



SmartBridge Administrator Manual

Version 1.0

Asante Network.,
47436 Fremont Blvd.
Fremont, CA 94538
support@asante.com
<http://www.asante.com>

Contents

1. INSTALLATION.....	3
1.1. ACCESSING YOUR ASANTE WEB CONFERENCING APPLIANCE	3
2. CONFIGURING THE ASANTE WEB CONFERENCING APPLIANCE.....	5
2.1. CONFIGURE SERVER IP SETTINGS	7
2.2. SYSTEM SETTINGS	9
2.3. MANAGING YOUR SSL CERTIFICATE.....	10
2.4. SCHEDULED MEETINGS AND ACTIVE MEETINGS.....	12
2.5. CUSTOMIZING THE MEETING START AND PROMOTION PAGES.....	13
2.6. INTEGRATION.....	15
2.7. LICENSING	17
3. CONFIGURING THE FIREWALL.....	18
3.1. BEHIND FIREWALL AND ACCESSIBLE BY USERS OUTSIDE FIREWALL.....	18
3.2. OUTSIDE THE FIREWALL	19
3.3. BEHIND FIREWALL AND NOT ACCESSIBLE BY USERS OUTSIDE FIREWALL	21
4. MANAGE USERS	22
5. START MEETINGS.....	23
6. REPORTING	25
7. RESET APPLIANCE	26
SUPPORT CONTACT.....	27

1. Installation

The Web conferencing server package includes:

- SmartBridge-8, SmartBridge-16, appliance (or server)
- Analog console cable
- Ethernet crossover-cable
- Power adaptor

1.1. Accessing your Asante Web Conferencing Appliance

There are two ways to access the SmartBridge-8, and SmartBridge-16 appliances: by using plug-and-play or by using an Ethernet crossover-cable. In either way, 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 (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 will be viewed.

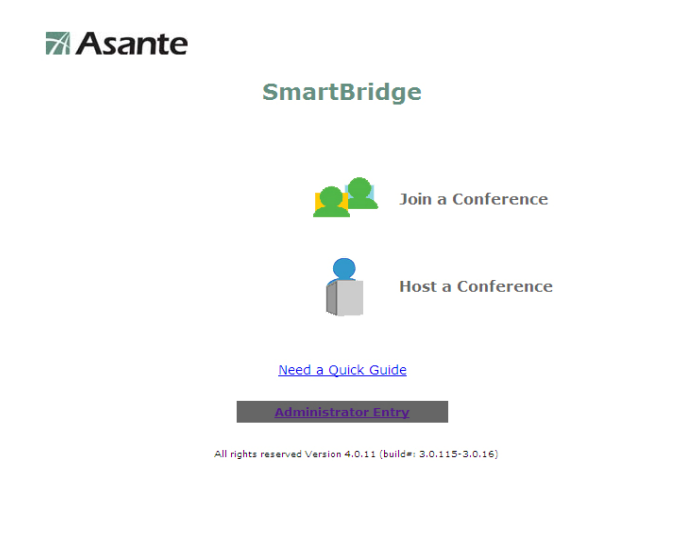


Figure 1.1. Home Page

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

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

The crossover-cable is used for the SmartBridge-8, and SmartBridge-16. Before you use the crossover-cable 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 SmartBridge-8, or SmartBridge-16, (as described above)
Wait for the ready light to turn green. This usually takes about 90 seconds
Connect the SmartBridge-8, or SmartBridge-16 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 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 SmartBridge-8, and SmartBridge-16, 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.

2. Configuring the SmartBridge Appliance

After you accessing the appliance server home page (Figure 1.1), click the “Administrator Entry” link and you will see the login page shown in Figure 2.1. Type

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.




The screenshot shows a login form with the following elements:

- Title:** Login
- Email field:** A text input box containing the text "admin".
- Password field:** A text input box containing masked characters (dots).
- Login button:** A button labeled "Login" located below the password field.

