ARGONNE NATIONAL LABORATORY
9700 South Cass Avenue
Argonne, IL 60439

ANL/MCS-TM-286

Venue Client User Manual

Access Grid Toolkit 2.3 Documentation

by

Ivan R. Judson, Susanne Lefvert, Eric Olson, Thomas D. Uram

The Futures Laboratory
Mathematics and Computer Science Division

Technical Memorandum No. 286

February 2006

Funding for this work has been provided by the U.S. Department of Energy under Contract DE-AC02-06CH11357 and by Microsoft Research.

About Argonne National Laboratory

Argonne is managed by UChicago Argonne, LLC, for the U.S. Department of Energy's Office of Science, under contract DE-AC02-06CH11357. The Laboratory's main facility is outside Chicago, at 9700 South Cass Avenue, Argonne, Illinois 60439. For information about Argonne and its pioneering science and technology programs, see www.anl.gov.

Availability of This Report

This report is available, at no cost, at http://www.osti.gov/bridge. It is also available on paper to U.S. Department of Energy and its contractors, for a processing fee, from:

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831-0062
phone (865) 576-8401
fax (865) 576-5728
reports@adonis.osti.gov

Disclaimer

Contents

Abstract 1
1.0 Introduction 1
2.0 Overview 2
3.0 Actions 4
3.1 Requesting a Certificate 4
3.2 Starting a Venue Client 7
3.3 Connecting to a Venue 8
3.3.1 Specifying Venue Address 8
3.3.2 Creating a Grid Proxy Certificate 8
3.4 Viewing a Profile 9
3.5 Changing Your Profile 9
3.6 Writing Text Messages 10
3.7 Saving Text Messages 10
3.8 Viewing Venue Properties 10
3.9 My Venues 11
3.9.1 Setting Your Home Venue 11
3.9.2 Going to Your Home Venue 11
3.9.3 Adding a Venue 11
3.9.4 Removing a Venue 12
3.9.5 Renaming a Venue 12
3.10 Navigating 12
3.11 Sharing Data 12
3.11.1 Adding Venue Data 13
3.11.2 Adding Personal Data 13
3.11.3 Deleting Data 13
3.11.4 Opening Data 13
3.11.5 Viewing Data Properties 14
3.12 Sharing Applications 14
3.12.1 Starting a Session 14
3.12.2 Joining a Session 14
3.12.3 Stopping a Session 15
3.12.4 Authorization 15
3.12.5 Opening a Monitor 15
3.12.6 Viewing Properties 16
3.13 Sharing Services 16
3.13.1 Adding Service 16
3.13.2 Opening a Service 17
3.13.3 Deleting a Service 17
3.13.4 Viewing Service Properties 17

3.14 Managing Certificates 17
3.14.1 Viewing Certificates 18
3.14.2 Importing a Certificate 18
3.14.3 Exporting a Certificate 18
3.14.4 Deleting a Certificate 18
3.14.5 Setting the Default Certificate 19
3.14.7 Destroying a Proxy 19
3.14.8 Viewing Trusted CA Certificates 19
3.15 Managing Your Node 20
3.15.1 Starting a Service Manager 20
3.15.2 Starting a Node Service 20
3.15.3 Opening a Node Management Window 20
3.15.4 Adding a Service Manager 21
3.15.5 Removing a Service Manager 21
3.15.6 Adding a Service 21
3.15.7 Enabling or Disabling a Service 22
3.15.8 Removing a Service 22
3.15.9 Changing Service Configuration 22
3.16 Authorization 23
3.17 Submitting an Error Report 24
3.17.1 Bugzilla 24
3.17.2 Automatic Bug Reports 24
4.0 About Certificates 24
4.1 Why Use Certificates? 25
4.2 Distinguished Name 25
4.3 Grid Proxy 25

Venue Client User Manual
Access Grid Toolkit 2.3 Documentation

by

Ivan R. Judson, Susanne Lefvert, Eric Olson, Thomas D. Uram

Abstract

This guide describes how to use the Access Grid Venue Client for the 2.3 release of the software. It provides users with a general overview of the system as well as detailed descriptions of how to perform different tasks ranging from requesting a certificate to setting a home venue. The objective of this document is to offer users a course of action when first operating the Venue Client. Additionally, this guide is a reference point for experienced users who wish more advanced information.

1.0 Introduction

The **Access Grid** is an Internet-based model for video conferencing that focuses on group-to-group communication, using an ensemble of resources including multimedia large-format displays, presentation and interactive environments, and interfaces to Grid middleware and visualization environments. For instance, the Access Grid is used for large-scale distributed meetings, collaborative work sessions, seminars, lectures, tutorials, and training. Even though the Access Grid is concentrated on group interactions, it also provides an access point for individual desktop users, permitting one-to-many or one-to-one communication.

The virtual meeting space, where people come together to collaborate in the Access Grid, is called a **Virtual Venue.** If authorized, the Venue provides users with all the necessary information needed to communicate with each other, including audio and video streams, user capabilities, data, services, applications, and connections to other venues.

Users connect to a Virtual Venue from their particular environment, identified as a **node**, which contains collaborative resources needed to provide high-quality user experiences. Access Grid users are given the ability to configure nodes according to their own preference. Examples of node configurations are a desktop using a Quick Camera or an entire room with several microphones,

cameras, and advanced display environments. Figure 1 shows one of several nodes available at Argonne National Laboratory.

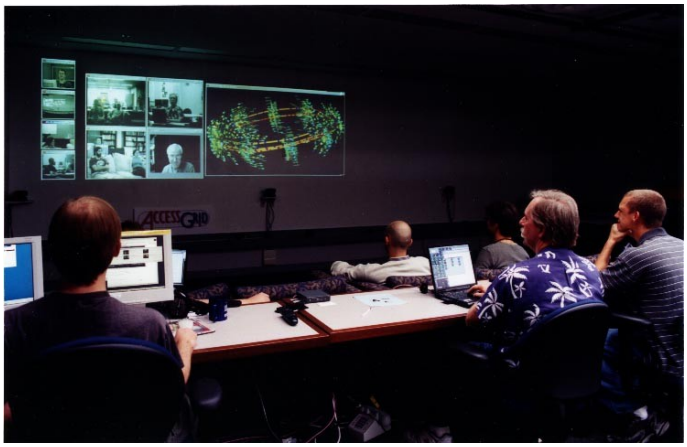

Figure 1 A Node at Argonne National Laboratory

2.0 Overview

The Venue Client, in Figure 2, is used to connect and participate in an Access Grid Virtual Venue. It displays the contents of the Virtual Venue, connections to other venues, and an interface to configure your node arrangement. The description below explains the different components that represent the Venue Client.

