TM-210, TM-270, TM-510, TM-560, TM-600, TM-800, TM-1000, TS-300, TS-700, TW-100 Administrator Manual

Version 6.0

The R-HUB TM-210 and TM-270 “6-in-1” web conferencing
and TW-100 webinar servers

The R-HUB TM-510 and TM-560 “6-in-1” web conferencing
and TS-300 remote support servers

The R-HUB TM-600, TM-800 and TM-1000 “6-in-1” web
conferencing and TS-700 remote support appliances

R-HUB Communications, Inc.
4340 Stevens Creek Blvd.
Suite 282
San Jose, CA 95129
support@rhubcom.com
http://www.rhubcom.com

Contents

1. Installation & Registration

The Web conferencing server package includes:

- TM-210, TM-270, TS-300, TM-510, TM-560, TM-600 TM-800, TM-1000, or TS-700 server
- Analog console cable
- Power cord. Power brick (for TM-210, TM-270, TS-300, TM-510, TM-560 only)

1.1. Accessing your R-HUB Web Conferencing Server

There are two ways to access the TM-210, TM-270, TM-510, TM-560 servers: by using plug-and-play or by using a direct cable connect. To access the TM-510, TM-560, TM-600, TM-800, TM-1000, TS-300 and TS-700 servers, use plug-and-play. In all cases, an Internet browser needs to be used to access and configure the server.

I. Plug-and-Play

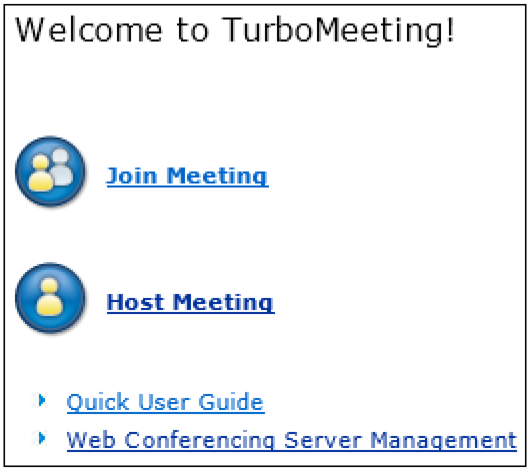
This method requires that you have:

- A DHCP server on your network
- A computer with Microsoft Windows (2000, 2003, XP, Vista, Windows 7, Windows 8, Windows 10)

It is important to follow the instructions below to start the server for initial setup:

1. Connect the server with an Ethernet cable (not a crossover cable) to your network
2. Plug in the power cord to automatically power on the server
3. Wait for the ready light to turn green. This usually takes about 30 seconds.

Open a browser on your computer and type "http://myonlinemeeting". The following page should appear:



Welcome to TurboMeeting!

Figure 1.1 Home Page

If the page does not display and you are familiar with your router, check the IP address your router has assigned to the R-HUB server, which is named “myonlinemeeting”. Then input the IP address in your browser’s address bar and you will be able to access the R-HUB server.

If the page does not display and you are not familiar with your router, go to the following initial startup method.

II. Local Access

For the TM-600, TM-800, TM-1000, and TS-700 servers only, if you fail to access the server by the above method, do the following:

- Plug in your keyboard, mouse and monitor to the server
- Power on the server
- Wait for 1 minute
- Type “**turbomeeting**” as the Username and “**password**” as the Password
- Wait for up to a couple of minutes and you will be connected to the Fedora desktop.
- Open a browser by clicking the browser icon on the top banner
- This will take you to the TurboMeeting web login page (Figure 1.2)
- Follow the sections below to configure the server using the browser.

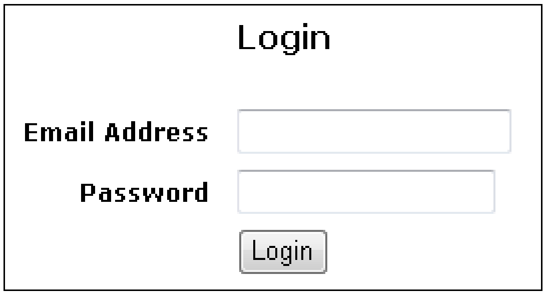


Figure 1.2. Login

For the TM-210, TM-270, TM-510 and TM-560 servers only, if you fail to access the server by Plug-and-Play, do the following:

- Plug a serial cable between the server and a computer
- Power on the server
- Wait for 1 minute
- Use HyperTerminal or the open source Tera Term program. The serial port settings are: Baud rate: 115200   Data: 8 bit   Parity: none   Stop: 1 bit
- Type “**admin**” as the Username and “**password**” as the Password
- Type “ifconfig” to determine the IP address (inet addr) of the server
- Follow the sections below to configure the server using the browser.

III. Direct-Cable Connection

The direct-cable connection method is for the TM-210, TM-270, TM-510 and TM-560. Before you use this method, configure your computer (in any operating system) with the following IP setting:

- IP Address: 192.168.1.100
- Subnet Mask: 255.255.255.0

Next, do the following:

- Disconnect your computer from any network including the wireless
- Power on the R-HUB server (as described above)
- Wait for the ready light to turn green. This usually takes about 90 seconds
- Connect the R-HUB server to your computer using a crossover-cable or any internet cable
- On your computer, open a browser and in the address bar type http://192.168.1.192. The home page (Figure 1.1) should display.
- Because your server is not connected to the Internet, when you click the link "Web Conferencing Server Management", the registration page (Figure 1.3) will not display. To bypass the registration page, type http://192.168.1.192/as/wapi/login?b=y.

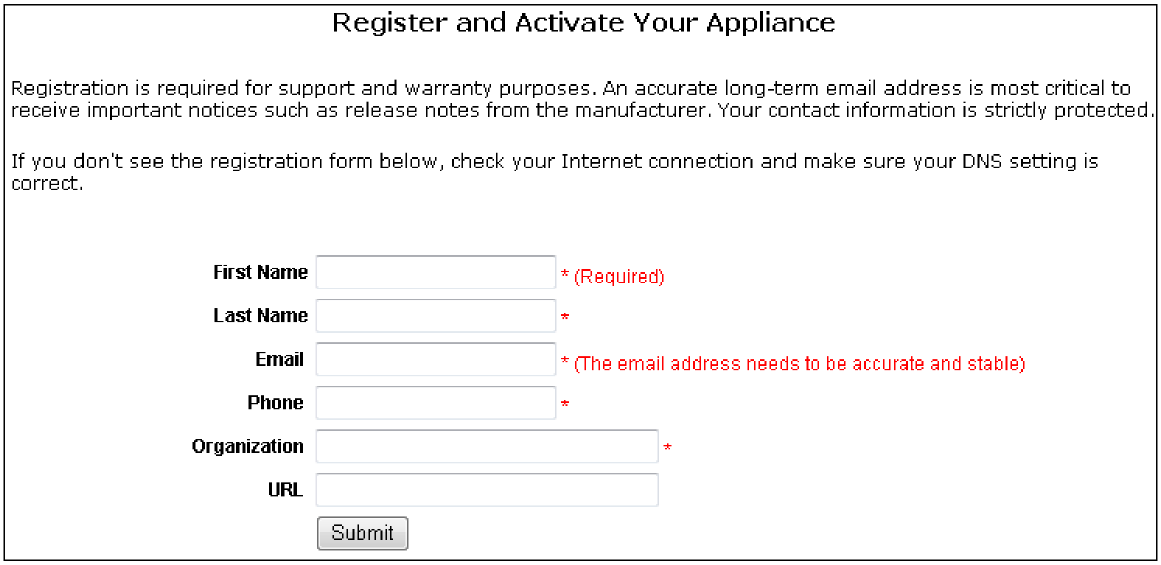
Once you have accessed the meeting server, you are ready to configure the server. Do not disconnect your computer from the meeting server before you complete the configuration described in the next section. After the configuration, connect the R-HUB server to your network using a regular Ethernet cable (which is not included).

Note that after you change the system IP settings, the web page will hang. You will need to use the new IP address to access the server.

1.2 Registering your R-HUB Web Conferencing Server

When you receive your R-HUB server, you have to register in order to receive software updates and technical support. To register your server, access the meeting server home page (Figure 1.1), and click the "Web Conferencing Server Management" link. The Registration Page (Figure 1.3) appears. If you are using the direct-cable connection method to access your server (Section 1.1, Part III), type http://192.168.1.192/as/wapi/login?b=y to bypass the registration page since the server is not connected to the internet yet.

It is important to specify an email address that will last a long time to insure that you receive important notices such as product release notes from the manufacturer.



Register and Activate Your Appliance

Registration is required for support and warranty purposes. An accurate long-term email address is most critical to receive important notices such as release notes from the manufacturer. Your contact information is strictly protected.

If you don't see the registration form below, check your Internet connection and make sure your DNS setting is correct.

First Name * (Required)

Last Name *

Email * (The email address needs to be accurate and stable)

Phone *

Organization *

URL

Figure 1.3 Registration Page

2. Configuring the R-HUB Web Conferencing Server

After you access the meeting server home page (Figure 1.1), click the “Web Conferencing Server Management” link. If your R-HUB server is new, you will have to submit

- **admin** for the Email field
- **password** for the Password field

To change the default administrator account, you use “Manage Users” (see Section 4) to change the default email and password to your choice.

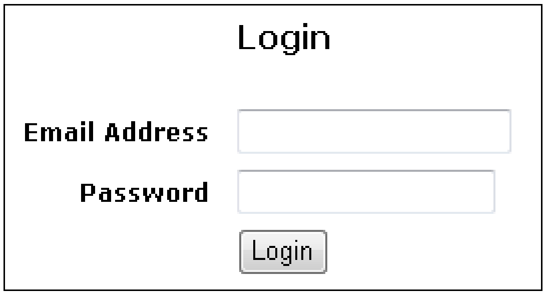
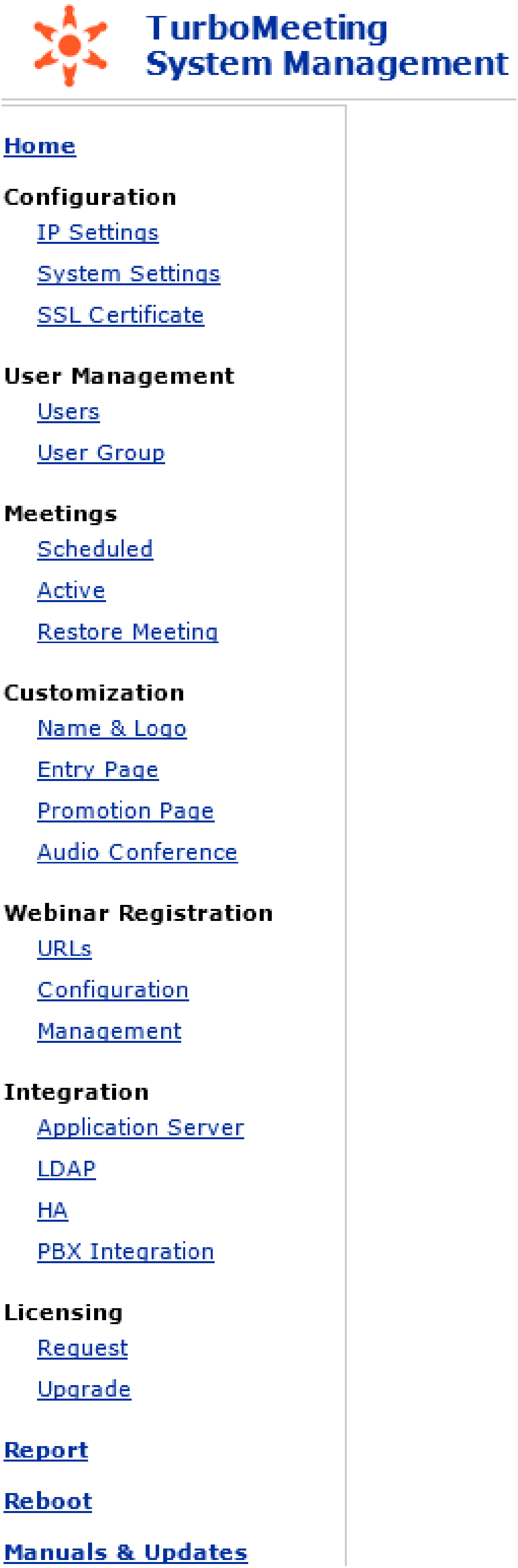


Figure 2.1 Login Page

After login, the **System Management** home page is displayed. The System Management Navigation frame is shown in Figure 2.2:



TurboMeeting
System Management

Home

Configuration

- IP Settings
- System Settings
- SSL Certificate

User Management

- Users
- User Group

Meetings

- Scheduled
- Active
- Restore Meeting

Customization

- Name & Logo
- Entry Page
- Promotion Page
- Audio Conference

Webinar Registration

- URLs
- Configuration
- Management

Integration

- Application Server
- LDAP
- HA
- PBX Integration

Licensing

- Request
- Upgrade

Report

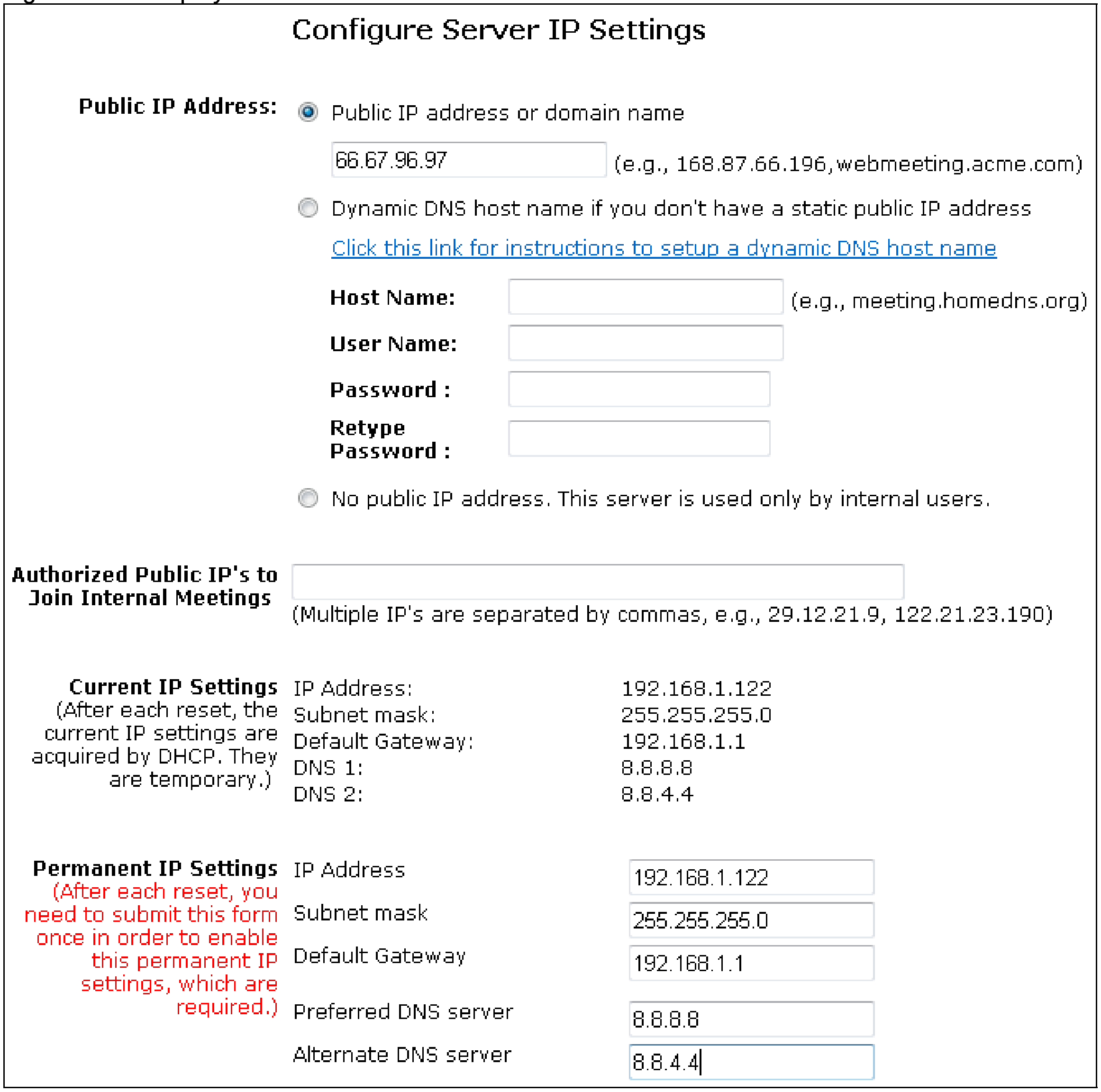
Reboot

Manuals & Updates

Figure 2.2 Management Home Frame

2.1. Configure Server IP Settings

In the left frame of the System Management page, under Configuration click the IP Settings link. Figure 2.3 is displayed:



Configure Server IP Settings

Public IP Address:

● Public IP address or domain name

66.67.96.97 (e.g., 168.87.66.196,webmeeting.acme.com)

○ Dynamic DNS host name if you don't have a static public IP address

Click this link for instructions to setup a dynamic DNS host name

Host Name: (e.g., meeting.homedns.org)

User Name:

Password :

Retype Password :

○ No public IP address. This server is used only by internal users.