Figure 2.1 Login Page

After login, the **System Management** home page is displayed in Figure 2.2

**SmartBridge System Management**[Sign Out](#)

[Home](#)

Configuration
[IP Settings](#)
[System Settings](#)
[SSL Certificate](#)

User Management
[Users](#)

Meetings
[Scheduled](#)
[Active](#)

Customization
[Name & Logo](#)
[Entry Page](#)
[Promotion Page](#)
[Audio Conference](#)

Integration
[Application Server](#)

Licensing
[Request](#)
[Upgrade](#)

[Report](#)

[Reboot](#)

[Manuals & Updates](#)

Server Profile

Number of Meeting Rooms	5
Number of Concurrent Users	10
Serial Number	10243
Model	RHUB200
System Version	4.0.11 (build#: 3.0.16)
Mac Address	00:e0:f2:36:00:3c

IMPORTANT : [Register](#) to ensure:

- ▶ Software is properly updated
- ▶ You are informed of the most recent changes
- ▶ You receive the manufacturer support and warranty

Figure 2.2 Management Home frame

Fig 2.2

2.1. Configure Server IP Settings

Configure Server IP Settings

Public IP Address: Public IP address or domain name
 (e.g., 168.87.66.196, webmeeting.acame.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:	192.168.1.200
Subnet mask:	255.255.255.0
Default Gateway:	192.168.1.1
DNS 1:	68.87.76.182
DNS 2:	68.87.78.134

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

IP Address	<input type="text" value="192.168.1.200"/>
Subnet mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Preferred DNS server	<input type="text" value="68.87.76.182"/>
Alternate DNS server	<input type="text" value="68.87.78.134"/>

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 appliance.

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 SmartBridge by the domain name you set at DynDNS.

Note that Asante offers the DynDNS client as a convenience to our customers. Asante 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 Asante.

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 "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 that the DNS setting is correct. A wrong DNS setting will stop the meeting server from connecting to the Asante Communications' release servers for automatic updates.

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 6 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.



The screenshot shows the 'System Settings' interface. It includes a 'Language' dropdown menu set to 'English', a 'Time Zone' dropdown menu set to '(GMT-08:00) Pacific Time (US & Canada)', and 'Time & Date' fields for hours (21), minutes (40), and date (09/23/2009). There are two checkboxes: 'Enable auto update of system (recommended)' which is checked, and 'Access this server only via SSL (this will reduce system performance)' which is unchecked. At the bottom, there are 'Submit' and 'Cancel' buttons, and an 'Update System Now' button with a note '(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 SmartBridge System Management UI can be changed to English, Chinese (Simplified), Chinese (Traditional), Japanese or Spanish.

Time Zone and Time & Date

Set the correct time zone, time and date for the SmartBridge.

Enable auto update of system

The SmartBridge retrieves software updates automatically if this is enabled. . This is done at 3 AM for the time set on the appliance.

Access this server only via SSL

By default, screen images during a meeting are transmitted with proprietary encryption for efficiency. However, you can use SSL for encryption by enabling the **Access this server only via SSL** option. See the section **Manage Your SSL Certificate** about how to upload your own SSL Certificate.

Update System Now

This feature retrieves updated SmartBridge software from the Asante 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: * (Required) (e.g., webmeeting.aceme.com)

Organization Name: * (e.g., Aceme, Inc.)

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

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

Country: ▼

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 SmartBridge. 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.

Step 2: Purchase Your SSL Certificate

Go to <http://www.instantssl.com> and purchase an "Instant SSL" certificate with the CSR you just created. During the checkout on the website, select "Apache-ModSSL" as the "Web Server Software". This system SSL function has been only tested with an Instant SSL certificate by Comodo Certificate Authority (CA). Comodo is a high quality, affordable CA.

