M200/500 Administration Manual

Version 1.0

The Zultys web conferencing and remote support appliance

Zultys, Inc.
771 Vaqueros Ave
Sunnyvale, CA 94085
support@zultys.com
http://www.zultys.com

Contents

M200/500 Administrator Manual

1. Install

The M200/500 Web conferencing server package includes:

- M200/500 appliance
- Analog console cable
- Ethernet crossover-cable
- Power supplier

1.1 Access to M200/500

There are two ways to access M200/500: plug-and-play and using an Ethernet crossover-cable. Either way, an Internet browser needs to be used to access and configure the server.

I. Plug-and-Play

This method requires you have:

- A DHCP server on your network
- A computer with Microsoft Windows (98, 2000, XP or Vista)

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

1. Connect the server with an Ethernet cable (not the crossover-cable in the package) 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:

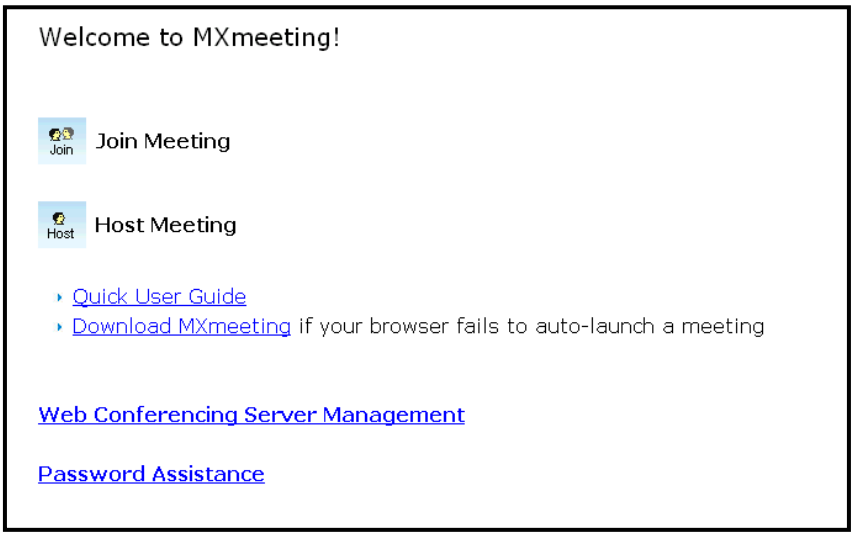


Figure 1.1. Home Page

If the page does not display and you are familiar with your router, check the IP address your router has assigned to the Zultys appliance, which is named "myonlinemeeting". Then input the IP address in your browser and you can access the Zultys appliance.

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

II. Crossover-cable

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 M200/500 (as described above)
- Wait for the ready light to turn green. This usually takes about 90 seconds
- Connect the M200/500 to your computer using the included crossover-cable or any Internet cable
- Open a browser on your computer and type http://192.168.1.192. The home page (Figure 1.1) should display.

Once you have accessed to 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 M200/500 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 appliance.

1.2 Configure the M200/500

After you access the meeting server home page (Figure 1.1), click "Manage User Accounts and the Meeting Server" link and you will see the login page shown in Figure 1.2. Type

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

To change the default administrator account, you use "Manage Users" (see Section 3) to change the default email and password to your choice.

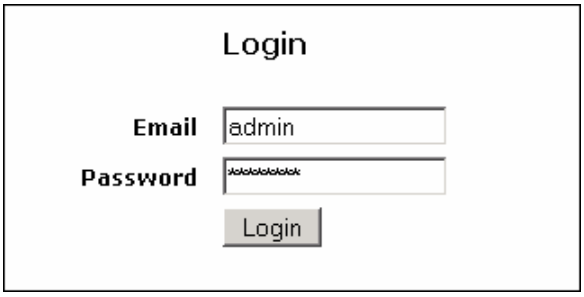


Figure 1.2 Login Page

After login, the **Server Management** home page is displayed (Figure 1.3):

