



VidyoConferencing™ Administrator Guide

for Super and Tenant Administrators



System Version 3.2

Document Version A

TABLE OF CONTENTS

1. About This Guide.....	11
Understanding the Different System Accounts.....	11
The System in Brief.....	11
Conventions Used in This Guide.....	12
2. Definitions	13
Terms Used in This Guide.....	13
Vidyo Concepts and Equipment	13
Users	15
Tenants	16
Meeting	17
Meeting Rooms	17
Groups	17
VidyoLines.....	18
Install	18
Endpoint	18
3. Upgrading Your VidyoConferencing System	20
4. Configuring Your Vidyo Server	22
Logging in to the System Console of Your Vidyo Server and Changing the Default Password	23
Configuring the Network Settings at the System Console	25
Changing the Remaining Default Passwords	28
Supporting Multiple System Console Accounts	29
Understanding System Administrator Console Menu Options	31
Understanding the More Options System Administrator Console Menu	33
Managing Network Routes.....	35
Adding a Network Route	36
Removing a Network Route.....	37
Removing all of Your Network Routes.....	38
Navigating Your Network Routes	38
Configuring SNMP	39
Enabling SNMP	39
Configuring an SNMPv2 Community String	40
Configuring Local SNMPv3 User (User-based Security Model).....	41
Configuring an SNMP Notification.....	43
Managing Hostnames.....	46
Adding a Hostname	47
Removing a Hostname.....	48
Removing all of Your Hostnames.....	49
Navigating Your Hostnames	49
Logging in to the Super Admin Portal.....	50

TABLE OF CONTENTS

Checking the Status of the Components	50
Requesting System Licenses and Applying System License Keys	51
Requesting Your Vidyo Licenses	51
Applying the System License Keys to Your System.....	52
Setting the Language for the Super Admin Interface	53
Setting Your Preferred Language Using the Upper-Right Drop-Down Outside the System	54
Setting Your Preferred Language from Settings > Super Account Inside the System.....	54
Adding Multiple Super Admin Accounts	55
5. Enabling the Management Interface	57
Moving VidyoPortal Applications to the Management Interface	58
The Management Interface on VidyoRouter and VidyoGateway	59
Moving Your VidyoRouter Applications to the Management Interface	59
Moving Your VidyoGateway Application to the Management Interface	60
Adding Static Network Routes.....	61
6. Configuring System Settings as the Super Admin	63
Checking Your Platform Network Settings	63
Applying System License Keys to Your System.....	64
Applying System License Keys to Your System Using the Hot Standby Software Option.....	67
Understanding Vidyo License Consumption by User Type	68
Understanding Licensing Notifications	68
Uploading Endpoint Software	68
Activating an Endpoint Installation File	71
Deleting an Endpoint Installation File.....	72
Performing System Maintenance.....	72
Backing Up the Database	73
Downloading a Backup File.....	74
Uploading a Backup File.....	75
Restoring a Backup File Located on Your VidyoPortal.....	76
Restoring a Backup File No Longer on Your VidyoPortal	77
Deleting a Backup File That's on the VidyoPortal.....	77
Restoring The Database to the Factory Default	78
Upgrading Your VidyoPortal System Software	78
Downloading Your VidyoPortal Installation Logs History	80
Viewing Your VidyoPortal Installed Patches.....	80
Restarting Your System.....	81
Configuring the CDR Database for Remote Access in the Super Admin Portal	82
Exporting and Purging CDR Files from the Super Admin Portal	83
Downloading Audit Logs	84
Configuring Status Notify.....	85
Enabling Syslog	85
Managing Your Super Accounts	86
Viewing Your Super Accounts.....	86

TABLE OF CONTENTS

Editing Super Account Information and Changing the Password.....	87
Customizing the System	88
Customizing the About Info.....	88
Reverting To Default System Text on The About Info Screen.....	89
Customizing Support Info	90
Reverting To Default System Text on The Support Info Screen.....	91
Customizing Notification Information	92
Customizing the Invite Text	93
Reverting To Default System Text on The Invite Text Screen.....	96
Uploading Custom Logos	96
Changing Where the System Looks for PDF Versions of the Administrator and User Guides.....	98
Customizing Your VidyoPortal Login and Welcome Banners	99
Customizing Your Password Settings.....	103
Reverting To Default Password Settings on the Password Screen	104
Securing Your VidyoConferencing System	104
Configuring a Scheduled Room Prefix	104
Setting Global Features	105
Enabling VidyoWeb Access.....	105
Enabling VidyoMobile Access	106
Configuring System-Wide Search Options.....	108
Configuring System-Wide Inter-Portal Communication (IPC).....	108
7. Configuring Your Components as the Super Admin.....	113
Using the Components Table	113
Configuring Your VidyoManager Component	115
Entering General VidyoManager Information	115
Enabling VidyoManager Security.....	116
Entering VidyoManager Advanced Information	117
Accessing Your VidyoManager Configuration Page	119
Configuring Basic Settings on Your VidyoManager	120
Viewing System Settings on Your VidyoManager.....	121
Downloading Logs from Your VidyoManager	122
Logging Out of VidyoManager	123
Configuring Your VidyoRouter Component.....	124
Configuring VidyoRouter General Settings.....	124
Configuring VidyoManager Settings from the VidyoRouter	125
Configuring VidyoRouter NAT Firewall Settings	126
Enabling VidyoRouter Security	127
Configuring VidyoRouter Quality of Service (QoS)	128
Restoring VidyoRouter to Factory Default Settings.....	129
Accessing Your VidyoRouter Configuration Page	130
Configuring Basic Settings on Your VidyoRouter	130
Configuring Security on Your VidyoRouter	132
Viewing System Information on Your VidyoRouter	132

