![Vidyo - Personal Telepresence]

VidyoConferencing™ Administrator's Guide

System Version 2.1

Document Version 2.1-D

TABLE OF CONTENTS

TABLE OF CONTENTS

CONVENTIONS USED IN THIS GUIDE

Certain tasks cannot be undone. Perform these tasks only if you're absolutely sure that you must perform them. Whenever a task cannot be undone the following warning appears before the task is described:

Warning: The following task cannot be undone.

Some tasks overwrite or erase an entire database. In addition to the above warning message you'll also see the icon to the left of this paragraph as an additional warning next to the task's steps. Don't say we didn't warn you!

There are also warnings about less serious consequences of an action:

Warning: When the system is restarted or shut down all calls in progress are ended.

Text you type into an onscreen field or a browser address bar is shown in a monospaced font. So is text you type in at the command line or on screen. Variables are shown in blue, surrounded by angle brackets:

`http://<URL or IP>/super`

On all pages in the system, a red star (*****) denotes a field that cannot be left blank.

A Special Note About This Guide

This guide is distributed as a PDF file and although you can, or course, print it out, it's most useful when viewed onscreen. All page references in bold light blue are links. When viewing this PDF document onscreen you can click on a bold light blue page number to move to the referenced page.
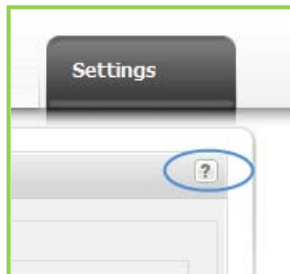
You should also know that this guide serves as your online Help system. When you click on a screen's Help button the appropriate page is opened in a new tab or window in your browser. However, it's important to understand that you can generally perform multiple tasks on the same screen. That means that when you click the Help button, the specific instructions for the task you're performing might not appear. If that's the case, just scroll down a page or two and you'll find the assistance you're looking for.

Here's one more point. Even if you've taken one of our classes it's a good idea to at least skim (and actually read, if you're really serious) this entire guide before starting to configure your system. It's really not as deadly dry as most manuals and we've even salted the screenshots with some unusual information just to help you keep from dozing off.

ABOUT THE VIDYOCONFERENCING SYSTEM

Who Are We?

We're Vidyo, Inc., creators of what we (and our customers) believe is the most advanced and cost-effective video conferencing system in the world. There are three ways your organization can get VidyoConferencing capability.

- We can host the system for you. (In which case you don't need this manual. We take care of everything.)

- One of our resellers can host the system for you. (And you won't need this manual either.)

- Your organization can license a system from us or one of our resellers. (In which case this Admin Guide will be indispensable to you as you set up and maintain the system.)

Who Are You?

You're an IT professional who understands and manages your organization's network. You have a solid understanding of Internet protocols, network topologies and general networking concepts.

The System in Brief

The VidyoConferencing system allows users to connect to and have conversations with other system users using the best of online video technology. Each end user has a portal (web page) that can be viewed in Internet Explorer, Firefox, Chrome and its own window. The portal allows system users to search and find other users, place direct (point-to-point) calls, and gather in virtual online "meeting rooms."

Users also have VidyoDesktop programs on their (Windows or Macintosh) computers that enable them to participate in point-to-point direct video meetings and multiple participant video conferences. It displays up to eight other participants and users can also choose to view their own images like you can watch two channels on a TV with PIP (picture-in-picture). This feature is called Self-View.

For the full experience the user needs a video camera, microphone and speakers. The camera, mic and speakers can be the kind built into most laptops these days, and a headset can take the place of the mic and speakers. Alternatively, we have a list of devices we've tested and have found to provide the best experience. (See the lists of recommended webcams, headsets and echo-cancelling speakerphones on page **10**.

The optional VidyoGateway server allows interoperability with older conferencing systems. VidyoGateway also allows people to call into a conference from an ordinary landline or cell phone for voice-only participation.

This document is the user guide for the three types of administrators that run the system:

- Super Administrator – Configures and maintains the network.

- Administrator/Tenant Administrator – Configures and maintains user settings.

- Operator – Has a subset of Admin privileges.

There are separate guides for VidyoPortal end users and the VidyoRoom™ appliance.

 In order to be able to use the system, a VidyoPortal needs to be installed and configured, and users and "rooms" need to be set up. Super Administrators use a secure portal (a set of web pages called simply, the

Super Portal) to perform their tasks while Admins, Tenant/Admins and Operators use a different portal (the Admin Portal, a different set of web pages) to perform their tasks.

The Super Admin's rights are a superset of the Admin/Tenant Admin's. However when a Super Admin clicks on an option (button or link) to perform a task that an Admin can do, the Admin portal login page will open in a new tab or browser window and Super Admin will log in as an Admin.

The Admin's rights are a superset of the Operator's rights and they both log into the Admin portal. When Operators log into the Admin Portal, the tabs for tasks that they can't perform (involving Groups and Portals) are not displayed to them.

This guide is divided into the following major sections:

System Settings – Configuring settings a Super Admin creates for the system as a whole

Components – Configuring of the VidyoPortal's components, such as the VidyoManager, VidyoRouter, VidyoProxy and VidyoGateway

Tenants – Configuring of the tenants (defined below) using the system, including licenses, cross-tenant access and network components

Users – Creating and managing the Vidyo system's user accounts.

Meeting Rooms – Creating and managing the virtual meeting rooms in the system, including controlling aspects of live meetings.

Groups – Assigning users and rooms to provisioning groups.

Admin Settings – Configuring settings created by an Administrator or Operator.

DEFINITIONS USED IN THIS GUIDE

Vidyo Concepts and Equipment

- **Portal –** A single web page[1] (for end users) or a series of web pages (for Super Admins, Admins and Operators) that are used to interact with the system. It's also how the users access their "rooms." Each user is automatically assigned a room when their account is set up but a user can actually have more than one room (all accessed via his or her portal). An end user uses his or her portal to make direct point-to-point (person-to-person) video calls and to set up and use their "room(s)" (virtual conference room(s)). (But the UI for the end user in a call or conference is his or her VidyoDesktop software.)

- **VidyoRouter Cloud Edition** – (Sometimes referred to simply as "Vidyo Cloud" for brevity.) An enhanced topology that increases network bandwidth efficiency, decreases latency and optimizes how VidyoRouters handle traffic. It is now the standard licensing model for VidyoConferencing, although we still support the older Ports model. A small organization with few locations may not need to use all of the capabilities of Vidyo Cloud right away but it's built-in, doesn't cost extra and it's ready to go when you need it.

- **VidyoDesktop** – The program that enables users to view other users in a direct call or a conference. The program resides on users' computers. There are Windows and Macintosh versions of the software.

- **VidyoGateway –** An optional rack-mountable appliance that easily connects legacy equipment—including MCUs—to your VidyoConferencing system.

- **VidyoOne** – Our smallest capacity Vidyo server. It is designed for smaller organizations that don't need the full power of our standard VidyoPortal server.

- **VidyoPortal –** A powerful server that incorporates the VidyoManager, VidyoRouter technology and VidyoPortal software all in one purpose-built unit.

- **VidyoProxy** – A software component built into both the VidyoPortal and VidyoDesktop that enables authorized endpoints to connect while denying unauthorized connections. It also enables NAT and firewall traversal, as described in the Firewall and NAT Deployments chapter that starts on page 129.

- **VidyoReplay** – An optional rack-mountable appliance that enables users to stream live or pre-recorded video. For instance, a webinar can be broadcast live to participants and also saved to be played back on demand by those who missed the original broadcast or want to view it again.

- **VidyoRoom –** As explained below, a VidyoRoom is not an actual physical room. It's a robust appliance that is typically installed into an *actual* conference room. It can deliver HD-quality video at up to 60 frames per second. Informally we often call the VidyoRoom a "room system."

- **VidyoRouter –** The part of the system that routes video and audio streams between endpoints. It also intelligently identifies and adjusts to bandwidth and network constraints. Every VidyoPortal con-

---

[1] While the user portal is one page, end users perceive it as multiple pages because the page's contents change completely (via Flash) as the user performs various functions.

tains one VidyoRouter and you can purchase additional units to add additional capacity (up to 100 HD VidyoLines per VidyoRouter) to your system.

Users

A user is anyone who uses the system. There are six types of users. In a small organization, one person might assume the roles of both Super Admin and Admin, when appropriate.

- **Super Admin** – Has administrative privileges and is responsible for general portal configuration including network settings, components configuration, maintenance (backup and upgrades), tenant configuration and global settings. In a multi-tenant system, has full administrative privileges above the tenant admin and all regular tenant admin rights.

- **Admin/Tenant Admin** – Has administrative privileges. Can add, delete and manage users, set up public rooms, and set up groups (which define maximum number of participants and bandwidth for users). When we say that a task can be performed *only* by an Admin, we don't mean that the Super Admin can't do it. He or she just has to log in to the Admin portal to do the task. When you've got your Super Admin hat on and you click on certain buttons or links in the Super Admin portal you may find yourself automatically whisked off to the Admin portal.

- **Operator** – Can manage users and meeting rooms. The operator has the same rights as the administrator except that an operator does not have access to the Groups and Settings tabs. (Operators log into the Admin portal but they simply do not see the Groups and Settings tabs.)

- **Normal** – The end user. Each user has a portal (Web page) from which they can join meetings (i.e., teleconferences), control their own meetings, and place direct (point-to-point) calls. They can also change their passwords and (optionally) set PIN codes that other users will require to join their meetings.

- **Executive Desktop** – An Executive Desktop is a premium user license that's assigned to a specific user account. Executive Desktops are available only with the new VidyoLines licensing model (which is now our standard licensing model—as opposed to the older Seats and Ports model). An Executive Desktop doesn't require or consume a VidyoLine license to participate in calls or conferences yet an Executive Desktop user is never denied service due to lack of shared VidyoLine availability. Executive Desktops are ideal for mission-critical applications like executive use, emergency medicine, emergency management, real-time financial markets and so on. Executive Desktop users can also decode (receive) video signals at 1440p 60 fps (four times better than 720p HD). That means that in a call with four other uses an Executive Desktop user can see each participant's image in full 720p—a capability no other video conferencing system can match.

- **VidyoRoom** – This is not a physical room. It's an optional teleconferencing appliance (purpose built hardware running our custom software) that's generally placed in an actual conference room. It's the dedicated Vidyo endpoint appliance. It has the same rights as a normal user. It can be set up with a powered camera. If so, the Vidyoroom's Administrator can enable Far End Camera Control (FECC), which allows other conference participants to pan and tilt the camera remotely (so they can, in effect, "look around the room"). The VidyoRoom is the only component that's also a user. And it's the only user that's also a component. It comes with its own set of documentation.
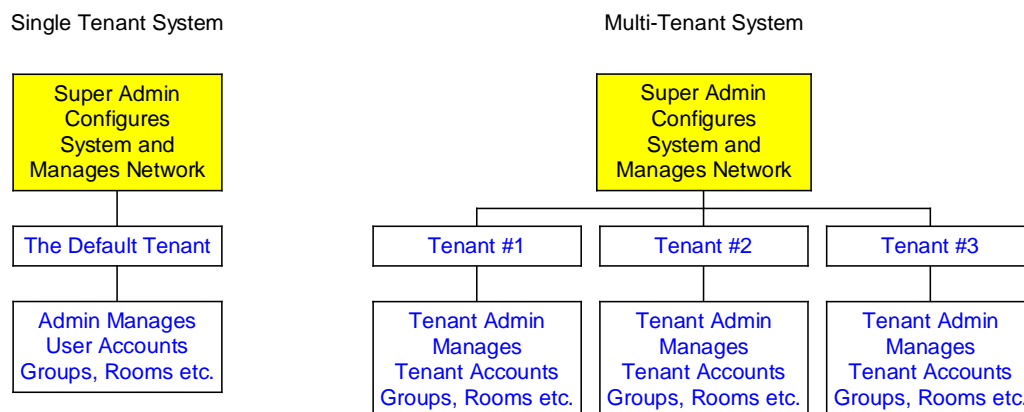
- **Legacy** – A device such as an ordinary telephone or a conferencing system that uses traditional H.323 and SIP-based videoconferencing solutions. A legacy device has no personal room. (See below for the definition of personal room.) There is also a provision for guest users (if enabled). Guest users are users you invite to a meeting who are not registered with the system. To invite users, you simply email them an invitation that contains your room URL (the link to your personal room). Standard (boilerplate) text is provided. The Super Admin can customize the text as desired. The Admin (or Tenant Admins) can edit the text for their tenant(s). Users can edit each invitation they send (in order to add date and time or any other information). The guest user clicks the link in the invitation email, downloads the software if they haven't before from that machine, and then enter their name to be able to join the meeting. Guest users have only the ability to join a conference. They don't have the ability to log in to the system on their own or receive incoming calls. Refer to the separate Quick Guest Guide for more details.

Tenants

- **Tenant** – Each Vidyo system has at least one tenant, called the default tenant. If you choose not to use the system's built-in multi-tenant capability, every user in your entire organization belongs to the default tenant.

- **Multi-Tenant** – Much as a web hosting company can host multiple websites for a variety of customers, a single VidyoPortal system can be set up to host multiple organizations, called tenants. A single organization might also wish to divide up its users into multiple sets of tenants. In the latter case the Super Admin will likely want to enable "cross-tenant access" so any user can reach any other user.

Single Tenant System | Multi-Tenant System

Super Admin Configures System and Manages Network

The Default Tenant → Admin Manages User Accounts Groups, Rooms etc.

Tenant #1 / Tenant #2 / Tenant #3 → Tenant Admin Manages Tenant Accounts Groups, Rooms etc.

The chart above illustrates the differences and similarities of single tenant and multi-tenant systems. Both types of system have a Super Admin in charge of configuring and managing the system as a whole. In a single tenant system one Admin manages all user accounts and creates and manages provisioning groups and public rooms. In a multi-tenant system the Tenant Admin has the exact same duties, but only for his or her tenants.

Of course none of this precludes (for instance) the same person from wearing both the Super Admin and Admin hats at different times, as appropriate. And a single person could be the Tenant Admin for more than one tenant. In fact, nothing in the system prohibits one (overworked) soul from being the Super Admin and the Tenant Admin for every tenant in a multi-tenant system.

- **Tenant Name** – A simple identifier within the system and among other tenants. If you're hosting multiple organizations it might be the organization's common name (Acme Corp., Jones Foundation and so on). If you've divided your organization into different tenants the name might reflect the tenant's role in your organization (Board Members, Sales, New York Office and so on.)

- **Tenant URL** – The tenant's URL is the URL/FQDN that tenants use to access their virtual portals.

Meeting Rooms

Meeting rooms are virtual rooms where users of the Vidyo system can gather for VidyoConferences. There are two types of meeting rooms:

- **Personal –** Each user is automatically assigned his or her own personal room. This is the equivalent of a "personal office" in the physical world. Upon creating a User account a personal room is automatically generated.

- **Public –** Common public spaces may also be created by Admins and Operators only. These are the equivalent of conference rooms in the physical world, i.e., a virtual meeting room.

Groups

Users, public meeting rooms and VidyoRooms belong to provisioning groups. There is always at least one group, called the default group.

- Such groups are managed by Admins/Tenant Admins.

- Groups are subsets of Tenants. You don't have to create any groups. But doing so allows you to allocate resources among Tenants in a way that may better suit your organization's requirements. For example, all of your branch managers could be in a group that is allowed greater bandwidth usage.

- The configurable attributes of a Group include the maximum number of participants and maximum bandwidth per participant for the conference room.

- The values for the maximum number of users in a call and the maximum bandwidth allowed per call apply to Groups, and all private meeting rooms and users inherit those values when they are added to a group.

  Note: The bandwidth of guest users and public rooms are an exception. There is no provision to limit their bandwidth.

- You can change the maximum number of participants allowed in a personal room only by changing the group the user belongs to.

- The bandwidth limitation is per user, so changing the group a user belongs to might also affect their bandwidth limitation-and the maximum number of participants that can be in their room.

The default group has the following factory configuration:

- Maximum Number of Participants in One Room: 10

- Maximum Receive Bandwidth Per User: 10,000 kbps

- Maximum Transmit Bandwidth Per User: 10,000 kbps

Note: As stated, the *bandwidth* limitation is per *user*, so two users that are in different groups can have different limitations while participating in the same conference. The *maximum number of participants* is limited according to the *room* the meeting is held in—so this applies to all users in a meeting.

Meeting

A meeting is an audio and/or video connection of a meeting room with two or more users interacting and sharing their media streams/presentations.

VidyoLines

VidyoLines are now the standard licensing model that supersedes the Seats and Ports model. (The Seats and Ports model is still supported for existing installations.) System set up and maintenance procedures differ from the seats and ports model. This guide shows you how to use the VidyoLines model. VidyoLines are a **perpetual** software license for a single logical connection through the VidyoRouter™—either point-to-point or multi-point for a low fixed regional price. A simple way to think about a VidyoLine is that it is similar to a phone connection on an IP PBX. Every phone uses a licensed connection when in a call and releases the license for someone else to use when the call is ended.

When Vidyo initially brought its revolutionary software-based video conferencing architecture to the marketplace, the market required some education with regard to the new desktop paradigm and how the VidyoRouter architecture changed the game. In doing so, Vidyo chose to implement a pricing model that was analogous to the existing hardware-based, room-centric solutions to make it easier to compare its pricing to traditional solutions.

As the market model has begun to shift and there is rapid growth in demand for desktop videoconferencing, Vidyo is moving to an aggressive software pricing model. VidyoDesktop™ clients connect through the VidyoRouter to other endpoints and conferences using low cost, perpetually licensed VidyoLines. VidyoRoom™ and VidyoGateway™ connections are effectively free since they don't consume VidyoLine licenses. VidyoLine simplifies the pricing model by eliminating separate VidyoPortal™ seat licenses as well as the distinction between concurrent multi-point vs. point-to-point users.

Seat

VidyoLines have done away with the concept of seats. We provide the following explanation for reference or if you happen to still be using our Ports licensing system. In that model one seat was required for each user in your organization who had an account on the system. There were three kinds:

- Admin
- Operator
- Normal

However when setting up Admin and Operator accounts if the "Allowed to log into user portal" checkbox was left unchecked, then that account did not require a seat. Super Admins never required seats because they can't place and receive calls (at least not when they were wearing their Super Admin hats; they may also have had a separate user account so they could use the system like other members of your organization—that user account would consume a seat).

Port

One port is required for each user in a multiparty conference or in a room. Every user (including a Vidyo-Room) who connects to a meeting room uses a port. A legacy device (e.g., an MCU-based system or a telephone) connecting to a conference uses a port. In the older Ports and Seats versions of VidyoDesktop, direct user-to-user calls did not consume a port.

Install

An install represents one installation of the VidyoDesktop client software. There are versions for Windows and Mac OS. A guest user (perhaps a customer or vendor with whom you wish to use the system) also requires an install.

Guest

A guest is a person outside your organization who has been invited to participate in a multiparty conference. A guest can participate only be responding to an invitation emailed by a regular user. Guests cannot initiate or receive direct calls. In the VidyoLine licensing model a guest does use a VidyoLine when connected. A guest does not consume a seat but consumes a port and may consume an install.

Once a guest has installed the VidyoDesktop client software he or she can be invited to participate in multiparty conferences from any VidyoPortal system in the world without needing another installation (if the Guest feature is enabled).

Endpoint

A device, such as a desktop, laptop, or VidyoRoom that enables a user to participate in direct (point-to-point) video calls and video conferences. Two points worth remembering:

- The VidyoRoom is the only endpoint that's also considered a user.

- Even though people can participate in conferences in audio-only mode (if your system has a VidyoGateway) by using cell phones and landlines, they are not considered endpoints because they cannot have the VidyoDesktop software installed.

"You"

When we use the word "you" in this guide we are referring to the role required to perform the operation, e.g., in describing tasks performed at the Super Admin level, "you" refers to a Super Admin; when referring to tasks performed at the Admin/Tenant Admin level "you" refers to a user with at least Admin/Tenant Admin privileges.

3. Recommended/Minimum Requirements

These parameters pertain to the VidyoDesktop client.

SUPPORTED OSES AND BROWSERS

- **Windows** XP, Vista and Windows 7 (32- and 64-bit)

    - Browsers: Internet Explorer, Firefox, Safari, Chrome

- **Macintosh** OS X 10.5 Leopard and later (Intel CPUs only)

    - Browsers: Firefox, Safari, Chrome

RECOMMENDED CONFIGURATION (ENCODES HD AND DECODES UP TO HD)

- Windows 7

- i7 based system

- Core 2 Quad with DDR2 or DDR3 memory

- Hyper-Threading Technology

- 2 GB or more RAM

- 256 MB or more video RAM (VRAM)

- 40 MB of free hard disk space

RECOMMENDED CONFIGURATION (ENCODES SD AND DECODES UP TO HD)

- Windows XP SP2

- Core 2 Duo 2 GHz

- Hyper-Threading Technology

- 2 GB RAM

- 128 MB video RAM (VRAM)

- 40 MB of free hard disk space

MINIMUM CONFIGURATION (ENCODES CIF AND DECODES UP TO SD)

- Windows XP SP2

- Pentium 4

- 1Gb RAM

- 128 MB video RAM (VRAM)

- 40 MB of free hard disk space

WEBCAMS:

Recommended

- Logitech HD Pro Webcam C910 - Encodes up to HD

- Logitech Pro B910 HD Webcam - Encodes up to HD

- Logitech Webcam Pro 9000 - Encodes up to HD

- Logitech Quickcam Pro 9000 – Encodes up to HD

- Logitech Webcam Pro C905 - Encodes up to HD

- Logitech Quickcam Pro for Notebooks - Encodes up to HD

- Logitech Quickcam Orbit/Sphere AF - Encodes up to HD

- Logitech Quickcam Vision Pro - Encodes up to HD

- Creative Live! Cam Socialize HD - Encodes up to HD

   Note: It's a good idea to go to the manufacturer's website and read some online reviews before purchasing any webcam. Some can achieve HD quality only by lowering frame rates.

Supported

- Apple iSight (Built in Webcam)

- Logitech Webcam HD C310

- Logitech Webcam C600

- Gigaware 2.0MP PC Camera

- HP Elite AutoFocus

- Globalmedia iREZ K2r Webcam

- Microsoft MS Lifecam NX-6000

- Hercules Dualpix Infinite

- Liquid Digital Solutions aGent V4 HD

USB HEADSETS

Recommended

- Microsoft Lifechat LX-3000

- Plantronics DSP-400 (Use with included DSP adapter 02.)

- Cyber Acoustics AC-840, AC-850

Supported

- Microsoft Lifechat ZX-6000 Wireless Headset

- Logitech ClearChat Comfort USB

- Logitech ClearChat PC Wireless

ECHO-CANCELLING SPEAKERPHONES

Recommended

- ClearOne Chat 50, Chat 60
- Plantronics Calisto 420
- Phoenix Duet Executive
- Yamaha PJP-20UR, PJP-25UR
- (Jabra) Jabra SPEAK 410
- (Konftel) Konftel 300

Supported

- ClearOne Chat 150

SOME HINTS FOR YOUR END USERS

We include the following hints in a number of our guides aimed at end users. We thought it would be handy for you to have them in this guide too.

How to Get The Best VidyoConferencing Experience

The VidyoConferencing system is designed to work through all sorts of network and endpoint (e.g., your computer) deficiencies and still deliver quality audio and video. However, we've discovered a few things you can do to help ensure you get the best possible experience. Here are some tips we think you'll find helpful:

- Use a wired network connection when possible and disable wireless (802.11 b, g, n).
- Use recommended audio/video devices to prevent echo and other audio/video issues.
- Plug each device (camera, microphone etc.) directly into one of your computer's USB ports whenever possible rather than a USB hub (whether it's one you added to your computer or is built in to you laptop's docking station).
- If you're using a laptop avoid running on battery—it reduces performance and video quality.
- If your computer has a Power Plan (All Windows and Mac laptops do) choose "High Performance."
- Make sure you have the latest drivers (like your DirectX video driver if you're a Windows user) for the devices you use during VidyoConferencing (camera, microphone etc.).

You should change the default passwords to all your servers to ensure their security and prevent unauthorized access. These are:

- Admin Console/SSH Menu for:
  - VidyoPortal (Default IP address: 192.168.1.100)
  - Stand-alone VidyoRouter (Default IP address: 192.168.1.105)
  - VidyoGateway (optional component) (Default IP address: 192.168.1.110)
  - VidyoReplay (optional component) ((Default IP address: 192.168.1.115)
- VidyoPortal/VidyoOne Super Administrator
- VidyoPortal/VidyoOne Administrator (per tenant)
- VidyoPortal/VidyoOne Super Administrator
- VidyoRouter Administrator
- VidyoManager Administrator
- VidyoProxy Administrator
- VidyoGateway Operator

Console/ Shell Admin (SSH) Menu

Certain tasks are performed at the console/shell admin menu. They're described fully in the Console/Shell Admin Menu Appendix starting on page .

To secure access perform the following steps for each component.

VidyoPortal/VidyoOne, standalone VidyoRouter and/or VidyoGateway and/or VidyoReplay:

1. Connect a keyboard and a VGA display directly to the server.

   This is the preferred method, especially if you're not an expert SSH user.
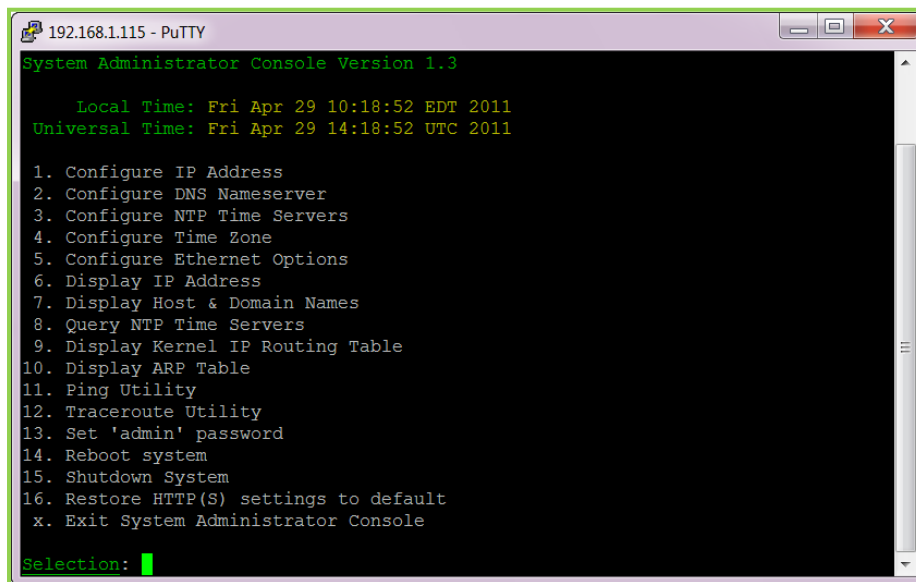
   OR

1. Establish an SSH connection to the server on port 2222.

2. Log in using the default Administrator account:
   - User Name: `admin`
   - Password: `password` (case sensitive)

3. From the onscreen menu type `13. Set 'admin' password` to change the default password.

The screenshot below shows the System Administrator Console as seen after login via SSH using the open source PuTTY client running on Windows 7. The menu may look slightly different depending on how you connect and the program (if you use the SSH method described in Step 1) you use to do so.

It's important to understand that the Admin account you set from `13. Set 'admin' password` is strictly for accessing and using this console/shell admin menu. It has nothing to do with ordinary Admins who work only in the GUI.

For other tasks you can perform at the console see the Console/Shell Admin Appendix on page **125**.

VidyoPortal/VidyoOne Super Administrator

Log into the Super Admin portal (Page **18**) and change the Super Admin password as described in Super Account on page **34**.

VidyoPortal/VidyoOne Admin

Change the Administrator login as described in Edit a User on page **87**. In a multi-tenant system, this must be done for each Tenant Administrator.

VidyoRouter Admin

Log into your VidyoRouter (Page **48**) and change the password as described in VidyoRouter Password Tab on page **52**.

VidyoManager Admin

Log into your VidyoManager (Page **42**) and change the password as described in VidyoManager Password Tab on page **47**.

VidyoProxy Admin

Log into your VidyoProxy (Page **65**) and change the password as described in VidyoProxy Password Tab on page **69**.

VidyoGateway Operator (optional component)

Change the user ID and password in the Reset Account tab, as described in the VidyoGateway Operations Guide.

VidyoReplay Admin (optional component)

Change the user ID and password in the Reset Account tab, as described in the VidyoReplay Administrator's Guide.

The first step in configuring your VidyoConferencing System is to perform system setup. System setup is performed by a Super Admin user, typically a network system administrator responsible for management of the overall VidyoConferencing System.

To perform system setup the Super Admin:

1. Configures the network settings for the VidyoPortal/VidyoOne/VidyoRouter at the console as described in the Vidyo Server Getting Started Guide.

   If you have not configured your network settings, see the Guide before proceeding. You cannot configure your Vidyo server until it is working on your network.

Tasks the Super Admin Performs[2]

- **Resetting the Super Admin Account Password –**The password for the Super Admin. This should be changed after the first log in.

- **Setting Platform Network Settings** – Set at the secure shell (SSH) console

  You can view the settings (read-only) in the Super Admin portal.

  Note: See the Vidyo Server Getting Started Guide that came with your Vidyo server and the Shell Admin Appendix on page **125** for information about network settings.

- **Uploading System Licenses** –The total number of VidyoLines be allocated to tenants of the system based on their requirements.

- **Uploading Endpoint Software** – The VidyoDesktop and VidyoRoom client software that you can make available to your users.

- **Selecting the System Language** – The default system language

- You can choose between English, French, German and eight others.

- **Setting up Components** – The VidyoGateway, VidyoRouter, VidyoManager and VidyoProxy components that can be used by tenants/users of the system.

- **Tenants** – Tenant configuration for the default tenant, or for each tenant in a multi-tenant system.

  System setup applies globally to the VidyoConferencing System, including all the tenants of a multi-tenant system, and must be completed *before* creating users, groups and rooms. Such administrative tasks are managed by an Admin user after the initial system setup has been completed. For information about admin login see Logging into Your VidyoRouter on page **48**.

For descriptions of the task Admins/Tenant Admins perform see What Admins and Tenant Admins Do on page **82**.

---

[2] Some of these tasks may not be necessary when you first set up your system because they will have been preset at the factory. You'll need to know how to perform them if you want to change the factory defaults.

HOW TO SET THE SYSTEM LANGUAGE

You can select your preferred language for the Super Admin log-in page from the drop-down menu in the upper right corner of the Super Admin Login page before you ever actually log in as the Super Admin. The VidyoConferencing System is available in eleven languages:

English	German	Japanese
Spanish	Italian	Chinese
French	Portuguese	Korean
Finnish	Polish	

Once you select a language, the login page language changes immediately into your chosen language.
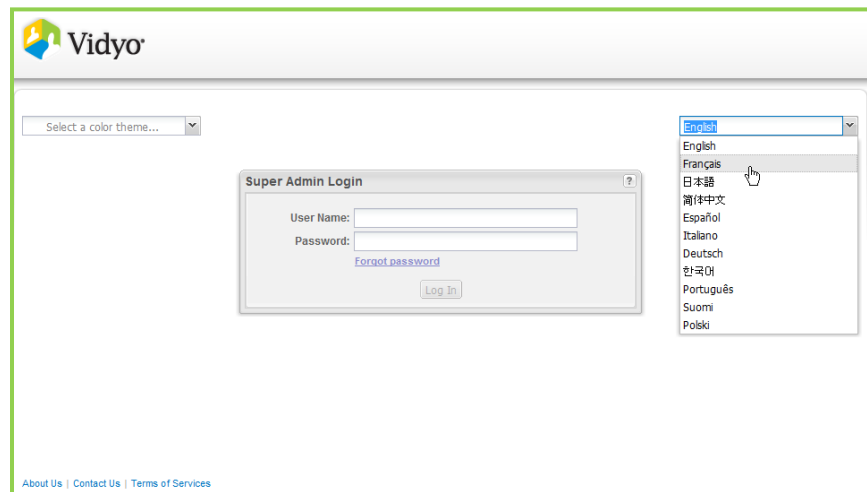
You can also change the color scheme by using the dropdown menu in the upper left-hand corner of the page.

Note: You can change the Super Admin's preferred language, if you want to.

1. Log in as Super Admin.

2. Click on the Settings tab.

3. Click Super Account on the left-hand menu.

4. Select the Super Admin's language preference from the dropdown menu.

5. Click the Save button.

   The system's preferred (default) language for other users will not be affected by this change.
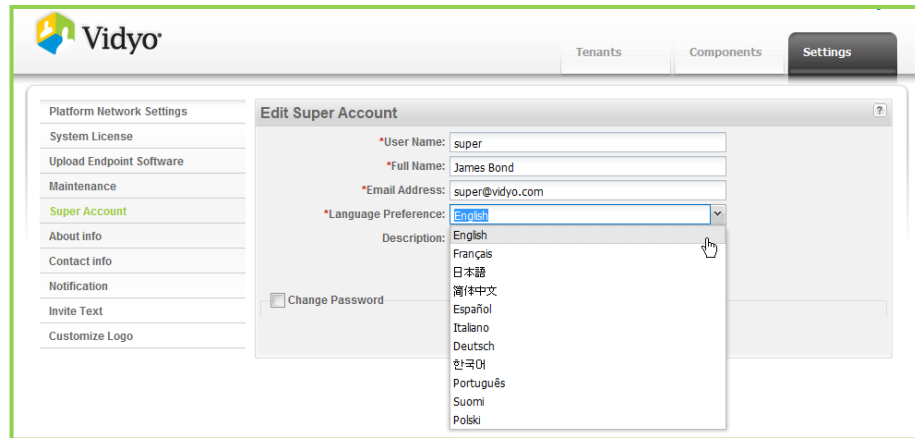
To perform system setup, you must log in as a Super Admin user. To log in as a Super Admin, enter the URL or IP address for the VidyoPortal in the address bar of a web browser, followed by a forward slash and the word "super."

```
http://<URL or IP>/super
```

1. Log in with the default Super Admin user name and password:

   User Name: `super`
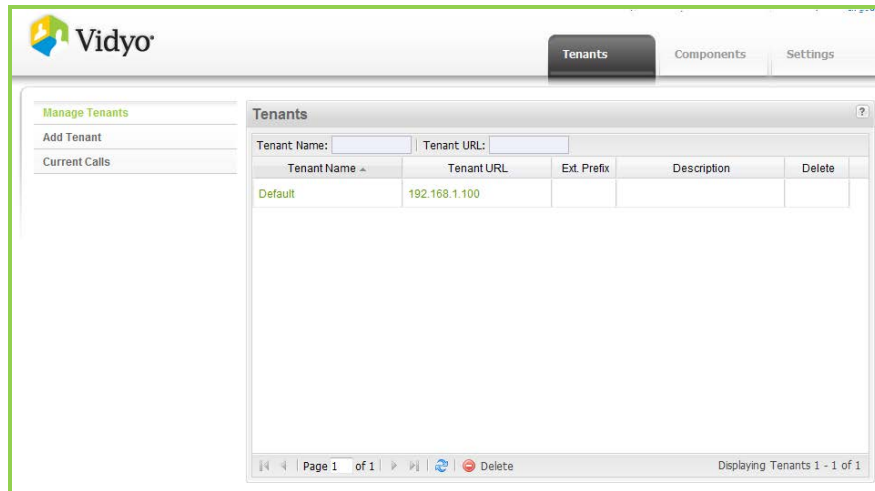
   Password: `password` (case sensitive)

Note: You should change the Super Admin user name and password as soon as possible. For information about changing the Super Admin login, see Super Account on page 34.

Only the Super Admin is able to log into the Super Admin portal.

After you log in, the Super Admin page opens, initially to the Tenants tab.

HOW TO PERFORM SYSTEM SETUP

Settings

In this chapter we're going to move down the main menu on the left-hand side of the Settings tab and explain what each setting means and what you need (or have the option) to do.
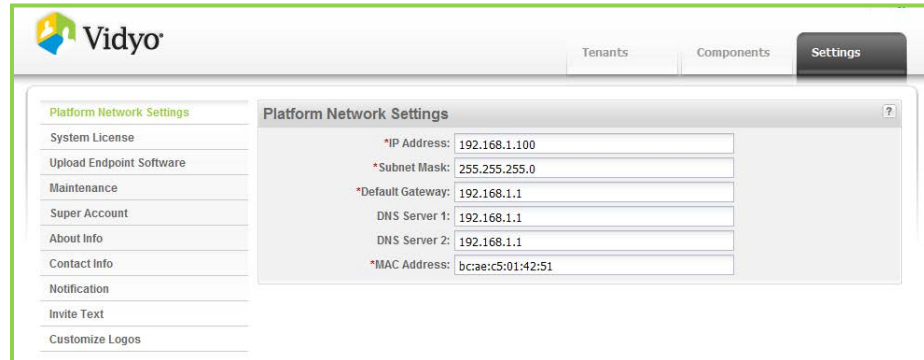
Click the Settings tab. You begin system setup by configuring settings that apply globally to the VidyoPortal system in the Settings tab. These settings must be configured before proceeding to further system setup.

The Settings tab enables you to configure the following global settings:

- System Licenses
- Endpoint Software
- Maintenance
- Super Account (login)
- Plus other optional settings

How to Check Your Platform Network Settings
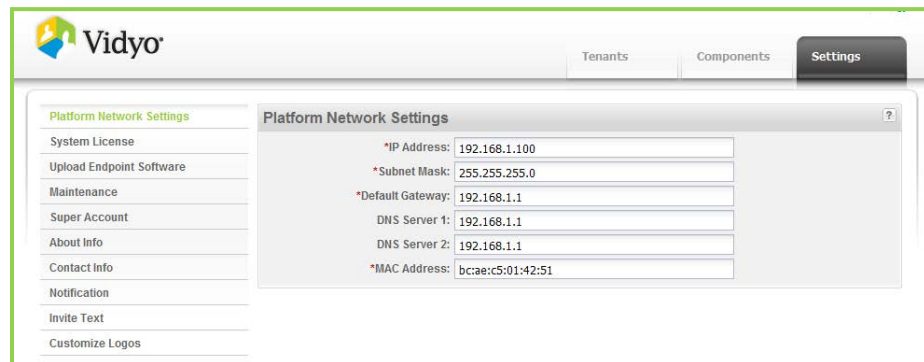
You must configure your Platform Network Settings at the Admin Console/Secure Shell (SSH) Menu prior to performing system setup, as described in the Vidyo Server Getting Started Guide that came with your VidyoPortal. It's also described on page 13. If you haven't configured your network settings yet, see the Guide. The Platform Network Settings form seen here in the Portal is read only. It offers a report/overview of the network settings for the VidyoPortal.

How to Upload and Activate your System License

Your VidyoPortal comes with a system‑wide license. The license defines:

- The term (length) of your license,

- The number of Seats,

- Ports/VidyoLines,

- Installations,

   …available for use as well as whether it is:

- A single- or multi-tenant system,

- Licensed for OCS integration,

- Licensed for encryption,

- Licensed for external database support.

The license needed to use your VidyoPortal comes in two encrypted files, one for the VidyoManager and one for the VidyoPortal. They're either sent by email or downloaded from the Vidyo Website. Also included is a text file describing the license.

To activate your VidyoPortal, upload the license files using the Upload System License page.

Note: You must upload the VidyoManager license (`vmlicense`) before uploading the system license (`syslicense`).

1. Click the Select File button.

Select File button

2. Select the VidyoManager license file (`vmlicense`) from its location on your computer or local network.

3. Click the Upload button to import it.

4. Repeat the process for the system license (`syslicense`).

   These are what license files look like:

5. After uploading the license files, enter the license key and license token

   You can find these in both the email you will have received with your licenses and the LicenseInfo text file.

After the token is applied, the system features and number of seats, ports and downloads specified by your license appear in the System License list. Scroll through this list to view all the features of your license.

Note: If running a multi-tenant system, you must then allocate the total number of seats, ports and installations authorized by the license to each tenant in your system, as needed. For more information, see Managing Tenants on page **73**.

The licensable features for the VidyoPortal are:

- Ports/VidyoLines
- Seats (no longer relevant in the VidyoLines licensing model)
- Installations
- Multi-tenant (on or off)
- Encryption (AES)
- OCS
- External Database

License Consumption by User Type

	VidyoLines Licensing Model	Both VidyoLines and Ports Licensing Model		Ports Licensing Model *
User Type	**VidyoLines**	**Install**	**Seat**	**Port ****
Super Admin	—	—	—	—
Admin	✓***	✓	✓***	✓
Operator	✓***	✓	✓***	✓
User	✓	✓	✓	✓
Guest	✓	✓	—	✓
VidyoRoom	—	—	—	✓
VidyoGateway	—	—	—	✓

* Superseded by the VidyoLines model but still supported.

** Ports are consumed only on multi-point calls, one port per user.

*** If calling ability has not been enabled for these users they do not consume a seat.

Ports and Licensing Notifications

If you provided one or more licensee addresses at the time of purchase they will be embedded into your license. If you are using the Ports licensing model the licensee and Super Admin will receive notifications when there are 45, 30, and 15 days left in your license. And in the final week they'll get one every day.

The Super Admin and Admin and Tenant Admins will receive a license warning when you have only 25 installs left. If you don't purchase additional installation licenses you'll receive additional warnings at 15, and

five installations left. Your current installs never expire. If you run out you just won't be able allow any new users who need to install the software until you purchase more.

How To Upload Endpoint Software
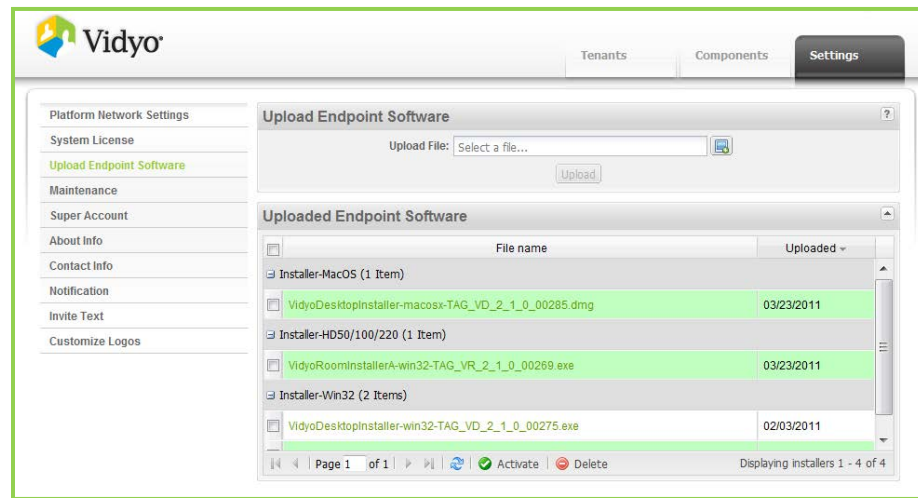
When new versions of the VidyoDesktop and VidyoRoom client software become available from Vidyo, you can upload the new software to your servers using this page so your users will be automatically prompted to download the new version when they next log in.

Both the Super Admin and Admin can upload endpoint software by taking the same steps. As you can see you click the Settings tab on the top navigation bar and then click Upload Endpoint Software from the left-hand menu.

1. Download the latest version of the software to your computer.

   The link will have been provided to you by your reseller or Vidyo Customer Support.

2. Click the Select File button.

3. Select the client software from its location on your computer.

4. Click the Upload button to import it.
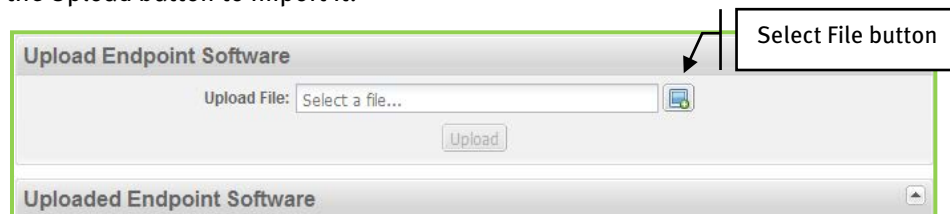
The software will then attempt to upload it. Throughout the process, the upload status will be displayed. When the endpoint installation file is uploaded, it appears in the Uploaded Endpoint Software list under its corresponding heading. Scroll through this list to view all available installation files.

To avoid failure messages, make sure you are uploading Vidyo software only. The software file name will end in an .exe extension for Windows and VidyoRoom and .dmg for Macintosh.

We recommend uploading the latest version of the software when it becomes available to help make sure all system users are utilizing the most up-to-date Vidyo software.

You can upload up to four different versions of each type of endpoint software (VidyoDesktop for Macintosh, VidyoDesktop for Windows and so on), but for each type you must make just one active. It is the active version that downloads automatically for VidyoPortal users when they first use the system or upgrade to a new version. The Admin for each tenant can deploy the version you activate, activate a different version or upload and activate another version, as needed.
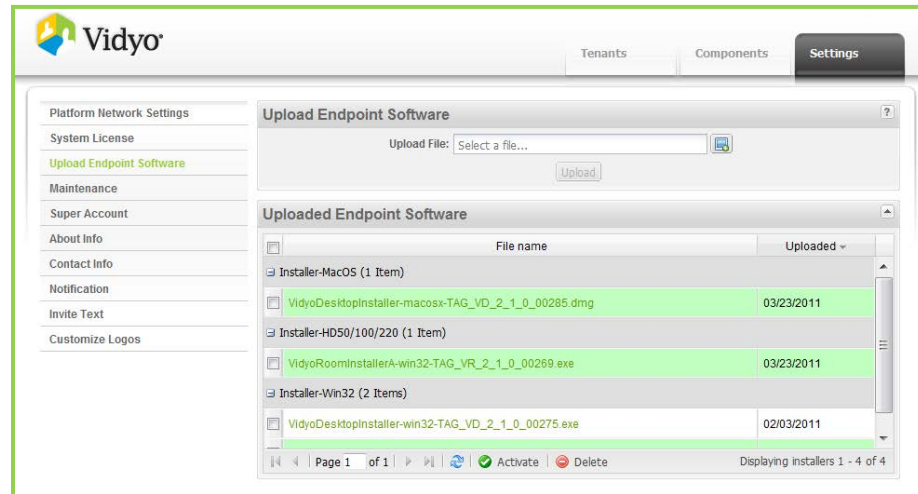
You can sort the list of installation files by file name and upload date by clicking the File name and Uploaded headings.

1. To hide all the installation files of one type, click the ⊟ button next to the file type heading.
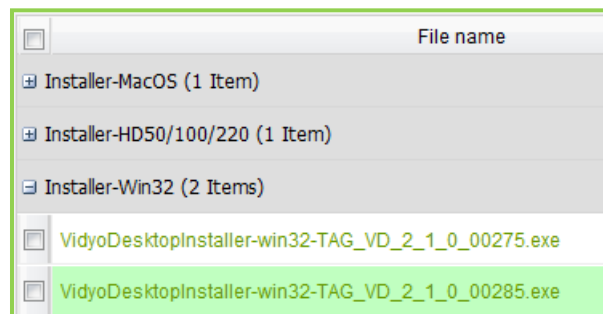
Rolled up headings (top two) and two Windows files, with one being active (the bottom file highlighted in green)

This "rolls up" the files under that heading.

2. Click the + button to re-display the installation files.

How To Activate An Endpoint Installation File

1. Select the checkbox to the left of the file name.

2. Click the Activate button at the bottom of the list.

    The file name appears highlighted in green.
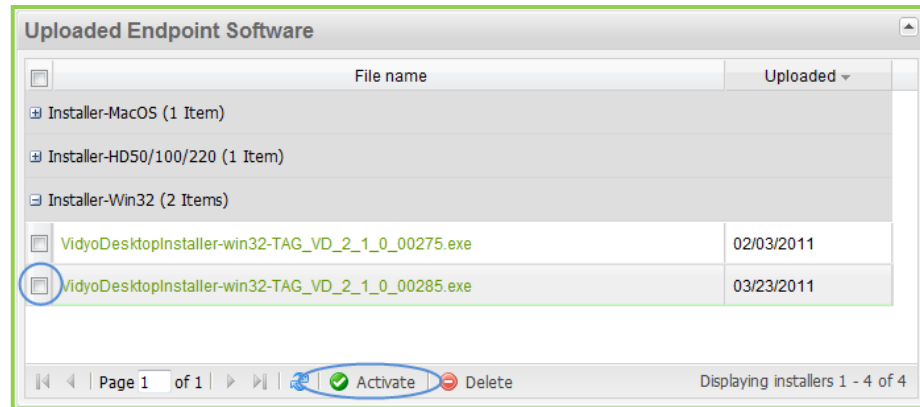
How to Delete Endpoint Installation Files

1. To delete an installation file or group of files, select the checkbox(es) for the files you wish to delete.

2. Click the Delete button to the right of the Activate button.

   If you delete a file by mistake you always upload it again provided you have not deleted it from your computer. If the file you mistakenly deleted is the current version of the client you also have the option of downloading it again from your reseller or Vidyo Customer Support.

MAINTENANCE

The next button on the Settings tab page is the Maintenance button. When you click it you'll its screen has a number of sub-tabs. The Database sub-tab is open.

Understanding the Database

The database contains everything **but:** the basic network settings of the system (IP, DNS, hostname, NTP); the SSL security certificates loaded and CSR information; and the license keys (each of these would need to be reset separately should a unit need to be replaced/rebuilt). See the CDR Appendix, which starts on page 171 for more information on the CDR database.)

The Database tab shows a list of backed up databases on the VidyoPortal hard drive, as well as the file creation dates.

How to Back Up the Database
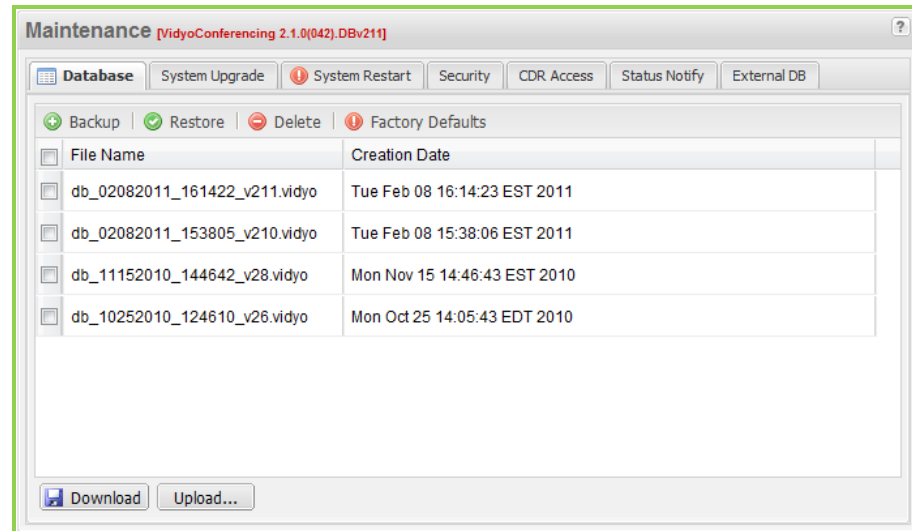
1. Click the Backup button at the top of the database list.

   A confirmation dialog box opens.
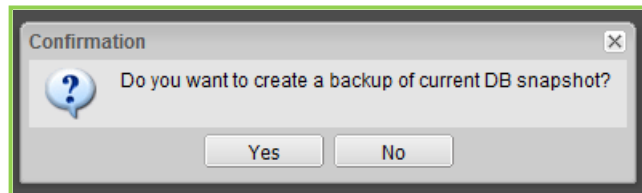
2. Click the Yes button.

   A backup copy of the database is made *on the VidyoPortal*. A success confirmation dialog box appears.
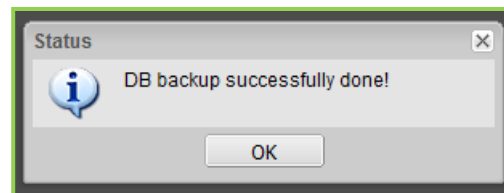
   Warning: Because the database is backed up on the VidyoPortal itself, making a backup does not protect you from a hard drive failure on the VidyoPortal. You should periodically download backups to an offsite computer.

How to Download a Backup File

1. Select the checkbox next to the backup version you wish to download.

2. Click the Download button.
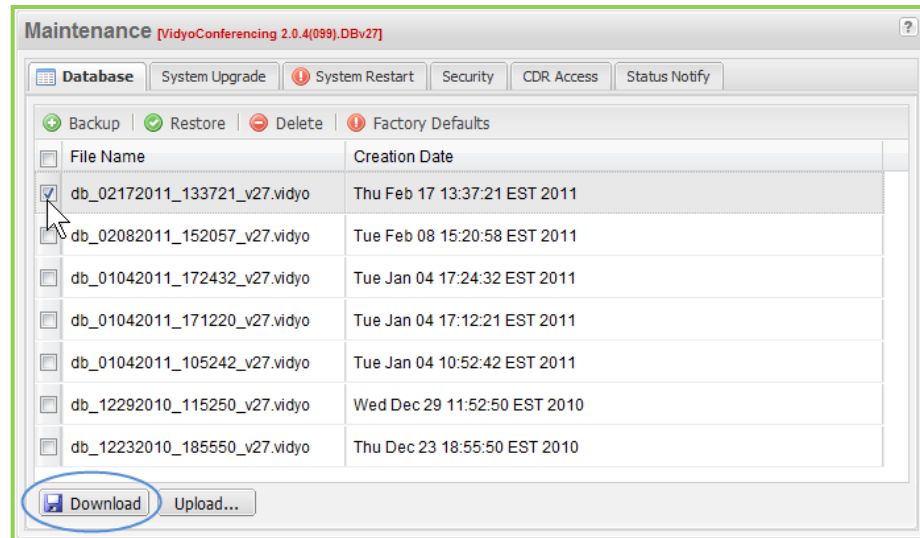
A confirmation dialog box opens.
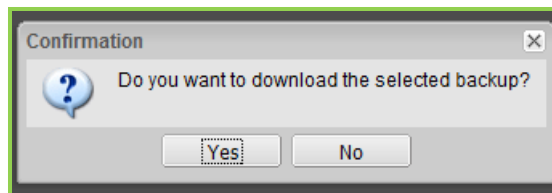
3. Click the Yes button.

Your browser's standard Open/Save File dialog box opens.
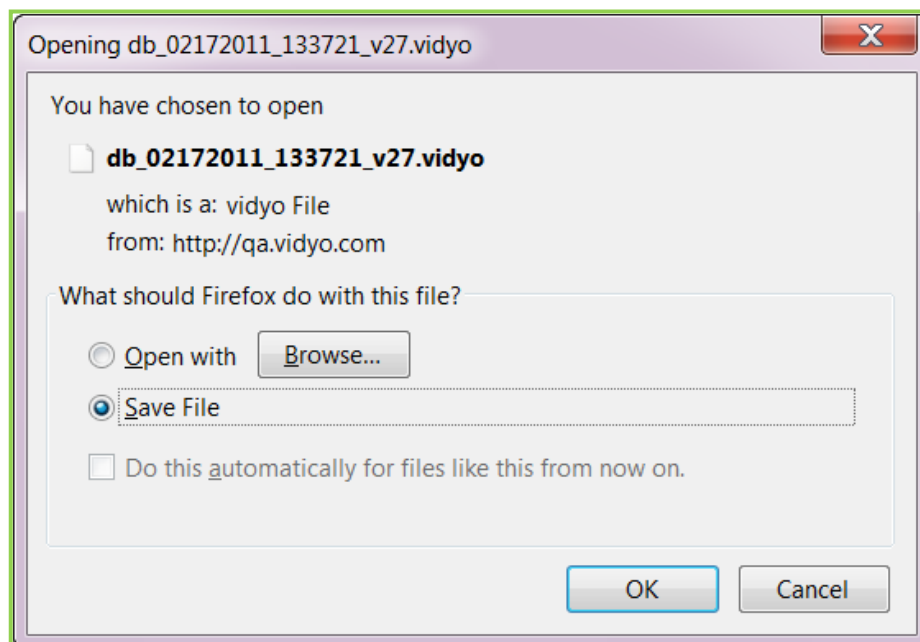
4. Ensure the Save File option is selected.

5. Click the OK button to save the database to the location you've set your browser to save files.

Now that you've downloaded the database you have a true backup.

How to Upload a Backup File

Uploading a backup file is easy.

1. Click the upload button in the database table.

   The Uploading backup file dialog box opens.
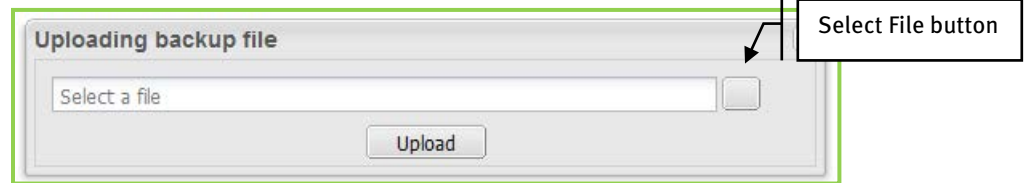
2. Click the Select File button.

   Your OS's standard File Upload dialog box opens

3. Locate the file on your computer or other computer on your network.

4. Click the Open button in the File Upload dialog box.

5. Click the Upload button on the Uploading backup file dialog box.

   The file uploads and is listed in the Database table.

How to Restore a Backup File

If the database you wish to restore is still on the VidyoPortal restoring takes just two clicks.

Note: The system license of the database you're restoring must match the system license of the system to which you are restoring it.

Warning: The following task will destroy the current database file. It's best to make a backup of the current database file before restoring a prior version.
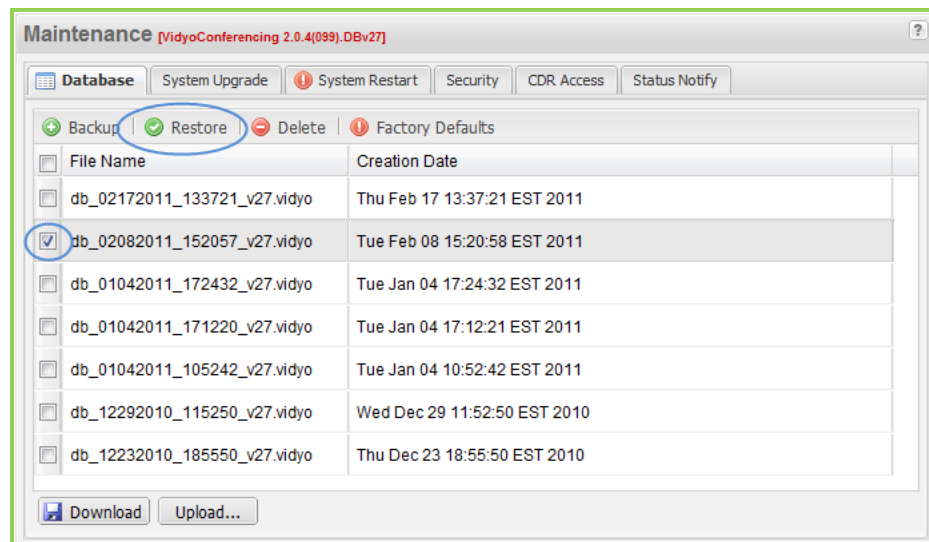
1. Select the database you wish to restore.

2. Click the Restore button.

Warning: The following task will destroy the current database. It's best to make a backup of the current file before restoring a prior version.

If you want to restore a database file that is no longer on the VidyoPortal:

1. Follow the directions above on uploading a database file.

2. Follow the instructions above for restoring a database file.

How to Delete a Backup File That's on the VidyoPortal

Warning: The following task cannot be undone.

To delete unnecessary or outdated versions of the database:

1. Click the checkbox next to the version you wish to delete.

2. Click the Delete button at the top of the database table.

3. Confirm the action in the dialog box that opens.

Warning: The following task cannot be undone.

To wipe the database clean and restore it to the factory defaults:

1. Click the Factory Defaults button at the top of the database table.

2. Confirm the action in the dialog box that opens.

Lots of warnings, huh? That's why it's a good idea to have a rock solid back-up schedule and stick to it.

How to Upgrade The System

The System Upgrade tab is used for upgrading the VidyoPortal/VidyoOne software version as well for applying system add-ons (such as SNMP) or patches.

The Vidyo server upgrade filenames contain the server product abbreviation, version number and/or Add-on/Patch name, and have a `.vidyo` extension (example: `TAG_VC_2_1_0_x.vidyo`).

Vidyo server upgrade files are available through your reseller or Vidyo Customer Support as they become available.
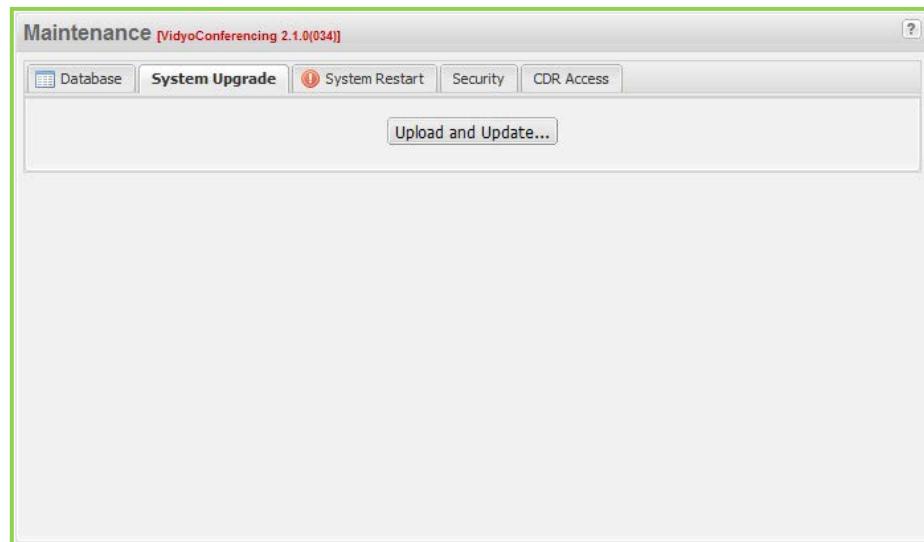
Warning: The following task cannot be undone.

To apply a system upgrade:

1. Click the Upload and Update button

   The Uploading new server software file dialog box opens.
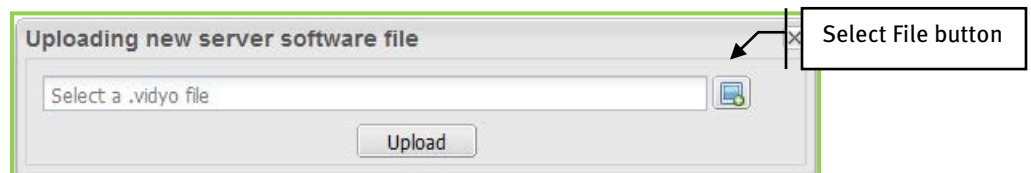
2. Click the Select File button.

   Your OS's standard File Upload dialog box opens

3. Locate the `.vidyo` file on your computer or other computer on your network.

4. Click the Open button in the File Upload dialog box.

5. Click the Upload button in the Uploading new server software file dialog box.

   The file uploads and the server reboots. Wait at least five minutes for the system to reboot.

Warning: The upgrade process terminates all calls in progress.

You might want to email users ahead of time and perform the upgrade when system usage is lowest.

How to Restart The System

The System Restart tab is used to restart or shutdown the portal server.

1. To reboot the VidyoPortal, click the Restart button

2. Confirm the action in the dialog box that opens.

   This will power cycle the server.

1. To shut down the VidyoPortal, click the Shutdown button.

2. Confirm the action in the dialog box that opens.

   This will power down the server.

Warning: Once the server shuts down you can power it back up **only** by physically pressing the power button on the front of the unit.

Warning: When the system is restarted or shut down all calls in progress are ended.

You might want to email users ahead of time and perform the upgrade when system usage is lowest.

Security

The next sub-tab in the Maintenance section is Security.
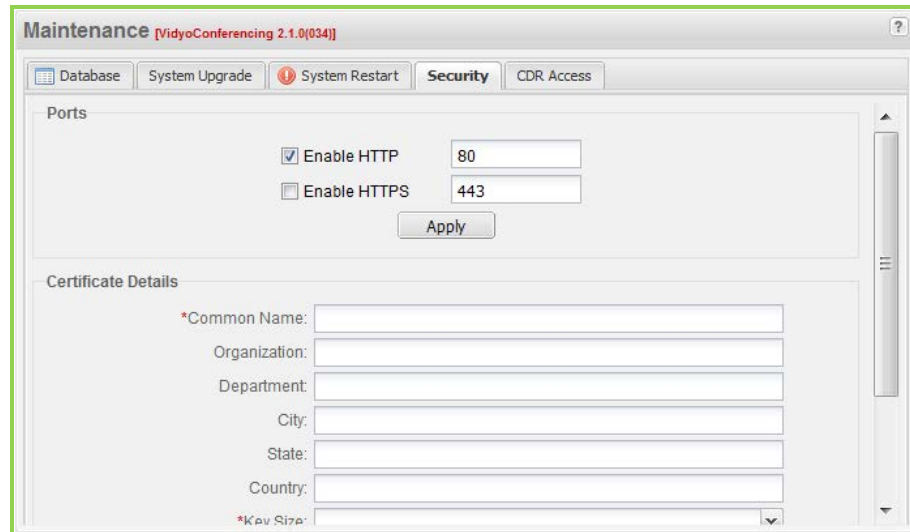
The Security tab enables you to deploy an SSL certificate to guarantee the authenticity of your VidyoPortal/VidyoOne to users. For information about implementing end-to-end security for your VidyoConferencing system, see the Security Appendix that starts on page **149**.

CDR Access
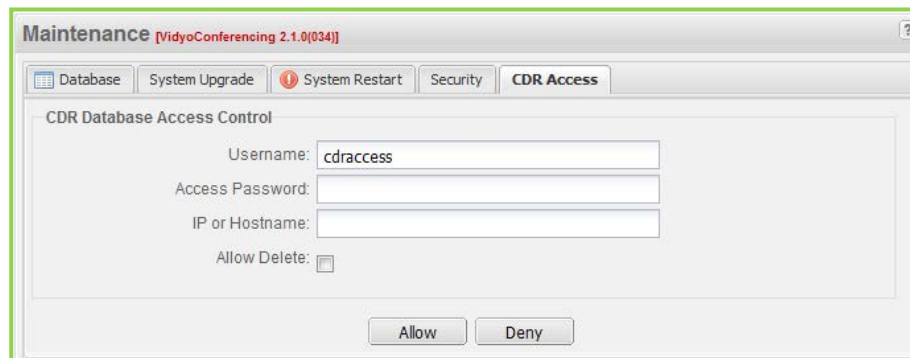
The Call Detail Records (CDR) database resides on the same server as the Web portal (VidyoPortal). The CDR database stores the following records:

- Point-to-point call summary

- Conference call summary

- Client installation summary

The VidyoPortal has been configured to allow remote MySQL clients to read and delete the details from all the tables within the CDR database. The CDR access tab enables you to grant permission via the access password and host IP or hostname for the cdraccess user.

