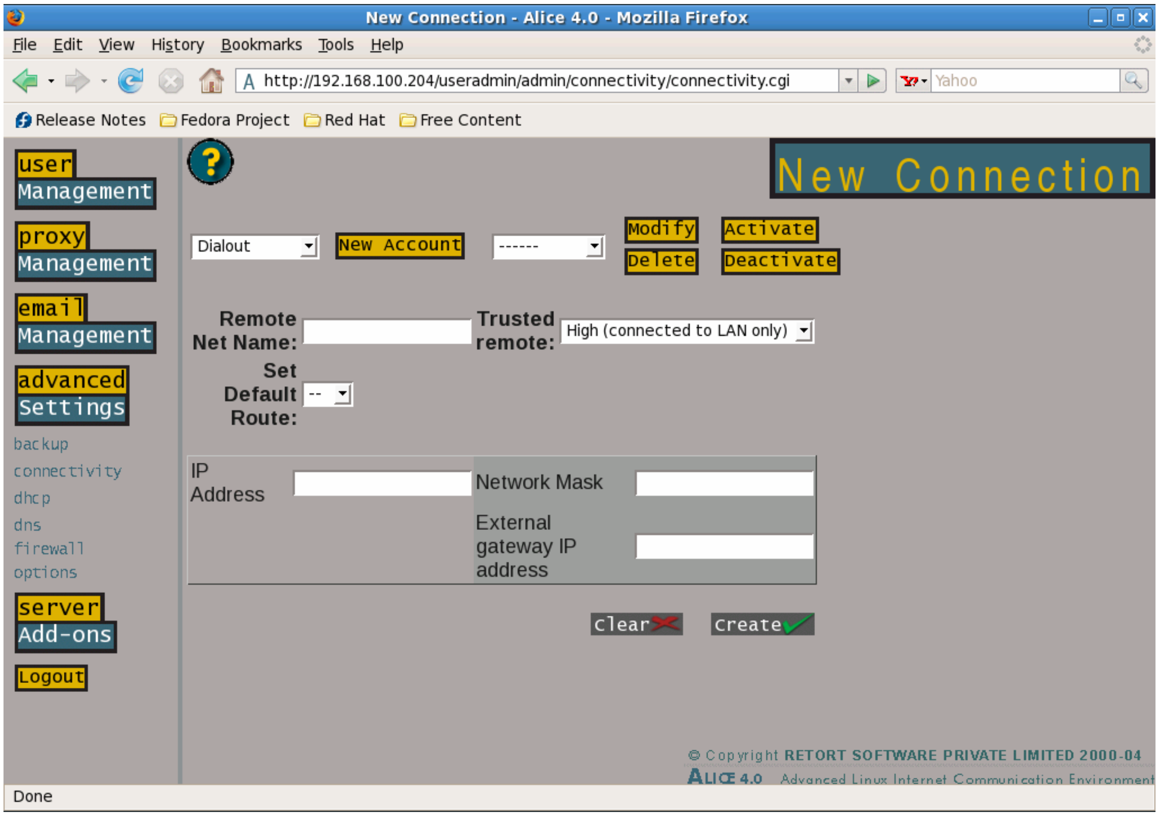
IP Address

Network Mask

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04

ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.25 –The â€˜Local Net Connectivityâ€™ Screen



http://192.168.100.204/useradmin/admin/connectivity/connectivity.cgi

Dialout | ------

Remote Net Name:

Trusted remote: High (connected to LAN only)

Set Default Route: --

IP Address:

Network Mask:

External gateway IP address:

Fig. 1.26 -The â€˜Remote Net Connectivityâ€™ Screen

1.6.2.1.3 Remote Net

This options allows different networks to get connected to known networks via Router or a Gateway

Remote Net Name: Specify a name for the profile. Use a simple name that can be easily identifiable. The profile name can be only alphabets or alphanumeric (provided it starts with a character).

Trusted Remote: Low (Direct Internet) - Used when Alice connects to the internet. High (Internal Networks) - Allows Alice to work with multi subnets within the LAN.