Authorized Public IP's to Join Internal Meetings

(Multiple IP's are separated by commas, e.g., 29.12.21.9, 122.21.23.190)

Current IP Settings (After each reset, the current IP settings are acquired by DHCP. They are temporary.)

IP Address:	192.168.1.122
Subnet mask:	255.255.255.0
Default Gateway:	192.168.1.1
DNS 1:	8.8.8.8
DNS 2:	8.8.4.4

Permanent IP Settings (After each reset, you need to submit this form once in order to enable this permanent IP settings, which are required.)

IP Address	192.168.1.122
Subnet mask	255.255.255.0
Default Gateway	192.168.1.1
Preferred DNS server	8.8.8.8
Alternate DNS server	8.8.4.4

Figure 2.3 Configure Server IP Settings

Note that if you change the IP settings and submit the changes, your browser may hang because the IP is changed. You should use the updated IP to access the server.

The following describes the fields in Figure 2.3.

- **Public IP Address**

  In order for users outside your LAN to host or join meetings, you have to assign a public IP address. If you don't have a fixed public IP address, you can go to http://www.dyndns.com to set up a domain name and copy the domain information and your DynDNS user account information to the meeting server configuration page. After that, you can always access your R-HUB server by the domain name you set at DynDNS.

  Note that R-HUB offers the DynDNS client as a convenience to our customers. R-HUB is in no way affiliated with DynDNS or responsible for their service. Any fees that you may incur with DynDNS are between you and DynDNS and have nothing to do with R-HUB.

- **Authorized Public IP's to Join Internal Meetings**

  If you have branch offices outside your LAN and you don't have a VPN, use this setting to allow employees from those branch offices to join an internal secured meeting hosted in your LAN.

- **Current IP Settings**

  These are the IP addresses that the meeting server has currently.

- **Permanent IP Settings**

  The Permanent IP Settings refer to the desired IP settings you want your meeting server to have. The permanent IP address can be the same as the "Public IP Address" or different from the "Public IP Address". If the permanent IP is a local IP address, it will be different from the public IP address. In such a case, you will need to do port forwarding on your firewall router to forward TCP traffic from the ports (80 and 443) and TCP and UDP traffic from the port (8889) at the public IP address to the corresponding ports at the permanent IP address. See the next section for details.

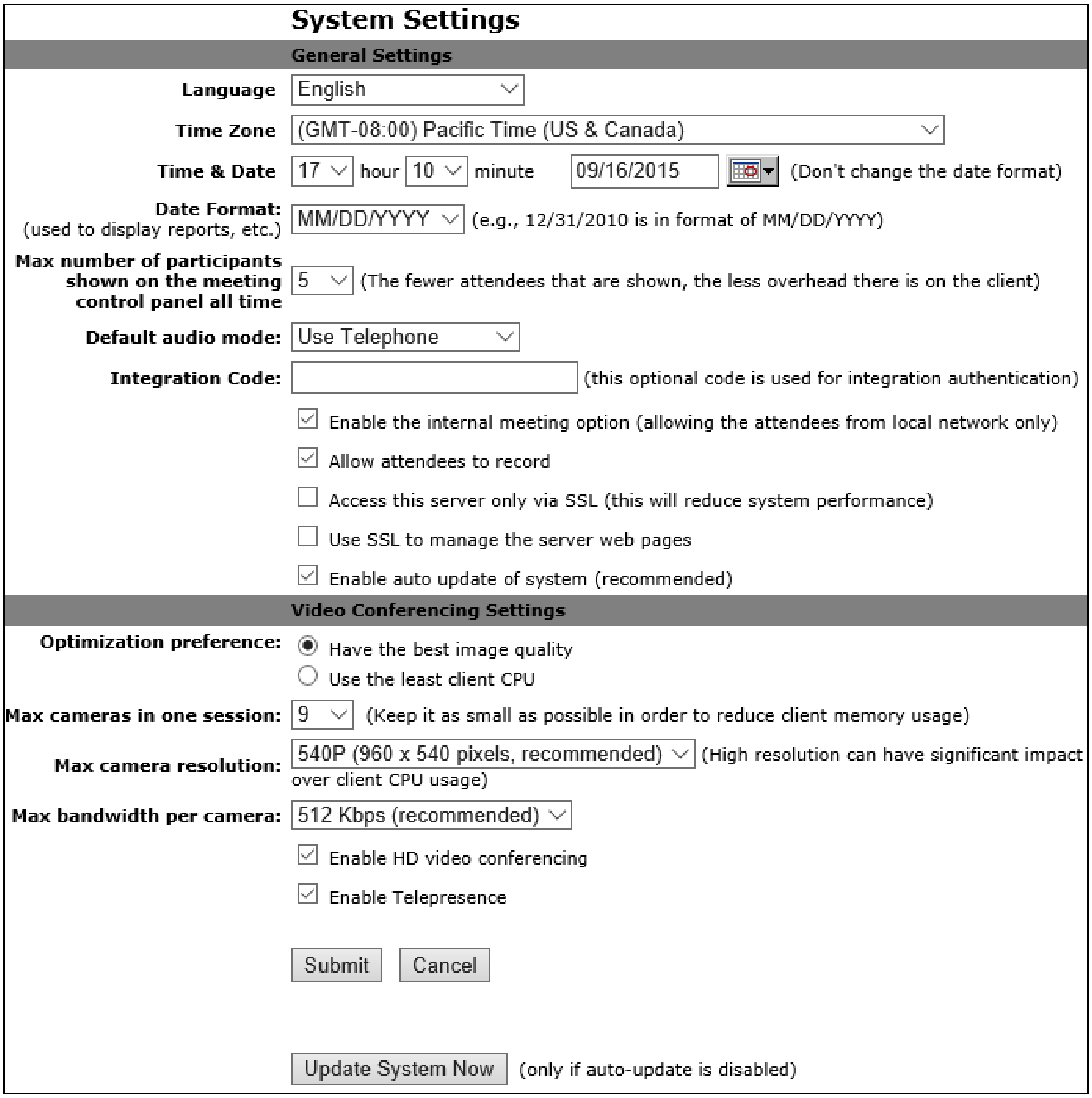
  Carefully check that the DNS settings are correct. Correct DNS settings are needed to allow the meeting server to connect to the R-HUB Communications' release servers so firmware updates can be applied. Correct DNS settings are also needed to allow updated audio conference numbers to be sent to your meeting server.

  Note that after you change the permanent IP settings, the web page will hang because the server IP address has been changed. You will need to use the new IP address to access the server.

If you make a mistake in configuration, you need to reset the server. See Section 7 for details.

2.2. System Settings

In the left frame of the System Management page, under Configuration click the System Settings link. Figure 2.4 is displayed.



System Settings

General Settings

Language	English
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
Time & Date	17 hour 10 minute 09/16/2015 (Don't change the date format)
Date Format: (used to display reports, etc.)	MM/DD/YYYY (e.g., 12/31/2010 is in format of MM/DD/YYYY)
Max number of participants shown on the meeting control panel all time	5 (The fewer attendees that are shown, the less overhead there is on the client)
Default audio mode:	Use Telephone
Integration Code:	(this optional code is used for integration authentication)

☑ Enable the internal meeting option (allowing the attendees from local network only)

☑ Allow attendees to record

□ Access this server only via SSL (this will reduce system performance)

□ Use SSL to manage the server web pages

☑ Enable auto update of system (recommended)

Video Conferencing Settings

Optimization preference:	● Have the best image quality ○ Use the least client CPU
Max cameras in one session:	9 (Keep it as small as possible in order to reduce client memory usage)
Max camera resolution:	540P (960 x 540 pixels, recommended) (High resolution can have significant impact over client CPU usage)
Max bandwidth per camera:	512 Kbps (recommended)

☑ Enable HD video conferencing

☑ Enable Telepresence

(only if auto-update is disabled)

Figure 2.4 System Settings

The following describes the fields in Figure 2.4.

- **Language**

  The language for the TurboMeeting System Management UI can be changed to English, Chinese (Simplified), Chinese (Traditional), French, German, Japanese, Spanish or Portuguese.

- **Time Zone, Time & Date,** and **Date Format**

  Set the correct time zone, time and date, and date format for the R-HUB server.

- **Max number of participants shown on the meeting control panel all time**

  Set the maximum number of participants that are shown in the “short list” in the meeting control panel. The presenter can open a window that shows a “long list” of all the meeting participants. Attendees that require attention (such as if they raise their hand) move to the top of each of these lists. The “long list” can be sorted by participant name.

- **Default audio mode**

  Set the default audio mode for attendees who have not already chosen their audio mode. The possible settings are “Use Telephone” and “Use Mic & Speakers”. The host of the meeting can override this setting in TurboMeeting’s Tools | Preferences dialog.

- **Integration Code**

  Use this to specify your own Integration Code which you can specify when using the integration features shown on our web site including the URL to schedule a meeting.

- **Allow attendees to record**

  This setting determines whether any attendees are allowed to record during a meeting.

- **Allow attendees to record**

  This setting determines whether any attendees are allowed to record during a meeting.

- **Access this server only via SSL**

  By default, screen images during a meeting are transmitted with R-HUB proprietary 256-bit encryption for efficiency. However, you can use SSL for encryption by enabling the **Access this server only via SSL** option. Your own SSL certificate is not required for this setting.

- **Use SSL to manage the server web pages**

  This setting determines if SSL is always used when displaying the TurboMeeting System Management web pages. It is recommended that you use your own SSL certificate with this setting so that web browsers do not complain about a domain name mismatch. See the section **Manage Your SSL Certificate** about how to upload your own SSL Certificate.

- **Enable auto update of system**

  The R-HUB server retrieves software updates automatically if this is enabled. This is done at 3 AM for the time set on the server. Updates typically happen twice per year.

- **Video Conferencing Optimization preference**

This setting lets your attendees “Have the best image quality” of the webcams at the expense of higher CPU usage or “Use the least client CPU” at the expense of using more bandwidth. Each user can override this setting in their client’s Tools | Preferences “Video” tab.

- **Max cameras in one session**

  This setting is a limit for the maximum number of webcams that can be started in an HD Video Conference. The downside of setting a high number, like the maximum of 30, is that the Windows and Mac client software will use more memory the higher this value is.

- **Max camera resolution**

  This setting specifies the maximum resolution for any one webcam in an HD Video Conference. The choices are:
    - 1080P (1920x1080 pixels)
    - 720P (1280x720 pixels)
    - 540P (960x540 pixels, recommended)
    - 360P (640x360 pixels)

  540P is a good trade-off between webcam clarity and bandwidth usage. 1080P and to some extent 720P could produce problems on slower computers, but our algorithms adjust for slower computers to automatically reduce CPU usage.

- **Max bandwidth per camera**

  This setting specifies the maximum resolution for any one webcam in an HD Video Conference. The choices are:
    - 128 Kbps
    - 256 Kbps
    - 384 Kbps
    - 512 Kbps (recommended)
    - 768 Kbps
    - 1 Mbps
    - 2 Mbps

  512 Kbps is a good trade-off between webcam clarity and bandwidth usage. A higher number could affect bandwidth usage at your company depending on the size of the meetings. This setting typically only affects the webcams that the viewer sees as larger. Our algorithms reduce bandwidth by only sending the webcam size that is required by the viewer. Thus, if the viewer sees one full-screen webcam, the download bandwidth usage in this case will be similar to that of four webcams that fill up the same screen.

- **Enable HD video conferencing**

  Turning off this setting will remove the ability for hosts to start HD Video Conferences and take away the ability for presenters to switch to HD Video Conference mode.

- **Enable Telepresence**

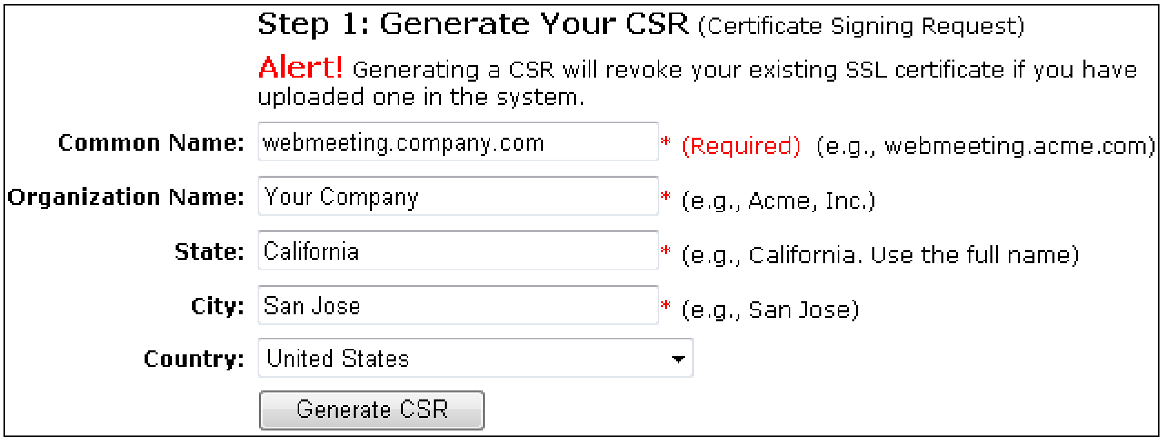
  Turning off this setting will remove the ability for each participant to use telepresence feature, which is the ability to use up to 8 monitors connected to one computer to see screen sharing on one monitor and webcams on the remaining monitors

- **Update System Now**

This feature retrieves updated R-HUB server software from the R-HUB web site.

2.3. Managing Your SSL Certificate

In the left frame of the System Management page, under Configuration click the SSL Certificate link. Step 1 of setting up an SSL certificate is displayed as in Figure 2.5.



Step 1: Generate Your CSR (Certificate Signing Request)

Alert! Generating a CSR will revoke your existing SSL certificate if you have uploaded one in the system.

Common Name: webmeeting.company.com * (Required) (e.g., webmeeting.acme.com)

Organization Name: Your Company * (e.g., Acme, Inc.)

State: California * (e.g., California. Use the full name)

City: San Jose * (e.g., San Jose)

Country: United States

Figure 2.5 Setting up an SSL Certificate, step 1

The following describes the fields in Figure 2.5.

- **Common Name**

  This is the domain name for your R-HUB server. This must match the domain name you specify in your SSL certificate.

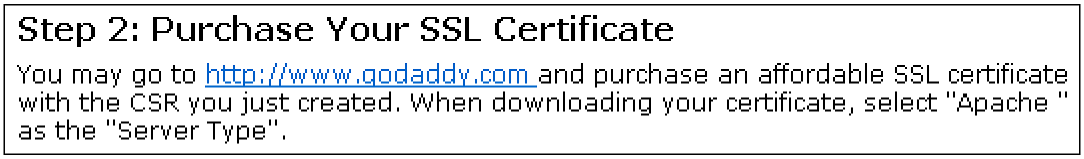
- **Organization Name**

  This is the Organization Name you specify in your SSL certificate.

- **State, City** and **Country**

  This is the State, City, and Country that you specify in your SSL certificate.

Next, obtain an SSL certificate as shown in Step 2 (Figure 2.6). For the SSL certificate, specify the same Common Name, Organization, State, City and Country that you specified in Step 1. Choose the SHA-2 signature algorithm for your SSL certificate, if you are given a choice.