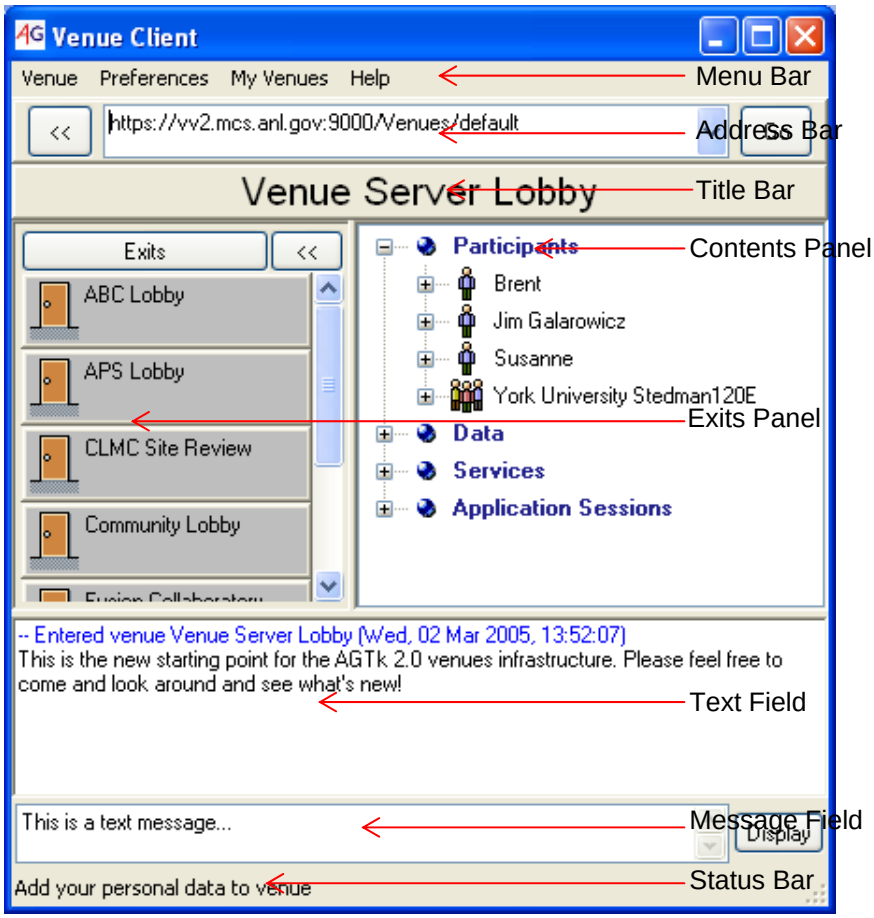

Figure 2 Venue Client

The **Address Bar** is used to connect to a venue. You are allowed to enter two different types of addresses in the address bar, either the default venue on a venue server (https://host:port/Venues/default) or the actual address of a specific venue (https://host:port/Venues/unique id). For instance, in Figure 2 you can see the Venue Client connected to default venue on a venue server running on host "vv2.mcs.anl.gov" using port 9000. After writing the address in the address bar, click the "Go" button to connect to the venue.

The **Title Bar** includes the name of the venue you are currently connected to.

The **Contents Panel** displays participants of the venue, present data, applications, and services available to share. Users can join the venue either as a single participant or as a node. A node is a group of people taking part in the venue together in which all of the participants are sharing the same collaborative capabilities, for example, watching the venue projected on a white screen with cameras placed strategically around the room.

The **Exits Panel** shows other venues linked to this venue, connected through exits, enabling users to travel through the venue space. Next to the door icon you

can see the name of the connected venue. The venue description is displayed as a tool tip that shows up if the mouse is held over the exit.

All venue participants and nodes will receive the text available in the **Text Field**. You can write a short message in the **Message Field** and display the text by clicking on the “Display” button.

3.0 Actions

This section describes how to use the Venue Client. The discussion begins with basics such as setting up certificates and gradually covers more complex issues as managing a node.

3.1 Requesting a Certificate

To connect to a venue, you must have a valid certificate (for more information about certificates, see Section 4.1). **You have to request and configure your certificate only once**; the same certificate can then be used for all future Access Grid interactions. Also, you are allowed to use the same certificate on several machines; hence, if you already have a certificate, you can simply export your certificate files over to the other machines.

1. ***Open the Certificate Request Wizard***. From the Access Grid Toolkit 2.3 Start menu, select **Request a Certificate**.

2. Click **Next >** in the first page of the wizard; see Figure 3.

Figure 3 Certificate Request Wizard; Step 1

3. ***Select Certificate Type.*** There are three kinds of certificates, as shown in Figure 4. The most common one is the *Identity Certificate,* which should be used by every person connected to the Access Grid. It identifies you as an individual and makes sure you are who you say you are. The instructions given in following steps are for Identity Certificate requests. If you instead want to run a service, for example a Venue Server, you can use a *Service Certificate*. The advantage of the Service Certificate is that it is unique for a service and users do not have to enter a password every time they wish to start the service. The third type of certificate is the *Anonymous Certificate*. It will allow you instant access to enter a venue without any approval from a Certificate Authority. However, certain venues may not allow anonymous admission because of security concerns. The Access Grid team recommends using an Anonymous Certificate only when really required, for example if your old certificate expired and you do not have time to wait for a new Identity Certificate to be approved.

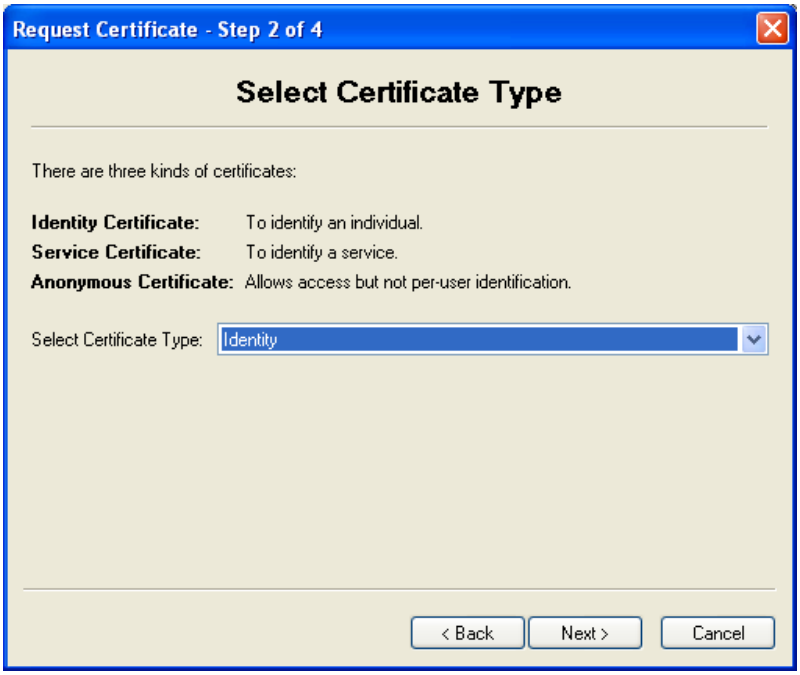

Figure 4 Certificate Request Wizard; Step 2

4. ***Enter Your Information***. After you select an Identity Certificate option from the drop down menu, the third wizard page (Figure 5) will appear. The page will prompt you for necessary information to create your identity certificate and the “distinguished name” you will be associated with (for more information about distinguished names read Section 4.2). Take care to remember the password you select because you will be using this in the future. Also, certificate requests with incorrect first and last names will not be approved.

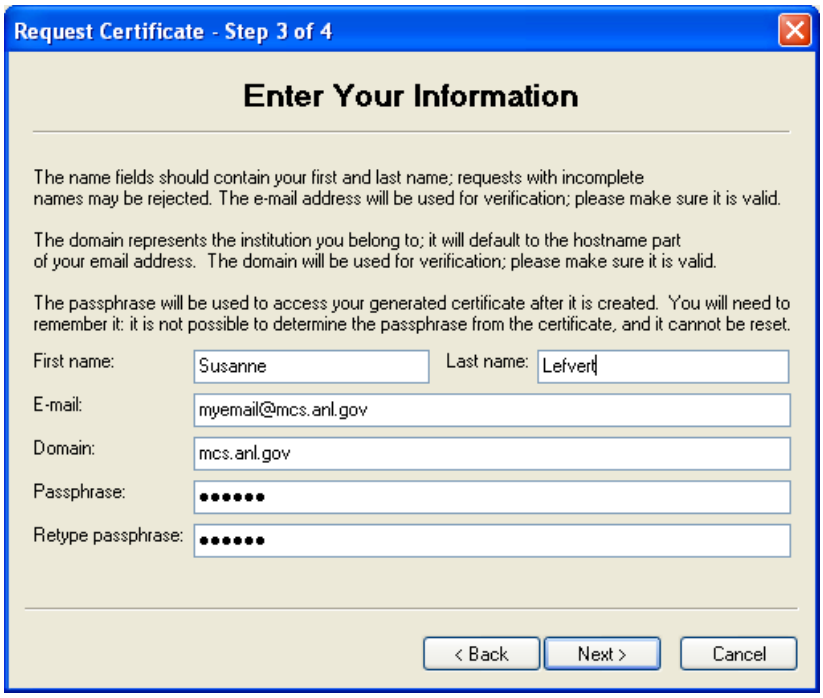

Figure 5 Certificate Request Wizard; Step 3

5. ***Review.*** Review the information that will be included in your certificate and click **Finish** to submit the request; see Figure 6. The certificate will be approved manually. This process may take some time depending on how many requests are being processed at the moment; please be patient. When your request has been approved, you will receive an e-mail containing instructions on how to install your certificate. For further questions regarding certificates, send an e-mail to agdev-ca@mcs.anl.gov.

