

Argonne National Laboratory  
9700 South Cass Avenue  
Argonne, IL 60439

---

ANL/MCS-TM-287

---

**Virtual Venue Management Users Manual:**  
Access Grid Toolkit Documentation, Version 2.3

by

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

Mathematics and Computer Science Division

Technical Memorandum No. 287

February 2006

Funding for this work has been provided by the US 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](http://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](mailto:reports@adonis.osti.gov)

## **Disclaimer**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor UChicago Argonne, LLC, nor any of their employees or officers, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of document authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof, Argonne National Laboratory, or UChicago Argonne, LLC.

# Contents

Abstract .....	1
1.0 Introduction .....	1
2.0 Venue Management .....	2
3. 0 Actions .....	5
3.1 Using Venue Management .....	5
3.1.1 Setting Up a Certificate .....	5
3.1.2 Creating a Grid Proxy .....	9
3.2 Starting a Venue Server .....	10
3.3 Connecting to a Venue Server .....	10
3.4 Adding a Venue .....	10
3.4.1 General .....	11
3.4.2 Encryption .....	12
3.4.3 Addressing .....	12
3.5 Modifying the Venue .....	13
3.6 Removing a Venue .....	14
3.7 Changing the Server Multicast Range .....	14
3.8 Changing Server Encryption Settings .....	14
3.9 Setting Server Authorization .....	15
4.0 About Certificates .....	15
4.1 Purpose of Certificates .....	15
4.2 Distinguished Name .....	16
4.3 Grid Proxy .....	16

# Virtual Venue Management Users Manual

Access Grid Toolkit Documentation

Version 2.3

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

## Abstract

An Access Grid Venue Server provides access to individual Virtual Venues, virtual spaces where users can collaborate using the Access Grid Venue Client software. This manual describes the Venue Server component of the Access Grid Toolkit, version 2.3. Covered here are the basic operations of starting a venue server, modifying its configuration, and modifying the configuration of the individual venues.

## 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. 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, however, 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.

The image in Figure 1 shows one of several nodes available at Argonne National Laboratory.