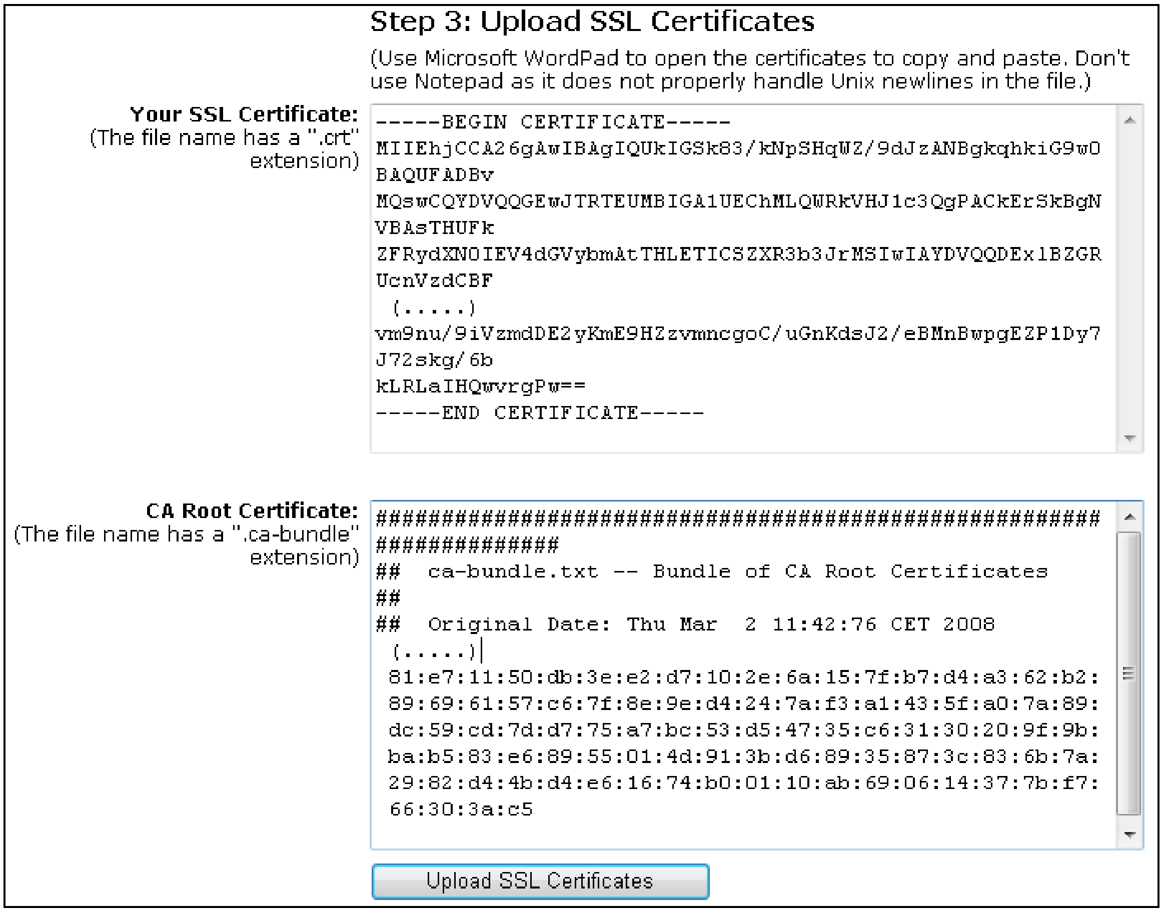


Step 2: Purchase Your SSL Certificate

You may go to http://www.godaddy.com and purchase an affordable SSL certificate with the CSR you just created. When downloading your certificate, select "Apache " as the "Server Type".

Figure 2.6 Setting up an SSL Certificate, step 2

You should use Chrome or Firefox to upload your SSL Certifcates. Locate your SSL Certificate file and your CA Root Certificate file (which may be called a “bundled root”). Sometimes your SSL provider may bundle these two into the same file. Using Microsoft WordPad, copy and paste the contents of these files into the files shown in step 3 (Figure 2.7).



Step 3: Upload SSL Certificates

(Use Microsoft WordPad to open the certificates to copy and paste. Don't use Notepad as it does not properly handle Unix newlines in the file.)

Your SSL Certificate: (The file name has a ".crt" extension)

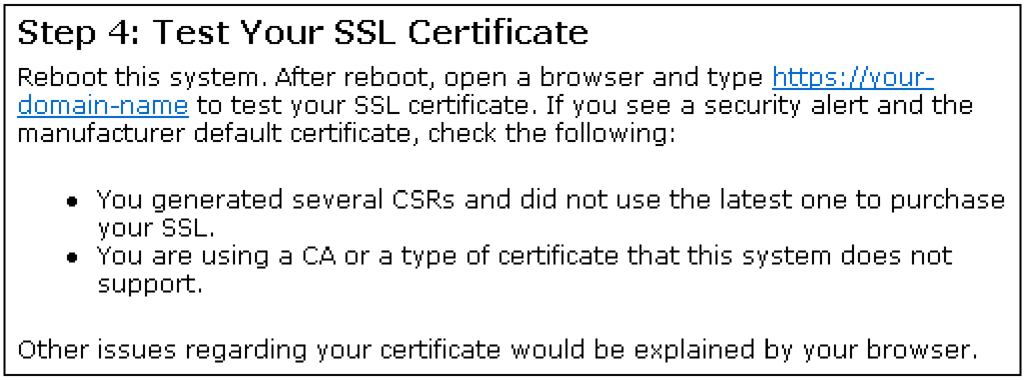
```
-----BEGIN CERTIFICATE-----
MIIEhjCCA26gAwIBAgIQUkIGSk83/kNpSHqWZ/9dJzANBgkqhkiG9w0
BAQUFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgPACkErSkBgN
VBAsTHUFk
ZFRydXN0IEV4dGVybmAtTHLETICSZXR3b3JrMSIwIAYDVQQDEx1BZGR
UcnVzdCBF
 (.....)
vm9nu/9iVzmdDE2yKmE9HZzvmncgoC/uGnKdsJ2/eBMnBwpgEZP1Dy7
J72skg/6b
kLRLaIHQwvrgPw==
-----END CERTIFICATE-----
```

CA Root Certificate: (The file name has a ".ca-bundle" extension)

```
#######################################################
##############
##  ca-bundle.txt -- Bundle of CA Root Certificates
##
##  Original Date: Thu Mar  2 11:42:76 CET 2008
 (.....)
 81:e7:11:50:db:3e:e2:d7:10:2e:6a:15:7f:b7:d4:a3:62:b2:
 89:69:61:57:c6:7f:8e:9e:d4:24:7a:f3:a1:43:5f:a0:7a:89:
 dc:59:cd:7d:d7:75:a7:bc:53:d5:47:35:c6:31:30:20:9f:9b:
 ba:b5:83:e6:89:55:01:4d:91:3b:d6:89:35:87:3c:83:6b:7a:
 29:82:d4:4b:d4:e6:16:74:b0:01:10:ab:69:06:14:37:7b:f7:
 66:30:3a:c5
```

Figure 2.7 Setting up an SSL Certificate, step 3

Test your SSL Certificate as described in step 4 (Figure 2.8).



Step 4: Test Your SSL Certificate

Reboot this system. After reboot, open a browser and type https://your-domain-name to test your SSL certificate. If you see a security alert and the manufacturer default certificate, check the following:

- You generated several CSRs and did not use the latest one to purchase your SSL.
- You are using a CA or a type of certificate that this system does not support.

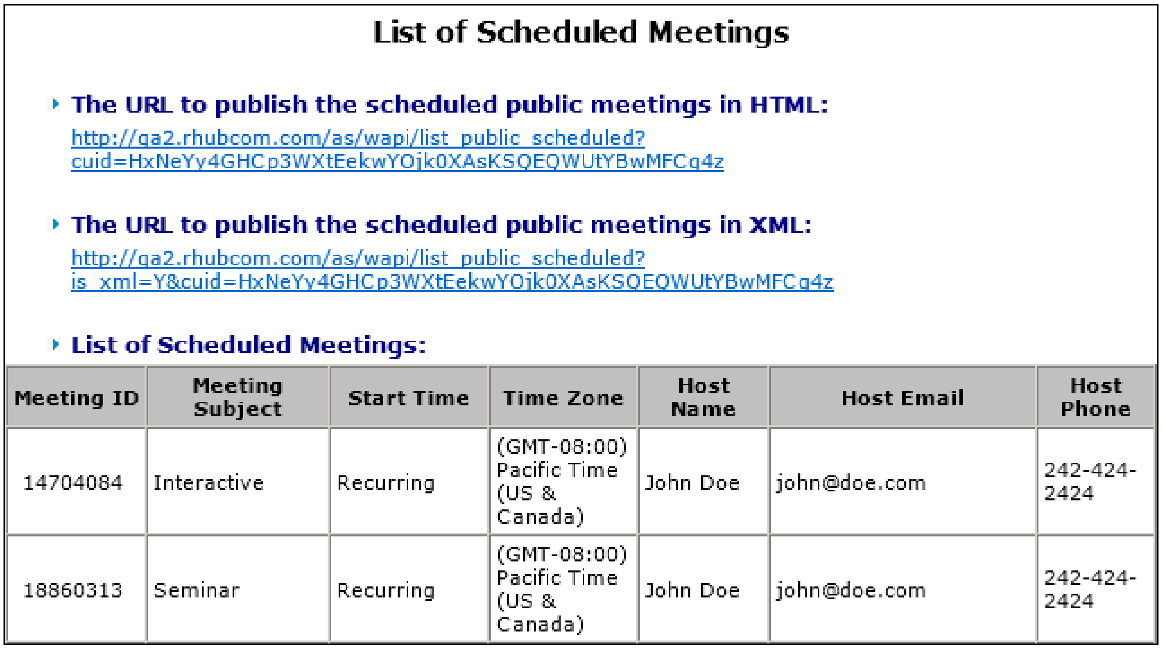
Other issues regarding your certificate would be explained by your browser.

Figure 2.8 Setting up an SSL Certificate, step 4

Note that the R-HUB server does not accept wildcard certificates.

2.4. Scheduled Meetings and Active Meetings

In the left frame of the System Management page, under Meetings click the Scheduled link. This feature shows you the list of scheduled meetings for your R-HUB server. The provided URLs show all of the public meetings and provide a link for how to join the meeting.



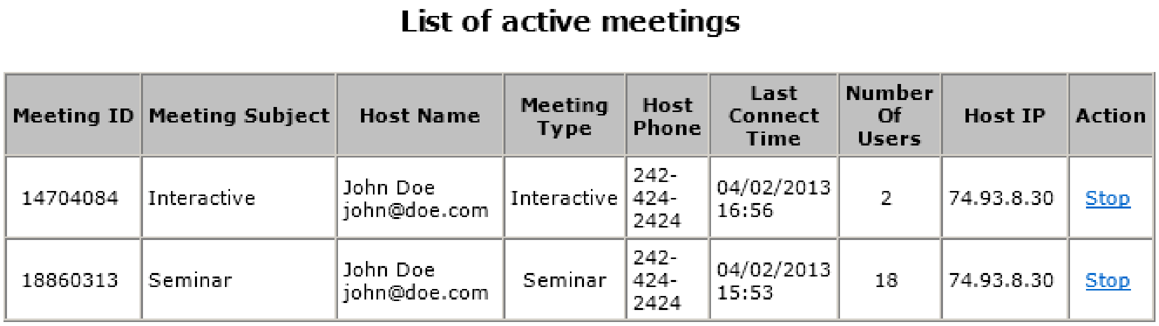
List of Scheduled Meetings

- **The URL to publish the scheduled public meetings in HTML:**
  http://qa2.rhubcom.com/as/wapi/list_public_scheduled?cuid=HxNeYy4GHCp3WXtEekwYOjk0XAsKSQEQWUtYBwMFCq4z
- **The URL to publish the scheduled public meetings in XML:**
  http://qa2.rhubcom.com/as/wapi/list_public_scheduled?is_xml=Y&cuid=HxNeYy4GHCp3WXtEekwYOjk0XAsKSQEQWUtYBwMFCq4z
- **List of Scheduled Meetings:**

Meeting ID	Meeting Subject	Start Time	Time Zone	Host Name	Host Email	Host Phone
14704084	Interactive	Recurring	(GMT-08:00) Pacific Time (US & Canada)	John Doe	john@doe.com	242-424-2424
18860313	Seminar	Recurring	(GMT-08:00) Pacific Time (US & Canada)	John Doe	john@doe.com	242-424-2424

Figure 2.9 List of scheduled meetings

In the left frame of the System Management page, under Meetings click the Active link. This feature shows you the list of active meetings for your R-HUB server. As the administrator, you can stop an Active meeting by clicking the Stop link as shown in Figure 2.10.



List of active meetings

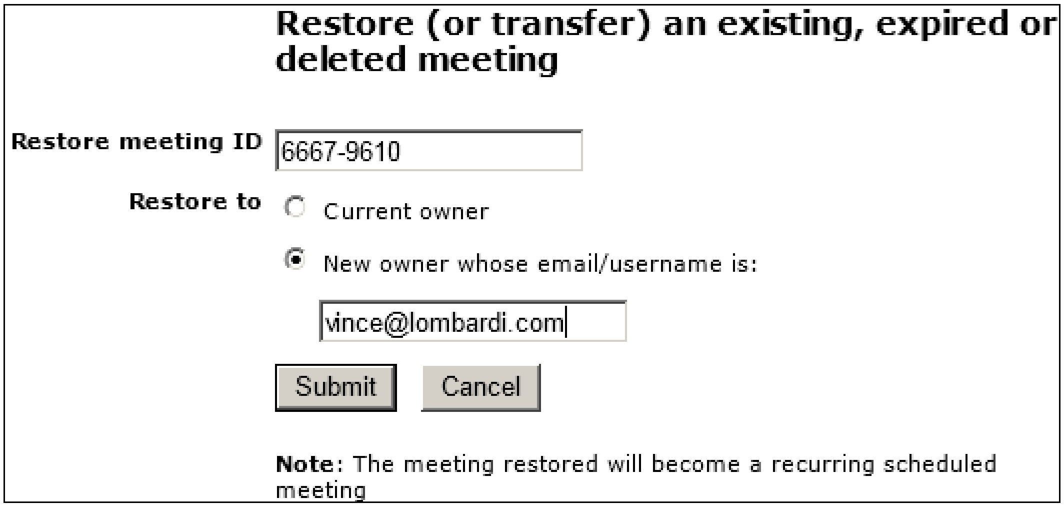
Meeting ID	Meeting Subject	Host Name	Meeting Type	Host Phone	Last Connect Time	Number Of Users	Host IP	Action
14704084	Interactive	John Doe john@doe.com	Interactive	242-424-2424	04/02/2013 16:56	2	74.93.8.30	Stop
18860313	Seminar	John Doe john@doe.com	Seminar	242-424-2424	04/02/2013 15:53	18	74.93.8.30	Stop

Figure 2.10 List of active meetings

2.5. Restore or Transfer Existing, Expired or Deleted Meetings

In the left frame of the System Management page, under Meetings click the Restore Meeting link. This feature allows you to restore a meeting that has expired or was deleted; and it allows you to transfer a meeting to another user, which is helpful if the original host of the meeting is unavailable.

To restore a meeting to its original owner, enter the meeting ID and select Restore to “Current owner”; click “Submit”. To transfer a meeting to a new owner, enter the meeting ID, select Restore to “New owner whose email/username is” and specify the email id or user name; click “Submit”.



Restore (or transfer) an existing, expired or deleted meeting

Restore meeting ID: 6667-9610

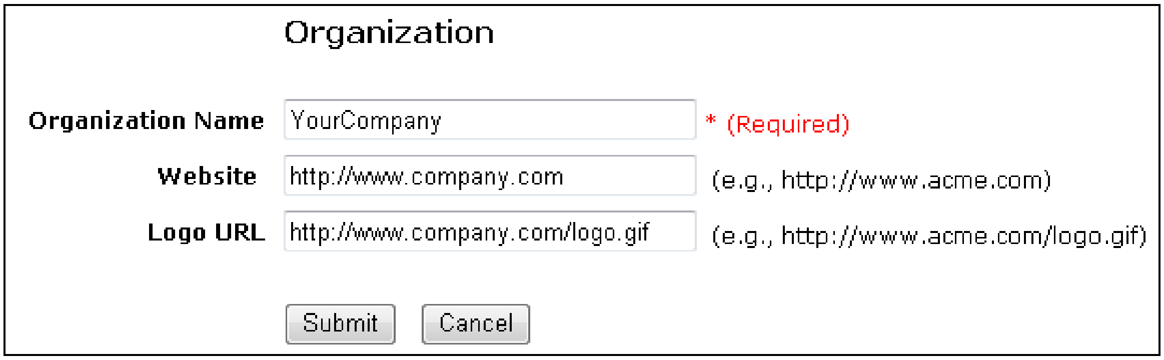
Restore to:
○ Current owner
● New owner whose email/username is: vince@lombardi.com

Note: The meeting restored will become a recurring scheduled meeting

Figure 2.11 List of scheduled meetings

2.6. Customizing the Meeting Start and Promotion Pages

In the left frame of the System Management page, under Customization click the Name & Logo link. This feature allows the Administrator to use show your company’s name and logo on the standard meeting home page.