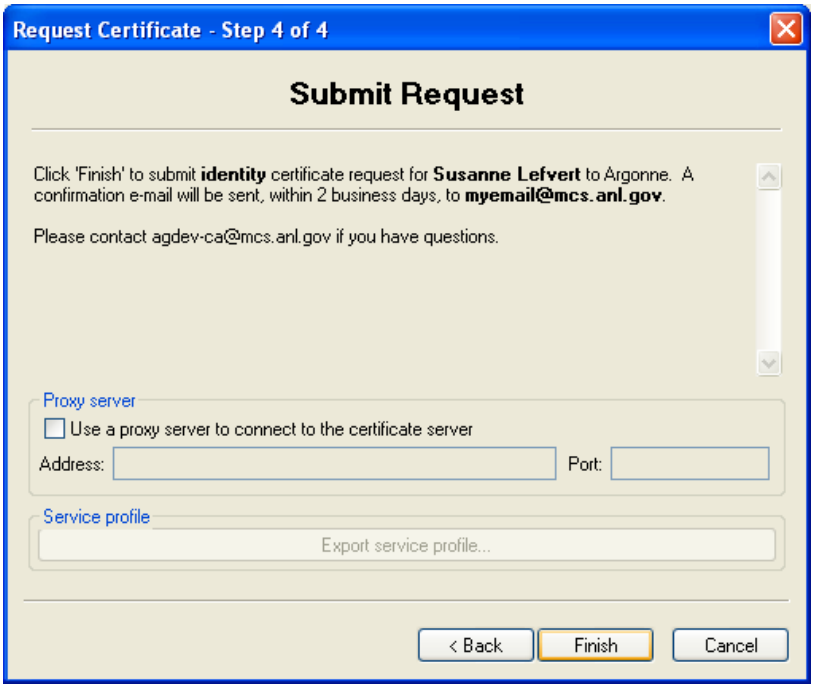

Figure 6 Certificate Request Wizard; Step 4

6. ***Install Certificate.*** To install the certificate, open the Venue Client and go to **Preferences – Manage Certificates – Certificate Manager…**. In the **Certificate Requests** tab, you will see a list of requested certificates and their current status. Click the **Check status** button to view the current status of your requests. If the status is **Ready to Install**, select the certificate from the list and click the **Install Certificate** button. The certificate is now installed, and you are ready to use it with your Venue Client.

3.2 Starting a Venue Client

If this is the first time you are using the Venue Client, a profile dialog will appear, and you should enter your information, which will be used to represent you in venues (see Figure 6). You are required to fill in at least your name and email address, but it is helpful if you enter as much information as possible. Keep in mind that you can change the profile at any time (see “Changing your Profile,” Section 3.5). When you are present in a venue, your profile information will be made available for every participant in that venue (read “Viewing a Profile,” Section 3.4)

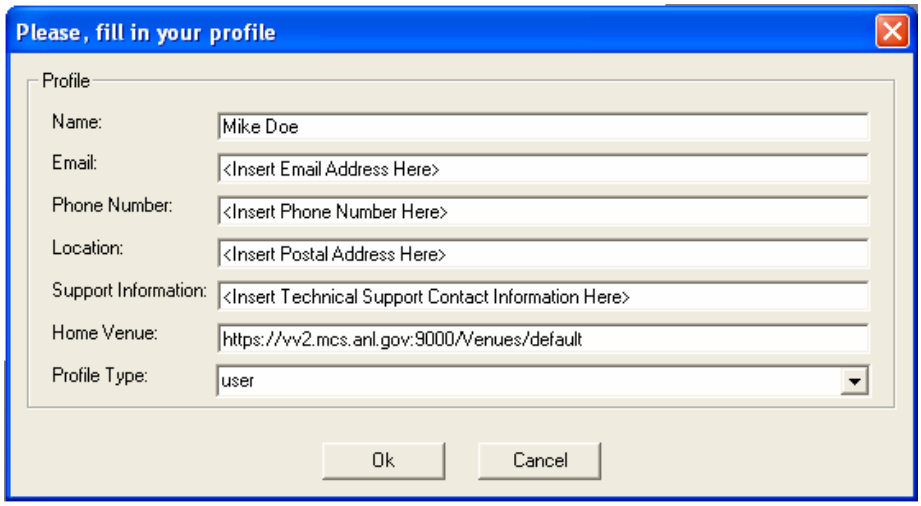

Figure 7 Profile Dialog

Notes:
Location: Your physical location, for instance, Argonne National Laboratory.
Support Information: Information on how to contact the responsible person for this node, for example, support@mcs.anl.gov.
Home Venue: The address that will show up in the Address Bar when you start the Venue Client.
Profile Type: One of two types: (1) user – a single participant connected via laptop or desktop machine, or (2) node –a group of people using the same collaborative environment

3.3 Connecting to a Venue

We discuss here the requirements for connecting successfully to a venue.

3.3.1 Specifying Venue Address

Enter the venue address in the **Address Bar**, and then click **Go** to enter the venue. Apart from venue addresses (https://<host>:<port>/<unique id>) you can enter the address of the default venue on a venue server (https://<host>:<port>/Venues/default), as shown in Figure 8.

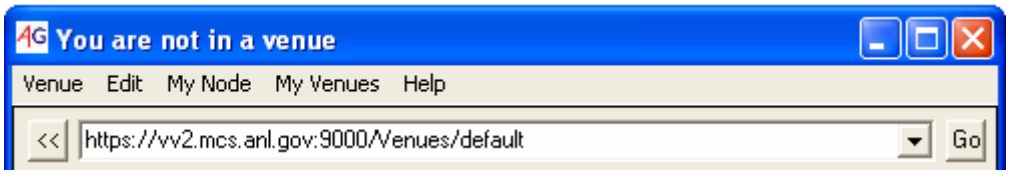

Figure 8 Using the Address Bar to Connect to a Venue

3.3.2 Creating a Grid Proxy Certificate

To successfully connect to the venue server, you have to have a valid grid proxy certificate (for more information, read Section 4.1). If such a certificate is missing,

the dialog (see Figure 9) will enable you to create a proxy. Fill in the password you chose when you initially requested your certificate in the **Pass phrase** field. You can set details of this grid proxy by clicking the **Proxy Details…** button. The "Proxy lifetime (hours)" field indicates how long this proxy certificate will be valid; the default value is 8 hours, but you may change this number. When the proxy life time expires, you will be prompted for your password again. After specifying the validity of the proxy, click **OK**.