For detailed information about working with the CDR database, see the CDR Appendix on page **171**.

External DB
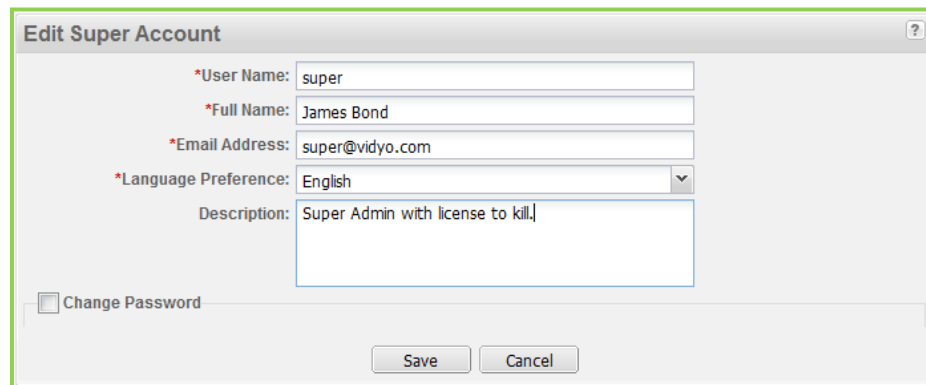
The portal stores its data in a SQL database inside the VidyoPortal appliance itself. If your license includes the External Database Support option, you'll see the External DB tab. This license allows you to store the

database on a separate server, if desired. Please contact Vidyo Customer Support if you would like to implement this feature.

SUPER ACCOUNT

The next button on the Settings menu allows you to change settings for the Super Account itself.
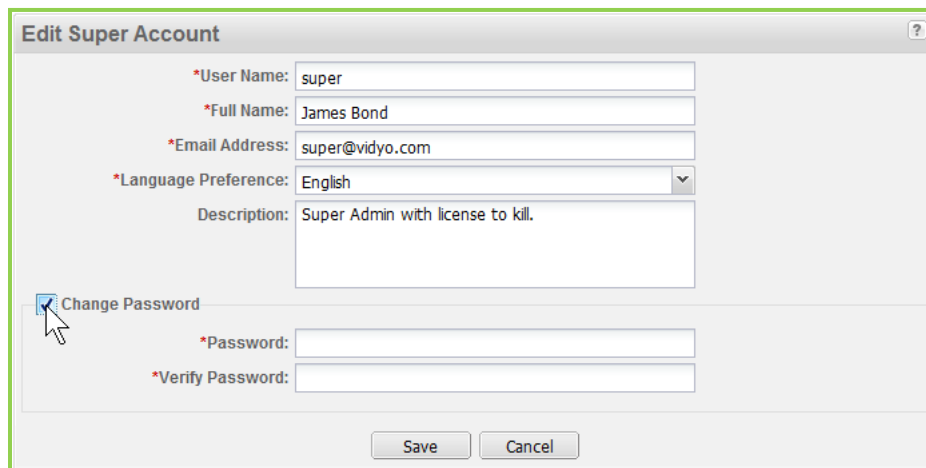
As you can see, there are five fields you can change and the first four can't be left blank. Change them as desired.

For security purposes, you should change the password for Super Admin access as soon as possible.

1. Click the Change Password button.

   The dialog box extends to include the Password and Verify Password fields.

2. Enter your new password in the New Password field.

3. Enter your new password again in the Verify New Password field.

4. Assuming the system doesn't complain about a failure to match when you're done typing, click the Save button to complete the password change.

   The system will complain that the passwords don't match right up until the moment you type the very last letter in the Verify New Password field even if the letters do match. Don't let this throw you.

Note: As you can see, you can change the Super Admin's full name but you can't change the default user name "super."

How to Enter "About Us" Information

The next button on the Settings menu allows you to create "About Us" information. Note that in the screenshot we've included the Settings menu to keep you oriented.
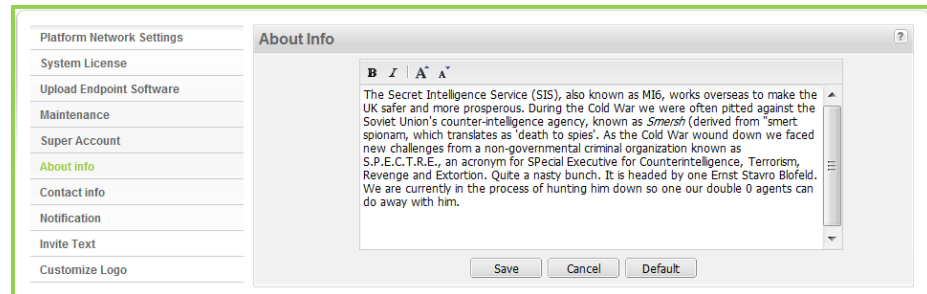
The About Info page enables you to create and format an About Us page that appears when users click the About Us link at the bottom of the VidyoPortal home page and the VidyoPortal Admin and Super Admin pages. The About Info text box provides a tool bar to apply bold and italic formatting and change the point size.

Note: Because of a limitation of Adobe Flash, URLs can be inserted into the text but they must conform to HTML 1.1 specifications.

1. Enter text or paste text you have copied from another application.

2. Apply any formatting desired.

3. Click the Save button

Warning: The following task cannot be undone.

1. If you wish to destroy the custom About Info text and revert to the default text supplied by Vidyo, click the Default button.
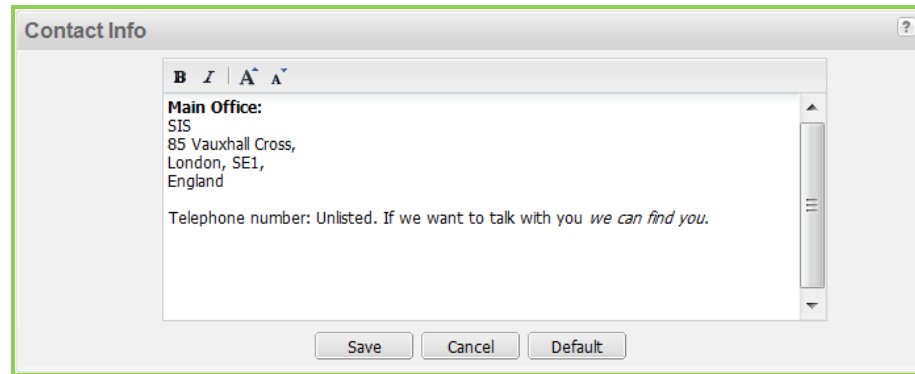
   Since there is no confirmation dialog box, it's a good idea to keep a copy of any customized text you have in a separate text file somewhere convenient in case you click the Default button by accident.

   Note: The About Us page you create at the Super Admin level can be overridden at the tenant level by Tenant Admins.

How to Add And Edit Contact Info

Below the About Info button is the Contact Info button.

The Contact Info page enables you to create and format a contact page that appears when users click the Contact info link at the bottom of the VidyoPortal home page and the VidyoPortal admin and Super Admin pages, as well as the login page. This is information your users need to contact the VidyoPortal Super Administrator.

Note: Because of a limitation of Adobe Flash, URLs can be inserted into the text but they must conform to HTML 1.1 specifications.

1. Enter text or paste text you have copied from another application.

2. Apply any formatting desired.

3. Click the Save button
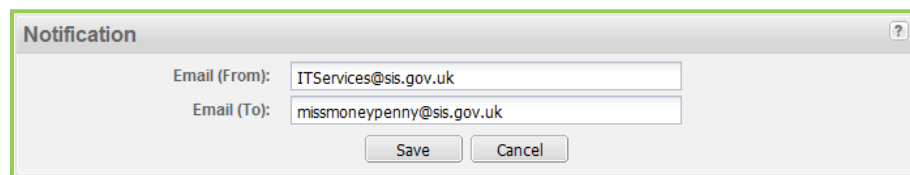
Warning: The following task cannot be undone.

1. If you wish to destroy the custom Contact Info text and revert to the default text supplied by Vidyo, click the Default button.

Note: The contact information page you create at the Super Admin level can be overridden at the tenant level by Tenant Admins.

How to Set up Notification Information

Next on the Settings left-hand menu is the Notification button.

The Portal provides some automated information. The "From" address you enter is used for automated emails sent out by the portal, such as confirmations to new users of their accounts, and so on. If you don't set a "From" address some SMTP servers may block emails.

You can elect to have status updates about the Vidyo system sent to an IT staff person in your organization. The "To" address should be the email address of the person who should receive alerts for action required by the portal.

1. Enter valid email addresses in the From and To fields.

2. Click the Save button

Note: The notifications you create at the Super Admin level can be overridden at the tenant level by Tenant Admins.

How to Create Invite Text

Next on the Settings left-hand menu is the Invite Text button.

The Invite Text page enables you to create the boilerplate email messages sent by users to invite guests to attend meetings in their rooms.

There are three kinds of invitations.

- **Email Content** text is sent for Vidyo Conferences.

- **Voice Only** text is sent to those who will participate in voice-only mode via telephone.

- **Webcast** text is sent to invite people to participate in a webcast.

    This option will be visible only if your system has the optional VidyoReplay server.

As with the other informational text boxes in the Settings section you can use the text as is or modify it as you wish. If you decide to delete the default text and replace it with new text it's important for you to understand how to use the two green buttons in the upper right hand corner of the page.

1. Click the button to insert a [ROOMLINK] placeholder for the link to the user's room.

    When the user creates an email invitation, the VidyoPortal automatically enters the correct URL. This placeholder is required.

2. Click the ☎ button to insert an [EXTENSION] placeholder for the dial-in number and extension (if an extension has been set) needed to dial into the user's room (and optionally, a PIN required to enter the room).

    When the user creates an email invitation, the VidyoPortal automatically inserts the correct extension (and PIN, if the user has chosen to require one). This placeholder is optional.

3. Click Save to save the message.

Warning: The following task cannot be undone.
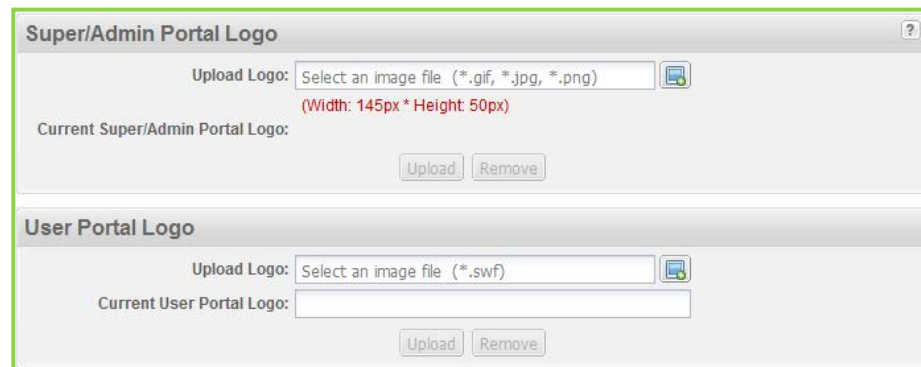
1. If you wish to destroy all custom invitations and revert to the default text supplied by Vidyo, click the Default button.

    Since there is no confirmation dialog box, it's a good idea to keep a copy of any customized text you have in a separate text file somewhere convenient in case you click the Default button by accident.

Note: The invitation message you create at the Super Admin level can be overridden at the tenant level by Tenant Admins.

Users can also edit the invitation text you (or their Tenant Admins) create on this page before sending them out. For instance, if a meeting will take place at some time in the future, they'll want to include the date and time of the meeting.

How to Customize The System Logos

You can upload your organization's logo to customize and brand your VidyoConferencing system.

The Super/Admin Portal Logo is used for customizing the logo for the Super Admin and Tenant Admin pages. The uploaded logo must be **145 x 50** pixels and can be in the `.gif`, `.jpg` or `.png` formats.

The User Portal Logo uploaded by the Super Admin is the default logo for each tenant User Portal page. But the logo can be customized for all User Portal pages.

Each Tenant Admin can upload a different logo for each User Portal. The uploaded logo should be **150 x 50** pixels and it should be in the `.swf` format. (The `.swf` file extension originally stood for ShockWaveFlash, from which it was originally derived. Adobe subsequently changed its meaning to "small web format." Go figure.)

The `.swf` format is vector-based as opposed to a bitmap so it allows the logo to dynamically resize for different screen resolutions and window sizes. That means the exact size of the logo is less important than the

aspect ratio. No matter what size your logo image is make sure it's at a 3:2 aspect ratio. If you use a logo with different proportions it'll be stretched or squeezed.

In the User Portal, the custom logo replaces the Vidyo logo in the top left corner of the page, and a VidyoPower logo appears in the bottom right corner.

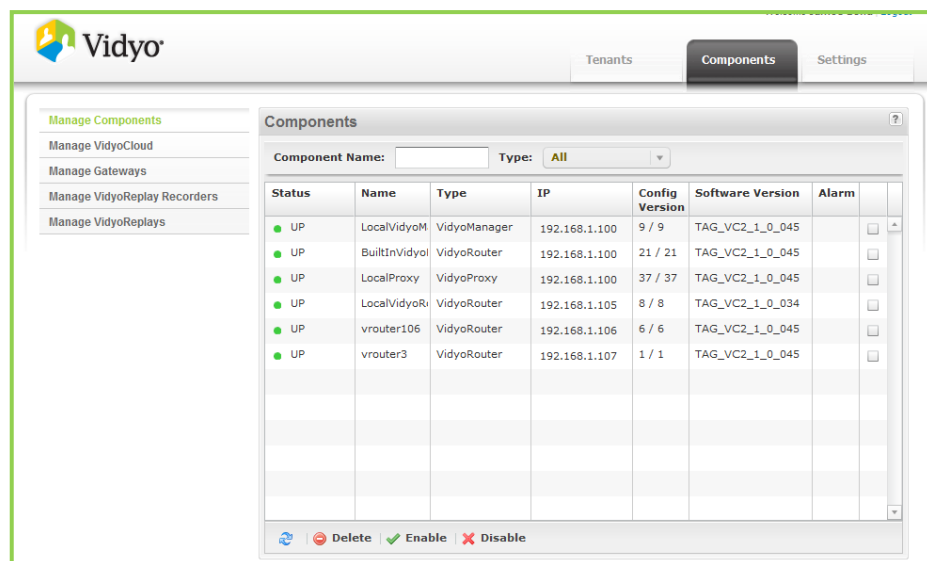The logo in current use appears under the Upload Logo field.

Vidyo provides a service for converting logos to `.swf` format. Please contact your reseller or Vidyo Customer Support for details.

Components are the (software and/or hardware) devices that enable your Vidyo system to operate. You can add components to your system to give it added capabilities or capacities, such as connecting to a legacy conferencing system. You must register these components with your VidyoPortal in order for them to work with your VidyoConferencing system. The Components tab enables you to add the following components:

- **VidyoManager** – The software component necessary to the functioning of the VidyoPortal. *Do not perform any tasks on the VidyoManager other than those described below or on specific instructions from Vidyo Customer Support.*

- **VidyoRouter** – Routes video and audio streams between endpoints and intelligently identifies and adjusts to bandwidth and network constraints. One VidyoRouter is built into every system (we call it the embedded or local VidyoRouter) and you can purchase additional routers (we call them standalone VidyoRouters) to increase call capacity.

- **VidyoProxy** – A software component through which all inbound and outbound traffic is channeled to traverse a firewall.

- **VidyoGateway** – An optional component that connects the VidyoPortal to legacy conferencing systems and landlines and cell phones (for voice-only participation).

Overview Of The Components Table

When you click the Manage Components navigation tab the Components table opens. You can drag and drop the columns to arrange them in the order you prefer. The table contains eight columns:

Status – A component can be in one of four states.

- A green dot in the status column means it's installed and operating.

- A yellow dot means the component is new, i.e., it's been installed but has not been completely configured yet.

- A red dot means the component isn't working. Hover your mouse pointer over the alarm sign in the Alarm column to read the alarm message.

- A gray dot means the component is disabled. This means an admin has taken the device offline, perhaps to perform maintenance.

Name – When you install a component you must give it a descriptive name, which is displayed here.

Type – This column displays the type of component, as described in the preceding section.

IP Address – The IP address assigned to the component.

Config Version – This version is not to be confused with the Software Version, which is the next column. This column shows the *Configuration* Version. Every time you change some aspect of a component's configuration it increments the version number on the left side of the slash character. The system polls each component for its status and configuration version every 15 seconds. So in no more than 15 seconds after you change a component's configuration, the number on the right side of the slash should increment also. In other words, if you haven't made a change in the last 15 seconds, the numbers on both sides of the slash character should be the same.

Software Version – This is the actual software version this component is running.

Alarm – If a component is not working properly you'll see the yellow alarm symbol in this column. Hover your mouse button over it to read a brief description of the fault.

Select Checkbox – Select this box to take an action on the selected component. At the bottom of the screen you can see the actions you can take: Delete, Enable or Disable.

Also at the bottom of the screen on the left-hand side is the Refresh button. You'll see it on many screens throughout the Admin and Super Admin pages. Click it to ensure you are viewing the current status of the information displayed on the screen.

 If you double click on the Status indicator of a component you'll open a screen where you can configure various aspects of the component. If you single click on the component's IP address a local configuration login page opens so you can make further changes.

For more information on these components see:

- VidyoManager Configuration on page 42.
- VidyoRouter Configuration on page 48.
- VidyoProxy Configuration page 65.
- The VidyoGateway Guide (a separate manual included with your documentation suite if you've purchased this optional component).

Each component's configuration is set and stored in the portal's database, and pushed to a component upon saving its settings.
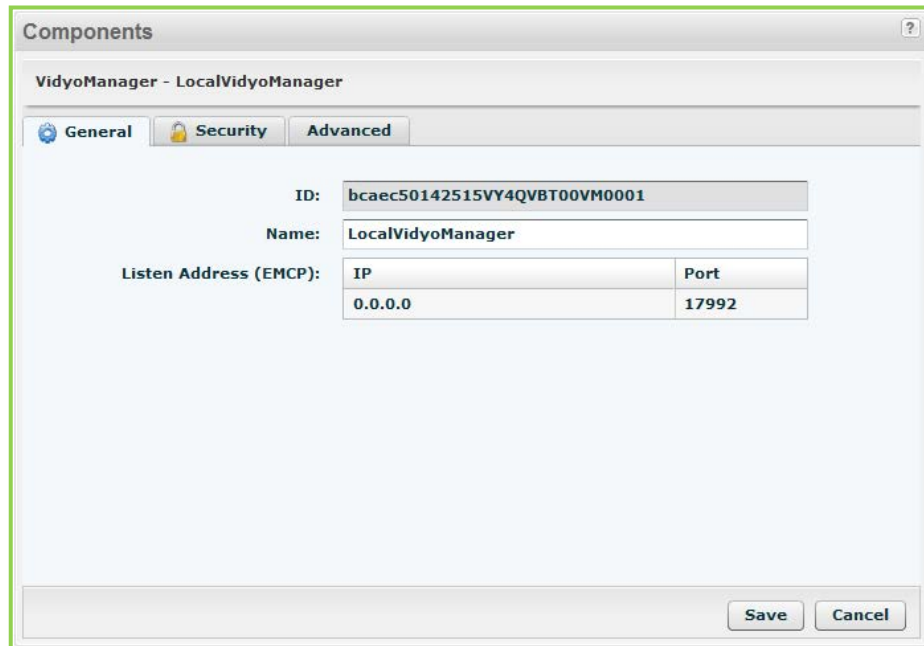
- You can access the configuration pages of each registered component by double clicking the Status, Name or Type of the component entry line on the Components page.
- You can access the component's own local webpage configuration screen by clicking on its IP address in the IP column. (The first page you'll see will be the component's log-in page. Log in as an *Admin*, not Super Admin.)

HOW TO CONFIGURE YOUR VIDYOMANAGER

To configure the VidyoManager, double-click on its line to access the VidyoManager's configuration page.

VidyoManager General Tab

ID – The VidyoManager ID is automatically created and set by the system; you can't change it.

Name – Is the display name, or label, for the VidyoManager.

Listen Address (EMCP) – The EMCP address and ports are used by VidyoDesktop, VidyoRoom and Vidyo-Gateway clients to communicate with the VidyoManager. Do not change this address unless required for NAT traversal or enabling Security. Refer to the Security Appendix on page **149** and Firewall and NAT Deployments on page **129** before editing the EMCP settings.

VidyoManager Security Tab
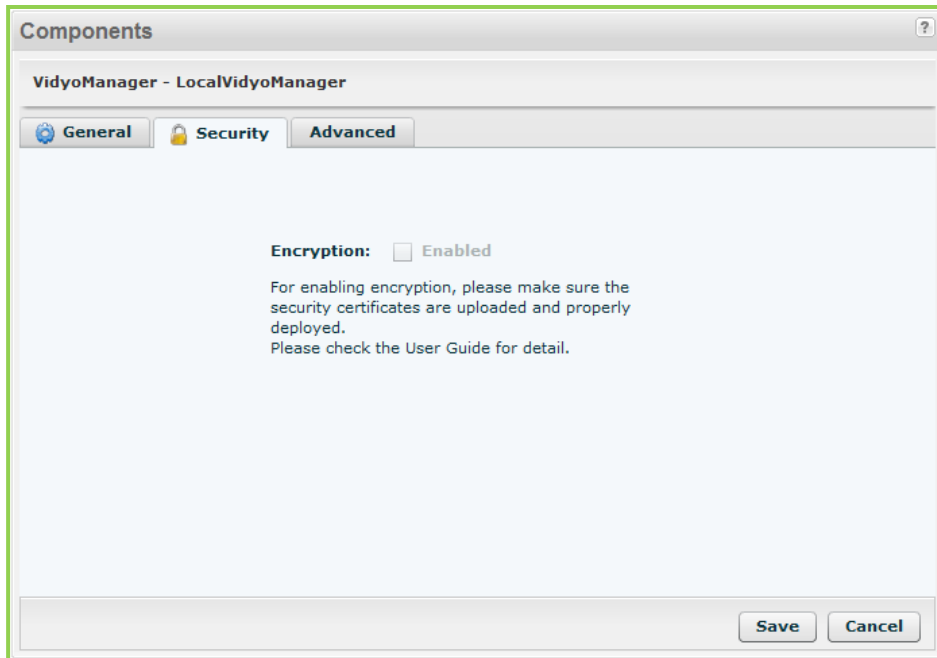
Select the Enabled checkbox to enable TLS (Transport Layer Security) security for the VidyoManager. Additional configuration is required. (If the Encryption checkbox will not accept a click, like the one shown above, it's because your portal doesn't have the proper encryption.) For information about enabling end-to-end security for your VidyoConferencing system, see the Security Appendix on page **149**.

Click the Save button to save the setting.

VidyoManager Advanced Tab
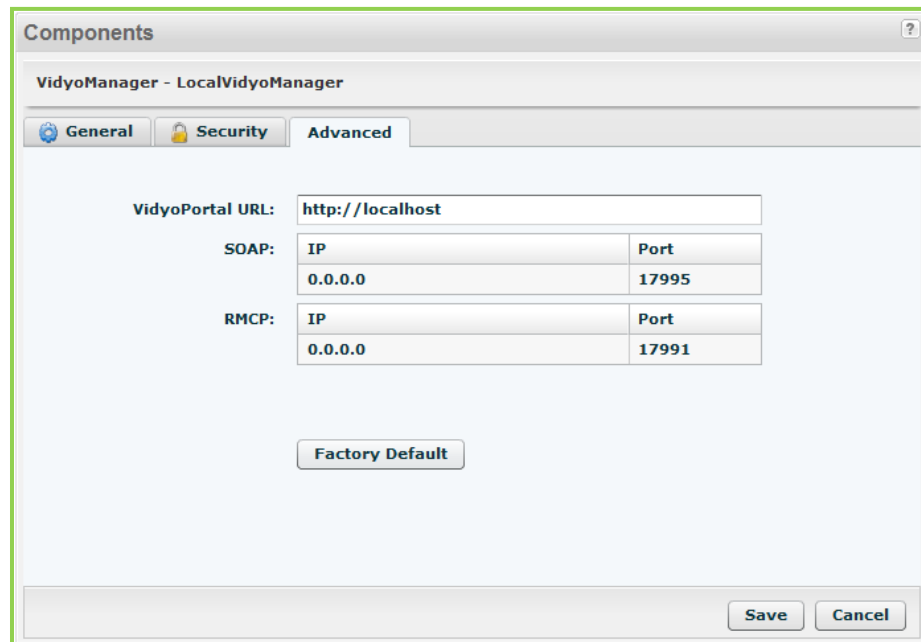
The VidyoManager Advanced setting should be changed only upon direction of Vidyo Customer Support.

- **Connect Address** – Specifies the address the VidyoManager uses to communicate with the VidyoPortal. Do not change this address.

- **SOAP** – This information determines how the portal communicates with the VidyoManager.

- **RMCP** – The RMCP address and port is used by the VidyoRouter to connect to the VidyoManager.

- **Factory Default** button – Click this to return the VidyoManager settings to their factory defaults.

THE VIDYOMANAGER CONFIGURATION PAGE

Like the VidyoRouter and VidyoProxy, the VidyoManager has its own set of configuration pages. But unlike the other two components, the VidyoManager configuration are mostly for checking its configuration rather than changing it.
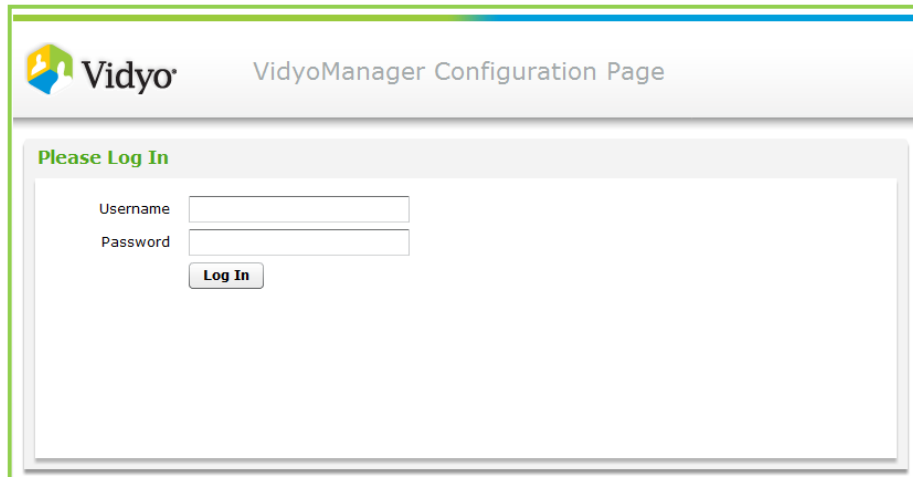
To log into your VidyoManager launch your browser and enter its address to:

`http://<URL or IP>/vm2conf/`

Log in using the default Administrator account:

- User Name: `admin`

- Password: `password` (case sensitive)

Note: Although the default username for this page is "admin," in the normal course of business only the Super Admin accesses these pages.

Note: An alternative route to this page is to click on the IP address of the VidyoManager in the Components page.

VidyoManager Basic Tab

The Config Server field tells the VidyoManager (and other components) where to look for their configuration information. Generally, "localhost" is the content that is entered in the field, although it could also contain the IP address or URL of your portal. Do not change this address unless required for NAT traversal or enabling Security. Refer to Firewall and NAT Deployments on page **129** and the Security Appendix on page **149** before editing the Config Server settings.

VidyoManager System Tab
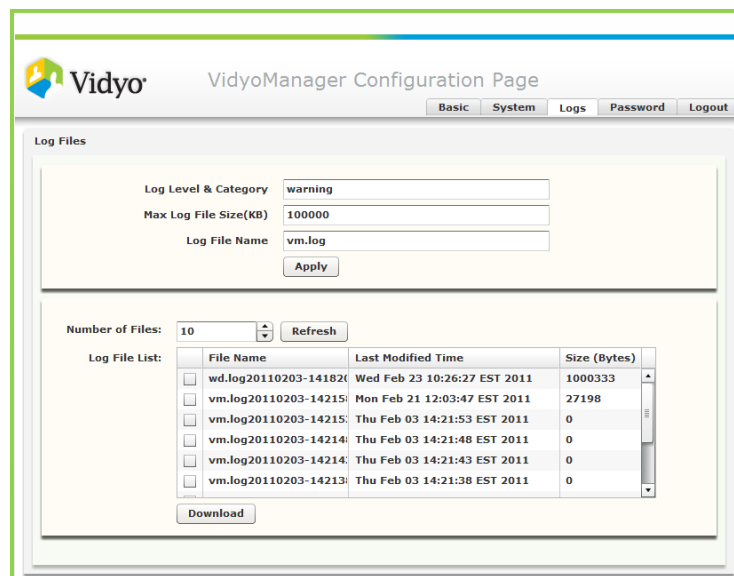
On the System tab, you can view the network settings for the VidyoManager.

VidyoManager Logs Tab

Generally, you need not change anything on the Logs tab. The default settings keep the last ten 1-MB log files. To troubleshoot a problem, Vidyo Customer Support may ask you to download one or more log files. Clicking the Download button creates a zip file you can save on your desktop and attach to an email you send to Vidyo.

VidyoManager Password Tab

This tab enables you to change your password. You'll need to enter your current password first and enter your new password twice for confirmation.

VidyoManager Logout Tab

Clicking the Logout tab opens a dialog box that asks you to confirm your intent to logout of the VidyoManager.
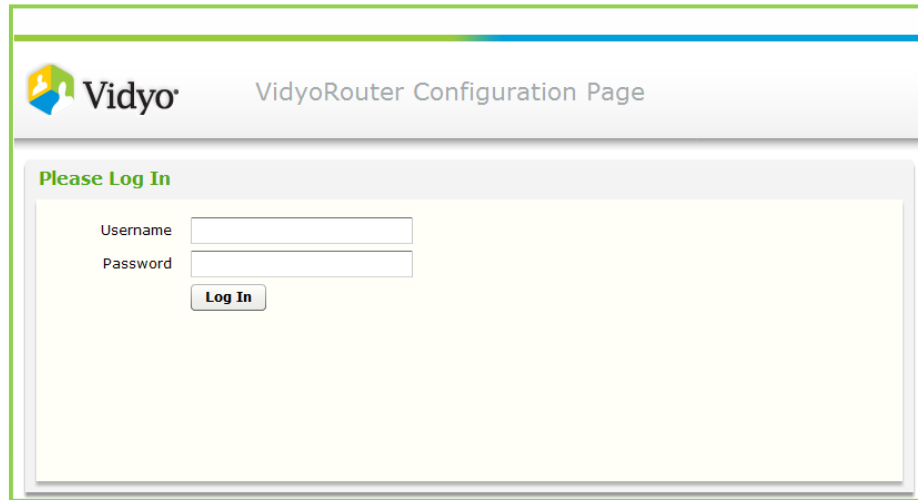
HOW TO CONFIGURE YOUR VIDYOROUTER

Your VidyoRouter transports video and audio streams between endpoints. It also intelligently identifies and adjusts to bandwidth and network constraints.

The embedded (local) VidyoRouter is pre-configured at the factory. Edit the embedded VidyoRouter configuration only if guided to do so by Vidyo Customer Support for more advanced configurations.

Stand-alone (additional) VidyoRouters, however, do need some configuring. In order to do so, you first have to leave the Components tab (or you can leave it open and open another tab in your browser) to do one quick configuration setting on the VidyoRouter Configuration Page.

To log into your embedded or standalone VidyoRouter, launch your browser (or open a new tab) and enter its address:

`http://<URL or IP>/vr2conf/`
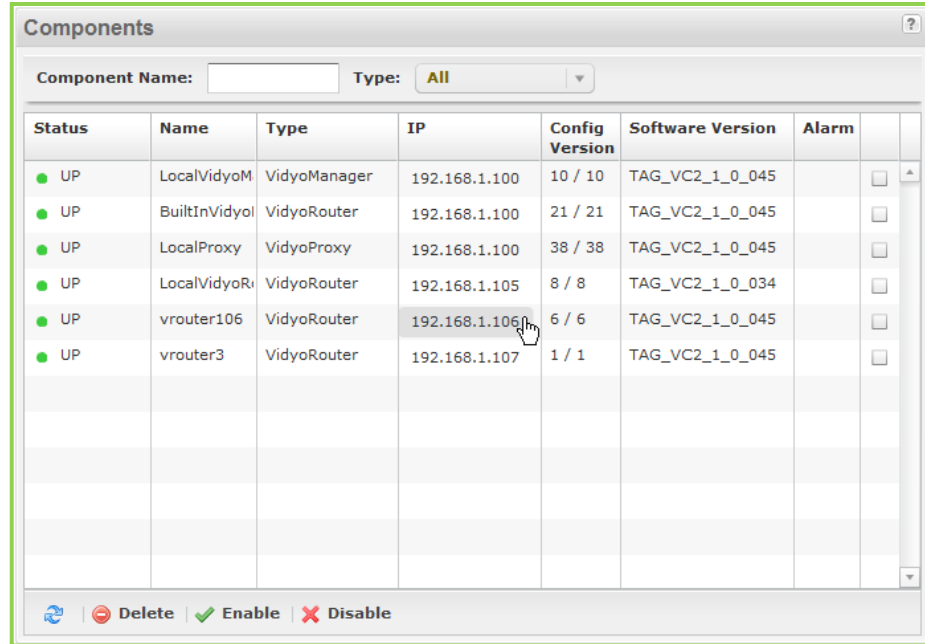
Log in using the default Administrator account:

- ■ User Name: `admin`
- ■ Password: `password` (case sensitive)

Note: Although the default username for this page is "admin," in the normal course of business only the Super Admin accesses these pages.

Note: An alternative route to this page is to click on the IP address of the VidyoRouter in the Components page.

The VidyoRouter Configuration Page opens set to its Basic tab.

The only task you *must* do for every external VidyoRouter is to tell it where to find its Config Server.

The Config Server field tells the VidyoRoute where to look for its configuration information. For the local embedded VidyoRouter "`localhost`" is the Config Server. For standalone routers it's the IP address or URL of your portal.

1. Enter the VidyoRouter's IP Address.
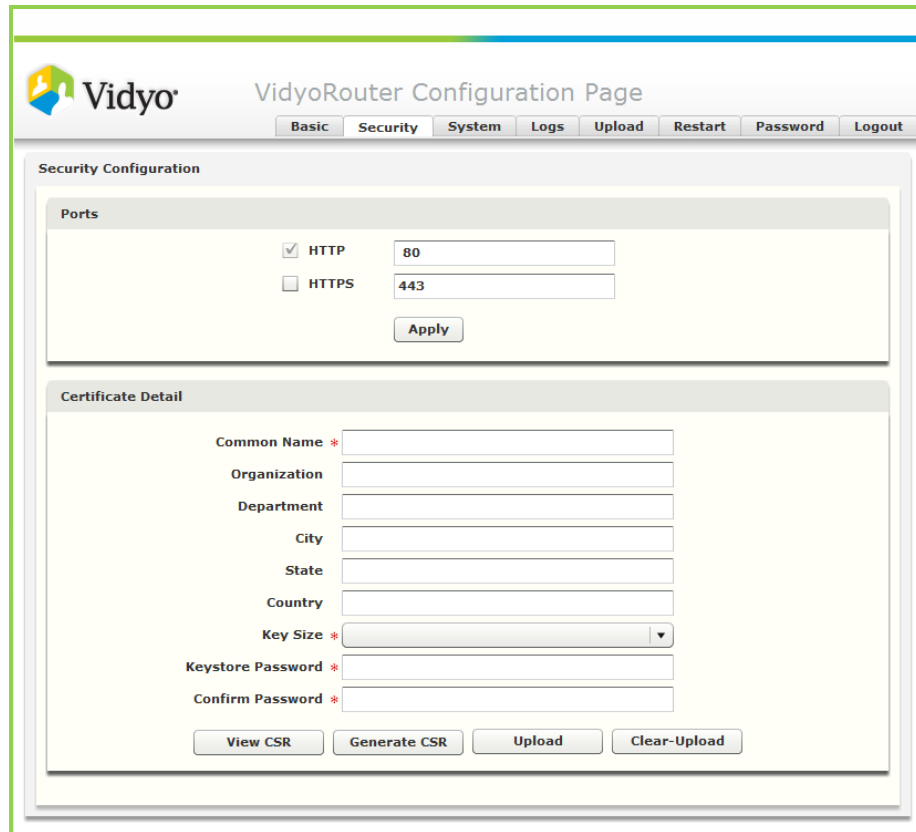
   Remember this is only for additional routers. The embedded VidyoRouter should already be set to localhost and you should not change it.

2. Click the Apply button for the VidyoRouter to register.

That's all you really have to do on this page (and then only for external routers). But as long as we've moved to the VidyoRouter Configuration Page we might as well go over the other tabs. There's not a lot you must do with the other tabs.

VidyoRouter Security Tab
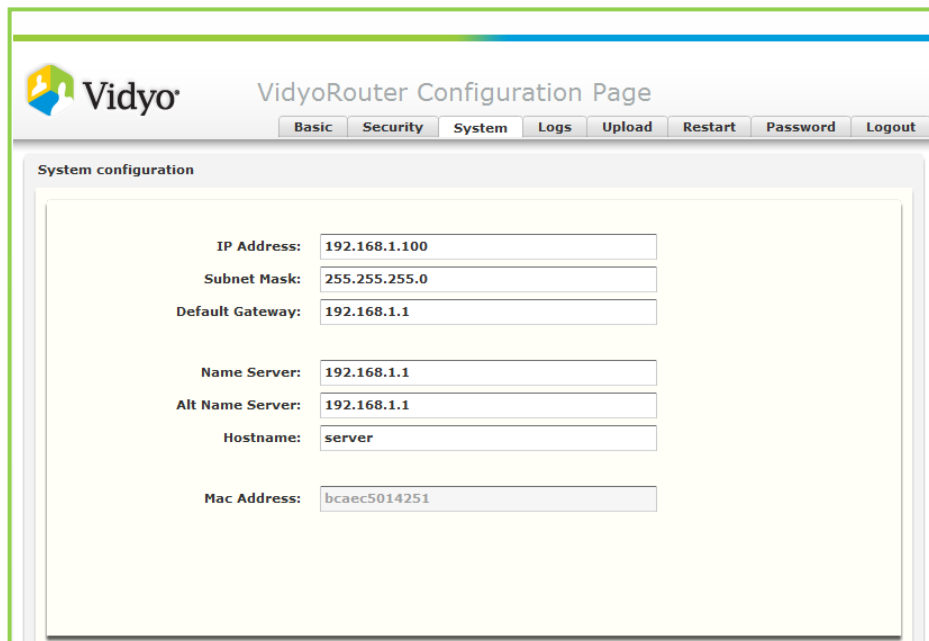
Entering information on this tab is optional. For detailed information on using VidyoRouter security refer to the Security Appendix on page **149**. Don't change any of the information for the embedded VidyoRouter. Its settings are configured in the Super Admin pages.

VidyoRouter System Tab

The text in the fields of the System tab are read-only. This page serves as a convenient summary of basic system information.

VidyoRouter Logs Tab

The system logs events in a succession of log files. Normally you won't have to concern yourself with this. Vidyo Customer Support personnel may ask you to download one or more logs (to your desktop) and then attach them to an email to send to Vidyo Customer Support when they're troubleshooting a problem for you.

VidyoRouter Upload Tab

Warning: Upgrades cannot be rolled back.

Warning: When the system is restarted or shut down all calls in progress are ended.

You might want to email users ahead of time and perform the upgrade when system usage is lowest.

10. VidyoRouter Configuration

The sole button on the Upload tab says it all. You use this tab to upload and upgrade the VidyoRouter software. When you receive a new version of the software from Vidyo, this is the page you come to apply the upgrade.

Note: The embedded VidyoRouter is upgraded automatically when the portal is upgraded. Use this page only to upgrade standalone routers using the appropriate version. VidyoRouter upgrade filenames look like this: `TAG_VC2_1_X-VR.vidyo`.

VidyoRouter Restart Tab
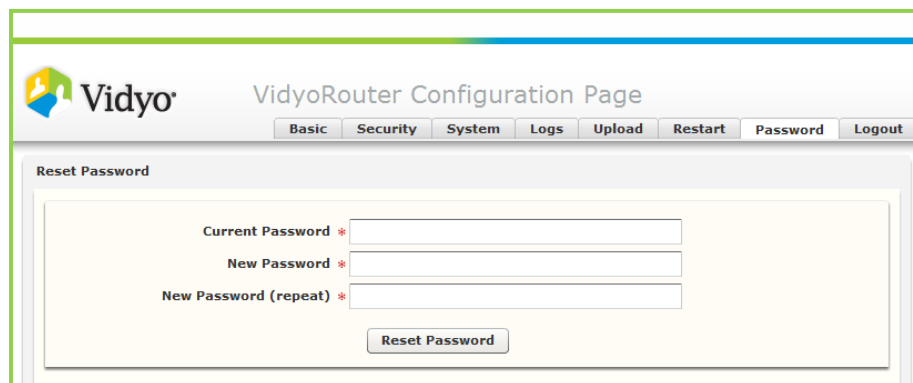
This tab enables you to restart or shutdown your VidyoRouter. You're required to enter your username and password before you can do either.

Warning: Once the server shuts down you can power it back up only by physically pressing the power button on the front of the unit.

Warning: When the system is restarted or shut down all calls in progress are ended.

You might want to email users ahead of time and perform the upgrade when system usage is lowest.

VidyoRouter Password Tab

This tab enables you to change your password. You'll need to enter your current password first and enter your new password twice for confirmation.

VidyoRouter Logout Tab

Clicking the Logout tab opens a dialog box that asks you to confirm your intent to logout of the VidyoRouter.

Meanwhile Back on The VidyoRouter Page under the Components › Manage Components Tab

As you'll recall, we started out on the VidyoRouter page under Manage Components. To recap, we started from here:
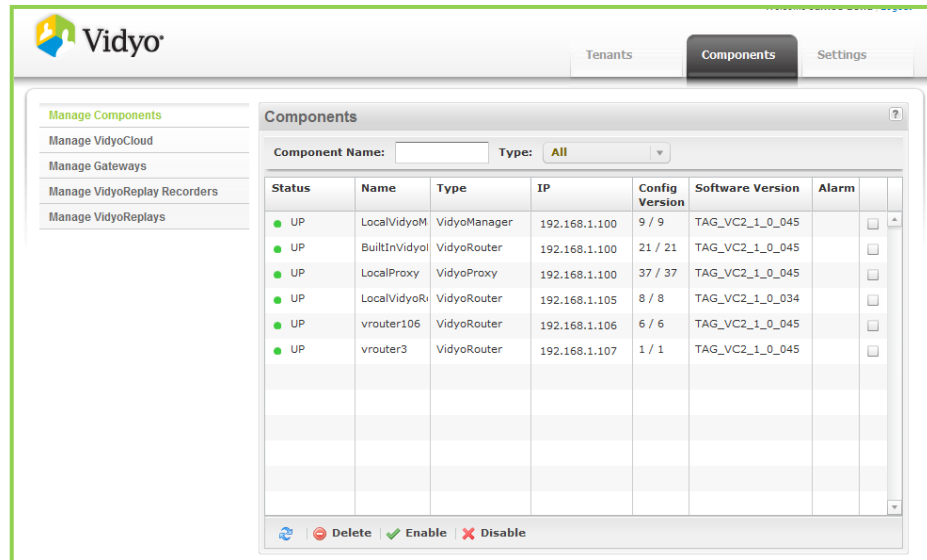
To configure a VidyoRouter, double-click anywhere on its line in the table *but* its IP address to access the VidyoRouter's component configuration.

Note: As you complete each task be sure to click the Save button before moving to the next tab.

Vidyorouter General Tab
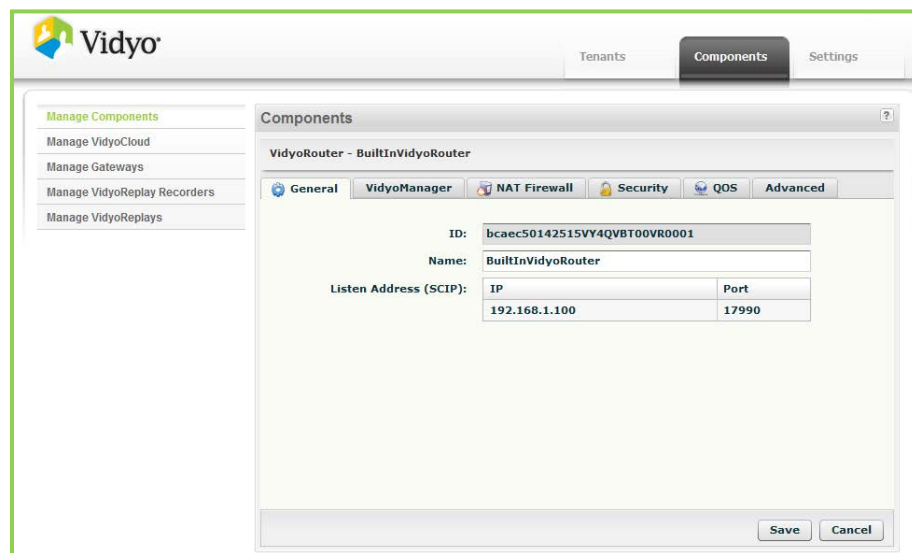
ID – The VidyoRouter ID is automatically created and set by the system; you can't change it.

Name – Is the display name, or label, for the VidyoRouter.

1. Enter a name for your VidyoRouter.
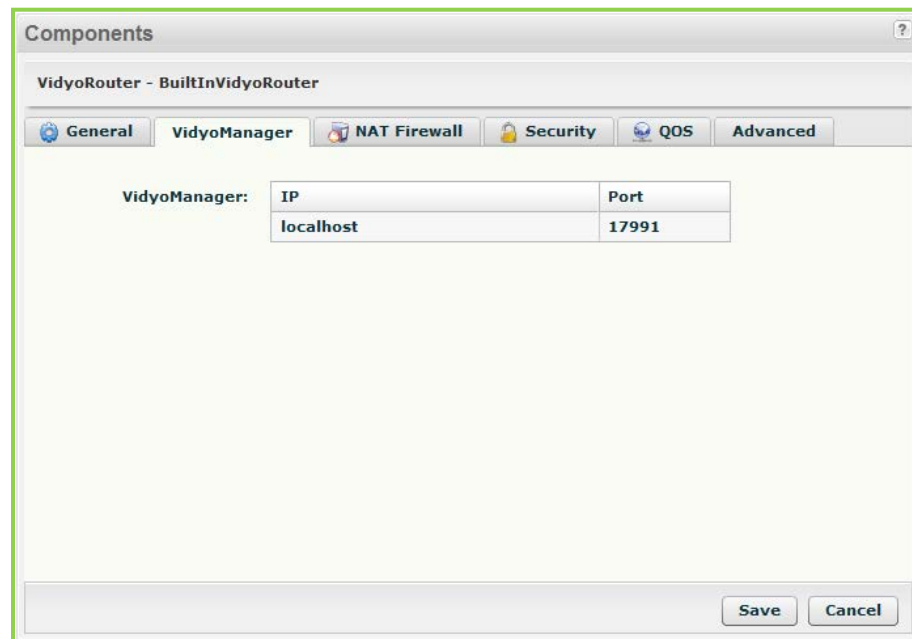
This is the minimum required to authorize a Standalone VidyoRouter. It's a good idea to name your routers in a way that will help you remember their locations, like NYC VidyoRouter 1, NYC VidyoRouter 2 and so on.

SCIP Listen Address – The IP and port VidyoDesktop, VidyoRoom and VidyoGateway clients use to communicate with the VidyoRouter using Vidyo's proprietary network protocol. This is the listening address of the VidyoRouter. The address 0.0.0.0 means to bind to all Ethernet ports.

- Don't change this address unless required for NAT traversal or enabling Security.

  Refer to Firewall and NAT Deployments on page **129** and the Security Appendix on page **149** before editing the SCIP settings.

VidyoRouter VidyoManager Tab

VidyoManager – This is the address the VidyoRouter uses to communicate with the VidyoManager. Change this setting only if you're using full portal security as outlined in the Security Appendix that starts on page **149**.

VidyoRouter NAT Firewall Tab

This page is used for traversal of a NAT when the portal/VidyoRouter is hosted behind a NAT. Please refer to Firewall and NAT Deployments on page **129**.

STUN Server Address – If the system is NATed without a 1:1 port mapping, you must configure the VidyoRouter to use a STUN server residing on the WAN side for network traversal.

1.   Enter its IP address and port number here.

A STUN server generally uses port 3478.

Note: The Media Address Map feature is the preferred configuration option. Choose only one option; enabling both options will cause the system to malfunction.

Media Address Map – If the system is NATed with a 1:1 port mapping, hence no port translation, you can define local ‹·› public address mappings.

2.   Enter the local and remote IP address for each mapping.

The remote IP address is the IP address the system is NATed to from the side users connect from.

Media Port Range – Enables you to define a range of ports available in a firewall.

3.   Select or enter the Start and End port numbers.

OR

3.   If only one port is available, enter the same port number in each field.

VidyoRouter Security Tab
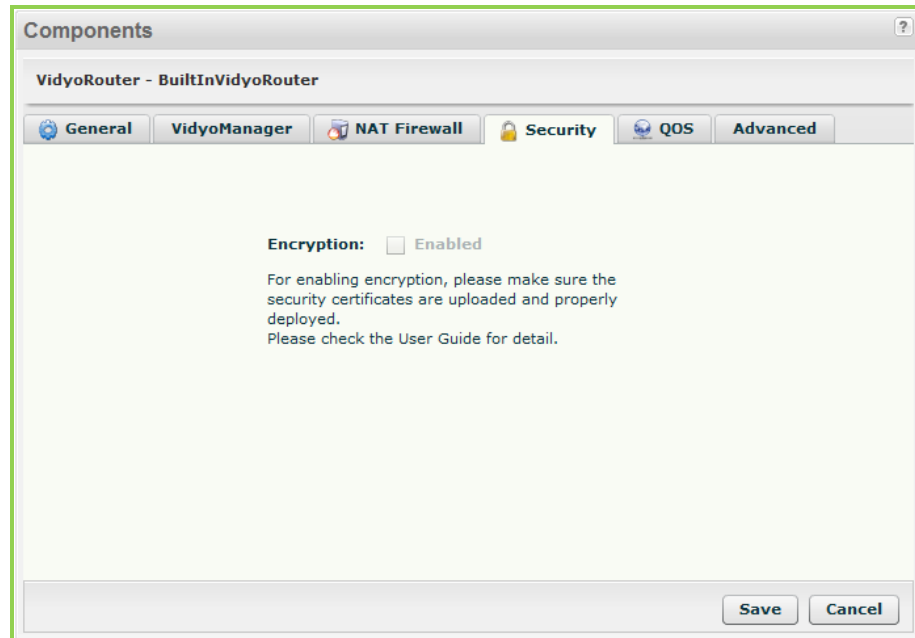
Encryption –

1. Select the Enabled checkbox to enable TLS (Transport Layer Security) security for the VidyoManager.

    (If the Encryption checkbox will not accept a click, like the one shown above, it's because your portal doesn't have the proper encryption license.) For information about enabling end-to-end security for your VidyoConferencing system, see the Security Appendix that starts on page 149.

2. Click the Save button to save the setting.

VidyoRouter QOS Tab
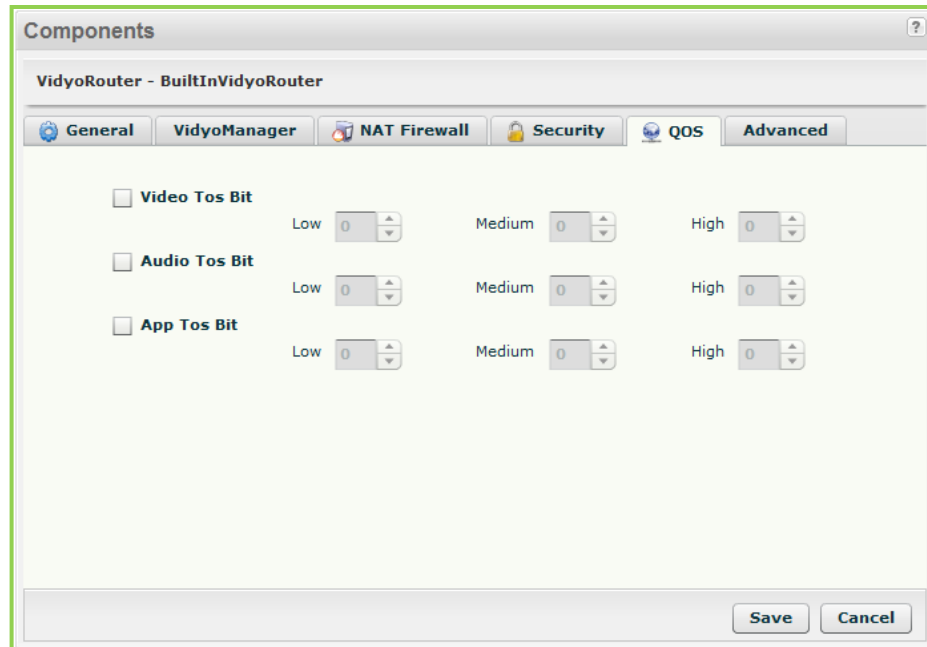
Video Tos Bit/Audio Tos Bit/App Tos Bit – Enables you to assign video, audio and application packets a low, medium or high priority.

1. Enter or select a value that specifies the Tos bit for each priority level, Low, Medium and High.

Note: We recommend setting QoS policies on the network equipment using IP policies rather than here.

VidyoRouter Advanced Tab
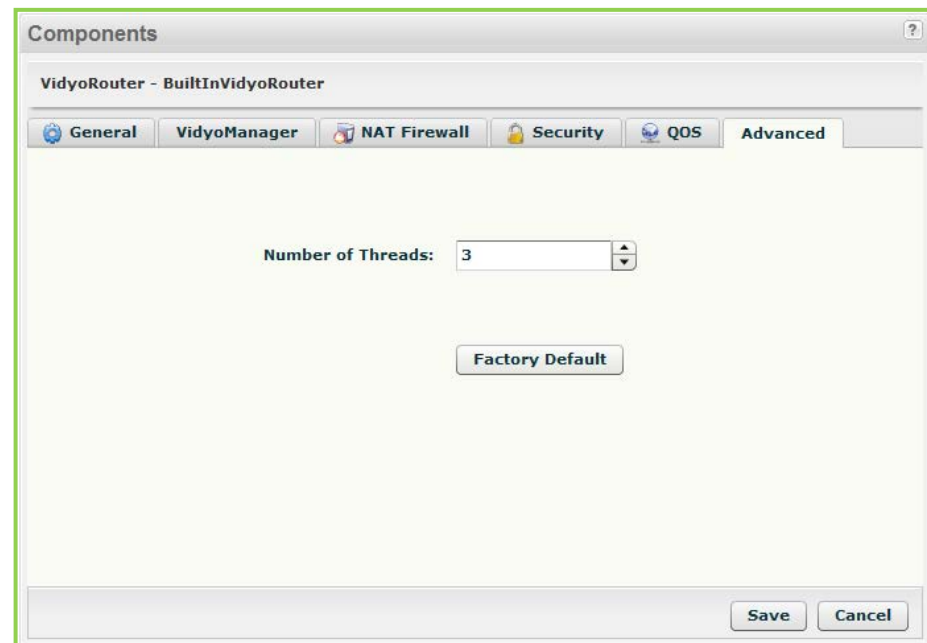
Number of Threads – Sets the number of threads (or CPU cores) the VidyoRouter will use on the server. The Default is three threads.

■   Change this to four threads only for stand-alone Routers NOT running VidyoProxy.

■   For any VidyoRouter running alongside the portal, VidyoManager, or VidyoProxy, this setting should remain set to three threads.

Repeat these steps for each VidyoRouter in your system.

After you've configured your VidyoRouters you can place them into pools for optimum usage.
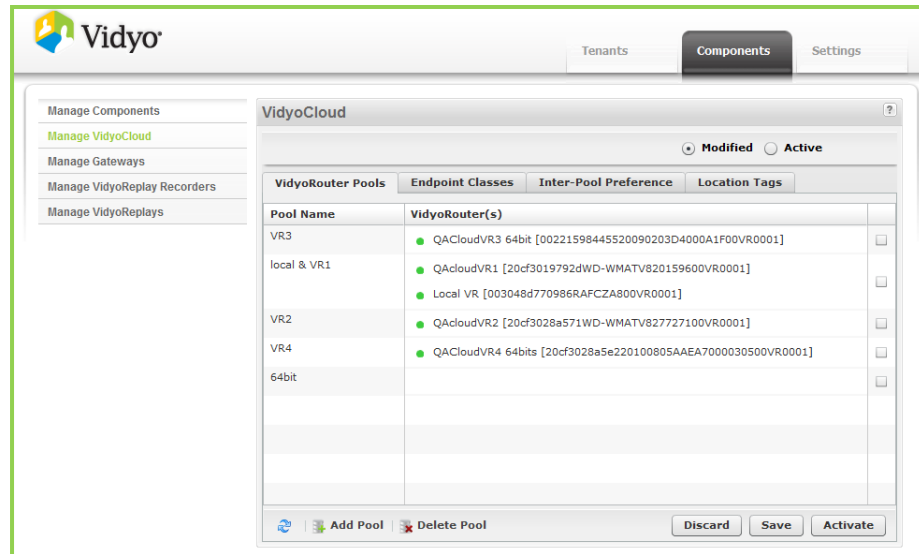
VidyoRouter Pools

A VidyoRouter can handle up to 100 simultaneous active users. If you need additional capacity you can purchase additional VidyoRouters. If you do, you can group them into "pools." Typically you might do this to group sets of VidyoRouters that are near each other geographically (e.g., group your American-based VidyoRouters in one pool and your European-based VidyoRouters into another pool). Another reason might be to reserve one or more VidyoRouters to a certain group of users in your organization (e.g., top level management).

- A VidyoRouter can be in only one pool.

- A pool can contain one or more VidyoRouters.

- If you have only one VidyoRouter it's still in a pool.

- Multiple VidyoRouters in a pool provide failover across the pool.

With the VidyoRouter Cloud Edition capability now included with your VidyoConfererencing system you can use VidyoRouter Pools more efficiently than ever before. For more information see Using VidyoRouter Cloud Edition starting on page 111.

Warning: Changes to the Network, like creating or deleting VidyoRouter pools, require a system restart.

You might want to email users ahead of time and perform the upgrade when system usage is lowest.

How to Create a VidyoRouter Pool

1. Log in to the Super Admin Portal.

2. Click the Components tab on the top navigation bar.

3. Click Manage Vidyo Cloud on the left-hand menu.

    Notice the option button labeled Active in the upper right-hand corner. More on that in a moment.
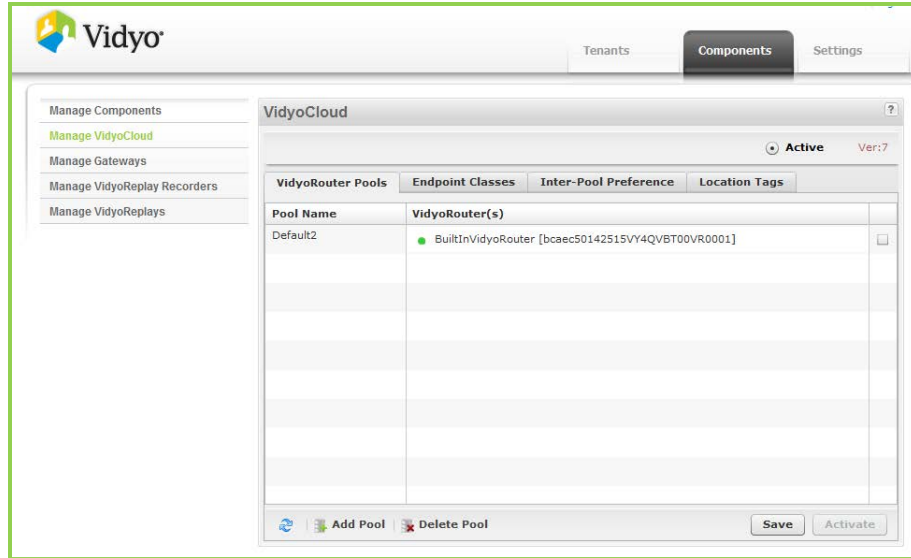
4.   Click the Add Pool button.

The Vidyo Cloud Table opens, with the VidyoRouter Pools tab selected.
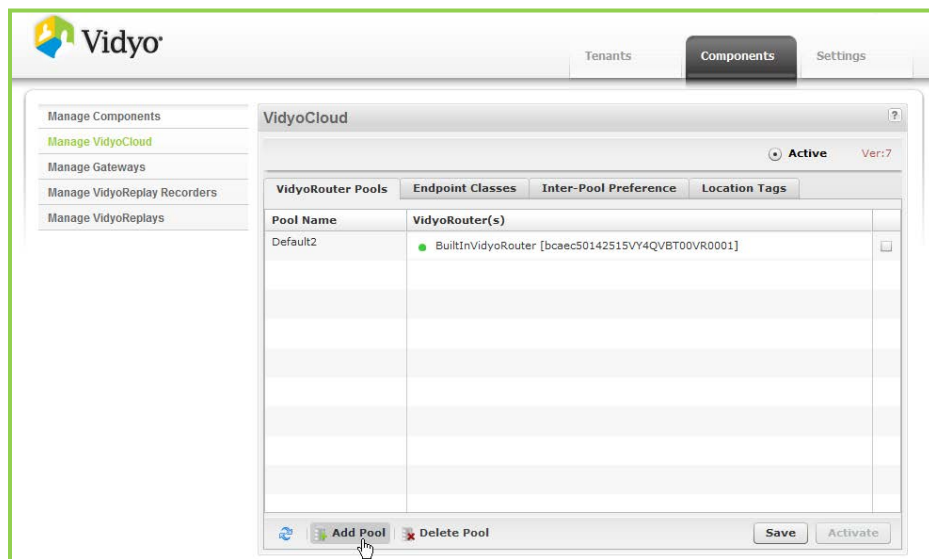
5.   Click the Add Pool button at the bottom of the page.
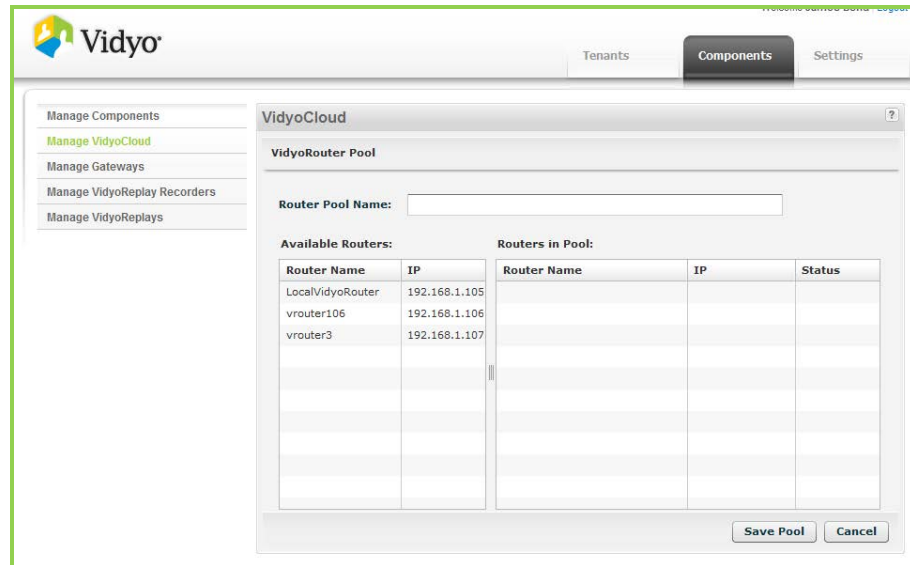
The VidyoRouter Pool table opens. All of your available routers will be listed in the Available Routers section in the table.
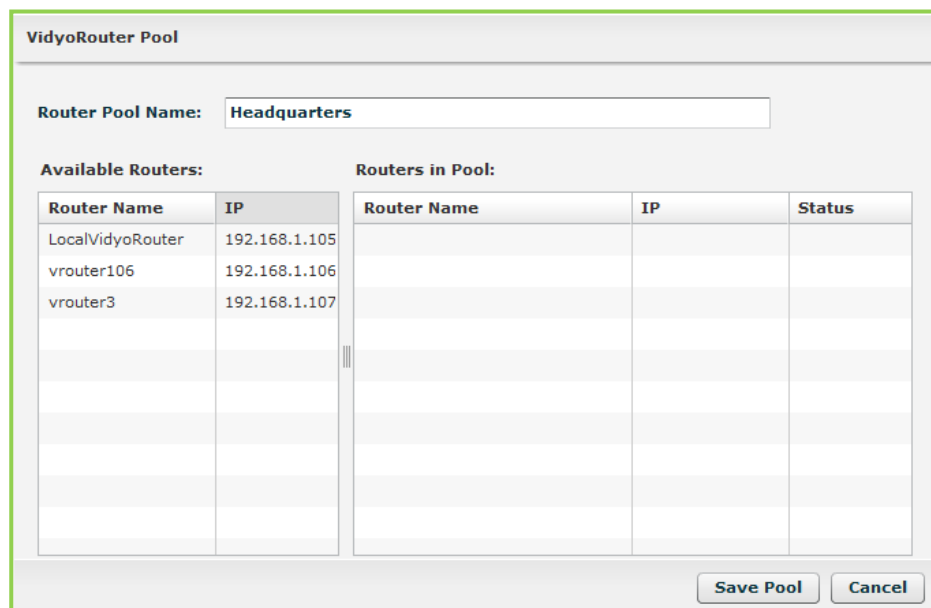
6. Enter a name for the pool you're creating in the Router Pool Name field.

    It's a good idea to use pool names that will remind you where they're located or their purpose, like "New York," "Paris" or "Board Members" and so on.