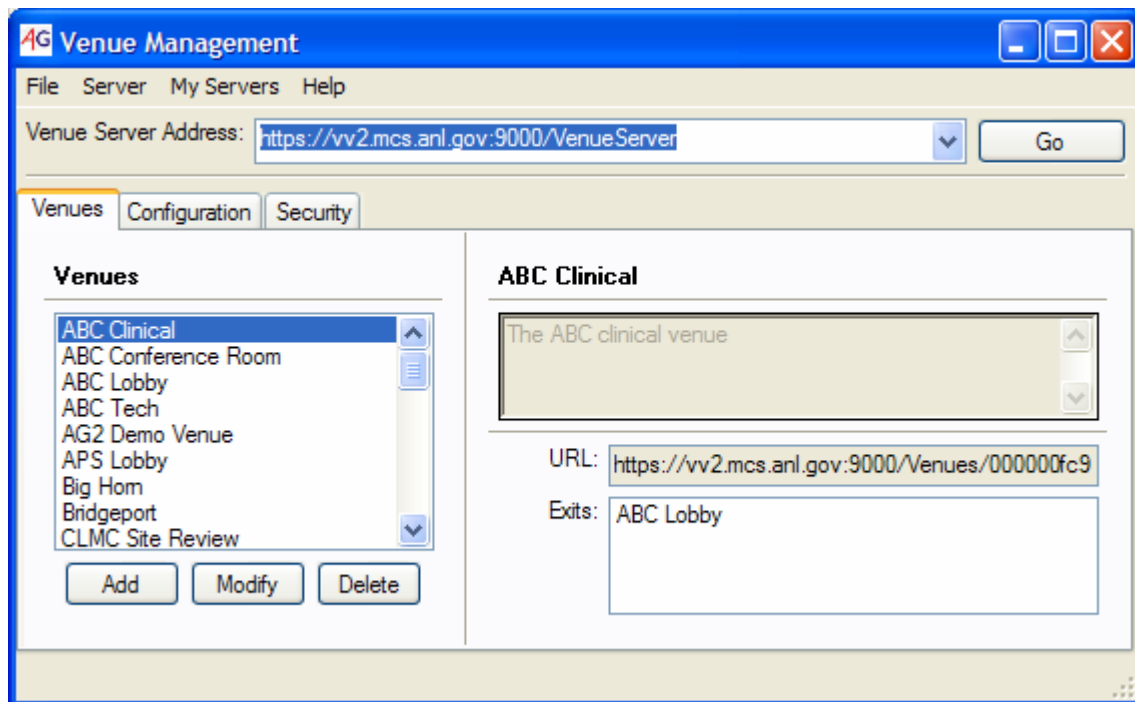


**Figure 1** A node at Argonne National Laboratory

## 2.0 Venue Management

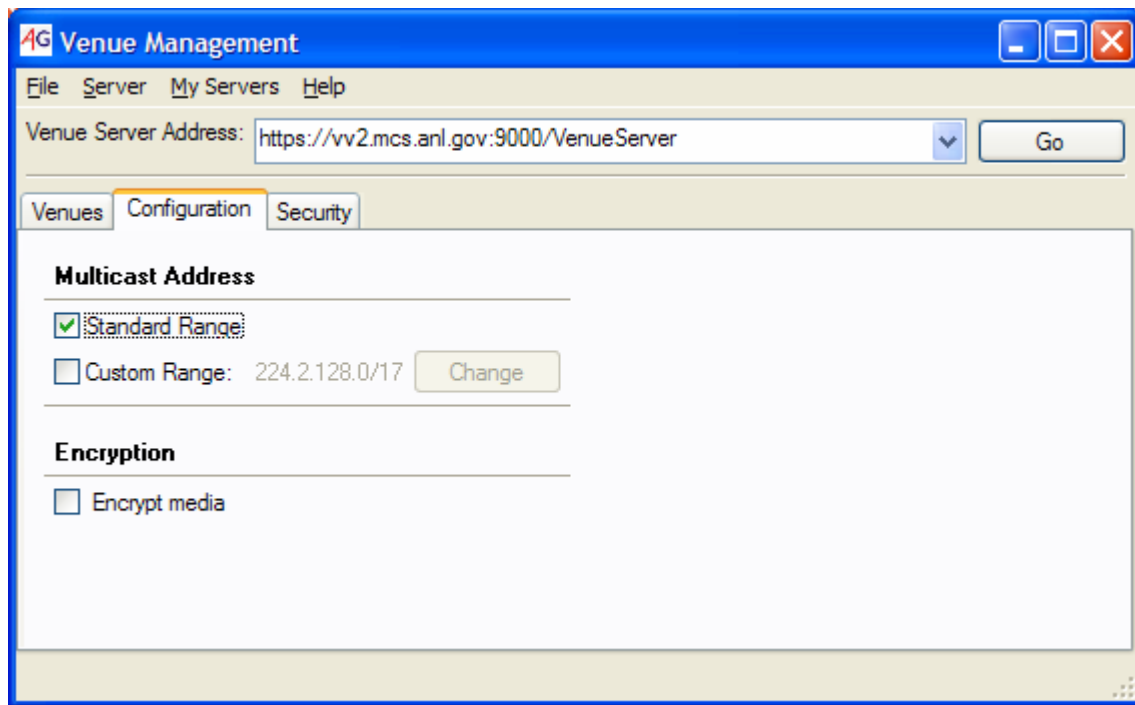
This manual focuses on management of the Virtual Venue. Venue Management is an administrative tool used to create and maintain venues located on a server. It includes information about present venues on the server, server administrators, and the type of encryption used for media communication.

Figure 2 shows the Venue Management client connected to a venue server at <https://vv2.mcs.anl.gov:9000/VenueServer>. The **Venues** tab displays a list of venues currently up and running, with the selected venue's information displayed to the right. The buttons **Add**, **Modify**, and **Delete** seen under the list can be used to add a new venue or to modify or delete the selected venue from the list.