Set Default Route: This option allows to select the default gateway for the particular network.

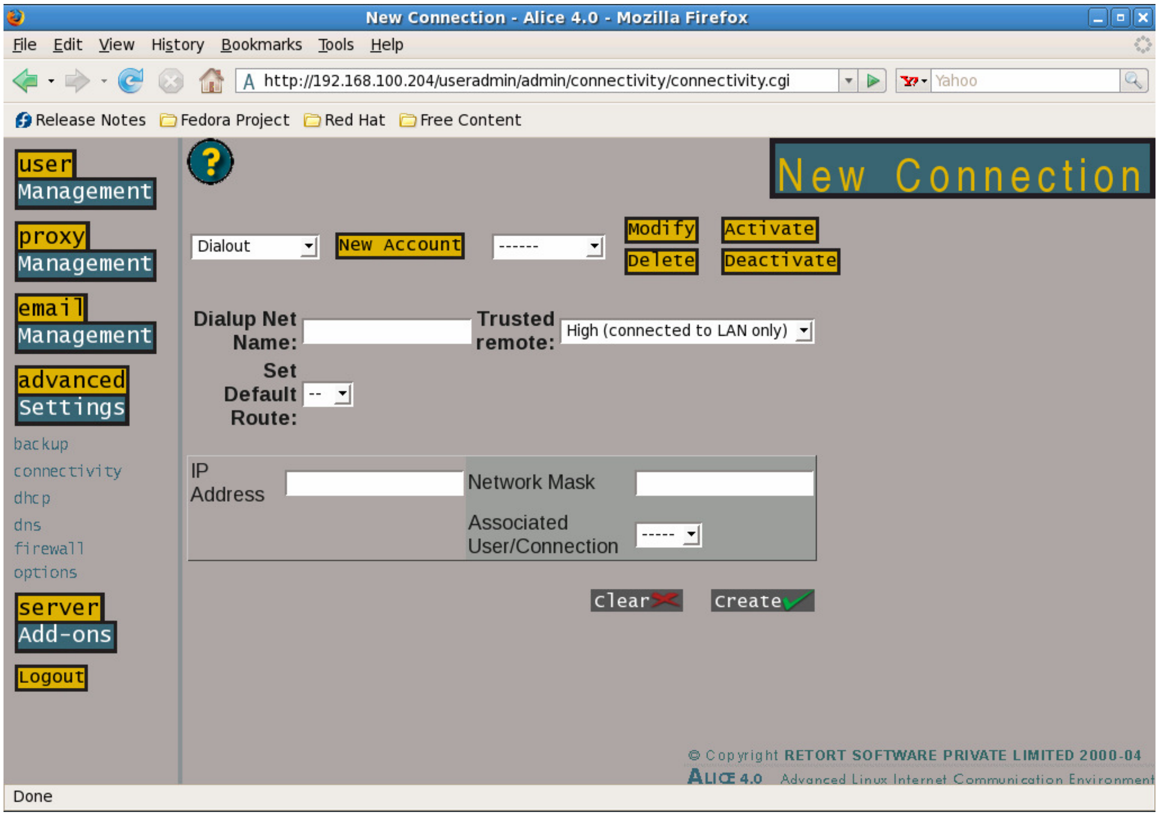
IP Address: Specify the IP address in this field but this IP address should not be a part of the LAN IP addressing scheme. It is recommended that the third number should be different from the IP address of the Alice server.

Network Mask: Depending upon the IP address specify the corresponding network mask.

External gateway IP address: Enter the IP address of the gateway through which you are connecting to the remote server. This may be a Router or a gateway machine.

Clear: Clears all data and does not save it. A new form will be presented to enter the data again.

Create: It creates a connection profile with specified Local Net settings and saves the settings.