TABLE OF CONTENTS

Downloading Logs from Your VidyoRouter	134
Upgrading Your VidyoRouter	134
Restarting Your VidyoRouter	137
Logging Out of Your VidyoRouter	137
Configuring VidyoRouters and VidyoProxys Using Their Configuration Pages.....	138
Setting the Configuration Page Address of Your VidyoRouter	138
Setting the Configuration Page Address of Your VidyoProxy	139
Configuring a VidyoRouter using its Configuration Page.....	139
Configuring a Standalone VidyoProxy using its Configuration Page.....	141
VidyoGateway Configuration	142
Making Initial VidyoGateway Configurations on Your VidyoPortal	142
Making Initial VidyoGateway Configurations on Your VidyoGateway	143
Making Initial VidyoGateway Configurations on Your VidyoPortal (Continued)	143
Adding a VidyoGateway to Your VidyoPortal	143
VidyoReplay Recorder and VidyoReplay Configuration	145
Making Initial VidyoReplay Recorder or VidyoReplay Configurations on Your VidyoPortal.....	145
Making Initial VidyoReplay Recorder or VidyoReplay Configurations on Your VidyoReplay	145
Making Initial VidyoReplay Recorder or VidyoReplay Configurations on Your VidyoPortal (Continued).....	145
Adding a VidyoReplay Recorder to Your VidyoPortal	146
Adding a VidyoReplay to Your VidyoPortal.....	147
Configuring VidyoCloud.....	148
Enabling the VidyoCloud.....	149
Creating a VidyoRouter Pool	150
Removing a VidyoRouter from a Pool	153
Deleting an Entire VidyoRouter Pool	153
Activating the VidyoCloud Configuration	154
Creating User Location Tags	155
Creating Endpoint Rules	157
Configuring Inter-Pool Preferences	160
Configuring Inter-Portal Communication When Using VidyoCloud.....	162
8. Using the VidyoPortal and VidyoRouter Virtual Editions (VE).....	163
Understanding the VE Requirements	163
VidyoPortal Virtual Machine Provisioning Requirements	163
VidyoRouter Virtual Machine Provisioning Requirements	164
Understanding VMware Best Practices.....	164
Understanding VidyoPortal and VidyoRouter VE Support of VMware Features	164
Installing VidyoPortal VE	165
Installing VidyoRouter VE	175
9. Managing Tenants as the Super Admin	186
Using the Tenants Table	186
Understanding How to Add A Tenant	187

TABLE OF CONTENTS

Adding a Tenant	187
Adding a Default Tenant or Adding a New Tenant	187
Enabling Cross-Tenant Access	190
Making the VidyoManager Component Available.....	191
Making the VidyoProxy Components Available.....	191
Making the VidyoGateway Components Available	192
Selecting a VidyoReplay Recorder	193
Making the VidyoReplay Components Available.....	194
Assigning Location Tags	195
Enabling or Disabling VidyoMobile on Your Tenant	196
Allowing Inbound and Outbound Inter-Portal Communication	197
Adding the New Tenant to Your System.....	198
Deleting a Tenant	199
Viewing Current Calls	199
10. Managing Users as the Tenant Admin.....	201
What Tenant Admins Do	201
Logging In as a Tenant Admin.....	201
Setting the Language for the Admin Interface	202
Using the Users Table.....	203
Adding a New User	204
Editing a User	207
Deleting a User	207
Adding a Legacy Device	208
Importing Users	209
Understanding Exporting Users.....	210
Exporting Users	211
11. Managing Meeting Rooms as the Tenant Admin.....	212
Using the Manage Meeting Rooms Table	212
Adding a Meeting Room.....	213
Editing a Meeting Room.....	215
Deleting a Public Meeting Room	217
Viewing Current Calls	218
Understanding Controlling Meetings	218
Controlling a Meeting Room	219
Configuring Moderator PIN, Room Link, and Room PIN Features.....	222
Setting the Moderator PIN on Your Room	224
Moderating Another Person's Room.....	225
Moderating Rooms Using a Tablet	227
Managing Participants.....	229
12. Managing Tenant Admin Groups as the Tenant Admin	230
Using the Manage Groups Table	230