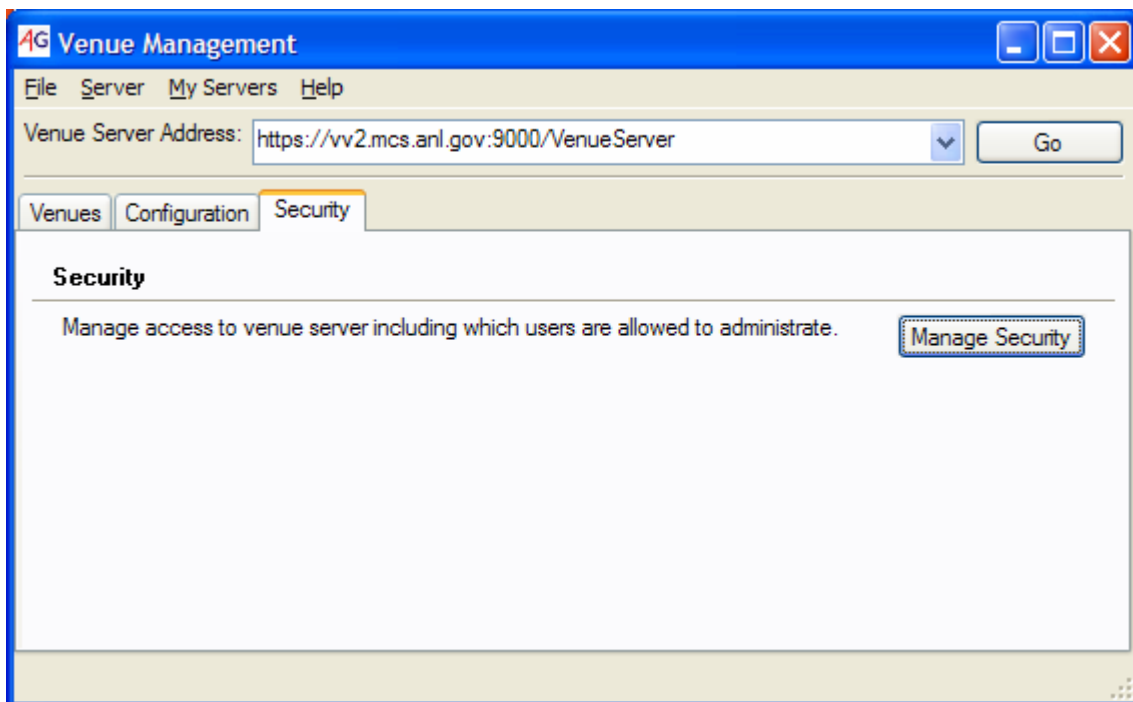
**Figure 2** Venue Management, with the **Venues** tab selected

The second tab, shown in Figure 3, includes details about the server configuration. Multicast addresses are by default assigned from a standard range but can be customized in the **Multicast Address** box to fulfill users' needs. If the **Encrypt Media** option is set, new venues will, by default, use encrypted media streams. However, each venue has the option to change the encryption setting.



**Figure 3** Venue Management, with the **Configuration** tab selected

The **Security** Tab in Figure 4 allows you to change the authorization setting for the venue server. This is described in more detail below.



**Figure 4** Venue Management, with the **Security** tab selected

### 3.0 Actions

This section describes various actions the user can take to start using Venue Management. It also provides information on how to add, modify, or remove a venue or a venue server administrator and how to set the venue server configuration.

### 3.1 Using Venue Management

In this section we discuss how to select and set up a certificate and how to create a Grid proxy.

#### 3.1.1 Setting Up a Certificate

To connect to a venue server, you need a valid Grid identity 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 to the other machines.

1. **Start Venue Management.** The Venue Management software provides a mechanism for requesting certificates to use with the Access Grid. When starting Venue Management, the Certificate Request Wizard will open automatically if you do not have certificates already installed.
2. Click **Next >** in the first page of the wizard, shown in Figure 5.





**Figure 5** Certificate Request Wizard; Step 1

3. ***Enter your Information.*** The second wizard page, in Figure 6, will appear prompting you to choose the type of certificate you want to request; the choices are Identity, Service, and Anonymous. Most users will want to request an identity certificate. Service certificates are used for running venue servers, bridge servers, and so forth. Anonymous certificates do not identify the user and are passwordless.