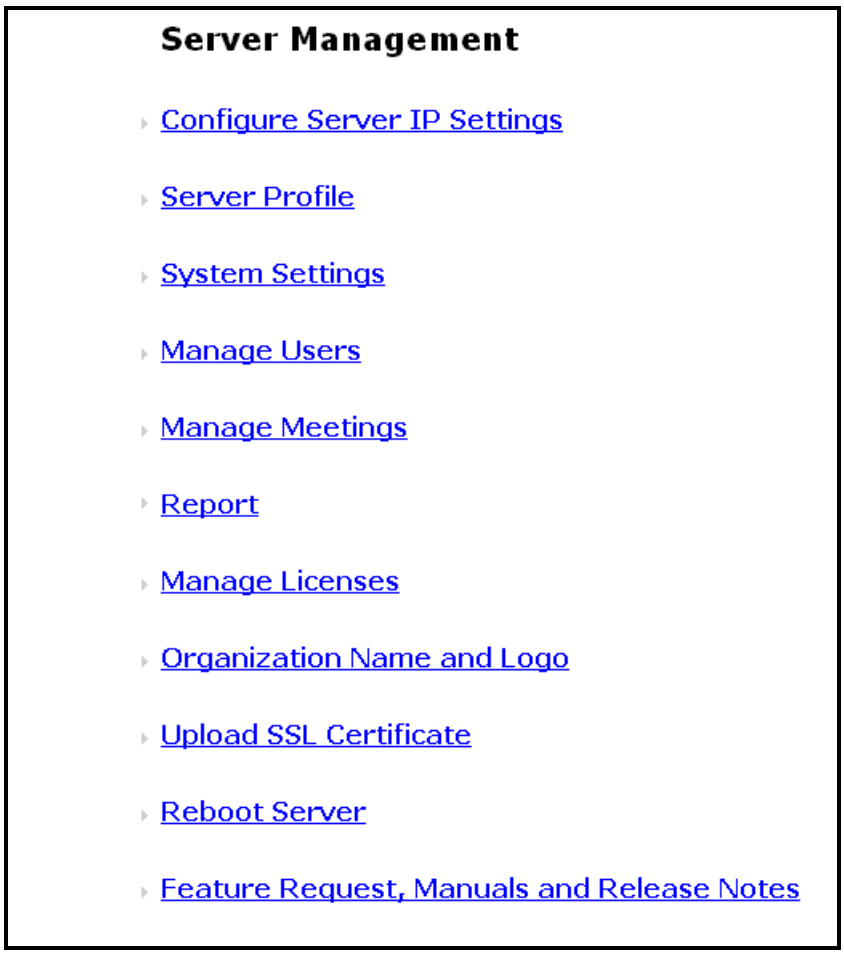


Figure 1.3 Management Home Page

Click the "Configure Server IP Settings" link. Figure 1.4 is displayed:

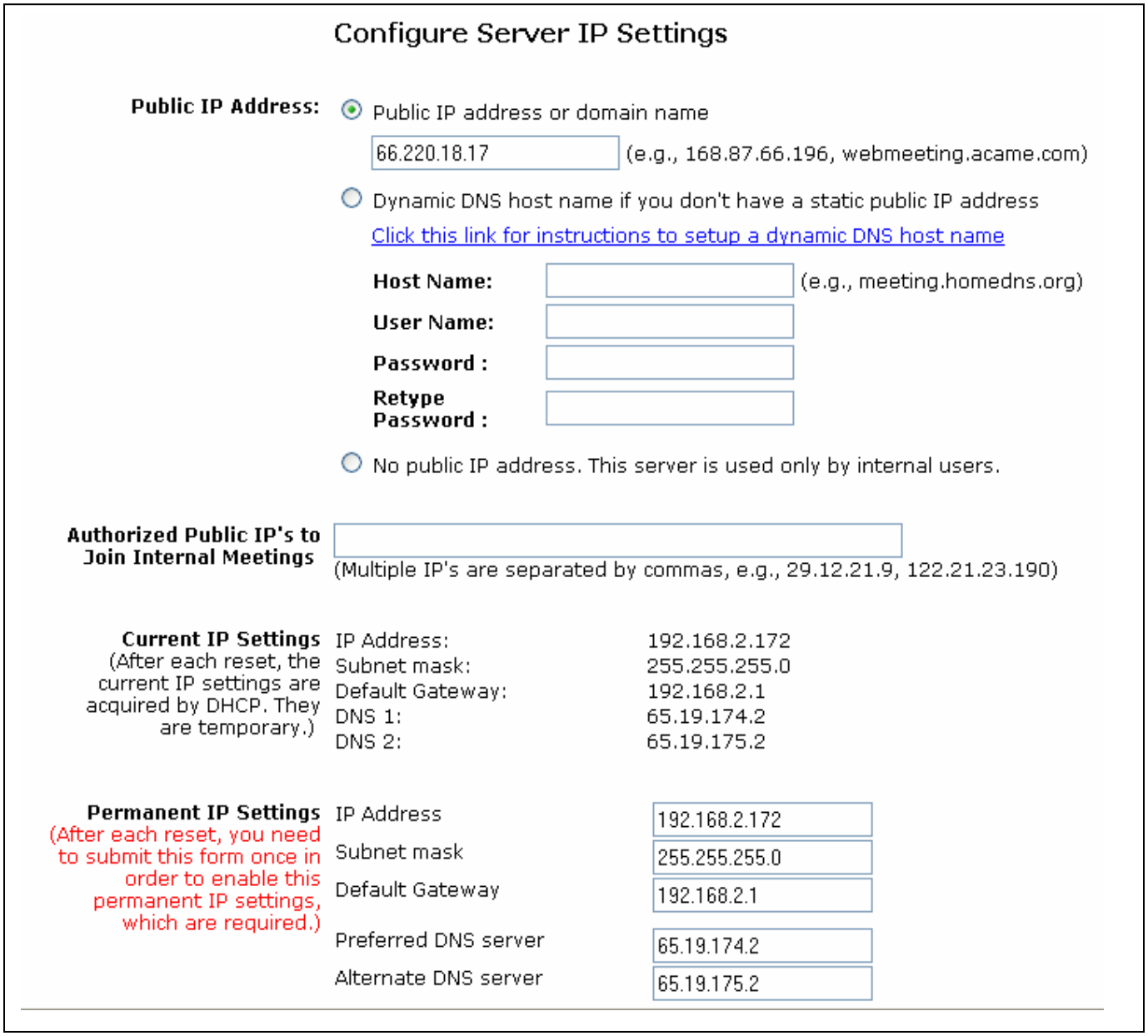


Figure 1.4 Configure Server IP Settings

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 appliance.

The following describes the fields in Figure 1.4.

- **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 Zultys appliance by the domain name you set at dyndns.

- **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**

  Those IP addresses are what the meeting server has currently.

- **Permanent IP Settings**

  The Permanent IP setting refers to the desired IP settings you want your meeting server to have. The permanent IP address can be the same as "Public IP Address" or different from "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, 443 and 8889) at the public IP address to the corresponding ports at the permanent IP address. See the next section for details.

  Carefully check if the DNS setting is correct or not. A wrong DNS setting will not allow the meeting server to connect to the Zultys Communications' release servers for auto-update.

  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 appliance.

If you make a mistake in configuration, you need to reset the appliance. See Section 5 for details.