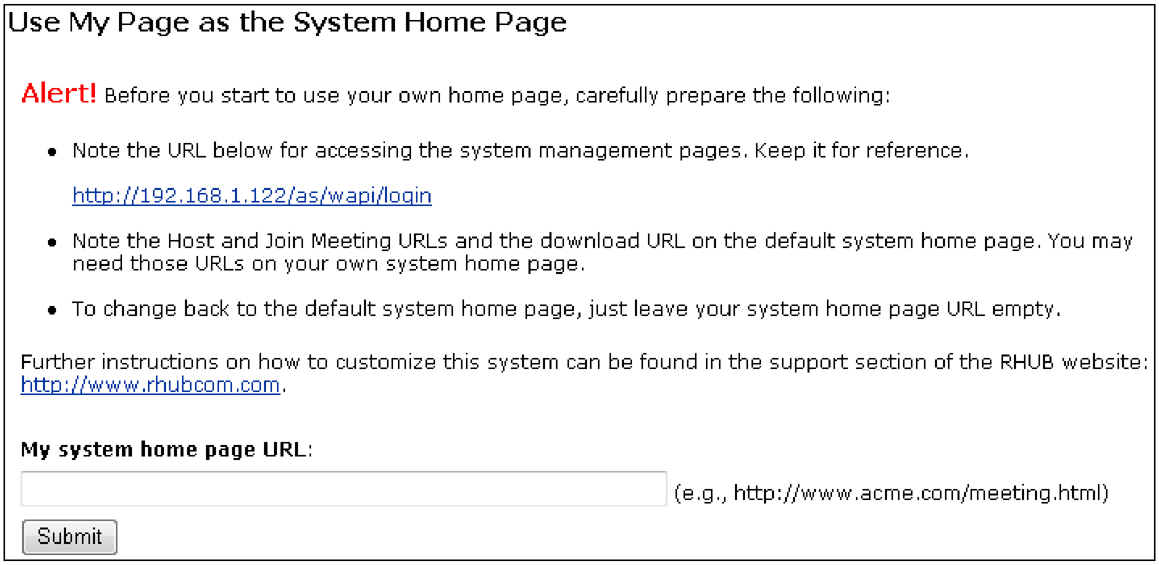


Organization

Organization Name	YourCompany	* (Required)
Website	http://www.company.com	(e.g., http://www.acme.com)
Logo URL	http://www.company.com/logo.gif	(e.g., http://www.acme.com/logo.gif)

Figure 2.12 Change the name and logo on standard meeting home page

In the left frame of the System Management page, under Customization click the Entry Page link. This feature allows the Administrator to use a different home page as the standard meeting home page.



Use My Page as the System Home Page

Alert! Before you start to use your own home page, carefully prepare the following:

- Note the URL below for accessing the system management pages. Keep it for reference.

  http://192.168.1.122/as/wapi/login

- Note the Host and Join Meeting URLs and the download URL on the default system home page. You may need those URLs on your own system home page.
- To change back to the default system home page, just leave your system home page URL empty.

Further instructions on how to customize this system can be found in the support section of the RHUB website: http://www.rhubcom.com.

My system home page URL:

(e.g., http://www.acme.com/meeting.html)

Figure 2.13 Use a new page for the meeting home page

The system home page specified in Figure 2.13 should contain ways for users to host and join meetings. There are two ways for users to host and join meetings:

1. click URLs (or buttons associated with the URLs) on your page
2. submit forms on your page

Using URLs is the easiest way for customization. Using forms gives you a better control of customization. In the following examples, substitute for `yourMeetingServerAddress` the host name (e.g. webmeeting.company.com) for your R-HUB server.

Here is the URL that is used to host a meeting:

```
http://yourMeetingServerAddress/as/wapi/goto_downloader?role=host
```

Here is the URL that is used to join a meeting:

```
http://yourMeetingServerAddress/as/wapi/goto_downloader?role=attendee
```

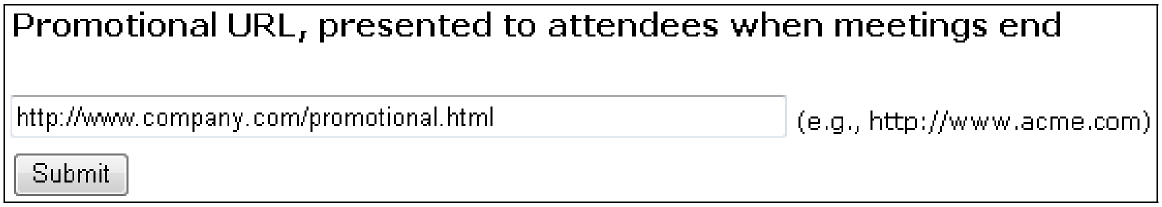
Here is the HTML code used to allow users to host a meeting:

```
<form action=”http://yourMeetingServerAddress/as/wapi/goto_downloader”
      method="post">
   <input type="hidden" name="role" value="host">
   Email Address:
      <input type="text" name="email" value="">
   Password:
      <input type="password" name="user_password" value="">
   <input type="submit" name="submit" value="Host Meeting">
</form>
```

Here is the HTML code used to allow users to join a meeting:

```
<form action="http://yourMeetingServerAddress/as/wapi/goto_downloader"
      method="post">
   <input type="hidden" name="role" value="attendee">
   Meeting ID:
      <input type="text" name="meeting_id" value="">
   Meeting Password:
      <input type="password" name="password" value="">
   Your Name:
      <input type="text" name="name" value="">
   <input type="submit" name="submit" value="Join Meeting">
</form>
```

In the left frame of the System Management page, under Customization click the Promotion Page link. This allows the Administrator to change the web page that meeting attendees see when a meeting ends. The web page can be used to solicit feedback, sell products or services, or display your organization's home page.

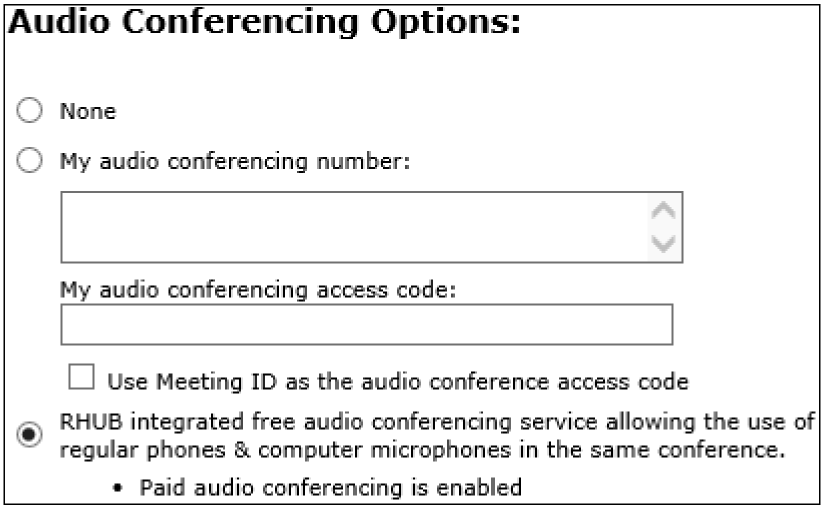


Promotional URL, presented to attendees when meetings end

http://www.company.com/promotional.html (e.g., http://www.acme.com)

Figure 2.14 Change default promotion page

In the left frame of the System Management page, under Customization click the Audio Conference link. This allows the Administrator to use their company's own audio conferencing phone number. It also tells you if you have signed up for R-HUB's paid audio conferencing.



Audio Conferencing Options:

○ None

○ My audio conferencing number:

My audio conferencing access code:

□ Use Meeting ID as the audio conference access code

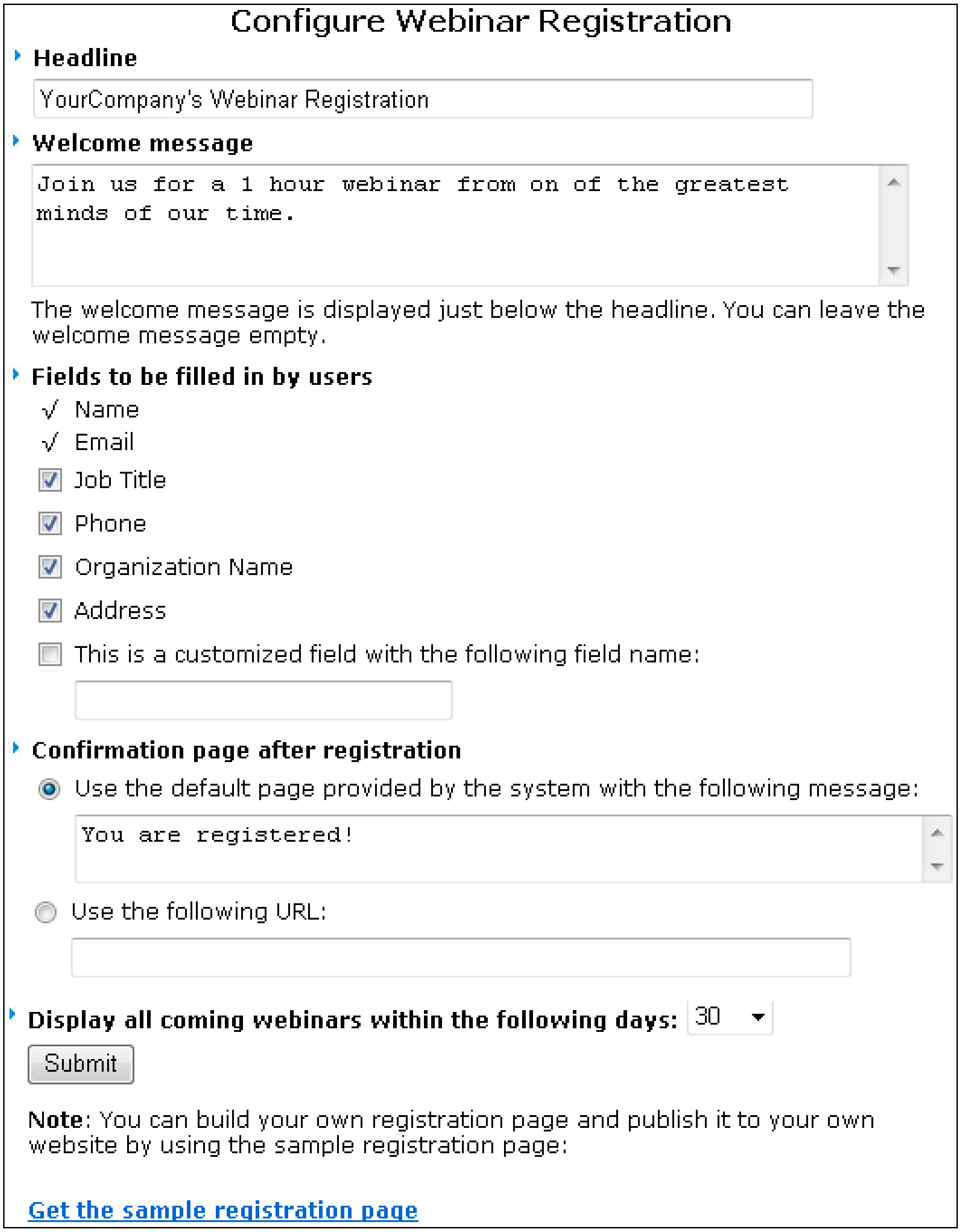
● RHUB integrated free audio conferencing service allowing the use of regular phones & computer microphones in the same conference.

- Paid audio conferencing is enabled

Figure 2.15 Change audio conference phone number

2.7. Webinar Registration

In the left frame of the System Management page, under Webinar Registration click the Configuration link. This feature allows the Administrator to setup a registration page for all of your webinars. Figure 2.16 shows the fields that can be customized for this registration page:



Configure Webinar Registration

Headline

YourCompany's Webinar Registration

Welcome message

Join us for a 1 hour webinar from on of the greatest minds of our time.

The welcome message is displayed just below the headline. You can leave the welcome message empty.

Fields to be filled in by users

- √ Name
- √ Email
- ☑ Job Title
- ☑ Phone
- ☑ Organization Name
- ☑ Address
- □ This is a customized field with the following field name:

Confirmation page after registration

● Use the default page provided by the system with the following message:

You are registered!

○ Use the following URL:

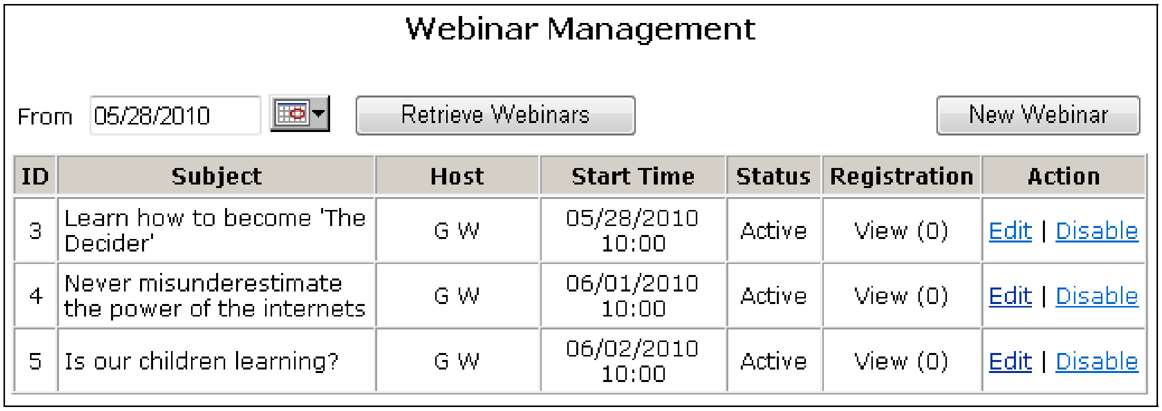
Display all coming webinars within the following days: 30

Note: You can build your own registration page and publish it to your own website by using the sample registration page:

Get the sample registration page

Figure 2.16 Registration page for all webinars

In the left frame of the System Management page, under Webinar Registration click the Management link. This feature allows the Administrator to list, create, edit and disable upcoming webinars.   As shown in Figure 2.17:

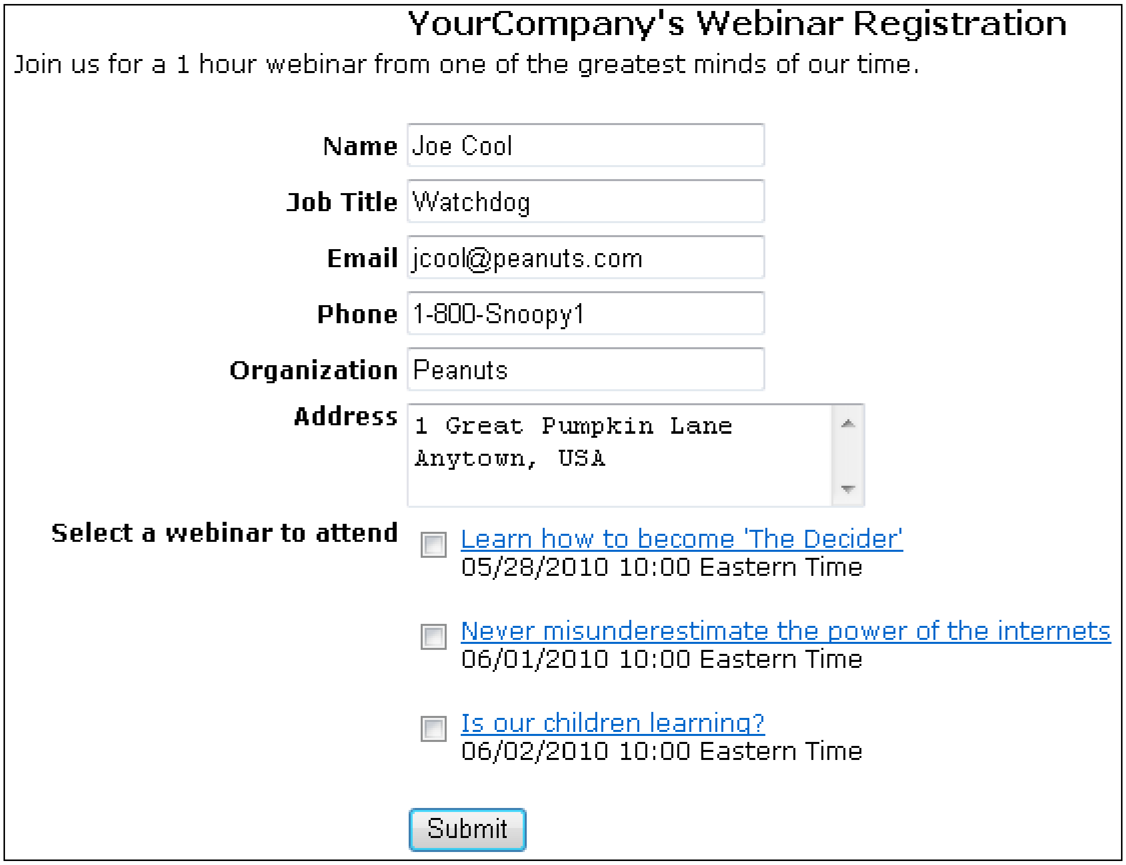


Webinar Management

ID	Subject	Host	Start Time	Status	Registration	Action
3	Learn how to become 'The Decider'	G W	05/28/2010 10:00	Active	View (0)	Edit | Disable
4	Never misunderestimate the power of the internets	G W	06/01/2010 10:00	Active	View (0)	Edit | Disable
5	Is our children learning?	G W	06/02/2010 10:00	Active	View (0)	Edit | Disable

Figure 2.17 List, Create, Edit and Disable Webinars

The resulting registration page for webinar attendees will look what is shown in Figure 2.18:



YourCompany's Webinar Registration

Join us for a 1 hour webinar from one of the greatest minds of our time.