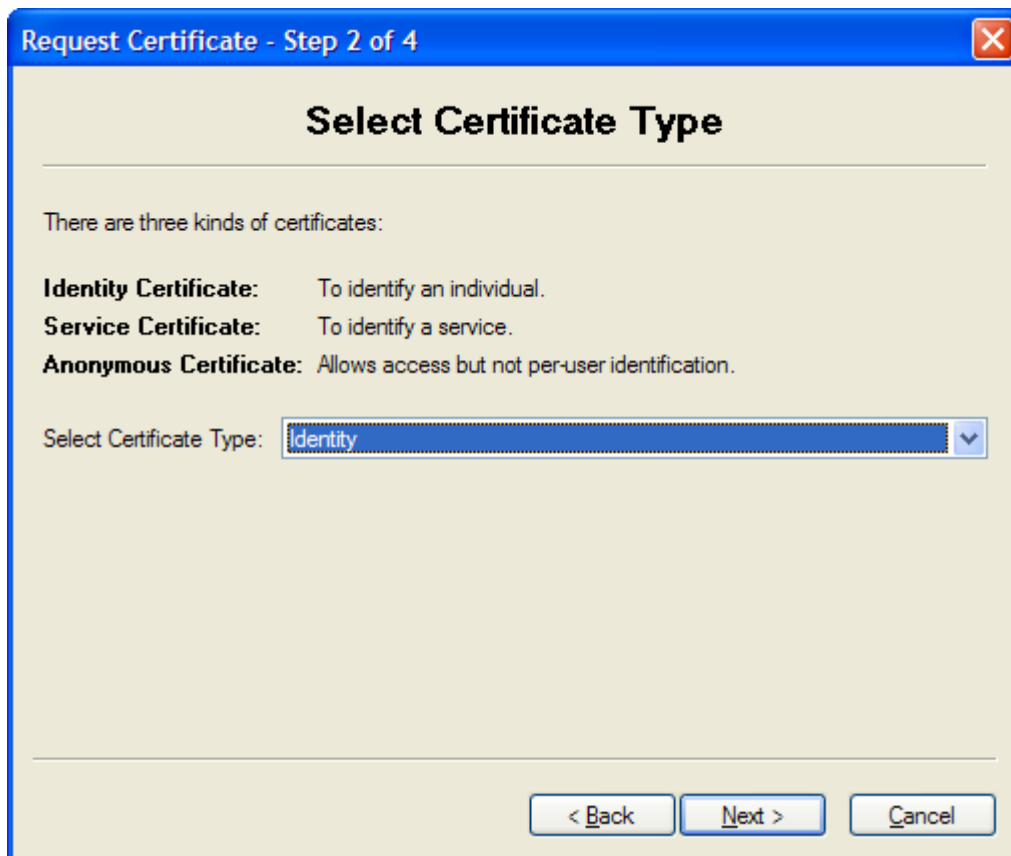


Figure 6 Certificate Request Wizard; Step 2

4. **Enter your Information.** The third wizard page, in Figure 7, will appear prompting you for necessary information to create your certificate and the distinguished name you will be associated with (for more information about distinguished names read Section 4.3). 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.

**Request Certificate - Step 3 of 4**

### Enter Your Information

The name fields should contain your first and last name; requests with incomplete names may be rejected. The e-mail address will be used for verification; please make sure it is valid.

The domain represents the institution you belong to; it will default to the hostname part of your email address. The domain will be used for verification; please make sure it is valid.

The passphrase will be used to access your generated certificate after it is created. You will need to remember it: it is not possible to determine the passphrase from the certificate, and it cannot be reset.

First name:  Last name:

E-mail:

Domain:

Passphrase:

Retype passphrase:

< Back   Next >   Cancel

**Figure 7** Certificate Request Wizard; Step 3

5. **Review.** Review the information that will be included in your certificate, and click **Finish** to submit the request (Figure 8). Identity and Service certificates will be approved manually; Anonymous certificates are approved automatically. Manual approval 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 questions regarding certificates, send e-mail to [ag-mcs@mcs.anl.gov](mailto:ag-mcs@mcs.anl.gov).