New Connection - Alice 4.0 - Mozilla Firefox

http://192.168.100.204/useradmin/admin/connectivity/connectivity.cgi

New Connection

Dialout

Dialup Net Name:

Trusted remote: High (connected to LAN only)

Set Default Route: --

IP Address

Network Mask

Associated User/Connection: -----

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04

ALICE 4.0 Advanced Linux Internet Communication Environment

Done

Fig. 1.27 -The â€˜Dial-Up Netâ€™ Screen

1.6.2.1.4 Dial-up Net

This option is used to bring up the routing when the respective connection comes up. This connection request may be at either end.

Dial-up Net Name: Specify a name for the profile. Use a simple name that can be easily identifiable. The profile name can be only alphabets or alphanumeric (provided it should start with a character).

Trusted Remote: Low (Direct Internet) - Used when Alice connects to the internet. High (Internal Networks) - Allows Alice to work with multi subnets within the LAN.

Set Default Route: This option allows to select the default gateway for the particular network.

IP Address: Specify the IP address in this field but this IP address should not be a part of the LAN IP addressing Scheme. It is recommended that the third number should be different from the IP address of the Alice server.

Network Mask: Depending upon the IP address specify the corresponding network mask.

Associated User/Connection: This is the drop down box with the names of the users who have been allowed access. Users can be granted access from the Server add-ons>Dialin interface.

1.6.2.2 Modify Account

This control come in handy to modify an existing account which you may need to do due to various reasons.

a)From the â€œConnectiv ityâ€□ option, select the account to be modified from the drop down list, and click on the â€˜Modifyâ€™ Button.

b)The Saved data for the profile is now displayed. Make the necessary changes, and click on â€˜Updateâ€™ to save the changes.

c)To retain the previously entered data without making any changes, click on the â€˜Clearâ€™ button.

1.6.2.3 Delete Account

Select the account to be deleted from the drop down list, and then click on Delete to erase the account. This will permanently delete the account.

1.6.2.4 Activate Account

A profile that is created cannot be used for connectivity unless it is activated. Select the particular account, and click on â€˜Activateâ€™ . The option to activate an account is also presented at the time of creating a new account. Active profiles can be recognized by a carat (^) sign before their name.

1.6.2.5 Deactivate Account

This is used to deactivate an existing account in order to stop it from functioning. Chose the account to be deactivated from the drop down list, and click â€˜Deactivateâ€™. A deactivated account can always be activated at a later date via the manner described in the above section.

Note: In case you modify the current active connectivity account, a new account called 'active' is created. Select 'active' from the drop-down menu and click on the â€˜Activateâ€™ button to over-write the previously entered configuration for the connectivity account that was created.

1.6.3 Options

This allows you to change the zone and/ or date on the system.

Clicking on â€˜Change Zoneâ€™ will take you to a screen showing a drop down list of the various time zones, while clicking on â€˜Change Dateâ€™ will allow you to change the date and time either by changing the value in the fields, or by specifying the amount to be added or subtracted.

1.7 Server add-ons

These refer to the additional features that have been opted for by the organization, and thus will be different for different organizations. As we intend to keep making more services available to our customers, this section is liable to keep changing, and we urge you to check our website for the latest version of the manual.

1.7.1 Dialing

This screen is brought up when a remote user dials into the server. If a Multiport card is installed, the make would need to be specified, or else the port on which the modem is attached is to be specified. Next specify an IP Address which can be assigned to theremote user. Make sure that the user is allowed access to dial into the server by checking the box against his name, and clicking on â€˜Updateâ€™.

1.7.2 Fax Server

This interface allows you to use the Alice as a server to send and receive faxes, and hence provides an economical mode of communication. Members of the LAN, can send or receive faxes from their desktops. The faxes will be delivered to the fax machine at the otherend. It is also possible to configure Alice to get its input from a fax machine.