Figure 2.6 Setting up an SSL Certificate, step 2

Locate your SSL Certificate file and your CA Root Certificate 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
ZFRydXNOIEV4dGVybmAtTHLETICSZXR3b3JrMSIwIAYDVQOEx1BZGR
UcnVzdCBF
(.....)
vm9nu/9iVzmdDE2yKmE9HZzvmncgoC/uGnKdsJ2/eBMnBwpgE2P1Dy7
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
```

Upload SSL Certificates

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

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 SmartBridge. 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://webmeeting.company.com/as/wapi/list_public_scheduled?cuid=FRF0E2IIAQdEQB4zEw5yFGAUAqdBQTU%3D						
▶ The URL to publish the scheduled public meetings in XML: http://webmeeting.company.com/as/wapi/list_public_scheduled?is_xml=Y&cuid=FRF0E2IIAQdEQB4zEw5yFGAUAqdBQTU%3D						
▶ List of Scheduled Meetings:						
Meeting ID	Meeting Subject	Start Time	Time Zone	Host Name	Host Email	Host Phone
34028138	Seminar	Recurring	(GMT-12:00) International Date Line West	John Doe	jdoe@company.com	NA
39161351	Remote support	Recurring	(GMT-12:00) International Date Line West	John Doe	jdoe@company.com	NA

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 SmartBridge. 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	Host Name	Host Email	Host Phone	Last Connect Time	Number Of Users	Host IP	Action
57899716	John Doe	jdoe@company.com	NA	09/23/2009 PM 5:26:32	46	66.67.96.97	Stop
89541306	John Doe	jdoe@company.com	NA	09/23/2009 PM 5:26:31	2	66.67.96.97	Stop

Figure 2.10 List of active meetings

2.5. Customizing the Meeting Start and Promotion Pages

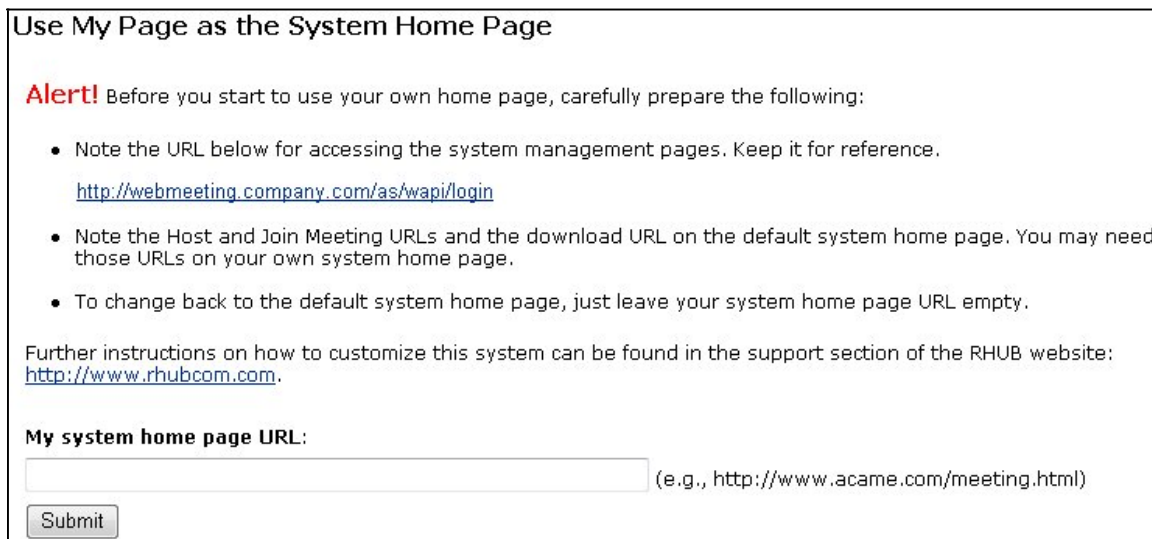
In the left frame of the System Management page, under Customization click the [Name & Logo](#) link. This feature allows the Administrator to use show your company's name and logo on the standard meeting home page.