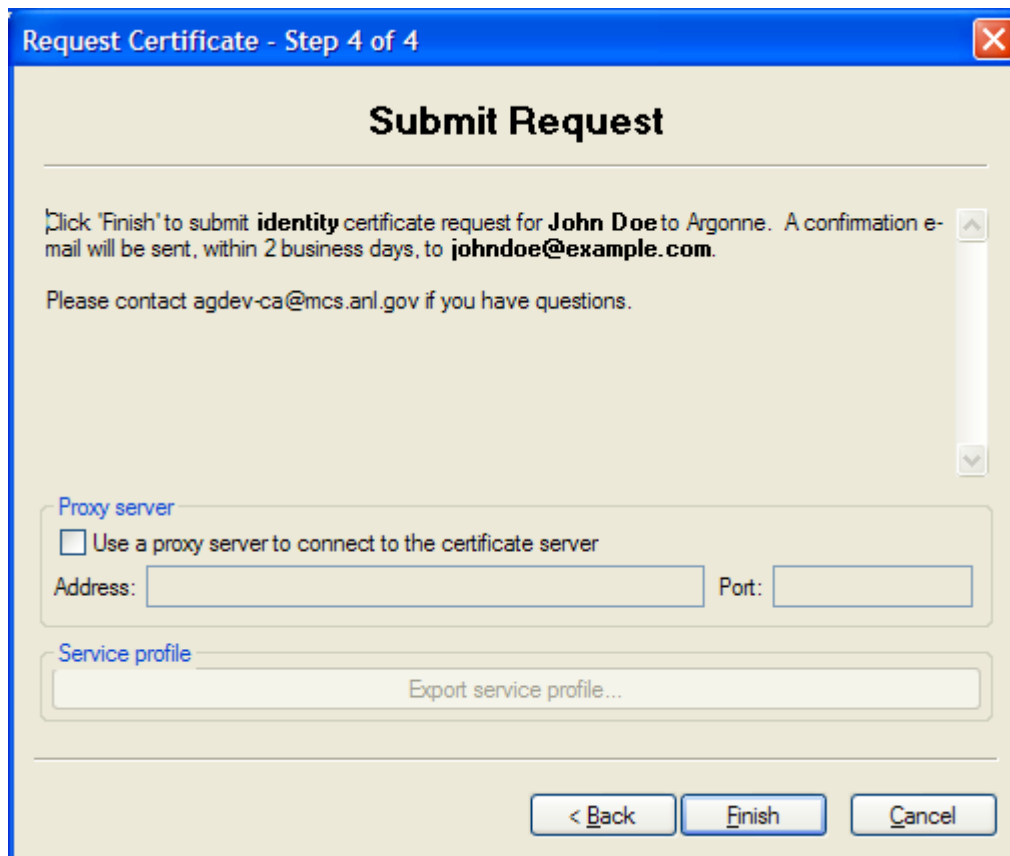
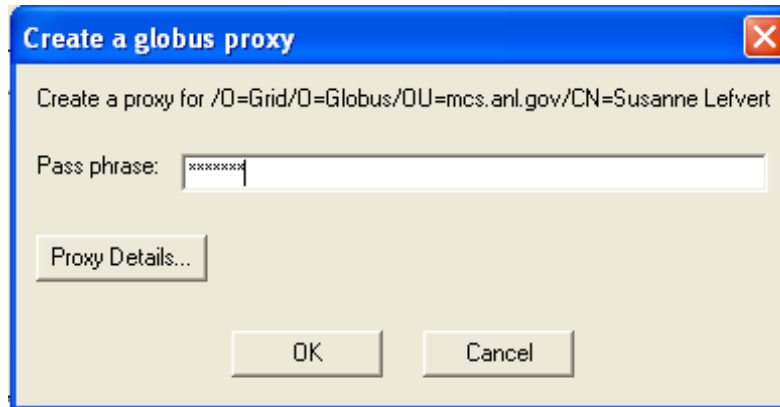


Figure 8 Certificate Request Wizard; Step 4

6. **Install the 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 get 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.

### 3.1.2 Creating a Grid Proxy

To successfully connect to the venue server, you need a valid Grid proxy certificate (for more information, read Section 3.1). If such a certificate is missing, the dialog (see Figure 9) will enable you to create a proxy. In the **Passphrase** field, fill in the password you chose when you initially requested your certificate. 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

## 3.2 Starting a Venue Server

For Windows users:

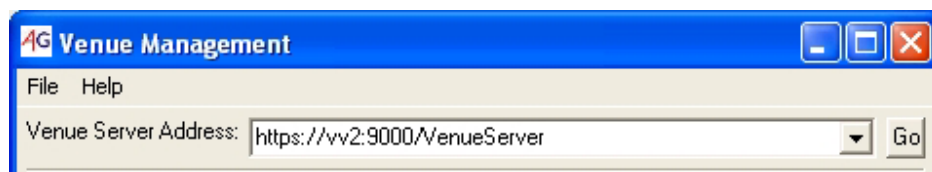
Go to the Start menu, and select **All Programs - Access Grid Toolkit - Services - Venue Server**. The default server URL address is <https://localhost:8000/VenueServer>. If your proxy has expired, you will be prompted for your password.

For Linux users:

Run VenueServer.py on the command line; use the `--help` flag to list available options. If your proxy has expired, you will be prompted for your password.

## 3.3 Connecting to a Venue Server

To connect to a Venue Server, enter the venue server URL (<https://<host>:<port>/VenueServer>) in the address bar, and then click **Go**; see Figure 10.