7. In the Available Routers section point to a VidyoRouter in the Router Name column and drag and drop it to the Router Name column in the Routers in Pool section.
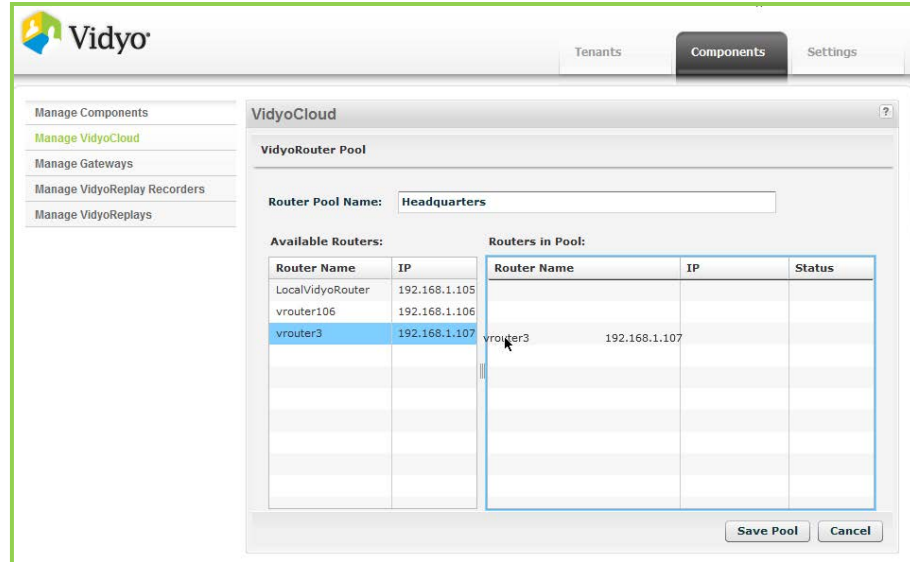
8. Repeat this process for each VidyoRouter you wish to add to this pool.

9. When you're done click the Save Pool button.

   The following information dialog box appears:
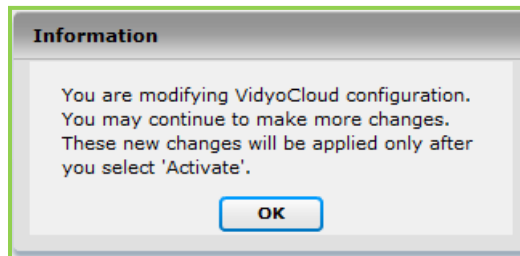
   Note that the main image behind the dialog box is blurred and the Activate button has now been joined by a Modified button.
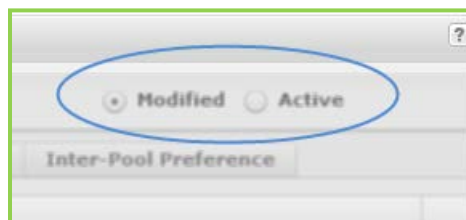
   This is to remind you that by starting to change the configuration you are now working on a modified version of the system.

10. Click the OK button

   You'll be returned to the Vidyo Cloud table. The original configuration remains unchanged for now. If you need to interrupt what you're doing to say, deal with an urgent matter, you could click the Save button and your modified version will be saved but your current configuration would not be disturbed. Later you could come back and continue working until you are ready to activate your changes.

11. Click the Activate button to activate all of your changes.

You'll first see this dialog box:

Confirmation

Activating modified VidyoCloud configuration
will disconnect active conferences, continue?

Yes   No
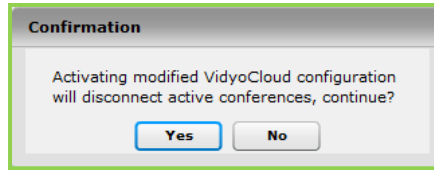
This is reminding you that modifying the system requires a restart. That's a good reason to warn your users when you're going to do maintenance and to do it when your system usage is lowest. After you click OK you'll see yet another dialog box:

Information

VidyoCloud configuration activated. Please allow
a couple of minutes for new configuration to
take effect.

OK
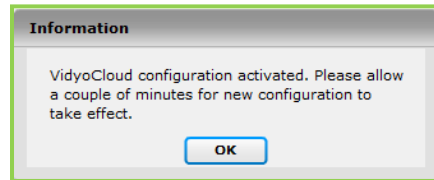
This is just reminding you that the system takes a few minutes to restart. If more than a couple of minutes go by with no apparent change try clicking your browser's Refresh button.

Adding Additional Routers

■ When you want to add additional routers to a pool open the Vidyo Cloud table and double-click the pool's name. You add additional routers in the same way you added the first one.

How to Remove a Router From a Pool

1. Open the Vidyo Cloud table

2. Double-click the name of the pool the router is in.

This will open the VidyoRouter Pool table.

3. Simply drag and drop the router's name from the Router Name column in the Routers in Pool section on the right to the Available Routers section on the left.

You can then add the VidyoRouter to another pool if you want to. This operation merely removes the VidyoRouter from the pool it was in. All of the VidyoRouter's configuration information remains intact.

How to Delete an Entire Pool
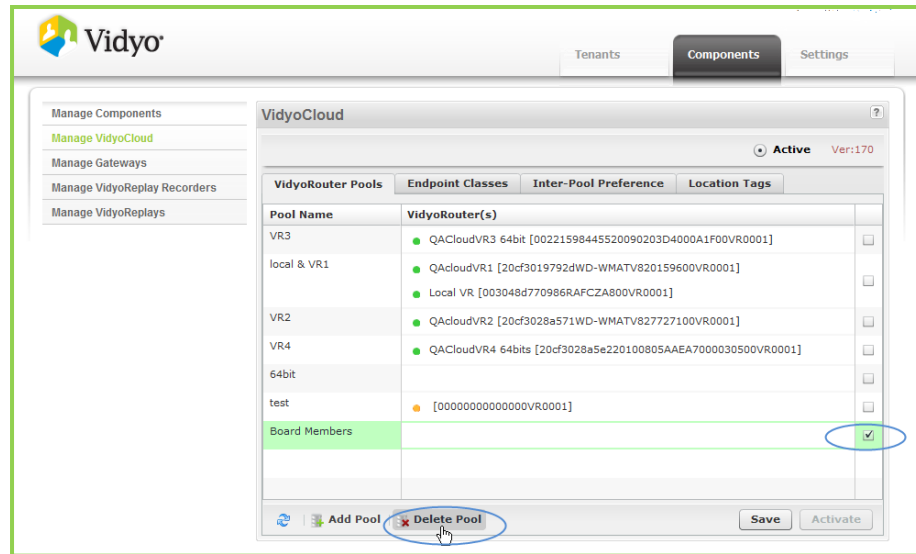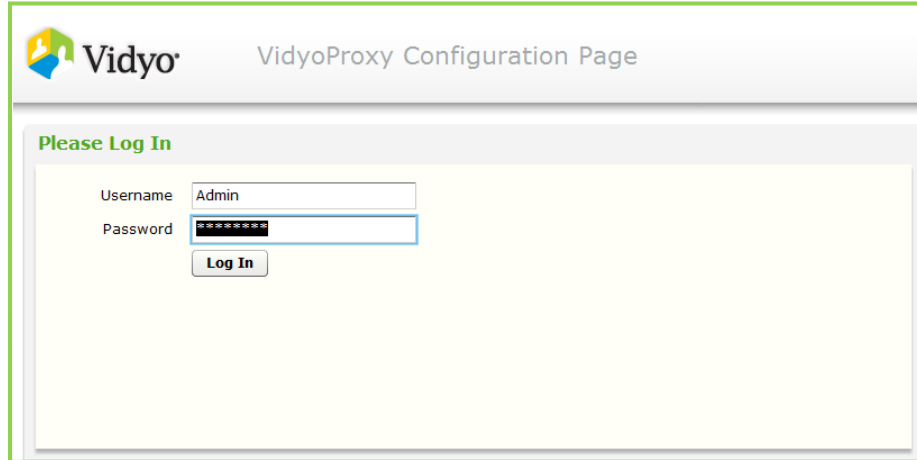
1. Open the Vidyo Cloud table.

2. Click the checkbox to the right of the pool(s) you wish to delete.

3. Click the Delete Pool button below the table.

4. Confirm your decision to delete the pool in the dialog box that opens.

Note: Deleting a pool does **not** delete the configuration information of any routers that were in the pool.

HOW TO CONFIGURE YOUR VIDYOPROXY

In order to configure a VidyoProxy you first have to leave the Components tab (or you can leave it open and open another tab in your browser) to do one quick configuration setting on the VidyoProxy Configuration Page.

To log into your embedded or standalone VidyoProxy, launch your browser (or open a new tab) and enter its address:

`http://<URL or IP>/vp2conf/`

Log in using the default Administrator account:

- User Name: `admin`

- Password: `password` (case sensitive)

Note: Although the default username for this page is "admin," in the normal course of business only the Super Admin accesses these pages.

Note: An alternative route to this page is to click on the IP address of the VidyoProxy in the Components page.

Configuring your VidyoProxy is very similar to configuring your VidyoRouter. Once you log into your VidyoProxy you again see the Basic tab open.

Note: For technical reasons there are no Help buttons on these configuration pages, so it's a good idea to have this manual open on your screen or have a print-out of it handy when you perform the tasks described here.

VidyoProxy Basic Tab
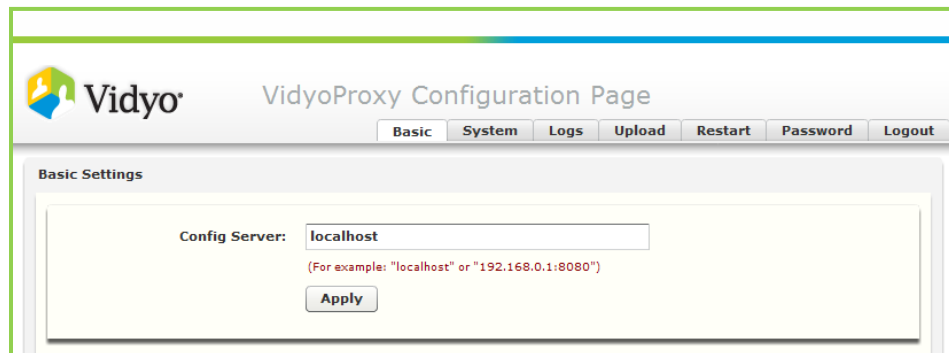
- The Config Server field tells the VidyoProxy (and other components) where to look for their configuration information. For the local embedded proxy "localhost" is the config server. For a standalone proxy it's the IP address or URL of your portal. Click the Apply button for the Proxy to register.

Note: Do not change this address on the embedded VidyoProxy unless required for NAT traversal or enabling Security. Refer to Firewall and NAT Deployments on page **129** and the Security Appendix on page **149** before editing the Config Server settings.

VidyoProxy System Tab

- In the System Configuration section of the System tab, you can view the network settings for the VidyoProxy.

VidyoProxy Logs Tab

- Generally, you need not change anything on the Logs tab. The default settings keep the last ten 1-MB log files. To troubleshoot a problem, Vidyo Customer Support may ask you to download one or more logs files. Clicking the Download button creates a zip file you can save on your desktop and attach to an email you send to Vidyo.

VidyoProxy Upload Tab

Note: Actually you're unlikely to need to use this page because the VidyoProxy is automatically updated with a portal or router update.

Warning: Upgrades cannot be rolled back.

Warning: When the system is restarted or shut down all calls in progress are ended.

You might want to email users ahead of time and perform the upgrade when system usage is lowest.

VidyoProxy Restart Tab
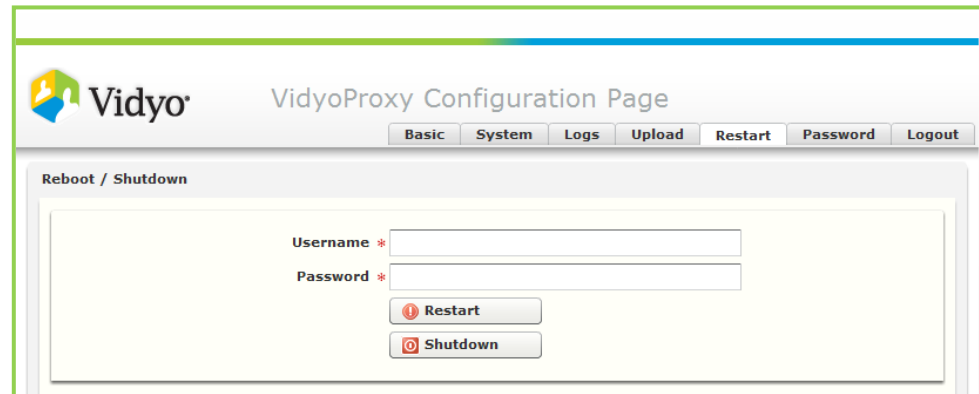
- This tab enables you to restart or shutdown your VidyoProxy. You're required to enter your username and password before you can do either.
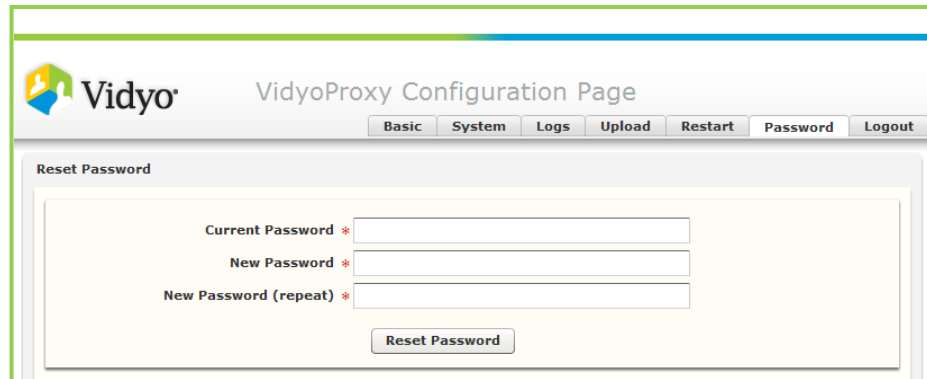
Warning: Once the server shuts down you can power it back up only by physically pressing the power button on the front of the unit.

Warning: When the system is restarted or shut down all calls in progress are ended.

- You might want to email users ahead of time and perform the upgrade when system usage is lowest.

VidyoProxy Password Tab

■   This tab enables you to change your password. You'll need to enter your current password first and enter your new password twice for confirmation.

VidyoProxy Logout Tab

■   Clicking the Logout tab opens a dialog box that asks you to confirm your intent to logout of the VidyoProxy.

Meanwhile Back on The VidyoProxy Page under Components > Manage Components Tab

VidyoProxy General Tab

ID – The VidyoProxy ID is automatically created and set by the system, it cannot be changed.

Component Name – Is the display name, or label, for the VidyoProxy.

1.   Enter a name for your VidyoProxy.

This is required to authorize a VidyoProxy running on a stand-alone VidyoRouter.

URL – The IP or URL address and port the VidyoProxy will listen on.

2. Enter either the IP address or FQDN/URL of the server followed by a colon and the port the proxy should use.

FQDN/URL must be used for servers hosted behind a NAT or when using encryption. Refer to Firewall and NAT Deployments on page **129** and the Security Appendix on page **149**.

For additional detail on the VidyoProxy, refer to the VidyoProxy Appendix on page **141**.

Note: Default VidyoProxy configuration is `localhost:443`. Users will not be able to use the VidyoProxy until you've changed the localhost string to the IP or FQDN of the VidyoProxy.

HOW TO MANAGE VIDYOGATEWAYS

If your organization has purchased a VidyoGateway be sure to read the VidyoGateway Operations Guide that was included with it. This section is meant to be a convenient quick guide to the VidyoGateway.

To recap, a VidyoGateway is the optional component that permits legacy devices like MCUs, and ordinary landline and cell phones to participate in videoconferences. (Telephones can send and receive only the audio portion of the teleconference.)

The Manage Gateways page enables you to add and delete VidyoGateways from your system.
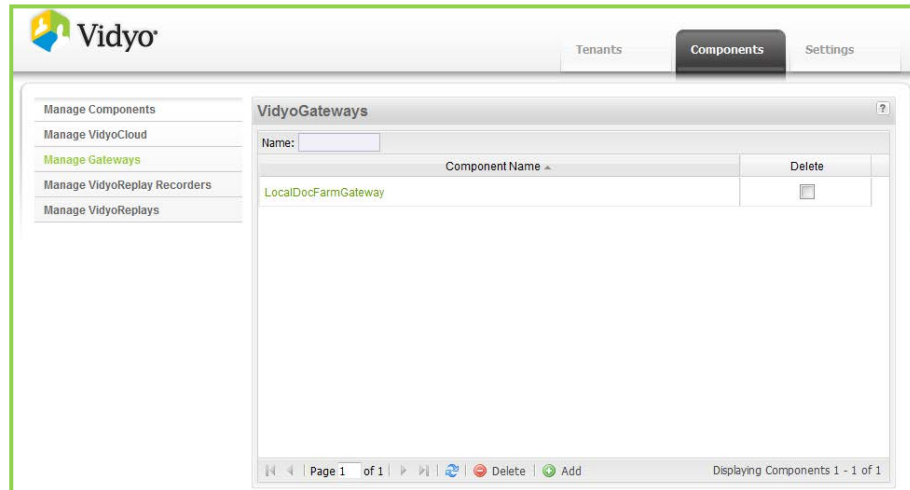
To add or edit a Gateway click the Add button at the bottom of the page. The Add Component: New VidyoGateway page opens.
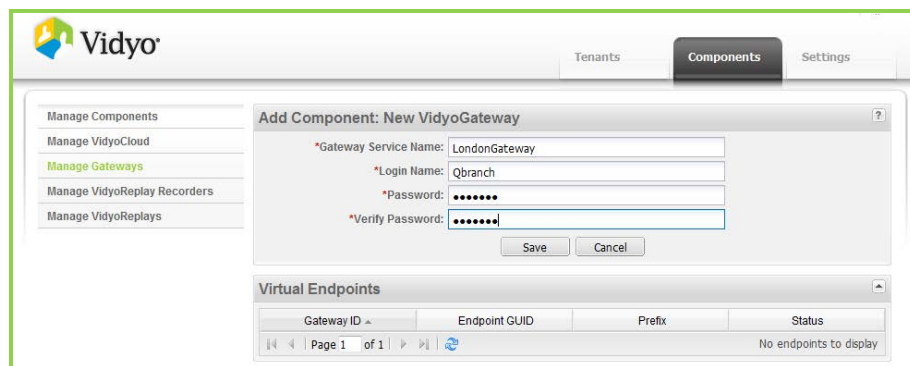
Enter the required fields:

1. **Gateway Service Name** – Enter a descriptive name for the gateway.

2. **Login Name** – Enter the login name the gateway will use to register and authenticate with the portal.

3. **Password** – Enter the password the gateway will use to register and authenticate with the portal and verify it.

4. Click the Save button

Once the Gateway registers, you will see its list of configured services listed in the Virtual End-points table.

- To refresh the table, click the Refresh button.

- To scroll through any pages of listed services, click the Page direction arrows.

- To delete an existing Gateway select the checkbox in the far right column then click the Delete button at the bottom of the page.

- For more comprehensive information on configuring and using VidyoGateways, refer to the Vidyo-Gateway Operation Guide (a separate manual included in your documentation suite if your organization has licensed VidyoGateway).
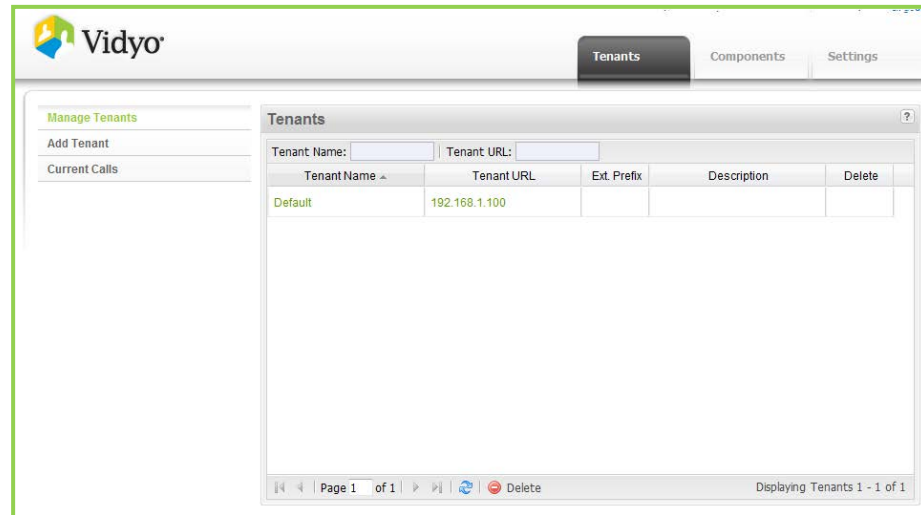
Every Vidyo system has at least one tenant, called the *default* tenant. If your VidyoConferencing System is licensed for multi-tenant mode, you can create multiple tenants.

Tenants are configured at the Super Admin level so you must be logged in as a Super Admin.

Note: You must set up tenants *after* you have configured the settings and components for your VidyoPortal system. If you have not yet configured system settings and components, configure them before attempting to add any tenants.

Overview Of The Tenants Table

HOW TO ADD A TENANT

There are a maximum of nine steps to adding (and configuring) a tenant. Some steps can be skipped if your installation or the tenant you're configuring has not licensed certain capabilities.

1. Basic Tenant Settings

2. Permit Cross-Tenant Access

3. Assign VidyoManager Components

4. Assign VidyoProxy Components

5. Assign VidyoGateway Components (Skip if VidyoGateway is not being used.)

6. Assign VidyoReplay Recorders (Skip if VidyoReplay is not being used.)

7. Assign VidyoReplay Components (Skip if VidyoReplay is not being used.)

8. Assign Location Tags (See the Managing the VidyoRouter Cloud chapter that starts on page 111.)

9. Save the Tenant Configuration

How to Configure a Tenant

Note: In the following topic there are frequent references to the Left Arrow button and the Right Arrow button. This is what they look like:

Left Arrow button: ⬅ Right Arrow button: ➡
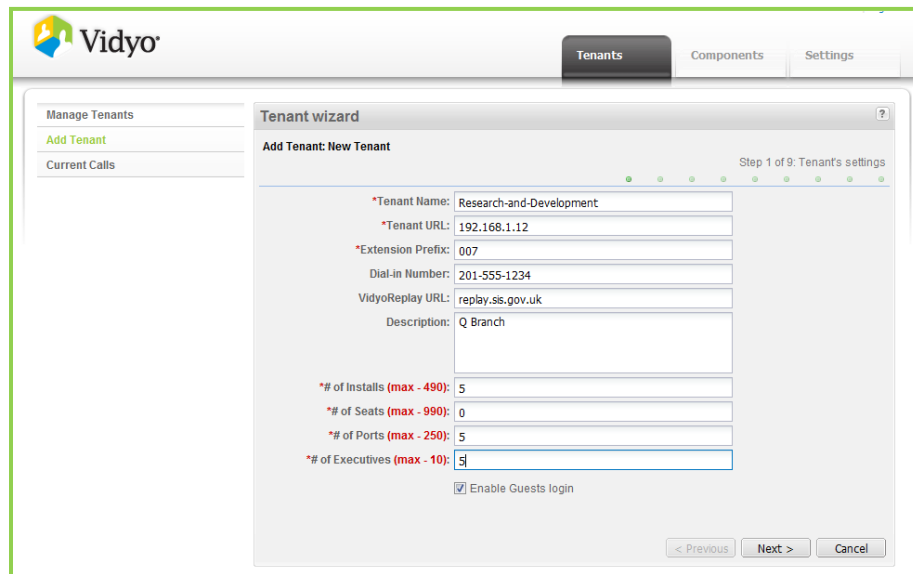
Perform the following procedure to configure the default tenant or to add a new tenant to your system. Even if you're using a multi-tenant system, set up the default tenant before setting up other tenants.

And remember, you must first log in as the Super Admin before configuring Tenants.

1. To configure the default tenant, click the Default name and perform the following steps.

    OR if your system is licensed for multi-tenant mode:

1. In the Tenants tab, click the Add Tenant link to display the first of nine pages of the tenant wizard.

2. Enter or edit the following information for the tenant:

    ■ **Tenant Name** – A unique name identifying the tenant.

      This name is displayed in the user directory and on the title bar of the client window when in a call.

      Note: Spaces are not valid characters.

    ■ **Tenant URL** – The FQDN or URL used by this tenant's users to access the portal.

      Note: If you have single-tenant system, you don't have to define the URL of the system, but we recommend you do since the URL enables the link to the Admin pages. You can also use your server's IP if it does not have a URL.

    ■ **Ext. Prefix** – A prefix added to extension numbers enabling multiple tenants to use the same extension numbers without conflict.

      An extension is not required unless you have multiple tenants. (This can be likened to an area code on the phone system.)

> **Note**: If you do create multiple tenants it's important to the proper functioning of the system that all tenants have extension prefixes with the *same number of digits*. If you assign the first tenant a two-digit extension prefix you should assign all other tenants two-digit extension prefixes. If you assign the first tenant a three-digit extension prefix, you should assign all other tenants three-digit extension prefixes and so on.

- **Dial-in Number** – The phone number that voice-only participants dial to access conferences

- **VidyoReplay URL** – If this tenant has the VidyoReplay option this is the URL this tenant's users go to use VidyoReplay. If VidyoReplay has not been licensed, entering information in this field has no effect,

- **Description** – A short description of the tenant for informational purposes.

- **# of Installs** – The number of endpoint software installations to allocate to the tenant.

  The total number of installs for all tenants cannot exceed the total number specified in the system license.

- **# of Users** – The maximum number of users this tenant can create.

  The total number of users for all tenants cannot exceed the total number specified in the system license. (If you're using the older Seats/Ports model enter the number of seats for this tenant.)

- **# of Ports** – The maximum number of ports allocated to the tenant.

  Ports are pooled among all tenants.

  Important: Allocate only as many ports to each tenant as needed. For example, if you have a 50-port license, you could allocate up to 50 ports per tenant, which would permit one or two tenants to consume all the ports, leaving none for other tenants.

- **# of Executives** – Executive Desktop users are a feature of the now standard VidyoLines licensing model. However, Executive Desktop licenses are purchased as separate licenses in your VidyoLines package. Each Executive Desktop has guaranteed system access. So if you purchase 100 VidyoLines and five Executive Desktops, then even when your system is at full capacity your five users with Executive Desktop privileges can still make calls.

- **Enable Guests login** – When selected, gives the tenant the option of allowing guest logins.

  When unselected, it prevents the tenant's users from allowing guest logins.

Cross-Tenant Access

3. Click the Next button to proceed to Step 2 of 9.

   If you have a multi-tenant system you can enable cross-tenant access for your tenants on this page. Cross-tenant access gives the users of one tenant the ability to place direct calls to and conference with users of another tenant.

   The list of available tenants appears in the Available Tenants list on the left.

4. To enable cross-tenant access, select one or more tenants in the Available Tenants list and click the Right Arrow button to move the tenant(s) to the Selected Tenants list.

   This allows the users of tenant you are configuring to call users in the Selected Tenants list. In order to allow the selected tenant's users to call the tenant being created or edited you need to repeat this process for each selected tenant. (In other words, the operation provides only a *one-way* ability to *initiate* calls.)
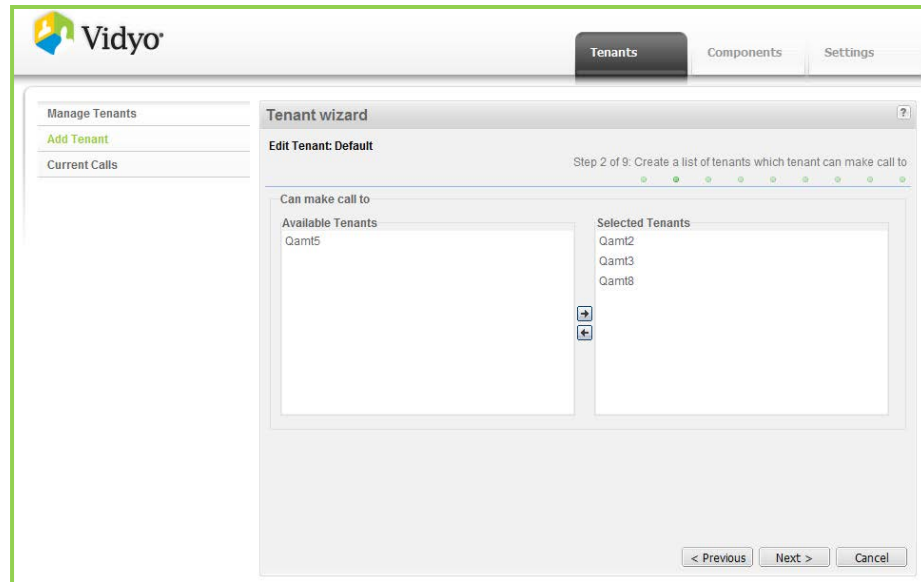
All tenants that appear in the Selected Tenants list are eligible for cross‑tenant access. You can move a tenant from the Selected Tenants list back to the Available Tenants list by selecting it and clicking the Left Arrow button.

VidyoManager Components

1. Click the Next button to proceed to Step 3 of 9.
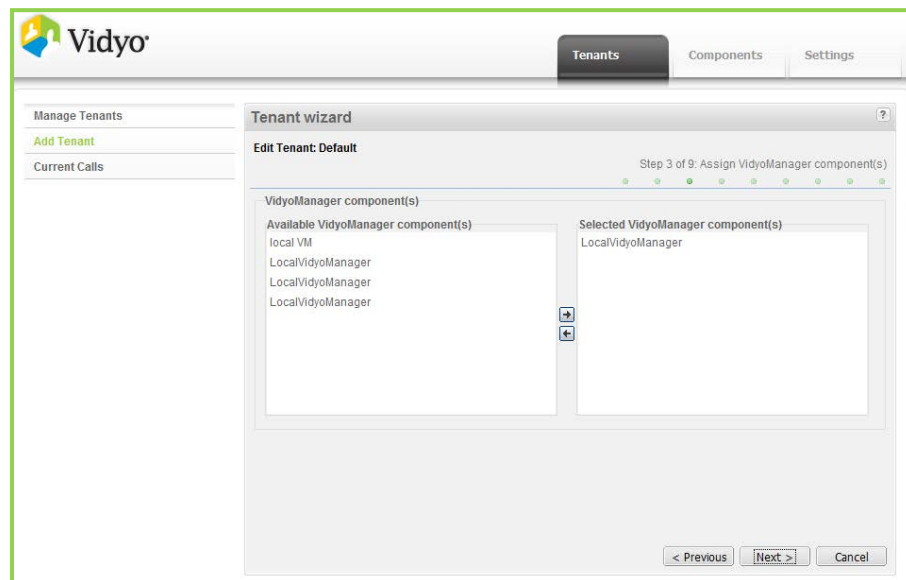
In this page, you can make available to the tenant the VidyoManager component you set up previously. The tenant admin can then choose among these components as necessary. You must make at least one VidyoManager component available to the tenant.

The list of available VidyoManagers appears in the Available VidyoManager component(s) list on the left.

2. To select a VidyoManager, select one or more in the Available VidyoManager component(s) list and click the Right Arrow button to move them to the Selected VidyoManager component(s) list.

VidyoProxy Components

1. Click the Next button to proceed to Step 4 of 9.
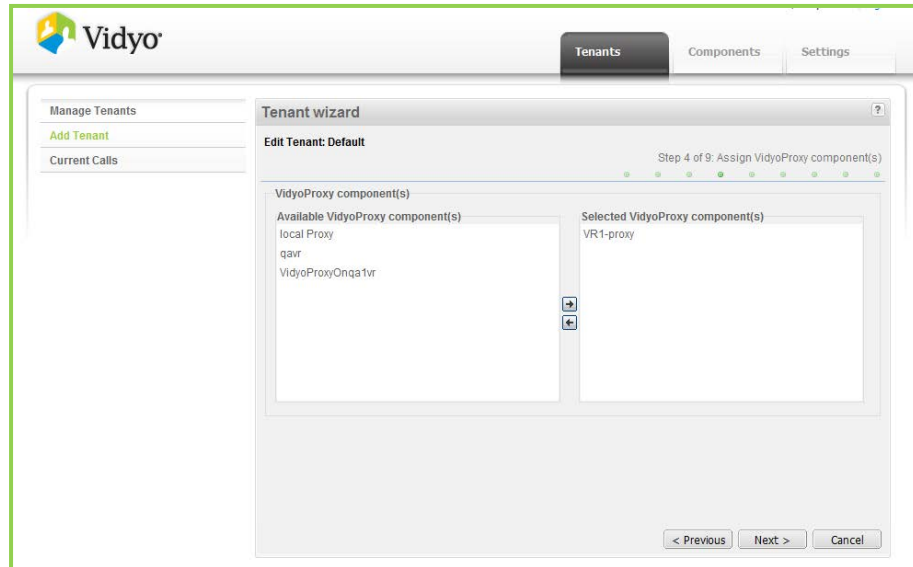
You assign a VidyoProxy in a similar manner to how you assigned a VidyoManager.

2. To select a VidyoProxy, select one or more in the Available VidyoProxy component(s) list and click the Right Arrow button to move them to the Selected VidyoManager component(s) list.

VidyoGateway Components

1. Click the Next button to proceed to Step 5 of 9.
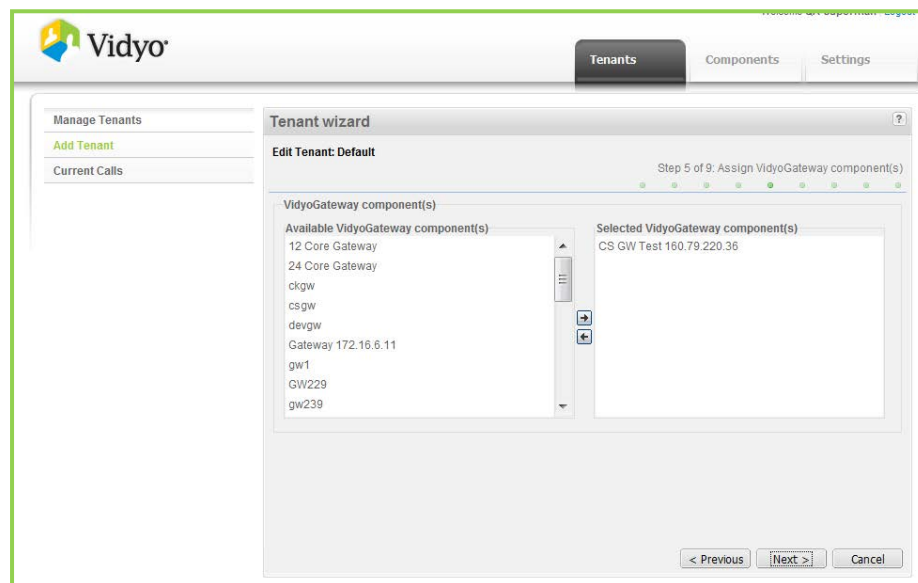
In this page, you can make available to the tenant the VidyoGateway components you set up previously. The Tenant Admin can then choose among these components as necessary. If you are not using a VidyoGateway, you can skip this step.

The list of available VidyoGateways appears in the Available VidyoGateway component(s) list on the left.

2. To select a VidyoGateway, select one or more in the Available VidyoGateway component(s) list and click the Right Arrow button to move them to the Selected VidyoGateways list.

3. All VidyoGateway components that appear in the Selected VidyoGateway component(s) list are available to the tenant. You can move a VidyoGateway from the Selected VidyoGateway component(s) list back to the Available VidyoGateway component(s) list by selecting it and clicking the left arrow button.

Note: If you are running a multi-tenant system and want to share a single VidyoGateway with multiple tenants, create a tenant that contains only the VidyoGateway(s) to be shared and set, in both directions, the visibility rules for each tenant.

VidyoReplay Recorders

1. Click the Next button to proceed to Step 6 of 9.
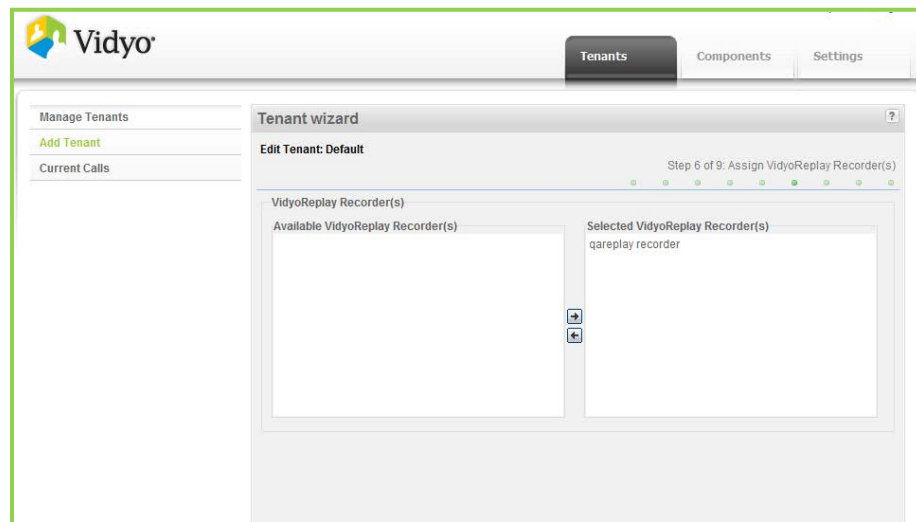
VidyoReplay is an optional 1U rack mount server that adds webcast recording, cataloging and replay of VidyoConferences to a VidyoConferencing system. (If you don't have VidyoReplay you can skip this step.) By now you know the drill.

1. To select a VidyoReplay Recorder, select one or more in the Available VidyoReplay Recorder component(s) list and click the Right Arrow button to move them to the Selected VidyoReplay Recorders list.

VidyoReplay Components

1. Click the Next button to proceed to Step 7 of 9.

Look familiar? It works the same way too.

2. To select a VidyoReplay Component, select one or more in the Available VidyoReplay Recorder component(s) list and click the Right Arrow button to move them to the Selected VidyoReplay Components list.
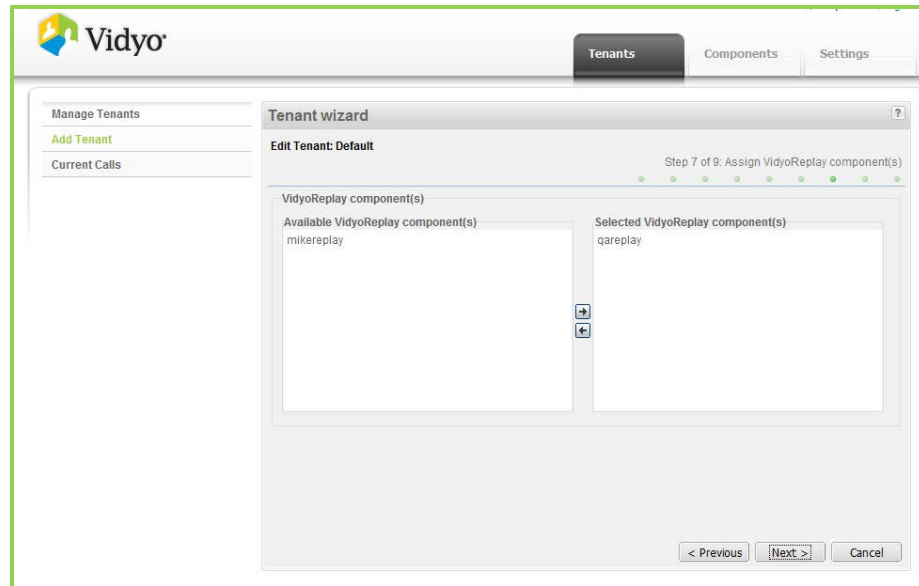
Assign Location Tags

1. Click the Next button to proceed to Step 8 of 9.
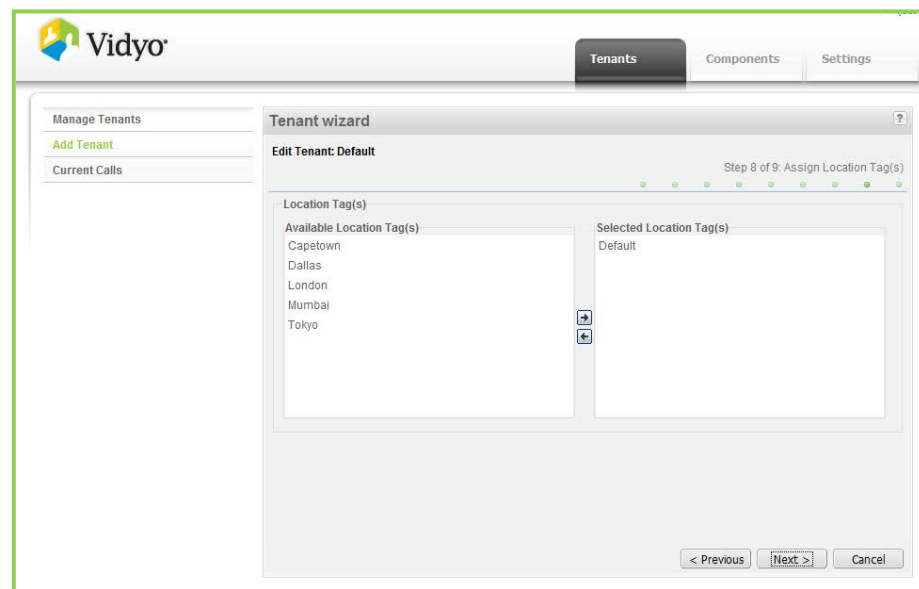
In this page, you can assign Location Tags (that the Super Admin has set up according to the instructions on page 112) to the Tenant. The Tenant Admin can then choose among these Location Tags as necessary. At a minimum you must at least assign the default tag to the tenant.

To assign a Location Tag, select one or more in the Available Location Tag(s) list and click the Right Arrow button to move the Location Tag(s) to the Selected Location Tag(s) list.

Saving The Tenant Information

1. Click the Next button to proceed to Step 9 of 9.
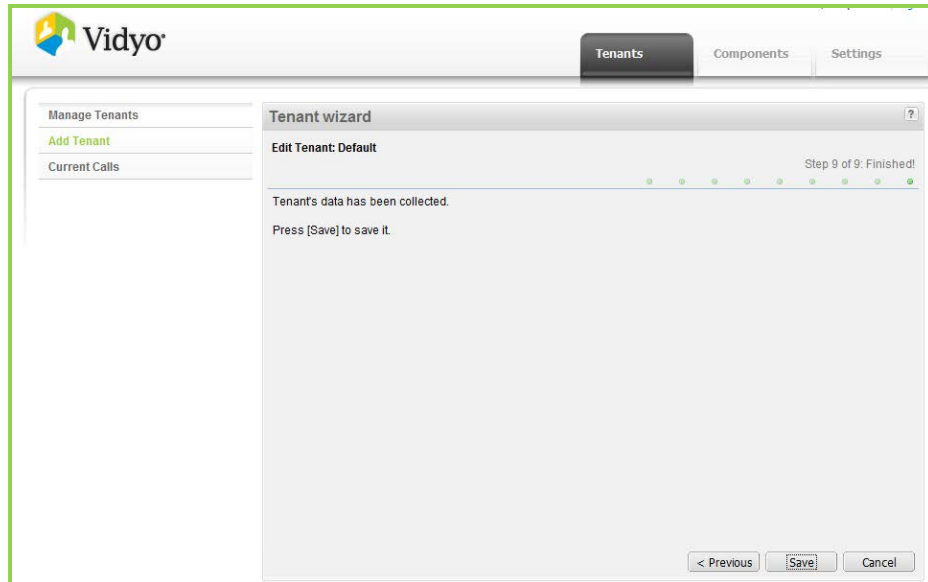
2. Click the Save button to finish configuring this tenant.

   Alternatively you can also click the Previous button as many times as necessary to go back and change any of the data you entered.

How to Delete a Tenant

Warning: The following task cannot be undone.

Warning: Deleting a tenant deletes all of its user accounts and public rooms.

1. From the Manage Tenants screen click the checkbox under Delete for the tenant you wish to remove.

2. Click the Delete button at the bottom of the Tenants table.

3. Click OK in the confirmation dialog box that appears.

CURRENT CALLS

The Current Calls page is available in both the Admin and Super Admin portals.

- In the Admin portal click on the Meeting Rooms tab on the top navigation bar then click Current Calls on the left-hand menu.

- In the Super Admin portal click on the Tenants tab on the top navigation bar then click Current Calls on the left-hand menu.

The Current Calls page in the Admin portal displays this information:

- **Name –** The display name of the caller.

- **Extension –** The extension number of the caller.

- **VidyoRouter –** The VidyoRouter the caller is using.

- **VidyoRouter Pool** – The VidyoRouter Pool to which the VidyoRouter belongs.

The Current Calls page in the Super Admin displays the same information and in addition it shows it in the left-most column:

- **Tenant Name** – The name of the tenant to which the user belongs. You can hide the calls for a tenant by clicking the − button to the left of the user's name. It becomes the + button. It's a toggle. Click it again to view the calls. Scroll to view calls by all tenants.

The information in this is page is for monitoring only. You cannot manage or control calls in the Current Calls page. For information about controlling a meeting, see How You Can Control Meetings on page .

Name ▲	Extension	VidyoRouter Name	VidyoRouter Pool
Current Calls			?
⊟ bhupesh_Default (Conference)			
VR1	101	qa5vr2_64bit.8GB	int-qa5vr2
⊞ Pilot_Test_Room_Default (Conference)			
⊟ pmac_Default_qa3_Default (Point-to-Point)			
Mac-.-Book Pravin_Napuri	007	qa5vr2_64bit.8GB	int-qa5vr2
qa3 test	10092	QAC-VR3 64bit.8GB	ext-qacloudvr3
⊟ qa10_Default_qa1_Default (Point-to-Point)			
QA 10	1010	qa5vr2_64bit.8GB	int-qa5vr2
qa1 test	10090	QAC-VR3 64bit.8GB	ext-qacloudvr3

|◀ ◀ | Page 1 | of 2 | ▶ ▶| | 🔁   Displaying calls 1 - 18 of 18

The Current Calls Table in the Admin Portal

Tenant Name	Name ▲	Extension	VidyoRouter Name	VidyoRouter Pool
Current Calls				?
⊟ bhupesh_Default (Conference)				
Default	VR1	101	qa5vr2_64bit.8GB	int-qa5vr2
⊞ Pilot_Test_Room_Default (Conference)				
⊟ pmac_Default_qa3_Default (Point-to-Point)				
Default	Mac-.-Book Pravin_Nap	007	qa5vr2_64bit.8GB	int-qa5vr2
Default	qa3 test	10092	QAC-VR3 64bit.8GB	ext-qacloudvr3

|◀ ◀ | Page 1 | of 2 | ▶ ▶| | 🔄   Displaying calls 1 - 14 of 14

The Current Calls Table in the Super Admin Portal

WHAT ADMINS AND TENANT ADMINS DO

After the Super Admin has configured the system (and created tenants if running a multi-tenant system) the Admin or Tenant Admin can carry out their role as system administrators.

The tasks Admins and Tenant Admins perform include:

- Creation and maintenance of user accounts.

- Creation of user provisioning groups. (Optional but often very useful.)

- Creation and maintenance of public rooms.

- Deployment and management of endpoint software

  By deployment we're referring to uploading new endpoint software onto the VidyoPortal itself. Once the endpoint client programs are loaded on the VidyoPortal, users are notified when they next use their VidyoDesktop programs to download and install the new software themselves.

- Setting the system language and guest access.

- The Admin user can also customize a Contact Us page to enable VidyoConferencing users to contact them for help with the system, as well as an About Us page, and set up the boilerplate text for email conference invitations.

So What's The Difference Between an Admin and a Tenant Admin?

Nothing really. If you have a single-tenant system then you need one Admin account to do the above tasks. In a multi-tenant system, each tenant has its own Tenant Admin.

Note: If you're running a multi‑tenant VidyoPortal system, the Super Admin can assign a different Tenant Admin user to each tenant on the system or have some or all of the tenants administered by one person. The Super Admin can always log into any tenant by using an Admin log-in.

To perform Admin setup, you must log in as an Admin/Tenant Admin.

- To log in as an Admin, enter the IP or URL of your portal followed by a forward slash and the word "admin."

- To log in as a Tenant Admin, enter the tenant URL in the address bar of a web browser, followed by a forward slash and the word "admin."

  http://<URL or IP>/admin
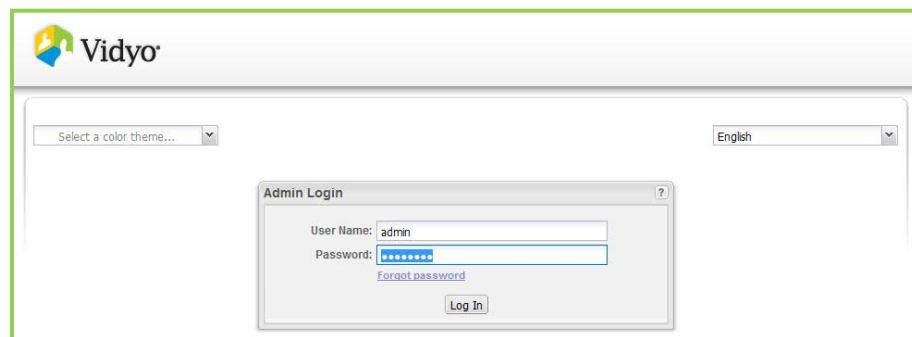
- Log in using the default administrator account:

- User Name: `admin`

- Password: `password` (case sensitive)

Note: Change the Admin password as soon as possible.

The VidyoConferencing System is available in eleven languages:

English	German	Japanese
Spanish	Italian	Chinese
French	Portuguese	Korean
Finnish	Polish	
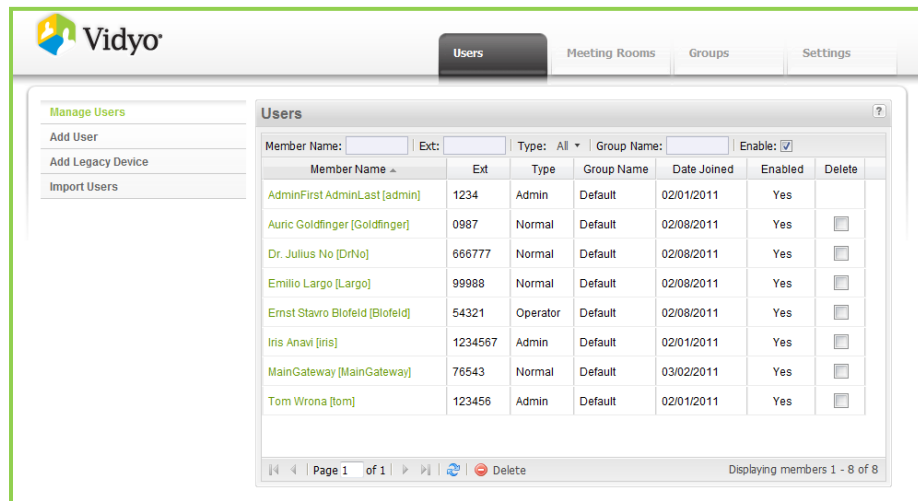
Select your preferred language from the drop-down. Once selected, the form will change immediately into that language and the language you've chosen will be your default language.

16.   Managing Users/Tenants

You use the Users tab to add/delete/edit your Vidyo system's users. This includes adding both personnel in your organization, as well as adding accounts for your VidyoRooms. This section of the document walks you through how to perform these actions.

To manage users login to the Admin portal. To access the Users section of the website, click the Users tab in the top navigation bar. You'll see Users tab highlighted on the top navigation bar of Users-related pages. To access the functions within this section, use the left-hand menu to manage and add users.

Overview of the Users Table

You can drag and drop the columns to arrange them in the order you prefer. Information contained in the table includes:

- Member Name
- Extension
- User Type
- Group Name
- Date Joined (i.e., the date the user was added)
- Enabled/Disabled
- Checkbox for Delete
- Help (The little box with the ? in it in the upper right hand corner.)

The Users table lists all users in the system. Search fields at the top of the table enable you to quickly and easily search by member name, extension, group name, or whether the user is enabled/disabled.

Note: The search is done by display name and username. This is the user name shown in the portal. It isn't necessarily the user's full name.

HOW TO ADD A NEW USER

If you're an administrator your first task is to log in and change the default password. You can also add yourself (or another person) as an administrative user.

Next, you should enter all other users of the system. To add users, follow the steps below and refer to the figure above. (Alternatively, you can bulk upload users using the Import Users function. Refer to How to Import Users on page **89** for more information about bulk upload of users.)

1. Click the Users tab in the top navigation bar.

2. Click the Add User button in the left-hand menu.

3. Select the User Type from the drop‑down list:

   - **Admin –** Has administrative privileges and capabilities as defined in this document.

   - **Operator –** Can manage users and meeting rooms. The operator has the same rights as the administrator except an operator cannot change any system settings nor manage groups.

   - **Normal –** Can join meetings, control their own meetings, and place direct calls. Can change their passwords, set their PIN Codes and invite guests, unless the administrator has disabled this capability.

   - **VidyoRoom –** The physical Vidyo endpoint appliance. Has the same rights as a normal user.

   - **Executive –** Executive Desktop users are a feature of the now standard VidyoLines licensing model. However, Executive Desktop licenses are purchased as separate licenses in your VidyoLines package. Each Executive Desktop has guaranteed system access. So if you purchase 100 VidyoLines and five Executive Desktops, then even when your system is at full capacity your five users with Executive Desktop privileges can still make calls.

4. Fill out all the required fields.

   All fields preceded by a red asterisk ***** are required.
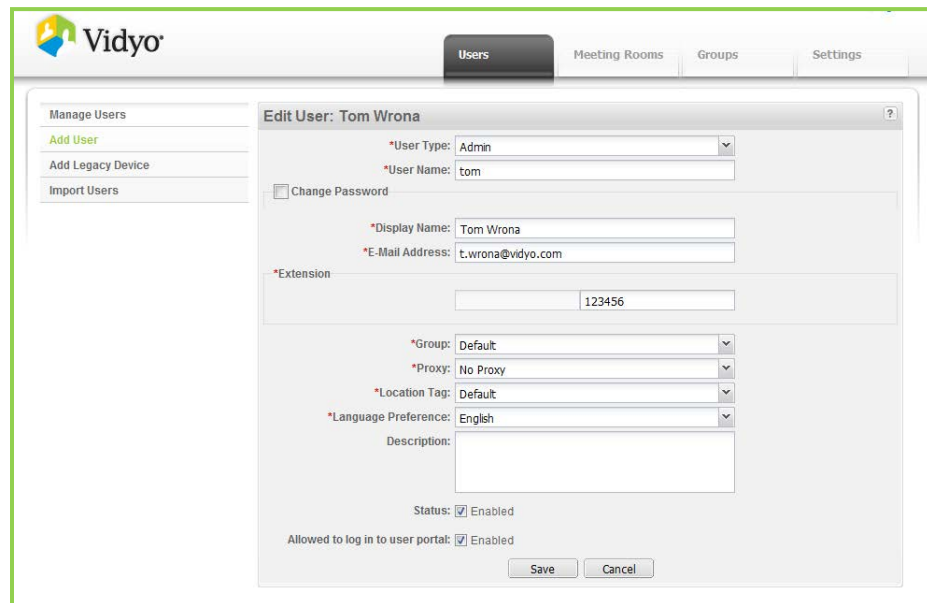
■ **User Name –** The name the user logs in with. This must be unique to the user and begin with an alphabetical character. If your intended entry has already been taken, you will be prompted to select a different name.

Not applicable to VidyoRoom users; the equivalent to Username for VidyoRooms is System Name.

■ **Password fields –** You must enter the password field identically two times to set the password. Users may change their passwords later.

■ **Display Name –** The displayed name of the person you are adding to the system. In the case of a VidyoRoom system, it is the system name set by the administrator and that appears in the top left corner of the home page. Users can see the names of other users in a conference overlaid at the bottom of their images in their VidyoDesktop programs by Clicking Configuration (the button that looks like a gear) then options and then clicking the Show Participant Names checkbox. The name they see for each user is his or her "Display Name"

■ **E-Mail Address –** Enter a valid email address for the user. This is the address to which the new account email will be sent. If notifications are enabled and a user's email address is not set correctly the user may not be able to use the Forgot Password function.

■ **Extension –** The numeric extension you want associated with the user. This must be unique to the user. If your intended entry has already been taken, you'll be prompted to select a different extension.

■ **Group –** Select either the default group or another group you have created. Changing the group may change the maximum number of users and the bandwidth allowed for the user's personal Meeting Room. Note that you must define groups prior to assigning groups. For more information about managing groups, see Managing Groups on page **98**.

■ **Proxy –** A VidyoProxy device set up by the super admin. This device is used to route traffic through one port to traverse a firewall. All Vidyo systems include a VidyoProxy but one may not be in use in your system.

■ **Location Tag –** Select the user's Location Tag from the dropdown list. For more on Location Tags see the entry under the VidyoRouter Cloud Edition chapter on page **112**.

■ **Language Preference –** Select the default language for the specific user you are adding. Use System Settings to apply system-wide language settings you chose at installation. For information, see How to Set the System Language on page **103**. Select any other language to change the language for this specific user only.

■ **Description –** Details or data regarding the person you are adding.

■ **Status –** Deselecting the Enabled checkbox puts a user on hold with all their information intact. They will not show up in searches in the portal or be able to log in. (If you're using the old Seats and Portals licensing model only enabled users consume a seat.)

■ **Allowed to login to user portal –** Admin and operator accounts may not need to be able to login like a regular user, saving a seat. Deselect this box to disable the account's ability to log in.

5. Save the user information

   ■ If some information is missing, incorrect, or already in the system, you will receive an error message at the top of the screen with prompts about what fields must be addressed.

   ■ When all required fields are complete and valid, the data will be saved to the database, you will be taken to the main table, and a success message will be displayed at the top of the page.

Note: The successful configuration of a VidyoProxy does not guarantee that the address is correct and/or that the VidyoProxy is actually installed and running at that address.

HOW TO EDIT A USER

To edit a user:

1. Click the Users tab in the top navigation bar.

2. Click the Manage Users button in the left-hand menu.

3. Find the user to edit by using the search filters, sorting on the headers and pagination.

4. Click the user's name to display the Edit User page.

5. On the Edit User page, edit the user's information as needed.

   You can edit any of the settings. For a description of these settings, see How Add a New User on page 85.

6. When you are done, save the updated user information.

   You return to the Users page.
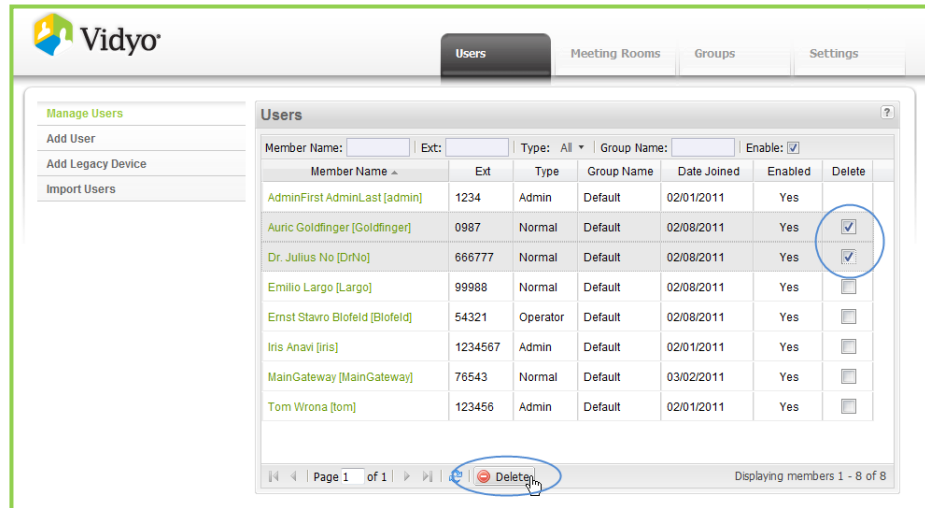
HOW TO DELETE A USER

Warning: The following task cannot be undone.

If a user leaves the organization or should no longer have access to the system and needs to be removed, you can delete a user completely from the system

1. Click the Delete checkbox at the far right of the user's listing.

   You can select multiple users, if desired

2. Click the Delete button at the bottom of the page and answer Yes to all prompts.

   If you delete a user, you also delete his or her personal meeting room. Deletion removes the user's personal meeting room completely and permanently from the system and cannot be undone

As an alternative to deleting a user you can deselect the Enabled checkbox on the User's page to change their status to disabled. Disabling a user puts them on hold with all their information intact. They will not show up in searches on the end user Web portal or be able to log-in. However, you can re-enable them at any time. See How to Edit a User on page .

HOW TO ADD A LEGACY DEVICE
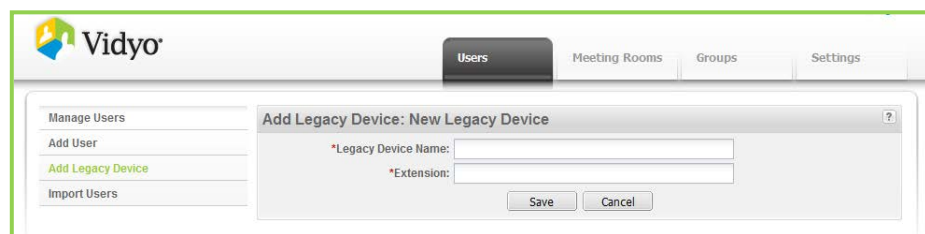
This feature is used in conjunction with the VidyoGateway to ease dialing from the VidyoPortal to legacy (H.323 and SIP) endpoints and telephones. This feature allows you to add legacy systems as users in the VidyoPortal. Specify the legacy device name and extension and click the Save button. See the separate VidyoGateway Guide for more information.

HOW TO IMPORT USERS
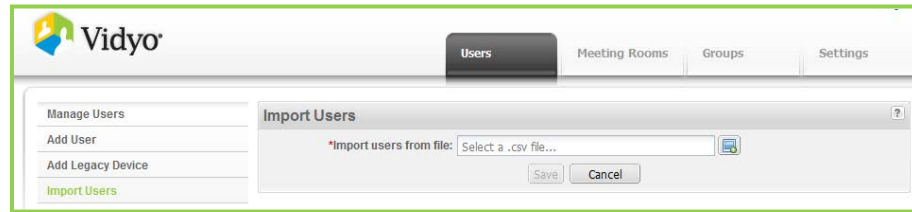
You may create a `.csv` file of user information and upload this document to add many users at once. All will be created as normal users. Note that the first line of the file is used as a header only and will not be imported as one of the added users. All `.csv` files must use UTF8 encoding.

Username	Password	Displayname	Email	Extension	Group	Language	Description	Proxy	Location
aID	pwd	aFullName	mailen@v.com	90001	Default	en	Update later	bigProxy	New York
Nome utente	Password	Visualizza	mailit@v.com	90002	Default	it	Aggiorna in seguito	bigProxy	Roma
Nombre de usuario	Contraseña	Pantalla	mailes@v.com	90003	SpGroup	es	Actualizar más tarde	bigProxy	Puerto Rico
Nom d'utilisateur	Mot de passe	Afficher	mailfr@v.com	78004	FrGroup	fr	Mettre à jour ultérieurement	bigProxy	Lyons
ユーザ名	パスワード	%iを表示	mailes@v.com	90508	JaGroup	ja	後で更新	bigProxy	Kobe
사용자 ID	암호	표시	mailes@v.com	67802	KoGroup	Ko	나중에 업데이트	bigProxy	Seoul
用户名	密码	显示	mailes@v.com	50089	ScGroup	sc	稍后更新	bigProxy	Shanghai
Nome de usuário	Senha	Exibir		80077	PTGroup	pt	Atualizar mais tarde	bigProxy	Brasilia
Benutzername	Kennwort	Anzeige	mailes@v.com	736390	DeGroup	de	Später aktualisieren	bigProxy	Berlin
Käyttäjänimi	Salasanaa	Näyttönimi		847648	FiGroup	fi	Kuvaus	bigProxy	Helsinki
Nazwa użytkownika	Haslo	Nazwa wyświetlana	mailes@v.com	892291	PoGroup	po	Opis	bigProxy	Kraków

The proper column labels for the spreadsheet are (from left to right):

1. **Username**

2. **Password**

3. **Displayname**

4. **Email**

5. **Extension –** The user's unique extension

6. **Group –** The provision group to which the user belongs. (See Managing Groups on page **98**.)

7. **Language**

8. **Description –** Optional field for any text (job description, special comments, etc.)

9. **Proxy –** The Proxy to which this user has been assigned, if any. (Optional)

10. **Location –** The location tag assigned to the user. (See How to Create a User Location Tag on page **112**.)

Note that you must define groups prior to assigning groups. For more information about managing groups, see Managing Groups on page **98**.

All fields are required except for Proxy and Description.

Once you have created your .csv file, save it to your desktop, then use the upload feature on this page to locate and upload the document.

Each language is identified with a two-letter code, as follows:

- **English –** en

- **Italian –** it

- **Spanish –** es

- **French –** fr

- **Japanese –** ja

- **Korean –** ko

- **Simplified Chinese –** sc

- **Portuguese –** pt

- **German –** de

- **Finnish –** fi

- **Polish –** po

The rightmost column enables you to assign each user to a VidyoProxy, if desired. (It's optional.)