The screenshot shows a form titled "Organization" with three input fields and two buttons. The first field is "Organization Name" with the value "YourCompany" and a red asterisk indicating it is required. The second field is "Website" with the value "http://www.company.com" and a note "(e.g., http://www.acme.com)". The third field is "Logo URL" with the value "http://www.company.com/logo.gif" and a note "(e.g., http://www.acme.com/logo.gif)". Below the fields are "Submit" and "Cancel" buttons.

Figure 2.11 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.



The screenshot shows a form titled "Use My Page as the System Home Page". It starts with an "Alert!" section: "Alert! Before you start to use your own home page, carefully prepare the following:" followed by three bullet points. The first bullet point says "Note the URL below for accessing the system management pages. Keep it for reference." and provides the URL <http://webmeeting.company.com/as/wapi/login>. The second bullet point says "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." The third bullet point says "To change back to the default system home page, just leave your system home page URL empty." Below the alert is a note: "Further instructions on how to customize this system can be found in the support section of the RHUB website: <http://www.rhubcom.com>." At the bottom, there is a label "My system home page URL:" followed by an input field and the text "(e.g., http://www.acame.com/meeting.html)". A "Submit" button is located below the input field.

Figure 2.12 Use a new page for the meeting home page

The system home page specified in Figure 2.12 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 SmartBridge.

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.

<p>Promotional URL, presented to attendees when meetings end</p> <input type="text" value="http://www.company.com/promotion.html"/> (e.g., http://www.acame.com)
<input type="submit" value="Submit"/>