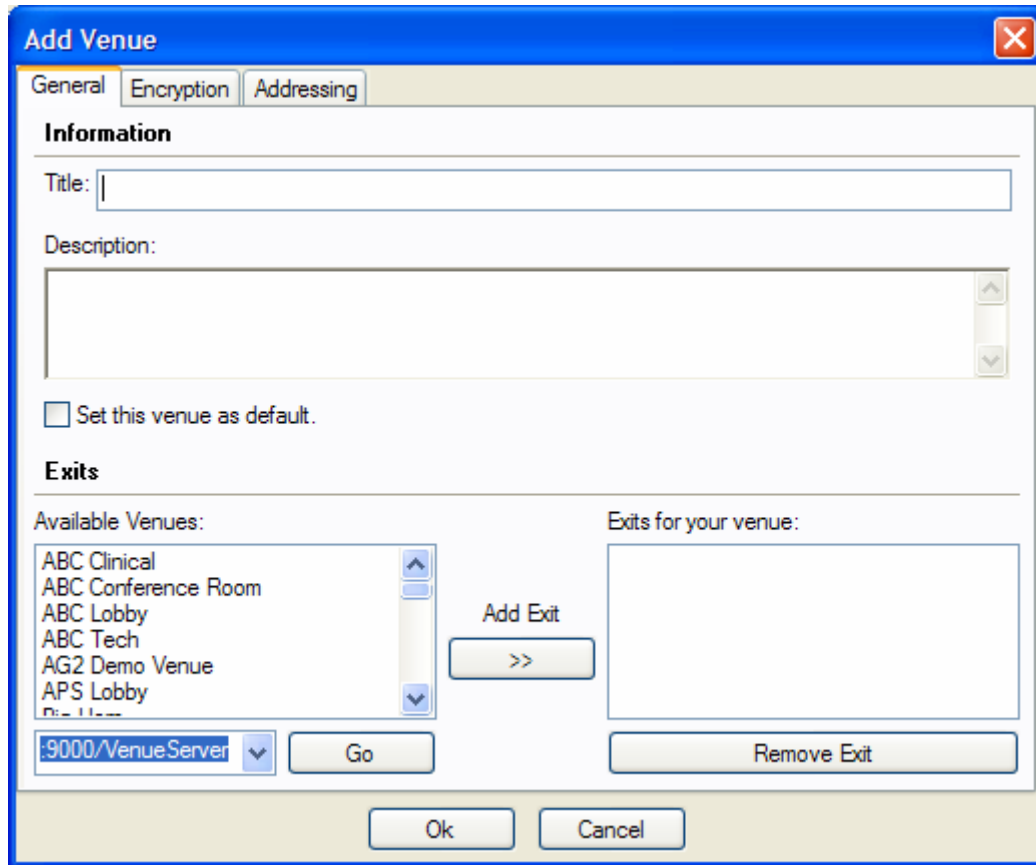


**Figure 10** Use the address bar to connect to a venue server

## 3.4 Adding a Venue

Click on **Add** under the list of venues in the **Venues** tab. You will then see the dialog in Figure 11 appear. The dialog is separated into three tabs: **General**,

**Encryption**, and **Addressing**. At a minimum, you need to specify the title of the venue and give it a description in the **Information** section of the **General** tab.



**Figure 11** Creating a new venue – **General** tab

### 3.4.1 General

**Information.** The **Information** section shown in Figure 11 lets you give the new venue a **Title** and a short **Description**. This is the minimum information required to create a venue. If you want this venue to be the default venue of the server, mark the check box labeled **Set this venue as default**. Each participant connecting to <https://host:port/Venues/default> will then automatically get directed to enter this venue.

**Exits.** To connect this venue to other venues, use the **Exits** section shown in Figure 11. By default, venues located on the server you are connected to get displayed in the box labeled **Available Venues**. However, you can get venues from other servers by entering the URL address of the remote server, available under the list of exits, and clicking **Go**. To add an exit, select a venue, and use

the **Add Exit** button. In the list to the right you can see exits added to this venue. If you want to remove an exit, select the exit you wish to delete, and click **Remove Exit**.

### 3.4.2 Encryption

From the **Encryption** tab illustrated in Figure 12, you are given the option to modify the encryption setting. If you mark **Encrypt Media**, media streams in this venue will be encrypted. You can decide whether you want to specify a key for the encryption or leave the **Optional Key** field blank. The key will then be assigned automatically.