Configuration for other areas of the system is self-explanatory. To understand how to customize the system, please follow the steps below for more information:

1. Go to www.zultys.com/webconferencing
2. Click the "Support" link
3. Click the "Customization" link.

2 Configure Firewall

There are three ways to deploy the M200/500:

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.

2.1 Behind Firewall and Accessible by Users outside Firewall

This deployment (Figure 2.1) is most popular and it is typically done by connecting the M200/500 with the DMZ port of your router. You can also place the M200/500 anywhere on your LAN.

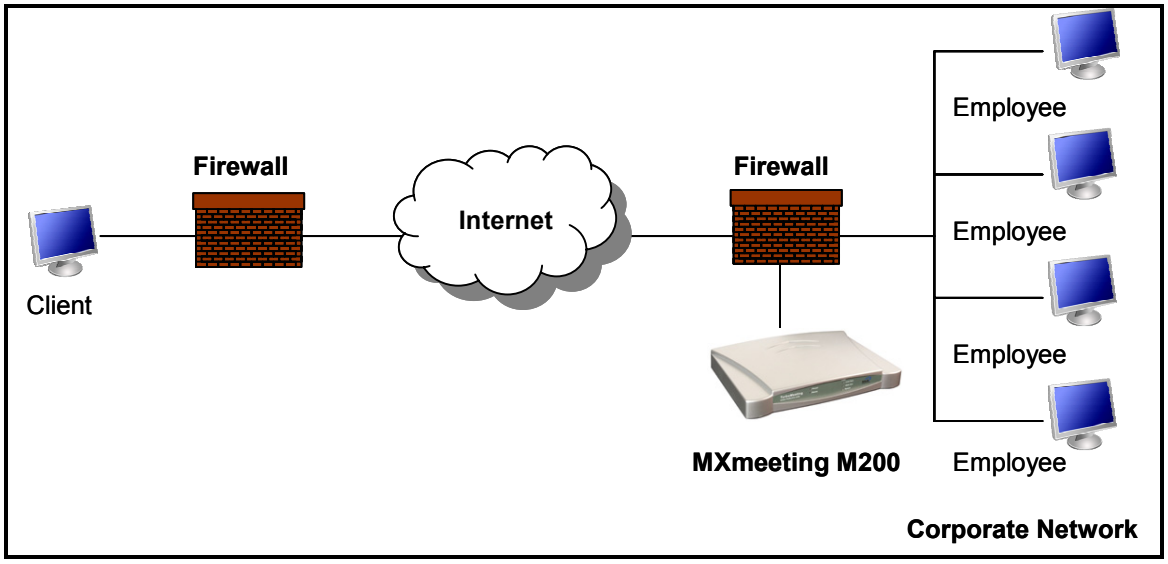


Figure 2.1 Inside Firewall and Accessible by Users outside Firewall

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

If you are using a SOHO or home router, opening inbound ports and making port forwarding are pretty straight forward. 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 2.2. Fill in the three TCP ports (80, 443 and 8889) and your Zultys appliance local IP address. The firewall configuration is done.

In Figure 2.2, the "Private IP address" is the Zultys appliance 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	TCP	192.168.1.192	8889 - 8889

Figure 2.2 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 (including Virtual Network) can join Note: You can manually augment the list of acceptable IP addresses as well
- External meetings that anyone including attendees outside your firewall can join.

2.2 Outside Firewall

With this deployment (Figure 2.3), M200/500 is completely outside your corporate firewall. There is no firewall configuration needed.

To configure server setting (Figure 1.4) 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".

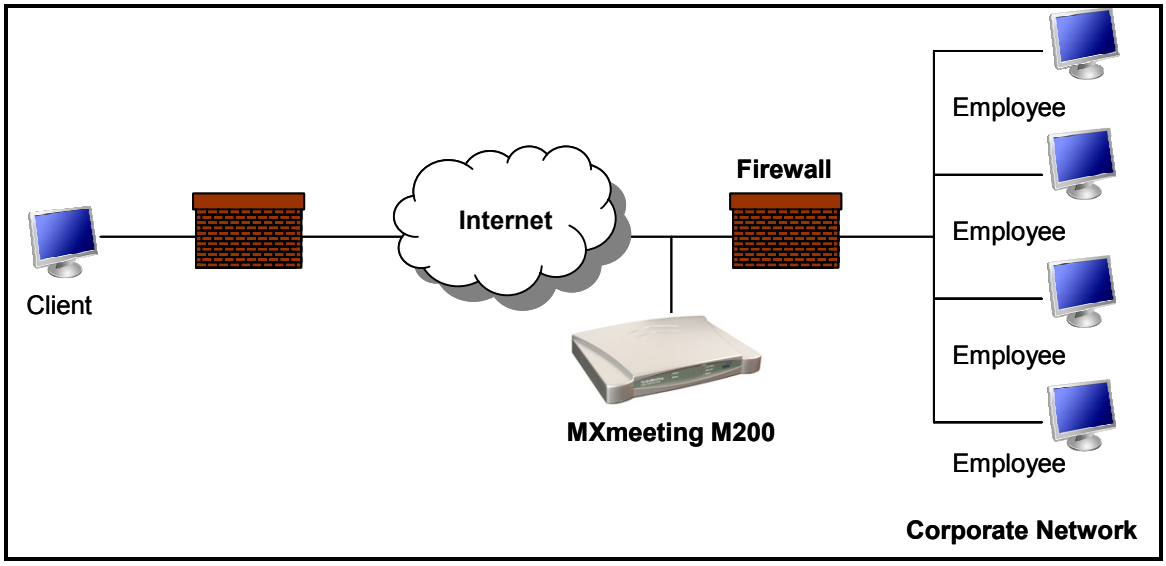


Figure 2.3 Outside the Firewall Deployment

2.3 Behind Firewall and Not Accessible by Users outside Firewall

This deployment (Figure 2.4) disconnects 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 setting configuration page (see Section 1.2), you choose the option "No public IP address. This server is used only by internal users.", and assign a static local IP, subnet mask, default gateway, and DNS for the meeting server (Figure 1.4) and only