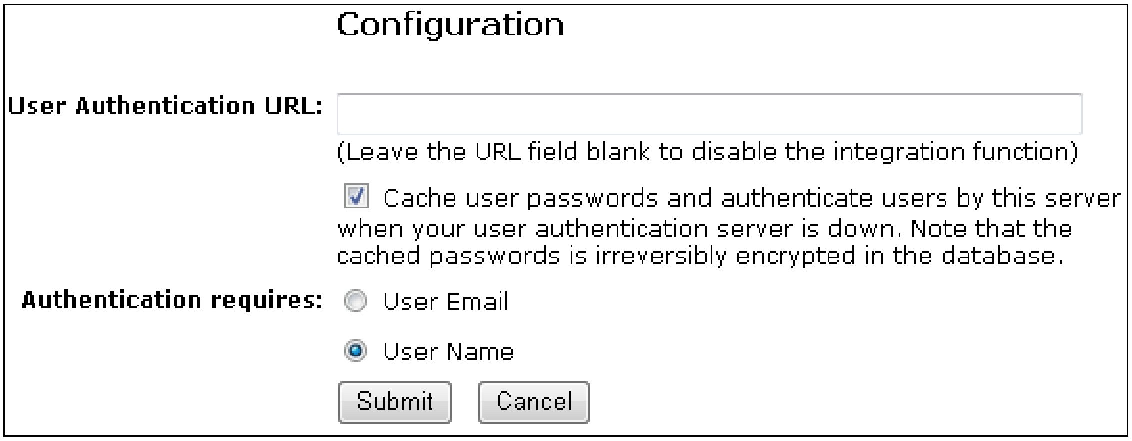
Name	Joe Cool
Job Title	Watchdog
Email	jcool@peanuts.com
Phone	1-800-Snoopy1
Organization	Peanuts
Address	1 Great Pumpkin Lane Anytown, USA
Select a webinar to attend	□ Learn how to become 'The Decider' 05/28/2010 10:00 Eastern Time
	□ Never misunderestimate the power of the internets 06/01/2010 10:00 Eastern Time
	□ Is our children learning? 06/02/2010 10:00 Eastern Time

=

Figure 2.18 Webinar Registration page for Attendees

2.8. Integration with Application Server

In the left frame of the System Management page, under Integration click the Application Server link. This feature allows the Administrator to use their own authentication server, such as a CRM system, for user authentication.



Configuration

User Authentication URL:

(Leave the URL field blank to disable the integration function)

☑ Cache user passwords and authenticate users by this server when your user authentication server is down. Note that the cached passwords is irreversibly encrypted in the database.

Authentication requires: ○ User Email

● User Name

Figure 2.19 Integration with your server for user authentication

For more details on how to integrate with an authentication server:

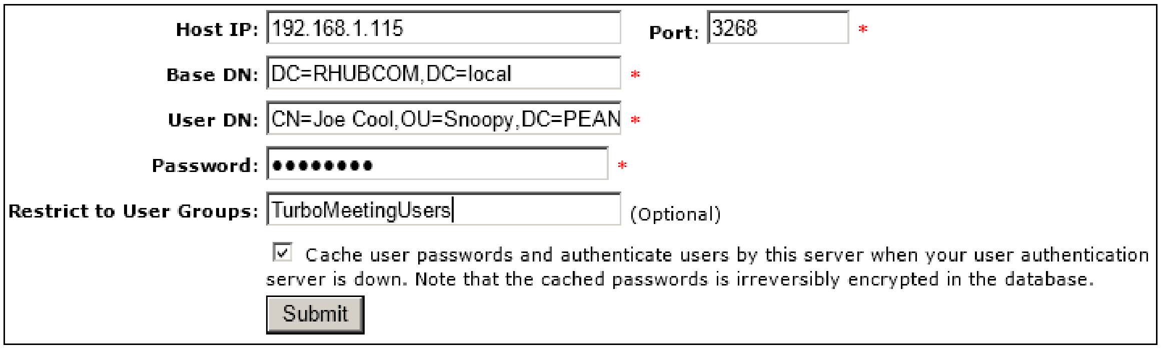
1. Go to http://www.rhubcom.com
2. Click the “Support” link
3. Click the Integration link

If “User Name” is chosen for “Authentication requires” on this page, it also applies to users created manually in the R-HUB server.

2.9. Integration with LDAP for User Authentication

LDAP Integration works on all servers. The LDAP feature is enabled for free on the TM-600, TM-800, TM-1000, and TS-700 servers. Login to your R-HUB server and enter the management page shown in Figure 2.2. Under Integration click the LDAP link and you will be shown the settings in Figure 2.20. To integrate with the LDAP server, specify:

- the LDAP server’s IP address as the Host IP address
- the LDAP Port for TCP communication (not the SSL port). We recommend port 3268.
- any user’s distinguished name as the User DN
- the Password for the user specified in the User DN field



Host IP: 192.168.1.115 Port: 3268 *

Base DN: DC=RHUBCOM,DC=local *

User DN: CN=Joe Cool,OU=Snoopy,DC=PEAN *

Password: •••••••• *

Restrict to User Groups: TurboMeetingUsers (Optional)

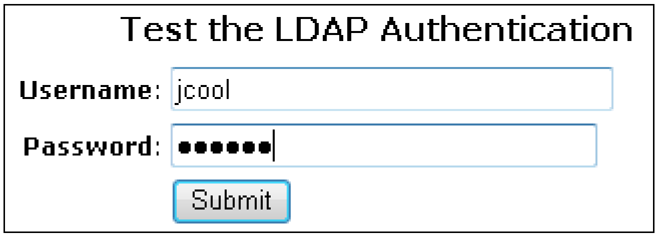
☑ Cache user passwords and authenticate users by this server when your user authentication server is down. Note that the cached passwords is irreversibly encrypted in the database.

Figure 2.20 Enable LDAP integration

Only LDAP Version 3 is supported. No SSL encryption can be used for User DN and Password authentication. Simple Bind authentication is used to connect to your LDAP server. If a user with valid credentials fails to pass authentication by your LDAP server, check the following:

- Your LDAP configuration meets with the work conditions of this system.
- Your LDAP entries have the "distinguishedName" (DN) attribute filled with proper values. Empty values are not allowed. A Microsoft Active Directory server should automatically fill proper values for distinguishedName. To determine a distinguishedName for a user (i.e.: a User DN), use an LDAP browser like JXplorer, or on Windows ADSI Edit (adsiedit.msc)

You can test whether individual users can be found for the given LDAP settings as shown in Figure 2.21. Enter the login name and password for a specific user. The resulting page will say either "LDAP authentication succeeds" or show a detailed trace of where the LDAP authentication failed.



Test the LDAP Authentication

Username: jcool

Password: ●●●●●●

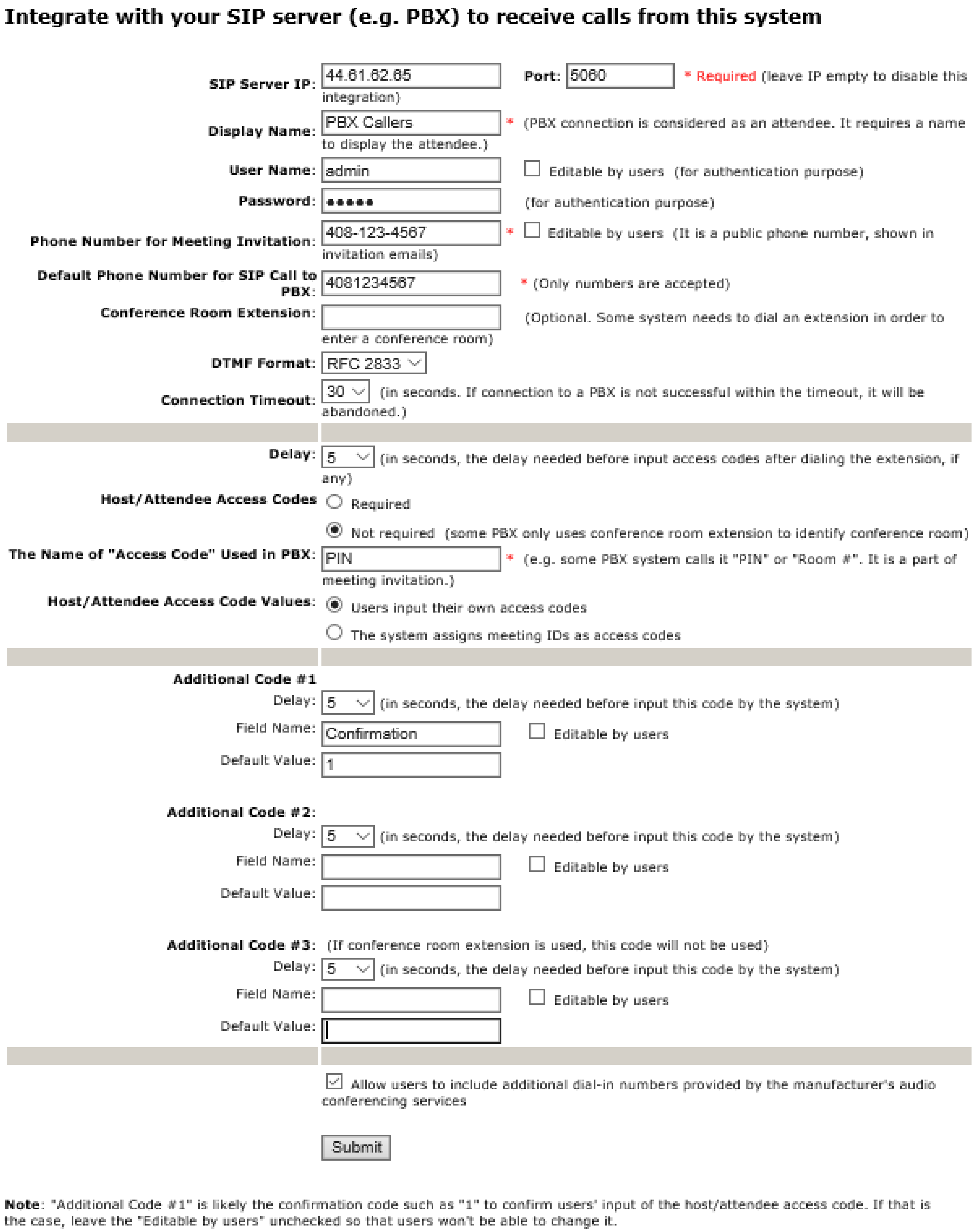
Figure 2.21 Test specific LDAP Users to insure correctness of LDAP settings

If you have an LDAP server with many thousands of users, or if only a small subset of your LDAP users are going to host meetings on the R-HUB server, you can achieve faster LDAP user lookups by specifying multiple Base DN's. Taken together, these multiple Base DN's will likely have fewer users than your entire LDAP tree.

2.10. Integration with a PBX System Option

The PBX integration is an option that must be purchased. When PBX integration is enabled on your R-HUB server, the meeting host connects to your PBX server and participants can call into your PBX and talk with R-HUB's audio conference callers and TurboMeeting VoIP talkers if the R-HUB administrator chooses to "Allow users to include additional dial-in numbers provided by the manufacturer's audio conferencing services".

When the PBX integration setup is complete, TurboMeeting will display a "Connect" button when a meeting is running. When the host clicks this Connect button, a connection with your PBX system (or SIP server) is initiated.



Integrate with your SIP server (e.g. PBX) to receive calls from this system

SIP Server IP: 44.61.62.65 **Port:** 5060 * Required (leave IP empty to disable this integration)

Display Name: PBX Callers * (PBX connection is considered as an attendee. It requires a name to display the attendee.)

User Name: admin ☐ Editable by users (for authentication purpose)

Password: ●●●●● (for authentication purpose)

Phone Number for Meeting Invitation: 408-123-4567 * ☐ Editable by users (It is a public phone number, shown in invitation emails)

Default Phone Number for SIP Call to PBX: 4081234567 * (Only numbers are accepted)

Conference Room Extension: (Optional. Some system needs to dial an extension in order to enter a conference room)

DTMF Format: RFC 2833

Connection Timeout: 30 (in seconds. If connection to a PBX is not successful within the timeout, it will be abandoned.)

Delay: 5 (in seconds, the delay needed before input access codes after dialing the extension, if any)

Host/Attendee Access Codes ○ Required

● Not required (some PBX only uses conference room extension to identify conference room)

The Name of "Access Code" Used in PBX: PIN * (e.g. some PBX system calls it "PIN" or "Room #". It is a part of meeting invitation.)

Host/Attendee Access Code Values: ● Users input their own access codes

○ The system assigns meeting IDs as access codes

Additional Code #1

Delay: 5 (in seconds, the delay needed before input this code by the system)

Field Name: Confirmation ☐ Editable by users

Default Value: 1

Additional Code #2:

Delay: 5 (in seconds, the delay needed before input this code by the system)

Field Name: ☐ Editable by users

Default Value:

Additional Code #3: (If conference room extension is used, this code will not be used)

Delay: 5 (in seconds, the delay needed before input this code by the system)

Field Name: ☐ Editable by users

Default Value:

☑ Allow users to include additional dial-in numbers provided by the manufacturer's audio conferencing services

Note: "Additional Code #1" is likely the confirmation code such as "1" to confirm users' input of the host/attendee access code. If that is the case, leave the "Editable by users" unchecked so that users won't be able to change it.

Figure 2.22 PBX integration settings

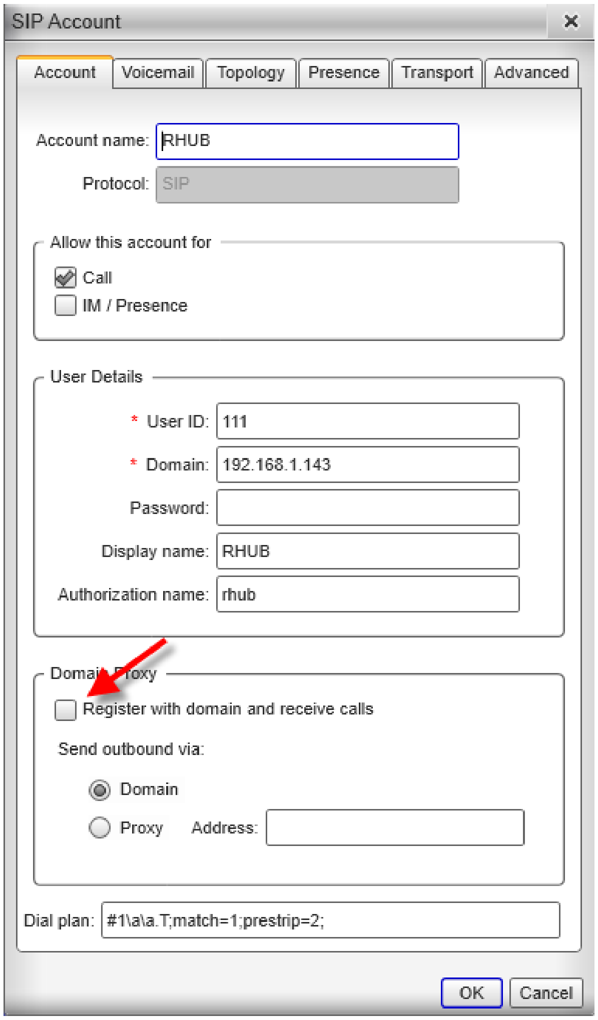
The **SIP Server IP** (or SIP Server domain name) and **Port** are what the R-HUB Audio Conferencing server needs to call into your SIP Server. The **Display Name** is the name that appears in the TurboMeeting application's list of Telephone callers. The **Phone Number for**

Meeting Invitation is your SIP Server's phone number that TurboMeeting lists in the email invitation and in the GUI. The **Default Phone Number for SIP Call to PBX** is the phone number that is required by the SIP protocol. This is any number that the PBX can accept. It is not necessarily a real telephone number, but it could be.

The other parameters are the special values that need to be entered to get into a meeting room. If a value is **Editable by users**, then there will be a corresponding profile field for each user in TurboMeeting's Tools | Preference's "Conference Call" settings.

These ports must be open for the R-HUB SBC (Session Border Controller) to call in to your PBX:
UDP 5060-5070
UDP: 20000-30000
You can limit access on these ports to IP address: 64.71.140.86 (the R-HUB SBC, which is the caller IP). You don't need another static IP address for your PBX. You can still use 80/443 for your web server if it uses the same IP address.