Note: The `.csv` file must contain comma-separated values. Microsoft Excel produces fields separated by semicolons, which prevents the file from importing successfully.
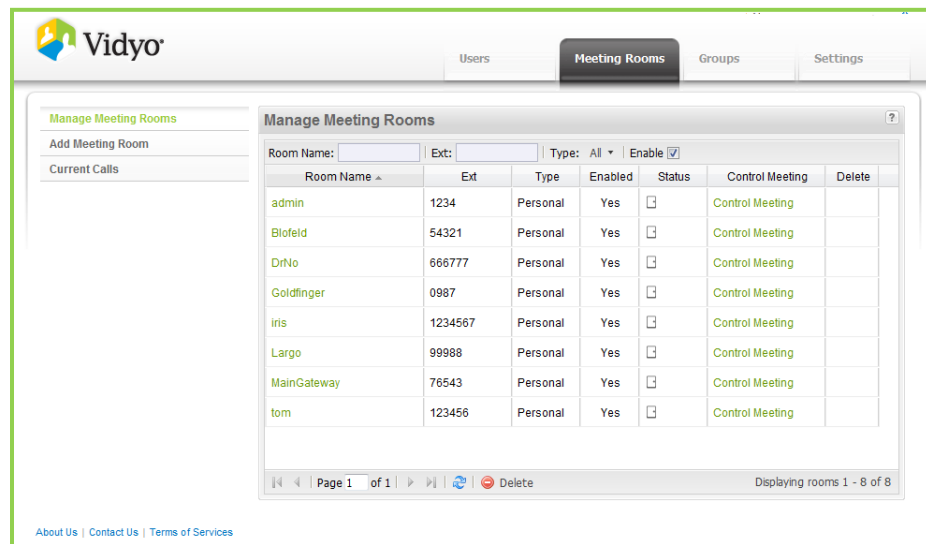
Every user has a personal room that is automatically assigned to him or her, similar to an office in the physical world. The admin or operator can also add public rooms that are not associated with a particular user, similar to conference rooms in the physical world.

To manage meeting rooms login to the Admin portal.

The Manage Meeting Rooms section is used to Add/Delete/Edit rooms in the VidyoConferencing system. This section of the document walks you through how to perform these actions. To access the Manage Meeting Rooms section of the Website, click the Meeting Rooms tab in the top navigation bar. Use the left navigation bar to add and manage meeting rooms.

Overview of the Manage Meeting Rooms Table

The Manage Meeting Rooms table lists all rooms in the system. Search fields at the top of the table allow you to quickly and easily search by room name, room type, extension and whether the room is enabled or disabled.

You can drag and drop the columns to arrange them in the order you prefer. Information contained in the table includes:

- Room Name

- Extension

- Room Type

- Enabled/Disabled

- Status

   Empty, Full, Locked, PIN-Protected

The first icon shows whether the room is empty or full. This room is empty. The icon would be dark if the room were full. The second icon appears only if the room is locked. The third icon appears only if the room is PIN protected. Both the user and the Admin can control the latter two options.

91
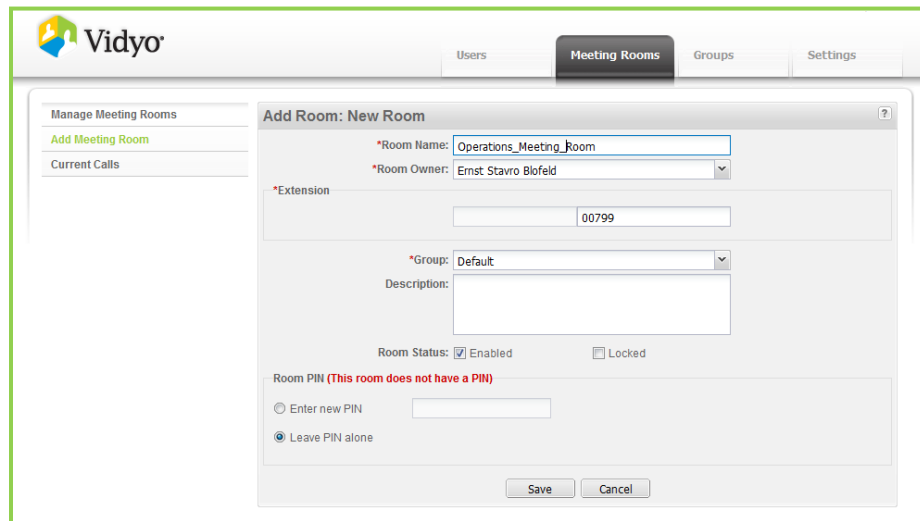
■   Control Meeting Link

■   Delete Checkbox

Note that you can delete only public rooms. To delete a personal room you must delete the user associated with that room.

You may be surprised to see many rooms populated in the table before ever creating rooms; remember, this is because each user added to the system automatically receives a corresponding personal room.

How To Add a Meeting Room

Note: Only Public Rooms can be added here. Personal Rooms are automatically generated when you add a new user.
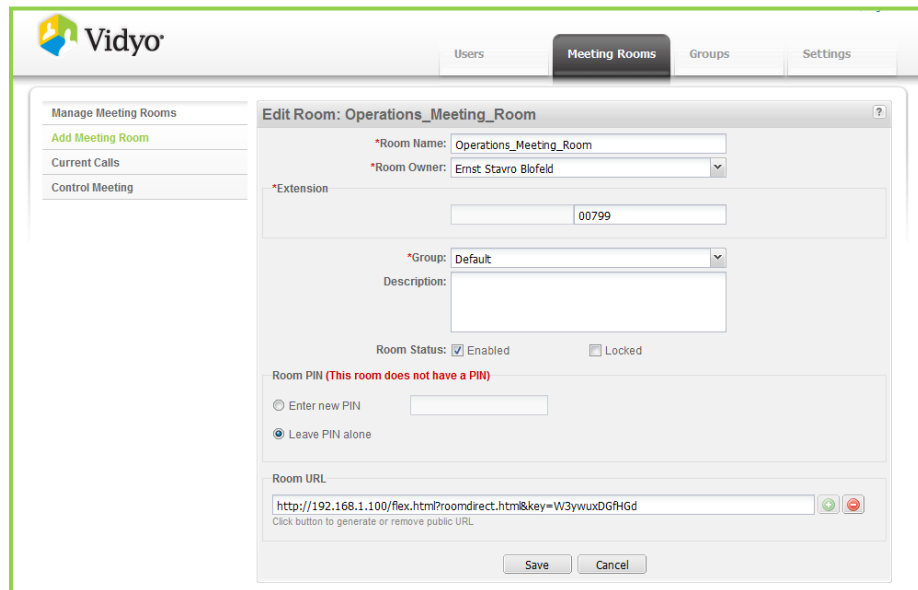
1.   Click on Meeting Rooms on the top navigation bar.

2.   Click on the Add Meeting Rooms button in the left-hand menu.

3.   Add the following required fields:

■   **Room Name** – **The name must be unique and begin with an alphanumeric character and can't contain spaces. The only other valid characters are periods, underscores and dashes.** The system will alert you if an existing name was entered.

■   **Room Owner** – the person selected as room owner will be able to manage and control meetings in the public room. The dropdown provides a list of users to select from. (You can also type in the field to narrow the list)

■   **Extension** – Number used for user's direct calls and speed dial. It must be numeric and it must be unique.

■   **Group** – The default group is selected automatically. If you have created other groups and want to associate the room with a particular group, select it from the dropdown here. Remember, groups have special designations of maximum participants and maximum bandwidth privileges.

For more information on groups see Managing Groups on page 98.

4. Enter information in the following optional fields as needed:

   - **Enabled Checkbox** – Deselecting this checkbox will allow for a room to be put "on hold" with all its information intact. It will not show up in searches on the end user web portal.

   - **Room Status** – Lists whether the room is enabled and/or locked.

   - **Enter new PIN** – For the Meeting Room to be PIN protected, enter the value here. Participants of this meeting are prompted to enter this PIN before being admitted to the meeting. Make sure you provide meeting invitees with this PIN.

   - **Leave PIN Alone** – This setting retains the current PIN, if one is in use.

   - **Description** – Enter any information that would be useful for the users, such as: "This room is for the weekly sales meeting."

   - **Note**: A room owner can change his or her room's lock/unlock status and PIN at any time from the Portal.

5. Click the Save button to save the meeting room settings.

   - If some information is missing, incorrect, or already in the system, you will receive an error message at the top of the screen, which prompts you regarding what fields must be addressed.

   - When all required fields are complete and valid, the data will be saved to the database and you will be taken to the main table.

How to Edit a Meeting Room

You can edit the settings for any meeting room as needed, including changing or removing the room URL. The room URL is the link necessary for a user to join the meeting room. For information about the other meeting room settings, see How to Add a Meeting Room on page .

1. Click on the Meeting Rooms tab in the top navigation bar.

2. Click on the Manage Meeting Rooms link in the left-hand menu if it isn't selected automatically.

3. Click on the Room Name of the room you wish to edit.

    The room's page opens. Edit any of the fields, as necessary.

4. You can change or delete the room URL, which is the link necessary for users to join the room.

    This link is used by guest users to join a conference.
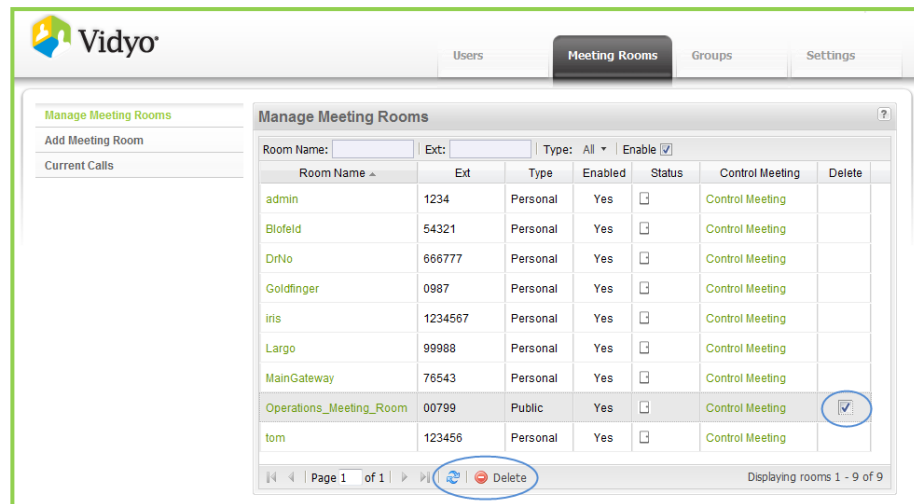
5. To change the room URL, click the **+** button to the right of the Room URL field.

    The system automatically generates a new URL.

6. To delete the current room URL, click the **−** button to the right of the Room URL field.

7. Click the Save button to save the meeting room settings.

    ■   If some information is missing, incorrect, or already in the system, you will receive an error message at the top of the screen, which prompts you regarding what fields must be addressed.

    ■   When all required fields are complete and valid, the data will be saved to the database, you'll be taken to the main table and a success message will be displayed at the top of the page.

How to Delete a Meeting Room

(Note that in the screenshot above only one room has a Delete checkbox. That's because it's the only public room listed.) If a Public Room is no longer needed there are two ways to remove it. You may delete a Public Room completely from the system, or you may disable a room, as discussed above. (Disabling a room puts it on hold with all its information intact. It will not show up in searches on the end user Web portal.) To delete a Personal Room, one that is associated with a user, you *must* delete the user. Refer to How to Delete a User on page **88**. Deleting the user will automatically delete his or her room.

Warning: The following task cannot be undone.

To delete a Public Room The first step is to find the appropriate room to delete.

1. Click on the Meeting Rooms tab on the top navigation bar.

2.   Click on Manage Meeting Rooms on the left-hand menu.

3.   Find the room you wish to delete by using the search filters, sorting on the headers, and pagination.

4.   Select the checkbox(es) under the Delete column of the room(s) you want to delete.

5.   Click the delete button at the bottom of the page and answer yes to all prompts.

This change is permanent and cannot be undone.

How You Can Control Meetings

Note: The above screenshot happens to show only private rooms, which cannot be deleted. (When you delete a user his or her room is deleted too.) Admins and Operators can control a meeting room while a meeting is in session.

Admins and Operators can:

- Lock or unlock the meeting.

- Disconnect any user.

- Mute any user or disconnect any video ability of any user.

- Define or remove a room PIN.

- Create and delete a room URL.

- Invite users to attend the meeting.

You must click on a specific, individual meeting before you can control it.

1.   Click on Meeting Rooms on the top navigation bar.

2.   Click on Manage Meeting Rooms on the left-hand menu.

3.   Find the room you wish to control by using the search filters, sorting on the headers, and pagination.

4.   Once the room(s) has been found click on the Control Meeting link in the Control Meeting column.

This opens a new window with the meeting's information.
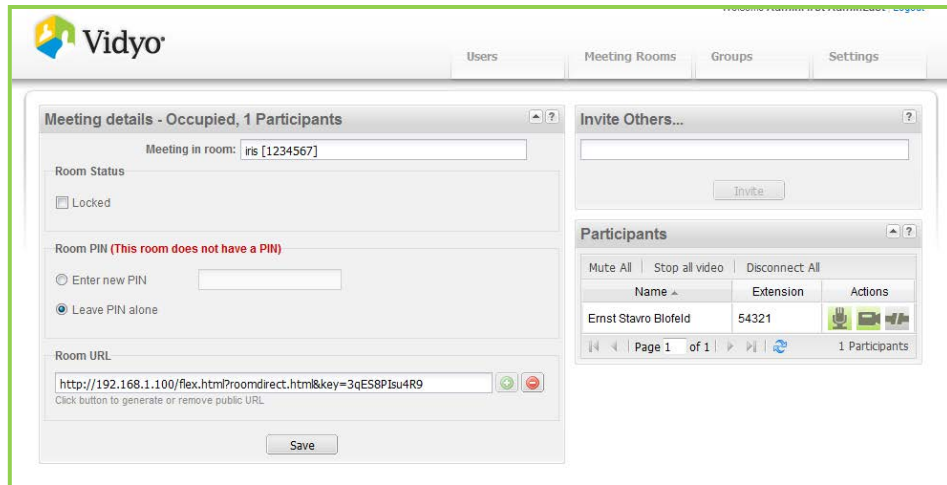
Once you've selected the meeting there are a number of actions you can take.

- **Lock/unlock a room –** Under Room Status, select the Locked checkbox to prevent new attendees from joining a meeting; deselect the checkbox to open the meeting to more attendees.

- **Room PIN –** To define a PIN number for the meeting room, select Enter new PIN and enter a four-character PIN in the field. To lock in the new PIN, click Leave PIN alone. To remove or change a PIN, select Enter new PIN, delete or edit the PIN number, then select Leave PIN alone.

- **Room URL** – You can change or delete the room URL, which is the link necessary for users to join the room for a meeting.
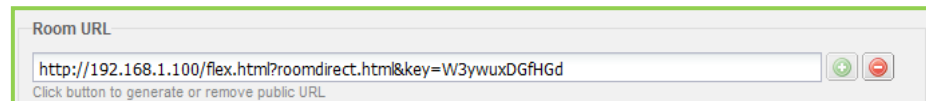
5. To change the room URL, click the circular white on green **+** button next to the Room URL field.

   The system automatically generates a new URL.

6. To delete the current room URL, click the **–** button.

How to Manage Participants

- In the Participants section select any attendee.

- Click the camera button to stop or start the attendee's outbound video.

   This is called Privacy Mode whether initiated by the Admin or the attendee.
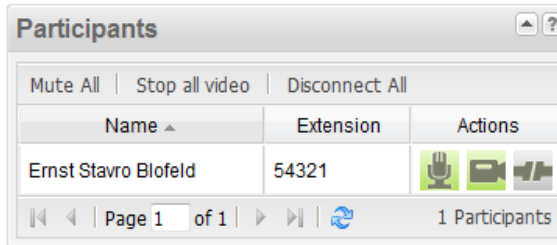
Blofeld's mic and camera are on.
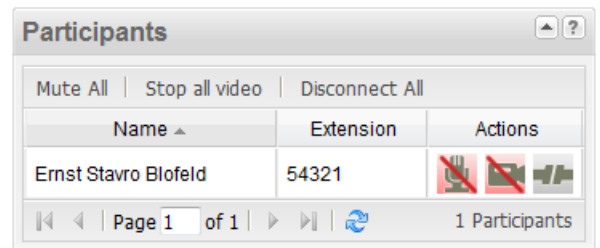
Blofeld's mic and camera are off.

- Click the Microphone button to mute or unmute the audio for the attendee.

  You turn the outbound video on or off and mute and unmute the outbound audio independently.

Disconnect any meeting attendee – Click the Connect button to the right of the camera button to disconnect any attendee from the meeting, and then confirm your decision in the dialog box that opens.

Invite Others – You can search for and invite other users to a meeting currently in session.
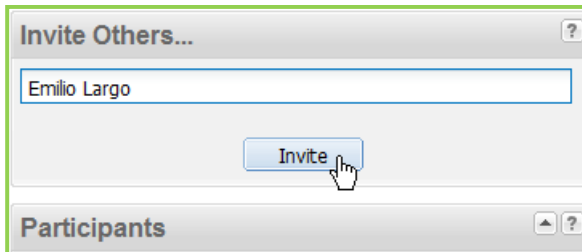
To search and invite other participants to a meeting – Typing a few characters brings up a list of suggestions of online users.

- You can select from these suggestions or keep typing your full entry.

- You can use the wildcard character % to bring up the full list of online users.

- After clicking the name of a user or personal room, click the Invite button.

- A message is sent to the user through the Vidyo system, inviting them to call into the meeting.
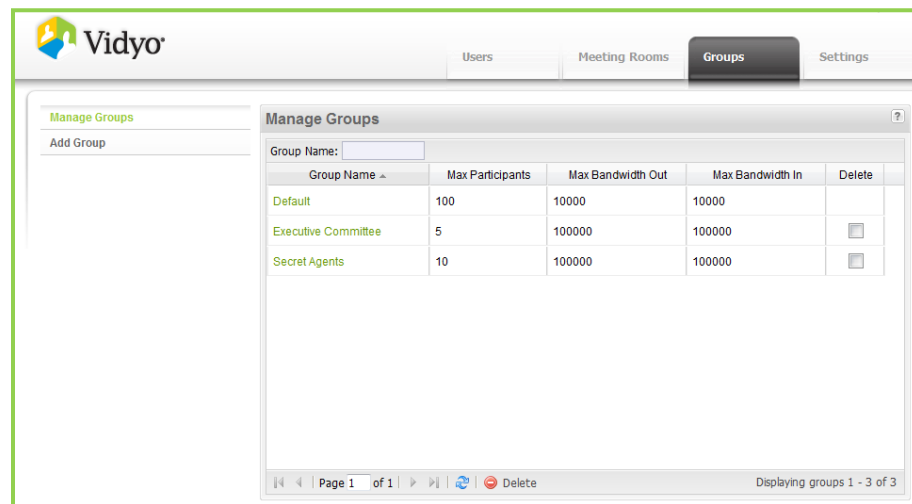
GROUPS

Groups are special designations of users who have the common attributes like number of maximum participants and maximum bandwidth privileges. Users are assigned to the default group automatically unless a new group is created by the Admin/Tenant Admin or Operator. The admin or operator must then specifically assign users to these non-default groups. For additional information about groups, see the definition of Groups on page 7.

You may choose to create groups based on specific employees' needs or departmental divisions. Changing the group will change the maximum number of participants and bandwidth allowed for each user in the group's Personal Meeting Room. Some employees may require more or fewer meeting participants, and some may require lesser or greater bandwidth. Set up groups based on these needs.

You use the Manage Groups table to add, delete, and manage groups in the Vidyo system. This section of the document walks through how to perform these actions. To access the Groups section of the Website, click the Groups tab in the top navigation bar. To access the functions within this section, use the left-hand menu to manage and add Groups.

Overview of the Manage Groups Table

Note that the Default group doesn't have a checkbox in the Delete column. You can't delete the Default group.

You can drag and drop columns to arrange them in the order you prefer. Information in the table includes:

- Group Name
- Maximum Participants
- Maximum Bandwidth Out
- Maximum Bandwidth In
- Delete Checkbox

The Manage Groups Table lists all groups in the system. Search fields at the top of the table allow you to quickly and easily search by group name.
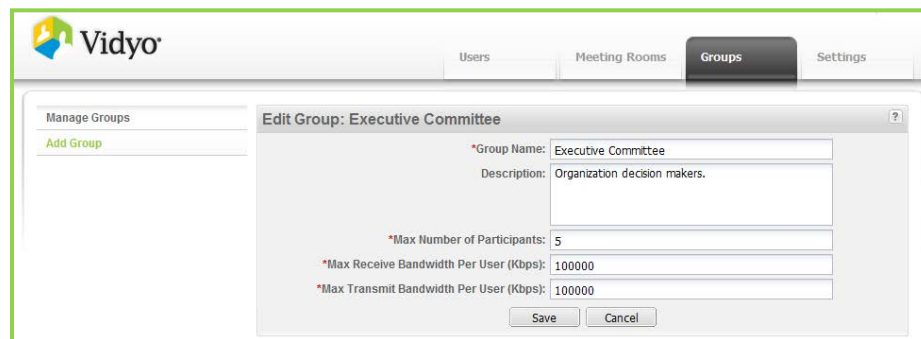
How to Add a New Group

To add a new group:

1. Click on the Groups tab on the top navigation bar.

2. Click on the Manage Groups link in the left-hand menu.

3. Enter the following required fields:

   - **Group Name:** This is the name of the group. The system will check to see that it is unique. If a group name has already been taken, you will be prompted to choose a different name.

   - **Max Number of Participants:** This is the maximum number of participants per meeting of the group. There is a minimum of two participants required for any group.

   - **Max Receive Bandwidth** – This is the maximum receive bandwidth in kbps per user. Enter a numeric value for the maximum receive bandwidth.

   - **Max Transmit Bandwidth** – This is the maximum transmit bandwidth in kbps per user. Enter a numeric value for the maximum transmit bandwidth.

4. Add an optional description for the group in the **Description** field.

5. Click the Save button to save the group settings.

   - If some information is missing, incorrect, or already in the system, you will receive an error message at the top of the screen, with prompts about what fields must be addressed.

   - When all required fields are complete and valid, the data will be saved to the database, you will be taken to the main table, and a Success message will be displayed at the top of the page.

How to Edit a Group

99

You can edit the settings for any group.
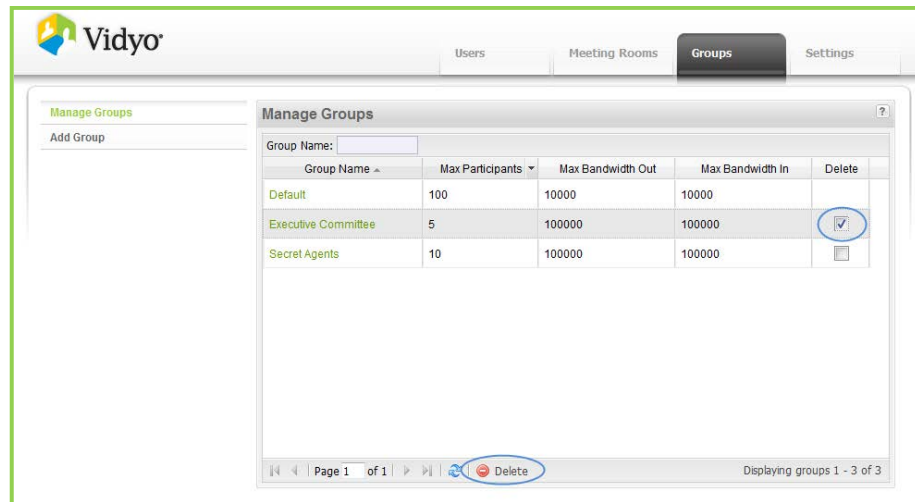
To edit the settings for a group:

1. Click on the Groups tab on the top navigation bar.

2. Click the group name link for the group you want to edit.

3. Edit the settings as needed.

   For information about settings, see How to Add a New Group on page **99**.

4. Click the Save button to save the group settings.

How to Delete a Group

Warning: The following task cannot be undone.

1. Click on the Groups tab on the top navigation bar

2. Click on Manage Groups on the left-hand menu.

3. Find the group you wish to delete by using the search filters, sorting on the headers, and pagination.

4. Once the group(s) has/have been found, click the checkbox(es) in the Delete column for the group(s).

5. Click the Delete button at the bottom of the Groups table.

6. Click the Yes checkbox in the Confirmation dialog box that opens.

   This change cannot be undone. Of course you have merely deleted the group. The accounts of users that were in that group remain otherwise unchanged.

SET UP AND MAINTENANCE

How to Check Your License Terms
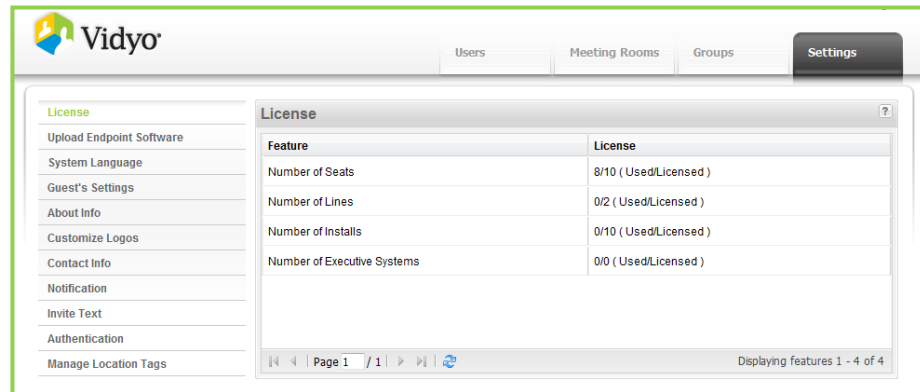
The License page under the Settings tab provides you with a report of:

- How many seats are licensed and how many have been allocated (used).

- How many lines are licensed and how many have been allocated (used).

- How many installs are licensed and how many have been allocated (used).

- How many Executive Desktops (here called Executive Systems) are licensed and how many have been allocated (used).

How to Upload Endpoint Software
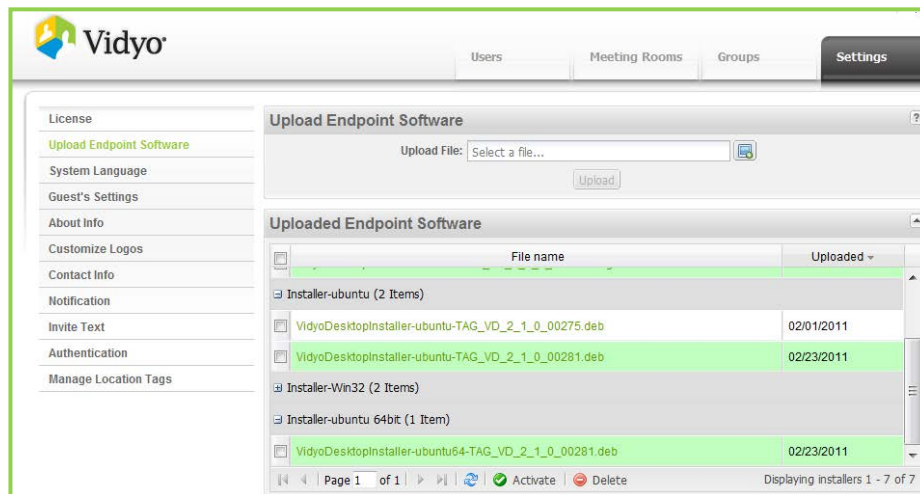
When new versions of the Vidyo software become available from Vidyo, you can upload the new software using this page so that users of the system will automatically be prompted to download the new version.

Available client types are:

- VidyoDesktop for Windows

- VidyoDesktop for Macintosh OS X

- VidyoRoom HD-220, HD-200, HD-100 and HD-50

The Super Admin user uploads the latest version of Vidyo client software and makes it available to all users of the VidyoConferencing System. An Admin user can also upload Vidyo client software, if necessary, and make it available to the just the users for whom they have admin responsibility.

In the Upload Endpoint Software page, you can upload up to four different versions of each type of endpoint software (VidyoDesktop for Macintosh, VidyoDesktop for PC and so on), but for each type you must make just one active. It is the active version that downloads automatically for VidyoPortal users when they first use the system or upgrade to a new version.

To upload an endpoint installation file, click the Select File button and select the file from its location on your computer or local network.
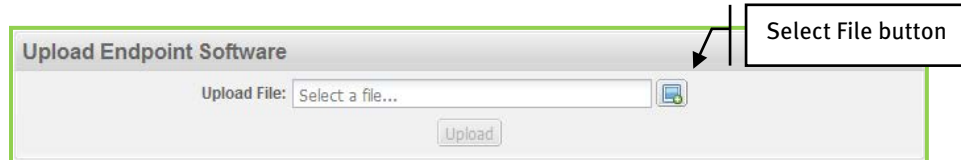
After selecting the installation file, click the Upload button to import it. When the endpoint installation file is uploaded, it appears in the Uploaded Endpoint Software list under its corresponding heading. Scroll through this list to view all available installation files.
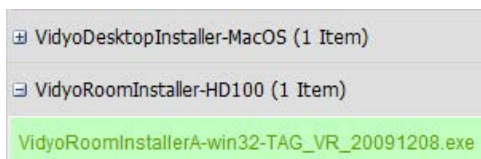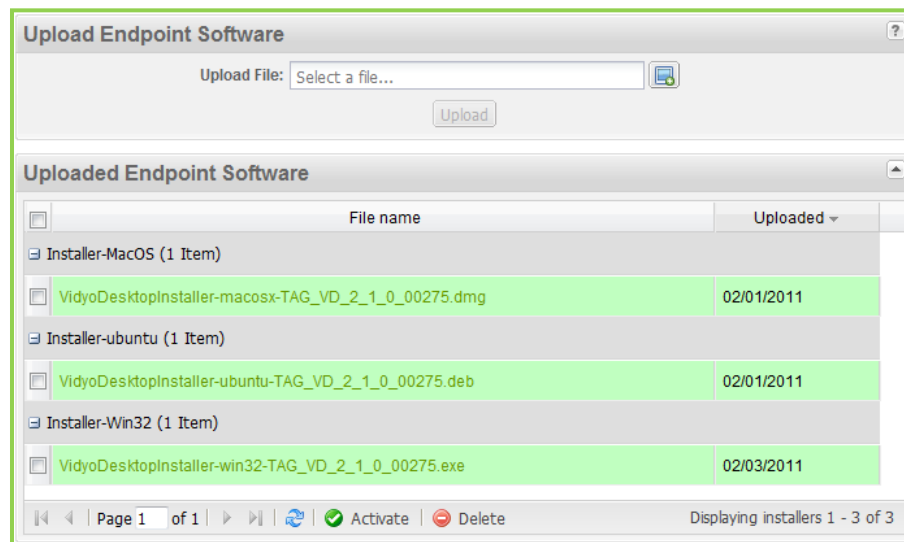
Rolled up heading (top) and active installation file (bottom)
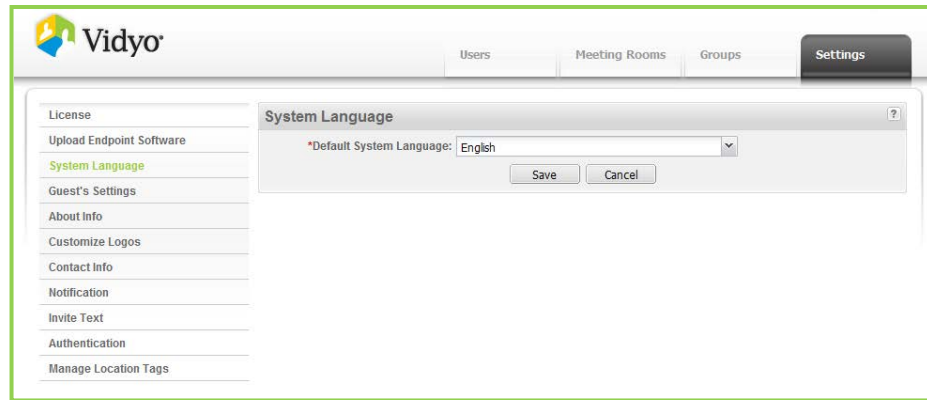
How to Set the System Language

The VidyoConferencing System is available in eleven languages:

English	German	Japanese
Spanish	Italian	Chinese
French	Portuguese	Korean
Finnish	Polish	

You can select your preferred language from the Default System Language drop-down menu. This overrides the language set by the Super Admin. Once selected, the page will change immediately into your chosen language and it will be the system's (or your tenants') default language. You can change the preferred language for a particular user/tenant as described in

Guest's Settings
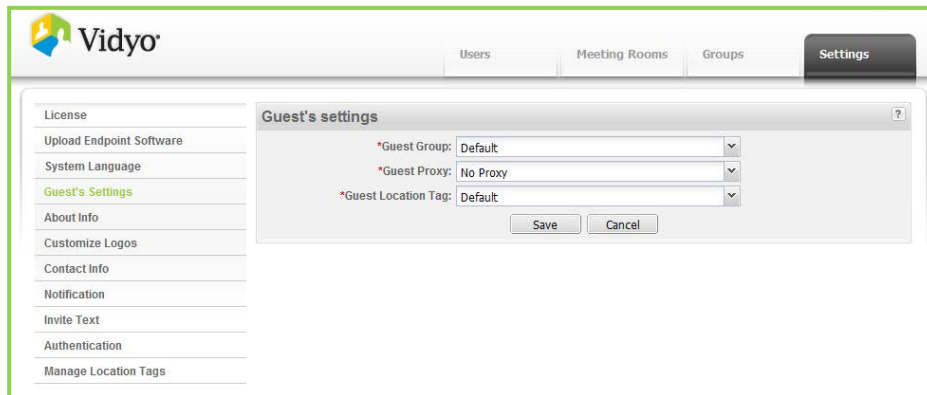
The Guest's Settings page enables you to assign guest users to a group and specify a VidyoProxy for all guest users, if one is available for your VidyoConferencing System. A guest user is a user who is not registered with the VidyoConferencing System but who can join meetings to which they are invited by a user.

1. In the Settings tab, select Guest's Settings and do the following:

2. To assign guest users to a group, from the Guest Group list, select a group.

3. To assign a VidyoProxy to guest users, from the Guest Proxy list, select a VidyoProxy device. If no VidyoProxys appear in the list, none are set up for your system.

4.   Click the Save button to save your changes.

How to Enter "About Us" Information
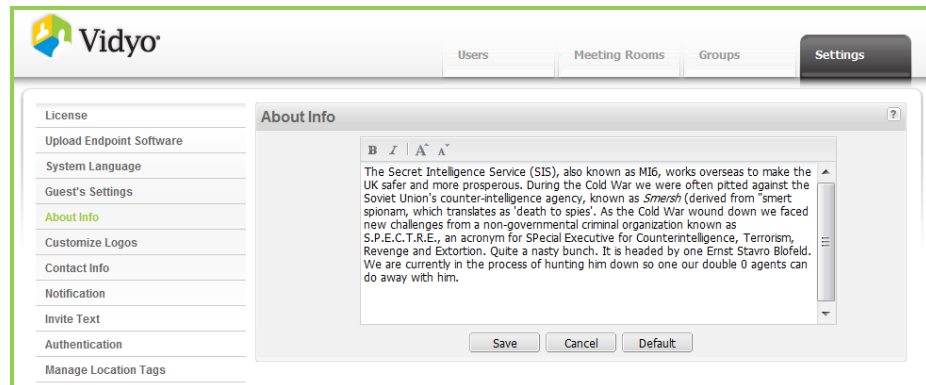
The About Info page enables you to create and format a page that appears when users click the About Us link at the bottom of the VidyoPortal homepage and at the bottom of the VidyoPortal admin and super admin pages. This can be any kind of information you want to provide to your users. The About Info page provides a tool bar you can use to apply formatting to text, including font, color, styles and numbered and bulleted lists and add hypertext links. After you have created and formatted text, click the *Save* button. Your edits go into effect immediately.

Note: About Us settings created or changed at the Tenant Admin level override settings created at the Super Admin level.

Warning: The following task cannot be undone.

1.   If you wish to destroy the custom About Info text you've created and revert to the default text created by your Super Admin, click the Default button.

Since there is no confirmation dialog box, it's a good idea to keep a copy of any customized text you have in a separate text file somewhere convenient in case you click the Default button by accident.

How to Customize The User Portal Logo
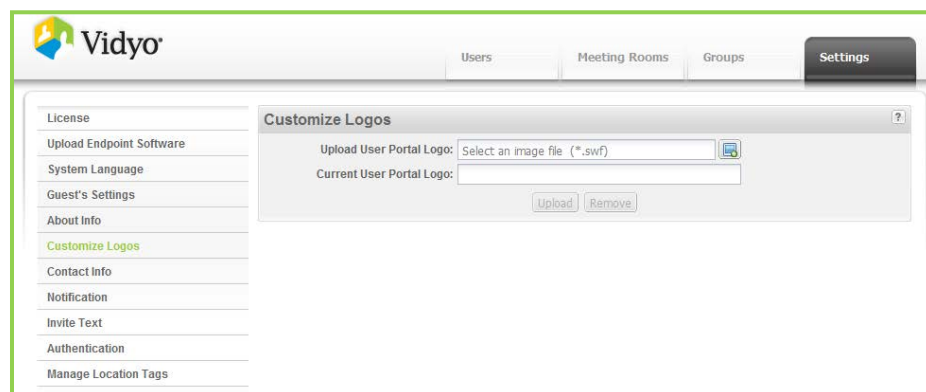
You can upload your organization's logo to customize and co-brand your VidyoConferencing system. The logo must be sized to 150 by 60 pixels and be in the `.swf` format. The `.swf` format allows the logo to dynamically resize for different screen resolutions and window sizes. It replaces the Vidyo logo that appears in the

upper left corner of each super admin, admin and VidyoPortal page. When you use a custom logo to replace the Vidyo logo, a VidyoPower logo appears in the lower right corner.

The filename of a custom logo in use appears in the Current Logo field.

Note: For best appearance, use a logo saved with a transparent background.

How to Add And Edit Contact Information
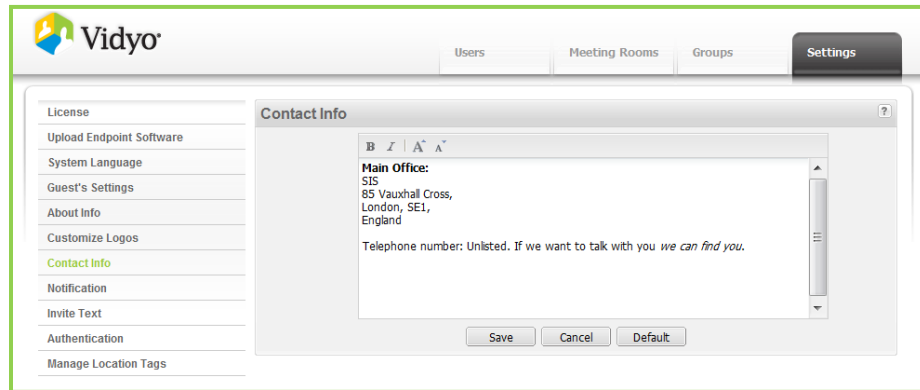
The Contact info page enables you to create and format a contact page that appears when users click the Contact info link at the bottom of the VidyoPortal home page as well as the login page. This is information your users need to contact you, the Tenant Admin. The Contact info text box provides a tool bar to apply bold and italic formatting and change the point size. After you have finished, click the Save button. Your edits go into effect immediately.

Note: Contact Information settings created or changed at the Tenant Admin level override settings created at the Super Admin level.

Warning: The following task cannot be undone.

1. If you wish to destroy the custom Contact Information text you've created and revert to the default text created by your Super Admin, click the Default button.

Since there is no confirmation dialog box, it's a good idea to keep a copy of any customized text you have in a separate text file somewhere convenient in case you click the Default button by accident.

How to Add and Edit Notification Information
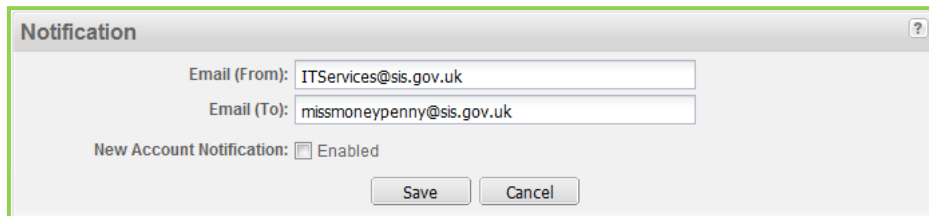
The Portal provides some automated information. The "From" address you enter is used for automated emails sent out by the portal, such as confirmations to new users of their accounts, etc. If you don't set a "From" address SMTP servers may block emails.

You can elect to have status updates about the Vidyo system sent to an IT staff person in your organization. The "To" address should be the email address of the person who should receive alerts for action required by the portal.

Enter valid "From" and "To" email addresses and click the Save button. Multiple email addresses/contacts are currently not supported.

Note: Notification settings created or changed at the Tenant Admin level override settings created at the Super Admin level.

How to Create Invite Text

The Invite Text page enables you to create the boilerplate email message sent by users to invite guests to attend meetings in their rooms and, if you have VidyoReplay to invite them to a webcast.

1. Click the 🟢 icon to insert a [ROOMLINK] placeholder for the link to the user's room.

   When the user creates an email invitation, the VidyoPortal automatically enters the correct URL. This placeholder is required.

2. Click the 🟢 icon to insert an [EXTENSION] placeholder for the dial-in number and extension (if an extension has been set) needed to dial into the user's room (and optionally, a PIN required to enter the room).

   When the user creates an email invitation, the VidyoPortal automatically inserts the correct extension (and PIN, if the user has chosen to require one). This placeholder is optional.

3. Click the Save button to save the message.

106

Warning: The following task cannot be undone.

1. If you wish to destroy all custom invitations and revert to the default text supplied by your Super Admin, click the Default button.

    Since there is no confirmation dialog box, it's a good idea to keep a copy of any customized text you have in a separate text file somewhere convenient in case you click the Default button by accident.

Users can also edit the invitation text you create on this page before sending out them out. For instance, if a meeting will take place at some time in the future, they'll want to include the date and time of the meeting.

Note: Invitation settings created or changed at the Tenant Admin level override settings created at the Super Admin level.

How to Set Up Authentication
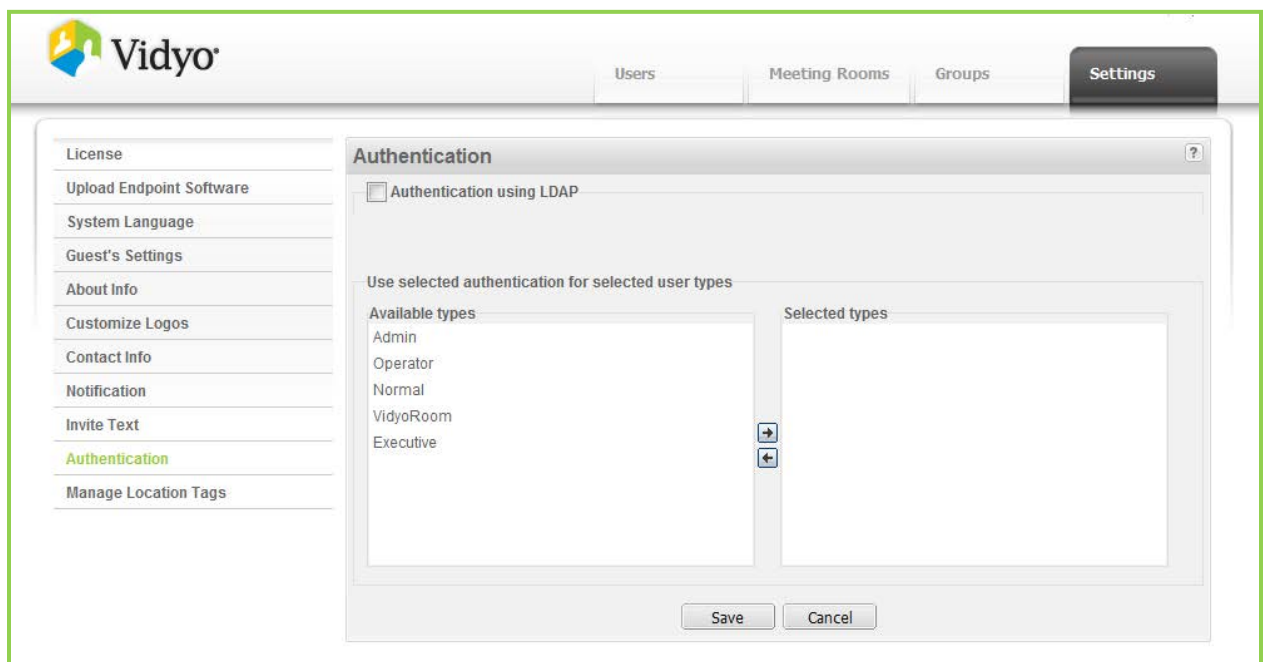
You arrive at the Authentication page by clicking on the Settings tab on the top navigation bar and then clicking Authentication on the left-hand menu.

The Authentication page enables you to define an external LDAP server such as Microsoft Active Directory to authenticate users. When LDAP authentication is enabled, the VidyoPortal passes logins to the LDAP server for password authentication.

Any kind of user can be authenticated by LDAP (normal, operator, admin, VidyoRoom, etc.).

Note: With LDAP enabled, the Forgot your password? link on the User VidyoPortal login page and the Change Password link on the User My Account page are not available. The User Guide advises users to contact the LDAP system administrator to reset the password.

To enable LDAP authentication:

1. Import LDAP user information into the VidyoPortal as described in How to Import Users on page 89.
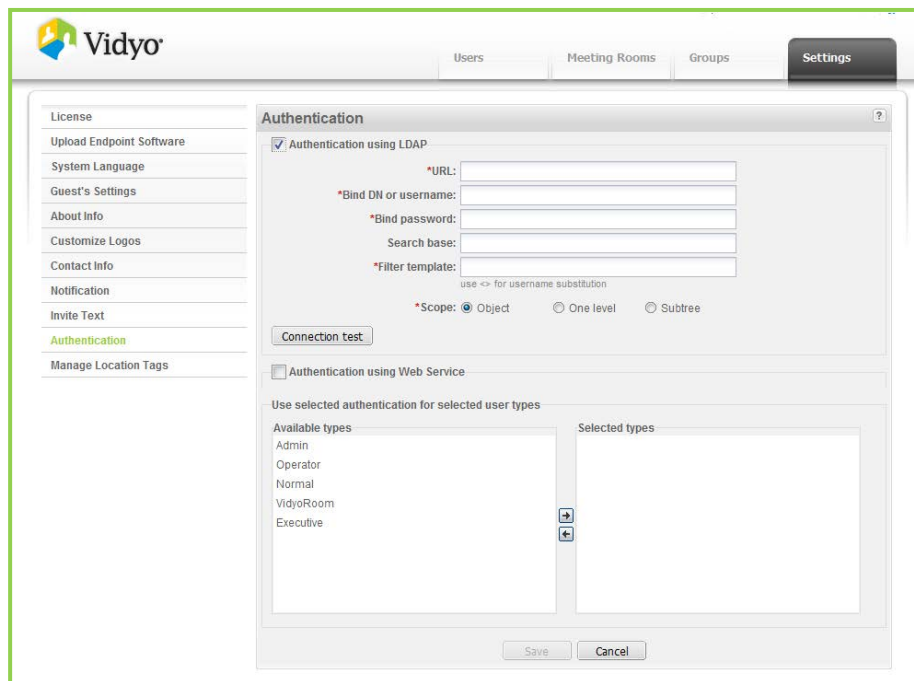
    This requires you to export users from the LDAP database to a `.csv` file.

107

Note: All users must have the same domain.

2. In the Authentication tab, select Authentication using the LDAP checkbox.

   The Authentication screen expands.

3. Enter the following information:

   ■ **URL** — Enter the LDAP server URL. The format is: ldap://ip_address:389

   ■ **Bind DN or username** — Enter the bind DN or user name to log into the LDAP server.

      For example, uid=user, ou=employees, dc=vidyo, dc=com.

      The user must be able to search the LDAP tree.

   ■ **Bind password** — Enter the password needed to bind with the LDAP server.

   ■ **Search base** — (Optional) The base object (baseObject) used for searching.

      For example, ou=employees, dc=vidyo, dc=com.

   ■ **Filter template** — Enter the configuration string to return the LDAP Distinguished Name (DN).

      For example, uid=‹› where "‹›" is replaced by the VidyoPortal user name during authentication.

   ■ **Scope** — Specify the base object (baseObject) to search. This can be one of the following:

      ■ **Object** - Search the named entry; typically used to read just one entry.

      ■ **One level** - Search the entries immediately below the base DN.

      ■ **Subtree** - Search the entire subtree starting at the base DN.

4. From the Available types list, select one or more user types to validate by LDAP

5. Click the Right Arrow button to move it/them to the Selected types list.

6. Click the Connection test button.

7. In the pop-up that appears, enter the LDAP user name and password.

8. If validation is successful and the LDAP settings are working, click the Save button to save the LDAP settings.

9. If validation fails, use a third-party LDAP tool such as LDAP Browser and try the same connection string you are using with the VidyoPortal.

    This will determine whether your LDAP settings are correct or not.

10. Verify LDAP authentication by logging into the VidyoPortal.

    If the login fails:

11. Verify that the user name and password are correct.

12. Verify the connection to the LDAP server.

    Normal users cannot log into the VidyoPortal until LDAP server connectivity is restored. For security reasons, there is no fallback to the VidyoPortal database.

Manage Location Tags

Location Tags are a feature of the new VidyoRouter Cloud architecture. The next chapter explains Location Tags in detail.
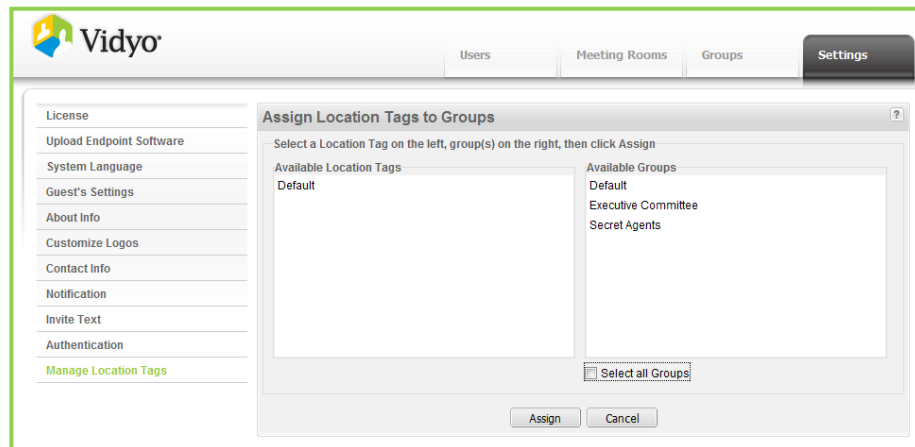
This screen allows you to assign default locations tags to groups. That way, if a user account is created without assigning it a Location Tag the user will inherit the default Location Tag for the Group he or she is in.

The onscreen instructions are well explained on the screen. To recap:

1. Select a Location Tag on the left-hand side of the screen.

2. Select one or more Groups (or all of them, via the Select All Groups Option).

3. Click the Assign button.

Note, before this task can be performed the Super Admin must have created Location Tags as explained on page **112**.

19.   *Admin/Tenant Admin Settings*

UNDERSTANDING THE VIDYOROUTER CLOUD

The VidyoRouter Cloud is an optional advanced topology for configuring VidyoRouters in the VidyoConferencing system. You can configure it at initial installation or do so at a later date, when your organization's network growth can benefit from it.

VidyoRouter Cloud Edition's top benefits include:

- More efficient network bandwidth utilization

- Improved end user experience in conferences by localizing traffic

- Support for large conferences spanning multiple VidyoRouters

- Shared capacity with floating licenses among regions

VidyoRouter Cloud Edition allows you (the Super Admin) to automatically assign each endpoint to a Pool of VidyoRouters based on rules you set up.

To recap and expand on what we covered in VidyoRouter Pools on page **70**, each VidyoRouter can handle 100 simultaneous users. If you need greater capacity you can add additional VidyoRouters.

Before VidyoRouter Cloud Edition, however, if one VidyoRouter reached its saturation point of 100 simultaneous users for a conference, any additional connection attempts would be refused, even if a second VidyoRouter in the same pool is hosting say, only 24 users. There was no way the first VidyoRouter could utilize the second VidyoRouter's unused capacity.

However, once VidyoRouter Cloud Edition is set up, when one VidyoRouter hits maximum capacity, instead of additional callers to the same conference failing to connect, they can be *cascaded* onto another VidyoRouter. If the second VidyoRouter maxes out, it can cascade to a third VidyoRouter in the pool and so on.

VidyoRouters in the same pool are usually in the same geographical location. VidyoRouters in different geographical locations should be allocated to different pools. So users can use their local VidyoRouters to join the same conference. (Before VidyoRouter Cloud Edition, all users in a given conference had to use the same VidyoRouter.)

Endpoint Classes and Rules Explained

To recap, an endpoint is any device that can be used to participate in a direct (point-to-point) call or a conference (e.g., VidyoDesktop, VidyoRoom and VidyoGateway). An Endpoint Class is a logical (as opposed to geographical) group of endpoints.

Each Endpoint Class defines a set of Router Pools to use and the order in which the system should attempt to connect to them. Each Endpoint Class has a set of rules, which is used to assign an endpoint to that class. You (as the Super Admin) create the assignment rules and the Router Pool information when you create the Endpoint Class.

As Super Admin you determine the order in which Endpoint Classes are evaluated. The first Endpoint Class containing a rule that matches the endpoint's information is the Endpoint Class that endpoint is assigned to.

Each Endpoint Class must have at least one rule and it can have as many rules as your network topology, setup and usage patterns require. There are only three kinds of rules.

- A rule can be based on a single local or (NATed) external IP or a range of IP addresses.

- A rule can be based on a Location Tag

  See below for how to create and assign Location Tags.

- A rule can be based on an Endpoint ID (for special situations)

  Each endpoint has a unique character string, called its Endpoint ID, which it automatically sends to the VidyoManager to identify itself.

As part of the process or setting up endpoint classes we recommend that you set up a catch-all rule that will accept all endpoints that do not match any of the endpoints classes you create. The catch-all can be an endpoint class that uses IP 0.0.0.0/0.

How to Create a User Location Tag

A Location Tag is a geographically-based name that can be assigned to a set of users, groups or guests. Each user is assigned a Location Tag when his or her account is created. It's a mandatory field. However, using location tags as the basis for a rule is optional. But it's a good idea to associate a user with his or her most used location. The user's Location Tag would be associated to a particular VidyoRouter Pool.

Location Tags are created by a Super Admin. Here's how it's done.

1. Log in as the Super Admin.

2. Select Components on the top navigation bar.

3. Click Manage Vidyo Cloud on the left-hand menu.

4. Click on the Location Tags tab under Vidyo Cloud.
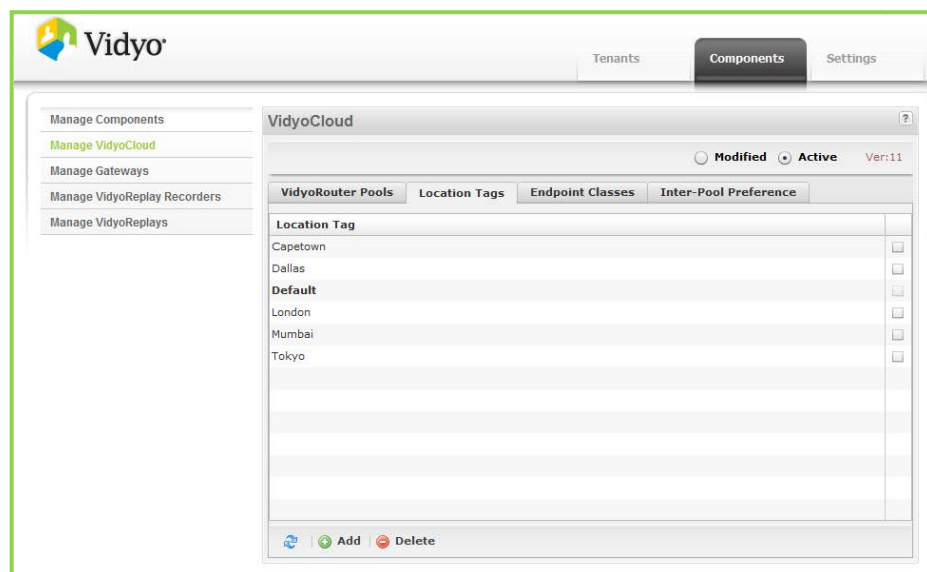
5. Click the Add button.

6. A little pop-up slides up where you can add a location.
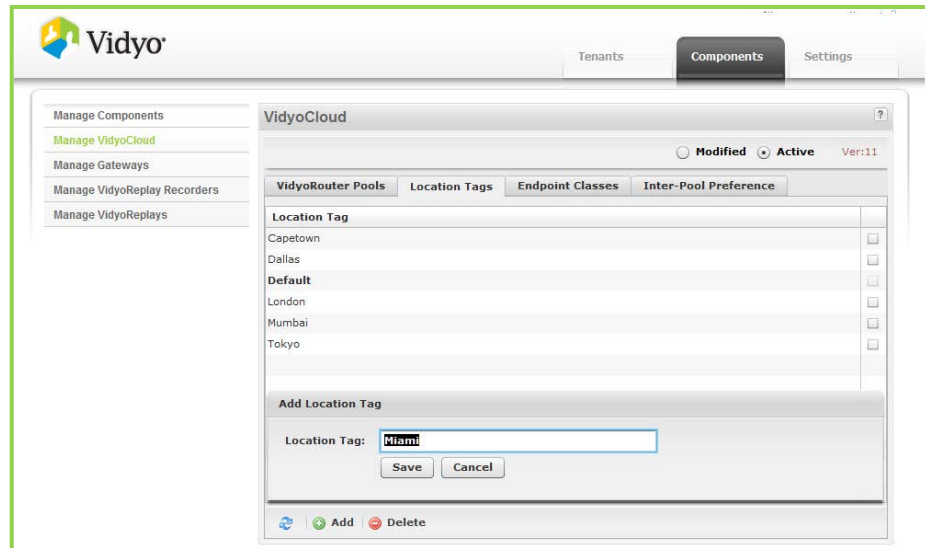
7. Enter the name of the Location Tag you wish to create and click Save.

For instructions on how to assign Location Tags to tenants see Assign Location Tags on page . It's part of the Managing Tenants chapter that begins on page .
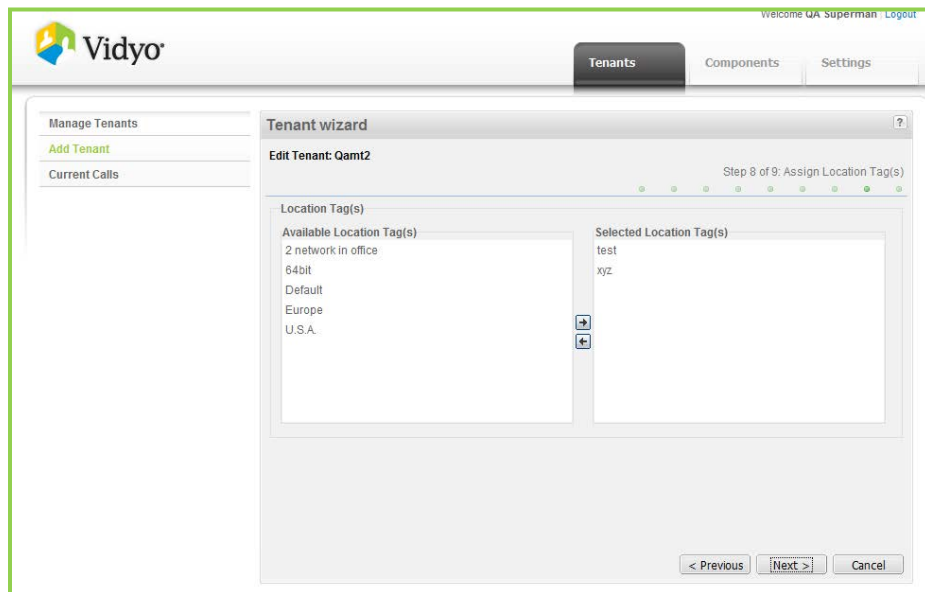
How to Create an Endpoint Class and Set Rules For It

Remember that you can create Endpoint Classes only after you have set up your VidyoRouter pools as described on page .

1. Login as the Super Admin user at your Super Admin portal.

2. Click the Components tab at the top navigation menu.

3. Click Manage Vidyo Cloud on the left-hand menu.

4. In the Vidyo Cloud table click the Endpoint Classes tab.
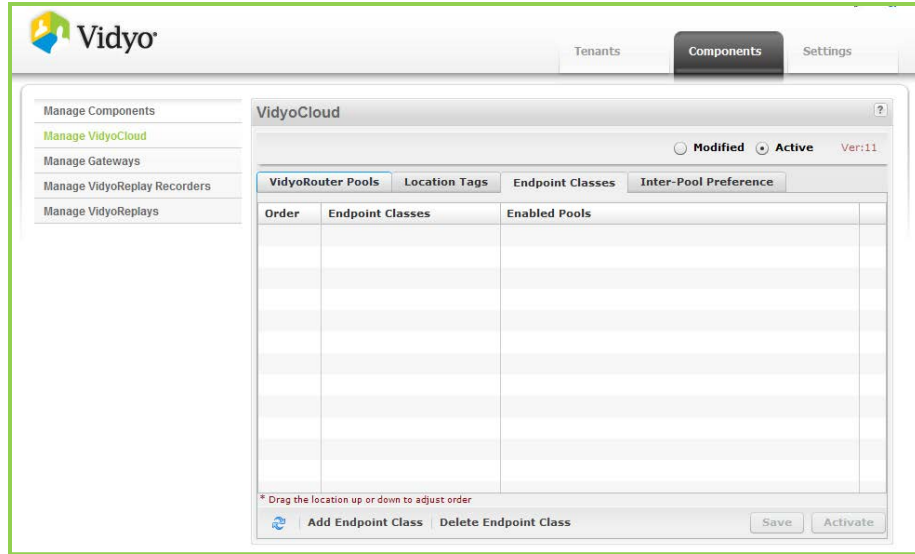
5. Click the Modified option button to start editing the active configuration.

   The very first time you do this there won't be a Modified button. Refer to the explanation on page **62**.
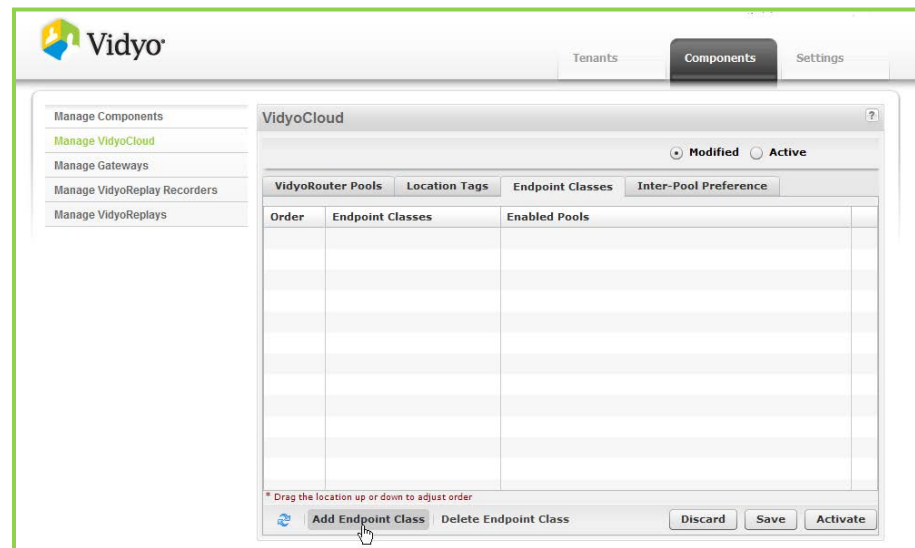
6. Click the Add Endpoint Class button.
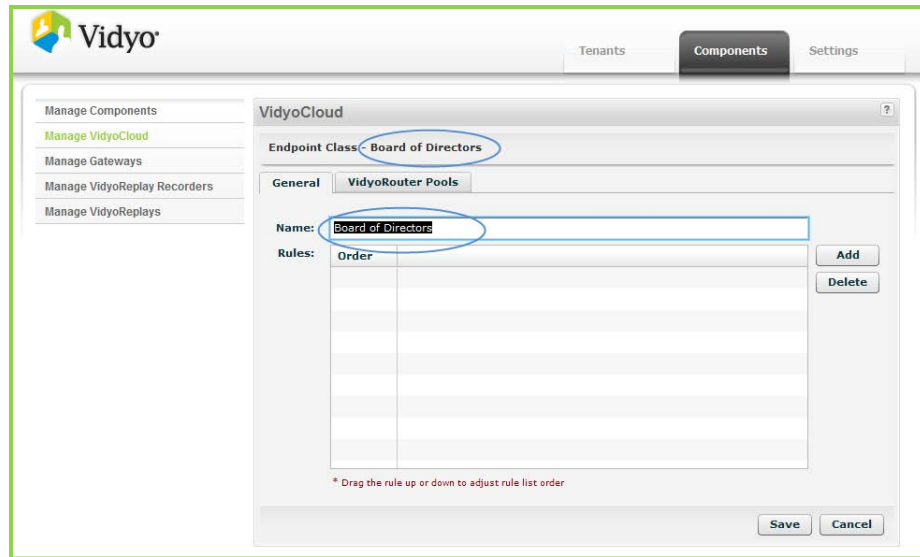
7. Type a name for the Endpoint Class.

   Note that as soon as you begin typing the name it appears as the title of the Endpoint Class above the name field. You can't click the Save button just yet. You need to make one or more rules that govern which pools the endpoints in this Endpoint Class will connect to.

Creating Rules

You must create at least one rule per Endpoint Class.

1. Click the Add button to create a rule.

   The Rule dialog box opens.
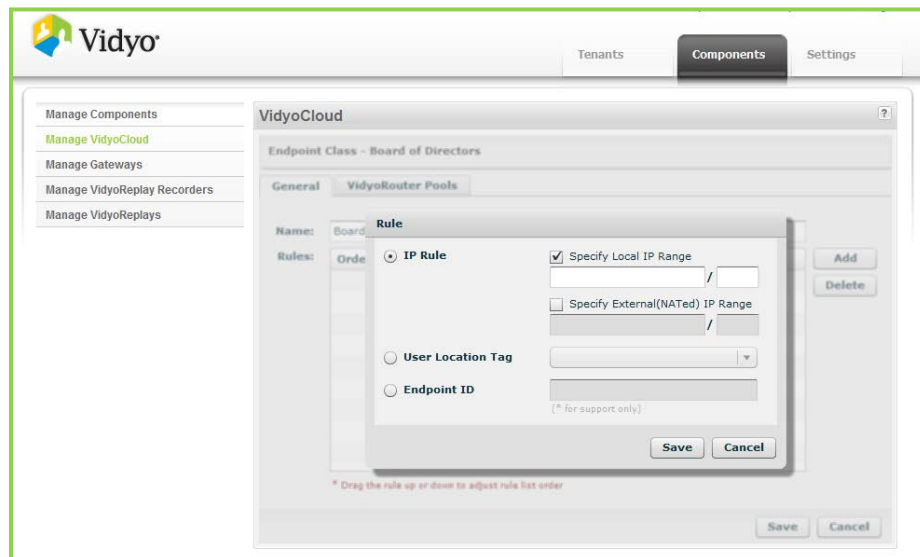
You can set only one rule in the Rule dialog box. Once you save it you can create additional rules by clicking the Add button again (as many times as you require to create as many rules as you want.) Remember, you're setting the rules for just this one Endpoint Class. After you've created other Endpoint Classes you can create rules for them.