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

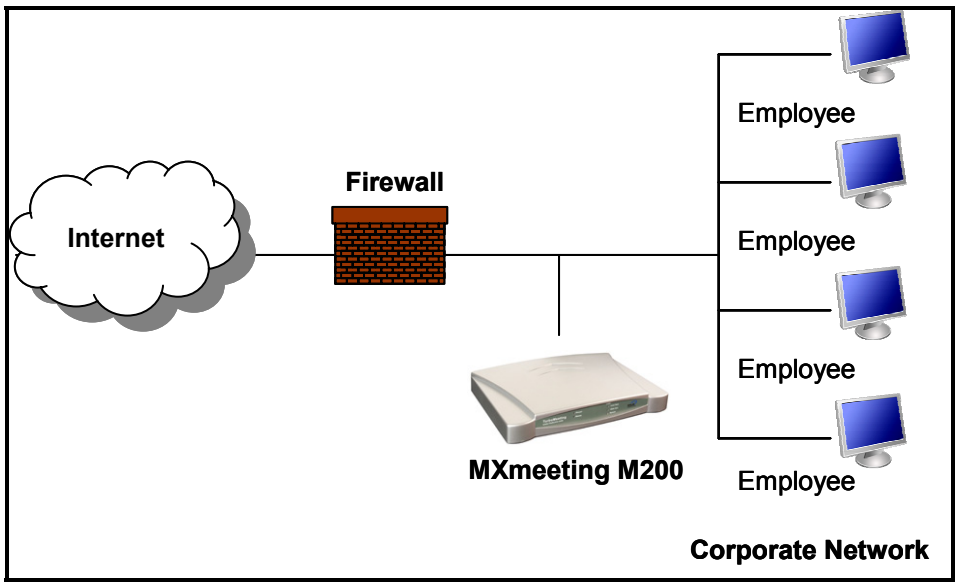
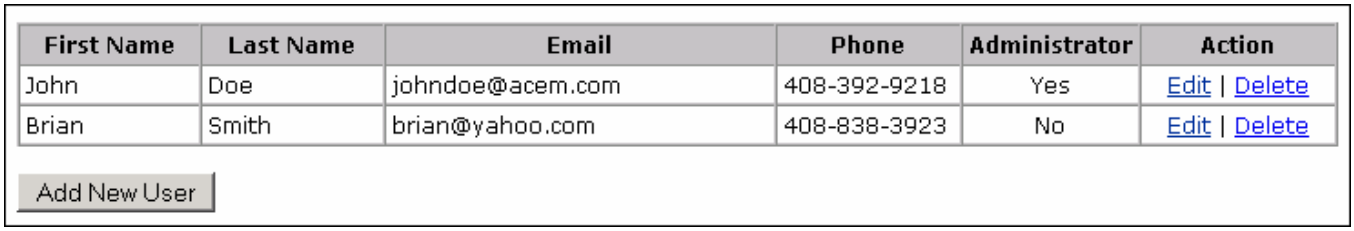


Figure 2.4 Inside Firewall and Not Accessible by Users outside Firewall

3. Manage Users

Login to the M200/500 and enter the management page shown in Figure 1.3. Click "Manage Users" link. A list of users will display as shown in Figure 3.1.



First Name	Last Name	Email	Phone	Administrator	Action
John	Doe	johndoe@acem.com	408-392-9218	Yes	Edit | Delete
Brian	Smith	brian@yahoo.com	408-838-3923	No	Edit | Delete

Add New User

Figure 3.1 List Users

You can click "Add New User" button to add a new user. Under the "Action" column, click on "Edit" to edit a user profile or "Delete" 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.