Please download the free X-Lite software and use it to call your SIP Server to come up with your settings. In X-Lite, it is important to uncheck "Register domain and receive call" as the R-HUB server will not register with the domain (see the X-Lite image below). After you verified that your settings work with X-Lite, the R-HUB server should work with the same settings.



Account name: RHUB
Protocol: SIP

Allow this account for
☑ Call
☐ IM / Presence

User Details
* User ID: 111
* Domain: 192.168.1.143
Password:
Display name: RHUB
Authorization name: rhub

Domain Proxy
☐ Register with domain and receive calls
Send outbound via:
● Domain
○ Proxy Address:

Dial plan: #1\a\a.T;match=1;prestrip=2;

Figure 2.23 Use X-Lite to debug PBX integration settings

3. Configuring the Firewall

There are three ways to deploy your R-HUB server:

1. Outside the Firewall
2. Inside the Firewall and Accessible by Users outside Firewall
3. Inside the Firewall and not Accessible by Users outside Firewall

Depending on the deployment, you may or may not need to configure your firewall.

3.1. Behind Firewall and Accessible by Users outside Firewall

This deployment (Figure 3.1) is most popular and it is typically done by connecting R-HUB server with the DMZ port of your router. You can also place the R-HUB server anywhere on your LAN.

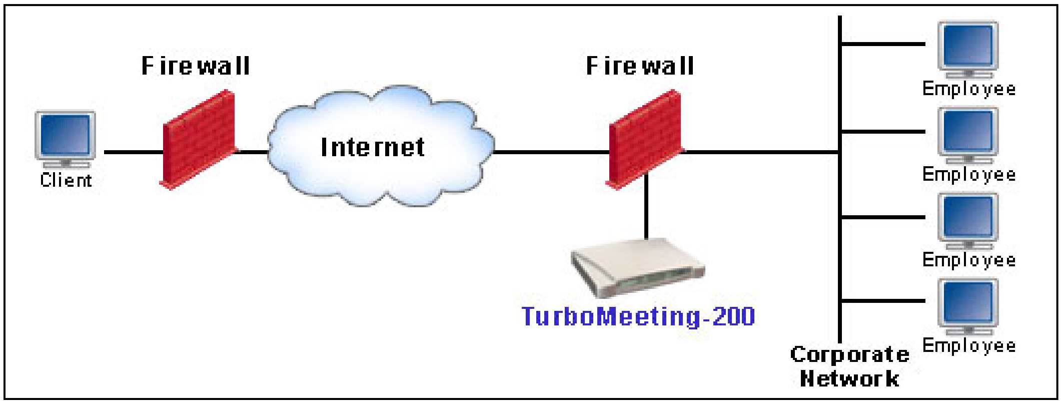
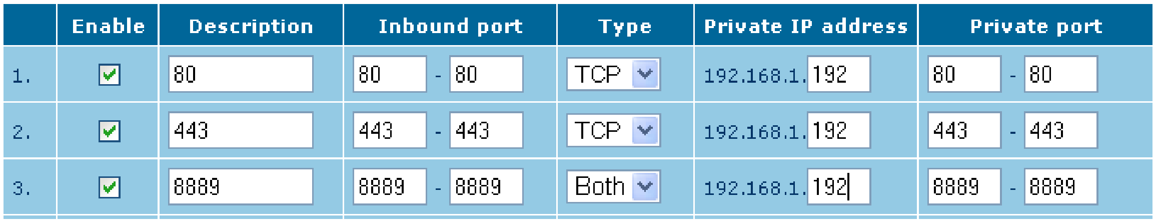


Figure 3.1 Inside Firewall and Accessible by Users outside Firewall

In order for external users to access your server, you need to open the inbound TCP ports: 80 and 443 and the TCP and UDP port 8889 on your firewall/router and forward the inbound TCP and UDP traffic on these ports to the corresponding ports of the local IP address of your R-HUB server.

If you are using a SOHO or home router, opening inbound ports and doing port forwarding are fairly easy. For example, in a LinkSys router, you usually look for the “Applications” link. In a Belkin router, you look for the “Virtual Servers” link. After clicking the link, you will see a page similar to Figure 3.2. Fill in the two TCP ports (80 and 443) and the TCP and UDP port (8889) and your R-HUB server local IP address. The firewall configuration is done.

In Figure 3.2, the “Private IP address” is the R-HUB server’s local IP address, which you define when you configure the meeting server IP settings; the “Inbound port” may be called “Source port”; the “Private port” may be called “Destination port”. You can input anything in the “Description” field. Don’t forget to check the “Enable” fields.



	Enable	Description	Inbound port	Type	Private IP address	Private port
1.	☑	80	80 - 80	TCP	192.168.1. 192	80 - 80
2.	☑	443	443 - 443	TCP	192.168.1. 192	443 - 443
3.	☑	8889	8889 - 8889	Both	192.168.1. 192	8889 - 8889

Figure 3.2 A sample of firewall configuration

This deployment gives you the maximum flexibility in terms of meeting access security control. With this deployment, you can host two types of meetings:

- Internal meetings that only users behind your firewall can join (including users in the Virtual Private Network, or VPN)
  Note: You can manually allow external users by specifying a list of IP addresses
- External meetings that anyone including attendees outside your firewall can join.

If you have difficulty in configuring port forwarding, please refer to the following URL for step-by-step guidance for your router:

http://portforward.com/english/routers/port_forwarding/routerindex.htm

On the page, find your router model or a model similar to yours. Click the link for your router. On the next page, click "Click here to skip this advertisement... ". Now it shows a long list of applications you can do port forwarding for. Just pick one application. Replace this application's port(s) with three different definitions for ports 80 and 443 using TCP and port 8889 using TCP and UDP.

3.2. Outside the Firewall

With this deployment (Figure 3.3), your R-HUB server is completely outside your corporate firewall. There is no firewall configuration needed.

To configure the server settings (Figure 2.3) for this deployment, you will need to obtain from your Internet service provider (ISP) the IP address, subnet mask, default gateway and DNS settings. Input the IP address in the "Public IP Address" field and other IPs in the "Permanent IP Settings".

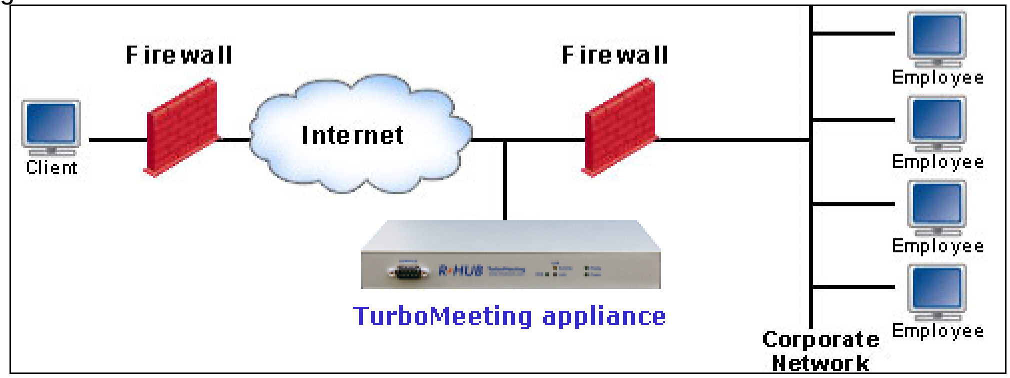


Figure 3.3 Deployment Outside the Firewall

3.3. Behind Firewall and Not Accessible by Users outside Firewall

This deployment (Figure 3.4) disallows users from connecting to the meeting server from the Internet outside your firewall and provides the maximum meeting access security. It will not allow any users outside your firewall (VPN) to join any meetings hosted on the server.

On the Server IP Settings configuration page (see Section 2.1), choose the option “No public IP address. This server is used only by internal users.” Then assign a static local IP, subnet mask, default gateway, and DNS servers for the meeting server (Figure 2.3).

You do not need to do any configuration on your firewall.

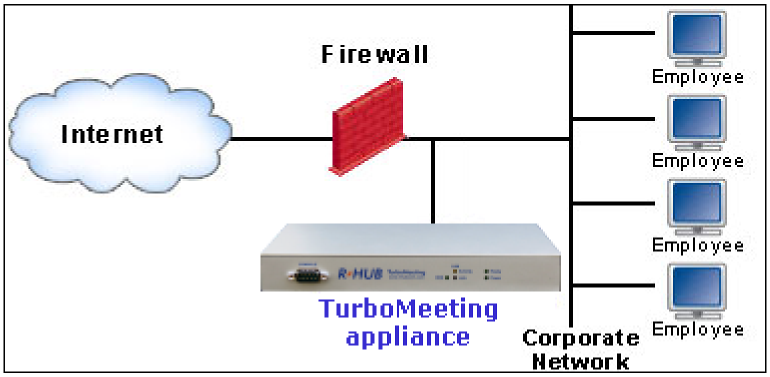
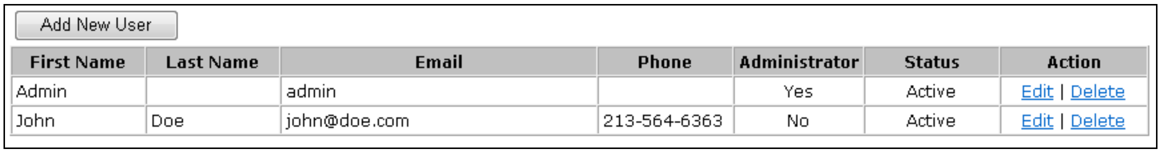


Figure 3.4 Inside Firewall and Not Accessible by Users outside Firewall

4. Manage Users

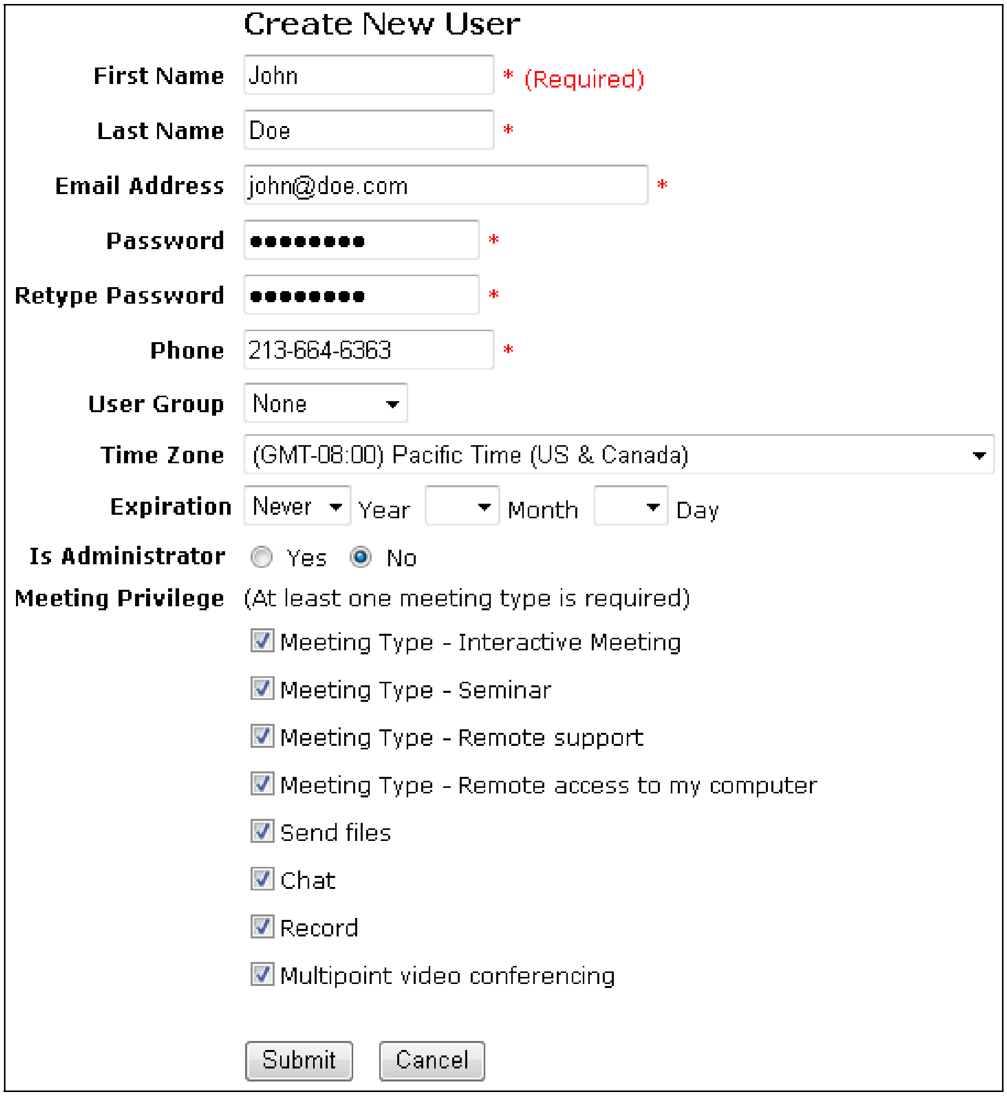
Login to the home page for your R-HUB server and enter the management page shown in Figure 2.2. Under the User Management category, click the **Users** link. A list of users will display as shown below.



First Name	Last Name	Email	Phone	Administrator	Status	Action
Admin		admin		Yes	Active	Edit | Delete
John	Doe	john@doe.com	213-564-6363	No	Active	Edit | Delete

Figure 4.1 List of Users

You can click the **Add New User** button to add a new user. Under the "Action" column, click the **Edit** link to edit a user profile or **Delete** link to delete a user profile from the system. Figure 4.2 below shows the page to create a user. You can define the meeting functions for each user.



Create New User

First Name	John * (Required)
Last Name	Doe *
Email Address	john@doe.com *
Password	●●●●●●●●● *
Retype Password	●●●●●●●●● *
Phone	213-664-6363 *
User Group	None
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
Expiration	Never Year Month Day
Is Administrator	○ Yes ● No
Meeting Privilege	(At least one meeting type is required)

☑ Meeting Type - Interactive Meeting

☑ Meeting Type - Seminar

☑ Meeting Type - Remote support

☑ Meeting Type - Remote access to my computer

☑ Send files

☑ Chat

☑ Record

☑ Multipoint video conferencing

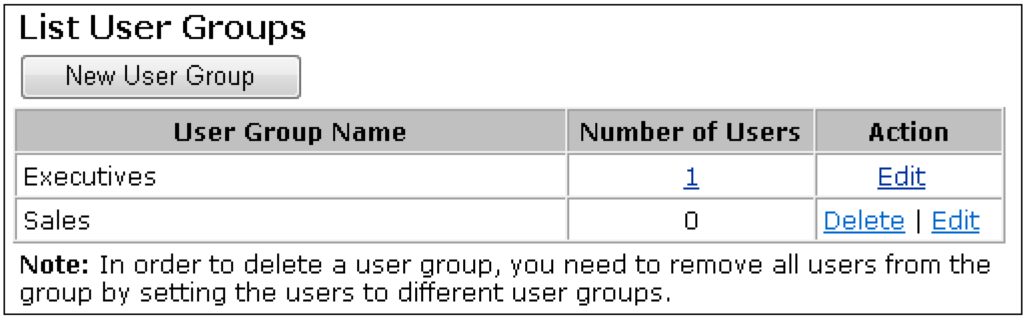
Figure 4.2 Create a user profile

4.1. User Groups

User groups can be created to define the same set of meeting privileges, audio conference setting and promotional URLs for a group of users. Once a user group is created, users can be assigned to this user group. This makes it easier to assign similar meeting privileges to similar users.

User Groups definitions can also apply to user groups defined in LDAP. When creating a User Group using the following steps, insure that the user group name exactly matches the LDAP user group name.

To access user groups, login to the home page for your R-HUB server and enter the management page shown in Figure 2.2. Under the User Management category, click the **User Group** link. A list of user groups will display as shown below.