Setting up Alice as the Fax Server:

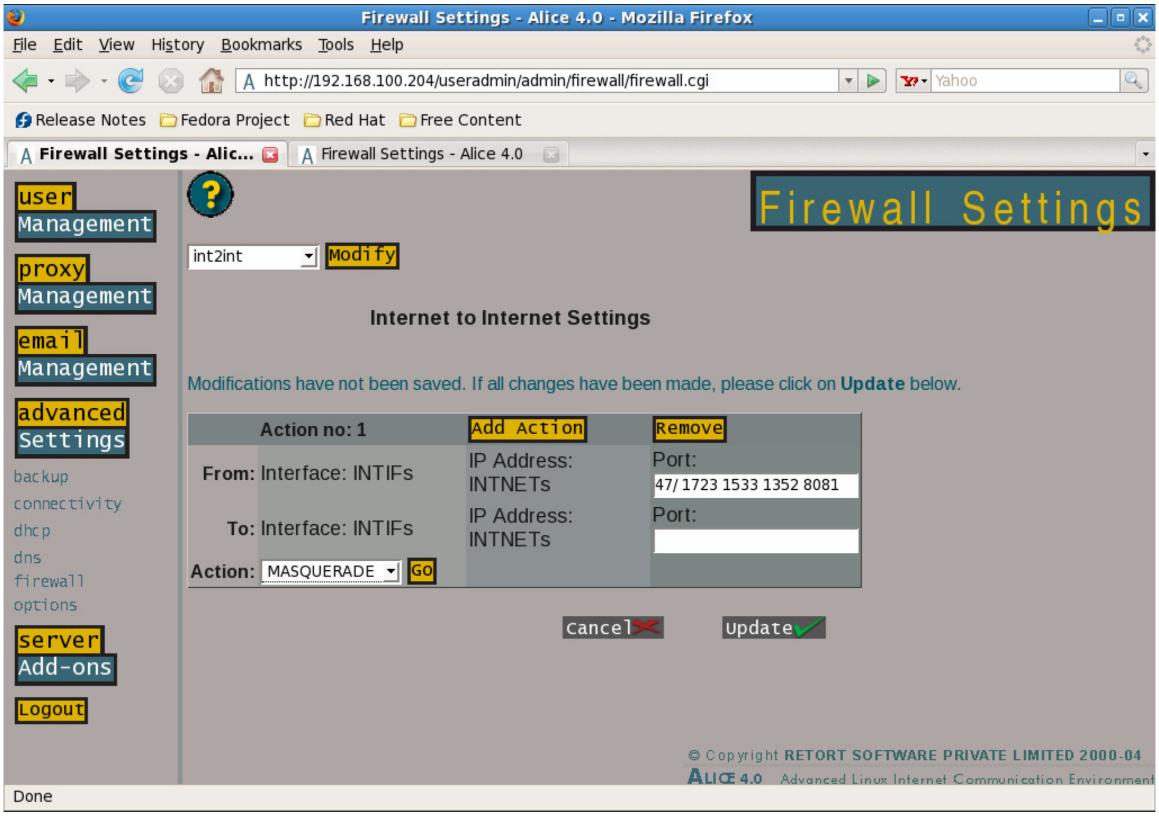
The interface requires the administrator to enter the com port on which the fax modem is connected. He can specify the users who have access to the facility, by filling their details under the MAP interface. Here, each user would be allocated a specific Number Prefix, which would be mapped to their email address, and serves as the identification for the recipient. Hence any person sending a fax to a particular person in the organization, would be faced by an Interactive Voice Response System (IVRS), when he dials the fax number, and would then need to enter the Number prefix for the particular person he wants to send the fax to. The fax would then be converted to an email, and be emailed to the user within the organization.

The User end:

In order for enable users to send faxes from their desktop, they would need to download a small application from the Alice server which would be available in their individual profile page when they log onto the Alice with their user name and password. This applicationsimulates a fax printer on the client machine, which treats the Alice server as the printer.Hence to send a fax from the desktop, the user would need to go to the File menu and select print. From the interface, he would now be required to select Alice as the printer from the drop down list and click on â€˜OKâ€™. This will present the user with a pop-up box, asking for the name and phone number of the recipient. Once that is completed, Alice will proceed to fax it to the relevant destination.