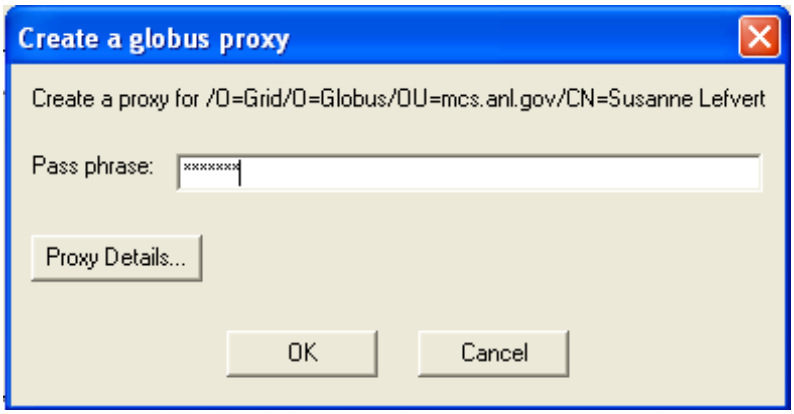

Figure 9 Creating a Grid Proxy

3.4 Viewing a Profile

Right click on the participant or node you want to see profile information about, and select **View Profile…**, as shown in Figure 10.

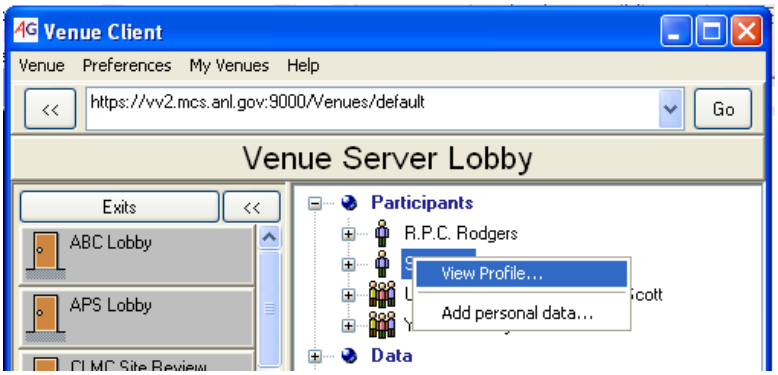

Figure 10 View Profile

3.5 Changing Your Profile

From the menu, choose **Preferences - Edit Profile…** as shown in Figure 11. When the Profile Dialog appears, edit the appropriate fields, and then click **OK**.

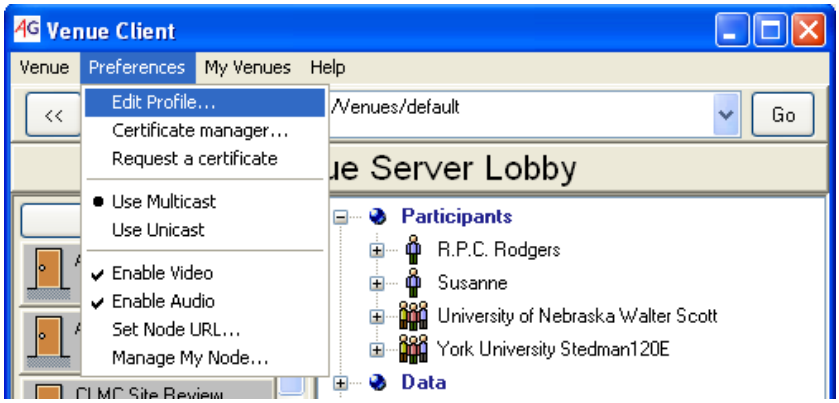

Figure 11 Edit your Profile from the Menu

3.6 Writing Text Messages

Enter text in the **Message Field**, and click **Display**. The text will show up in the **Text Field** for all participants in the venue; see Figure 12.

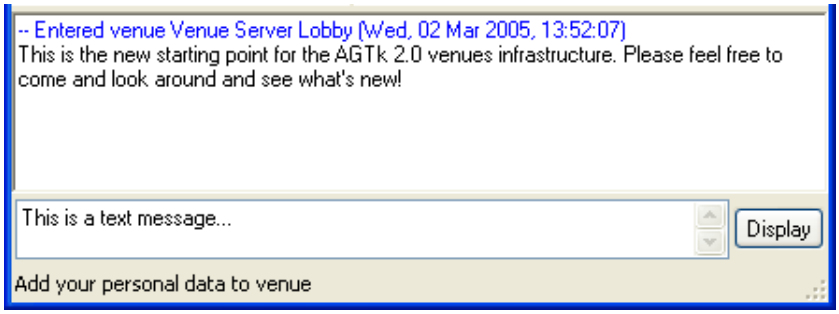

Figure 12 Text Chat

3.7 Saving Text Messages

To save text that has been posted in the **Text Field,** go to the **Venue** menu and select **Save Text**. In the dialog, enter the file location where you want to save the text and click **OK**.

3.8 Viewing Venue Properties

Currently, the only properties listed when selecting **Venue – Properties** from the menu are available streams. The dialog in Figure 13 displays multicast addresses and ports used for audio and video streams in the venue; it also shows whether the multicast address is statically or dynamically allocated.

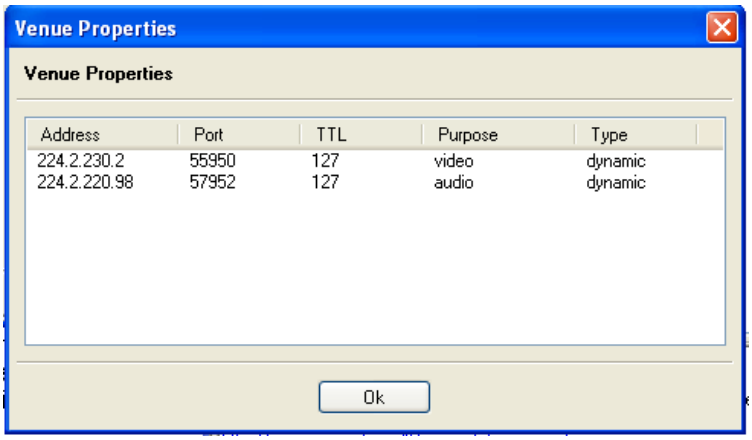

Figure 13 Venue Properties

3.9 My Venues

The **My Venues** menu option helps you to save and get easy access to Venues you are visiting often. You can set and go to your home venue and you can also add a list of venue names that, when clicked on, connects to associated venue. This functionality is available to avoid having to remember and type long addresses for venues you are visiting frequently, much like the "bookmark" feature in most Web browsers.

3.9.1 Setting Your Home Venue

The address to your home venue will always appear in the **Address Bar** when you first start the Venue Client. You can change this setting by selecting **Set as Home Venue** from the **My Venues** menu; the venue you are currently connected to will then be your home venue. You can also change your home venue from your profile; see Changing your Profile in Section 3.5.

3.9.2 Going to Your Home Venue

To connect to your home venue, select **Go to Home Venue** from the **My Venues** menu.

3.9.3 Adding a Venue

First, go to the menu and click on **My Venues - Add Current Venue**. The dialog (see Figure 14) opens with the current venue's name filled in automatically. You can change the name to whatever you want and then click **OK**. The name will be added to the list found under the **My Venues** menu option. When you select a name in the list, the Venue Client will try to connect to the associated venue.

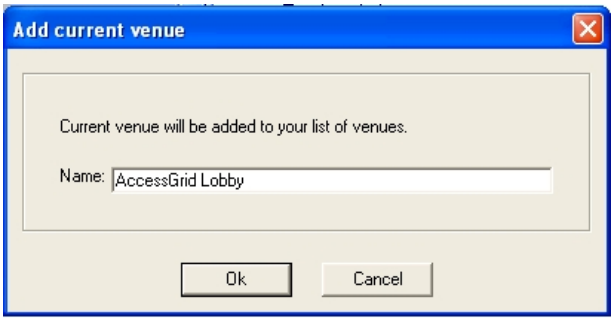

Figure 14 Associate a Venue Address with a Name

3.9.4 Removing a Venue

Go to **My Venues - Edit** in the menu bar, and right click the venue you want to delete. Select **Remove Venue,** and then press **OK**.