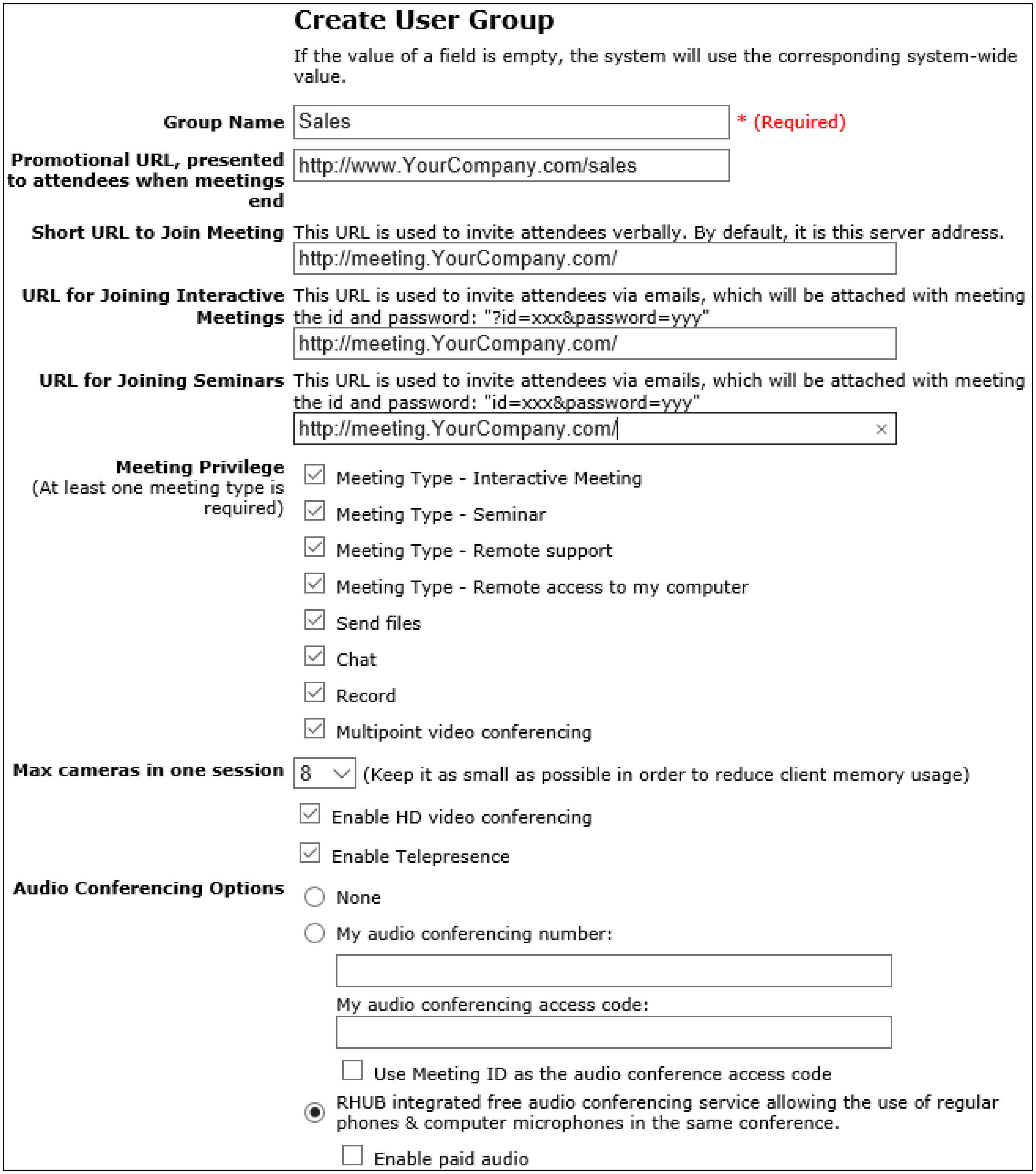
List User Groups

User Group Name	Number of Users	Action
Executives	1	Edit
Sales	0	Delete | Edit

Note: In order to delete a user group, you need to remove all users from the group by setting the users to different user groups.

Figure 4.3 List of User Groups

You can click the **New User Group** button to add a new user group. Under the “Action” column, click the **Edit** link to edit a user group or **Delete** link to delete a user group from the system. To delete a user group, you must first remove all the users from that group. Figure 4.3 below shows the page to create a user. You can define the meeting functions for each user group.



Create User Group

If the value of a field is empty, the system will use the corresponding system-wide value.

Group Name	Sales * (Required)
Promotional URL, presented to attendees when meetings end	http://www.YourCompany.com/sales
Short URL to Join Meeting	This URL is used to invite attendees verbally. By default, it is this server address. http://meeting.YourCompany.com/
URL for Joining Interactive Meetings	This URL is used to invite attendees via emails, which will be attached with meeting the id and password: "?id=xxx&password=yyy" http://meeting.YourCompany.com/
URL for Joining Seminars	This URL is used to invite attendees via emails, which will be attached with meeting the id and password: "id=xxx&password=yyy" http://meeting.YourCompany.com/
Meeting Privilege (At least one meeting type is required)	☑ Meeting Type - Interactive Meeting ☑ Meeting Type - Seminar ☑ Meeting Type - Remote support ☑ Meeting Type - Remote access to my computer ☑ Send files ☑ Chat ☑ Record ☑ Multipoint video conferencing
Max cameras in one session	8 (Keep it as small as possible in order to reduce client memory usage) ☑ Enable HD video conferencing ☑ Enable Telepresence
Audio Conferencing Options	○ None ○ My audio conferencing number: My audio conferencing access code: □ Use Meeting ID as the audio conference access code ● RHUB integrated free audio conferencing service allowing the use of regular phones & computer microphones in the same conference. □ Enable paid audio

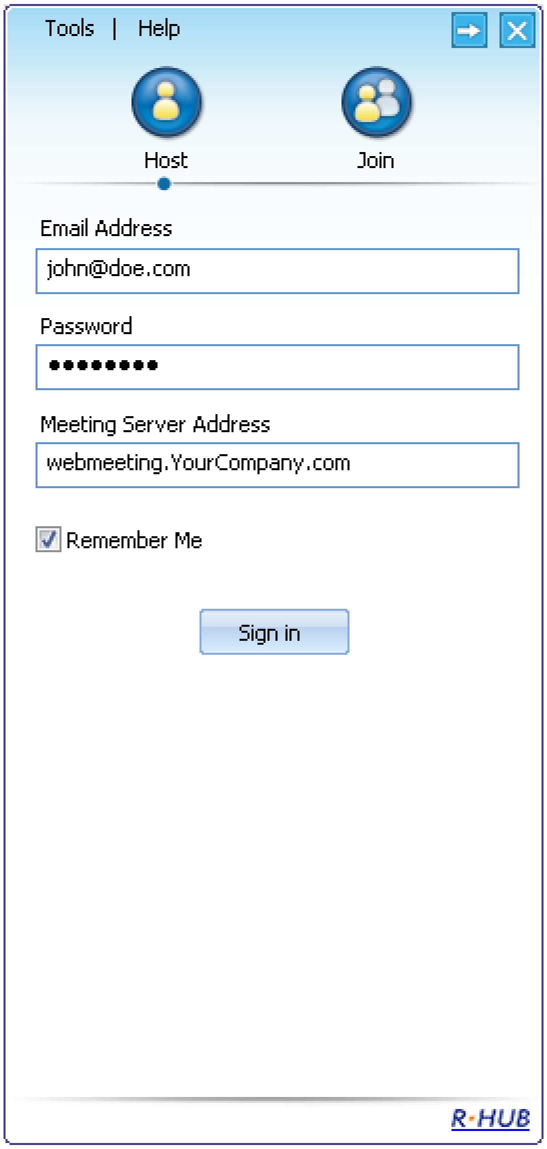
Figure 4.4 Create a user group

5. Start Meetings

After you complete the above configuration, you can start to host and invite people to join your meetings. Open your browser and type the IP address of the R-HUB server into your browser. You should see the home page shown in Figure 1.1.

Click the “Host” button to host a meeting. The next page will ask you to accept a Java Applet. Accept it. TurboMeeting starts to run (Figure 5.1).

The Meeting Server Address in Figure 5.1 is your meeting server IP address. Type your email and password to start a meeting. The meeting control panel switches to the entry meeting control panel shown in Figure 5.2.



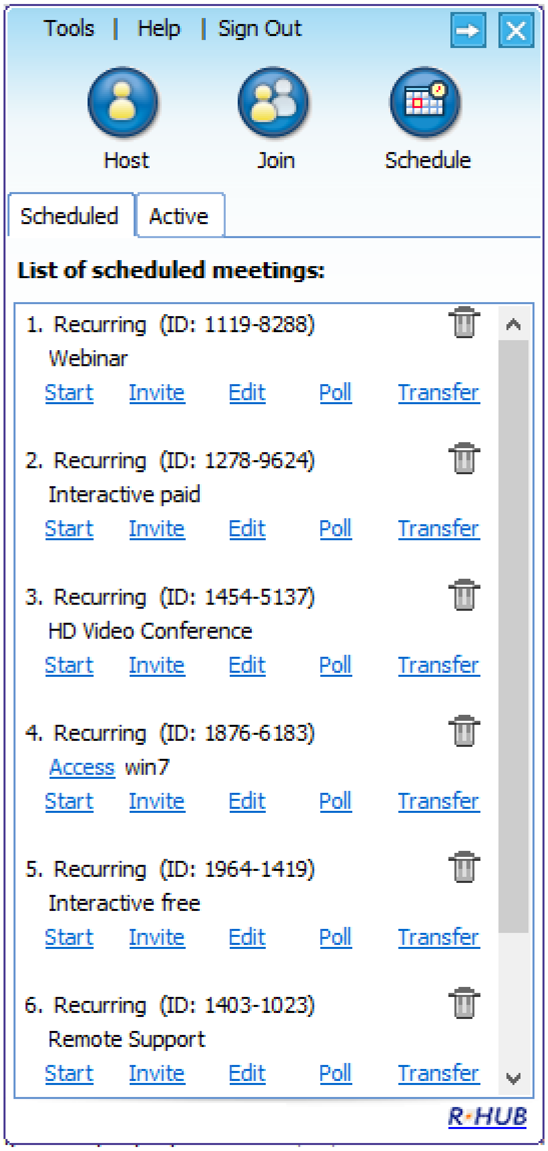
Email Address
john@doe.com

Password
●●●●●●●●●

Meeting Server Address
webmeeting.YourCompany.com

☑ Remember Me

Figure 5.1 Login to Start a Meeting



List of scheduled meetings:

1. Recurring (ID: 1119-8288)
Webinar
Start Invite Edit Poll Transfer

2. Recurring (ID: 1278-9624)
Interactive paid
Start Invite Edit Poll Transfer

3. Recurring (ID: 1454-5137)
HD Video Conference
Start Invite Edit Poll Transfer

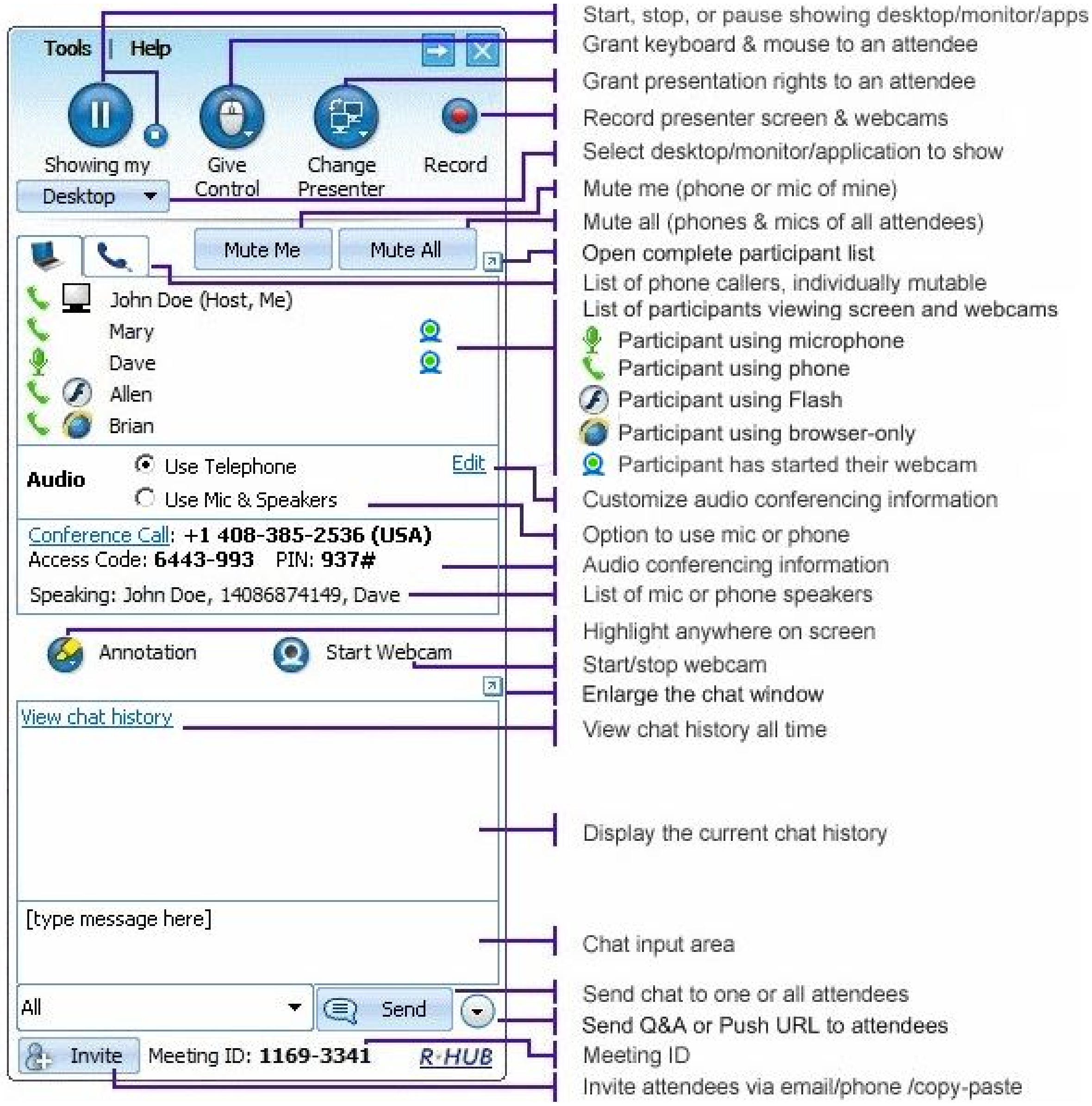
4. Recurring (ID: 1876-6183)
Access win7
Start Invite Edit Poll Transfer

5. Recurring (ID: 1964-1419)
Interactive free
Start Invite Edit Poll Transfer

6. Recurring (ID: 1403-1023)
Remote Support
Start Invite Edit Poll Transfer

Figure 5.2 Enter Meeting Control Panel

Click on the “Host” button as shown in Figure 5.2 and then select a meeting type. Your meeting starts (Figure 5.3).



Conference Call: +1 408-385-2536 (USA)
Access Code: 6443-993 PIN: 937#
Speaking: John Doe, 14086874149, Dave

Meeting ID: 1169-3341

Start, stop, or pause showing desktop/monitor/apps
Grant keyboard & mouse to an attendee
Grant presentation rights to an attendee
Record presenter screen & webcams
Select desktop/monitor/application to show
Mute me (phone or mic of mine)
Mute all (phones & mics of all attendees)
Open complete participant list
List of phone callers, individually mutable
List of participants viewing screen and webcams
Participant using microphone
Participant using phone
Participant using Flash
Participant using browser-only
Participant has started their webcam
Customize audio conferencing information
Option to use mic or phone
Audio conferencing information
List of mic or phone speakers
Highlight anywhere on screen
Start/stop webcam
Enlarge the chat window
View chat history all time
Display the current chat history
Chat input area
Send chat to one or all attendees
Send Q&A or Push URL to attendees
Meeting ID
Invite attendees via email/phone /copy-paste

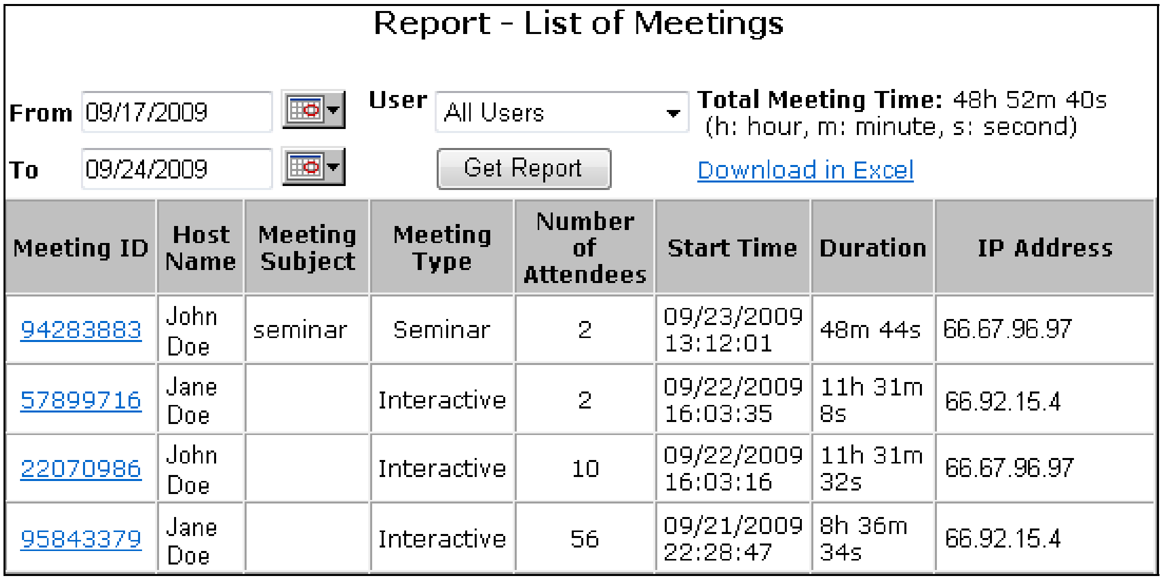
Figure 5.3 Main Meeting Control Panel

After the meeting starts, invite people to join your meeting by telling them the Meeting Server Address and the meeting ID shown on your meeting control panel. You can also click the “Invite” attendees button for more invitation details.