2. Enter the rule you wish to set.

3. Click the Save button.

   Pretty easy, right? The only thing you need to know now is what the rules actually mean.

   IP Rule – This is the most obvious one. Most of the time you'll likely specify a range of local or external IP addresses.

   User Location Tag – Once you have created location tags as explained on page , they will appear in the User Location Tag dropdown list.

   Endpoint ID – An endpoint's unique identifier. (This is used only in consultation with Vidyo Customer Service.)

   As soon as you click the Save button you've created your first Endpoint Class and your first rule.
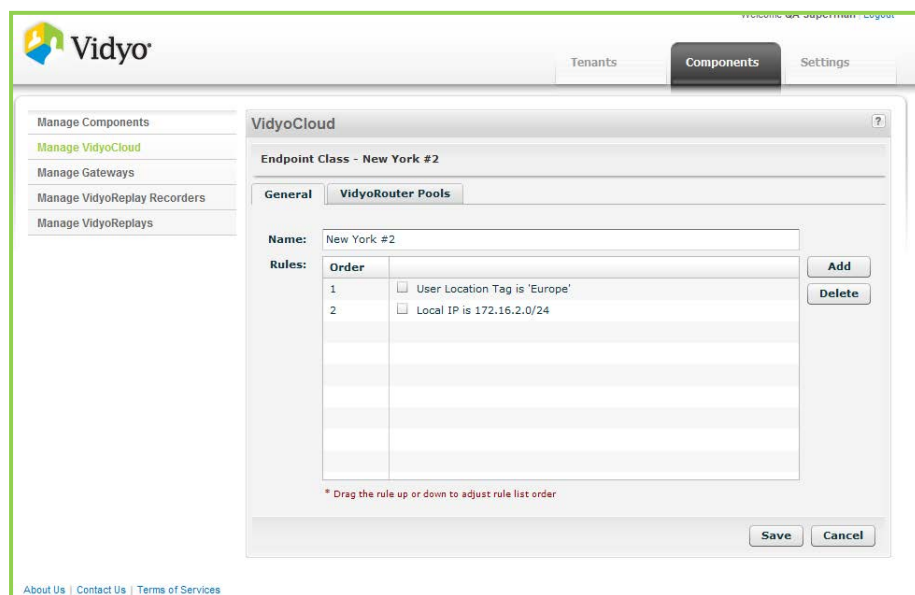
- To add another rule to this Endpoint Class click the Add button.

- To delete a rule select the checkbox that precedes it, then click the Delete button.

- After you have added or deleted a rule be sure to click the Save button.

- When you have multiple rules for an Endpoint Class you can change the order in which they're checked by dragging and dropping them in this list. The rules are applied in order from top to bottom.

How to Configure Inter-Pool Preferences

You can specify the priority that VidyoRouter Pools use when cascaded to other VidyoRouter Pools. For example, if you have VidyoRouter Pools in Sydney, Tokyo and New York you probably don't want your Sydney pool to cascade to your New York pool—at least not right off the bat. You'd probably want your Sydney pool to cascade to your Tokyo pool and as a second choice maybe your New York pool. Or you could specify that it never cascade to New York.

Inter-Pool Preference is a flexible tool that helps you get optimal usage out of the bandwidth you have between various VidyoRouter Pools you may have across the country or around the world. And it's easy to configure.

1. Log in as Super Admin

2. Click the Components tab on the top navigation bar

3. Click Manage Vidyo Cloud on the left-hand menu.

4. Click the Inter-Pool Preference tab in the Vidyo Cloud table.

If you study the screenshot below we bet you can probably figure out how this works by yourself. But in case you haven't had your first cup of coffee or tea today we'll explain the process.

5. First, note that the table lists all of your (or in this particular case, our) VidyoRouter Pools in the same order along *both* the vertical left-hand side of the table *and* across the top of the table.

6. Look at the drop-down menu that's at the intersection of VidyoRouter Pool VR2 along the top row and VidyoRouter Pool VR4 on the left-hand side.

7. All you have to do is go through the intersecting cells for all of your VidyoRouter Pools and click on whatever word is in that cell.

When you click in a cell a dropdown menu appears. As you can see you have four options:

   ■ High

   ■ Medium

   ■ Low

   ■ None

   (The default option is Medium)

8. Select the option for the cascading priority you want to set between the two VidyoRouter Pools.

117

Although performing this task is dead easy, as you can see, you might want to give some thought, before you start, to the physical locations of your pools and your existing and projected bandwidth and usage patterns

9. Repeat with all the VidyoRouter Pool pairs whose priority you want to change from medium.

10. As you work your way through the matrix click the Save button early and often, as you would if you were using a word processor or spreadsheet program.

   The first time you click the Save button the following dialog box appears.
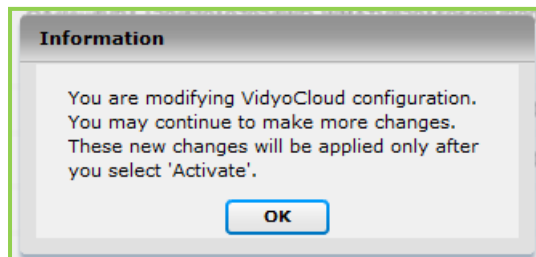
   In addition, a Discard button will appear so you can abandon your changes.

11. Click OK

12. When you're all done click the Activate button to activate your changes.

   When you click Activate the following dialog box appears to remind you that enabling your changes will disconnect everybody using the system.
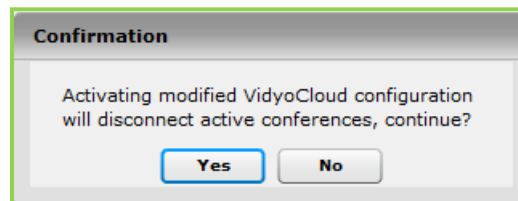
13. Click Yes

   Once you click yes, one final dialog box appears.
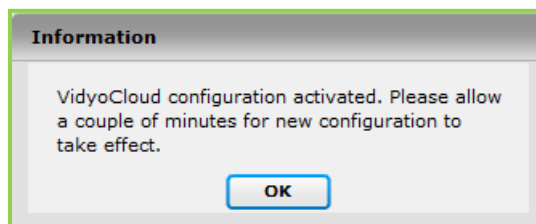
   The system has to restart in order for your changes to take effect.

14. Click OK

Congratulations. You've configured VidyoRouter Cloud Edition.

HDD Access LED **1**

LAN2 LED **2**

LAN2 LED **3**

Power LED **4**

LED	Display Status	Description
HDD Access LED	OFF	No Activity
	Blinking	HDD Data Read/Write
LAN LEDs (1, 2)	OFF	No LAN Connection
	ON	LAN connection is present
	Blinking	LAN is transmitting or receiving data
Power LED	ON	System power on
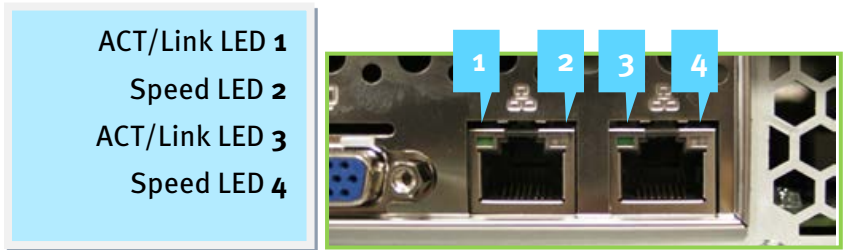
ACT/Link LED **1**

Speed LED **2**

ACT/Link LED **3**

Speed LED **4**

ACT/Link LED		Speed LED	
Status	Description	Status	Description
OFF	No link	OFF	10 Mbps connection
GREEN	Linked	ORANGE	100 Mbps connection
BLINKING	Data Activity	GREEN	1 Gbps connection

SERVER INSTALLATION

This section provides a quick setup checklist to get your VidyoPortal up and running. Following the steps in the order given should enable you to have the system operational within a minimal amount of time.

Unpacking the System

You should inspect the box the VidyoPortal was shipped in and note if it was damaged in any way. If the server itself shows damage, you should file a damage claim with the carrier who delivered it. Decide on a suitable location for the rack unit that will hold the VidyoPortal. It should be situated in a clean, dust-free area that is well ventilated. Avoid areas where heat, electrical noise and electromagnetic fields are generated. You will also need it placed near a grounded power outlet.

Preparing for Setup

The VidyoPortal does not ship with a rack rail hardware package as the system can be rack mounted without the use of rails. An optional rack rail package is available if you wish to order from your vendor. Follow the steps in the order given to complete the installation process in a minimal amount of time. Please read this section in its entirety before you begin the installation procedure outlined in the sections that follow.

Choosing a Setup Location

- Leave enough clearance in front of the rack to enable you to open the front door completely (~25 inches).

- Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.

- This product is for installation only in a Restricted Access Location (dedicated equipment rooms, service closets and the like).

Rack Precautions

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.

- In a single rack installation, stabilizers should be attached to the rack.

- In multiple rack installations, the racks should be coupled together.

- Always make sure the rack is stable before extending a component from the rack.

- You should extend only one component at a time—extending two or more simultaneously may cause the rack to become unstable.

Server Precautions

- Review the electrical and general safety precautions.

- Determine the placement of each component in the rack before you install the rails.

- Install the heaviest server components on the bottom of the rack first, and then work up.

- Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes and to keep your system operating in case of a power failure.

■ Always keep the rack's front door and all panels and components on the servers closed when not servicing to maintain proper cooling.

Rack Mounting Considerations on Ambient Operating Temperature

If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).

Reduced Airflow

Equipment should be mounted into a rack so that the amount of airflow required for safe operation is not compromised.

Mechanical Loading

Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.

Circuit Overloading

Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on overcurrent protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Ground (Earth)

A reliable ground must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (i.e. the use of power strips, etc.).

Basic Installation Procedure

The VidyoPortal server comes with two rack mounting brackets, which are located on each side at the front of the chassis. To mount the system into a rack, simply screw these brackets directly to the front of the rack (two screws for each bracket). The brackets can be located at the front of the chassis or moved approximately one-third to the rear of the chassis.

Installing with Rack Mount Kit

This section is only for customers that have the optional rack mount kit. Each of these assemblies consists of two sections: an inner rail that secures to the chassis and an outer rail that secures directly to the rack itself. This is a guideline for installing the unit into a rack with the optional rack kit. You should also refer to the installation instructions that came with the rack unit you are using.

Be aware that there are a variety of rack units on the market, which may mean the assembly procedure will differ slightly.

Installing the Chassis Rails

The two rail sections must be detached from each other prior to installation. Do this by depressing the locking tab on the inner rail to release it from its locked position then pull the two rails completely apart. Do this for both the left and right side rack rail assemblies.

Position the fixed chassis rail sections you just removed along the side of the chassis making sure the three screw holes line up. Note that these two rails are left/right specific. Screw the rail securely to the side of the chassis. Repeat this procedure for the other rail on the other side of the chassis. You will also need to attach the rail brackets when installing into a Telco rack.

Locking Tabs

Both chassis rails have a locking tab, which serves two functions. The first is to lock the server into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the server in place when fully extended from the rack. This prevents the server from coming completely out of the rack when you pull it out for servicing.

Installing the Server into the Rack

You should now have rails attached to both the chassis and the rack unit. The next step is to install the server into the rack. Do this by lining up the rear of the chassis rails with the front of the rack rails. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting).

When the server has been pushed completely into the rack, you should hear the locking tabs "click." Finish by inserting and tightening the thumbscrews that hold the front of the server to the rack.

Installing the Rack Rails

Determine where you want to place the Vidyo server in the rack. Position the fixed rack rail/sliding rail guide assemblies at the desired location in the rack, keeping the sliding rail guide facing the inside of the rack. Screw the assembly securely to the rack using the brackets provided. Attach the other assembly to the other side of the rack, making sure that both are at the exact same height and with the rail guides facing inward.

Installing The Server Into a Rack With The Optional Rackmount Kit
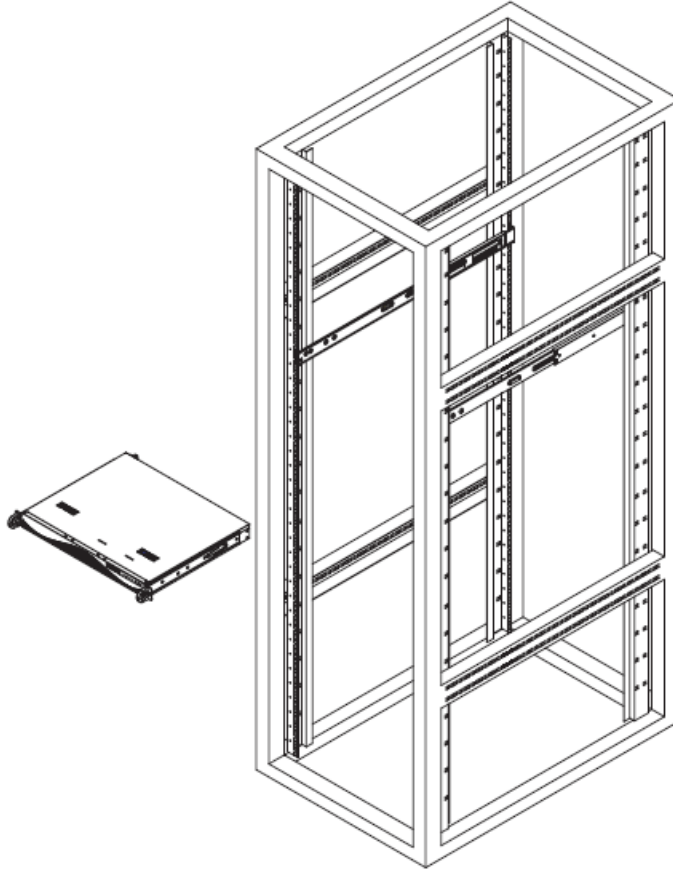
Installing the Server into a Telco Rack

If you are installing a Vidyo server into a Telco type rack, follow the directions given on the previous pages for rack installation. The only difference in the installation procedure will be the positioning of the rack brackets to the rack. They should be spaced apart just enough to accommodate the width of the Telco rack.
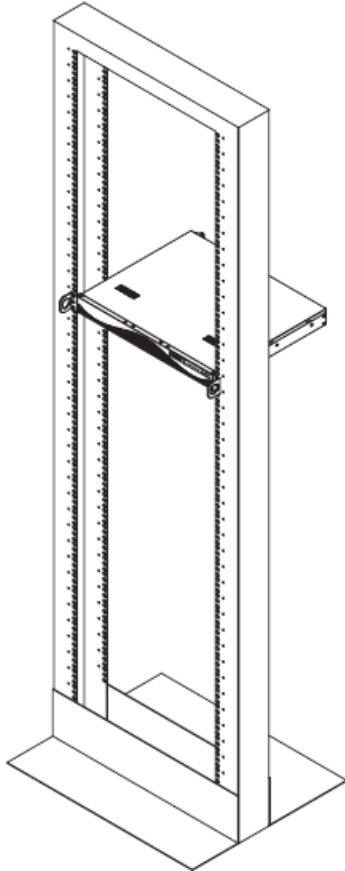
23. *Console/Shell Admin Menu Appendix*

Basic setup for all VidyoServers (VidyoPortal, VidyoRouter, VidyoGateway (optional) and VidyoReplay (optional) are performed at the console/shell admin menu. You access this menu by plugging a VGA monitor and a USB or PS2 keyboard directly into the server you intend to configure. Alternatively, If you're skilled at using SSH, you could log in using an SSH client. Either way you must also use an Ethernet cable to connect the server to your network.

```
 1. Configure IP Address
 2. Configure DNS Nameserver
 3. Configure NTP Time Servers
 4. Configure Time Zone
 5. Configure Ethernet Options
 6. Display IP Address
 7. Display Host & Domain Names
 8. Query NTP Time Servers
 9. Display Kernel IP Routing Table
10. Display ARP Table
11. Ping Utility
12. Traceroute Utility
13. Set 'admin' password
14. Reboot system
15. Shutdown System
16. Restore HTTP(S) settings to default
 x. Exit System Administrator Console

Selection: █
```

Note: The VidyoGateway console/shell admin menu does not include option `16. Restore HTTP(S) settings to default`.

For information on how to access the console/shell admin menu see the (separate) Vidyo Server Getting Started Guide.

Be sure to change the admin password for the console/shell admin menu using option `13. Set 'admin' password`.

The following table describes the console/shell admin menu commands available in the System Administrator Console used to configure initial network settings. Use these commands as appropriate to manage your Vidyo server.

Menu Command	Function	Sample Settings
1. Configure IP Address	Sets the server IP address and subnet mask and default gateway addresses. Initially, information must be configured locally.	**IP Address:** 192.168.1.100 **Subnet Mask:** 255.255.255.0 **Default Gateway:** 192.168.1.1

Menu Command	Function	Sample Settings
2. Configure DNS Nameserver	Specifies the Domain Nameserver. This information must be configured locally.	**Hostname:** server **Domain Name for Host:** xyzcompany.com **IP Address for Host:** 127.0.1.1 **NOTE:** Never change the host IP address. **Fully Qualified DN (FQDN):** server.xyzcompany.com **Primary DNS Server for** **Host:** 208.67.222.222 **Secondary DNS** **Server for Host:** 208.67.220.220
3. Configure NTP Timeservers	Sets the NTP (Network Time Protocol) timeservers. Change to synchronize the system with a different timeserver.	**Primary NTP Server:** time.nist.gov **Secondary NTP Server:** time-a.nist.gov **Tertiary NTP Server:** time-b.nist.gov
4. Configure Time Zone	Specifies the time zone you are working in. Change as needed for accurate billing records.	US/Eastern
5. Configure Ethernet Options	Sets the MTU (Maximum Transmission Unit) size. The default is 1500. Change if network MTU size is less than 1500. Turns autonegotiation on or off. It is on by default.	**MTU Size:** 1500 Autonegotiation: On

Menu Command	Function	Sample Settings
6. Display IP Address	Displays current IP address settings, IP address mode. You cannot change IP addresses in this screen.	**IP Address Mode:** STATIC **IP Address:** 192.168.1.100 **Subnet Mask:** 255.255.255.0 **Default Gateway:** 192.168.1.1
7. Display Host and Domain Names	Displays current host and domain name settings. You cannot change these settings in this screen.	**Hostname:** server **Domain Name for Host:** xyzcompany.com **IP Address for Host:** 127.0.1.1 **NOTE:** Never change the host IP address. **Fully Qualified DN (FQDN):** vidyo.com **Primary DNS Server for Host:** 208.67.222.222 **Secondary DNS Server: for Host:** 208.67.220.220
8. Query NTP Times	Queries the NTP servers. This command will not work if the domain name server is not defined.	
9. Display Kernel IP Routing Table	Displays how the server is configured for Ethernet routing. This information is display only.	
10. Display ARP Table	Displays router and MAC address information. This information is display only.	

Menu Command	Function	Sample Settings
11. Ping Utility	Pings network address. Press Control+C to stop pinging.	
12. Traceroute Utility	Displays the trace route to a specified address. You must enter the IP address of the device.	
13. Set 'admin' password	Sets the administrator password. The default is "admin." You should change this to a more secure password.	
14. Reboot System	Restarts the server. It can take up to a minute for the server to restart.	
15. Shutdown System	Shuts down the server.	
16. Restore HTTP(S) settings to default	Returns HTTP settings to their default values (HTTP and port 80) (This option is not included in the VidyoGateway console/shell admin menu.)	

NAT INTRODUCTION

The VidyoConferencing platform utilizes reflexive addressing to assist in the setup of Vidyo calls. Reflexive addressing is used when the end user is using VidyoDesktop to make a call from behind a NAT. This happens automatically and transparently to the user.

Reflexive addressing requires the VidyoRouter to have a public IP address in order to provide NAT traversal of the Vidyo endpoints. So if the VidyoRouter itself is placed behind a NAT, reflexive addressing won't work.

When the VidyoRouter is behind a NAT, the preferred configuration will use DNS to resolve properly to the server IP addresses. In some cases, a combination of the ICE and STUN protocols are used to determine the Public IP translated to the VidyoRouter. This appendix outlines how to configure the VidyoConferencing system to work when placed behind a NAT and still allow users to connect from the public Internet.

There are three basic areas that need to be addressed in order to configure the VidyoConferencing system to operate from behind a NAT. Each is explained in detail in the following sections.

- Firewall/NAT Configuration
- DNS configuration
- Vidyo Server configurations

There are several options to deploy the VidyoConferencing system in order to provide service for your entire organization:

- Place the VidyoPortal/VidyoRouter on a public Static IP address
- Place the VidyoPortal/VidyoRouter in a private network having a private Static IP address within the organization
- Place the VidyoPortal/VidyoRouter within the DMZ with a private Static IP address

In this section, we'll focus on the first scenario. Scenarios 2 and 3 for firewall and NAT traversal are covered in section three.

When deployed with a public IP address and no "server side" firewall or NAT, the Portal and VidyoRouter are reachable by either IP address or DNS name. This is the simplest scenario, since we're only concerned with the NAT and firewall at the far-end (client side).

Generally speaking, the client side firewall will most often permit any connection that initiates on the Private LAN to any outside network destination. In some cases, the local firewalls must be configured to allow each application from the inside to the Public Network.

VIDYOCONFERENCING FIREWALL PORTS

VidyoDesktop and VidyoRoom Requirements

To register to the Vidyo Portal and place calls, the client side connection must be open to the VidyoPortal on these TCP/UDP ports:

VidyoDesktop and VidyoRoom Connectivity to VidyoPortal and VidyoRouter		
TCP Port 80	HTTP: Outbound to Portal	Client to Portal authentication and GUI
TCP Port 443	HTTPS: Outbound to Portal (optional)	Optional for SSL connection to Portal
TCP Port 17992	EMCP: Outbound to Portal	Client connection to VidyoManager
TCP Port 17990	SCIP: Outbound to Portal	Client connection to VidyoRouter
UDP Ports 50,000 – 65,535	RTP/sRTP/RTCP: Bi-Directional to/from VidyoRouter	Audio and Video Media from participants (6 ports per participant). RTP and RTCP pair for each audio, video, and data collaboration stream.
UDP Timeout	General Comment	Change from Default (0:02:00 – 2 minutes) to something larger (e.g., 3:00:00 – 3 hours) to avoid call timeouts

Notes

- Some Firewalls have a UDP default timeout. On the Cisco PIX Firewall, for example, if the UDP timeout is not changed then the call will drop in exactly two minutes and the Vidyo client(s) would have to reconnect.

- The VidyoPortal also has an embedded VidyoRouter running on the same appliance. It's possible these will share the same IP address.

- Many newer consumer home firewalls have SPI (Stateful Packet Inspection) active by default. This may need to be disabled for better performance.

Note: For VidyoConferencing clients who are behind restricted firewalls where the ports above cannot be opened, Vidyo provides the VidyoProxy to address these users. Please refer to the VidyoProxy Appendix that begins on page .

Vidyo Server Requirements

To enable remote management access to the Vidyo servers, the following TCP/UDP ports need to be opened through any server-side firewall or NAT:

Management Access to VidyoPortal, VidyoRouter, VidyoManager and VidyoGateway		
TCP Port 80	HTTP: Inbound to Server	Web Access to VidyoPortal and VidyoRouter
TCP Port 443	HTTPS: Inbound to Server (optional)	Secure Web Access to VidyoPortal and VidyoRouter

Management Access to VidyoPortal, VidyoRouter, VidyoManager and VidyoGateway		
TCP Port 2222	SSH: Inbound to Server	SSH access to the VidyoPortal and VidyoRouter.

The following services outline the ports required for VidyoCloud cascading.

VidyoCloud Connectivity to VidyoPortal and VidyoRouter to VidyoRouter		
TCP Port 80	HTTP: Router to Portal	Client to Portal authentication and GUI.
TCP Port 443	HTTPS: Router to Portal (optional)	Optional for SSL connection to Portal.
TCP Port 17991	RMCP: Router to Portal	Router connection to VidyoManager.
TCP Port 17990	SCIP: Bi-Directional to/from VidyoRouters	Signaling connections between VidyoRouters.
UDP Ports 50,000 – 65,535	RTP/sRTP/RTCP: Bi-Directional to/from VidyoRouters	Audio and Video Media from participants (6 ports per participant). RTP and RTCP pair for each audio, video, and data collaboration stream.

The following services are optional on the VidyoPortal, VidyoRouter and VidyoGateway, and require the following TCP/UDP ports if they are used:

Other Services on VidyoPortal, VidyoRouter and VidyoGateway		
UDP Port 123	NTP: Outbound from Server	Network Time Protocol.
TCP Port 25	SMTP: Outbound from Server	Email notifications for new user accounts, lost passwords, and licensing notifications. VidyoPortal only.
TCP Port 3306	MySQL: Inbound to Server	Call Detail Record (CDR) access for billing systems. VidyoPortal only
TCP Port 389	LDAP: Outbound from Server	Optional authentication to LDAP/Active Directory.
TCP Port 636	LDAPS: Outbound from Server	Secure LDAP. Optional authentication to LDAP/Active Directory.
UDP Port 161 - 162	SNMP: Inbound to Server	Basic SNMP functions.
TCP and UDP 3478	STUN: Bi-directional to/from Server	Optional only if using STUN for NAT traversal.

24. Firewall and NAT Deployments Appendix

STEPS TO CONFIGURE VIDYOCONFERENCING WITH A FIREWALL/NAT

In this section, we'll discuss the steps to configure the VidyoPortal and VidyoRouter in a NATed firewall or DMZ environment. For this, the Vidyo servers are installed either fully behind a firewall on the corporate LAN, or installed in the firewall DMZ with one or more NATed addresses and Static IP address. The figure below illustrates an example of firewall/NAT topologies.

Example Dual Firewall/NAT Deployment
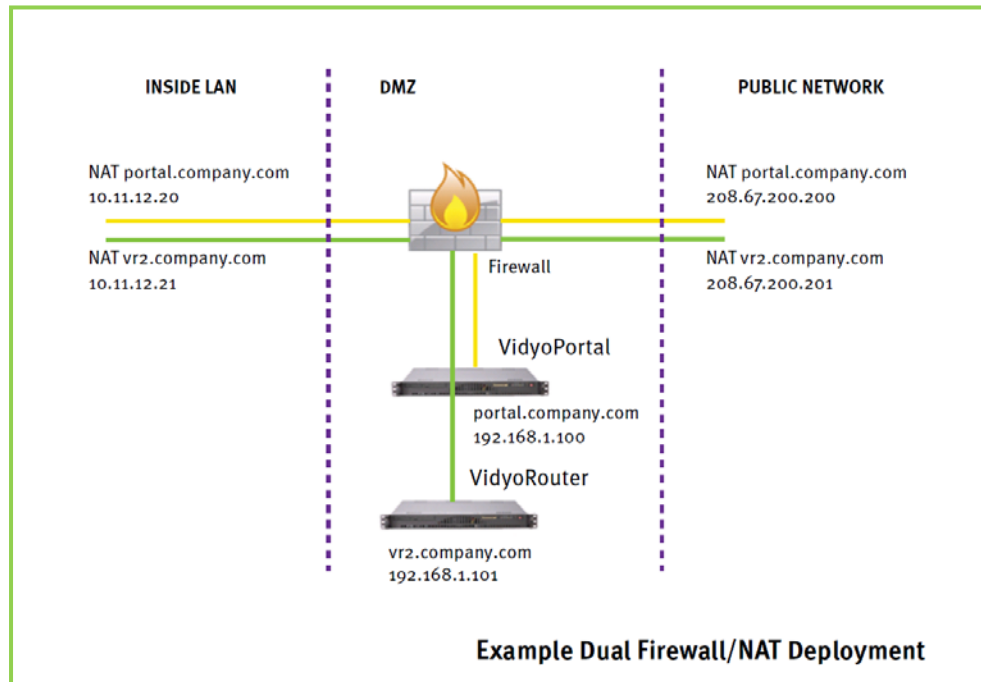
Note: This appendix doesn't apply to deployments using a VidyoProxy. Separate instructions are available for use with a VidyoProxy. The two deployment scenarios can coexist.

For this configuration, there are three tasks to accomplish:

1. Firewall/NAT Configuration
2. DNS configuration
3. Vidyo Server configurations

Note: Actual steps to configure the Firewall/NAT and DNS environments are outside the scope of this appendix, and will vary based on the Firewall/NAT and DNS servers to be used. This appendix focuses on the concepts only.

Firewall/NAT Configuration

Allocate an external (public) static IP address to use for the VidyoPortal/Routers and configure a one-to-one NAT statement to the desired private or DMZ static IP address. In cases where the internal network is NATed to the DMZ, a similar static NAT must be configured from the static private LAN to the Static DMZ server addresses.

With the NAT configured, you'll need to permit access to the TCP and UDP ports needed by the Vidyo solution. In the firewall access-control list, be sure to open these ports as a minimum:

- Inbound TCP Port 80 – web access to the portal and administrative interfaces

- Inbound TCP Port 443 – optional for SSL secured web access and calls

- Inbound TCP Port 17992 – EMCP protocol client connection to VidyoManager/VidyoPortal (configurable)

- Inbound TCP Port 17990 – SCIP protocol client connection to VidyoRouter (configurable)

- Bi-Directional UDP Port 50000 – 65535 – RTP/SRTP media, one RTP/RTCP port pair for each audio, video, data sharing stream in the conference

Lastly, it's beneficial to check the UDP timeout for the firewall. Some firewalls will limit the duration of UDP port openings, and this may cause the calls to terminate prematurely.

DNS/FQDN Configuration

For the firewall NAT traversal to properly communicate between servers and clients through the IP address translations, we will need to configure DNS properly for hosting the Vidyo servers in the DMZ or behind the NAT. In firewall deployments, Vidyo communicates based on DNS information rather than exposing IP addresses.

The DNS servers for both inside and outside networks (if different) will need to be configured for the Vidyo server's Fully Qualified Domain Name - FQDN. In our example, we are assuming the server is using the FQDN of portal.company.com.

Configure both public and private DNS records for the server FQDN. Regardless where the client resides, it needs to match the same hostname to the proper IP address, public Internet clients resolve to the outside NAT address, and internal WAN clients resolve to the inside IP address (either real IP or NAT inside address if double NAT is used) when they access the server URL. To test, from both the inside and outside subnets, ping to the server URL.

Vidyo Server Configuration

With the firewall configured for the proper NAT statements, the required TCP and UDP ports opened, and the DNS entries configured, you can move on to the configuration in the Vidyo servers to enable using DNS and to route calls properly between the LAN and Public Network.

You must configure the VidyoPortal and Routers to be aware of their DNS hostnames. This is done in the system console menu, option #2.

Set the server local hostname and domain name as well as the working DNS server address.

Note: It's very important to note that the IP address listed in this screen (127.0.1.1) must remain intact for proper communications.

In a firewalled installation, the VidyoManager, VidyoRouter(s) and VidyoProxy(s) need to be configured to use the server FQDN instead of the IP addresses.

Tenant URLs

1.   Login to the portal Super Admin pages, go to Tenants tab and select Manage Tenants:
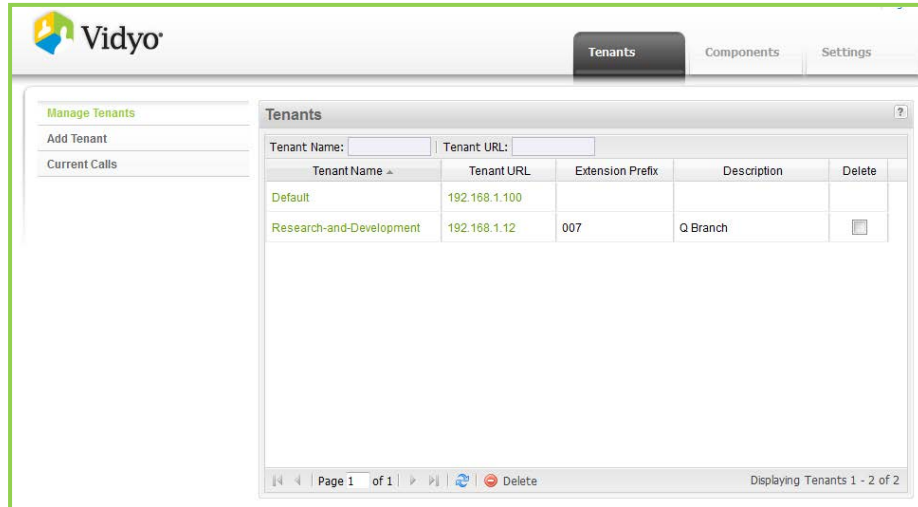
2.   Ensure that each Tenant (including the Default Tenant), is using a FQDN for Tenant URL.

VidyoManager Configuration

You will need to configure the VidyoManager to be addressed by its FQDN.

1.   Log in to the portal Super Admin pages, go to Components tab and select Manage Components,
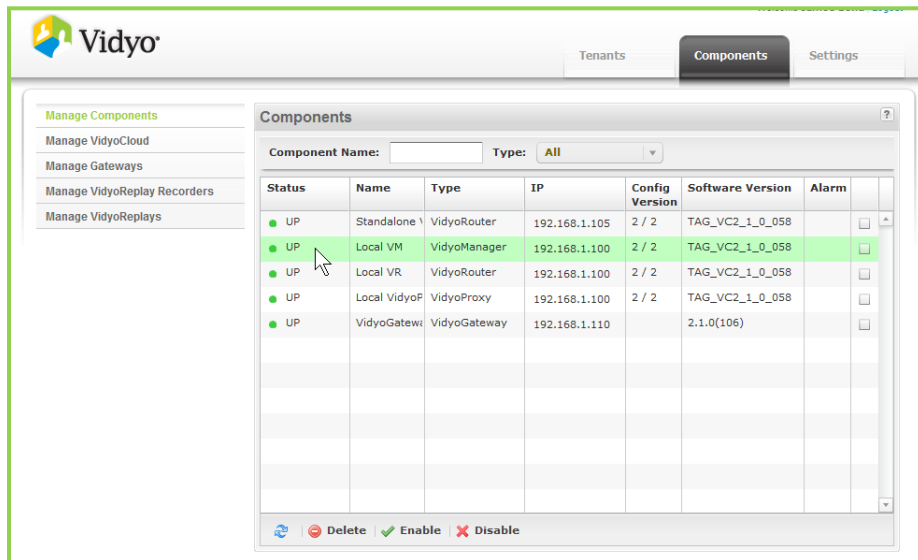
2.   Double-Click the Status of the VidyoManager entry:

3. Under Listen Address (EMCP), edit the EMCP address (VidyoManager address) by clicking the text in the IP column, and enter the server FQDN here, e.g., server.company.com.
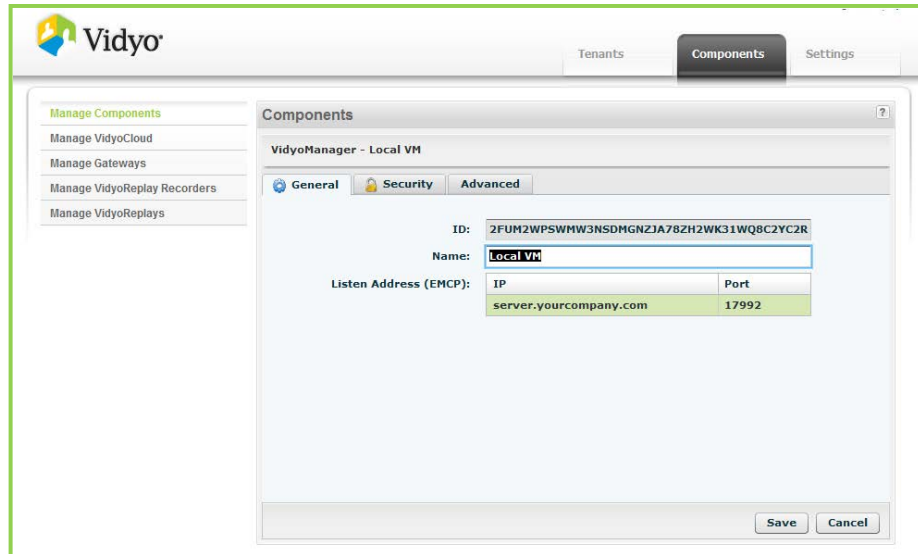
The EMCP Port column is where you can set the EMCP (VidyoManager) TCP Port. The default value for V2.0 is 17992; the default in V1 was 10000.

4. Edit the port according your needs and firewall rules.

5. Click the Save button.

VidyoRouter(s) Configuration

Next, you will need to configure each VidyoRouter to be addressed by its FQDN.

1. Return to the portal Super Admin pages, go to Components tab.

2. Select Manage Components.
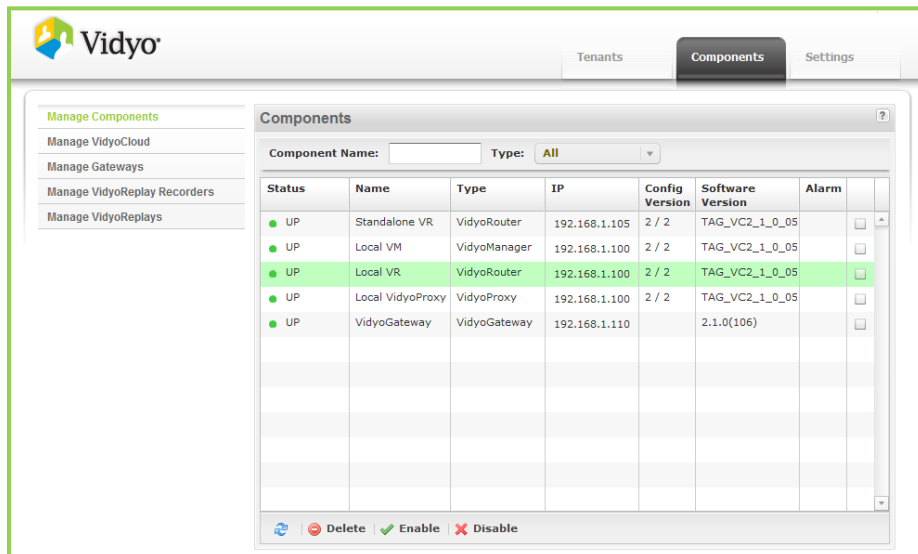
3. Double-Click the Status of the local (embedded) VidyoRouter entry.

135
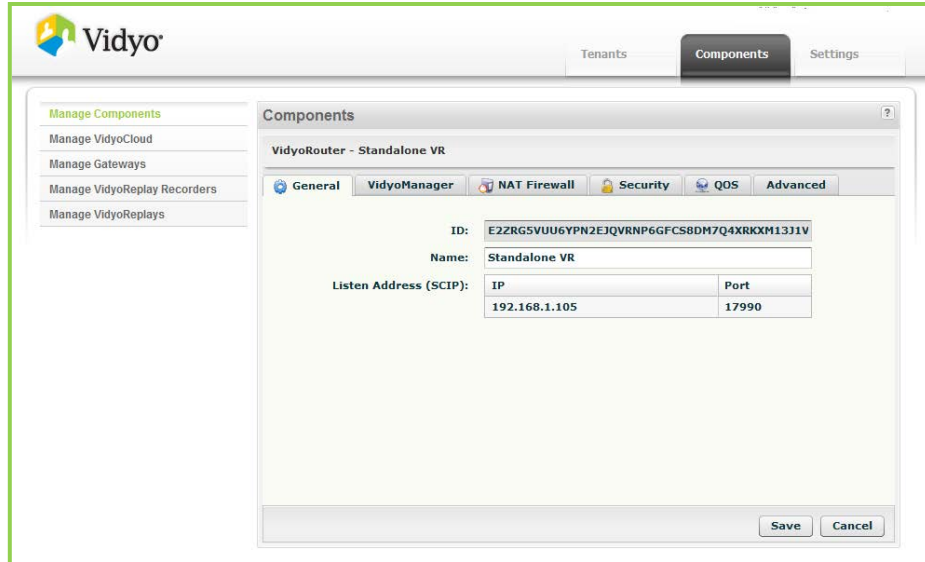
4. Under Listen Address (SCIP), edit the SCIP address. (VidyoRouter signaling address) by clicking the text in the IP column, and enter the server FQDN here—e.g., portal.company.com.

   The SCIP Port column is where you can set the SCIP (VidyoRouter) TCP Port. The default value for v2.0 is 17990; the default in v1 was 50000.

5. Edit the port according your needs and firewall rules.

   Next, you will need to configure the VidyoRouter to address its VidyoManager by FQDN.

6. In the VidyoRouter Component pages, go to VidyoManager tab.
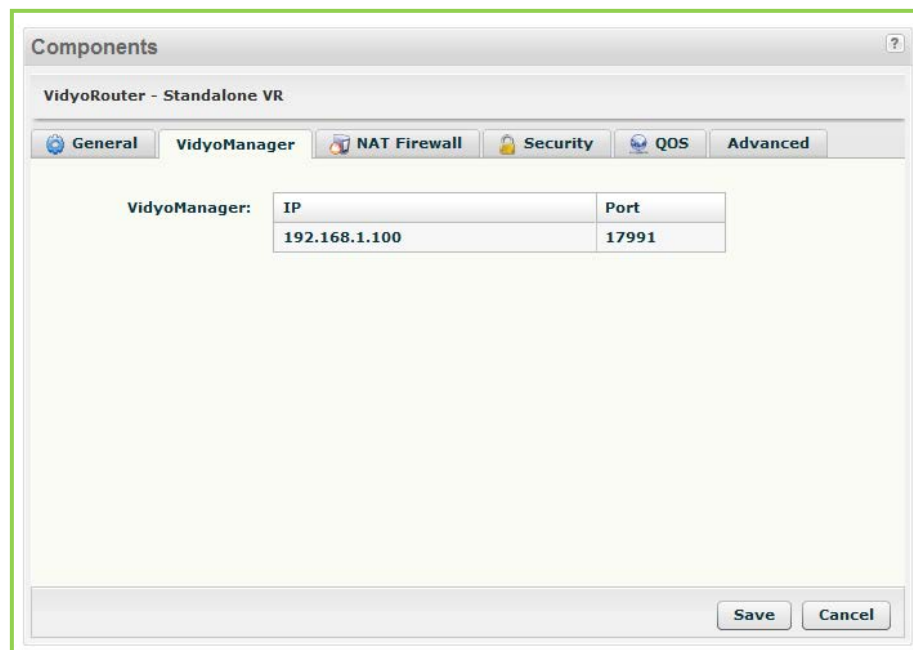
7. Under Vidyo Managers, edit the IP address by clicking the text in the IP column, and enter the server FQDN here—e.g., portal.company.com.

Next, you'll need to configure the VidyoRouter Media Mapping from private to public addresses.

8. In the VidyoRouter Component pages, go to the NAT Firewall tab.

9. Under Media Address Map, click the Add button and enter each NAT translation required.

10. For each NAT map, enter the Local IP Address (private) and Remote IP Address (public); the inside/outside NAT addresses needed.

   If there is a NAT from the private LAN towards the DMZ, you will need a media map rule for that.

11. Click the Save button.

In deployments where there is a dual NAT, one NAT from the public network to the server, and one from the private LAN to the server, there will be two Media Map statements.

As an alternative method to Media Address Mapping, you can choose to use a public STUN server. To use a STUN server, enter the IP or URL and Port of the public STUN server you wish to use. The default STUN port is 3478. Vidyo hosts a public STUN server at: stunusa.vidyo.com. Using a STUN server instead of Media Address Maps is needed when the Vidyo server is hosted behind multiple layers of NATs.

DO NOT configure both Media Address Maps *and* STUN; choose only one method. Configuring both will cause your system to malfunction.

REPEAT these steps for each additional Standalone VidyoRouter in your VidyoConferencing system

Each Standalone VidyoRouter server requires a unique and separate FQDN to the Portal server. Use each server's unique FQDN for the SCIP address on each VidyoRouter configuration.

For example: vr1.company.com, vr2.company.com, etc.

VidyoProxy(s) Configuration

Next, you will need to configure each VidyoProxy to be addressed by its FQDN.

1. Return to the portal Super Admin pages and go to Components tab / Manage Components:

2. Double-Click the Status of a VidyoProxy entry.

3. Under URL, enter the Proxy server's FQDN followed by the Proxy port, typically 443.
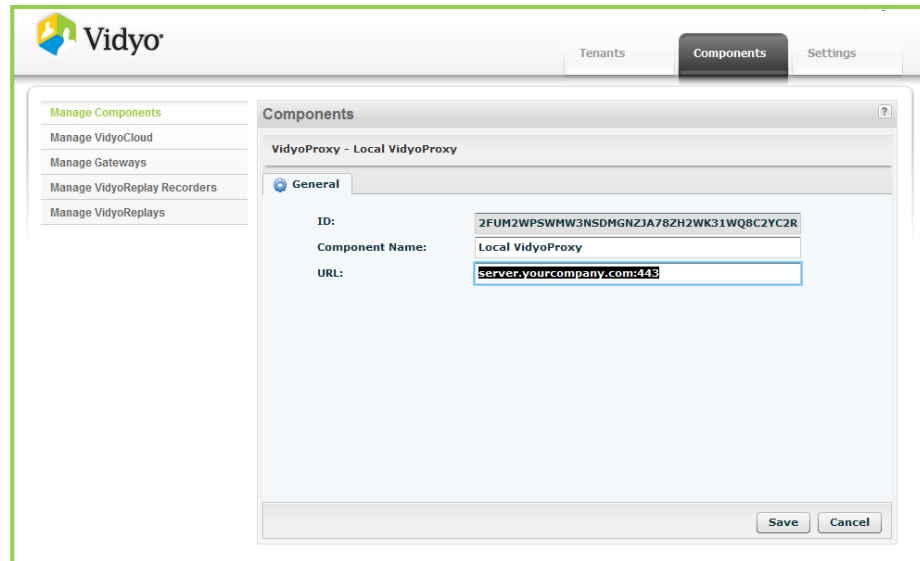
4. Click the Save button.

REPEAT these for each additional stand-alone VidyoProxy in your VidyoConferencing system

Use each server's unique FQDN for the address on each VidyoProxy configuration. You can use the same FQDNs as each standalone VidyoRouter uses that is hosting the Proxy—e.g., vr1.company.com, vr2.company.com, etc.

With the Firewall/NAT, DNS and Vidyo Server configurations completed, you can test the solution.

How to Test You Configuration

From both sides of the firewall/NAT, attempt to login to the VidyoPortal as a Normal user account. If the EMCP is traversing properly, the person icon in the upper left of the portal user page will turn **green**. If the icon remains grey, then either the EMCP address or port is not configured properly in the VidyoManager configuration, or the port is not configured correctly at the firewall/NAT.
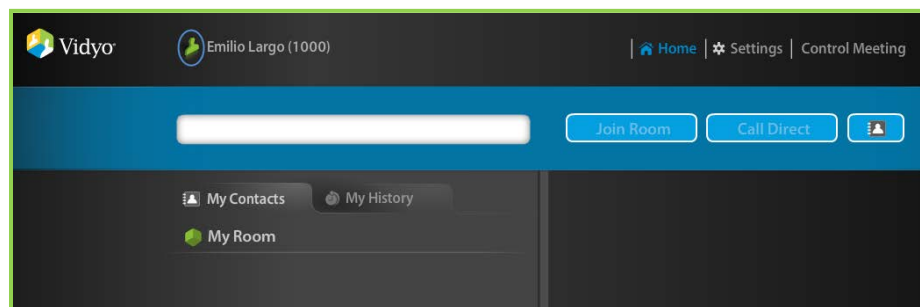
Once successfully logged in to the Portal, attempt to join the user's own Meeting Room ('My Room'). If a 'failed to Join conference' or 'failed to Join router' error message is received, then either the VidyoRouter SCIP address or port is not configured correctly in the VidyoRouter configuration, the port is not configured properly at the firewall/NAT, or the Portal server or client PC is unable to resolve the Router's FQDN.

1. Ensure that media connections succeed (send and receive video).

    Once successfully joined to the meeting room, you should see loopback video if you are the only participant in the room, or the video from other participants. If you receive loopback video, then it

means the media is traversing in both directions. If you receive another participant's video, ask them if they are receiving your video. If both sides are receiving each other's video, then that too means media traversal is working in both directions. If media traversal does not take place, then the UDP port range is not properly configured at the firewall/NAT.

2. Be sure to test from both the Inside LAN and from the Public Network by using the same URL—e.g., `http://<`portal.company.com`>`.

3. Also if using multiple Media Address Maps, test from each Remote network segment.

VIDYOPROXY SOLUTION FOR TRAVERSAL OF RESTRICTED NETWORKS

Overcoming Deployment Barriers Securely and Effectively

Utilizing the Internet to gain cost efficiencies is a significant advantage of the VidyoConferencing solution. Traversing company firewalls, NATs and web proxies can pose a challenge, particularly if you don't have control over the firewall, or your company policy prevents you from opening the necessary ports for VidyoConferencing signaling and traffic. The VidyoProxy solution was developed to address this challenge, securely and effectively.

The VidyoProxy solution comprises both client and server software components. The server component resides on the VidyoRouter appliance and is included with the purchase of the VidyoRouter. The client component is included with the VidyoDesktop purchase and resides in VidyoDesktop as an optionally configured component.

Vidyo Solutions for Firewalled Networks

Note: The actual steps to configure the Firewall/NAT and DNS environments are outside the scope of this chapter, and will vary based on the Firewall/NAT and DNS servers to be used. This chapter focuses on the configuration of the VidyoProxy solution only.

Note: This chapter assumes that HTTPS/SSL are not configured for the VidyoPortal or VidyoRouter.

VidyoPortal
portal.company.com
192.168.1.100

VidyoRouter
vr2.company.com
192.168.1.101

VidyoDesktop and Room negotiate dynamic UDP ports with VidyoRouter if the firewall is configured as "wide open."

The firewall must open 6 UDP ports per participant for the audio, video and data sharing.

VidyoDesktop

VidyoDesktop

VidyoRoom

VidyoConferencing Through Firewall Without VidyoProxy

VidyoPortal
portal.company.com
192.168.1.100

VidyoRouter
with Proxy
vr2.company.com
192.168.1.101

Vidyo's Proxy tunnels all packets though a TCP connection on port 443 only.

VidyoDesktop

VidyoDesktop

VidyoRoom

VidyoConferencing Through Firewall With Vidyo Proxy

KEY FEATURES AND FUNCTIONS OF VIDYO'S PROXY SOLUTION:

For implementations where the necessary range of UDP ports are opened on the company network, the VidyoDesktop client uses industry standard ICE/STUN to negotiate UDP ports directly with the VidyoRouter. These same protocols are employed for NAT traversal in version 1.x, or the VidyoDesktop uses the Media Mapping and DNS configured in the Portal and VidyoRouter (in versions 2.0 and higher).
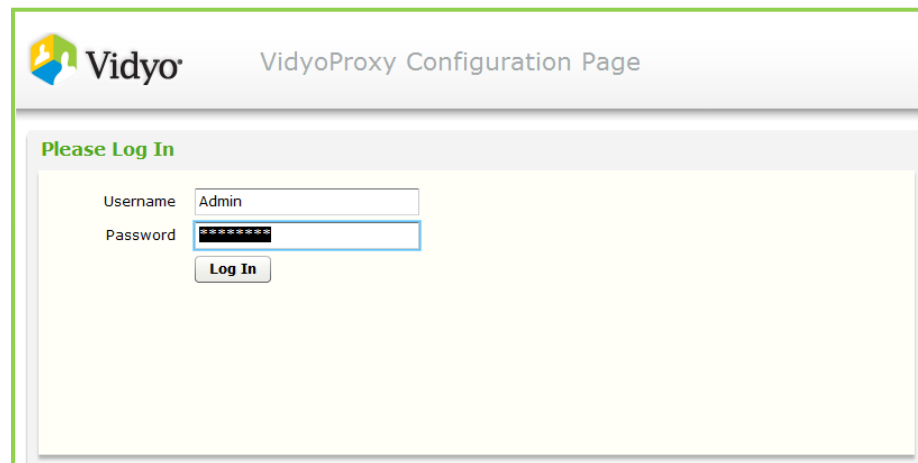
For implementations where the UDP ports are closed on the company network, the VidyoProxy solution overcomes these blocking issues in a secure fashion by tunneling on port 443 using industry standard TCP SSL (Secure Sockets Layer). The VidyoDesktop is able to auto-detect if firewall blocking is taking place and automatically fallback to Vidyo's proxy configuration as needed. Likewise, the user can force using the VidyoProxy from the Desktop client. If the firewall configuration is known, auto-detection can be easily over-ridden. Vidyo's proxy client software is included with the VidyoDesktop application and the proxy server software is included with the VidyoRouter application. The same proxy client and server software modules are also able to traverse Web Proxies. With version 2.0.3 and higher, the Proxy is supported from the Vidyo-Room series of endpoints.

While no additional hardware is necessary to implement the proxy solution, the proxy server software may be run independently on a separate VidyoRouter appliance to optimize performance for cases where the appliance running the VidyoRouter application is not in close proximity to the internal company network, or in cases where there is a large amount of Vidyo calls using the proxy.

HOW TO CONFIGURE YOUR VIDYOPROXY

The embedded (local) VidyoProxy is pre-configured at the factory. Edit the embedded VidyoProxy configuration only if guided to do so by Vidyo Customer Support for more advanced configurations.

Stand-alone (additional) VidyoProxys, however, do need some configuring. In order to do so, you first have to leave the Components tab (or you can leave it open and open another tab in your browser) to do one quick configuration setting on the VidyoProxy Configuration Page.

To log into your embedded or standalone VidyoProxy, launch your browser (or open a new tab) and enter its address:

```
http://<URL or IP>/vp2conf/
```

Log in using the default Administrator account:

- User Name: admin

- Password: password (case sensitive)

Note: Although the default username for this page is "admin," in the normal course of business only the Super Admin accesses these pages.

Note: An alternative route to this page is to click on the IP address of the VidyoProxy in the Components page.

Configuring your VidyoProxy is very similar to configuring your VidyoRouter. Once you log into your VidyoProxy you again see the Basic tab open.

Note: For technical reasons there are no Help buttons on these configuration pages, to it's a good idea to have this manual open on your screen or have a print-out of it handy when you perform the tasks described here.

VidyoProxy Basic Tab

- The Config Server field tells the VidyoProxy (and other components) where to look for their configuration information. For the local embedded proxy "localhost" is the config server. For a standalone proxy it's the IP address or URL of your portal. Click the Apply button for the Proxy to register.

VidyoProxy Configuration in the Portal

1.   After the server finishes rebooting log in to the Super Admin portal:

   `http://<URL or IP>/super`

2.   Click on the Components tab
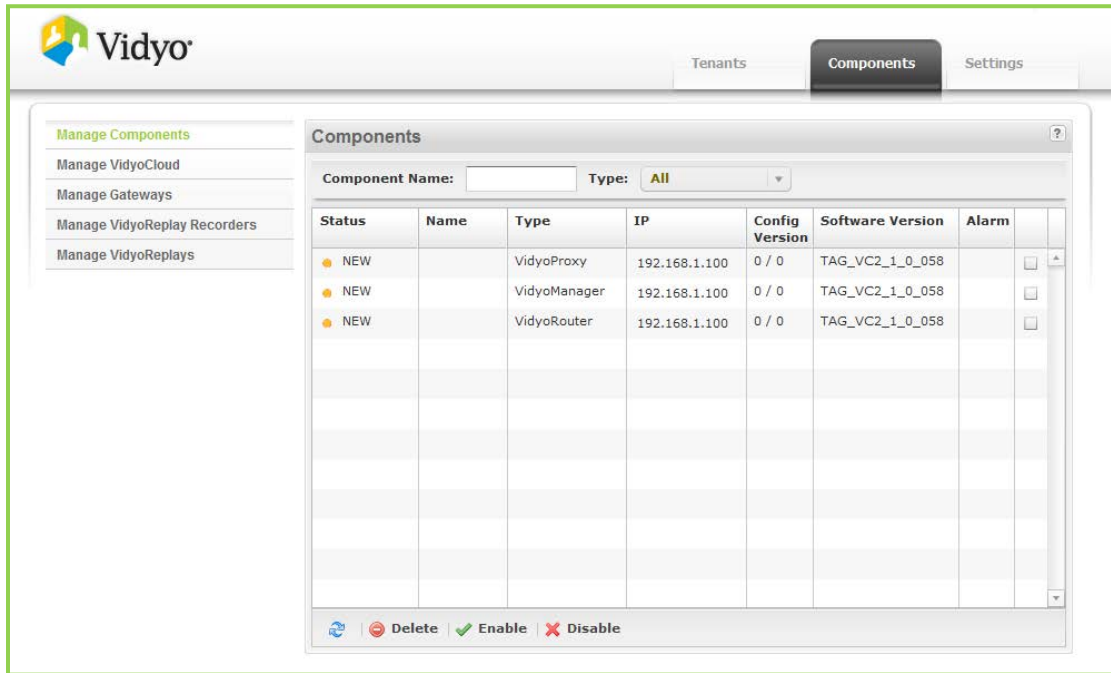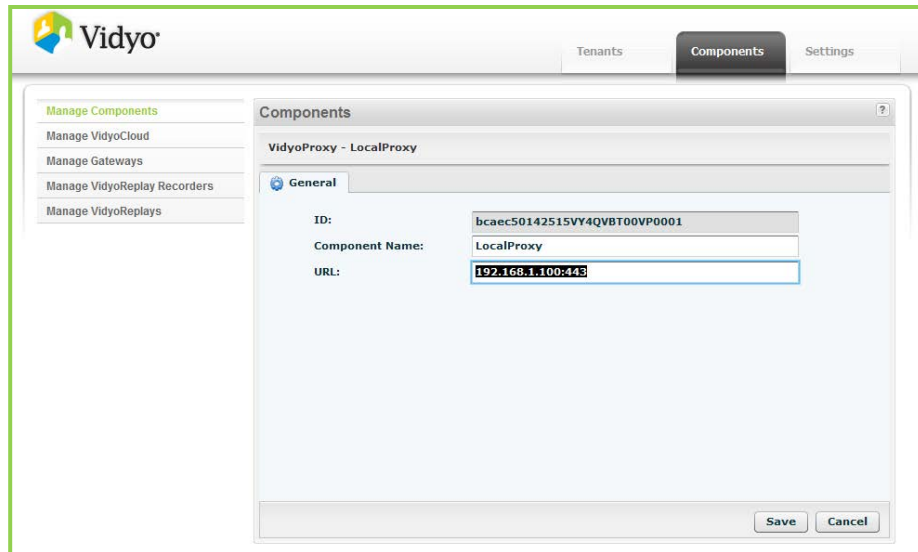
3.   Double-Click the LocalProxy to edit the predefined LocalVidyoProxy entry
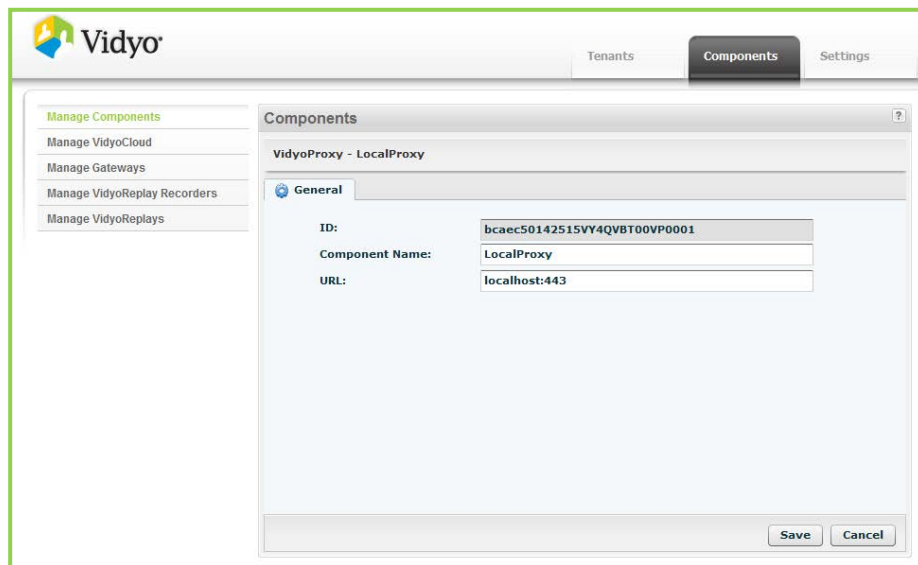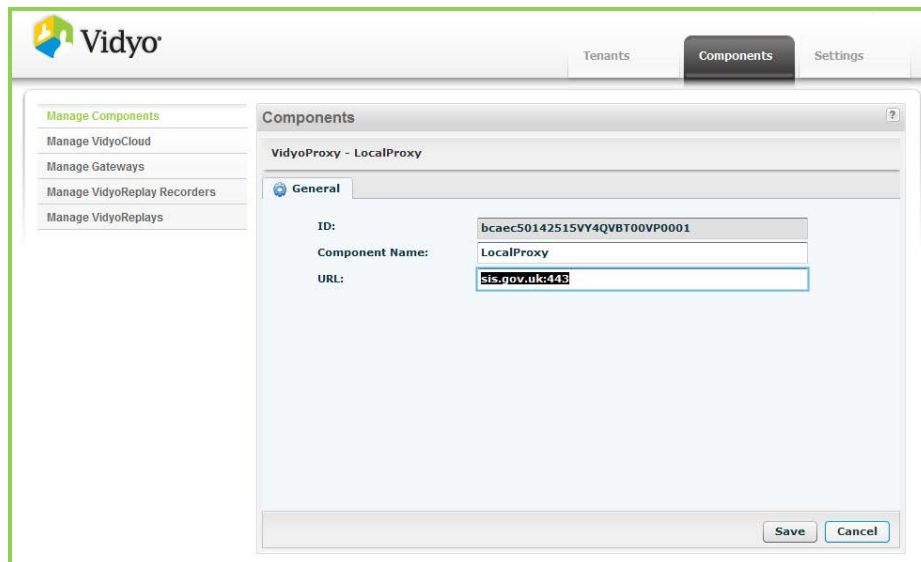
4.   Change the proxy URL to the URL or IP address of the server on which the VidyoProxy is installed.

5.   Leave the ":443" to indicate the TCP port to be used for the Proxy connections.

The IP address is shown above. The URL is shown below.

6. Click the Save button to save your changes.

7. (Go back to Components and make sure it's green with no alarms.)
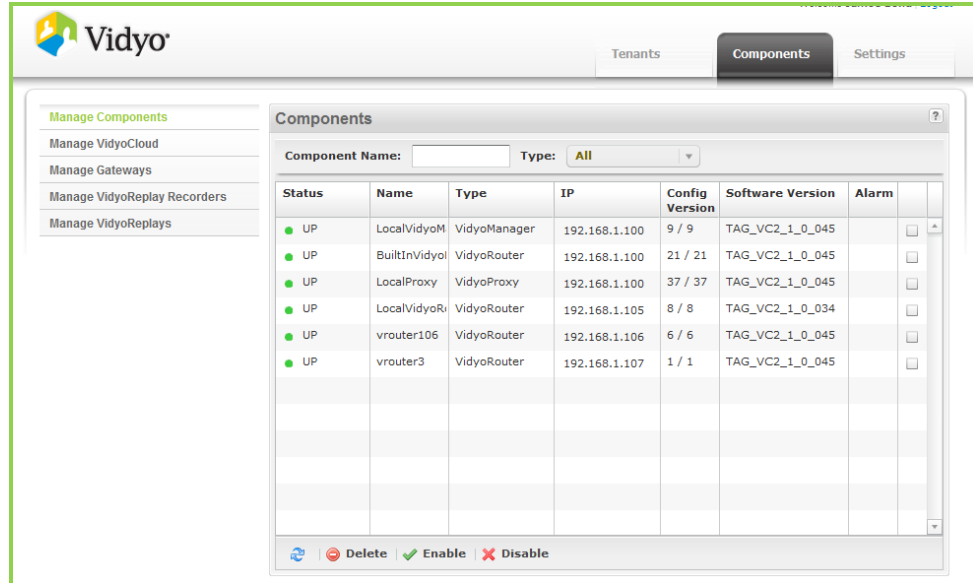
8. Repeat for each VidyoProxy in your VidyoConferencing system.