TABLE OF CONTENTS

Adding a New Group	230
Editing a Group.....	231
Deleting a Group	231
Configuring a Group for VidyoReplay Recorder and VidyoReplay Use	232
13. Configuring Settings as the Tenant Admin.....	234
Checking Your License Terms	234
Uploading Endpoint Software	234
Activating an Endpoint Installation File	237
Deleting an Endpoint Installation File.....	238
Setting the Tenant Language.....	238
Configuring Guest's Settings	239
Configuring Customization on Your Tenant	240
Customizing the About Info.....	240
Reverting To Default System Text on The About Info Screen.....	240
Customizing Support Information	241
Reverting To Default System Text on The Support Info Screen.....	242
Customizing Notification Information	242
Customizing the Invite Text	243
Reverting To Default System Text on The Invite Text Screen.....	246
Uploading Custom Logos on Your Tenant	246
Configuring Authentication	248
Configuring Authentication Using LDAP	248
Configuring Authentication Using Web Services	263
Managing Location Tags.....	265
Disabling Scheduled Rooms on Your Tenant.....	267
Exporting CDR Files from the Admin Portal.....	267
Configuring Inter-Portal Communication (IPC) on Your Tenant.....	268
Configuring Quality of Service (QoS) on Your Tenant	269
Configuring VidyoWeb on Your Tenant.....	271
14. Auditing	272
Downloading Audit Logs from Your VidyoPortal.....	272
Downloading Audit Logs from Your VidyoManager	273
Downloading Audit Logs from Your VidyoRouter	274
Downloading Audit Logs From Your VidyoGateway.....	275
Audit Log Content.....	276
Content Captured in the Audit Log.....	276
Sample Audit Log Content	278
15. Configuring OCSP	280
Enabling and Configuring OCSP	280
Enabling OCSP in the VidyoPortal and VidyoRouter and Configuring OCSP in the VidyoPortal... 280	280
Enabling OCSP in the VidyoGateway	282

TABLE OF CONTENTS

Disabling OCSP from the System Console	284
Appendix A. Firewall and Network Address Translations (NAT) Deployments.....	286
NAT Introduction.....	286
VidyoConferencing Firewall Ports	287
VidyoDesktop and VidyoRoom Requirements	287
Vidyo Server Requirements	288
Configuring VidyoConferencing With A Firewall NAT	290
Configuring the Firewall NAT.....	290
Configuring DNS and FQDN	291
Configuring the Vidyo Server.....	291
Configuring Tenant URLs	292
Configuring the VidyoManager.....	292
Configuring Each of Your VidyoRouters.....	294
Testing Your Configuration	297
Appendix B. VidyoProxy	298
VidyoProxy Solution for Traversal of Restricted Networks	298
Overcoming Deployment Barriers Securely and Effectively	298
Vidyo Solutions for Firewalled Networks	298
Key Features and Functions of Vidyo’s Proxy Solution	299
Configuring Your VidyoProxy.....	299
Appendix C. Security	300
Securing Your VidyoConferencing System with SSL and HTTPS	301
Generating or Uploading an SSL Private Key	302
Generating an SSL CSR.....	305
Certificates Received from Your Certificate Authority	308
Deploying Your Server Certificate.....	309
Deploying Your Server CA Certificates (Intermediates).....	311
Configuring HTTPS Port Settings on Your Applications.....	313
Importing Client Root CA Certificates from the Advanced Tab	313
Enabling SSL and HTTPS Only.....	315
Importing and Exporting Certificates from the Advanced Tab	317
Resetting Your Security Configuration to Factory Defaults	319
Configuring Client CA Certificates.....	320
Configuring Your Components to Work with HTTPS	321
Setting the Hostname and Domain on Your Vidyo Server.....	322
Setting the FQDN on Your VidyoManager Configuration Page	322
Setting the FQDN on Your VidyoRouter Configuration Page.....	322
Setting the FQDN on Your VidyoProxy Configuration Page.....	323
Setting the FQDN on Your Tenants.....	324
Configuring Each VidyoPortal Component to Use Your FQDN	325
Setting the FQDN in Your VidyoManager Component Configuration	325