6. Reporting

In the left frame of the System Management page, click the Report link to use the Reporting feature. The reporting feature allows the Administrator to view details on all meetings that have taken place using a R-HUB server. The report can be run for any specified dates and optionally for any set of users. The report data can also be downloaded into an Excel file.

Each user can get a report of their own meetings by logging into the Windows or Mac TurboMeeting application and going to the menu item Tools | Report.



Report - List of Meetings

From 09/17/2009 **User** All Users **Total Meeting Time:** 48h 52m 40s (h: hour, m: minute, s: second)

To 09/24/2009

Meeting ID	Host Name	Meeting Subject	Meeting Type	Number of Attendees	Start Time	Duration	IP Address
94283883	John Doe	seminar	Seminar	2	09/23/2009 13:12:01	48m 44s	66.67.96.97
57899716	Jane Doe		Interactive	2	09/22/2009 16:03:35	11h 31m 8s	66.92.15.4
22070986	John Doe		Interactive	10	09/22/2009 16:03:16	11h 31m 32s	66.67.96.97
95843379	Jane Doe		Interactive	56	09/21/2009 22:28:47	8h 36m 34s	66.92.15.4

Figure 6.1 Report of meeting activity

7. Reset Server

The following are two cases when you have to reset your server:

1. You forgot the administrator password
2. You move the server to a different network and you cannot access the server because you did not change the server IP settings for the new network while you could access the server in the previous network.

The R-HUB server does three things during the reset:

1. It resets the system administrator account to the default one: "admin" as the email and "password" as the password. If you have multiple administrators, it only resets the first admin account that it finds.
2. It changes the IP settings to use DHCP.
3. It removes your own system home page URL so that you can easily access the server by a new IP address.

The reset does not affect any other data including user profiles, meeting logs, scheduled meetings, SSL certificate, audio integration setting, etc.

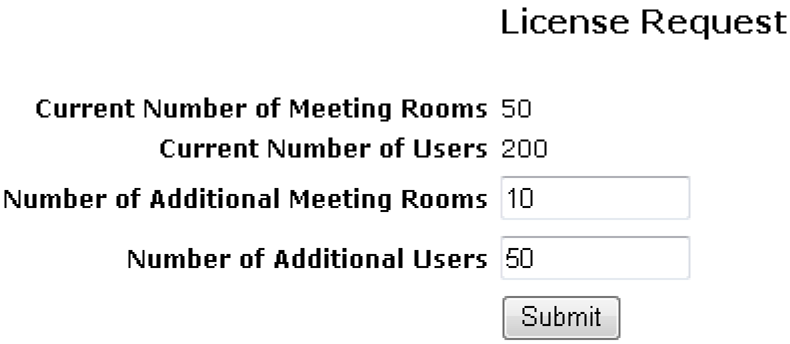
To reset the R-HUB TM-200, TM-210, TM-260, TM-270, TM-510, TM-560, TS-300, or TW-100 servers, you just push a pin into the reset button on the back and hold it for over 10 seconds until the “Ready” light turns off. After about 60 seconds when the “Ready” light turns on, you can access the server.

To reset the R-HUB TM-600, TM-800, TM-1000, or TS-700 servers, you need to connect it with your monitor, keyboard and mouse. The server runs in a Fedora Linux system. The default operating system login name is "turbomeeting" and the password is "password". After logging in, right click on the desktop and open a Terminal session. Type "./ResetTM", which resets the server. Then open a browser and type "http://localhost/as/wapi/login" to access the TurboMeeting administration pages. Use the system default account: "admin" as the email and "password" as the password.

Refer to the Section 1.1 about how to access your server after the reset.

8. License Upgrades: Additional Meeting Rooms and Users

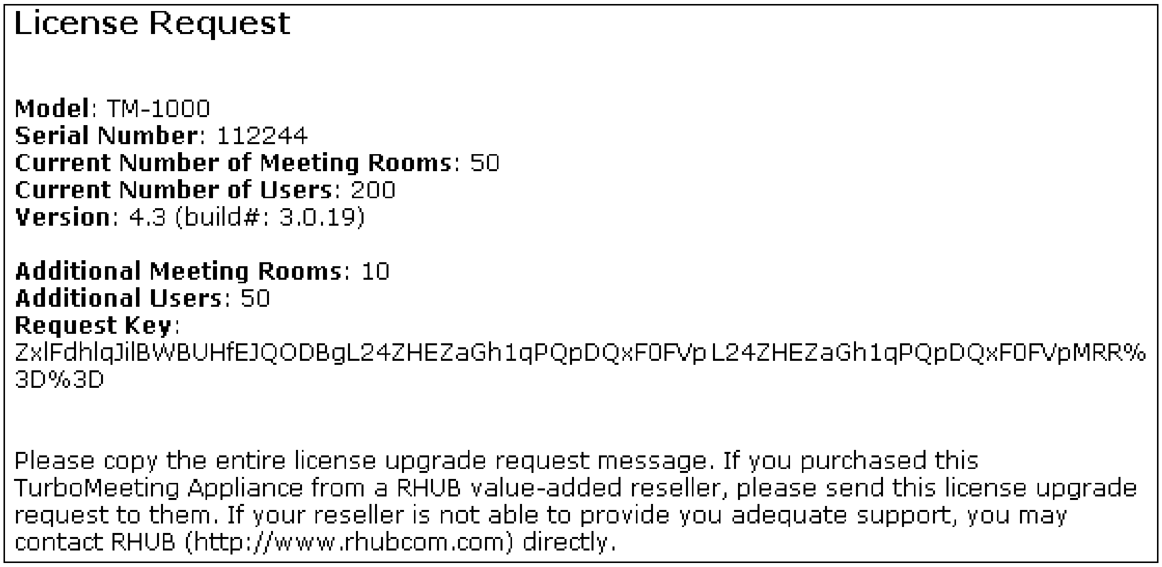
To add meeting rooms or additional user licenses to your server, login as an administrator to your TurboMeeting System Management web page and click the Request link. Then fill in the number of additional meeting rooms and users and click Submit:



License Request

Current Number of Meeting Rooms	50
Current Number of Users	200
Number of Additional Meeting Rooms	10
Number of Additional Users	50

Copy and paste the resulting page, below, into an e-mail and send it sales@rhubcom.com :



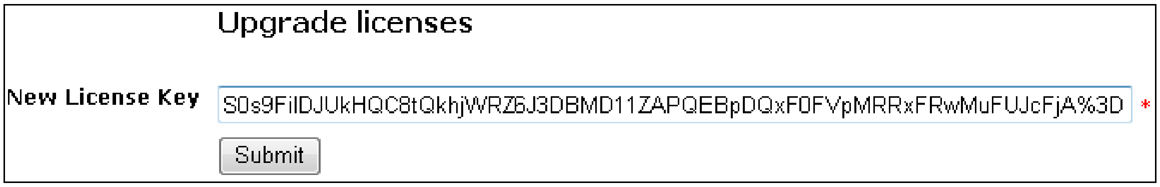
License Request

Model: TM-1000
Serial Number: 112244
Current Number of Meeting Rooms: 50
Current Number of Users: 200
Version: 4.3 (build#: 3.0.19)

Additional Meeting Rooms: 10
Additional Users: 50
Request Key:
ZxlFdhlqJilBWBUHfEJQODBgL24ZHEZaGh1qPQpDQxF0FVpL24ZHEZaGh1qPQpDQxF0FVpMRR%3D%3D

Please copy the entire license upgrade request message. If you purchased this TurboMeeting Appliance from a RHUB value-added reseller, please send this license upgrade request to them. If your reseller is not able to provide you adequate support, you may contact RHUB (http://www.rhubcom.com) directly.

You will be sent an e-mail with a license request key. Login as an administrator to your TurboMeeting System Management web page and click the Upgrade link. Copy and paste the Request Key into the New License Key field and click Submit. Your license will be upgraded.



Upgrade licenses

New License Key S0s9FilDJUkHQC8tQkhjWRZ6J3DBMD11ZAPQEBpDQxF0FVpMRRxFRwMuFUJcFjA%3D *

9. R-HUB High Availability Configuration and Operation

The R-HUB High Availability (HA) function requires two servers: a master server and a slave server. As soon as HA starts, the master server provides service to the TurboMeeting users and the slave server stands by until the master server goes offline. The master and slave server roles change automatically based on availability of a server. When the initial master server becomes offline for up to 20 seconds, the current slave server will become the master server and stay as the master server until it becomes offline.

Each server has an Ethernet port. Simply connect the port to your LAN. The following figure shows how it is deployed. It is not required that the two servers be on the same network although it is recommended.

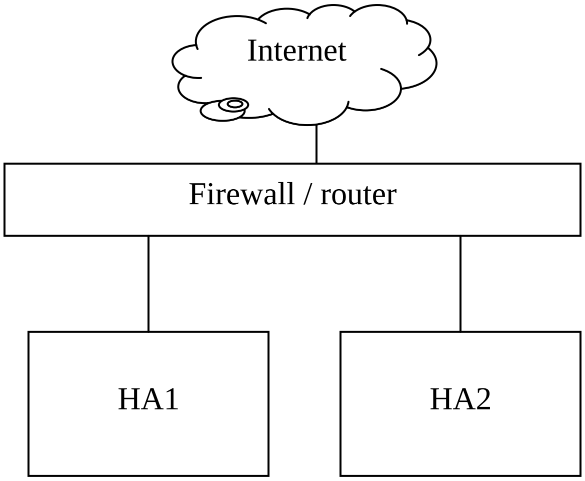


Figure 9.1 Master and Slave HA server setup

Here are the steps to deploy your HA cluster.

9.1. Backup your Database

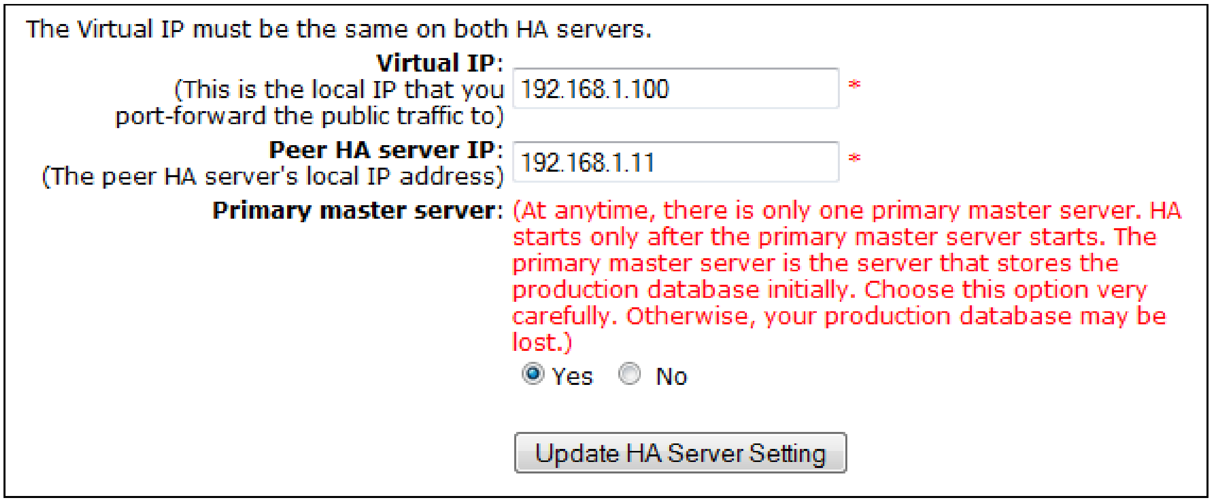
This is very important! Because the slave server’s database will be replaced with the master server’s database every minute, you should back up your database before you setup and start the HA servers. Also, it is recommended that you backup both the master server and slave server databases every day.

Since the HA servers may be automatically assigned with different public IP addresses over time, use the servers’ local IP addresses for backup. The HA servers’ local IP addresses never change unless you change them.

Please go to the following FAQ for backup instructions:
http://www.rhubcom.com/v4/web_conferencing/support.html#backup

9.2. Set up your HA Servers

The following are sample settings. Make both HA servers have the same virtual IP and configure your firewall to port forward the ports: 80 (TCP), 443 (TCP), 8889 (TCP & UDP) to this virtual IP address.



The Virtual IP must be the same on both HA servers.

Virtual IP: (This is the local IP that you port-forward the public traffic to) 192.168.1.100 *

Peer HA server IP: (The peer HA server's local IP address) 192.168.1.11 *

Primary master server: (At anytime, there is only one primary master server. HA starts only after the primary master server starts. The primary master server is the server that stores the production database initially. Choose this option very carefully. Otherwise, your production database may be lost.)

● Yes ○ No

Figure 9.2 HA server settings

9.3. Start or Stop HA Servers

You can start or stop an HA server is just a click of a button.

After an HA server starts, it will remain “Started” until you stop the server by clicking the “Stop HA Server” button. The HA started/stopped status is not affected by if the server is powered on or off.

The “Primary Master Server” is the HA server that holds the production database initially. **You must configure and make the primary master server work first.**

9.4. Check the HA Server Status

You can check the HA server status by clicking the “Refresh” button on the HA management page.

The HA running status is independent of the TurboMeeting server’s running status. That is, a running HA status does not mean that the TurboMeeting server application is running or is running without issues. A stopped HA status does not mean that the TurboMeeting server application has stopped running.

HA itself is a server application. Its purpose is to keep the high availability of the servers at the hardware, operating system, power and networking levels. When the master server is not available due to any issues with hardware, power, operating system, or networking, HA promotes the slave server as the master server within seconds.

When HA runs, it constantly does two jobs:

1. Detect the health of the peer server
2. Backup the production database from the master server to the slave server when there are changes to the production database.

You can monitor the HA server status via the following URL:

http://*TurboMeetingServerIP*:8885/__HA_STATUS__

The above URL shows the master HA server status. To check each HA server status, use the server's local IP for the "*TurboMeetingServerIP*" in the above URL.

Below is a sample output:

```
<__Return__><__Status__>SUCCEED</__Status__>
<__Reason__>HA has started. It is the SLAVE.</__Reason__>
<__IsDefaultMaster__>Y</__IsDefaultMaster__> </__Return__>
```

"SUCCEED" is shown if HA started successfully. Otherwise, a failure status is shown along with a reason for the failure.

9.5. Test if HA Works Properly

After you deploy the HA servers, you should test whether HA works properly. You need to find a way to access your server outside your firewall in a browser. The following are two basic test cases.

Case 1. Power failure

Turn off the power on the master HA server. You should be able to access your TurboMeeting service after 30 - 50 seconds of disruption. After the TurboMeeting service recovers, turn on the power on the server that was turned off and turn off the power on the other server.

Case 2. Ethernet connection failure

Unplug the Ethernet cables from one HA server, then after the new Master takes over plug in the unplugged Ethernet cable and unplug the Ethernet cable from the other server. You should be able to access your TurboMeeting service after about 30 seconds of disruption. Note that when you plug back in the cables, you will see that the server reboots. This is by design.

9.6. Your SSL Certificate Must Be Copied to Slave Server by R-HUB

If you upload your own SSL certificate to your R-HUB HA cluster, please contact R-HUB support to have them copy the SSL certificate from the primary server to the slave server. There is no way other way to install the SSL certificate on the slave server.

9.7. Suggested HA Update Procedure

The following procedure should be the steps you use to update the firmware on your HA servers. You should disable auto-updates on these servers and do manual updates using the following steps:

1. Disable HA on the current slave server, then disable HA on the current master server.
2. Update each server by clicking "Update System Now" in "System Settings".
3. After the update, enable HA on the current master server.
4. Wait 2 minutes, then enable HA on the current slave server.

When a major release becomes available, R-HUB will send email to the email ID in our warranty database, which is initially the email ID provided when you register the servers.

Support Contact

If you purchased the TurboMeeting Server from an R-HUB value-added reseller, please contact them for support. If your reseller is not able to provide you adequate support, your reseller will contact us or you can contact us directly.

R-HUB Communications, Inc.
4340 Stevens Creek Blvd.
Suite 282
San Jose, CA 95129
Tel: 408-899-2831 extension 2
Fax: 408-516-9612
support@rhubcom.com
http://www.rhubcom.com