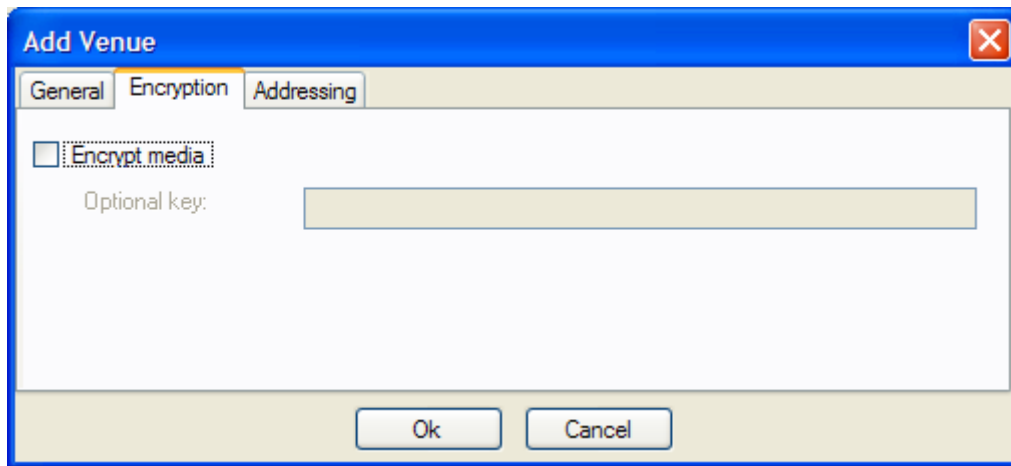


Figure 12 Creating a new venue – **Encryption** tab

### 3.4.3 Addressing

The media streams by default use dynamic multicast addressing; however, venues can be created with static addressing as well. With dynamic addressing, multicast addresses are allocated as needed when users enter a venue. Static addresses remain assigned to the venue independent of user activity. In the Addressing tab illustrated in Figure 13, static addressing of video and audio streams requires you to specify IP address, port, and a time-to-live value. The addresses should be in the multicast address range 224.2.0.0–239.255.255.255; the ports must be even; the TTL (time to live) is typically set to 127. The “Generate New Addresses” button may be used to query the VenueServer for multicast addresses.

**Add Venue**

General Encryption **Addressing**

☒ Use Static Addressing

**Video (h261)**

Address: 224 224 224 5 Port: 50000 TTL: 127

**Audio (16kHz)**

Address: 224 200 2 120 Port: 49888 TTL: 127

Generate New Addresses

Ok Cancel

**Figure 13** Creating a new venue – **Addressing** tab

### 3.5 Modifying the Venue

Select the venue you want to change, and then click on **Modify** under the list of venues in the **Venues** tab. A similar dialog to that used to add a venue is displayed (see Figure 11). Modify the appropriate fields, and then click **Ok**. (For more information about specific options, read Section 3.4). In addition to General, Encryption, and Addressing, the Modify Venue dialog has a fourth tab, **Security**. Access Grid venues use role-based security to establish an authorization policy, determining which participants to let in and with what authority. Administrators can decide who is allowed to perform different actions, such as entering the venue or adding data.

The **Security** tab in Figure 14 displays current authorization setting for the venue. The venue has a set of **Roles** that identifies different authorization privileges, or **Actions**, for groups of participants. When you select a role from the left panel, the right action panel shows you which actions are enabled for that role. When a role is being expanded, participants included in the 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, according to the menu opened by right clicking a role, participant, or action.