Figure 2.13 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 change the telephone number used for audio conferencing.

Audio Conferencing Options:

None

My audio conferencing number:

Use Meeting ID as the audio conference Access Code

Asante Free Audio Conferencing Service using a US conference call number

Figure 2.14 Change audio conference phone number

2.6. Integration

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.

Integration Settings

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.

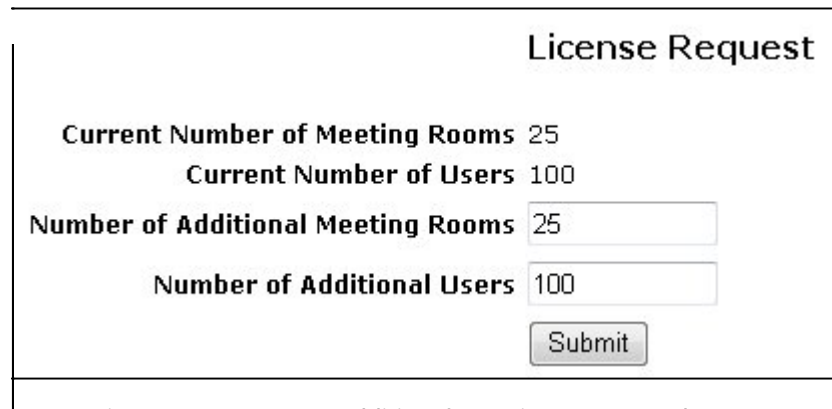
Figure 2.15 Integration with your server for user authentication

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

1. Go to <http://www.asante.com>
2. Click the "Support" link
3. Click the [Integration](#) link

2.7. Licensing

In the left frame of the System Management page, under Licensing click the [Request](#) link. This allows your SmartBridge to host more meetings and allow more users.



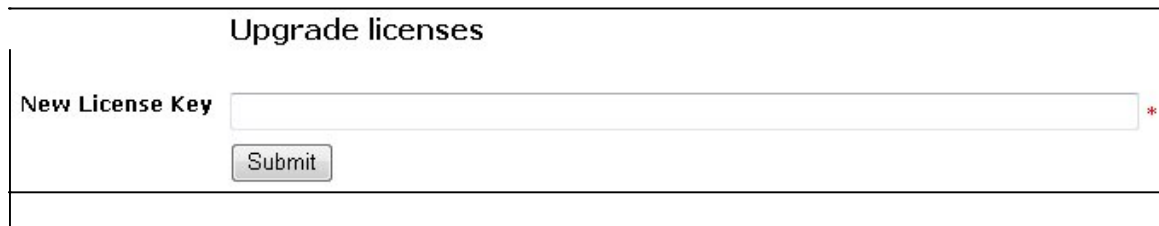
The screenshot shows a form titled "License Request" with the following fields and values:

Field	Value
Current Number of Meeting Rooms	25
Current Number of Users	100
Number of Additional Meeting Rooms	<input type="text" value="25"/>
Number of Additional Users	<input type="text" value="100"/>

Below the input fields is a "Submit" button.

Figure 2.17 Request additional meeting rooms and users

In the left frame of the System Management page, under Licensing click the [Upgrade](#) link. By filling in the license key and clicking submit, you can upgrade the license for your Asante appliance.



The screenshot shows a form titled "Upgrade licenses" with the following fields and values:

Field	Value
New License Key	<input type="text"/>

Below the input field is a "Submit" button.

Figure 2.18 Upgrade Asante license

3. Configuring the Firewall

There are three ways to deploy your SmartBridge-8 and SmartBridge-16