3.9.5 Renaming a Venue

Go to **My Venues - Edit** in the menu bar, and right click the venue you want to rename. Select **Rename,** fill in the new name, and then press **OK**.

3.10 Navigating

To the left side of the Venue Client is the Exits Panel, as shown in Figure 15, containing a list of names of other venues. If you place the mouse over one of the exits, the description of the venue shows up as a tool tip. If you click the left mouse button on one of the exits, you will leave the venue you are currently connected to and enter the other venue.

Figure 15 Navigating

3.11 Sharing Data

The Venue Client allows you to share data among users of the venue. Files can either belong to the venue or be user specific. A user may carry around personal data when walking between venues. Files belonging to a participant or node will therefore stay in the venue for as long as its owner is present. Venue data,

however, always stays in the venue until deleted. Personal user data is placed under the participant or node that owns the file, while venue data is found under the "Data" heading in the Contents Panel. **VenueClient.py**, in Figure 16, is one example of a personal file belonging to **Ivan's Office**, and **hello.txt** is owned by the venue.

Figure 16 Venue and Personal Data as Displayed in the Venue Client

3.11.1 Adding Venue Data

Right click on the **Data** heading, and choose **Add….** Or, from the menu, go to **Venue-Add Data….** A file browse dialog will show up from which you can pick the file you wish to add to the venue. Then press the **OK** button.

3.11.2 Adding Personal Data

Right click on your profile under the **Participant** heading, and choose the option **Add Personal Data**. A file browse dialog will show up from which you can pick the file you wish to add to your personal files. Click the **OK** button. Observe that personal data will be shown under your profile and not under the **Data** heading, illustrated in Figure 16.

3.11.3 Deleting Data

Right click on the data item, personal or venue specific, and choose **Delete**. A dialog will ask whether you really want to remove the selected data. Click **OK** to confirm.

3.11.4 Opening Data

Right click on the data item and choose **Open…**. If the file type is associated with an application, the data will be opened directly using that program. Otherwise you will be prompted for a program to associate with and handle the file.

3.11.5 Viewing Data Properties

Right click on the data item, and choose **Properties…**. A dialog will be opened showing the file name, the distinguished name of its owner, and file size.

3.12 Sharing Applications

A useful feature in the Access Grid is the ability to share applications among several participants. The software includes several applications that get installed along with the toolkit, such as the Shared Browser for viewing the Web together and the Shared Presentation for Powerpoint presentations. However, the Access Grid is not limited to preinstalled applications. Developers may create and plug in custom applications that can be made available for venue participants.

3.12.1 Starting a Session

Installed applications for your Venue Client are listed under **Start Application Session** in the **Venue** menu; see Figure 17. To start a session, select an application from the list. Give the session a name and a short description before adding it to the Venue. The newly created session is listed under the **Application Sessions** heading in the Venue Client.

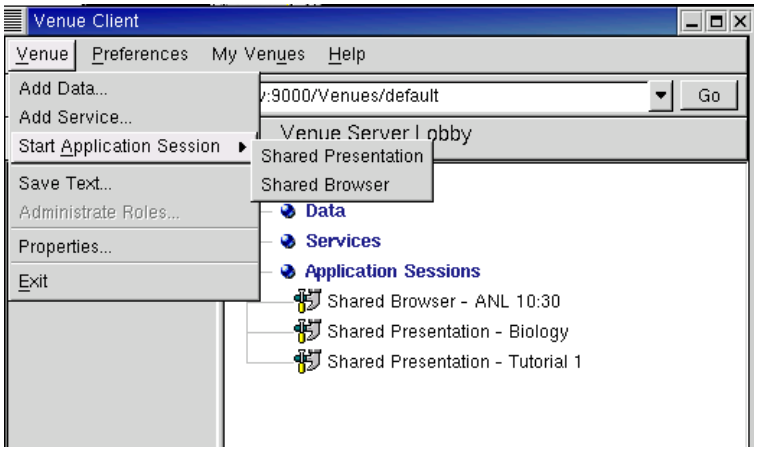

Figure 17 Shared Application Sessions

3.12.2 Joining a Session

To join an application session, right click the correct name under the **Application Sessions** heading and select **Open**, as shown in Figure 18. The appropriate application will then launch and display current session status.

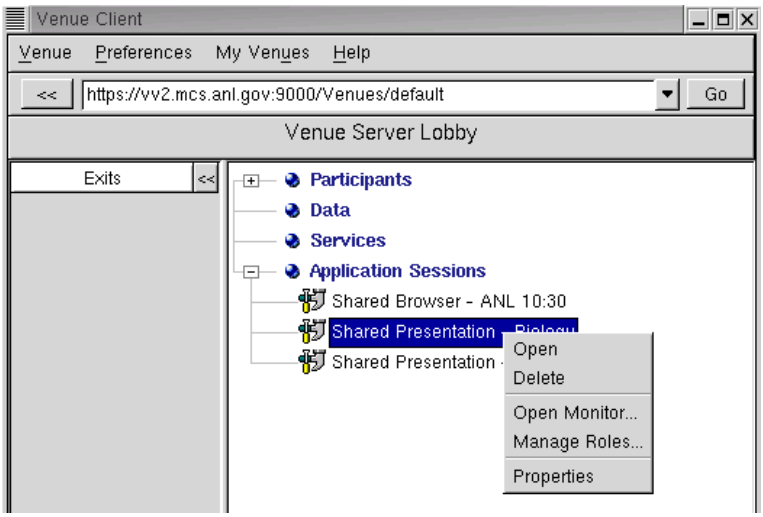

Figure 18 The Application Session Menu

3.12.3 Stopping a Session

To stop an application session, right click the correct name under the **Application Sessions** heading, and select **Delete**, as shown in Figure 18. A dialog will appear to check that you really want to delete the session. Click **OK** to confirm.

3.12.4 Authorization

Right click on the session you wish to authorize and select **Manage Roles…** A frame will display current authorization setting for this application session. The session has a set of **Roles** that identifies different authorization privileges for groups of participants. The authorization privileges are identified as **Actions**. When selecting a role from the left panel, you can see which actions are enabled for that role in the right action panel. When a role is being expanded, participants that are included in this role are shown. A participant may be added to several roles and is allowed to perform all actions for that set of roles. You may add/remove roles, add/remove participants to different roles, and add/remove actions to roles.

3.12.5 Opening a Monitor

If you want to determine those who are currently participating in an application session, you may right click the application session and select **Open Application Monitor…**. In addition to participants, the monitor displays events occurring in the session and data being exchanged among participants, as shown in Figure 19.

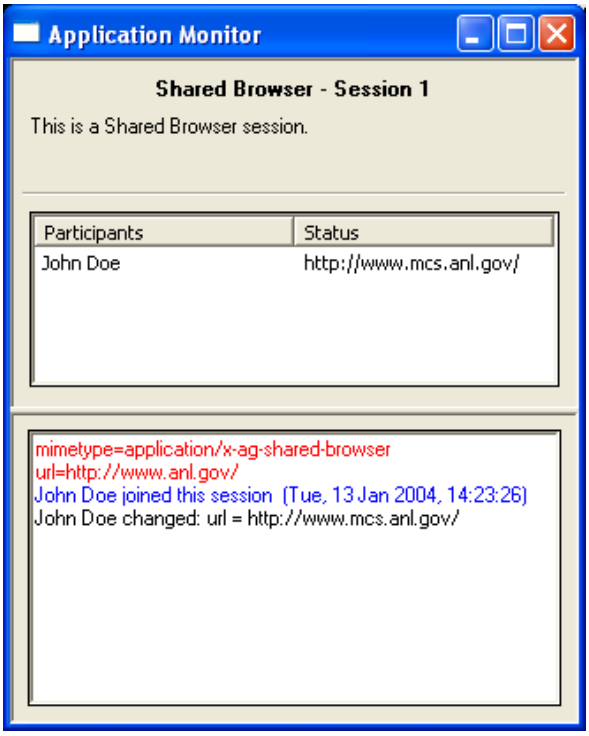

Figure 19 Application Monitor

3.12.6 Viewing Properties

To view session properties, right click on the application session and choose **Properties…**. A dialog will be opened showing the name, URL address, MIME type, and the description associate with the selected session.