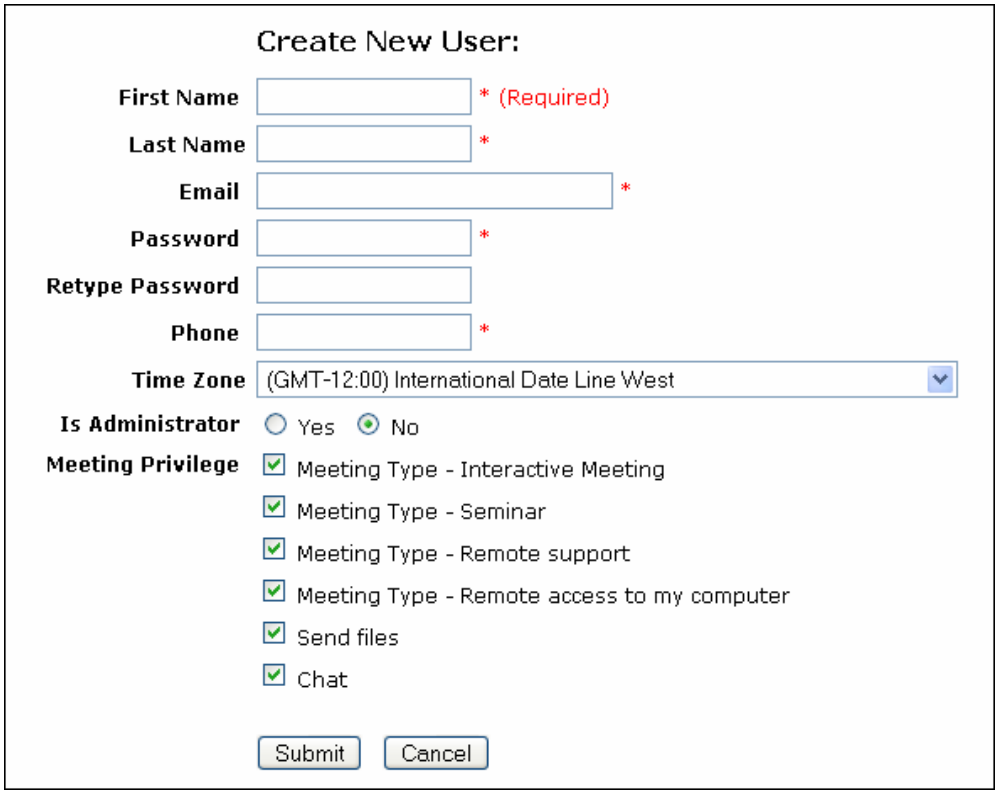


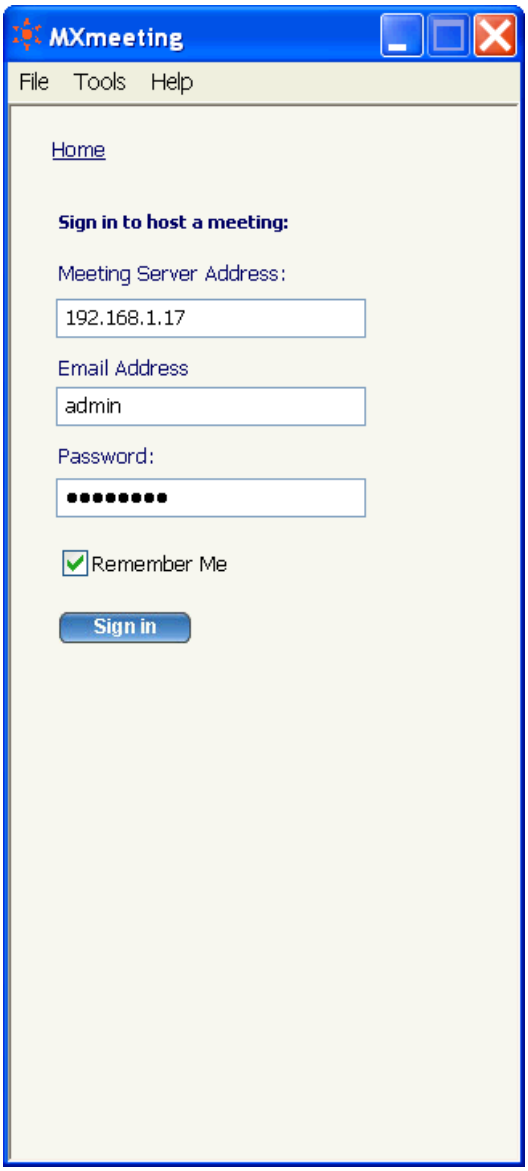
Figure 4.2. Create a user profile

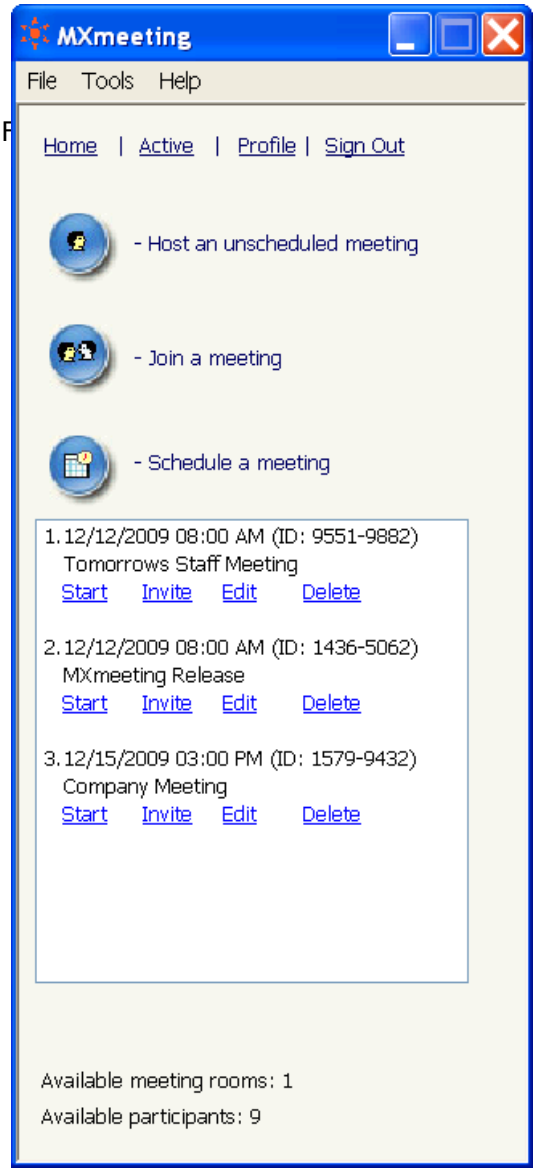
4. Start Meetings

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 M200/500 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. MXmeeting starts to run (Figure 4.1).

The Meeting Server Address in Figure 4.1 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 4.2.





F Figure 4.2. En

on the "Host an unscheduled meeting" button as shown in Figure 4.2 and then select a meeting type. Your meeting starts (Figure 4.3).