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 SmartBridge appliance with the DMZ port of your router. You can also place the SmartBridge anywhere on your LAN.

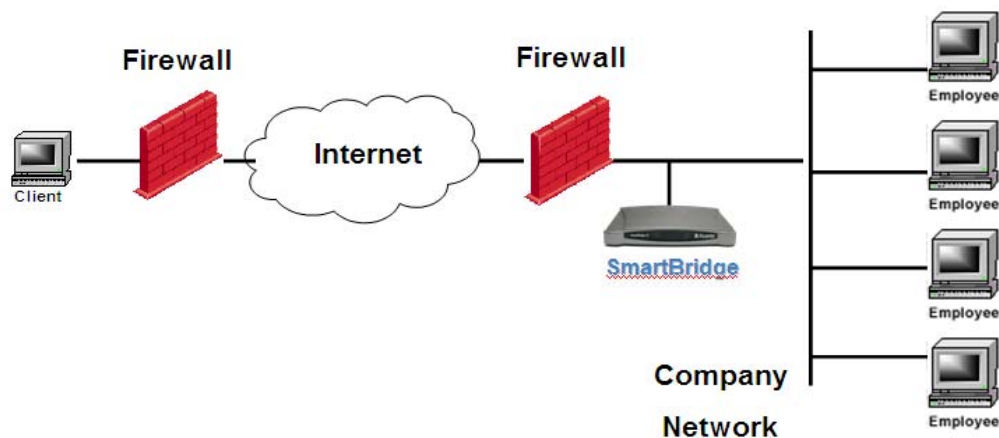


Figure 3.1 Inside Firewall and Accessible by Users outside Firewall

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 SmartBridge.

If you are using a SOHO or home router, opening inbound ports and doing port forwarding are fairly easy. For example, in a Asante/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 three TCP ports (80, 443 and 8889) and your SmartBridge local IP address. The firewall configuration is done.

In Figure 3.2, the "Private IP address" is the SmartBridge'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.	<input checked="" type="checkbox"/>	80	80 - 80	TCP	192.168.1.192	80 - 80
2.	<input checked="" type="checkbox"/>	443	443 - 443	TCP	192.168.1.192	443 - 443
3.	<input checked="" type="checkbox"/>	8889	8889 - 8889	TCP	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 a 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 closer to yours. Click the router. On the next page, click "Click here to skip this advertisement..." on the top right. Now it shows a long list of applications you can do port-forwarding for. Just pick one application. Replace the application ports by TCP 80, 443 and 8889, which SmartBridge uses.

3.2. Outside the Firewall

With this deployment (Figure 3.3), your SmartBridge 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".

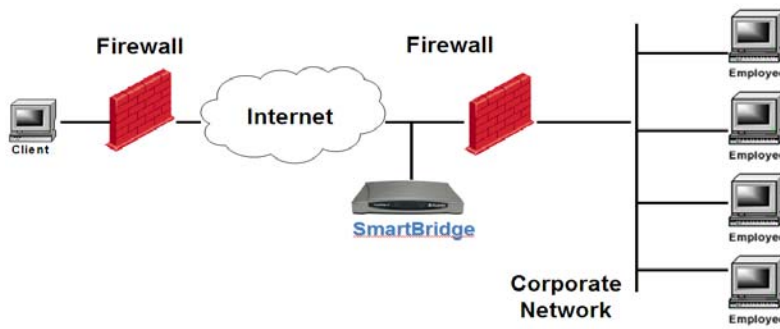


Figure 3.3 Deployment Outside the Firewall

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.

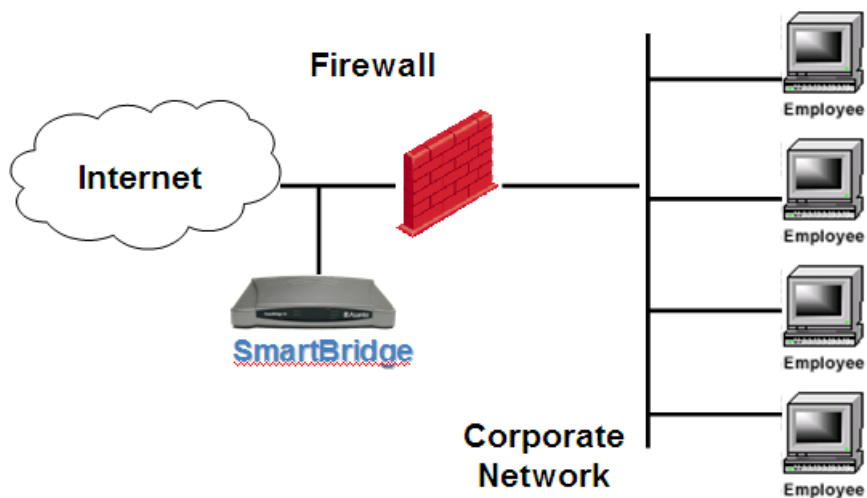


Figure 3.4 Inside Firewall and Not Accessible by Users outside Firewall

4. Manage Users

Login to the home page for your SmartBridge-8, and SmartBridge-16 appliance 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 in Figure 4.1.

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