3.13 Sharing Services

Services are often shared via the Access Grid. We describe here how you can add and delete such services.

3.13.1 Adding Service

Before adding a service to the venue, you need to know the address where the service is located and what MIME type to associate with the service. The MIME type helps the Venue Client to identify what type of service is being added and how to handle it. When you have gathered this information, right click on the **Service** heading and click **Add…**, or from the main menu choose **Venue-Add Service…**. In the dialog, enter name, URL address, MIME type, and the description you want to associate with the service. Then click **OK**. Figure 20 shows you an example of how to add a service that points to a Web Site.

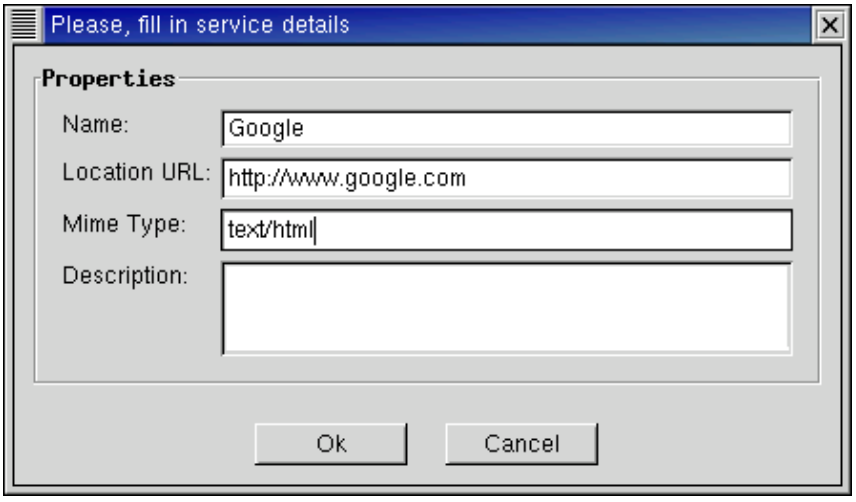

Figure 20 Add Service Dialog

3.13.2 Opening a Service

To open a service, right click on the service you wish to use, and select **Open**.

3.13.3 Deleting a Service

To delete a service, right click on the service you wish to remove, and select **Delete**. A dialog will appear to check that you really want to delete the service. Click **OK** to confirm.

3.13.4 Viewing Service Properties

To view service properties, right click on the service item and choose **Properties…**. A dialog will be opened showing the name, URL address, MIME type, and the description associate with the selected service.

3.14 Managing Certificates

Every user and service connected to the Access Grid must have a valid certificate issued by a trusted certificate authority. Certificates are a form of electronic identification that is superior to the well-known and widely used password strategy. This form of authentication aims to reduce the many problems seen with passwords, such as poorly chosen, forgotten, or insecurely stored passwords, in order to enable a reliable environment for collaboration. The certificate authority is responsible for giving you a certificate; thus make sure you really are who you say you are.

The most common certificate is the *Identity Certificate.* It is used to verify that a person is who he says he is when connected to the Access Grid. However, if you are going to run a venue server, or any kind of service, you should use a *Service Certificate.* The service certificate does not require a pass phrase and allows the server to stay up and running for longer periods of time.

3.14.1 Viewing Certificates

If you want to know which certificates you have installed, select **Preferences - Manage Certificates – Certificate Manager…** from the main menu. The **Certificates** tab (see Figure 21) shows all your certificates. If you want to see more details about a certificate, for instance validity, select it from the list and click the **View certificate** button to the right.

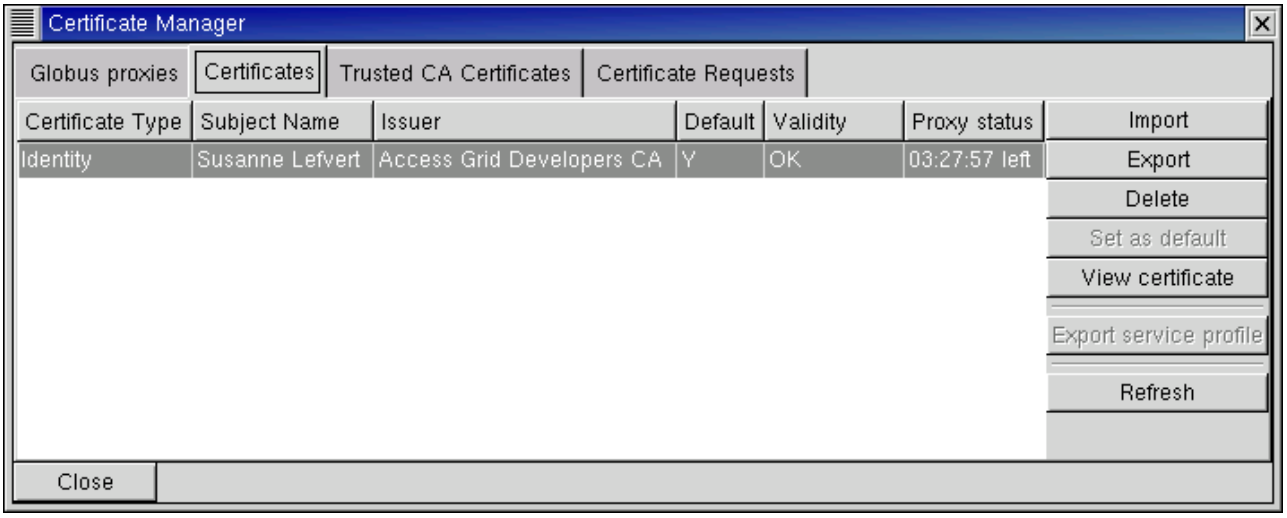

Figure 21 Certificate Manager – Certificates

3.14.2 Importing a Certificate

If you have a certificate you want to use with the Venue Client, you can import it from **Preferences – Manage Certificates – Certificate Manager…** menu. In the **Certificates** tab in Figure 21, click the **Import** button to the right. The file browse dialog that opens will let you specify location of the certificate file (usercert.pem) and the certificate key file (userkey.pem).

3.14.3 Exporting a Certificate

If you need to use your certificate on a different machine you can chose to export it to a file. In the main menu select **Preferences – Manage Certificates – Certificate Manager…**. Choose a certificate from the **Certificates** tab in Figure 21 and then click the **Export** button. Enter the name of the file you want your certificate to be saved to, and click **Export Certificate**.

3.14.4 Deleting a Certificate

From the main menu, select **Preferences – Manage Certificates – Certificate Manager…**. Choose a certificate from the **Certificates** tab in Figure 21 and then click the **Delete** button. A dialog will confirm that you really want to remove selected certificate; click **OK**.

3.14.5 Setting the Default Certificate

Your default certificate will automatically be used when you run the Venue Client and the pass phrase entered when creating a proxy have to be associated with that certificate. If you want to change default certificate, from the main menu select **Preferences – Manage Certificates – Certificate Manager…**. Choose a certificate from the **Certificates** tab (see Figure 21), and then click the **Set as default** button. You can determine which certificate is the default by looking at the **Validity** field in the header of the certificate list; it should be marked with a **Y**.