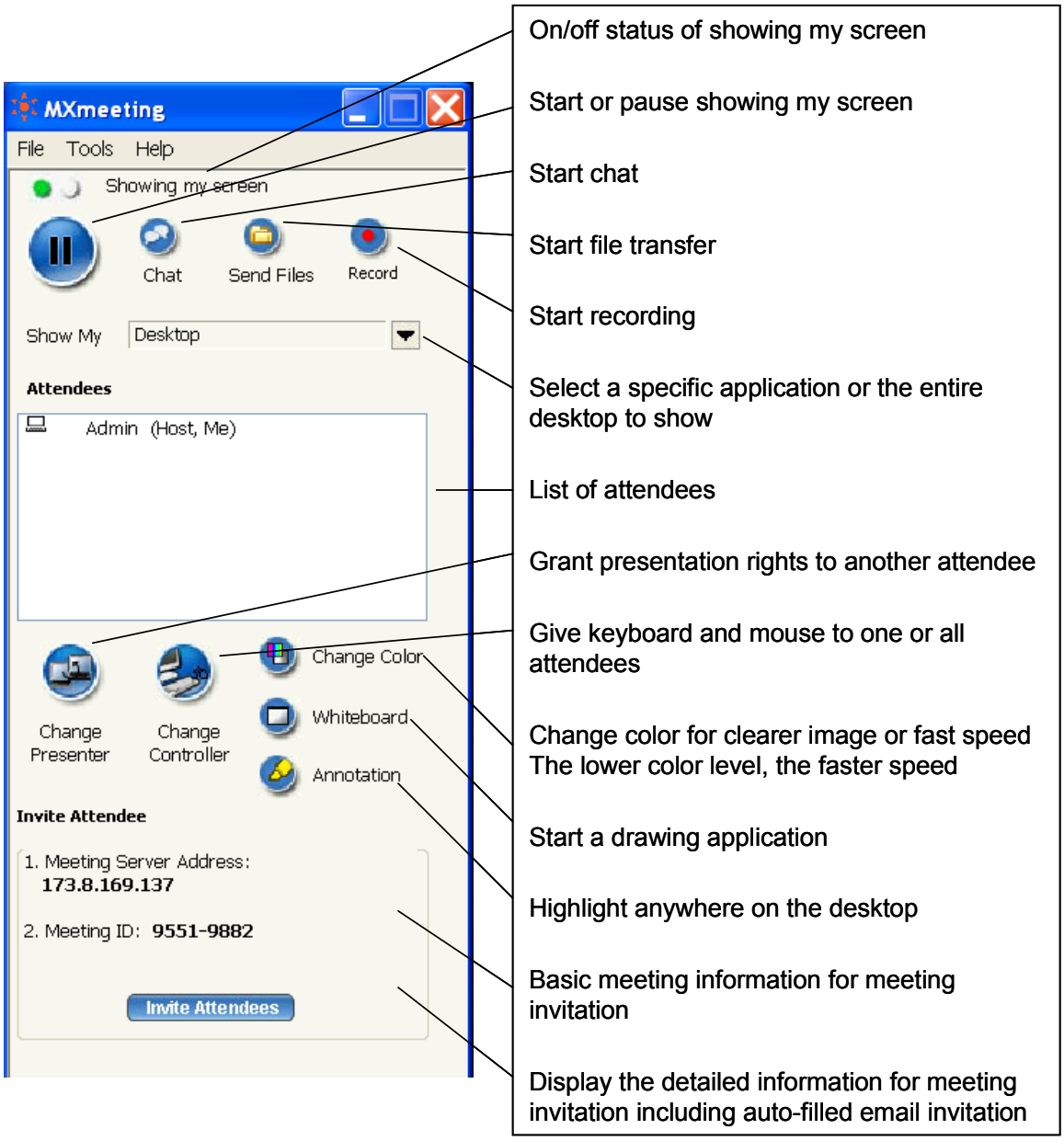


Figure 4.3. Main Meeting Control Panel

After the meeting starts, invite people to join your meeting by telling them the IP address and meeting ID shown on your meeting control panel. You can also click the "Invite Attendees" button for more invitation details.

5. Reset Appliance

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

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

The Zultys appliance does three things during the reset:

1. Reset 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 one's account.
2. Change the IP settings to use DHCP.
3. Remove your own system home page URL so that you can easily access the appliance 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 appliance, you just push a pin to the reset button on the back and hold it for over 6 seconds until the "Ready" light turns off. After over 20 seconds when the "Ready" light turns on, you can access the appliance.

Refer to the Section 1.1 for the access to your appliance after the reset.

6. Frequently Asked Questions:

How stable and scalable are MXmeeting appliances?

MXmeeting appliances are designed for both individual organizations and service providers. The stability and scalability have been well stress-tested by MXmeeting service provider customers worldwide. They rely on MXmeeting appliances to deliver high quality real-time web collaboration services to their customers. For example, one service provider has been using a M500 to support over 500 concurrent users during peak time although M500 is licensed to support only up to 100 concurrent users.

Complying with the high standards of system stability and scalability demanded by service providers, the MXmeeting appliance should meet your needs in terms of the system stability and scalability.

Do I need special IT skills to install an MXmeeting appliance? Do I need to maintain it?

If you know how to install and manage your home router, you are able to quickly install and setup MXmeeting appliances within 10 to 30 minutes.

MXmeeting appliance hardware (M200, M500) uses the components similar to those in your home and business routers. The hardware is extremely stable, no moving parts whatsoever. Just as you don't need to take care of your home router after it is installed, you don't need to maintain your MXMEETING appliance either. When new software is available, your MXMEETING appliance will automatically be updated. The MXMEETING appliance supports your critical meetings or remote-support sessions 24 x 7.

How are software updates handled?

Your MXmeeting appliance checks the MXmeeting release server everyday at midnight. If there is an update available, the appliance will automatically download and install. If you do not want the auto-update function, turn it off and use the manual update function. The system clock and auto-update settings are available under the "System Settings" on the web-based system console.

We encourage all of our MXmeeting clients to register with Zultys in order to receive system release notes from MXmeeting when software updates are available. The registration link is shown on the web administration console.