1.7.3 Firewall

This refers to the basic firewall that is provided with Alice. A more advanced version of the firewall, can also be opted for by the organization.Since this works on the principal of ports, choosing Allow or Deny for any particular service will Allow or Deny access to that service in the Internet to server traffic, and hence safeguard the server from any system intrusion attempts.



http://192.168.100.204/useradmin/admin/firewall/firewall.cgi

int2int

Internet to Internet Settings

Modifications have not been saved. If all changes have been made, please click on **Update** below.

Action no: 1

From: Interface: INTIFs
IP Address: INTNETs
Port: 47/ 1723 1533 1352 8081

To: Interface: INTIFs
IP Address: INTNETs
Port:

Action: MASQUERADE

© Copyright RETORT SOFTWARE PRIVATE LIMITED 2000-04
ALICE 4.0 Advanced Linux Internet Communication Environment

Fig. 1.28 –The â€˜Firewall Settingsâ€™ Screen

Advanced Firewall: if you have opted for the Advanced Firewall. Once again, this works on the principal of ports defined for specific communication interfaces, and provides the option for a series of actions that could then be allocated to specific ports on specific interfaces.The drop list provides you with the different GUI options for customizing your firewall.

The different options provided include:

User Defined specified by the administrator, and can be used for any interface or ports

Internet to Internet (int2int)
Internet to LAN (int2lan)
Internet to Server (int2ser)
LAN to Internet (lan2int)
LAN to LAN (lan2lan)
LAN to Server (LAN2ser)
Server to Internet (ser2int)
Server to LAN (ser2lan)
Server to Server (ser2ser)

The User Defined Interface can be used for any communication interface, while the other options are customized for specific purposes.

Choose User Defined from the drop down list, and click â€˜Modifyâ€™. Here you see screen for customizing User Defined Firewall Settings.

The Interface could be an Internet interface, or a LAN interface. The possible options can be seen in the drop down box below.

Deny:would deny all communication requests between the specified interfaces without any notification.

Reject: would deny all communication requests between the specified interfaces and will also send an error message.

Accept: would allow communication between the specified interfaces

SNAT: Source Nating

DNAT: Destination Nating

Redirect: The communication from interface one on the specified port would be redirected to the interface specified on the port specified.

Masquerade:

A form of NAT that that lets you use a single connected computer running Linux with a real IP address as a gateway for unconnected machines with a fake IP address.

By default all traffic on all ports is blocked. Using the different options, the administrator could specify the ports between which he would want to allow traffic and hence communication.

Thus, the administrator could open traffic from the server to the Internet (ser2int) on port 80 on the relevant interface (allowing for HTTP access) and then allow the same on the Internal LAN to the server (LAN2ser) thus allowing the members of the LAN permission to access the

Internet. The permissions for individual users could then be specified in the User Management screen.

Similarly, FTP access, etc. could also be enabled.

1.7.4 dns

The Domain Name System settings allow you to use the Alice server as the dns server for both your corporate domain(s), as well as your internal Intranet. Additions could be made for domains for which Alice serves as the Master or Slave. Setting Alice as a Master for a zone, would imply that Alice serves as the DNS server for that zone, while setting it as a Slave for a zone, would route the request to the correct DNS server.

Clicking on â€˜Editâ€™ will allow you to edit the records for a specific entry.

1.7.5 IPSec VPN

Short for Internet Protocol Security, IPSec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. This protocol encrypts both the header and the payload and on the receiving side an IPSec-compliant device decrypts each packet.
It works on the principle of secure certificates one common server certificate, and a personalized certificate for each individual user. The administrator would need to create a profile for each permissible user, based on which a set of two certificates would be generated for each user. Both certificates which would need to be imported on the client system (typically a Windows machine). The client would require a small program that can be downloaded from his profile on the

Alice server (accessed by logging in with his network login and password). This program once configured with the client's dial out settings, will establish the connections with the server thus, creating a Virtual Private Network, allowing the client access to the corporate LAN.