Assigning a VidyoProxy to Tenants

You need to assign each Tenant to a VidyoProxy in order for the Tenant's users to be able to use the VidyoProxy.
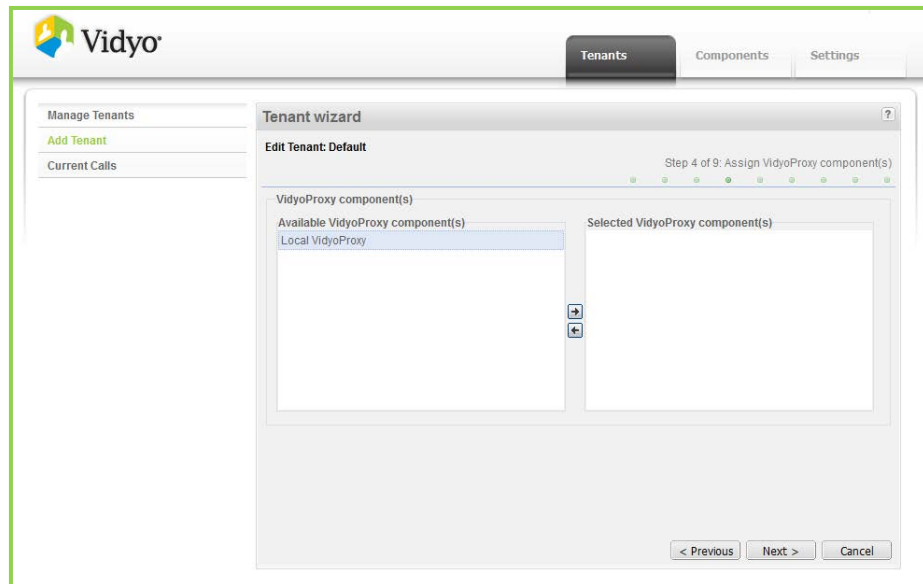
When you're done it looks like this:
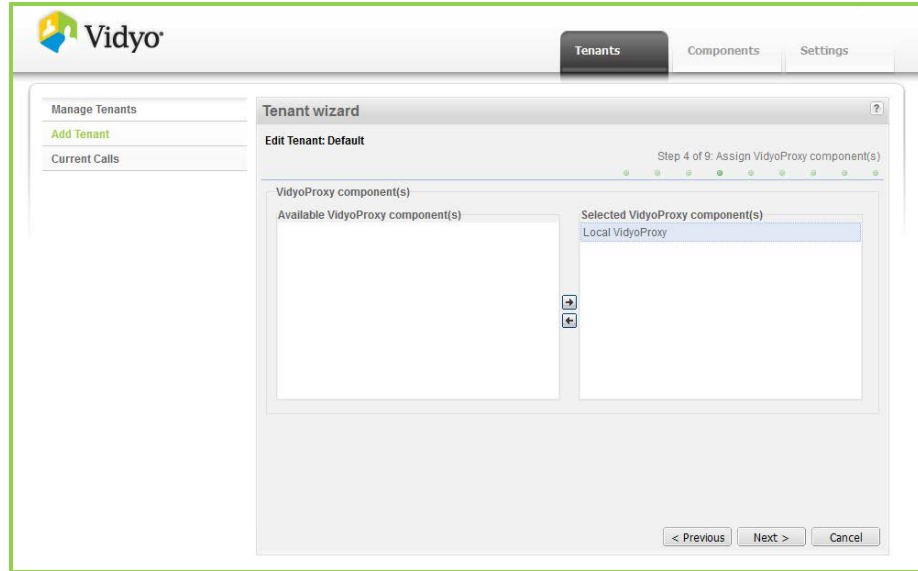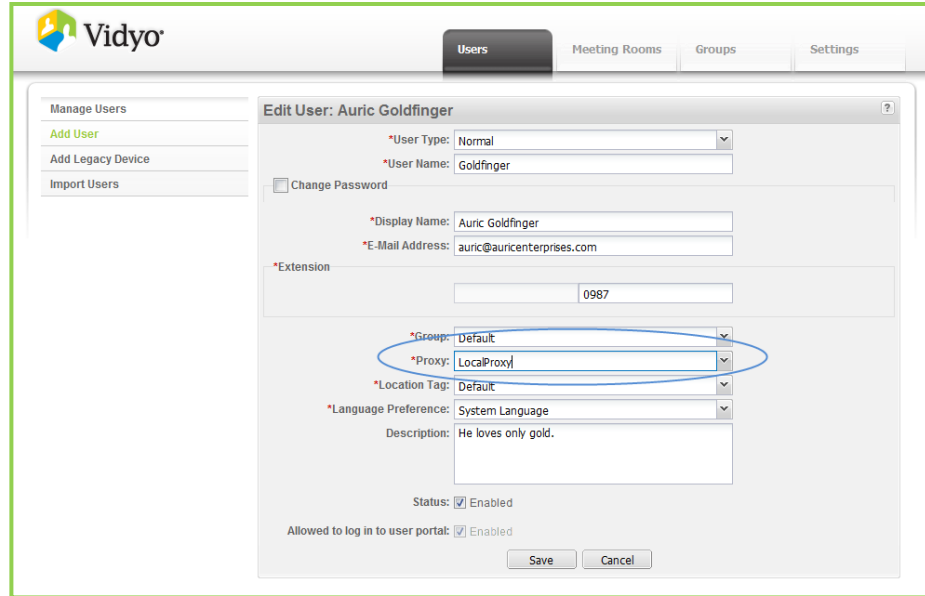
Assigning a VidyoProxy to Portal Users

You need to assign each user to a VidyoProxy in order for them to be able to use the VidyoProxy.

1.   Log in to your Admin portal

     `http://<`URL or IP`>/admin/`

2.   On the Users tab select Manage Users.

3. For each user set their preferred Proxy (to DefaultVidyoProxy or other VidyoProxy Component name created and preferred)

Note: For information on using the VidyoDesktop with VidyoProxy see the Using the VidyoDesktop During a Meeting chapter of the User Guide.

This appendix covers two aspects of implementing VidyoConferencing security:

- HTTPS – describes how to set up secure browsing for the VidyoPortal/VidyoOne.

- Encryption – describes how to set up encrypted endpoint management, signaling and media for end-to-end security for the VidyoConferencing system.

HTTPS is included as a standard option, however requires the purchase and/or acquisition of SSL certificate(s) from a valid CA (Certificate Authority). You may implement HTTPS without enabling Encryption for secure browsing only. HTTPS secure browsing uses a secured connection between the desktop user's browser, as well the VidyoRoom system's browser, and the VidyoPortal home page. It also secures the browser connection to the admin and super admin web pages, as well the VidyoManager, VidyoRouter and VidyoProxy local web pages. HTTPS uses standard SSL certification to provide secured browsing to these web pages, protecting usernames and passwords, as well actions on the pages. It guarantees that confidential information shared during a VidyoConference browsing session stays safe from attempts at phishing and hacking.

Encryption is an additional software option that requires the purchase of the Secured VidyoConferencing Option. Encryption also requires the implementation of HTTPS including the purchase and/or acquisition of SSL certificate(s) from a valid CA (Certificate Authority). Once Encryption is enabled, all calls are secured and encrypted for all users and components. Mixing secured and non-secured calls is not currently supported.

Encrypted end-to-end security uses AES-128 encryption to secure the connection between the VidyoDesktop and VidyoRoom clients and the VidyoManager {licensing and management} and VidyoRouter(s) {signaling and media}; as well connections between the VidyoConferencing components: VidyoPortal, VidyoManager, VidyoRouter(s), and VidyoGateway(s). It guarantees that confidential information shared during a VidyoConference stays safe from attempts at hijacking and eavesdropping.

Note: Enabling Encryption security adds about 30 percent overhead to the VidyoRouter, reducing the maximum number of calls from 100 to 75 for Standalone VidyoRouters; and from 50 to about 37 for the embedded VidyoRouter on VidyoPortals and VidyoOne servers.

Note: To configure security for your VidyoConferencing system you must have super admin access to the VidyoPortal and admin access to the VidyoManager and VidyoRouter.

SECURING THE VIDYOPORTAL/VIDYOONE BROWSING—IMPLEMENTING HTTPS

Implementing HTTPS for your VidyoConferencing system requires you to deploy a signed (verified) SSL certificate. You must register a certificate with a certificate authority such as VeriSign, GoDaddy, etc.

Note: An unsigned (self-issued) certificate does not provide a guarantee of security to your users.

How to Secure the Portal

1. Log into the VidyoPortal/VidyoOne as a Super Admin.

   For information about logging into the VidyoPortal as a Super Admin, see Super Admin Login on page 18.

2. Select the Settings tab and click Maintenance on the left-hand menu, then choose the Security tab:
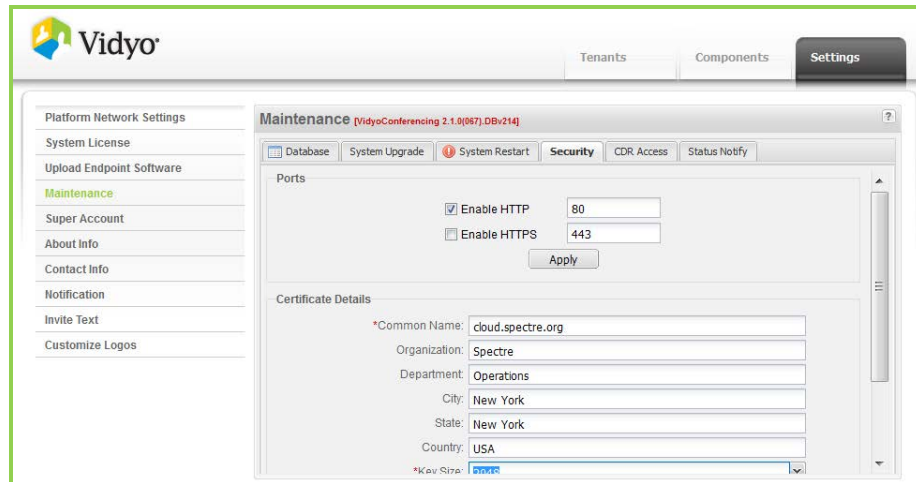
3. Create a Certificate Signing Request (CSR) by filling out the Certificate Details fields:
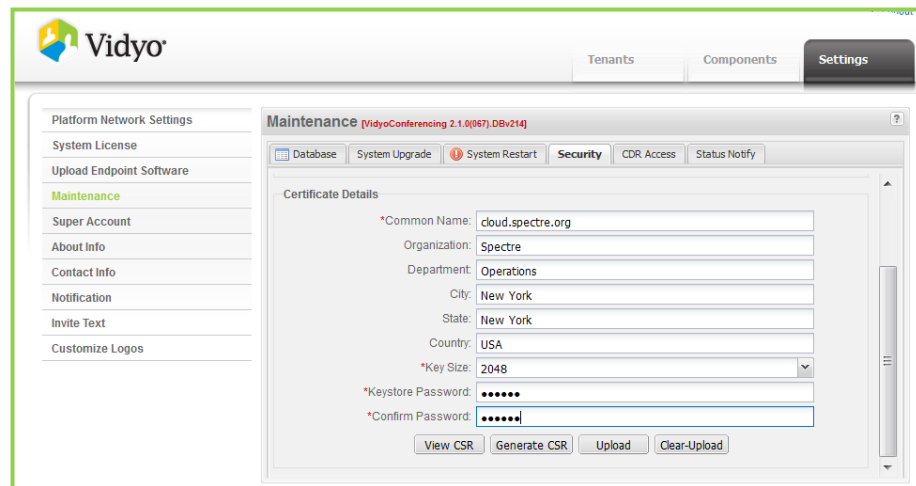
Take note that in the above screenshot we have scrolled down the security window from the previous screenshot.

CSR NOTES:

- You must fill out all of the fields to submit a valid CSR.

- Be sure to enter the Organization name exactly as it is registered for the domain registration.

- Be sure to use the same city, state and country as the domain registration.

- Do not abbreviate cities, towns or states. Countries may be abbreviated depending on the rules of your CA of choice. For example: you may use "USA" or "US". Check with your CA for their requirements on location fields.

- In the Key Size field, specify either 2048 or 1024 bit encryption. Some countries or CAs limit the key size. Observe the limitations in effect in your country. Check with your CA for Key Size requirements.

- The keystore password can be any password you choose and must contain a minimum of 6 characters.
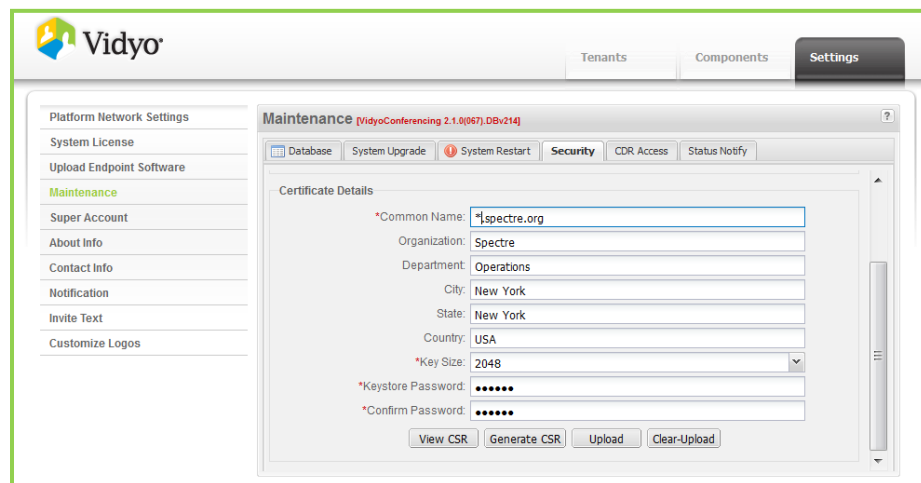
USING A WILDCARD CERTIFICATE IN A MULTI-TENANT SYSTEM

If you are running a multi-tenant system, all Tenant URLs must be in the same domain, and each use a unique sub-domain. You must then also use a wildcard SSL certificate. You must substitute an asterisk (*) wildcard character for the tenant sub-domain name (or sub-sub-domain name) in the Common Name, so the name of each tenant will automatically match the fully qualified domain name (FQDN) for the certificate.

For example: ***.company.com** or ***.portal.company.com**.

It is also recommended that you use sub-sub-domain names so that you can also use a wildcard DNS entry in your domain name server to resolve tenant URL addresses without requiring a separate entry for each tenant, and also avoid having to create a new DNS entry each time a new tenant is added.

The screen below represents a wildcard certificate entry example:

4. When you have entered information in all the Certificate Details fields, click the Generate CSR button.

    NOTE: If you previously generated your CSR and submitted it to your CA, **do not** regenerate another CSR unless you are correcting or changing information as needed and plan to resubmit the new CSR to your CA. Regenerating a CSR will invalidate any previous certificates based on the previous CSR.

    When the CSR is created, a confirmation message opens.

5. Click the View CSR button to view a read-only copy of the CSR request.
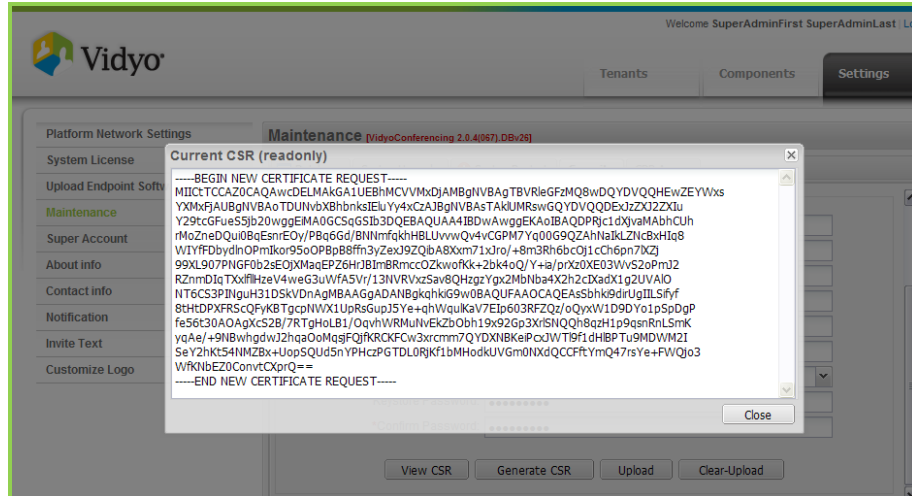
6. Copy all the information in the Current CSR window and provide it to your CA where requested. Be sure to include the header and footer lines:
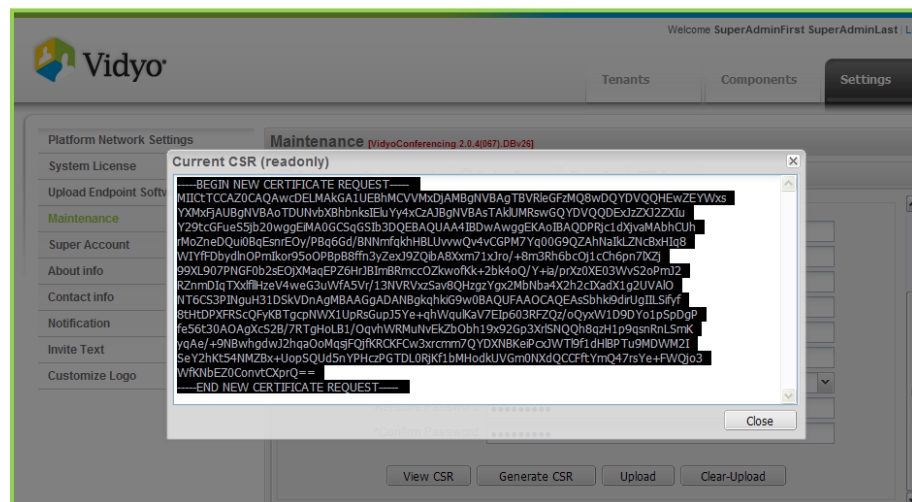
Deploying The Signed SSL Certificate(s)

NOTE: When selecting the certificate type from the CA, be sure to select Tomcat if available; if not, alternatively select Apache2. If neither, the format supported by the portal is base64 X.509 cer or PKCS#7. The portal does not currently support .p7b bundles; the certificates must be separated accordingly.

Perform the steps in this procedure after you receive certificate files back from your certification authority.

The CA returns at least a domain (server) certificate and may return a root and one or more intermediate certificates in separate files. (With some authorities, you may have to copy the certificate data from an email message into separate files.)

Your certificate authority may provide three types of files:

- ▪ Their root certificate file

- ▪ One or more intermediate certificate files (optional)

- ▪ The domain certificate file (may be titled 'server certificate')

152

The certificate authority may send you these files, or require you to download them from their website. Often, the certificates are not clearly identified, requiring you to identify each file type.

If your certificate authority provides certificate files in an email message, you must copy and paste the appropriate text for each certificate type into a separate file and save it with the correct extension, as described in the next section. Be sure to use a text editor that will not append each line with carriage returns.

Vidyo recommends following these guidelines in identifying the certificate files:

- The domain file normally contains your server's common name (or FQDN).

- Intermediate files often contain the character string "inter" somewhere in the file name. Once you identify which ones are the intermediates, you can then identify the root certificate file by process of elimination.

- The remaining file is the CA's root certificate file.

The CA may also only return the domain (server) certificate, and if needed or required, the root and/or intermediate certificates will need to be located and manually downloaded from the CA's website.

If the root and/or intermediate certificates were not provided to you, the Portal includes a default bundle of common CA root and intermediate certificates. If you are using a main-stream CA, the root and intermediate certificates may not be needed. Follow the steps in the next section to attempt uploading, and testing with, only the domain certificate to determine if root and/or intermediate certificates are required.

NOTE: Some CAs have several root and/or intermediate certificates available depending on the type of certificate you have ordered. Be sure to locate the appropriate matching root and/or intermediate certificates for your domain certificate. Contact your CA for assistance if you're not sure.

Uploading The Certificate File(s)

7. In order for the Portal to understand which certificate type each certificate is, you must edit and append the correct extension to each, as follows:

- Root certificate: `.root`

- Intermediate certificate (optional, one or more): `.inter`

- Domain certificate: `.domain`

    The certificate(s) you received will typically end with `.crt` or `.cer` extensions. Rename the extension for each certificate as outlined above:
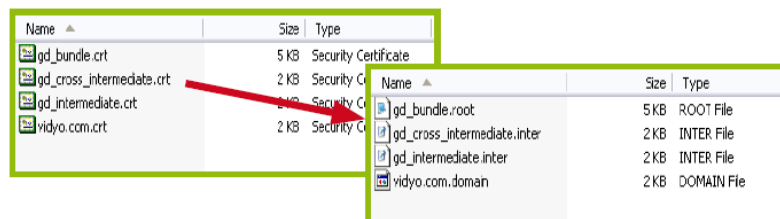
8. As the Portal includes a default bundle of common CA root and intermediate certificates, if you are using a main-stream CA, the root and intermediate certificates may not be needed. So start by first

attempting to upload, and test with, only the domain certificate to determine if root and/or inter-mediate certificates are even required.

9. Return to the Super Admin › Settings› Maintenance › Security tab window.

10. Click the Upload button

11. In the Uploading Certificate dialog box, click the Select File button to locate the **domain** certificate file on your computer or local network.
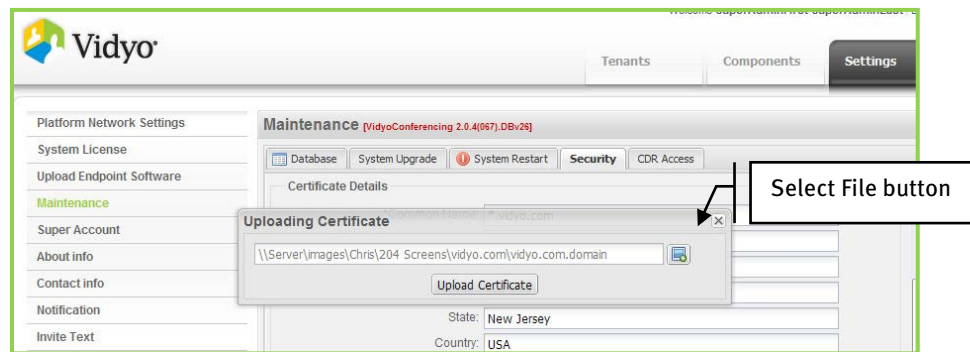
12. Click the Upload Certificate button to upload the domain certificate file.

    If the upload is successful the File Upload Success dialog box will open:
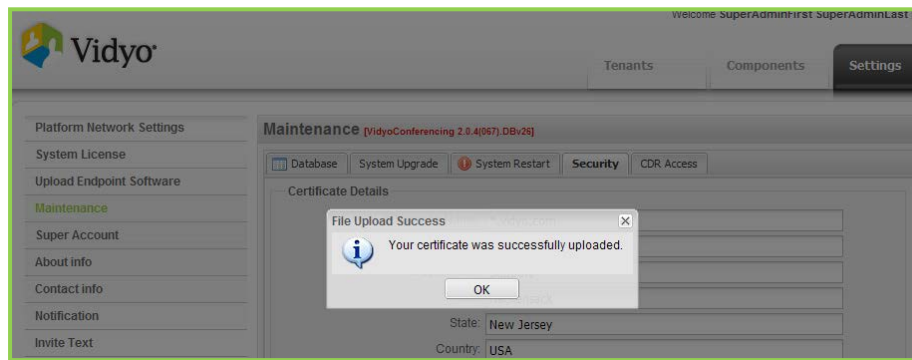
    If the domain certificate upload fails, go to step 15 on page **155**.

13. Select the Enable HTTPS checkbox and set the HTTPS port.
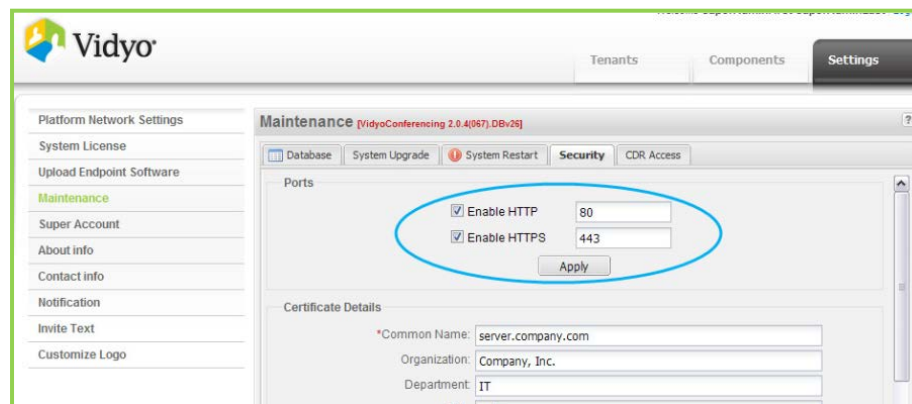
The HTTPS port should typically remain 443 (the default). Setting the HTTPS port to anything other than 443 will result in users having to manually add the port to their URL requests in their browsers.

NOTE: be sure the VidyoProxy loaded on the server is either disabled or running on a port other than 443 (or whatever port HTTPS is set to use).

Note: DO NOT disable HTTP until you are sure HTTPS is working properly.

14. Click the Apply button and confirm to restart the server.
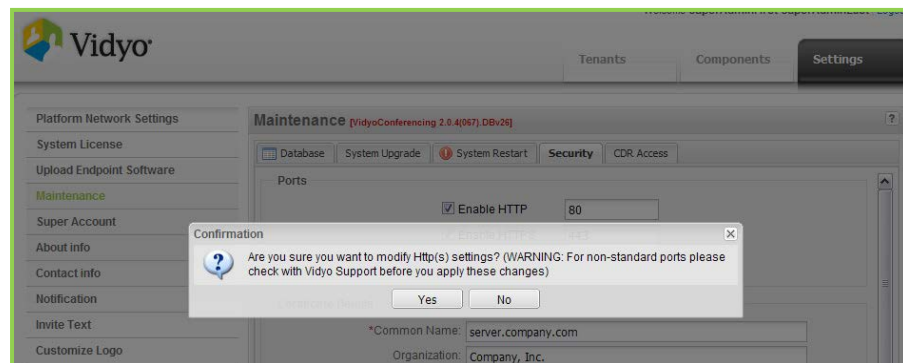
15. Browse to the Portal user login page to confirm that HTTPS is working properly and the browser does not post any security errors. Be sure to include the HTTPS header in the URL (e.g., `https://<portal IP or URL>`).

    Note: If your browser generates a root certificate error, first check that your PC/Mac has the latest root certificates update applied for your OS.

16. If you are successful browsing to the portal using HTTPS (you do not receive any browser errors), go to step 26 on page .

17. If you receive an error when browsing to the portal using HTTPS and you have the latest root certificate update applied to your computer, return to the super admin pages (Settings > Maintenance > Security) and deselect the HTTPS checkbox to disable HTTPS, click Apply and confirm to reboot the server.

18. Upon server reboot, return to the Super Admin pages (Settings > Maintenance > Security)

19. Click the Clear Upload button to reset the key chain.

20. Upload the full set of certificate files.

    Note: Be careful and **DO NOT** click the Generate CSR button.

21. Click the Upload button.

22. In the Uploading Certificate dialog box, click the Select File button to locate each certificate file on your computer or local network.
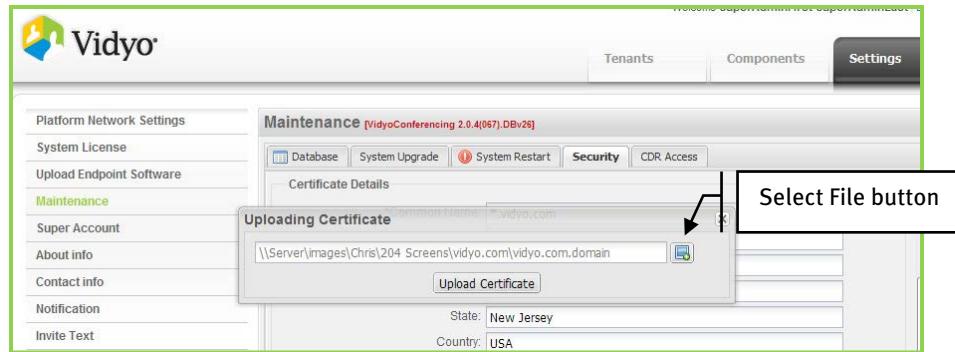
23. Upload the certificate files in the following order:

- Root

- Intermediate(s)

- Domain

24. Click the Upload Certificate button to upload each file.

Note: If you upload the certificate files in the wrong sequence, the certification process may not succeed. Click the Clear Upload button to reset the key chain, and then re-upload the files in the right order.

25. Return to step 10 and repeat steps 13 thru 16.

26. Log back into the super admin pages (Settings › Maintenance › Security) and *de*select the Enable HTTP checkbox to disable HTTP.

27. Click the Apply button and confirm to restart the server.

Note: Disabling HTTP will redirect all HTTP requests to HTTPS.

28. Verify the HTTP to HTTPS redirect is working and HTTPS access is still functional by browsing to the portal using the standard http header in your browser (e.g., ‹`http://<Portal IP or URL>`›). Your browser should be redirected to https, and you should not receive any browser security errors.

Steps continue on the next page after the following points.

Verifying An SSL Certificate

To confirm that you have successfully deployed a signed SSL certificate on the VidyoPortal, log into your VidyoPortal and verify that `HTTPS` appears on the left side of the address bar and that a lock icon appears (typically in the lower right corner). Some browsers emphasize an HTTPS session with a color like green or blue.

You can also verify your signed certificate by displaying information for it in your web browser. See the documentation that came with your web browser for information.

HTTPS Trouble—Recovering From HTTPS Failure

If HTTP is disabled, and you can no longer browse to the Vidyo server using HTTPS, you can disable HTTPS and re-enable HTTP browsing via the Shell Admin menu and invoking `Option 16`. Refer to the Shell Admin

Menu Appendix starting on page **125** of this Guide for information on accessing and using the Shell Admin Menu.

Setting The System Components To Work With HTTPS
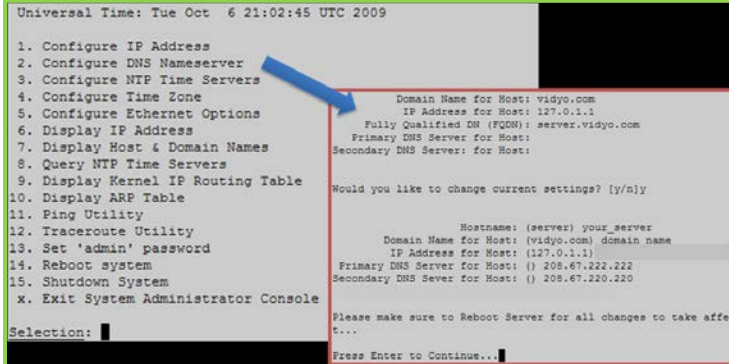
After implementing HTTPS, in order for the system to function you need to set up each component to listen on and address each other using a valid FQDN (URL or Common Name) as defined in the certificate applied.

Now you can set the server FQDN address:

You must configure the VidyoPortal and Routers to be aware of their DNS hostname(s). This is done in the system console menu, Option 2.

For more information on the system console menu, refer to the Shell Admin Menu Appendix starting on page **125**.

29. Set the server local hostname and domain name as well as working DNS server addresses:

NOTE: It's very important to note that the IP address listed in this screen (127.0.1.1) must remain intact for proper communications.

Now you can set each component to address the configuration server via FQDN:

30. Log into the VidyoManager local configuration pages `<URL>/vm2conf/` or click on the IP address of the VidyoManager in the Portal Components page.

The default administrator account for the VidyoManager local pages is:

- User Name: `admin`
- Password: `password` (case sensitive)

Note: Although the default username for this page is "admin," in the normal course of business only the Super Admin accesses these pages.

31. Under the Basic tab, set the Config Server to a valid FQDN of the portal as defined by the applied certificate:
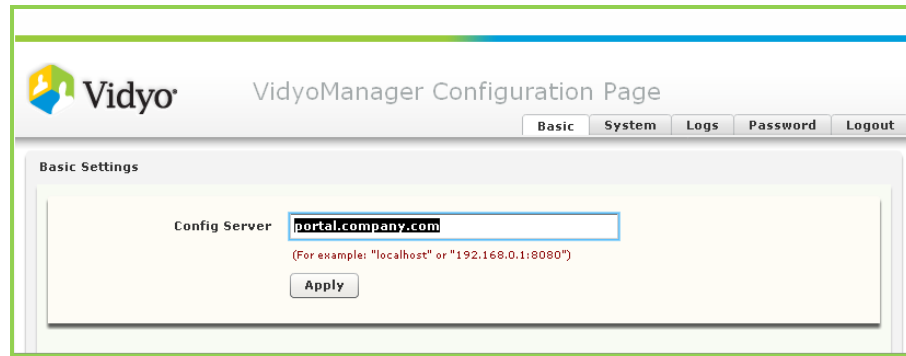
32. Click the Apply button, and OK to restart the VidyoManager.

Now you can configure the VidyoRouter.

33. Log into the VidyoRouter local configuration pages `<URL>/vr2conf/` or click on the IP address of the VidyoRouter in the Portal Components page.

The default administrator account for the VidyoRouter local pages is:

- ▪ User Name: `admin`

- ▪ Password: `password` (case sensitive)

34. Under the Basic tab, set the Config Server to a valid FQDN of the portal as defined by the applied certificate:
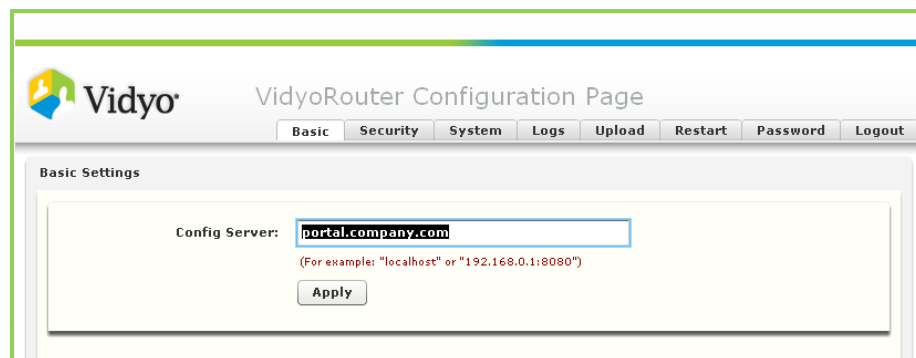
Now you can configure the VidyoProxy.

35. Log into the VidyoProxy local configuration pages `<URL>/vp2conf/`or click on the IP address of the VidyoProxy in the Portal Components page.

The default administrator account for the VidyoProxy local pages is:

- ▪ User Name: `admin`

- ▪ Password: `password` (case sensitive)

Note: Although the default username for this page is "admin," in the normal course of business only the Super Admin accesses these pages.

36. Under the Basic tab, set the Config Server to a valid FQDN of the portal as defined by the applied certificate:
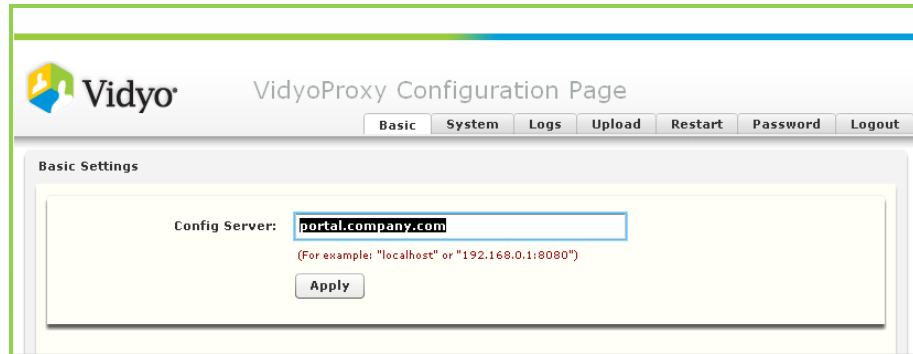
37. Click the Apply button, and OK to restart the VidyoProxy.

Configuring Tenant(s) to use FQDNs

38. Login to the portal Super Admin pages, and go to Tenants tab › Manage Tenants
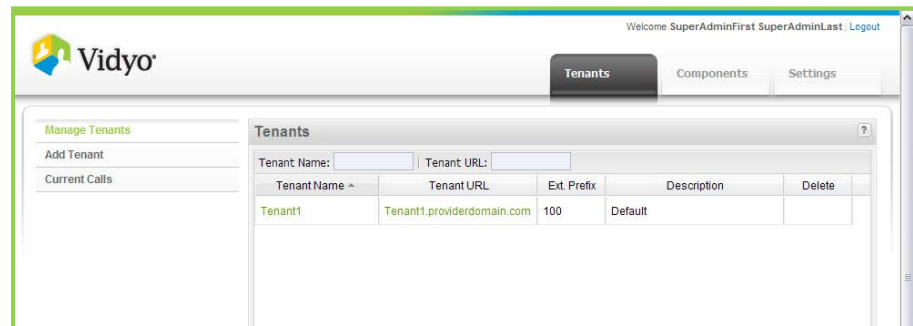
39. Ensure that each Tenant (including the Default Tenant), is using a valid FQDN for Tenant URL as defined by the certificate applied.

Refer to Managing Tenants starting on page **73** for more information on setting Tenant URLs.

Configuring Each Component to Use FQDNs

40. From the Super Admin pages, go to the Components tab:
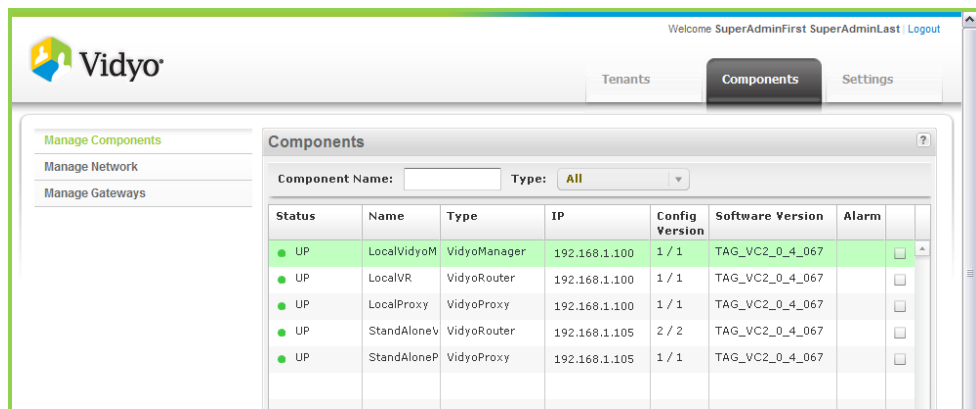
41. Double-click the Status on the VidyoManager row.

42. Under Listen Address (EMCP), edit the EMCP address (VidyoManager address) by clicking the text in the IP column, and enter a valid FQDN as defined in the certificate applied:
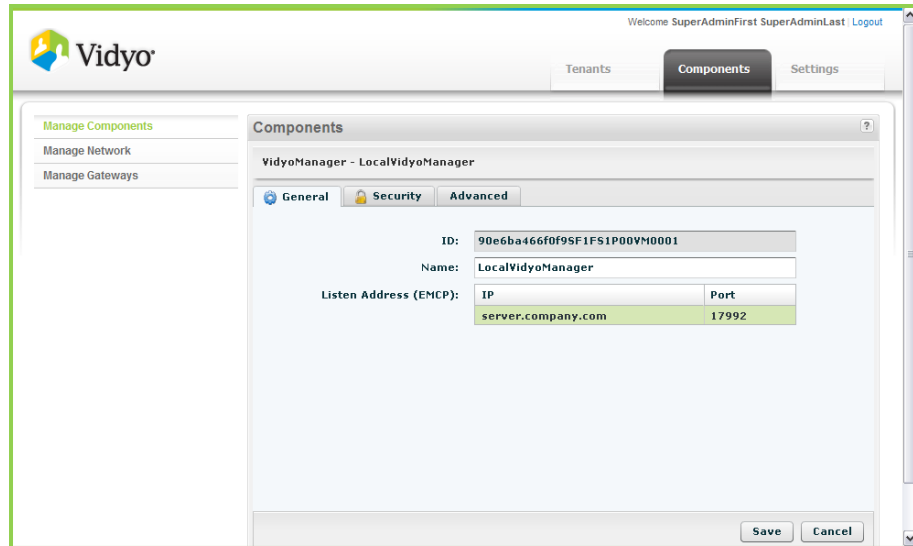
43. Click the Save button, and OK to confirm.

44. After returning to the Manage Components page, Double-Click the Status on the local (embedded) VidyoRouter entry.

45. On the General tab, Under Listen Address (SCIP), edit the SCIP address (VidyoRouter signaling address) by clicking the text in the IP field, and enter a valid FQDN as defined by the certificate applied:
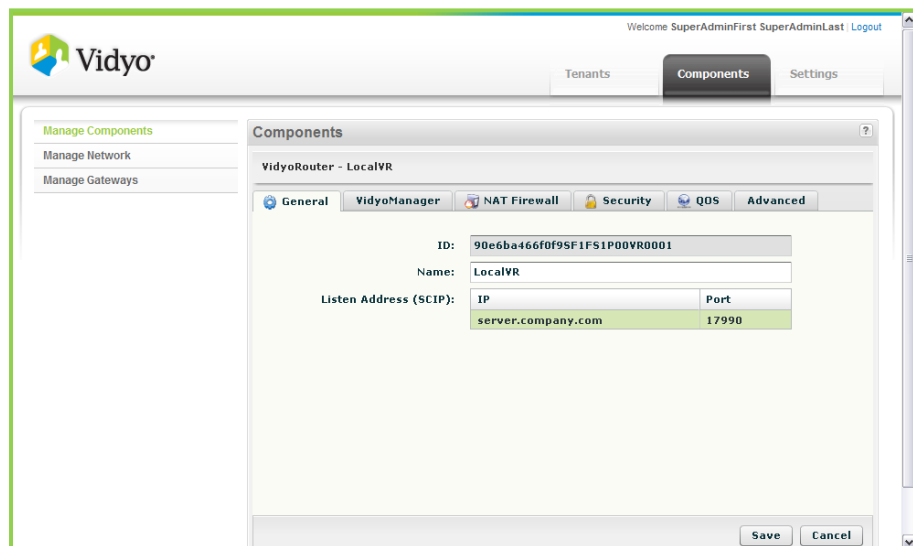
46. Click on the VidyoManager tab.

47. In the Vidyo Manager tab, edit the IP address by clicking the text in the IP column, and entering a valid FQDN as defined by the certificate applied:
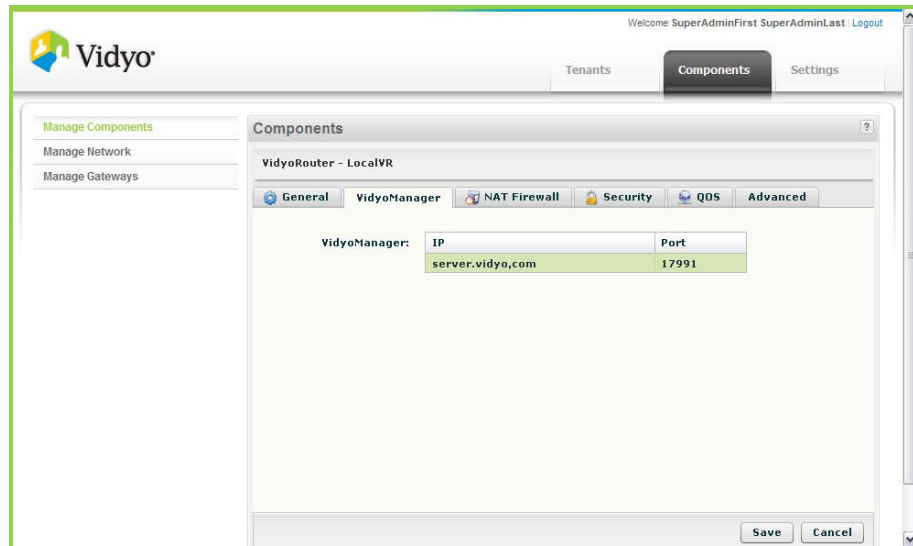
48. Click the Save button, and OK to confirm.

49. After returning to the Manage Components page, double-click the Status on the local (embedded) VidyoProxy entry.

50. In the URL field enter the Proxy server's valid FQDN as defined in the certificate applied, followed by a colon and the Proxy port (typically 443):
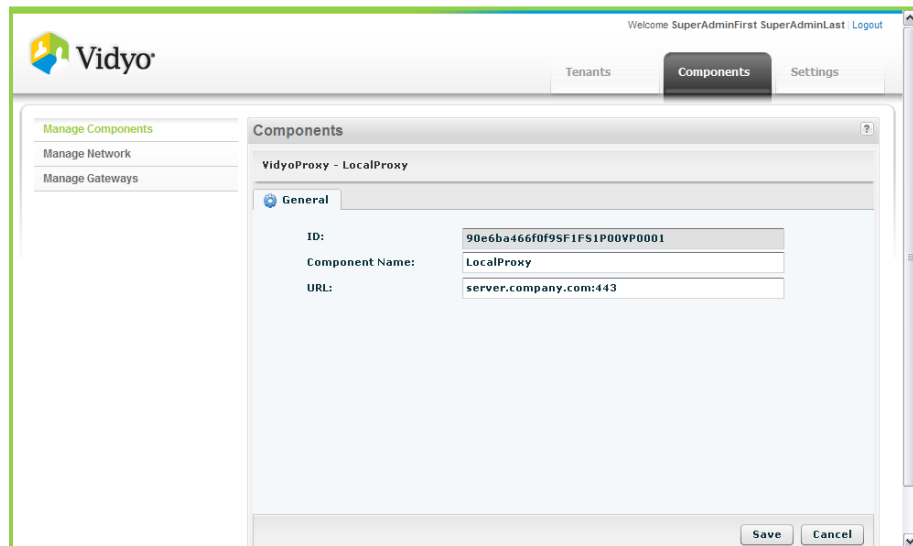
Refer to the VidyoProxy Appendix for more information on configuring VidyoProxy.

51. Click Save and OK to confirm.

52. Verify that all components are Online (Status UP) and have no Alarms:
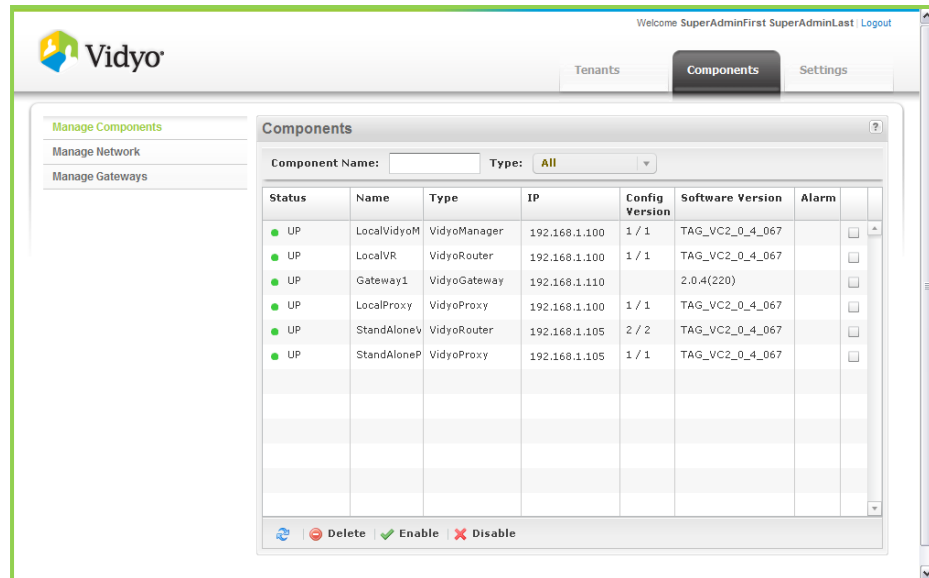
53. Login to a User Portal and place test calls to verify the Portal and components are functional.

> **Note:** If your system includes Standalone VidyoRouters, refer to the last section of this appendix for information on setting up and configuring HTTPS on Standalone Routers. For using HTTPS with VidyoGateways, refer to the subsections below.

Applying Portal SSL Certificate To Vidyoroom And VidyoGateway

You may need to apply the Portal's SSL root or full chain certificate to any VidyoRoom system(s) and/or VidyoGateway(s) connected to the VidyoPortal.

Both the VidyoRoom system(s) and VidyoGateway(s) include a default bundle of common CA root and intermediate certificates. If you're using a main-stream CA, the root and intermediate certificates may not be required to be uploaded to either the VidyoRoom system(s) or VidyoGateway(s) you may have. Test each first to see if they connect successfully to the HTTPS only enabled Portal using the default bundled certificates.

If they do not connect, follow the steps in the VidyoRoom User's Guide or VidyoGateway Administration Guide respectively for instructions on how to upload the portal's root or full chain certificate to the Vidyo-Room and/or VidyoGateway.

Note: For VidyoGateways to connect using HTTPS, the Gateway must also be set to connect to the portal via HTTPS, refer to the VidyoGateway Administration Guide for details.

Building The Portal Full Chain SSL Certificate

If your portal SSL chain includes intermediates, you may need to create and upload the full chain certificate to the VidyoRoom(s) and/or VidyoGateway(s).

An easy method to create the portal full chain certificate is to use the certificate Export feature built into the Firefox browser. To use the Firefox browser certificate Export, do the following:

1. Browse to the portal using the Firefox browser using an HTTPS request:

```
https://<portal URL>
```

2. Once the page loads, go to the Tools menu in Firefox and select Page Info, and then click on the Security icon (padlock) at the top of the window; or simply click on the padlock security icon in the lower right corner of the Firefox window.

3. Press the View Certificate button.

4. Select the Details tab, and press the Export button.

5. Browse to the location you wish to save the exported certificate.

6. From the Save as Type drop down, select 'X.509 Certificate with chain (PEM)'.

7. Enter a name for the file in the File Name field and click Save.

8. Rename the file saved with a `.crt` as the extension and upload to the VidyoRoom(s) and/or VidyoGateway(s) accordingly.

SECURING THE VIDYODESKTOP/VIDYOROOM—IMPLEMENTING ENCRYPTION

You must first secure the Portal browsing by implementing HTTP and SSL certification. If you have not previously enabled HTTPS, return to the first section in this appendix for steps on securing the portal and implementing HTTPS.

You must secure the connection between the VidyoDesktop/VidyoRoom and the VidyoManager and VidyoRouter(s) as described in this section to have a fully encrypted and secured VidyoConferencing system.

Note: Video, audio and application traffic to the VidyoManager is encrypted with TLS (Transport Layer Security). To the VidyoRouter, it is encrypted with SRTP (Secure Real-time Transport Protocol).

Verifying Vidyoportal Is Licensed For Encryption

Encryption is an optional feature that you can license for your initial installation or add on at some later time. It requires that the VidyoPortal license includes this option in order to implement encryption.

1. Log into the VidyoPortal/VidyoOne as a Super Admin.

   For information about logging into the VidyoPortal as a Super Admin, see Super Admin Login on page **18**.

2. Select the Settings tab and go to System License along the left column, scroll down to the Encryption line in the System License information section:

If Encryption is enabled in the portal License the setting will read **128 Bits**, otherwise it will show Disabled.

Enabling Encryption On The Vidyoconferencing System

You must first implement HTTPS on the VidyoPortal/VidyoOne prior to enabling Encryption on the system following the steps in the previous section of this appendix. The system components rely on the SSL certificates applied to authenticate each other for the encryption security. If you have not implemented and enabled HTTPS on the portal, please do so before proceeding to the follow steps.

To enable Encryption for full signaling and media security:

3. From the Super Admin pages, go to the Components tab.

4. Double-Click the Status on the VidyoManager entry.

5. Go to the Security tab and Check the Encryption Enabled check-box:
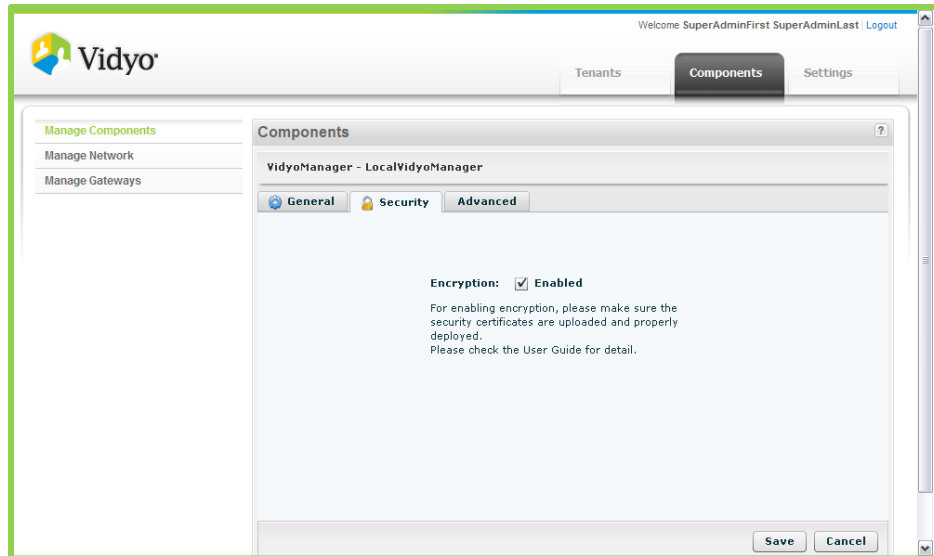
6. Press Save and OK to confirm.

7. After returning to the Manage Components page, Double-Click the Status on the local (embedded) VidyoRouter entry.

8. Go to the Security tab and Check the Encryption Enabled check-box:
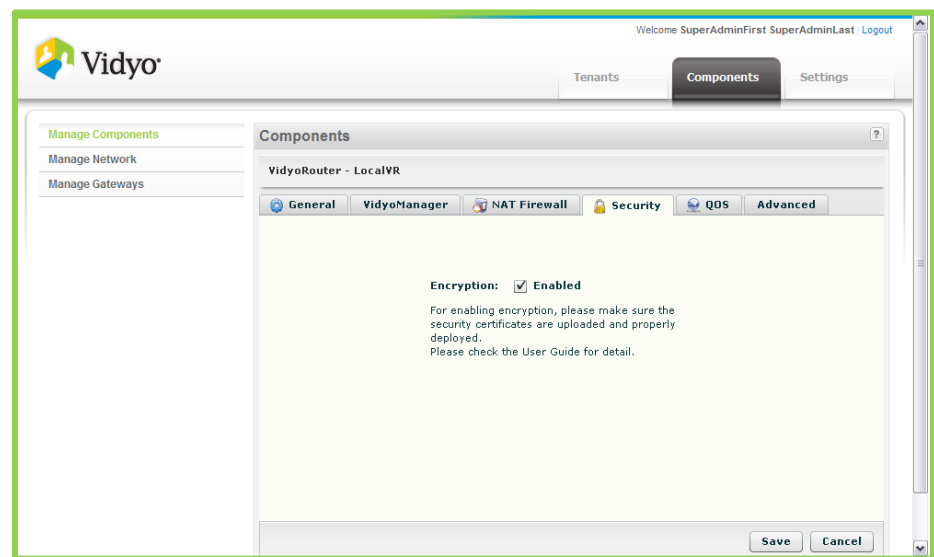
9. Press Save and OK to confirm.

10. Verify that all components are Online (Status UP) and have no Alarms.

    It may take a few moments for the components to return Online and/or clear Alarms):
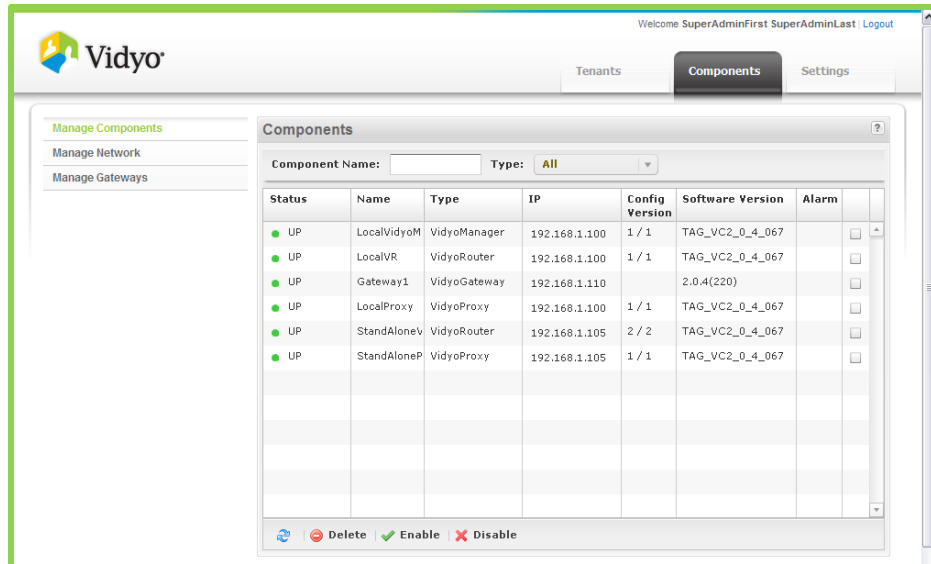
Note: If your system includes StandAlone VidyoRouters, refer to the last section of this appendix for information on setting up and configuring HTTPS and Encryption on StandAlone Routers.

For using Encryption with VidyoGateways, the Gateways must also be set to connect to the portal via Encryption, refer to the VidyoGateway Administration Guide for details.

Testing the VidyoDesktop and verifying encryption

When you have finished configuring encryption, you may confirm that you have a secure connection by performing the following steps:

1. Log into the VidyoPortal and join your own room or otherwise initiate a conference.

2. In the VidyoDesktop client, click the Configuration icon and select the Status tab. If you have a secure connection, you see Using Secure Connection in the Status page:
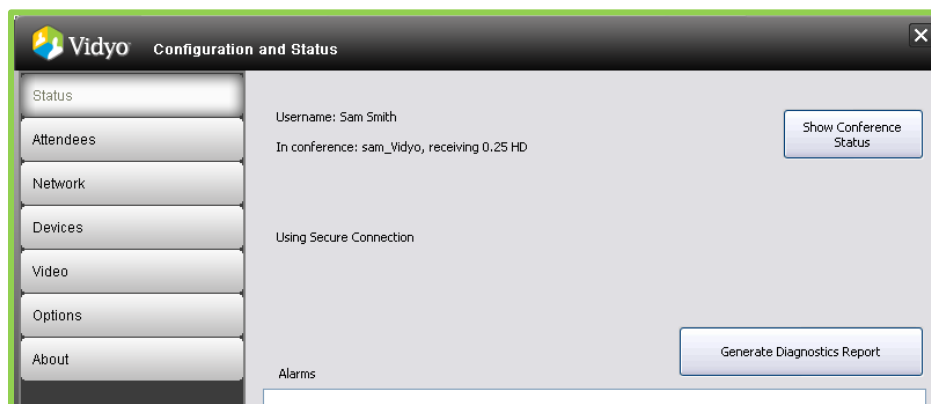
CONFIGURING A STANDALONE VIDYOROUTER/VIDYOPROXY FOR SECURITY

Note: For the local (embedded) VidyoRouter, you can skip this procedure because you have already created an SSL certificate as described in the first section of this appendix (the embedded VidyoRouter shares and uses the certificates applied to the portal).

If you are configuring a separate, standalone VidyoRouter for security then follow the information as follows.

Standalone Vidyorouters In A Https Only (Non-Encrypted) System

For using a standalone VidyoRouter and Proxy in a HTTPS ONLY system, WITHOUT ENCRYPTION, enabling HTTPS and applying SSL certificates on the standalone router is optional. The standalone router includes a bundle of common CA root and intermediate certificates so that it should work with your HTTPS enabled Portal without needing to setup, purchase, and apply separate SSL certificates to the standalone server.

Simply configure any standalone VidyoRouter and VidyoProxy components to use FQDNs to communicate with the other components as outlined in the setting the system components to work with https section of this appendix.

Configuring SSl Security On Standalone Vidyorouters

If you are using Encryption on your VidyoConferencing system, you must apply an SSL certificate to the standalone VidyoRouter as described in this section.

If Encryption is not enabled on your system, then SSL certification is not required for standalone VidyoRouters (see above).

Note: if you do apply SSL certificates for encryption, or other needs, on a standalone server and also plan to use the included VidyoProxy, take care not to enable HTTPS until the possible port conflict with the VidyoProxy's default port is addressed. The default Proxy port is 443. You must either configure the Proxy to use another port (Ex: 8443), or for HTTPS browsing to use a port other than 443.

Further Note: it is recommend not to enable HTTPS only on a standalone router as the web pages are for admins only and not for normal user access. Therefor it is easier to simply leave only HTTP access enabled and block the HTTP port (port 80) from outside, non-admin, access. Thus avoiding the issues of moving either the Proxy or HTTPS port to an alternate. Moving the Proxy port to an alternate port is found to defeat the Proxy's purpose, as the client user site that needs to use VidyoProxy will most likely not allow access to the alternate port. If you require that HTTPS must be enabled, it is then recommend to use an alternate port for HTTPS (e.g., 8443) and leave the Proxy set to use port 443.

For Encryption purposes, you may apply SSL certification without enabling HTTPS. HTTPS browsing is not required for signaling and media encryption on a standalone router.

To configure SSL on a StandAlone VidyoRouter:

1. Add the VidyoRouter to the VidyoConferencing system as described in the Configuring Components chapter in the VidyoConferencing Admin Guide.

2. Log into the VidyoRouter local configuration pages {URL}/vr2conf/or click on the IP address of the VidyoRouter in the Portal Components page.

   The default administrator account for the VidyoRouter local pages is:

   User Name: `admin`

   Password: `password` (case sensitive)

3. Under the Security tab, follow the same guidelines and steps as for the portal as outlined in the Securing the VidyoPortal/VidyoOne browsing - Implementing HTTPS section of this appendix.

Additional CSR NOTES for standalone VidyoRouters:

- You'll need a separate single-server certificate for each standalone VidyoRouter.

- Using a portal's single-server or wild-card certificate on a standalone router is not supported.

- Each standalone router will require its own unique FQDN (Common Name) (e.g., vr1.company.com, vr2.company.com, etc.).

- We recommend you use the same CA and root certificate type for each standalone router as used for the portal so as not to create root certificate validation issues between each server.

Configuring Encryption On Standalone Vidyorouters

You must first implement HTTPS and Encryption on the VidyoPortal, and apply SSL certification to the standalone VidyoRouter prior to enabling Encryption on a standalone router following the steps in the previous sections of this appendix. The system components rely on the SSL certificates applied to authenticate each other for the encryption security.

To configure Encryption on a StandAlone VidyoRouter:

4. Log into the VidyoRouter local configuration pages {URL}/vr2conf/or click on the IP address of the VidyoRouter in the Portal Components page.

5. Under the Basic tab, set the Config Server to a valid FQDN of the portal as defined by the portal's applied certificate:
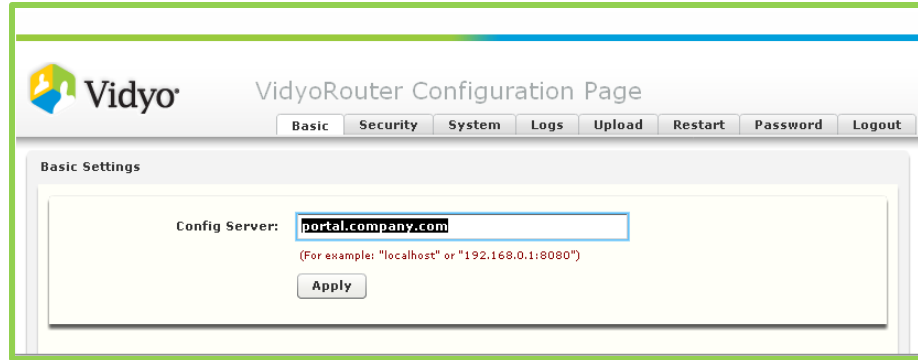
6. Click the Apply button, and OK to restart the VidyoRouter.

7. Log in to the Portal Super Admin, and go to the Components tab / Manage Components page, Double-Click the Status on the standalone VidyoRouter entry.

8. On the General tab, Under Listen Address (SCIP), edit the SCIP address (VidyoRouter signaling address) by clicking the text in the IP column.

9. Enter the valid FQDN of the standalone router as defined by the certificate applied:
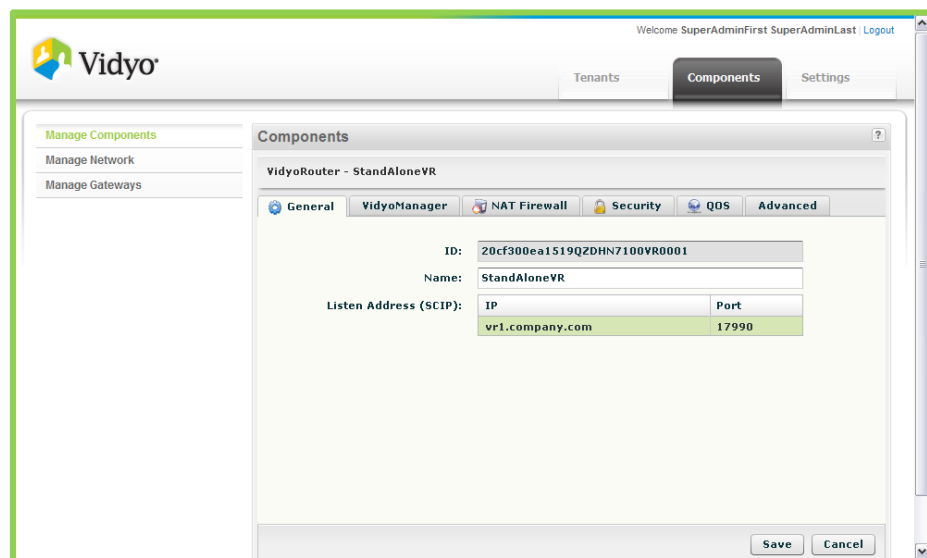
10. Go to the VidyoManager tab.

11. Under Vidyo Managers, edit IP address by clicking the text in the IP column, and enter a valid FQDN as defined by the certificate applied:
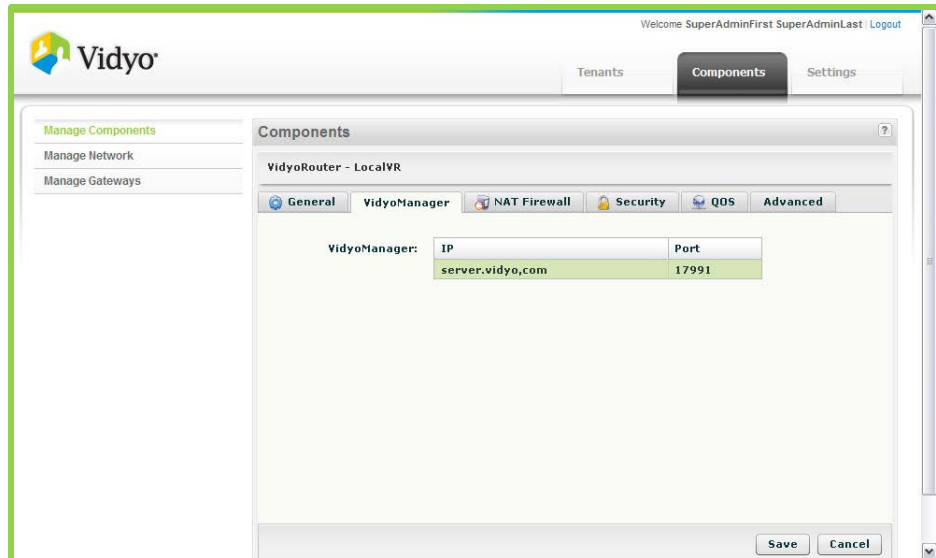
12. Go to the Security tab and Check the Encryption Enabled check-box:
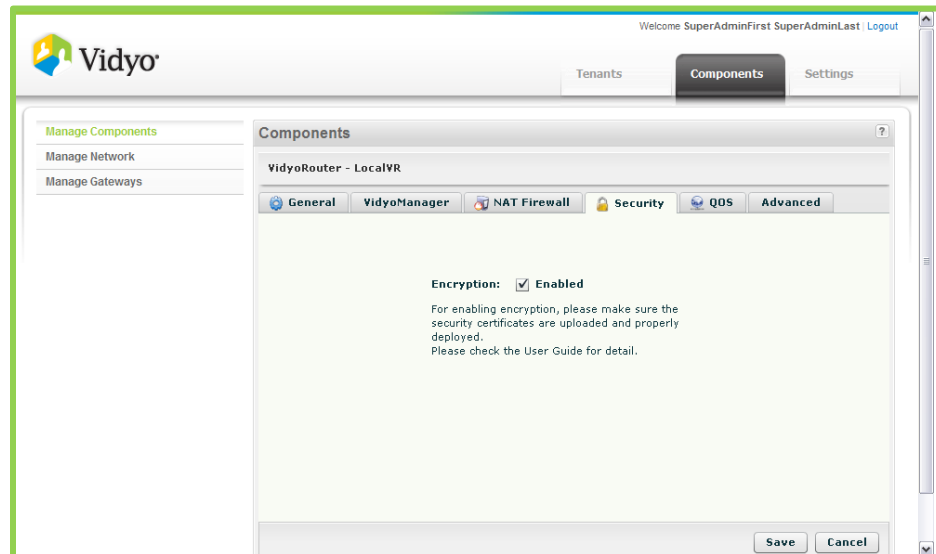
13. Press Save and OK to confirm.