3.14.6 Viewing Proxies

To view proxies currently running, select **Preferences – Manage Certificates – Certificate Manager…** from the main menu. The **Globus proxies** tab (Figure 22) shows a list of proxies and their information, including the certificate authority that issued the certificate and how long the proxy is valid. If you want more details, select a proxy from the list, and click the **View proxy** button.

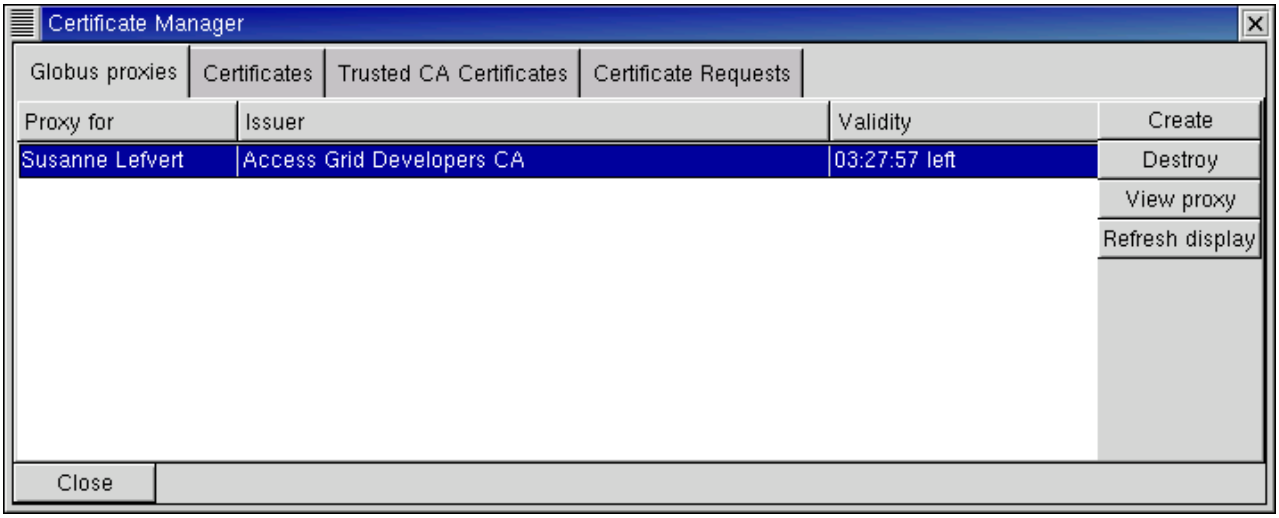

Figure 22 Certificate Manager – Proxies

3.14.7 Destroying a Proxy

Select **Preferences – Manage Certificates – Certificate Manager…** from the main menu. Choose a proxy from the list in the **Globus proxies** tab (see Figure 22) and click the **Destroy** button. A dialog will confirm that you really want to remove selected proxy; click **OK**.

3.14.8 Viewing Trusted CA Certificates

The certificates used by all participants in the venue are issued from a trusted certificate authority. To find out which certificates are accepted by your Venue Client, select from the main menu **Preferences - Manage Certificates - Certificate Manager…**. The **Trusted CA Certificates** tab lists acknowledged certificate authorities and their validity. To view more details about a certificate authority, select it from the list, and click the **View certificate** button.

3.15 Managing Your Node

A node consists of a node service, one or more service managers, and one or more services. An example of a node configuration, pictured in Figure 23, uses three machines: one for video creation, one for video display and one responsible for audio. The services, in this case, are used to produce and receive audio and video. Each machine runs a service manager communicating with services on that specific machine. The service managers are controlled by the node service, which can run on any machine. Default services used by the Venue Client are VIC for video and RAT for audio.

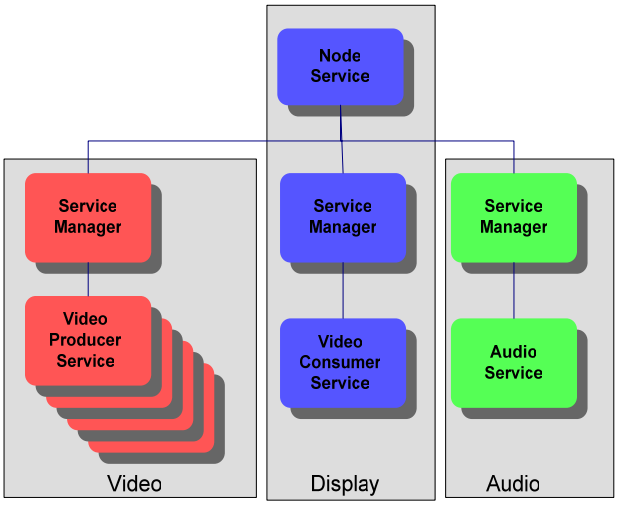

Figure 23 Example of an Access Grid Node Layout

3.15.1 Starting a Service Manager

If you want to start a service manager, run AGServiceManager.py.

3.15.2 Starting a Node Service

If you want to start a node service, run "AGServiceManager.py –n"; note that this will start the NodeService and a ServiceManager in the same process.

3.15.3 Opening a Node Management Window

The Venue Client allows you to set up and configure the resources available in your node layout. Go to the main menu and click on **Manage My Node…**; the Node Management Window will open. To the left side of the window you can see a list of Service Managers. A Service Manager is responsible for managing different services present in your specific node. In Figure 24, the Service Manager is running on zuz.mcs.anl.gov using port 11000. To the right side of the Node Management window, you can see a list of services corresponding to the selected item in the Service Manager list. The selected Service Manager is controlling one audio service responsible for sending and receiving voice communication.

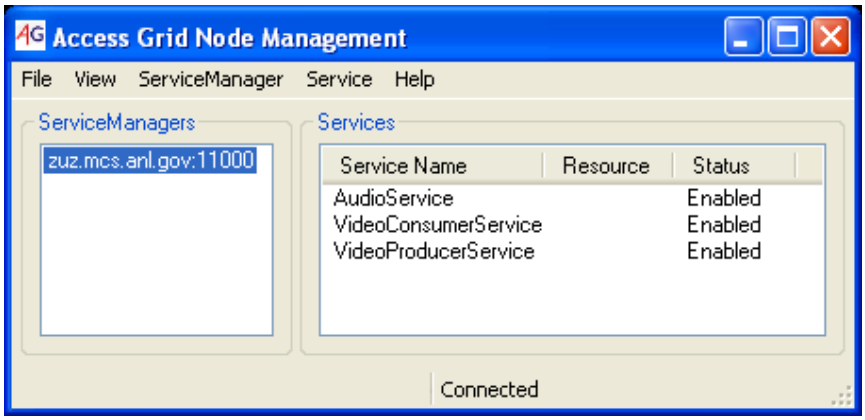

Figure 24 Node Management

3.15.4 Adding a Service Manager

If you want to add a new Service Manager, go to the main menu and select **ServiceManager - Add…**, or right click on the Service Manager and select **Add…**. Enter the computer in which the service manager is running and the port it is using. When you are finished, click **OK**. If the service manager is located on your local computer, it is sufficient to enter localhost as **Hostname**; see Figure 25.

Figure 25 Add Service Manager

3.15.5 Removing a Service Manager

Select the Service Manager to remove; then click **ServiceManager - Remove** in the main menu, or right click the Service Manager and select **Remove**. The Service Manager should disappear from the list.

3.15.6 Adding a Service

Select the Service Manager you wish to add a service to, select from the menu **Service-Add…** or right click on a Service Manager and click **Add…**. A window containing a list of all available services will be displayed. Select the service to add; then click **Ok**. In Figure 26 you can see three existing services to use for voice and video communication available for Service Manager zuz.mcs.anl.gov:11000.