I have hundreds of remote computers to be accessed. How do I organize them with the MXmeeting appliance?

In order to remotely access a computer, you need to start a meeting with the meeting type "Remote Access to This Computer" on the computer and input a computer name. In order to organize hundreds of computers, you name the computer carefully with a group name, for example, "New York, Sales Office, Tom's Vista".

To access the remote computer, sign in your MXmeeting client and then click the "Active" meeting link. It will display all remote computers that are accessible. Type "New York" in the search text box. It will display only those computers with "New York" in the computer names. Locate the computer you are interested. Click the meeting ID and type the meeting password. You access the computer now.

My appliance is not updated. What is wrong?

First, check your DNS setting, which is on the "Configure Server IP Settings" page. Make sure you have a right DNS address.

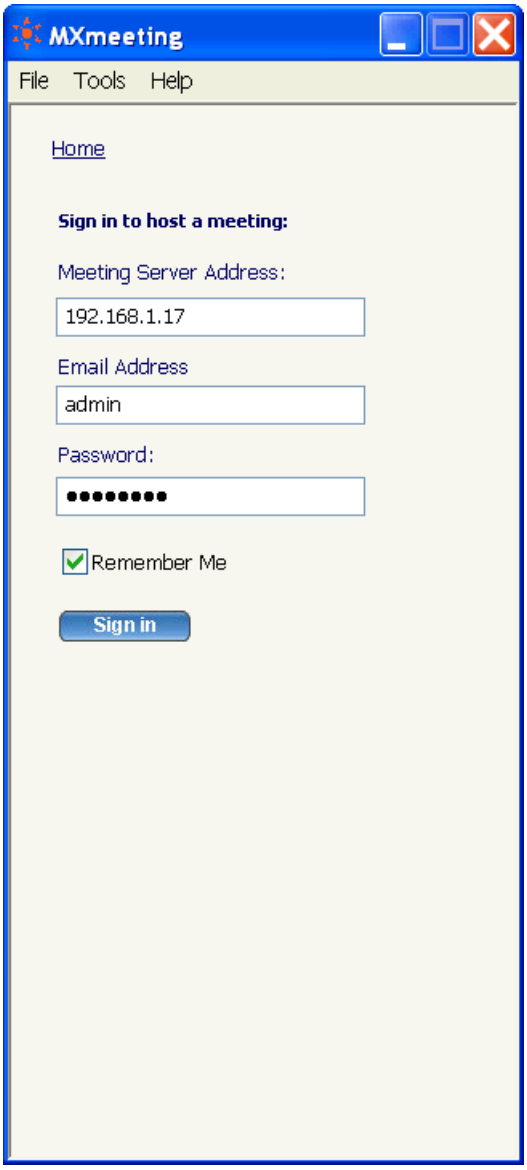
If your DNS setting is correct, go to "System Settings" page and see whether you have disabled the "Enable auto update of system (recommended) ". If it is disabled, click the "Update System Now" button to have your system updated.

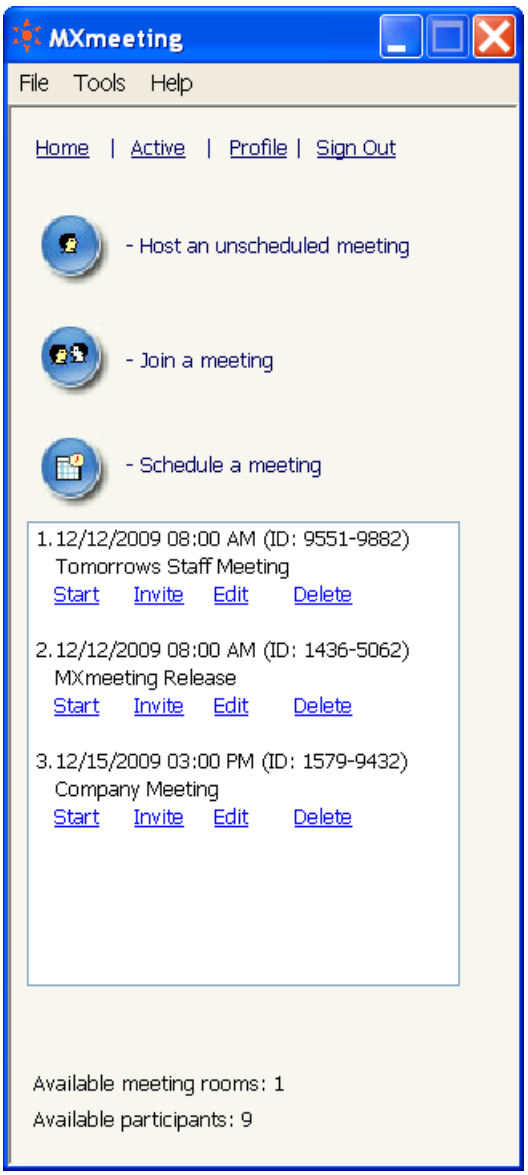
If it still cannot update, the only reason left is that your firewall is blocking the HTTP connection between your MXmeeting appliance and the MXmeeting release server. Configure your firewall to unblock the outbound TCP connection via the port 80 without any filtering rules just for the MXmeeting appliance. You may block the HTTP traffic after you get the system updated.

After I deploy my MXmeeting appliance behind my firewall, can I still invite attendees outside my firewall to join my meetings?

Yes, you can. All you need to do is to forward TCP traffic on ports 80, 443, and/or 8889 from your firewall/router to the MXmeeting appliance. All firewall/router devices including home routers provide this port forwarding function.

When you host a meeting, leave the box "Only attendees from my network" un-checked (the default). See the figure below:





Can anyone join my meetings?