14. Repeat all steps for each standalone VidyoRouter.

15. Verify that all components are Online (Status UP) and have no Alarms in the Super Admin Components page.

The VidyoConferencing system saves detailed records on conferences, point‑to‑point calls and client downloads. These Call Detail Records (CDR) are stored in a MySQL database on the VidyoPortal server. This appendix describes the schema, configuration and access mechanisms for CDR information.

The VidyoConferencing system maintains the following information in a MySQL database hosted on the VidyoPortal server.

- Client installations
- Point-to-point call activities
- Conference related activities

All time stamps used in CDR tables are based on the time zone configured for the VidyoPortal. The default time zone is the Eastern Time Zone (US & Canada, i.e., GMT-05:00). The time zone can be changed by secure shell (SSH) access by an Admin user.

CLIENT INSTALLATION TABLE

The ClientInstallation table provides information about VidyoDesktop client downloads and successful installations.

ClientInstallation Table Description

Field Name	Field Description
username	This field is captured in the XXX(YYY) format. XXX = Display Name. For a guest login, this is the Guest Name that the guest enters on the login page. YYY = username. For guest login, this is a random string.
tenantName	The name of the tenant a user is logged into. In a single‑tenant VidyoPortal, this is always Default.
EID	The Endpoint ID of a user's host machine.
ipAddress	The IP address of a user's host machine.
hostname	The name of a user's host machine.
roomName	The conference room a guest user joins.
roomOwner	The owner of the conference room a guest user joins.
timeInstalled	The time stamp for when a user downloads and installs the Vidyo-Desktop client.

ClientInstallation Table Examples

userName	tenantName	EID	ipAddress	hostName	roomName	roomOwner	timeInstalled
UserOne (Display Name)	Default	00219BD730DF-06083539383843839	172.16.1.145	User1PC			2009-03-26 10:03:50
Guestname (Random)	Default	10249BD730DF-06083539383437738	192.168.0.102	User1PC	User1	User1	2009-03-31 14:58:19

- The ClientInstallation table does NOT track the following events:

- Upgrades of the VidyoDesktop client

- Re-installation of the VidyoDesktop client

- Installation done by the following users:

    - Super Admin

    - Admin

    - Operator

- Installation of the VidyoRoom

- Installation of the VidyoGateway

CONFERENCE CALL TABLE

The ConferenceCall table keeps records every time a user joins and leaves a conference call.

ConferenceCall Table Description

Field Name	Field Description
CallID	A unique integer numerical ID that identifies a record in the table.
ConferenceName	The name of the conference room a user joins.
CallerName	The user name of a user logged into the VidyoPortal.
TenantName	The name of the tenant a user belongs to. For a single tenant VidyoPortal, the name is always Default.
JoinTime	The time stamp of when a user joins a conference.
LeaveTime	The time stamp of when a user leaves or is disconnected from a conference.

Field Name	Field Description

CallState	The state of a call. This can be either:
	
	    ■ IN PROGRESS
	
	    ■ COMPLETED
	
	    ■ SERVER RESTART
	
	If mid-conference, the server is restarted (for any reason) this call state will clarify that the time stamp is when the server comes back online.

ConferenceCall Table Examples

CallID	ConferenceName	CallerName	TenantName	JoinTime	LeaveTime	CallState
56	User3	User3	Default	2011-01-25 11:25:54	2 011 - 0 1 -2 5 11:25:58	COMPLETED
57	User2	User2	Default	2011-02-25 11:45:54	2 0 10 - 0 6 -2 5 11:46:58	COMPLETED

POINT-TO-POINT CALL TABLE

The PointToPointCall table keeps records every time a user makes a point-to-point call.

PointToPointCall Table Description

Field Name	Field Description
CallID	A unique integer numerical ID that identifies a record in the table.
ConferenceName	The ID of a temporary conference room created for a point-to-point call. It's formed by concatenating the caller username, callee username and a random number. (user1-user2-randomnumber). This value uniquely identifies a record in the table.
CallerName	The user name of a caller.
CallerTenantName	The name of the tenant a user belongs to. For a single tenant VidyoPortal, the name is always Default.
CallerJoinTime	The time stamp of when a caller joins a temporary conference room created to hold a point-to-point call.
CallerLeaveTime	The time stamp of when a caller leaves the temporary conference room created to hold the point-to-point call.

Field Name	Field Description
CalleeName	The username of the party called.
CalleeTenantName	The name of the tenant a callee belongs to. For a single-tenant VidyoPortal, this is always Default.
CalleeJoinTime	The time stamp of when a callee joins a temporary conference room created to hold the point-to-point call.
CalleeLeaveTime	The time stamp of when a callee leaves a temporary conference room created to hold a point-to-point call.
CallState	The state of the call: ■ RINGING ■ IN PROGRESS ■ REJECTED ■ CANCELED ■ NO ANSWER ■ COMPLETED ■ SERVER RESTART If in mid-conference, the server is restarted (for any reason), this call state will clarify that the time stamp is when the server comes back online.

PointToPointCall Table Examples

CallID	ConferenceName	CallerName	CallerTenantName	CallerJoinTime
56	User1-User2-86414220215	User1	Default	2011-02-17 13:45:45

Continued…

CallerLeaveTime	CaleeName	CalleeTenantName	CalleeJoinTime	CalleeLeaveTime	CallState
2011-02-17 13:45:45	User2	Default	2011-02-17 13:45:34	2011-02-26 10:03:50	COMPLETED

REMOTELY ACCESSING THE CDR DATABASE

Because the maximum number of entries in the CDR database is limited by the size of VidyoPortal storage, we advise you to delete old entries from time to time to avoid performance issues.

The VidyoPortal server is configured to allow remote MySQL clients to read and delete data. The VidyoCon-ferencing admin portal allows you to grant permissions for a password and IP address or host name for the *cdraccess* user.

The CDR database listens on port 3306.

You need the following information to connect remotely to the CDR database:

- **Database Name** = portal2 (in version 1.x, this was cdr)
- **Username** = cdraccess (limited to read and delete privileges)
- **Password** = configured using the VidyoPortal admin pages

Note: You can use the wildcard character "%" in the IP address or host name of the CDR database, *e.g.*, `192.168.1.% or %.vidyo.com.`

SUGGESTED CLIENTS/TOOLS

Vidyo recommends the following tools for accessing the CDR database in order to view and delete records and query the database for billing purposes and the creation of call reports.

MySQL Query Browser

MySQL Query Browser is a free tool from MySQL that enables you to run MySQL queries and develop SQL scripts. This tool can be used to browse the contents of tables in the CDR database. You can download it at http://www.mysql.com.

Navicat Lite

This section describes how to use Navicat Lite, a free development and administration tool, to retrieve in-formation from the CDR database.

1. Install Navicat Lite for MySQL.

   You can download it from the Navicat Web site (choose the Lite version):

   http://www.navicat.com

2. Obtain your workstation's IP address.

   If you don't know it, you can use the following Web site:

   http://www.whatismyip.com

   Configure the VidyoPortal to allow a connection from your IP address:

3. Log in as a super admin as described in Shell Admin Menu Appendix on page 125.

4. From the Settings tab, select Maintenance.

5. Select the CDR sub tab.

6. Enter your IP address or hostname.

7. Set a password.

8. To grant delete privileges, select the Allow Delete checkbox.

9. Click the Allow button.

10. In Navicat Lite, click the Connection button and choose MySQL.

The Connection dialog box appears.
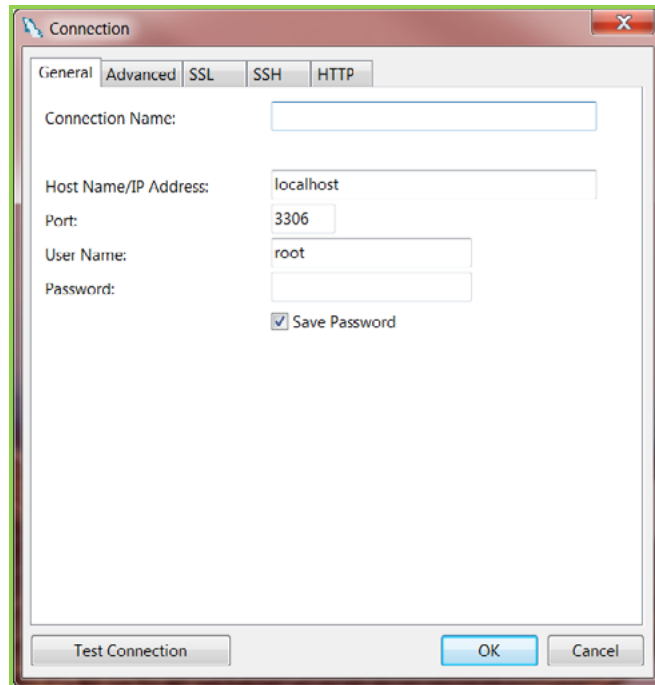
11. Configure connection settings as follows:

- **Connection Name** – Any name to identify the connection, *e.g.*, VidyoPortal CDR

- **Host name/IP address** – The IP address of your VidyoPortal

- **Username** – cdraccess

- **Password** – The one set in the VidyoPortal

12. To test the connection, click the Test Connection button.

If the connection is working, you see the following message:
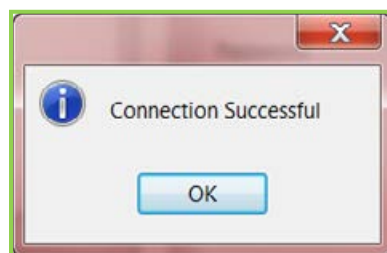
13. Click the OK button to save the connection.

The connection appears in the Connections pane on the left.
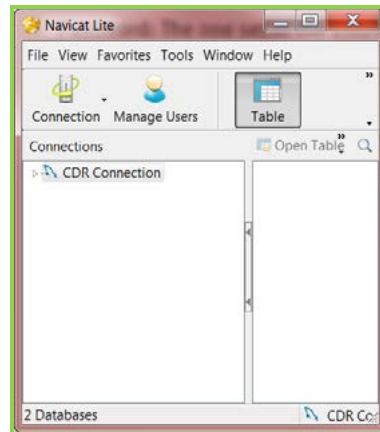
14. Double-click the connection name.
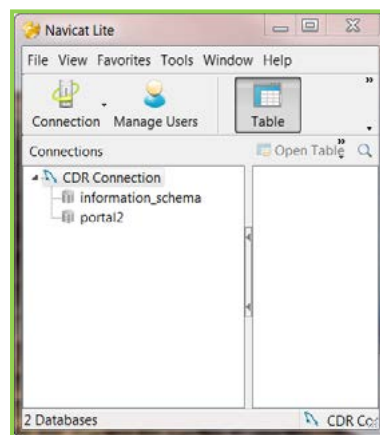
15. Double-click the *portal2* to reveal the tables contained in the database.
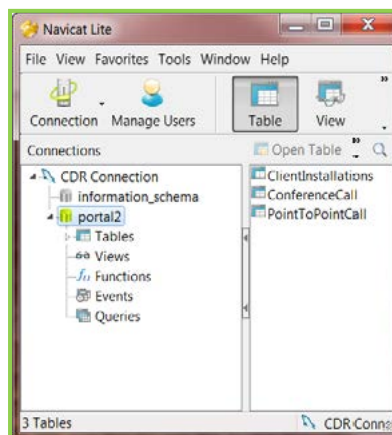
16. Double-click each table to view its contents.

28. *Microsoft Outlook Plug-In Appendix*

The Vidyo plug-in for Microsoft Outlook 2003, 2007 and 2010 permits you to schedule VidyoConferences from within Microsoft Outlook. A recipient of the message can join your conference room as either a registered user or guest.

The plug-in works with 32- or 64-bit Windows XP, Windows Vista and Windows 7 operating systems.

And it works with the three latest versions (2003, 2007 and 2010) of Microsoft Outlook. However, because of the way Microsoft changed things around a bit in Outlook 2010 the installation process is slightly different.

In Outlook 2010 Microsoft substantially changed the way things look and how you do things (what techies call the user interface or UI). If you have Outlook 2010 see the installation section for 2010 on page 182.

Note: Apple Macintosh users can be invited to meetings via Outlook, but there is no plug-in available for them to invite users themselves.

HOW TO INSTALL THE PLUG-IN FOR MICROSOFT OUTLOOK 2003 AND 2007

1. Close all Microsoft Office applications.

2. Download the appropriate Outlook plug-in from the download section of the web site at www.vidyo.com.

3. Run the install wizard and install the Outlook plug-in.

   You are prompted to accept the license and install the plug-in. (Don't be confused that the title of the licensing agreement reads "Vidyo Conferencing Outlook Plug-in 2.0.4. The plug-in is compatible with both 2.0.4 and 2.1 VidyoConferencing Systems.)

4. Respond to each prompt until the plug-in is successfully installed.
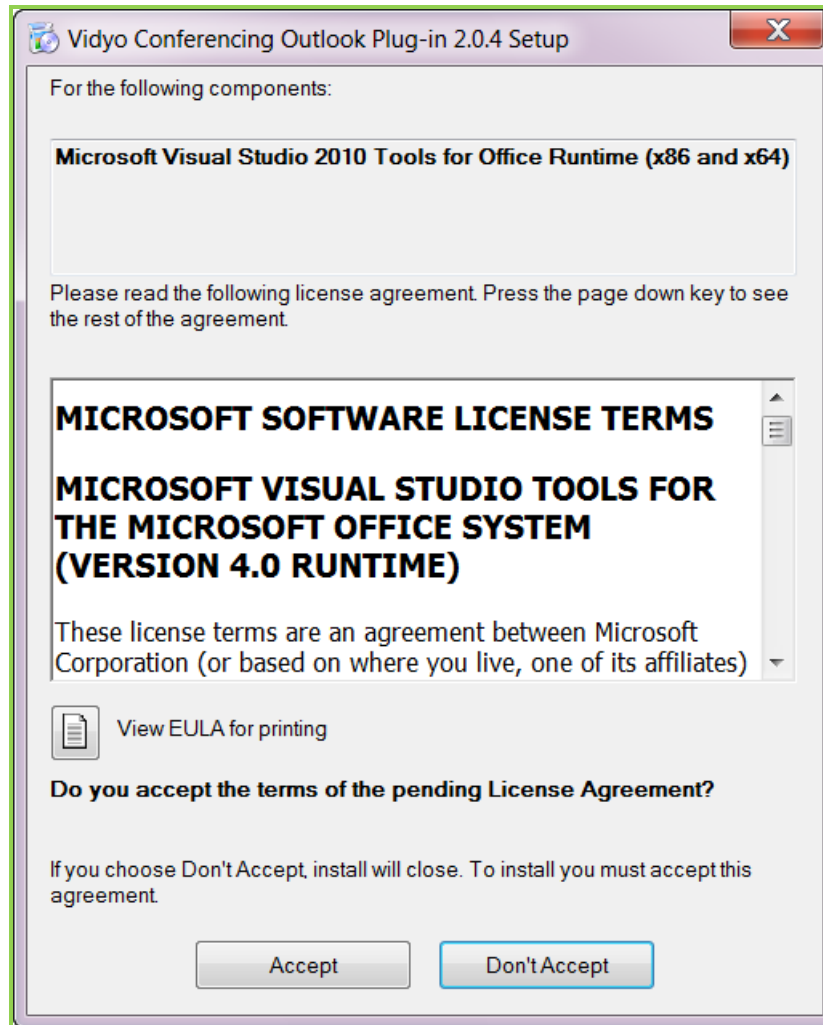
5. Launch Microsoft Outlook.

6. From the Tools menu, select Options to display the Options window.
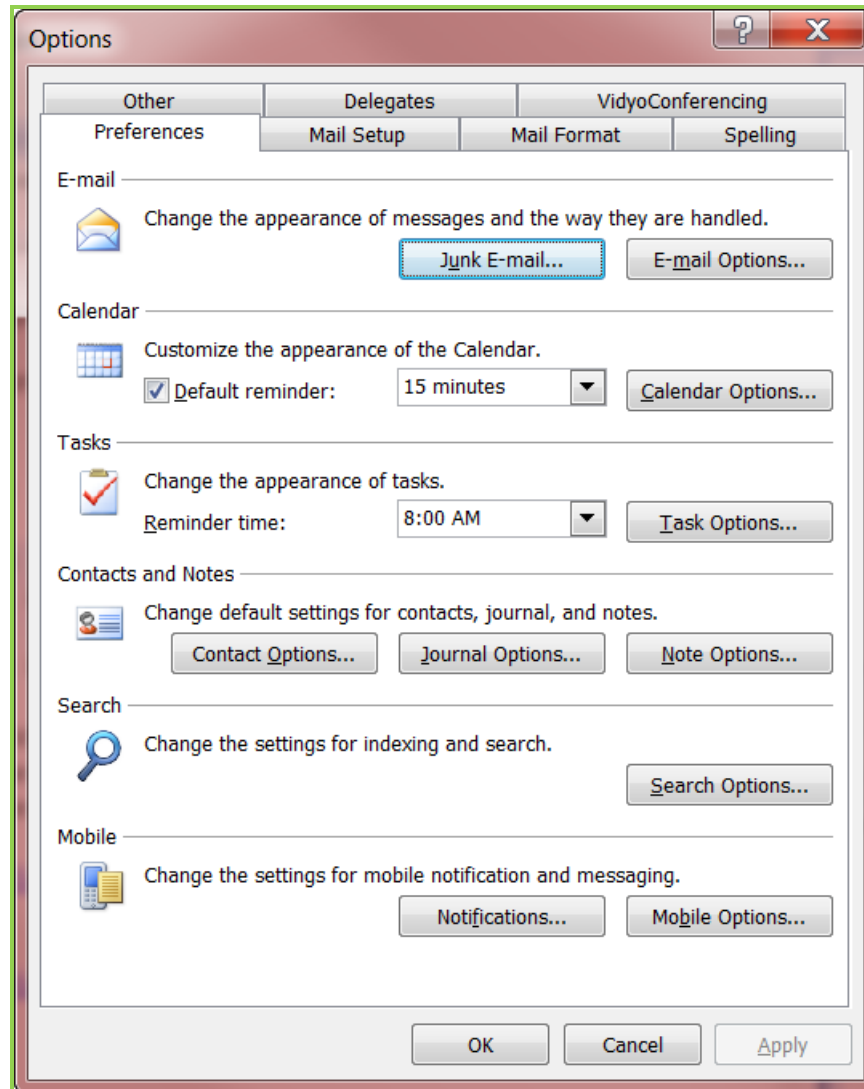
7. Select the VidyoConferencing tab.

8. Enter the following information:

   ▪ **Server** — The fully qualified URL for the VidyoPortal.

   ▪ **Example**: `http ://<`yourvidyoportal.com`>`

   ▪ **User ID** — Your VidyoPortal user name.

   ▪ **Password** — Your VidyoPortal password.

9. Click the Apply button.

10. Click the Test Configuration button.

11. If the configuration is successful, you'll see the following message:
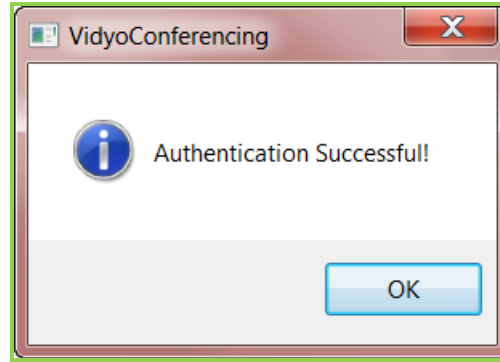
12. Click OK, and then click OK in the Options window.

HOW TO SEND A MEETING INVITATION IN OUTLOOK 2003 AND 2007

The Vidyo plug-in for Outlook inserts your room URL into an Appointment or Meeting Request message along with the room PIN, if you've chosen to use one, and boiler plate invitation text that you can edit. If you don't have a room URL, one is automatically created. The boilerplate invitation text is created by the VidyoConference administrator and can be modified. For information about creating a room invitation message, see the VidyoConferencing Administrators Guide.

To send a meeting invitation:

1. Create an Appointment or Meeting Request message.

   The VidyoConferencing button appears at the far right side of the tool bar.
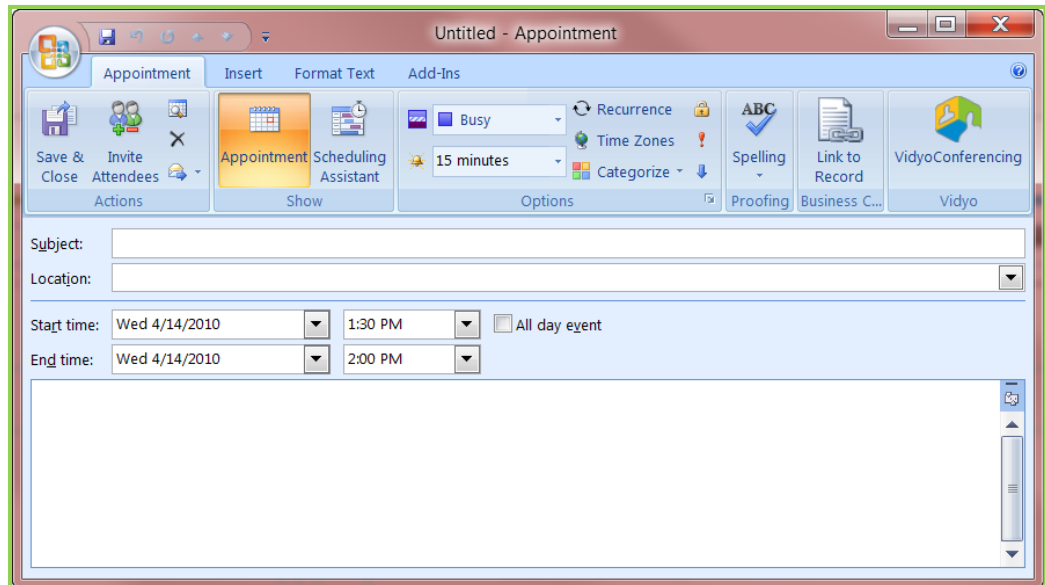
   Note: If you do not see the VidyoConferencing button in the tool bar, you have not finished configuring the Outlook plug-in. Try again or contact your system administrator Help Desk.

2. Click the VidyoConferencing button.

   The room URL (and room PIN if you have set one) appear in the body of the message along with standard boilerplate invitation text.
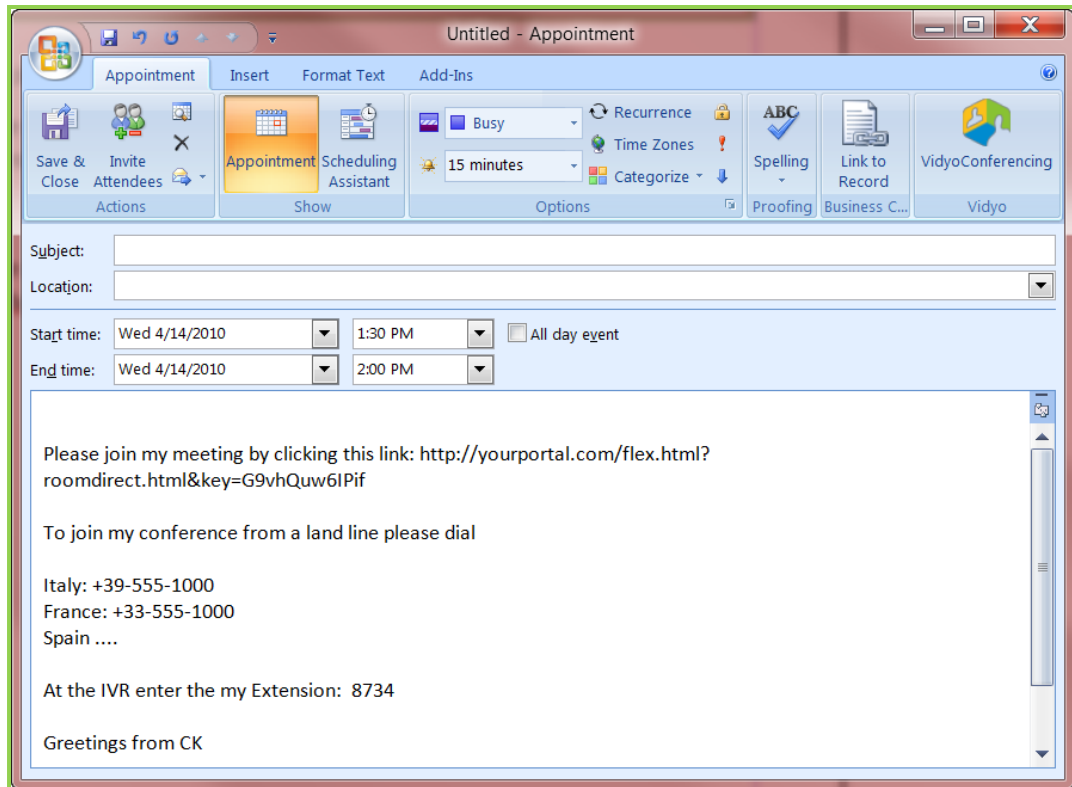
Note that your meeting invitation with the usual boilerplate text appears. You can add your own text to the invitation if you care to. You can also add or delete invitees and change the time and length of the meeting. Remember that you can use Outlook's Scheduling Assistant to determine when all of your invitees will be available.

3. Edit the text as desired and click the Send button.

HOW TO INSTALL THE OUTLOOK PLUG-IN FOR MICROSOFT OUTLOOK 2010

1. Close all Microsoft Office applications.

2. Download the appropriate Outlook plug-in from the download section of the web site at www.vidyo.com.

3. Run the install wizard and install the Outlook plug-in.

   You are prompted to accept the license and install the plug-in.

4. Respond to each prompt until the plug-in is successfully installed.
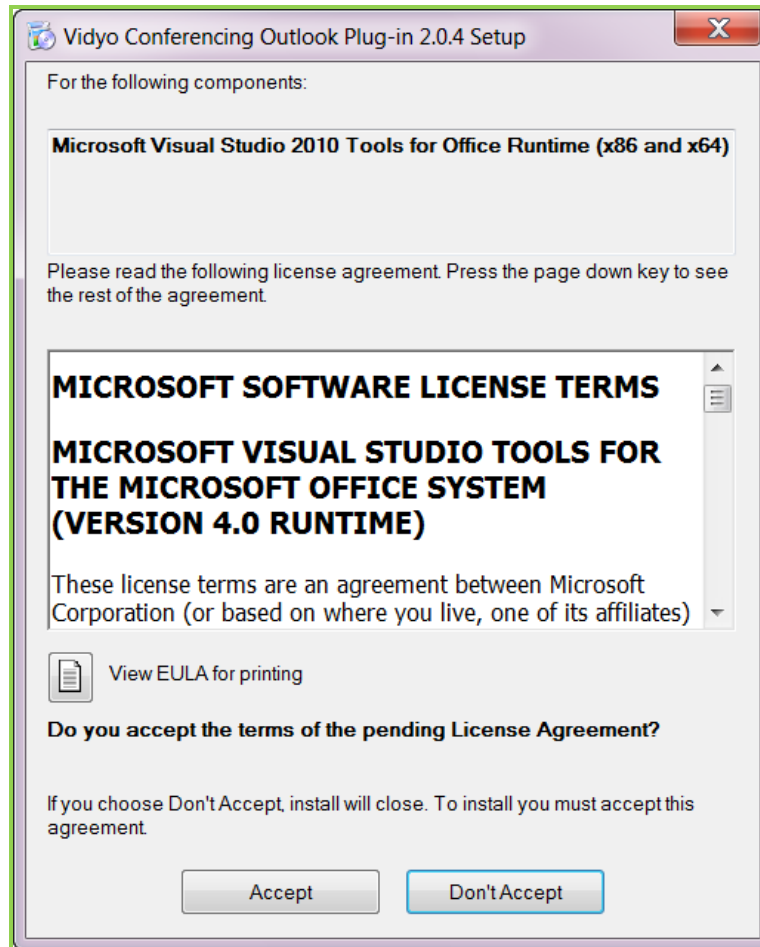
5. Launch Microsoft Outlook.

6. From the File menu choose Options.

28. Microsoft Outlook Plug-In Appendix
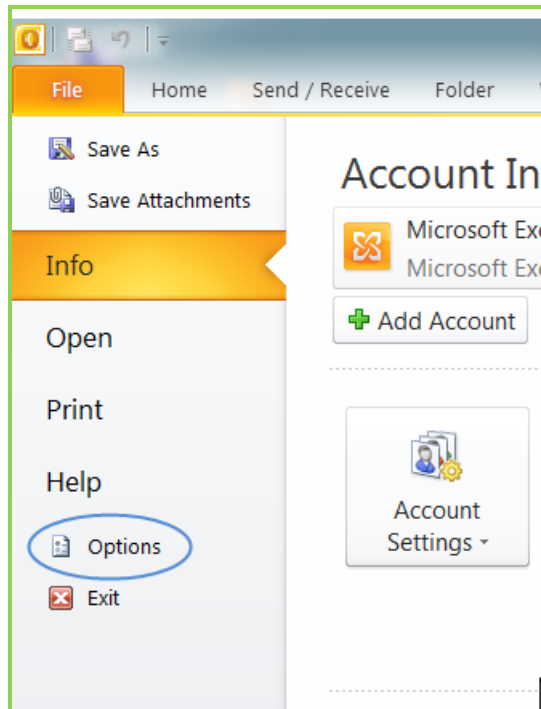
The Outlook Options dialog box opens.
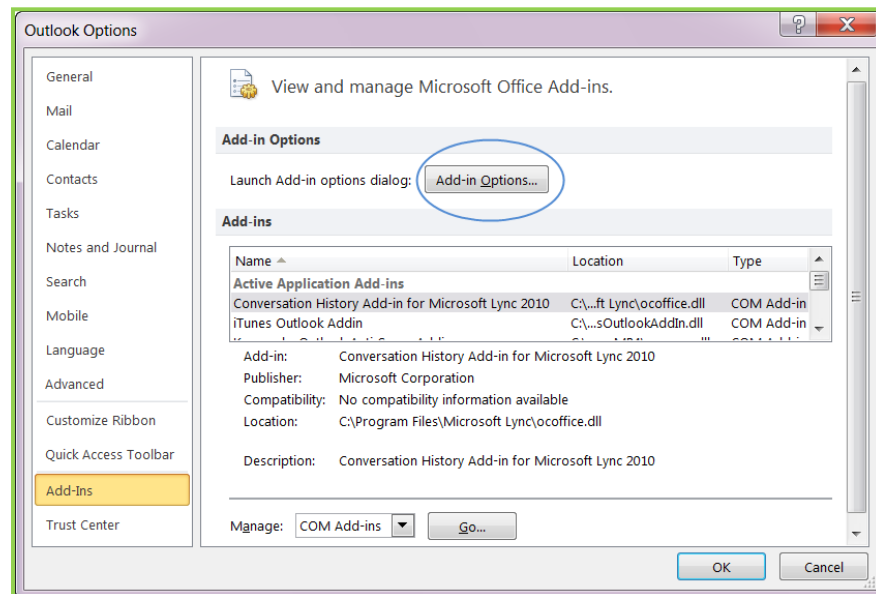
7. On the left-hand menu click on Add-ins.

8. Click the Add-in Options button.

The Add-in Options dialog box opens.
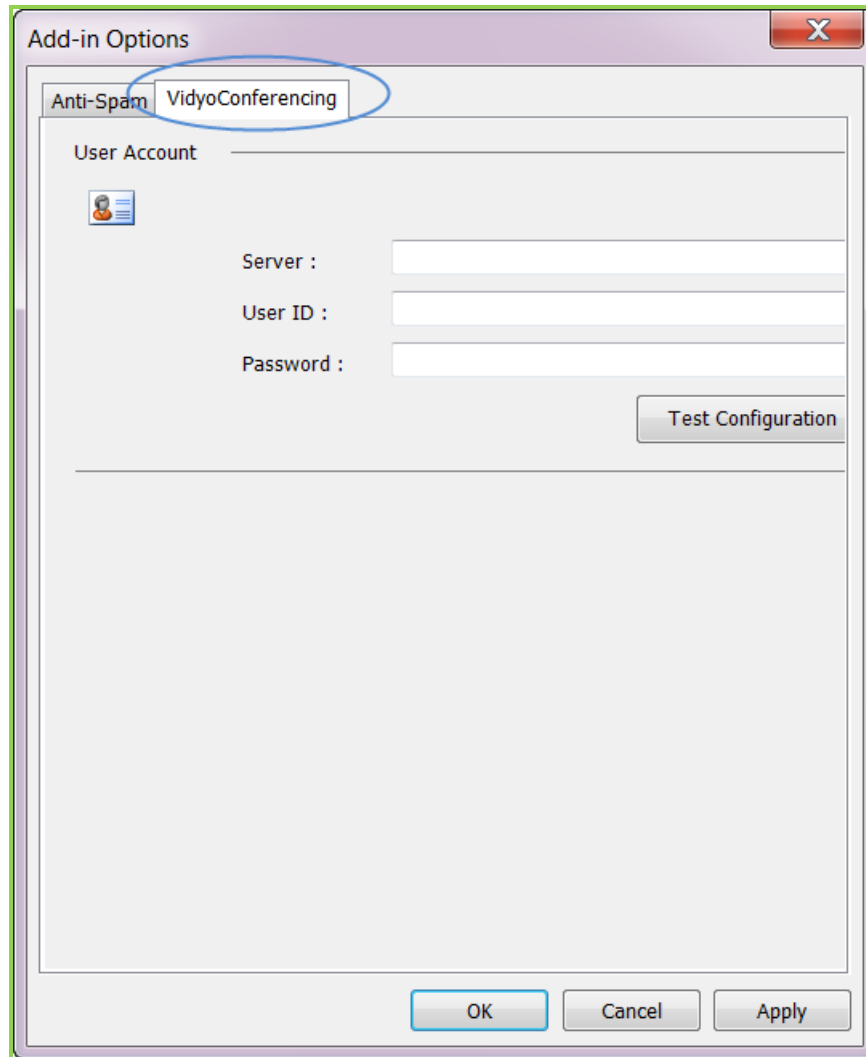
9. Click on the VidyoConferencing tab.

10. Enter the following information:

   ■ Server — The fully qualified URL for the VidyoPortal.

   Example: http://‹vidyoportal.yourcompany.com›

   ■ User ID — Your VidyoPortal user name.

   ■ Password — Your VidyoPortal password.

11. Click the Test Configuration button to make sure your setup works.

   If you successfully installed the add-in you'll see this dialog box:
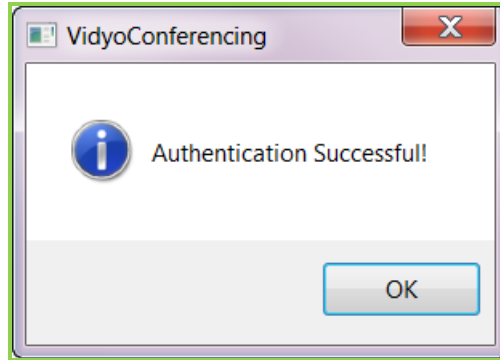
You've successfully installed the add-in.

12. Click the OK button to complete the installation.

If you get an error message like this one it means there was a problem:
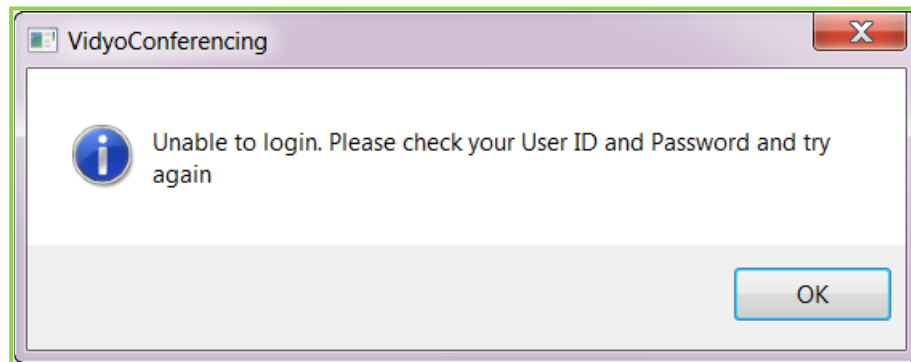
Contact your system administrator or your organization's IT department

HOW TO SEND A MEETING INVITATION IN OUTLOOK 2010

The Vidyo plug-in for Outlook inserts your room URL into an Appointment or Meeting Request message along with the room PIN, if you've chosen to use one, and boiler plate invitation text that you can edit. If you don't have a room URL, one is automatically created. The boilerplate invitation text is created by the VidyoConference administrator and can be modified. For information about creating a room invitation message, see the VidyoConferencing Administrators Guide.

4. Select the Meeting button Outlook toolbar.
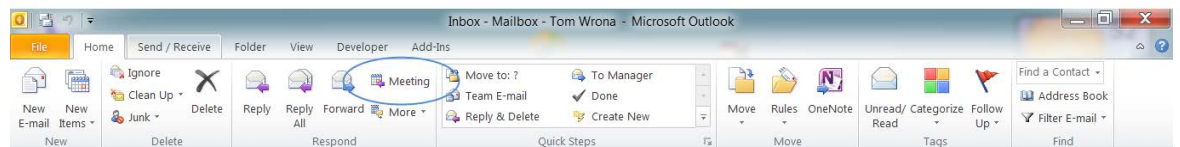
Note the VidyoConferencing button that appears at the far right of the menu bar.

5. Click the VidyoConferencing button.
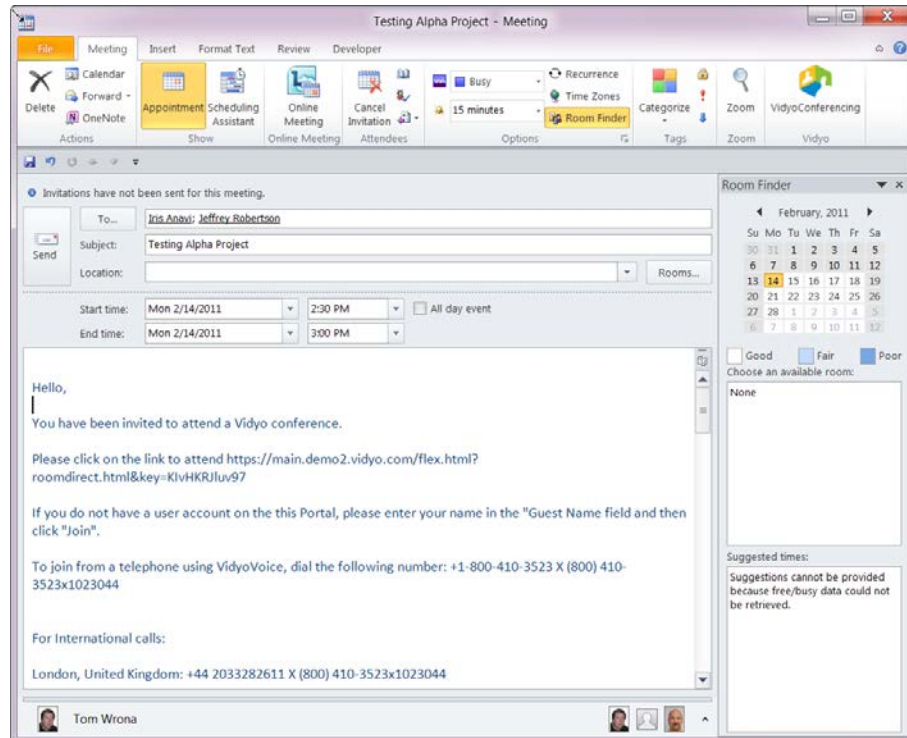
Note that your meeting invitation with the usual boilerplate text appears. You can add your own text to the invitation if you care to. You can also add or delete invitees and change the time and length of the meeting. Remember that you can use Outlook's Scheduling Assistant to determine when all of your invitees will be available.

6. Edit the text as desired and click the Send button.

A recipient of the message clicks the link to join your meeting. The link prompts a registered user to log into the VidyoPortal and join the meeting. It enables a contact without a VidyoPortal account to join the meeting as a guest.

29. *Microsoft Office Communicator and Lync Plug-ins Appendix*

OVERVIEW

Note: These are the virtually the same instructions that appear in the User Guide. See the Admin Setup section below for what you'll need to do as the Admin (for MOC only, not for Lync).

If your organization uses Microsoft Office Communicator (MOC) or its successor, Microsoft Lync, you can easily add VidyoConferencing capabilities to the one you use. Vidyo makes a plug-in that can be added to MOC and Lync.

The Vidyo Plug-in for MOC and Lync is an optional component (sold separately) that enables a VidyoPortal user to invite MOC or Lync instant messaging contacts to a meeting in the user's room. Both registered VidyoPortal users and guest users can be invited to join a meeting.

This plug-in works with:

- 32- and 64-bit Windows XP, Windows Vista and Windows 7 operating systems

  And with both of these (although, of course you can only have one or the other installed):

- Microsoft Office Communicator version R1 or R2 with a minimum licensing level of standard CAL

- Lync 2010.

Note: You use the same installer for both MOC and Lync. The installer automatically detects which program is installed on your computer and installs the appropriate plug-in for it.

Note: Apple Macintosh® users can be invited to meetings via Office Communicator, but there is no plug-in available for them to invite users.

ADMIN SETUP FOR OFFICE COMMUNICATOR

Office Communicator sign-in IDs and VidyoPortal user names must match exactly. If you are starting with a fresh VidyoPortal installation, you can use the bulk user import utility in the VidyoPortal to import Active Directory user IDs into the VidyoPortal database. However, if you do this, the Active Directory user IDs must match the Communicator/Lync sign-in IDs.

For information about importing Active Directory user IDs into the VidyoPortal, see the VidyoConferencing Administrators Guide.

Note: Synchronizing passwords is not currently supported.

Clickable URLs

1. Set Office Communicator server options for IM filtering to enable clickable links in IM sessions.

   This enables users not logged into their Vidyo accounts and guest users to easily join a VidyoConference. If these options are not set on the Communicator server, the links are sent as plain text links that cannot be clicked.

   For more information, refer to the Microsoft Office Communications Server 2007 Administration Guide in the section on how to disable URL filtering in IM message. Download the guide at:

http://www.microsoft.com/downloads/details.aspx?FamilyID=CB7DC2DE-4504-484E-9229-BD8614BE0633&displaylang=en

29.   *Microsoft Office Communicator and Lync Plug-ins Appendix*

PREREQUISITES

To perform the setup described in this appendix, you must first purchase Microsoft Office Communicator or Lync and the Vidyo plug-in.

- At the time of publication information regarding Microsoft Office Communicator 2007 R2 could be found online at this URL:

  http://office.microsoft.com/en-us/help/office-communicator-2007-resource-center-HA010237394.aspx?CTT=1

- At the time of publication information regarding Lync 2010 can be found online at this URL:

  http://office.microsoft.com/en-us/communicator-help/

- To purchase the Vidyo MOC and Lync Plug-in, contact your Vidyo sales representative at +1.866.99.VIDYO (+1.866.998.4396).

HOW TO INSTALL THE COMMUNICATOR PLUG-IN

To install the Vidyo Office Communicator Plug-in:

1. If you're currently running the Communicator client shut it down by right-slicking the green Communicator icon in the notification area (also called the system tray) and selecting Exit.
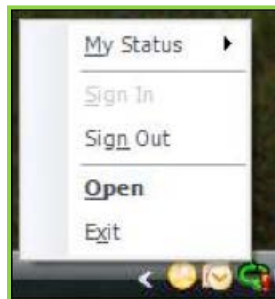
2. Get your copy of the plug-in installer as described by your system administrator or help desk.

   The installer is labeled:

   `ClientMOCIntInstaller-win32-TAG_VMOC_<X _X_X_XXXXX>.exe`, where ‹`X_X_XXXXX`› is the version of the installer. A convenient place to download it to is your desktop.

   Note: Don't be confused by the fact that the installer name contains "win32." It works with both 32-bit and 64-bit versions of Windows.

29. Microsoft Office Communicator and Lync Plug-ins Appendix

HOW TO INVITE PARTICIPANTS FROM OFFICE COMMUNICATOR

To invite participants to a meeting from the Office Communicator:

1. After you've logged into the VidyoPortal, log into the Office Communicator.

   Your Communicator sign-in ID is the same as your VidyoPortal user name (case sensitive). Your password may or may not be the same; contact your system administrator for information.

   Note: Being logged into Communicator does not automatically log you into the VidyoPortal.
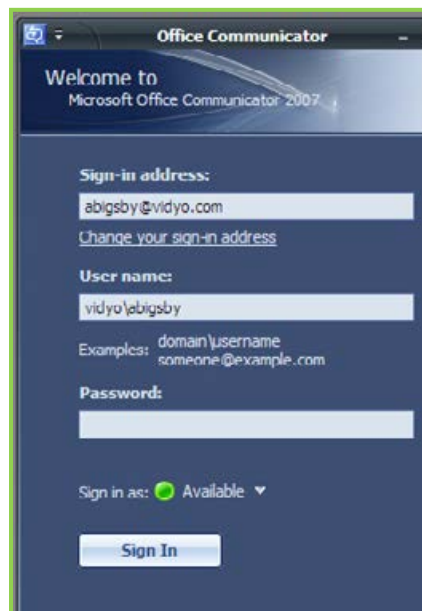
   You see a list of Communicator contacts.

29. *Microsoft Office Communicator and Lync Plug-ins Appendix*
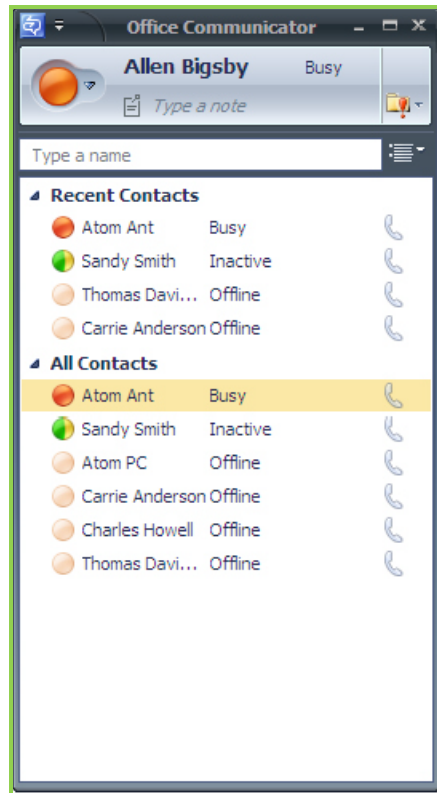
2. Type a name in the user bar and add it to the chat list.

    Add as many contacts as necessary.

3. Select participants from the list of added contacts (Shift-click or Control‑click to select multiple participants).

    Note: You can also select participants from an open conversation session window.

4. To start the VidyoConference, right-click the selected contacts and choose the VidyoConferencing command.

29. Microsoft Office Communicator and Lync Plug-ins Appendix
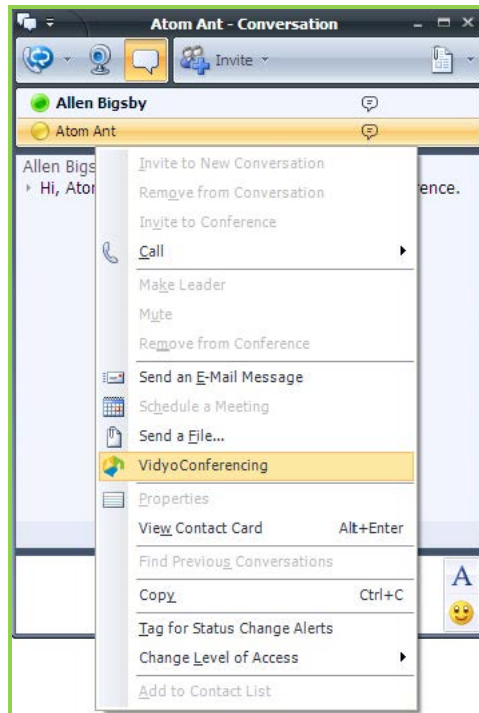
Your VidyoConference with the participants you selected begins.

For a user not logged into the portal or in another conference, and a contact without a VidyoPortal account, a Communicator IM message is sent that includes your room link.
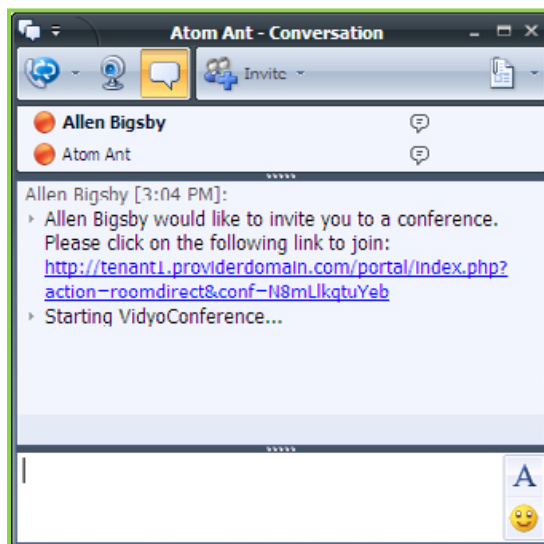
Clicking the link:

- Prompts a user to log into the VidyoPortal and join the meeting.

- Enables a contact without a VidyoPortal account to join the meeting as a guest.

29. *Microsoft Office Communicator and Lync Plug-ins Appendix*

MICROSOFT OFFICE COMMUNICATOR NOTES

- When a user enters a conference, their Communicator status changes to "Busy." A meeting scheduled in the Outlook Calendar for the same time overrides this status.

- You control a conference in the Control Meeting page of the VidyoPortal. See Controlling Your Meeting in the VidyoPortal in the VidyoPortal User Guide for information.

- Removing someone from a Communicator chat does not remove them from the VidyoConference. You must do this in the Control Meeting page of the VidyoPortal.

- Ending a meeting can only be done by closing the VidyoDesktop client or through the Control Meeting page in the VidyoPortal User Guide.

- Conference participants can disconnect themselves from a meeting by clicking the VidyoDesktop Disconnect button.

- You can drag participants from the main Communicator window contact list into a Communicator chat already in process to invite them to your meeting, or by right-clicking the contact and selecting the VidyoConferencing command.

To invite a legacy system, VidyoRoom or VidyoPortal user without a Communicator account, use the Invite by Email command in the Control Meeting page of the VidyoPortal. See Controlling Your Meeting in the VidyoPortal in the VidyoPortal User Guide more for information.

HOW TO INSTALL THE LYNC PLUG-IN

Installing the plug-in for Lync is very similar to installing it for MOC.

1. If you're currently running Lync shut it down by right-clicking the green Lync icon in the notification area (also called the system tray) and selecting Exit.
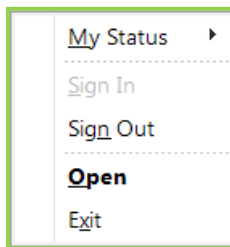
3. Get your copy of the plug-in installer as described by your system administrator or help desk.

   The installer is labeled:

   `ClientMOCIntInstaller-win32-TAG_VMOC_<X _X_X_XXXXX>.exe`, where `<X_X_XXXXX>` is the version of the installer. A convenient place to download it to is your desktop.

   Note: Don't be confused by the fact that the installer name contains "win32." It works with both 32-bit and 64-bit versions of Windows.

2. Start the Installer by double-clicking it.

   If you have Lync running and you forgot to exit it you'll see an error dialog box:

29. *Microsoft Office Communicator and Lync Plug-ins Appendix*
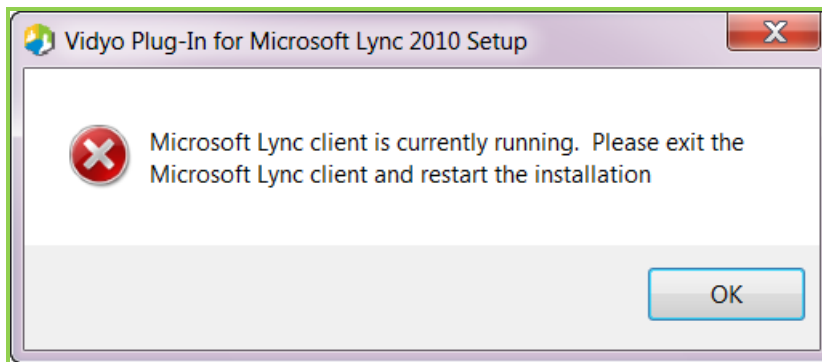
If this happens, like the box says, exit Lync and restart the installation.

Next, the Vidyo Plug-in for Microsoft Lync 2010 Welcome dialog box opens:
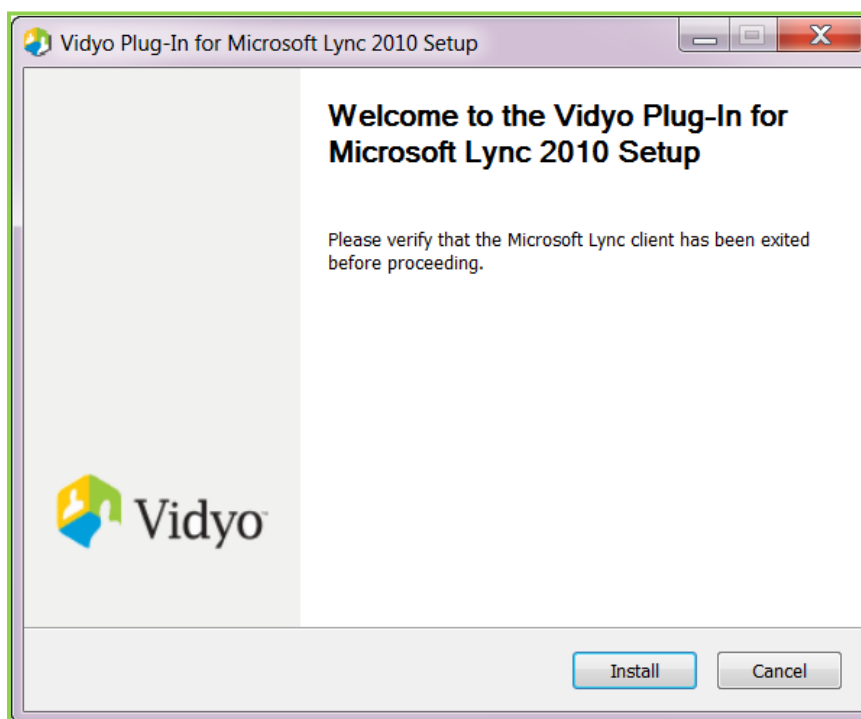
In just a few seconds the installation will be done and you'll see the Completing Setup dialog box.

3. Click the finish button.

When the installation is completed you'll be able to access Vidyo features from within Communicator

29. Microsoft Office Communicator and Lync Plug-ins Appendix
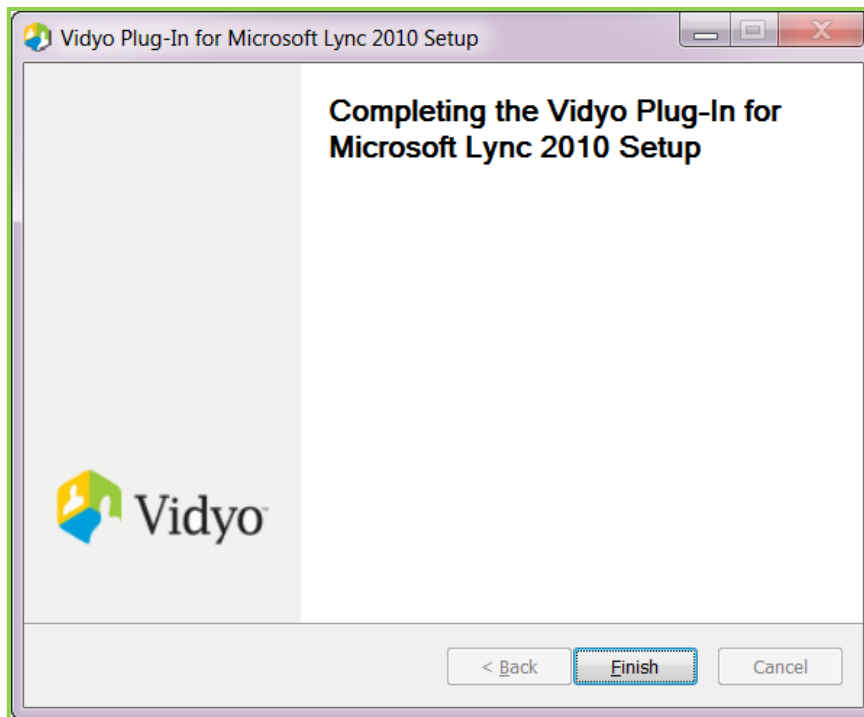
THE USER EXPERIENCE

How to Invite Participants from Lync

1. Log in to your Portal

   If Lync isn't set to start up automatically when you start Windows, start Lync. You're then also logged into the VidyoPortal, Your Lync sign-in ID is the same as your VidyoPortal user name (case sensitive). Your password may or may not be the same; contact your system administrator for information.

   Note: Being logged into Lync does not automatically log you into the VidyoPortal.

29.   *Microsoft Office Communicator and Lync Plug-ins Appendix*
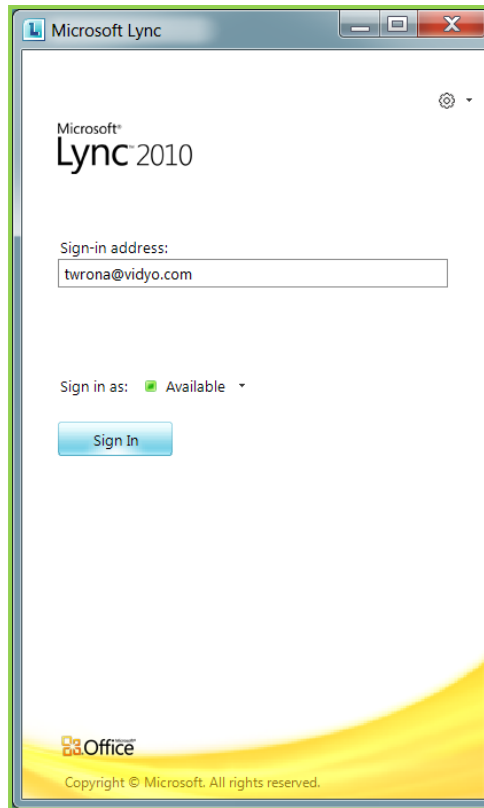
You see your list of Lync contacts.
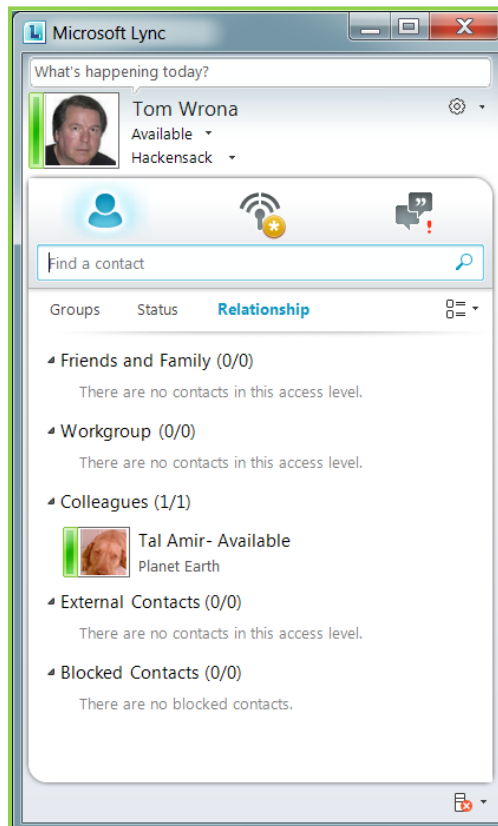
29. *Microsoft Office Communicator and Lync Plug-ins Appendix*

2. Type a name in the user bar and add it to the chat list.

    Add as many contacts as necessary.

3. Select participants from the list of added contacts (Shift-click or Control‑click to select multiple participants).

    Note: You can also select participants from an open conversation session window.

4. To start the VidyoConference, right-click the selected contacts and choose the VidyoConferencing command.
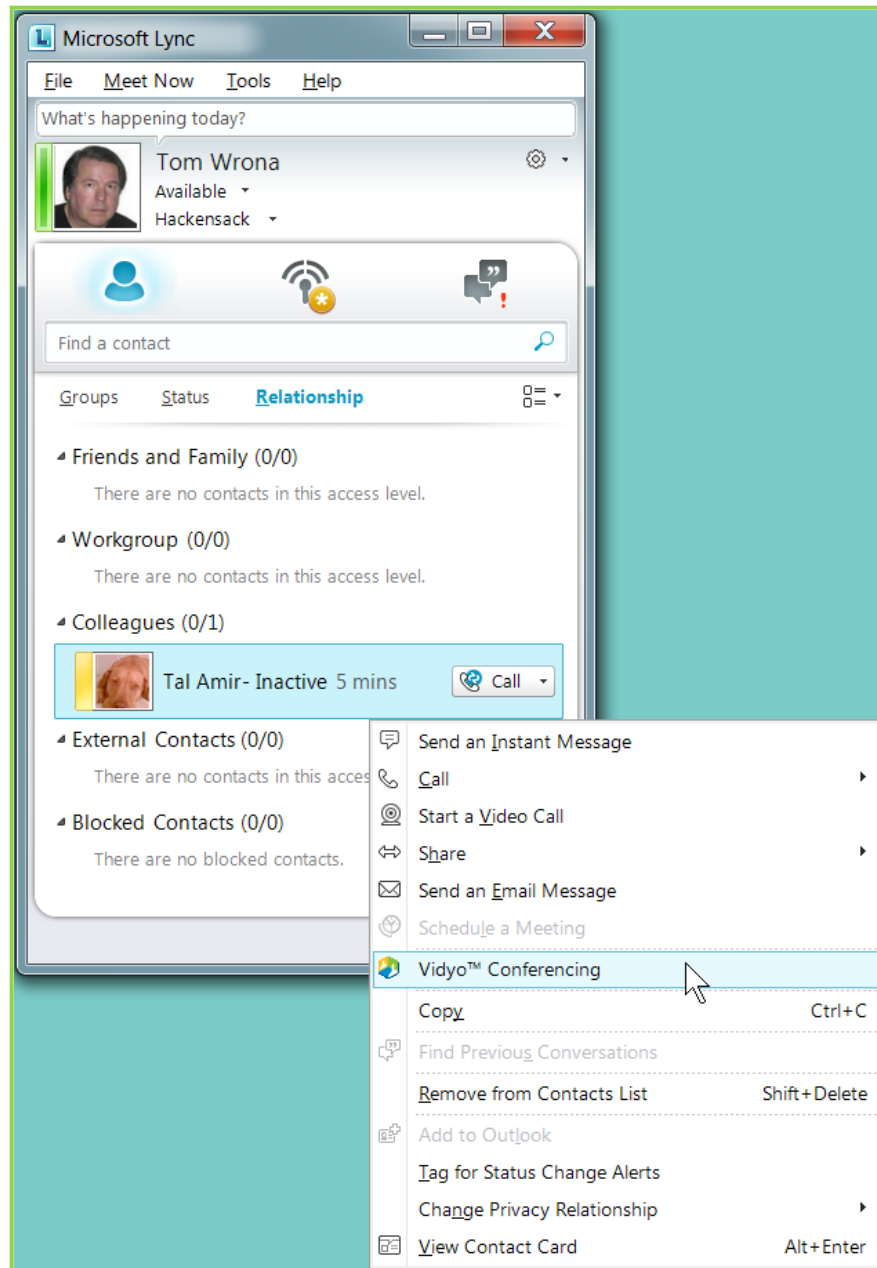
The Starting VidyoConference window opens.

29. Microsoft Office Communicator and Lync Plug-ins Appendix
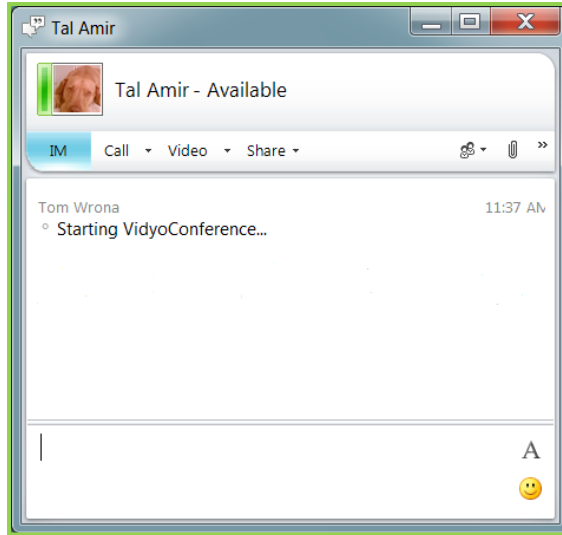
Your VidyoDesktop window also opens.