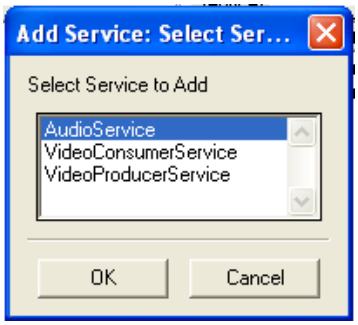

Figure 26 Add Service

3.15.7 Enabling or Disabling a Service

Select the service you wish to start or stop from the list of services. Go to the main menu and select **Services – Enable** or **Services-Disable**, or right click on the service and select **Enable** or **Disable**. You should now see the status field for the service you selected change accordingly in the list.

3.15.8 Removing a Service

Select the service you wish to delete from the list of services; choose from the main menu **Service – Remove,** or right click the service and select **Remove**.

3.15.9 Changing Service Configuration

Select the service you want to change, and choose from the main menu **Service - Configure…**.

3.15.10 Attaching to a Node

You can connect to a node service running on any machine by selecting from the main menu **File-Attach to Node**. Give the host and port information where the node service is running.

3.15.11 Loading a Configuration

An existing Service Manager configuration can be loaded with all services added automatically. From the main menu select **File-Load Configuration…**, and select the desired configuration from the list of names. Then click **OK**.

3.15.12 Saving a Configuration

If you know you will use your Service Manager configuration several times, it is a good idea to store the configuration. You can then simply load the configuration when you want to use it, instead of adding the same services all over again. In the main menu, go to **File-Save Configuration…**, specify the name you want the configuration to be associated with, and then click **OK**.

3.15.13 Using Unicast

If you are having problems with multicast on you network, you can use unicast until the problem is fixed. This will allow you to run the media tools even though you are not multicast enabled. From the **Preferences** Menu, in the Venue Client, select **Use Unicast**. Please note that not all venues are connected to a bridge server and will therefore not be able to provide the unicast option.

3.15.14 Enabling Video

The Venue Client provides a way to quickly turn your video on and off. Go to the **Preferences** menu and select **Enable/Disable Video**. If video is turned off, you will not send or receive any video.

3.15.15 Enabling Audio

The Venue Client provides a way to quickly turn your audio on and off. Go to the **Preferences** menu and select **Enable/Disable Audio**. If audio is turned off, you will not send or receive any audio.

3.16 Authorization

Access Grid venues have a role-based security to establish an authorization policy, determining which participants to let in and with what authority. Administrators can decide who are allowed to perform different actions, such as entering the venue and adding data.

To open the authorization frame, go to the **Venue** menu and select **Manage Roles…**. The frame in Figure 27 displays the current authorization setting for the venue. The venue has a set of **Roles** that identify different authorization privileges, or **Actions,** for groups of participants. When selecting a role from the left panel, you can see which actions are enabled for that role in the right action panel. When expanding a role, participants included in the role are shown. A participant may be added to several roles and can perform all actions for that set of roles. You may add/remove roles, add/remove participants to different roles, and add/remove actions to roles.

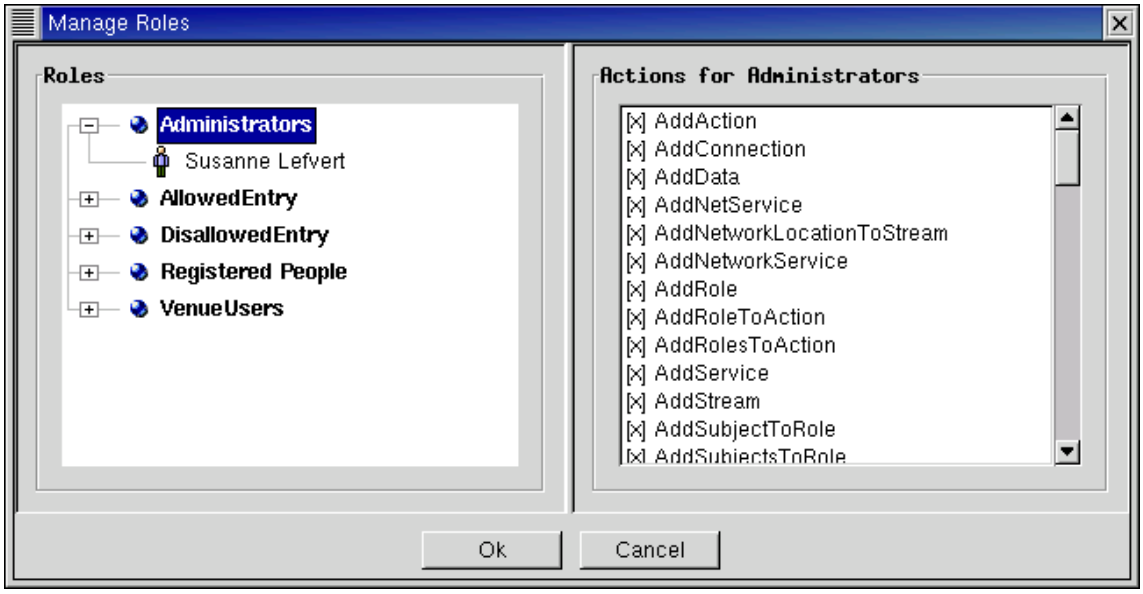

Figure 27 Authorization

3.17 Submitting an Error Report

To improve the quality of the Access Grid software, users are encouraged to submit bug reports when experiencing problems. Also, feature requests and improvements are welcome and can be submitted in the same fashion.

3.17.1 Bugzilla

Ideally, bug reports are entered manually at the Bugzilla Web site (http://bugzilla.mcs.anl.gov/). To do so, you need to set up an account with a valid e-mail address. The Access Grid development team will then process the bug at their earliest convenience, and comments will get sent to the reporter. This is the recommended way to file bugs because they get organized into categories and reporters will receive feedback and may submit additional information regarding the bug.

3.17.2 Automatic Bug Reports

If you do not have time to register with Bugzilla, you can file automatic bug reports using the Venue Client. In the **Help** menu select **Submit Error Report of Feature Request**. Though not necessary, you may enter an e-mail address where we can reach you if you are interested in providing more information regarding the problem. The bugs will be submitted to the Bugzilla system; however, the reporter will not receive updates, entered in Bugzilla, about the bug.

4.0 About Certificates

Every user and service in the Access Grid is required to have a valid identity certificate issued by a trusted certificate authority. Certificates are a form of electronic identification that is superior to the well-known and widely used

password strategy. This form of authentication aims to reduce the many problems seen with passwords, such as poorly chosen, forgotten, or insecurely stored passwords, in order to enable a reliable environment for collaboration. The certificate authority is responsible for giving you a certificate; , make sure you really are who you say you are.

4.1 Why Use Certificates?

A certificate is basically used to assure your security when connected to the Access Grid. The following are examples of security provided in the certificate mechanism:

1. Deal with authentication during log in procedures to identify who you are.
2. Authorize what resources people are allowed and have permission to access.
3. Preserve confidentiality by showing just the given individuals' resources and information they are supposed to see, secure transactions, and so forth.
4. Take care of users' integrity; for example, back up resources when something unexpected happens.

For more information about security through certificates, read http://www.globus.org/security/.

4.2 Distinguished Name

A distinguished name (DN) is a globally unique identifier that represents the user as an individual. In the Access Grid, DNs are constructed from entity name and domain information. The following is an example of a distinguished name: "/O=Grid/O=Globus/OU=mcs.anl.gov/CN=John Doe." On Windows you can find your distinguished name in the usercert.pem file, created when you requested your certificate, found in C:\Documents and Settings\<your user name>\Application Data\globus\usercert.pem. Linux users can run grid-cert-info –subject.

4.3 Grid Proxy

You are not actually using your certificate for authentication. Rather, you have to create a grid proxy certificate, which is used for authentication without requiring you to enter your pass phrase. Once you have initiated the proxy with your password, you will not have to enter it again until the proxy is invalid. However, longer validity means less security.