Figure 4.1 List Users

You can click **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 * (Required)

Last Name *

Email *

Password *

Retype Password

Phone *

Time Zone (GMT-12:00) International Date Line West ▼

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

Figure 4.2 Create a user profile

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 SmartBridge 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. SmartBridge 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.

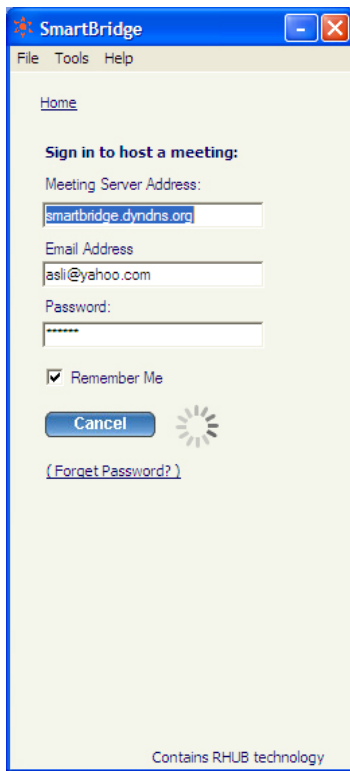
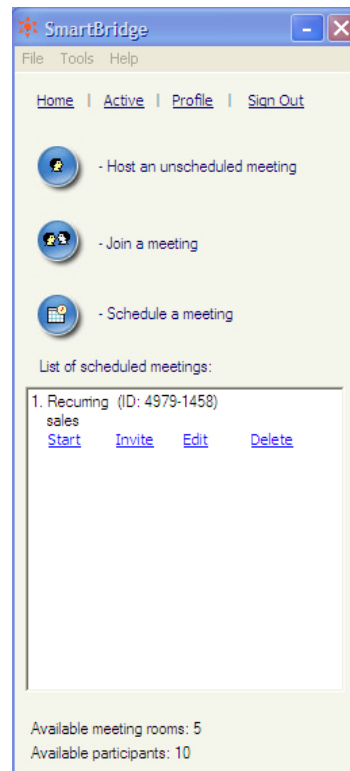


Figure 5.1 Start Meeting Figure



5.2 Enter Meeting Control Panel

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

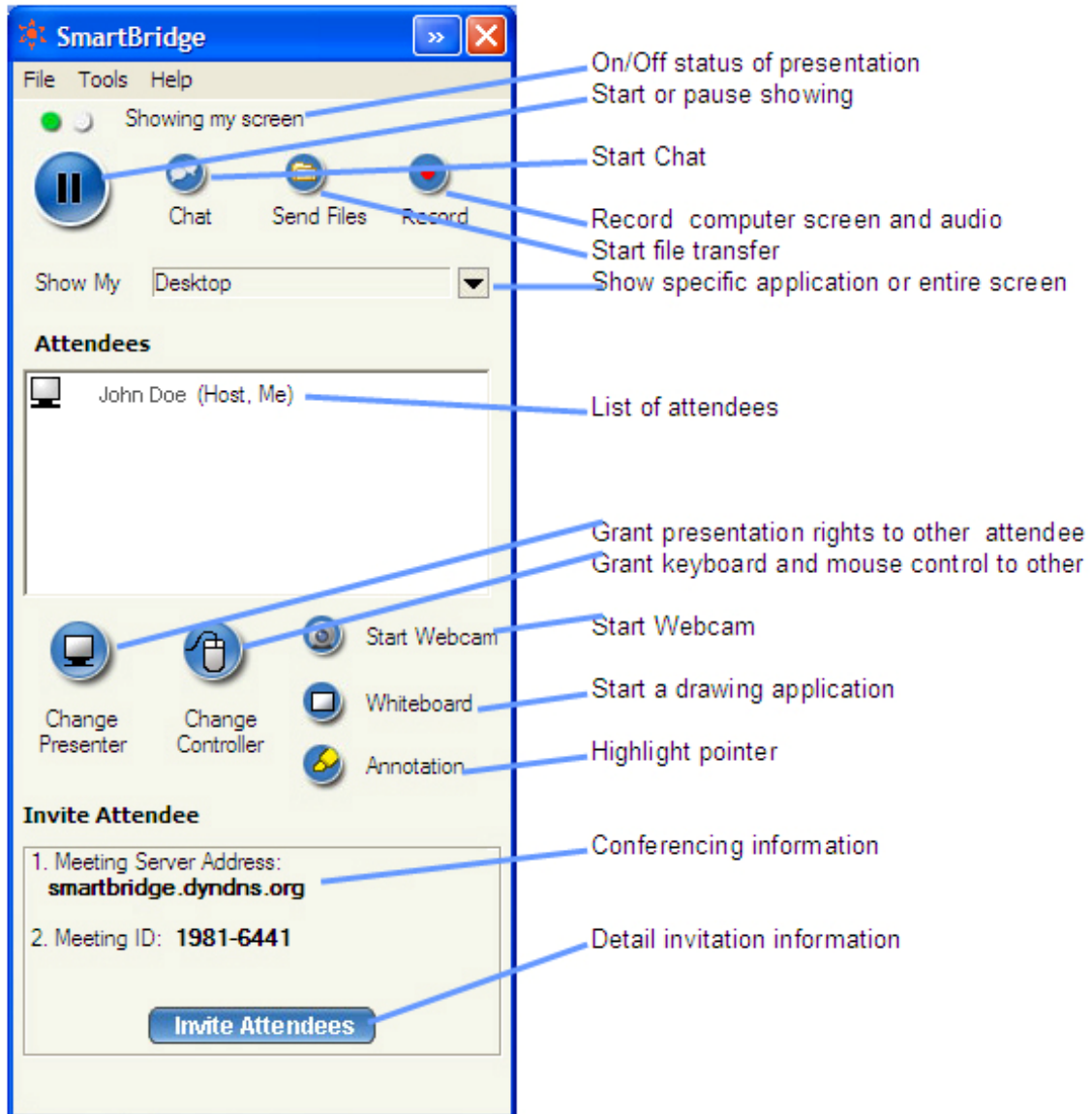




Figure 5.3 Main Meeting Control Panel


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.

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 SmartBridge. 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.

Report - List of Meetings

From 
User 
Total Meeting Time: 48h 52m 40s
(h: hour, m: minute, s: second)

To 

[Download in Excel](#)

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 Appliance

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

1. You forgot 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 SmartBridge 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 one's account.
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 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 Asante SmartBridge-8, SmartBridge-16, you just push a pin into 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 about how to access to your appliance after the reset.

Support Contact

If you purchased the SmartBridge Appliance from a Asante 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.

Asante Network

47436 Fremont Blvd.

Fremont, CA 94538

Tel: 408-435-8388

Fax: 510-438-6790

support@asante.com

<http://www.asante.com>