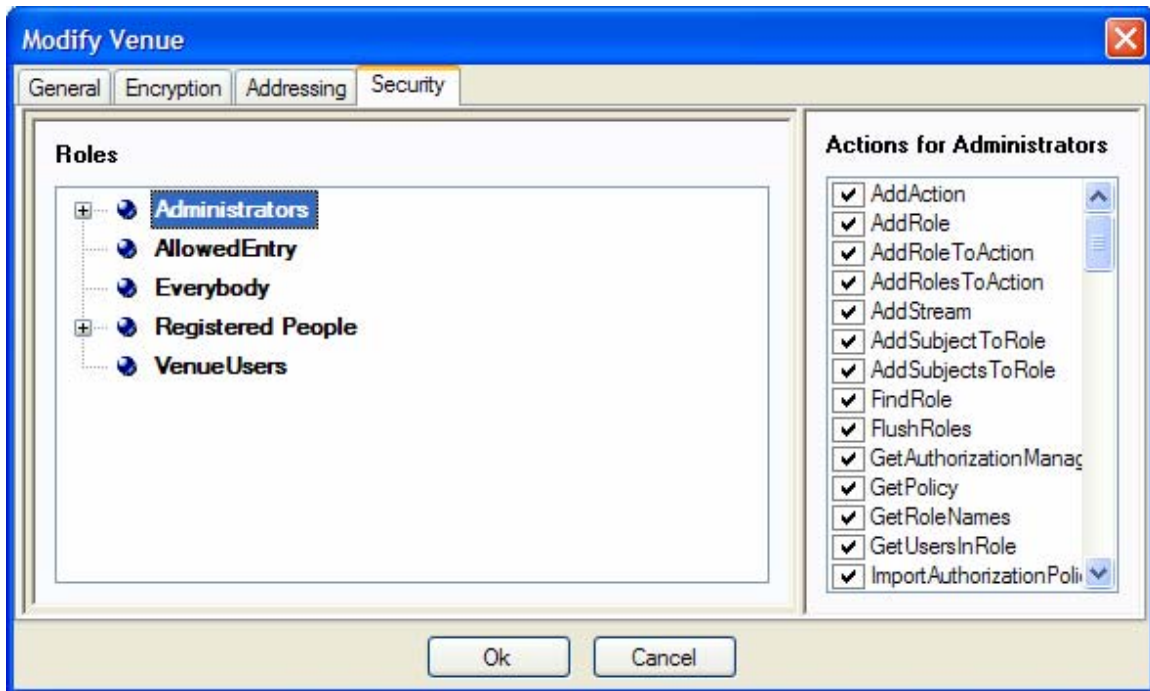


Figure 14 Venue authorization

### 3.6 Removing a Venue

Select the venue you wish to remove from the list of venues, and click the **Delete** button under the list. Click **Ok** in the next dialog to confirm that you want to remove the venue; it will disappear from the list.

### 3.7 Changing the Server Multicast Range

Multicast addresses, for all venues in the server, are by default assigned from a standard range. This can be changed by selecting **Custom Range** from the **Multicast Address** section in the **Configuration** tab and entering an IP address and a mask value. If you want to use static addressing for individual venues, you can specify that when you create a new venue (read Section 3.4)

### 3.8 Changing Server Encryption Settings

If you select **Encrypt Media** in the **Encryption** section of the **Configuration** tab, all venues on this server will by default use encryption. However, you still can change the encryption setting when adding a new venue, or you can modify an already existing venue (see Sections 3.4 or 3.5 for more information).

### 3.9 Setting Server Authorization

The **Authorization** section of the **Security** tab enables you to control the authorization for the server. The frame in Figure 15 displays the current authorization setting for the server. The server has a set of **Roles** that identifies different authorization privileges, or **Actions**, for groups of participants. When you select a role from the left panel, the right action panel shows you which actions are enabled for that role. When a role is being expanded, participants included in the role are shown. A participant may be added to several roles and 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, according to the menu opened by right clicking a role, participant, or action.

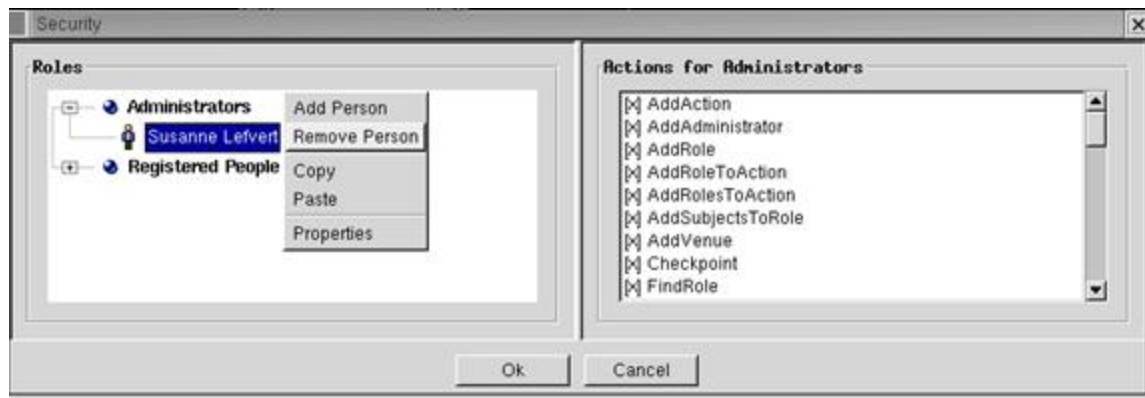


Figure 15 Server authorization

## 4.0 About Certificates

Every user and service in the Access Grid must have a valid certificate issued from 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.

### 4.1 Purpose of 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 yourself.
2. Authorize what resources people are allowed and have permission to access.
3. Preserve confidentiality by just showing 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, see <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 the 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."

### ***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.