29.   *Microsoft Office Communicator and Lync Plug-ins Appendix*

Note: You a use can also start a VidyoConference from an open chat window by right clicking on a person's name and selecting Vidyo™ Conferencing from the context menu. If the user is in a group conversation only the person on whom you right click will be included in the conference initially.
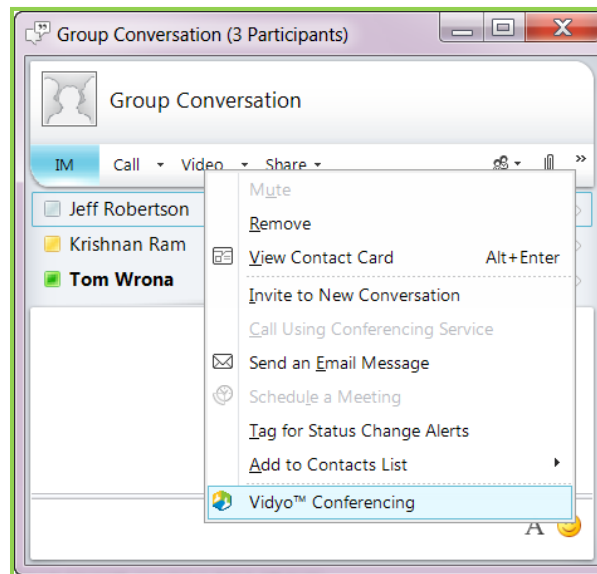
At the end of the call the Lync window says that the conversation was saved. This is a standard Lync message and **does not** mean that the audio/video portion of the conversation was saved. It just means that if you have the Turn on Logging feature in Lync so that any IMs you may have sent or received have been saved.
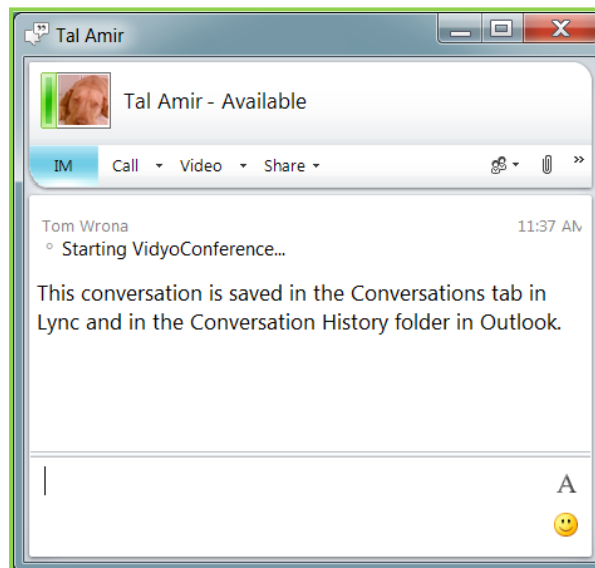
LYNC NOTES

- When a user enters a conference, their Lync status changes to "Busy." A meeting scheduled in the Outlook Calendar for the same time overrides this status.

- The user controls a conference in the Control Meeting page of the VidyoPortal.

29.   *Microsoft Office Communicator and Lync Plug-ins Appendix*

■ Removing someone from a Lync chat does not remove them from the VidyoConference. You must do this in the Control Meeting page of the VidyoPortal.

■ Ending a meeting can only be done by closing the VidyoDesktop or through the Control Meeting page in the VidyoPortal.

■ Conference participants can disconnect themselves from a meeting by clicking the VidyoDesktop Disconnect button.

■ You can drag participants from the main Lynx window contact list into a Lynx chat already in process to invite them to your meeting, or by right-clicking the contact and selecting the VidyoConferencing command.

To invite a legacy system, VidyoRoom or VidyoPortal user without a Lynx account, use the Invite by Email command in the Control Meeting page of the VidyoPortal.

30. Lotus Sametime Plug-In Appendix

HOW TO INTEGRATE THE SAMETIME PLUG-IN WITH YOUR VIDYO SYSTEM

We've created Lotus Sametime plug-ins so your Sametime users can access the power of VidyoConferencing right from within Sametime whether you're using Sametime alone or in conjunction with Lotus Notes.

You install the Vidyo Sametime plug-in exactly how you install all other plug-ins into Sametime.

Sametime sign-in IDs and VidyoPortal usernames must match exactly. If you are starting with a fresh VidyoPortal installation, you can use the bulk user import utility in the VidyoPortal to import usernames into the VidyoPortal database. If you do this, the database usernames must match the Sametime sign-in IDs exactly.

You should understand a few things about the differences between VidyoPortal usernames and Sametime userIDs. In Sametime, if you're using the notation `Jdoe/somecompany`, *only* `Jdoe` is considered the userID. Whatever comes after the slash is not part of the username.

While most VidyoPortal installations use just what we commonly think of as the username part as the VidyoPortal username (e.g., `Jdoe`), It's "legal" to use a full email address as the VidyoPortal username (e.g., `Jdoe@somecompany.com`). In the latter case, the Sametime username would have to be `Jdoe@somecompany.com` too.

How you get the VidyoConferencing plug-in to your users is up to you. "Adding optional features to the client after install" that starts on page 83 in the Lotus Sametime Standard: Installation and Administration Guide describes the ways you can distribute plug-ins. Having your users do it themselves from a URL you provide them is just one way:
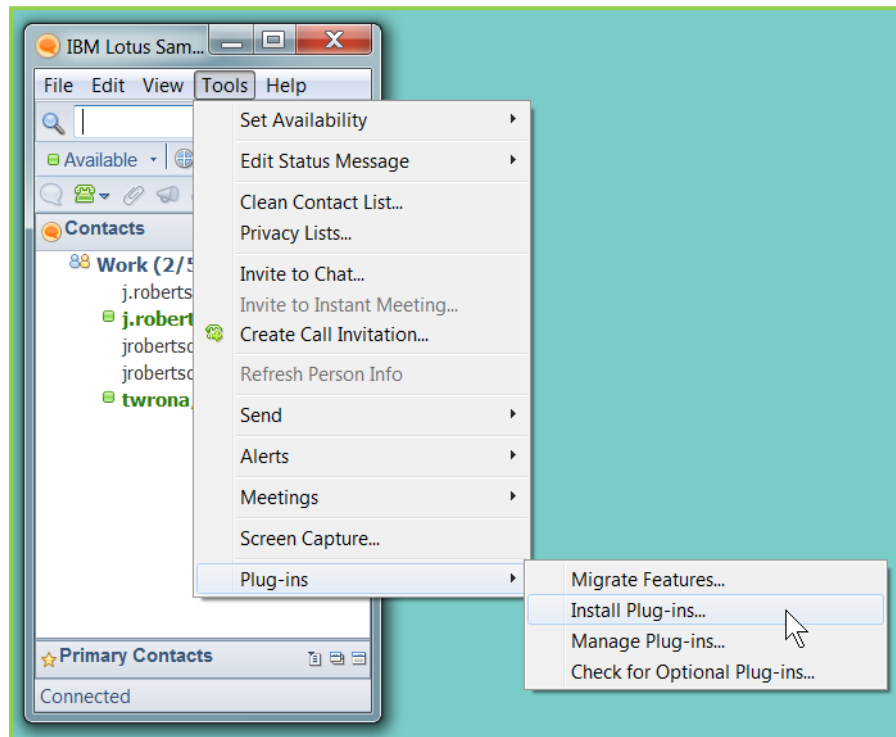
PREREQUISITES

To perform the setup described in this appendix, you must first purchase IBM Lotus Sametime (or IBM Sametime and IBM Lotus Notes). You then need to purchase the Sametime Vidyo plug-in version that matches your environment.

- To purchase the Vidyo Lotus Sametime Plug-in, contact your Vidyo sales representative at +1.866.99.VIDYO (+1.866.998.4396).

- Note: One version of the plug-in is designed to work in a Sametime-only environment. There's a separate version for using Sametime with Lotus Notes. Be sure to acquire the version that fits your environment.

Once the VidyoConferencing plug-in is installed, when a user right-clicks on a Sametime user's name the Start Vidyo™ Conference option is listed on the context menu As usual, the caller can click and then Shift+click to select a contiguous set of users or Ctrl+click to select individual users. If multiple users are selected, multiple users will be invited. Those who accept the invitation will participate in a multi-party conference.

30. Lotus Sametime Plug-In Appendix

THE USER EXPERIENCE

In order to start a VidyoConference or one-to-one meeting the calling user must be logged into his or her Portal. If not, the following error message appears:

Once the caller logs in the call can be made.

Any invitees who are not logged in to their VidyoPortals will receive a pop-up message like this one:
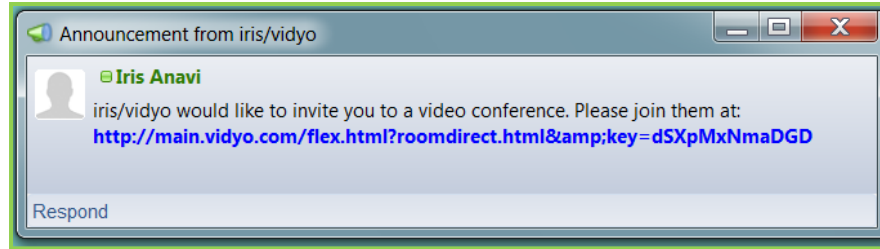
If the called party answers the call the VidyoDesktop opens as it normally does, with the user(s) who accepted the invitation appearing in the VidyoDesktop window. For any user who is not logged in to the VidyoPortal the caller sees the following message:
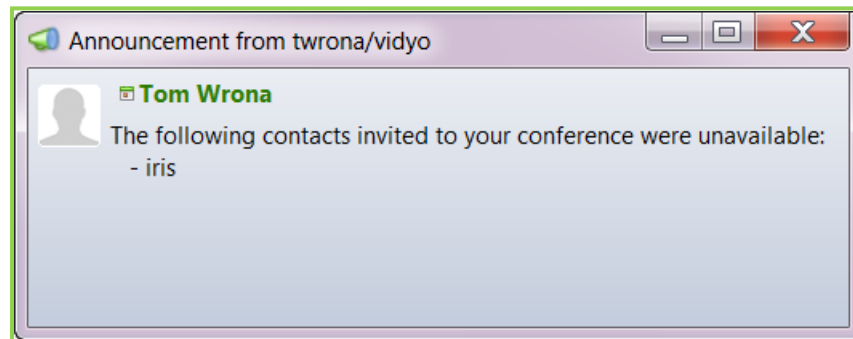
As with other Sametime windows, the exact shape, location and size of the window may vary.

31. Adobe Connect Vidyo Pod Appendix

OVERVIEW

Adobe Connect is a web conferencing tool from Adobe®. It allows an Adobe Connect host to create web based virtual meeting rooms that he or she can invite other users to join. The end users need only a web browser and the Adobe Flash Player to participate in the meetings. Within the scope of an Adobe Connect meeting room, the host can enable a number of tools, also known as Pods that provide a rich experience for communicating and collaborating.

Vidyo has developed a custom Pod (Vidyo Pod) that can be shared within an Adobe Connect meeting room session, to enable Vidyo's patented platform and technology for video conferencing as part of the Adobe Connect meeting.

This appendix describes both how to install the Vidyo Pod as an administrator and how your users will use it.

MINIMUM REQUIREMENTS

The following set of requirements need to be in place to use Adobe Connect Vidyo Pod

- Adobe Connect 8.0
- VidyoConferencing 2.1.0 or later
- Adobe Connect Vidyo Pod (swf file)
- Adobe Connect Vidyo Pod License (Web Portal User API) enabled on your VidyoPortal
- Adobe Connect URL configured in the crossdomain.xml file on your VidyoPortal

CONFIGURING CROSSDOMAIN.XML

Take the following steps to set up security requirements of the VidyoPortal to work with the Adobe Connect Vidyo Pod.

1. Log in to the Admin Console Portal using an SSH client.

2. Choose menu item `17. Configure Adobe Connect Plugin`.

```
      Local Time: Fri Jul 15 13:43:47 EDT 2011
Universal Time: Fri Jul 15 17:43:47 UTC 2011

 1. Configure IP Address
 2. Configure DNS Nameserver
 3. Configure NTP Time Servers
 4. Configure Time Zone
 5. Configure Ethernet Options
 6. Display IP Address
 7. Display Host & Domain Names
 8. Query NTP Time Servers
 9. Display Kernel IP Routing Table
10. Display ARP Table
11. Ping Utility
12. Traceroute Utility
13. Set 'admin' password
14. Reboot system
15. Shutdown System
16. Restore HTTP(S) settings to default
17. Configure Adobe Connect plugin
 x. Exit System Administrator Console

Selection: 17
```

31. *Adobe Connect Vidyo Pod Appendix*

The words `No Adobe Connect Server configured. Would you like to configure now?` Appear.

3. Type Y.

The words `Enter Adobe Connect Server URL` appear,

4. Enter the Adobe Connect server's a URL.

```
No Adobe Connect Server configured. Would you like to configure now? [y/n]
y
Enter Adobe Connect Server URL (e.g. adobeconnect.vidyo.com)
adobeconnect.vidyo.com
```

INSTALLING THE VIDYO POD

You (the Adobe Connect Administrator) can upload The Vidyo Pod to the Content › Shared Content section. This way all users with the appropriate permission can use the Vidyo Pod and don't have to upload it individually.

ADOBE CONNECT

Home | Content | Training | Meetings | Event Management | Reports | Administration

Shared Content | User Content | My Content | Forced Recordings | Content Dashboard

📁 Shared Content
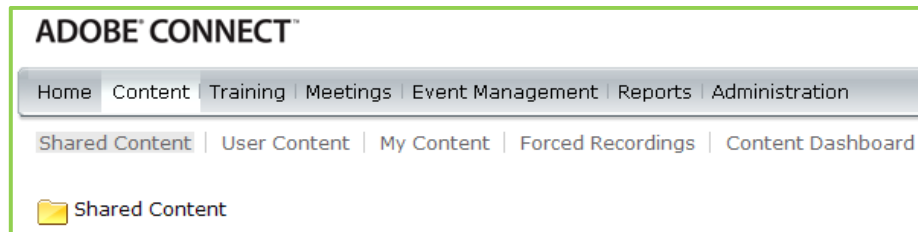
Alternatively an Adobe Connect meeting host can upload the Vidyo Pod in the content area of Adobe Connect using the following steps.

1. Log in to your Adobe Connect account.

2. Click Content on the main menu.

206
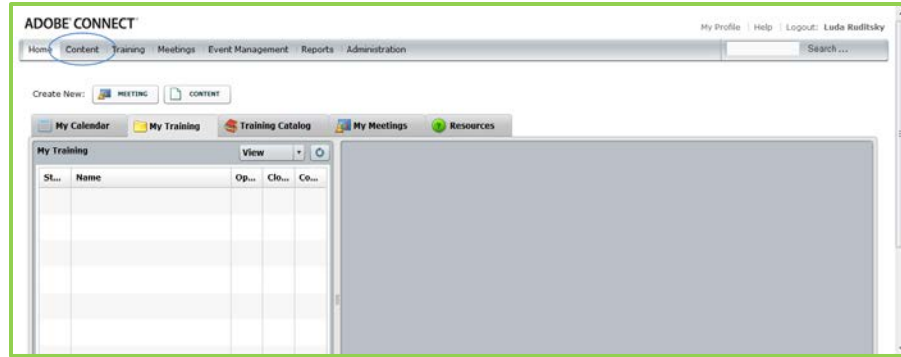
The Content sub-menu opens.
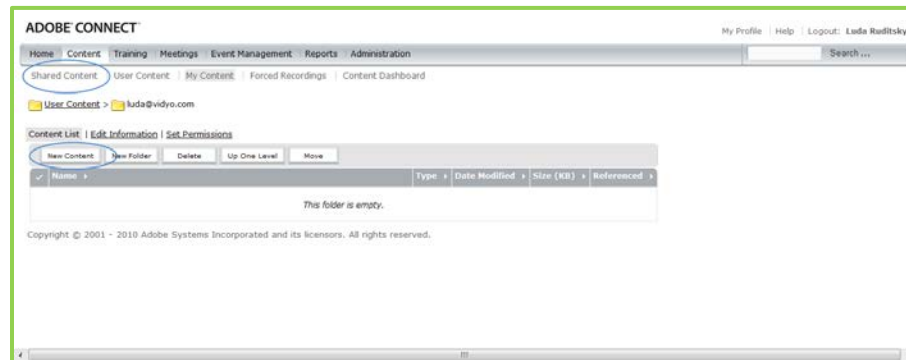
3. On the Content sub-menu click Shared Content.

4. Click on the New Content button.

    The screen changes.
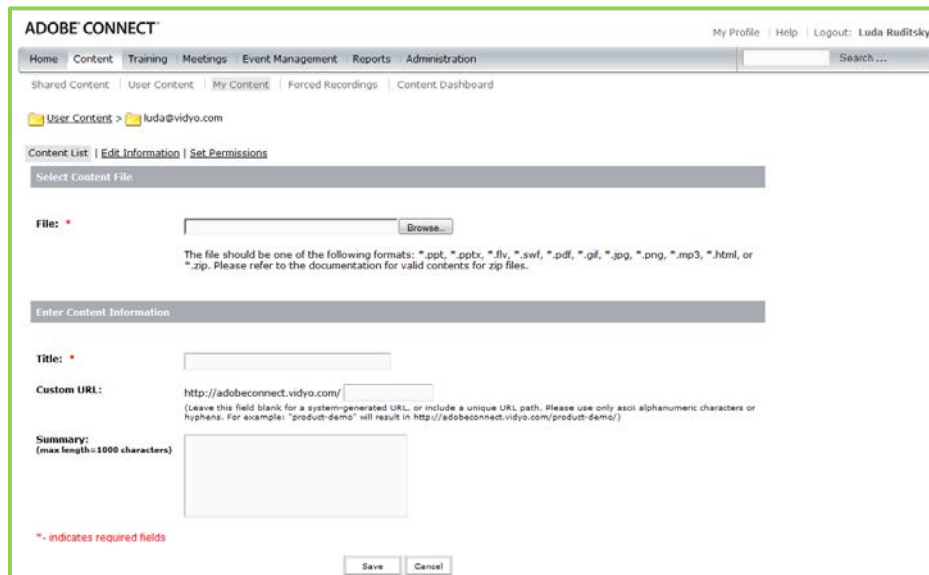
5. In the Select Content File section, click the Browse button.

    A dialog box opens.

6. In the dialog box select the Vidyo Pod located on your local computer or network and click OK.

7. In the Title field enter a title for this pod.

    For example, "Vidyo Pod Attendee List."

8. Optionally, you can provide a Custom URL for the Vidyo Pod.

    As the onscreen explanation states if you don't the system will generate a random name. You can give it a more meaningful name but it can contain only letters, numbers and hyphens.

9. Optionally, you can provide a brief summary related to the Vidyo Pod for future reference.

10. Click the Save button.

HOW TO LAUNCH THE VIDYO POD

1. Log in to your Adobe Connect server
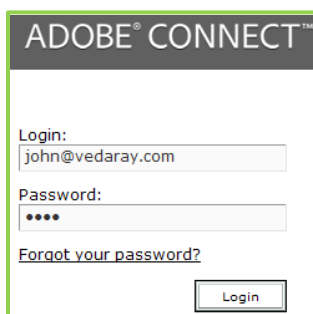
2. Start your meeting as you normally do.

    You'll see your Adobe Connect Meeting Room.

3. Click the Share My Screen drop down menu in the center of the screen.

The Select Document dialog box opens.

4. Click on Shared Content to select your Vidyo Pod.
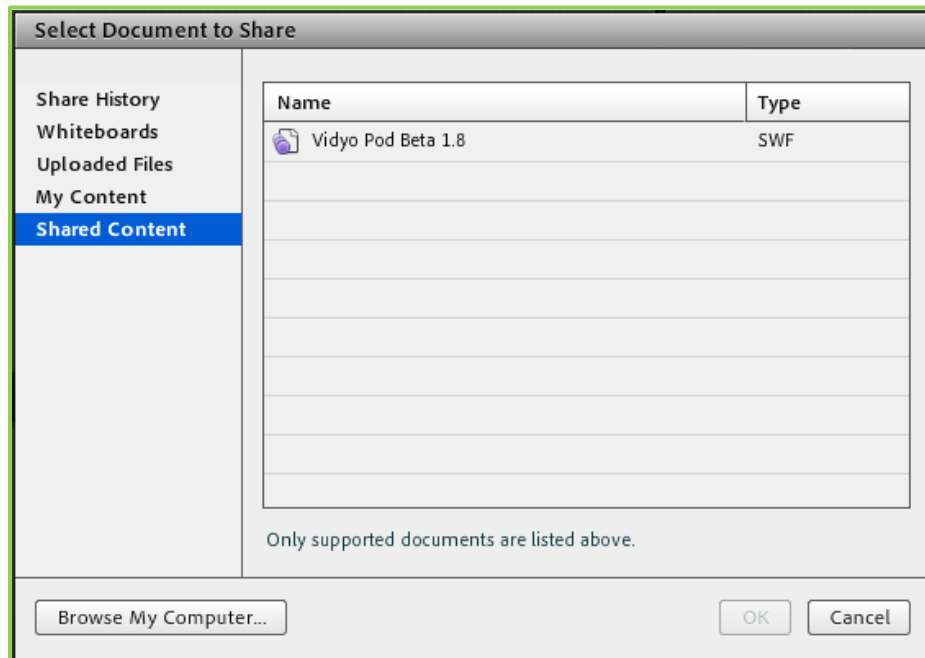
5. Click on the Vidyo Pod.

6. Click on the OK button.

31. Adobe Connect Vidyo Pod Appendix
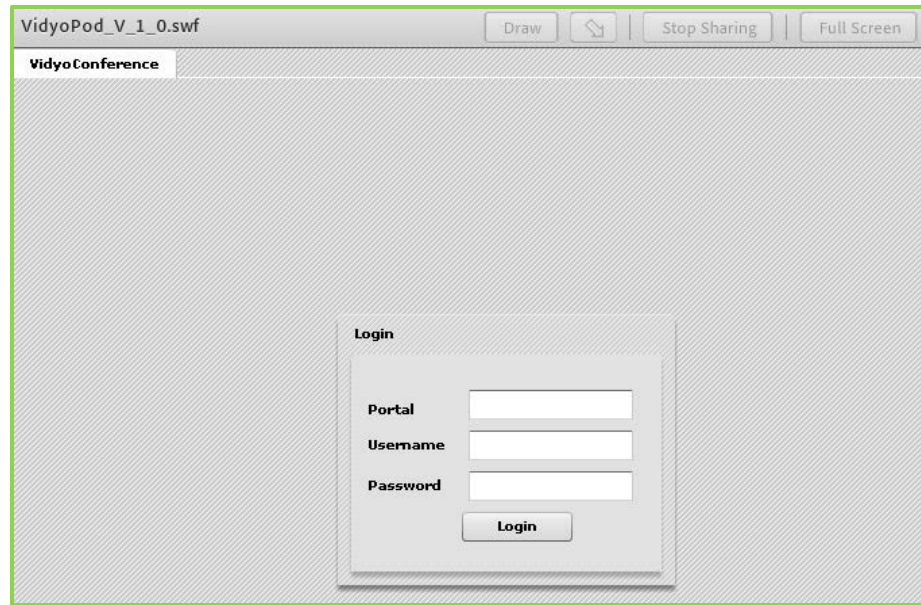
You're now ready to use the Vidyo Pod in your Adobe Connect Meeting.

Using the Vidyo Pod in Your Adobe Connect Meeting

When you start your Vidyo Pod the Vidyo Login Screen opens.

1. Log in to your VidyoPortal using your Vidyo credentials.
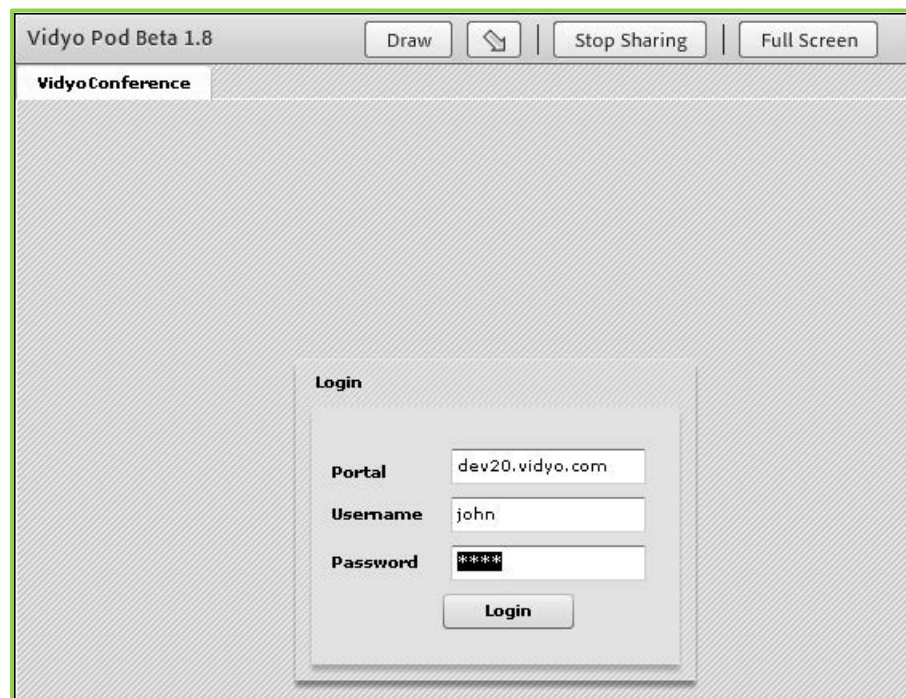
Your Meeting Room opens.
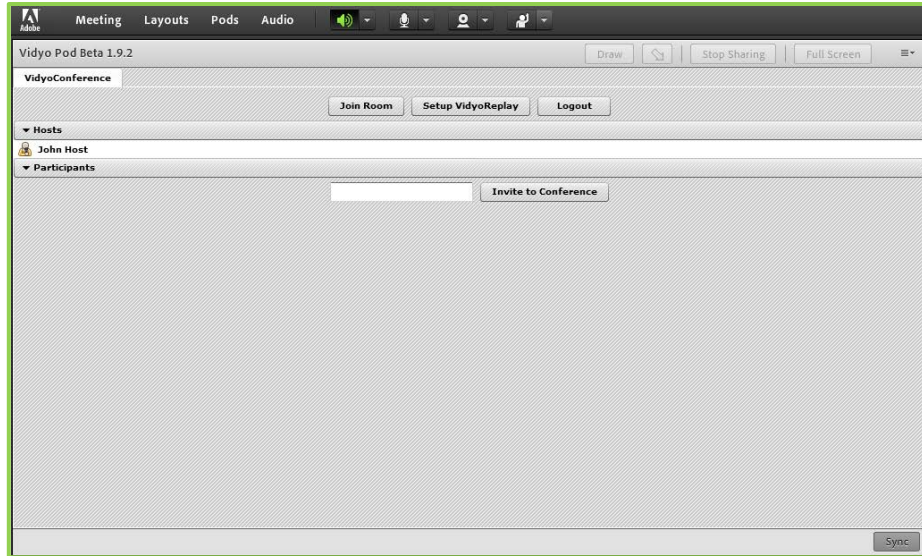
As additional participants enter your meeting, their names are displayed under Participants.
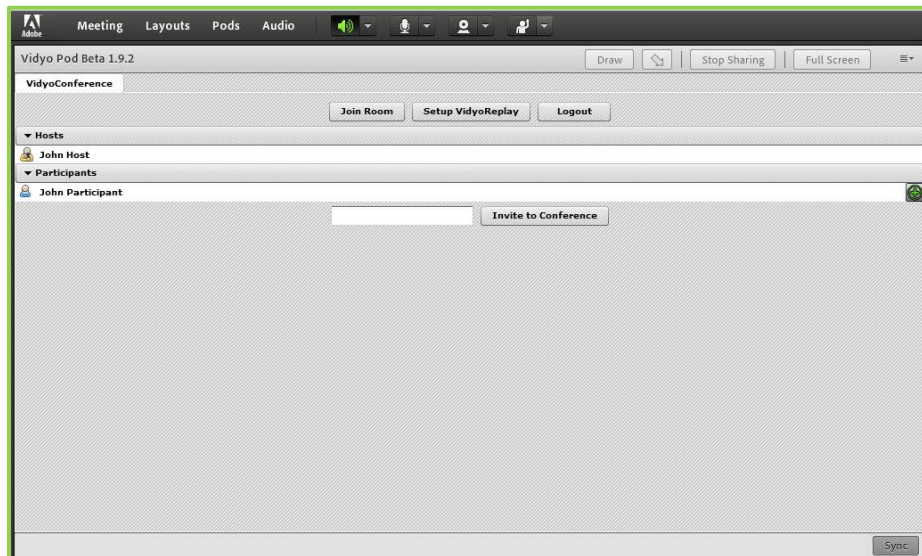
2. Click Join Room to start up a Vidyo session,

31. *Adobe Connect Vidyo Pod Appendix*
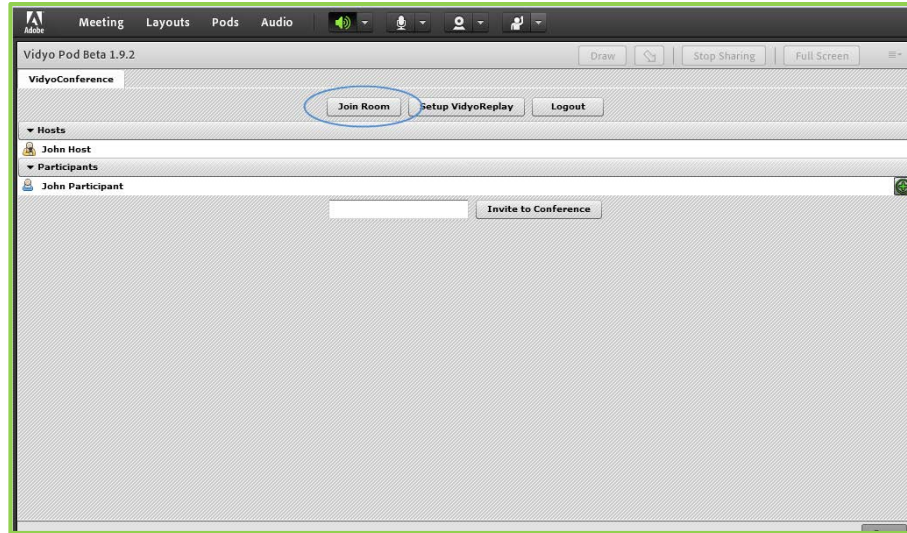
Your VidyoConference starts.
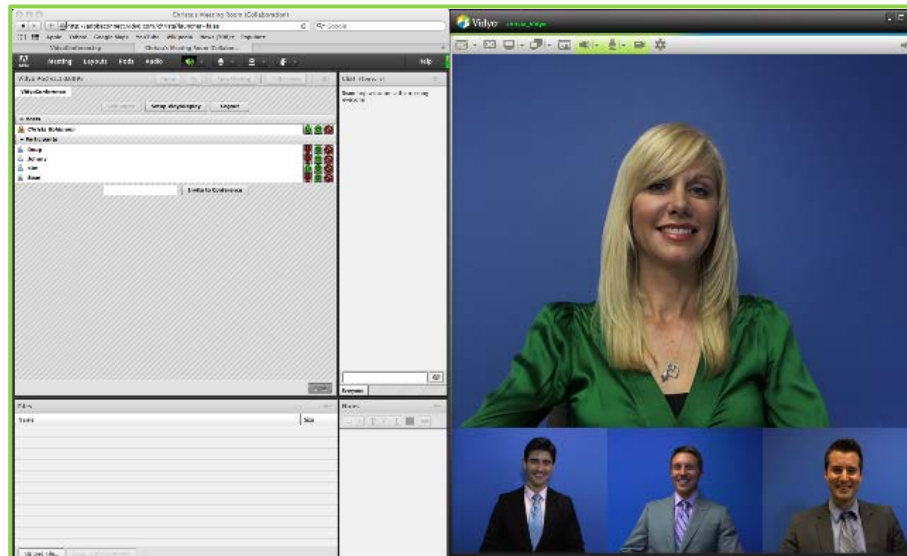
Once you join a VidyoConference you can control the session and toggle the audio and video for yourself as well as the participants using these buttons in your Vidyo Pod. For example clicking on the Vidyo Pod microphone icon will mute your microphone and the icon in the VidyoDesktop will show that your mic is muted.
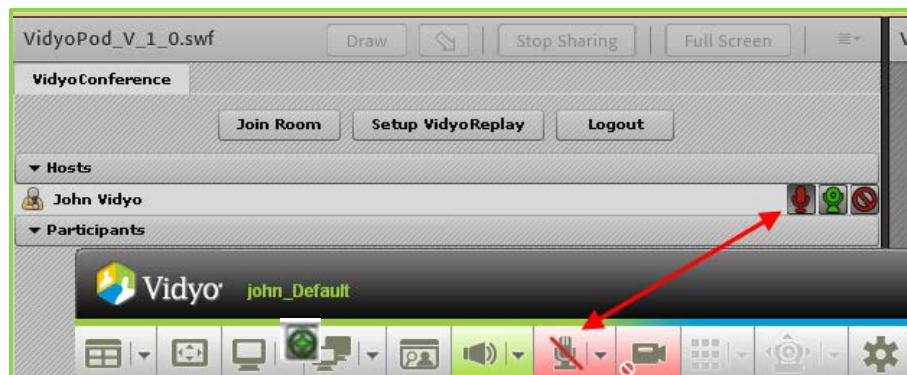
As the host, you can click on the button to the left of a participant's name to include the participant in the VidyoConference (provided he or she has VidyoDesktop installed)

As the host, you will be able to control the participants' VidyoDesktops using the appropriate buttons on the right edge of the row that contains their names.

Toggling off the video for a participant will cause the button for the participant to turn red causing the video feed to shut off.
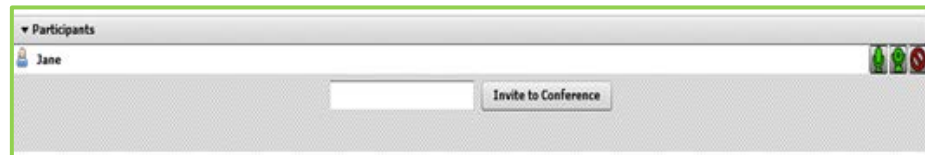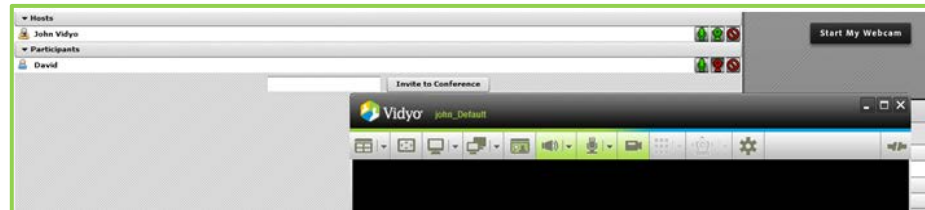
The audio toggle works the same way, as shown in the screenshot below.
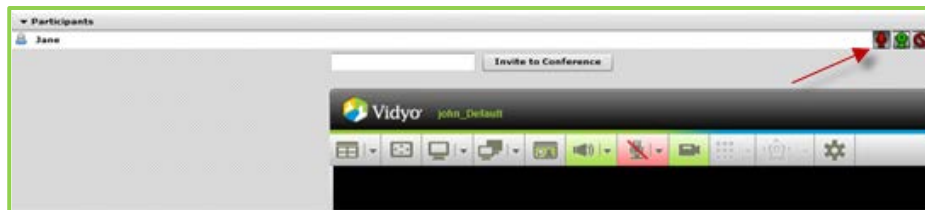
VidyoReplay supports near live video streams of Vidyo meetings in Flash format. The Vidyo Pod receives and displays it within the Vidyo Pod.

3. To configure VidyoReplay click the Setup VidyoReplay button.

The VidyoReplay dialog box appears.
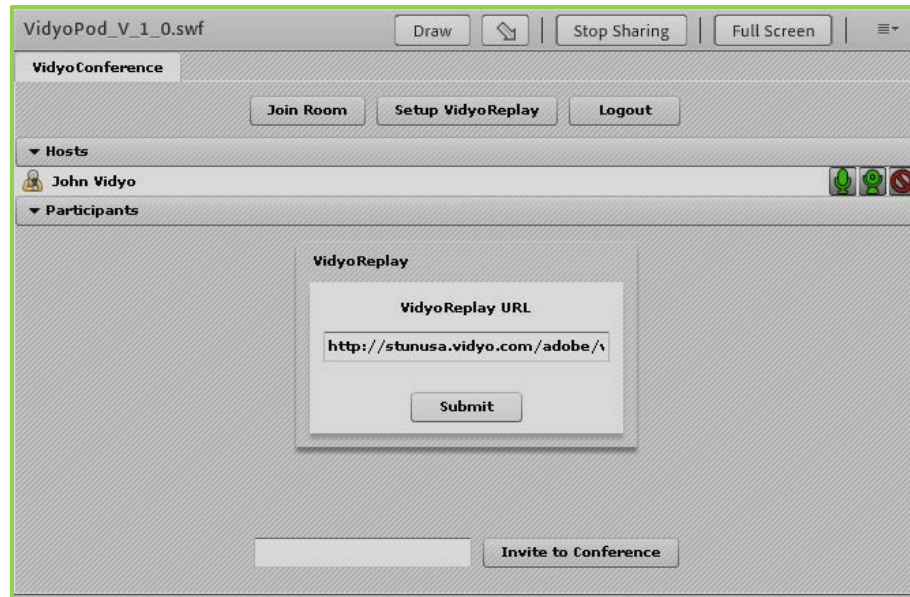
4. Enter the URL for your VidyoReplay.

    If you don't know what it is ask your system administrator or Help desk.

5. Click on the Submit button

    A new tab opens. It shows the streamed video that all the participants in the meeting can watch.
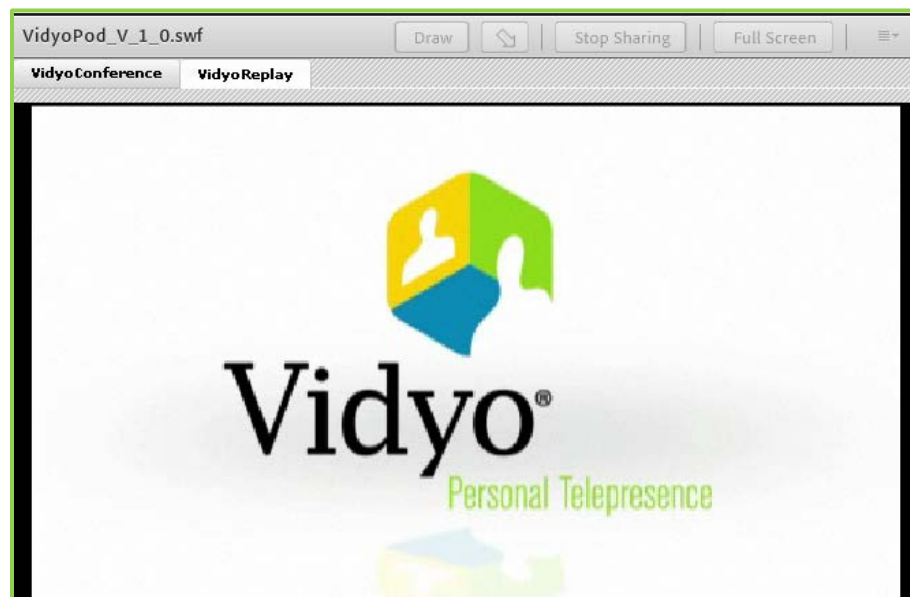
6. Use the ⊘ button to terminate the video session.

    As the host, clicking the ⊘ button will end the video conferencing session. Participants see the Call Disconnected dialog box.
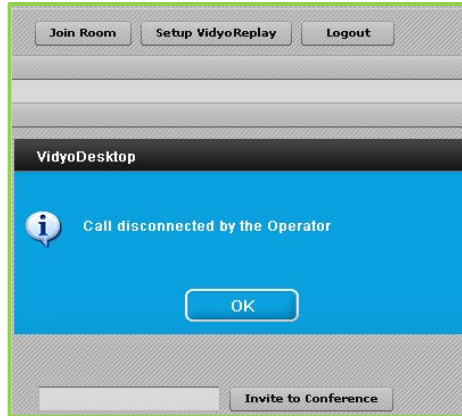
7. Click the Logout button to end your Vidyo Pod session.
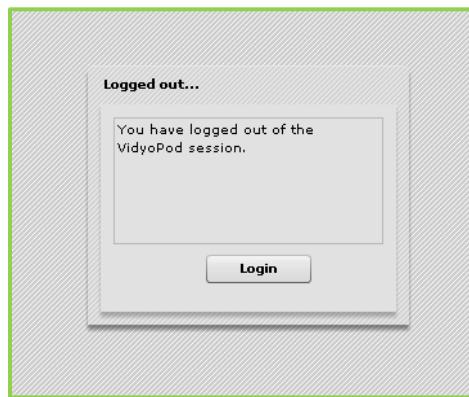
USING THE VIDYO POD AS A PARTICIPANT

When you enter a host's meeting room as a participant, the Vidyo Pod checks to see whether VidyoDesktop is installed on your computer. If the VidyoDesktop is not installed then you'll be prompted to install the VidyoDesktop. *(See the VidyoDesktop documentation for further information on installing the VidyoDesktop.)*
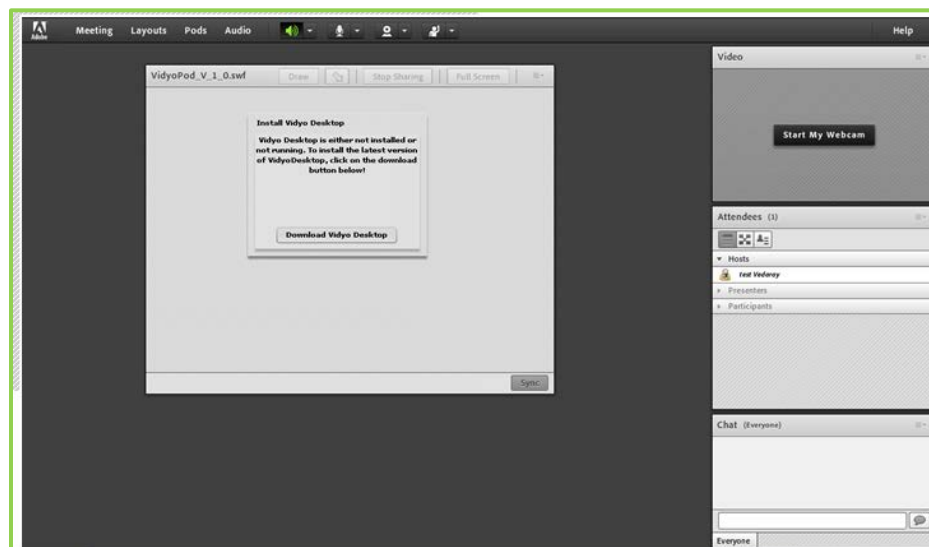
31.   Adobe Connect Vidyo Pod Appendix

When the VidyoDesktop is installed the Connecting box appears if the host has not yet started the Vidyo session

When the VidyoDesktop is started and you have joined the host's Vidyo session, the buttons will appear next to your name under the Participant section in the Vidyo pod. When the audio and video buttons are enabled, the buttons are green. Should the host decide to toggle off your video or audio, the buttons will turn red.

For example, if the host decides to toggle your video off, the icon next to your name will be red and then this will be reflected in the Vidyo Pod.
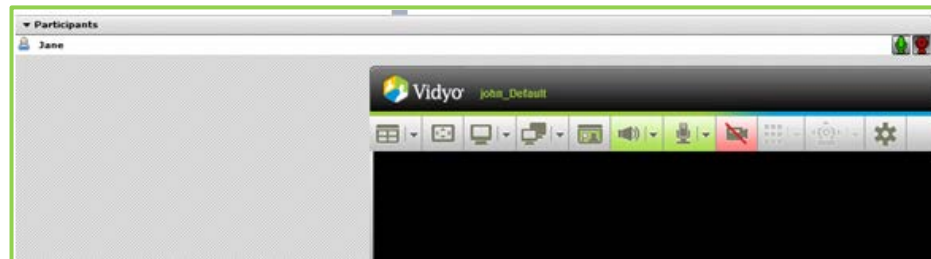
When the host disconnects the Vidyo session the Call Disconnected dialog box opens.
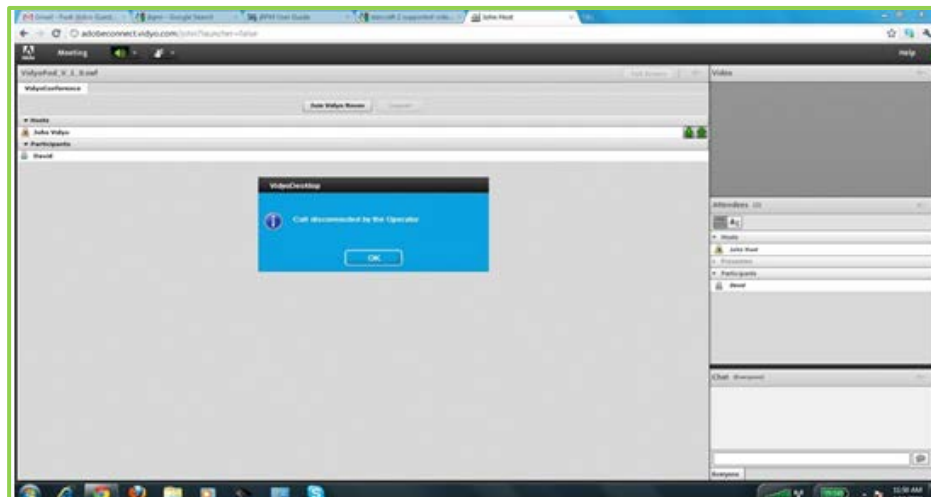
APACHE LICENSE

Version 2.0, January 2004.

http://www.apache.org/licenses/

Terms And Conditions For Use, Reproduction, And Distribution

    1.   **Definitions.**

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. **Grant of Copyright License.** Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sub-license, and distribute the Work and such Derivative Works in Source or Object form.

3. **Grant of Patent License.** Subject to the terms and conditions of this License, each Contributor here-by grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute pa-tent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent in-fringement, then any patent licenses granted to You under this License

4. **Redistribution.** You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

    1. You must give any other recipients of the Work or Derivative Works a copy of this License; and

    2. You must cause any modified files to carry prominent notices stating that You changed the files; and

    3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, pa-tent, trademark, and attribution notices from the Source form of the Work, excluding those no-tices that do not pertain to any part of the Derivative Works; and

    4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained with-in such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise com-plies with the conditions stated in this License.

Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submit-ted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License,

without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

5. **Submission of Contributions.** Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. **Trademarks.** This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. **Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. **Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

THE PHP LICENSE, VERSION 3.01

Copyright © 1999–2010 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from http://www.php.net/software/".

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see http://www.php.net.

PHP includes the Zend Engine, freely available at ‹http://www.zend.com.›

CURL LICENSE

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1996–2010, Daniel Stenberg, daniel@haxx.se.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

OPEN SSL LICENSE

Copyright © 1998–2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS

221

BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

ORIGINAL SSLEAY LICENSE

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIA-

BILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

X11 LICENSE

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

NSIS LICENSE

Copyright © 1995–2009 Contributors

Applicable licenses

- All NSIS source code, plug-ins, documentation, examples, header files and graphics, with the exception of the compression modules and where otherwise noted, are licensed under the zlib/libpng license.

- The zlib compression module for NSIS is licensed under the zlib/libpng license.

- The bzip2 compression module for NSIS is licensed under the bzip2 license.

- The lzma compression module for NSIS is licensed under the Common Public License version 1.0.

zlib/libpng license

This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

bzip2 license

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.

jseward@acm.org

COMMON PUBLIC LICENSE VERSION 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. Definitions

"Contribution" means:

a. in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and b. in the case of each subsequent Contributor:

> i. changes to the Program, and

> ii. additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. Grant Of Rights

a. Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b. Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c. Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d. Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. Requirements

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a. it complies with the terms and conditions of this Agreement; and

b. its license agreement:

   i. effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

   ii. effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii. states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv. states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a. it must be made available under this Agreement; and

b. a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. Commercial Distribution

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. No Warranty

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. Disclaimer Of Liability

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

6. General

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

Special exception for LZMA compression module

Igor Pavlov and Amir Szekely, the authors of the LZMA compression module for NSIS, expressly permit you to statically or dynamically link your code (or bind by name) to the files from the LZMA compression module for NSIS without subjecting your linked code to the terms of the Common Public license version 1.0. Any modifications or additions to files from the LZMA compression module for NSIS, however, are subject to the terms of the Common Public License version 1.0.

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. (http://fsf.org/) Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. **Additional Definitions.**

   As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

   "The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

   An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

   A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

   The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

   The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. **Exception to Section 3 of the GNU GPL.**

   You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. **Conveying Modified Versions.**

   If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

   a. under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

   b. under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. **Object Code Incorporating Material from Library Header Files.**

   The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

   a. Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

   b. Accompany the object code with a copy of the GNU GPL and this license document.

4. **Combined Works.**

   You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

   a. Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

   b. Accompany the Combined Work with a copy of the GNU GPL and this license document.

   c. For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

   d. Do one of the following:

      i. Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

      ii Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

   e. Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to

install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. **Combined Libraries.**

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b. Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. **Revised Versions of the GNU Lesser General Public License.**

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007Copyright © 2007 Free Software Foundation, Inc. (http://fsf.org/)

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. **Definitions.**

    "This License" refers to version 3 of the GNU General Public License.

    "Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

    "The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. **Source Code.**

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. **Basic Permissions.**

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. **Protecting Users' Legal Rights From Anti-Circumvention Law.**

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. **Conveying Verbatim Copies.**

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. **Conveying Modified Source Versions.**

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a. The work must carry prominent notices stating that you modified it, and giving a relevant date.

b. The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c. You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d. If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. **Conveying Non-Source Forms.**

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c. Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d. Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Re-

gardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e. Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. **Additional Terms.**

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under

those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a. Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b. Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c. Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d. Limiting the use for publicity purposes of names of licensors or authors of the material; or

e. Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f. Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. **Termination.**

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your li-

cense, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

9. **Acceptance Not Required for Having Copies.**

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. **Automatic Licensing of Downstream Recipients.**

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. **Patents.**

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. **No Surrender of Others' Freedom.**

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. **Use with the GNU Affero General Public License.**

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

14. **Revised Versions of this License.**

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. **Disclaimer of Warranty.**

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. **Limitation of Liability.**

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. **Interpretation of Sections 15 and 16.**

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

UBUNTU LINUX SOURCE CODE AVAILABILITY

Corresponding source code for the version of Ubuntu installed on the product is available online at http://cdimage.ubuntu.com/releases/.

A copy of the corresponding source code for the version of Ubuntu installed on the product is also retained by Vidyo and shall be made available upon requests for a price not more than Vidyo's reasonable cost of physically performing this service.

ZEND FRAMEWORK

Copyright © 2005-2008, Zend Technologies USA, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Zend Technologies USA, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

- THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Additional components used

- FreeTDS Library

- SMARTY Library

- PHPMailer Library

- Base.js library

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) VER. 1.0

- CDDL is derived from Mozilla Public License, the open source license that applies to use of Open H323. CDDL contains improvements to make it a more general license, and therefore more reusable. For example, CDDL clarifies the definition of "modifications" and simplifies notice requirements.

- You must make available any source code for COVERED SOFTWARE (i.e., the open source component) that you distribute in EXECUTABLE form by informing the recipient how it can obtain the source code in a reasonable manner through a typical medium for software exchange. (Sec. 3.1)

- "COVERED SOFTWARE" for the purpose of the CDDL means ORIGINAL SOFTWARE (source code and EXECUTABLE form—i.e., any form other than source code), MODIFICATIONS, or any combination of files including ORIGINAL SOFTWARE and files including MODIFICATIONS. (Sec. 1.3)

- You may distribute the EXECUTABLE under the terms of another license, provided it complies with the terms of the CDDL and does not alter the recipient's rights in the source code from those rights granted under the CDDL. (Sec. 3.5)

- You must include a copy of the CDDL with every copy of the source code form of the COVERED SOFTWARE you distribute. (Sec. 3.1)

- You must indemnify the upstream entities for any liability they incur because of any warranty you offer with your distribution of the COVERED SOFTWARE. (Sec. 3.4)

- If you assert a patent infringement claim (excluding declaratory judgment actions) against the individual or entity that made the ORIGINAL SOFTWARE or an individual or entity that created or contributed to a MODIFICATION, alleging that the ORIGINAL SOFTWARE or the MODIFICATION infringes a patent, the rights granted under the agreement will prospectively terminate upon 60 days notice from the individual or entity. The rights granted under the agreement will terminate automatically at the end of the 60 day notice period unless you withdraw your claim within the notice period. (Sec. 6.2)

Considerations if You Decide to Make MODIFACATIONS

- "MODIFICATIONS" for the purpose of the CDDL means the source code and EXECUTABLE for:

  - additions or deletions to an ORIGINAL SOFTWARE file that you make;

  - any new file that includes any part of the ORIGINAL SOFTWARE; or

  - any new file that you decide to contribute under the CDDL. (Sec. 1.9)

You must include a notice in each of your MODIFICATIONS that identifies you as the creator/contributor. (Sec. 3.3)

You grant a patent license to any downstream entity to any patents you have the right to license that are infringed by the making, using or selling of your MODIFICATIONS. However, no patent license is granted if the infringement is caused by:

third party modifications to your MODIFICATIONS;

combination of your MODIFICATIONS with other software and/or devices (other than the MODIFICATIONS covered under the CDDL); or

patents infringed without your MODIFICATIONS. (Sec. 2.2)

COMMON PUBLIC LICENSE (CPL) VER. 1.0

- The CPL has been superseded by the Eclipse Public License (EPL) ‹http://www.eclipse.org/legal/epl-v10.html›. However, you can continue to use the CPL for existing and new projects.

- You must make available any source code for any PROGRAM (i.e., open source component) you distribute in object code form. (Sec. 3)

- You must include a copy of the CPL with every copy of the source code form of the COVERED SOFTWARE you distribute. (Sec. 3)

- You may distribute the open source PROGRAM (i.e., in object code form) under your own license agreement provided that the agreement:

- complies with the CPL;

  - effectively disclaims all warranties on behalf of all CONTRIBUTORS (i.e., anyone that authored the original open source project or upstream distributors of it);

  - effectively excludes all liability for damages on behalf of all CONTRIBUTORS; and

  - states that the open source PROGRAM source code is available from you and informs the licensee how to obtain the source code in a reasonable manner through a typical medium for software exchange. (Sec. 3)

  - If you include the open source PROGRAM in a commercial product offering, you agree to defend and indemnify all other contributors against third party claims caused by your acts or omissions in the commercial product offering, other than intellectual property infringement. (Sec. 4)

  - If you institute patent litigation (including cross-claims or counterclaims in an ongoing lawsuit) against any individual or entity that distributes the open source PROGRAM with respect to a patent applicable to software, the patent licenses granted to you by that individual or entity will terminate as of the date the litigation is filed. If you institute patent litigation (including cross-claims or counterclaims in an ongoing lawsuit) against any individual or entity alleging that the open source PROGRAM infringes your patents, then all patent licenses granted to you by all upstream entities terminate. (Sec. 7)

Considerations if You Decide to Make MODIFICATIONS

- "PROGRAM" for the purpose of this license means:

  - initial code and documentation; and

  - any subsequent contributions (i.e., changes or additions) to the program, provided that they are made and distributed by a subsequent entity.

- However, any separate software modules distributed in conjunction with the PROGRAM under their own license agreement which are not derivative works of the PROGRAM are not "contributions," are not covered by the CPL, and need not be made available to others. (Sec. 1)

- You must identify yourself as the originator of your changes/additions to the PROGRAM in a manner that reasonably allows subsequent recipients to identify you as the originator of your changes/additions. (Sec. 3)

- You grant a copyright license to any downstream entity to your contributions to the PROGRAM, in source code and/or object code form. (Sec. 2)

- You grant a patent license to any downstream entity to any patent you have the right to license that are necessarily infringed by the use or sale of your contribution alone or when combined with the PROGRAM, in source code and/or object code form. The patent license applies to the combination of your contribution and the PROGRAM if, at the time you made your contribution, the addition of the contribution caused the combination to be covered by any patent you have the right to license. However, you have no liability to the downstream entity for third party claims of intellectual property infringement. (Sec. 2)

BINARY CODE LICENSE (BCL) AGREEMENT FOR THE JAVA SE RUNTIME ENVIRONMENT (JRE) VER. 6 AND JAVAFX RUNTIME VER. 1

You may reproduce and use internally the SOFTWARE (JRE Ver. 6 and JavaFX Runtime Ver. 1 in binary form, any other machine readable materials—e.g., libraries, source files—and documentation), complete and unmodified, for the sole purpose of designing, developing, testing and running your PROGRAMS (i.e., Java technology applets and applications and JavaFX technology applications).

However, you may not modify, decompile or reverse engineer the SOFTWARE. (Sec. 2-3)

- You may reproduce and distribute JRE Ver. 6 (but not JavaFX Runtime), provided that:

  - you distribute JRE v.6 complete and unmodified, and it is only bundled for the sole purpose of running your PROGRAMS;

  - the PROGRAMS add significant and primary functionality to JRE v.6 (i.e., they perform some task of function not performed by JRE v.6 acting alone);

  - you do not distribute additional software intended to replace components of JRE v.6;

  - you do not alter any proprietary legends/notices in JRE v.6;

  - you distribute the software subject to a license agreement that protects Sun Microsystems, Inc.'s interests consistent with the terms of the BCL; and

  - you agree to defend and indemnify Sun and its licensors for any damages or expenses in connection with any third party claim arising from your use or distribution of your PROGRAMS or JRE v.6. (Suppl. Lic. Terms, Sec. A)

The agreement may terminate if an IP claim is made against JRE v.6 (e.g., by you). (Suppl. Lic. Terms, Sec. F)

TERABYTE INC. END USER LICENSE AGREEMENT
License Agreement For Recovery Media Users

TeraByte, Inc. (TeraByte) grants to you (either an individual or an entity) (End User), and End User accepts, a license to use TBRS, and the Recovery Media containing one or more copies of TBRS, subject to the terms and conditions contained in this Agreement.

1   DEFINITIONS

1.1   "TBRS" means the collection of TeraByte programs included on the Recovery Media to restore disk partition and other information.

1.2   "Vendor" means the person or company from whom End User purchased computer software, equipment or other electronic equipment or devices ("System"), and who supplied End User with the "Recovery Media" with which this License Agreement is included.

1.3   "Recovery Media" means the CD or DVD disc or other computer memory medium, which: (a) was supplied by the Vendor to End User, together with computer software, a computer system or a computerized device supplied by Vendor, for the purpose of enabling the End User to restore one or more original disk configurations for that equipment or device, (b) con

2   LICENSE GRANT

2.1   End User is granted a nontransferable, nonexclusive right to use TBRS, as included on the Recovery Media and in the form distributed by the Vendor, for the sole purpose of restoring disk partition information and other information for the particular system or device with which the Recovery Media was provided to you by the Vendor. End User may make one backup copy of TBRS as included on the Recovery Media, provided that End User may not copy TBRS separately, but only as part of making a copy of the entire Recovery Media.

2.2   End User shall not use or copy TBRS except as provided in this License Agreement. End User shall not rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer TBRS, except that End User may transfer the Recovery Media containing TBRS to the recipient of the specific system or device associated with the Recovery Media, as part of any transaction of transferring such equipment or device to such recipient. Provided however that End User may only rent, lease or sell the System with the TBRS that was supplied with it with the express written consent of Vendor. Any acts or omissions violating any provision of this section 2.2 shall result in immediate and automatic termination of this License Agreement.

2.3   All rights not expressly granted herein are entirely reserved exclusively to TeraByte.

3   TERM AND TERMINATION

3.1   This License Agreement is effective until terminated. End User may terminate it at any time by destroying all copies of TBRS and notifying the Vendor or TeraByte in writing. This License Agreement will also terminate as otherwise provided in this License Agreement. On termination, End User shall return all copies of TBRS not destroyed to TeraByte, together with a written verification that the remaining materials have been destroyed.

4   PROPERTY RIGHTS AND CONFIDENTIALITY.

4.1 Recovery Media contains a copy of TBRS. TBRS is entirely owned by TeraByte, including but not limited to all copyrights and trade secret rights. End User may not reverse engineer, inspect, alter or modify in any manner TBRS or any associated proprietary notices and identifying information, and End User must use reasonable measures to prevent anyone else from doing so, including but not limited to all recipients and users of RecoveryMedia.

4.2 End User acknowledges that the source code and source code documentation for TBRS, and all other internal technical information and data regarding TBRS, comprise valuable trade secret information exclusively owned by TeraByte or licensed to TeraByte ("Confidential Information"), and that TeraByte does not provide End User with any access to, or right to gain access to, any of the Confidential Information. End User shall not seek to unlock, disassemble, or reverse engineer all or any part of TBRS, nor otherwise seek to gain, or assist others in gaining, access to Confidential Information. "Confidential Information" shall not include information which otherwise would be Confidential Information, to the extent that such information: (A) was publicly known or otherwise known to End User at the time of disclosure, or (B) became known to End User subsequent to disclosure in a manner involving no connection to any activities in violation of any person's or entity's confidentiality obligations to TeraByte. End User acknowledges that TeraByte will suffer irreparable harm, and will not have an adequate remedy in money or damages in the event End User, or any individual or company gaining or attempting to gain access to the Confidential Information by or through End User, breaches any of the foregoing provisions. TeraByte shall therefore be entitled to obtain an injunction against such breach or continued breach from any court of competent jurisdiction authorized hereunder immediately upon TeraByte's request, and without requirement of posting a bond. TeraByte's right to obtain injunctive relief shall not limit its rights to seek all other available remedies at law and equity.

5 WARRANTY DISCLAIMER

5.1 TBRS IS PROVIDED BY TERABYTE "AS IS." TERABYTE MAKES AND END USER RECEIVES NO WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6 LIMITATION OF LIABILITY

6.1 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER TERABYTE NOR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THIS SOFTWARE SHALL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH SOFTWARE, EVEN IF TERABYTE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR CLAIMS.

7 U.S. GOVERNMENT RESTRICTED RIGHTS

7.1 If the Software is licensed to a U.S. Governmental user, the following shall apply:

The Software and documentation licensed in this License Agreement are "commercial items" and are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with the Federal Acquisition Guidelines and related laws, any use, modification, reproduction, release, display, or disclosure of such commercial software or commercial software documentation by the US. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

245

8   TERMINATION. THIS LICENSE MAY BE TERMINATED BY TERABYTE IF:

8.1   End User fails to comply with any material term or condition of this License Agreement and End User fails to cure such failure within fifteen days after notices of such failure by TeraByte; or

8.2   End User's normal business operations are disrupted or discontinued for more than thirty days by reason of insolvency, bankruptcy, receivership, or business termination.

9   HIGH RISK ACTIVITIES.

9.1   Neither TBRS nor the Recovery Media, are fault-tolerant, and they are not designed, manufactured or intended for use on equipment or software running in hazardous environments requiring fail-safe performance, including but not limited to the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of TBRS or Recovery Media could contribute to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). TERABYTE AND ITS SUPPLIERS SPECIFICALLY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY RELATING IN ANY MANNER TO USE OF TBRS OR RECOVERY MEDIA FOR HIGH RISK ACTIVITIES. TERABYTE DOES NOT AUTHORIZE OR LICENSE USE OF TBRS OR RECOVERY MEDIA FOR ANY HIGH RISK ACTIVITY. END USER AGREES TO DEFEND AND INDEMNIFY TERABYTE, AND HOLD TERABYTE HARMLESS, FROM AND AGAINST ANY AND ALL CLAIMS, ACTIONS, LOSSES, COSTS JUDGMENTS AND DAMAGES OF ANY KIND IN CONNECTION WITH USE IN RELATION TO ANY HIGH RISK ACTIVITY OF ANY COPY OF TBRS OR ANY RECOVERY MEDIA.

10   GENERAL TERMS

10.1   Neither this License Agreement nor any rights or obligations hereunder shall be assigned or otherwise transferred by End User without prior written consent of TeraByte, except that this License Agreement shall be automatically assigned as a whole (and End User must not retain any copies of TBRS) upon any transfer by End User of the Recovery Media. TeraByte may assign this License Agreement entirely in its sole discretion without requirement of notice or consent.

10.2   This License Agreement shall be interpreted and enforced in accordance with and shall be governed by the laws of the State of Nevada, without regard to Nevada's choice-of-law rules. Any action or proceeding brought by either party against the other arising out of or related to this License Agreement shall be brought only in a or FEDERAL COURT of competent jurisdiction located in Clark County, NV (or, where there is no forum within Clark County with jurisdiction over the subject matter, the forum with such jurisdiction closest to Clark County within the U.S.A.). The parties hereby consent to in personam jurisdiction of said courts.

10.3   If any terms or provisions of this License Agreement shall be found to be illegal or unenforceable then, notwithstanding, this License Agreement shall remain in full force and effect and such term or provision shall be deemed stricken.

10.4   No amendment of this License Agreement shall be effective unless it is in writing and signed by duly authorized representatives of both parties. No term or provision hereof shall be deemed waived and no breach excused unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to or waiver of a breach by the other, whether express or implied, shall not constitute a consent to, waiver of or excuse for any other, different or subsequent breach.

10.5   This License Agreement shall be binding on and shall inure to the benefit of the heirs, executors, administrators, successors and assigns of the parties hereto, but nothing in this paragraph shall be construed as a consent to any assignment of this License Agreement by either party except as provided hereinabove.

10.6   End User acknowledges that End User has read this Agreement, understands it, and agrees to be bound by its terms. The End User further agree that this Agreement is the complete and exclusive statement of agreement between End User and TeraByte in regard to the subject matter herein, and supersedes all proposals, oral or written, understandings, representations, conditions, warranties, covenants, purchase orders and all other communications between End User and TeraByte relating to this Agreement. No additional terms, be they consistent or inconsistent with those contained in this Agreement, shall be binding on either party absent their mutual and prior specific written consent.

10.7   All provisions of this Agreement relating to post-termination actions, confidentiality, reverse engineering, and ownership shall survive any termination or expiration of this Agreement.

10.8   End User shall be solely responsible to insure that all software and other products shipped for export by End User in connection with this Agreement comply with all applicable export requirements of the U.S. and other governments.

10.9   There are no third party beneficiaries of any of the rights, obligations or representations in this Agreement.