You can invite anyone to join your meetings. You don't need to register them in the system. They do not need an MXmeeting appliance. However, you do need to register those users who want to host meetings using your MXmeeting appliance.

How much bandwidth does the system take? What are the minimum bandwidth requirements?

A typical PowerPoint presentation session over broadband connection requires only 1K bytes per second bandwidth on average. The peak speed varies depending on your available bandwidth.

For meeting hosts and interactive meeting attendees, the slow 28Kb dial-up modem speed is supported. For browser-based view-only meeting attendees, the minimum 200Kb download speed is required.

Do I need a fixed public IP?

No, you do not have to have a fixed IP. The MXmeeting appliance has integrated with the dynamic DNS service provided by http://www.dyndns.com. All you need to do is to register a user account, either a free one or a paid one. Then input the account information into the MXmeeting appliance system. After that, you can use a domain name of your choosing to access the MXmeeting appliance from anywhere over the Internet. The MXmeeting appliance will detect the changes of the public IP address of your router or modem and sync the changes with the DynDNS service.

Even if you have a fixed IP, it is still desirable to use the DynDNS service, which will allow you and your attendees to access your MXmeeting appliance by an easy-to-remember name rather than an IP address.

Can I reserve port 80 and 443 of my IP address for other purpose?

Yes, you can. However, it will have the following impacts to your MXmeeting system:

1. Your meeting server URL, which is shown in your meeting invitations, has to carry the port 8889 number, for example, http://webmeeting.acame.com:8889.
2. Some of your attendees may not be able to join your meetings since their firewalls do not allow traffic via any ports other than the standard Internet ports 80 or 443.
3. The meeting IDs, meeting passwords and user passwords will transmit over the Internet in plain text without SSL encryption.
4. You and your attendees will experience a longer time for the first-time connection since the MXmeeting client will try to use the port 443 SSL connection and eventually fail over to the port 8889. After the first-time connection, the next connections will be fast as the MXmeeting client remembers the working port.

How does the MXmeeting free audio conferencing work?

All MXmeeting appliances include audio conference call service at no extra cost to you. You may decide to use this service or choose your own audio conferencing method.

MXmeeting audio conferencing service provides a toll-based US number that can be dialed by all meeting participants. Participants are then charged their standard long-distance rate for calling this toll-based number, just as if they made a regular long-distance call.

MXmeeting does not provide toll-free audio conferencing service. You can select any of audio conferencing services including your own audio conferencing bridge. Integrating with audio conferencing is as easy as inputting a call number to the MXmeeting system. The call number will be passed to your meeting invitation messages and the MXmeeting meeting control panel automatically.

In addition to setting up a system-wide call number, each user can define his call number.

How do I purchase add-on licenses?

Login to the web console of the MXmeeting appliance and issue a license request to your reseller. After payment, the reseller will issue you a new license key that you can input into the MXmeeting appliance to upgrade your license.

Is a separate meeting room required for each registered user or can multiple users schedule a meeting for a room?

No meeting room is required for a registered user. A meeting room in the MXmeeting system is a measure of license in terms of the maximum number of active concurrent meetings. Before a meeting actually starts, a user does not hold any meeting room although he may have scheduled many meetings.

You can register as many users as you want in the system. The system only controls the number of meetings that are active and the number of total participants (hosts and attendees) in those active meetings.

I have a large screen. How do I limit what is viewed by the attendees?

Regardless of how large your screen is and how many monitors you have, the default view to your attendees is the scaled down version of your screen that fits your attendees' screen. This fit-to-screen display may not display a clear screen of yours because of the scale down effect. We suggest you select an application or a monitor to show. This also improves meeting traffic speed because only a portion of a screen image is transferred.

Do MXmeeting appliances provide SSL encryption? Can they be accessed by SSL only?

Every MXmeeting appliance comes with a manufacturer's default SSL certificate. Though the certificate does not match your domain name, it won't affect SSL-encrypted transmission between MXmeeting client and the MXmeeting appliance. All user passwords, meeting passwords and meeting IDs are transmitted via SSL. By default, a screen image is transmitted with MXmeeting proprietary encryption for efficiency.

You can configure your MXmeeting appliance in such a way that everything transmits over the Internet via SSL. Go to the system administration web console, click the "System Settings" link and check the option "Access this server only via SSL". In addition, you need to upload your own certificate in order to avoid the annoying security alert that is due to the default MXmeeting SSL certificate when users visit your MXmeeting appliance web pages.

Can anyone including MXmeeting staff access my appliance without my knowledge?

For M200, M500, no one can access the appliance without your knowledge, including MXmeeting staff. The appliance is self-protected. You can simply place the appliance outside your firewall and router.

In case you need the support that requires MXmeeting staff access to the appliance, you would login to the web console as a system administrator and execute a special command. While MXmeeting support staff remotely accesses your appliance, they cannot retrieve user passwords or passwords for remote access meetings. All those passwords are irreversibly encrypted in the database.

M800, M1000 are deployed in a regular Linux server. You need to place it behind your firewall and block all inbound ports to the server except the TCP ports: 80, 443, and 8889. The system is configured with a default password, which you should change after installation.

Is Java required to run MXmeeting?

No, Java is not mandatory. However, Java is used to facilitate the initial user experience to download and launch MXmeeting. MXmeeting client software itself is not dependent on Java in any way. If you do not have Java installed, you will be directed to a page to download the MXmeeting executable and run it.

7. Support Contact

If you purchased the MXmeeting Appliance from a Zultys 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.

Zultys, Inc.
771 Vaqueros Ave
Sunnyvale, CA 94085
Tel: 408-328-0450
Fax: 408-328-0451
support@zultys.com
http://www.zultys.com