TABLE OF CONTENTS

Setting the FQDN in Your VidyoRouter Component Configuration.....	326
Setting the FQDN in Your VidyoProxy Component Configuration.....	328
Verifying Your VidyoPortal Components are Online (Status: UP)	330
Applying VidyoPortal SSL Certificates to VidyoRooms	330
Building the VidyoPortal Full Chain SSL Certificate.....	331
Implementing Encryption Using the Secured VidyoConferencing Option	331
Verifying Your VidyoPortal is Licensed for Encryption	332
Enabling Encryption on the VidyoConferencing System	332
Testing the VidyoDesktop and Verifying Encryption	334
Appendix D. CDR	336
Understanding CDR Configuration	337
Configuring the CDR Database for Remote Access.....	338
Exporting and Purging CDR Files.....	338
CDR Version2.1 Tables.....	338
ClientInstallations2	338
ConferenceCall2.....	338
Appendix E. Hot Standby	343
Automatically and Manually Triggering Hot Standby.....	343
Configuring Your Settings in Preparation for Hot Standby.....	344
Setting IP and DNS Settings on VP1 and VP2	344
Verifying Correct Installation of VidyoPortal Licenses with the Hot Standby Option	345
Preparing the System Software and Database	346
Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.....	347
Configuring Hot Standby	350
Setting Hot Standby Configuration Values on VP1	351
Rebooting to Apply the New Hot Standby Configuration Values on VP1.....	355
Verifying VP1 Functionality.....	356
Setting Hot Standby Configuration Values on VP2	356
Generating and Importing the Security Keys.....	357
Validating the Security Keys	362
Triggering the First Database Synchronization from VP1	363
Verifying the Node Status on VP1 and VP2	364
Scheduling the Database Synchronization	365
Synchronizing VidyoPortal Database Information Automatically.....	365
Checking the Status of the Hot Standby Configuration	366
Forcing the Active VidyoPortal into Standby Mode from the Super Admin Portal	368
Importing a Security Key.....	369
Email Notifications.....	370
Upgrading Hot Standby VidyoPortals	371
Upgrading Your Hot Standby VidyoPortals while Keeping One Server Online	371
Upgrading Your Hot Standby VidyoPortals while Taking Both Servers Offline.....	373

TABLE OF CONTENTS

Appendix F. Reliability	376
Limitations of Reliability Prediction Models.....	376
General Prediction Methodology.....	376
Electronic Equipment Procedure.....	376
Component Parameters and Assumptions.....	376
Supplier MTBF Data	377
Subsystem MTBF Data Release Policy	377
MTBF Reliability.....	377
Appendix G. Licensing.....	378
Apache License.....	378
Curl License	380
Open SSL License	381
Original Ssleay License	382
X11 License.....	383
NSIS License.....	383
Common Public License version 1.0.....	384
GNU Lesser General Public License	388
GNU General Public License	390
Ubuntu Linux Source Code Availability	399
Zend Framework	400
Common Development And Distribution License (CDDL) Ver. 1.0.....	400
Common Public License (CPL) Ver. 1.0	402
Binary Code License (BCL) Agreement for the Java SE Runtime Environment (JRE) Ver. 6 and JavaFX Runtime Ver. 1	403
TeraByte Inc. End User License Agreement.....	403

1. About This Guide

Welcome to Vidyo, Inc., creators of 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.
- One of our resellers can host the system for you.
- Your organization can license a system from us or one of our resellers.

UNDERSTANDING THE DIFFERENT SYSTEM ACCOUNTS

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

This document provides information for the types of system accounts using your VidyoConferencing system:

- **The System Console Administrator** – This account configures and maintains the system and the network using the System Console and the Configuration Pages for VidyoRouter, VidyoProxy, and VidyoGateway™.
- **The Super Administrator** – Configures and maintains the entire VidyoConferencing system and the network using the Super Admin Portal.
- **The Tenant Administrator** – Configures and maintains the user settings for their own tenant or tenants in the VidyoConferencing system.
- **Tenant Operator** – Controls a subset of Tenant Administrator privileges.

In order to use the system, a VidyoPortal™ must 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, the Super Portal) to perform tasks while Tenant Admins, Operators, and Audit users access a different portal (the Admin Portal, which is a different set of web pages) to perform tasks.

The Super Admin's rights are a superset of the Tenant Admin's rights. However, when a Super Admin clicks a button or link to perform a task that an Admin can do, the Admin portal login page opens in a new tab or browser window, and the Super Admin can log in to the Admin portal using his or her Super credentials.

The Admin's rights are a superset of the Operator and Audit user type rights; however, they all log into the Admin portal. When Operators and Audit users log in to the Admin portal, the tabs for tasks they can't perform (involving Groups and Portals) are not shown.

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. This VidyoPortal allows system users to search and find other users, place calls, and gather in virtual online meeting rooms.

Users have the VidyoDesktop™ program on their Windows, Macintosh, or Linux computers that enable them to participate in VidyoConferences with just one other participant (known as a point-to-point or direct call) or with multiple participants. VidyoDesktop can display up to eight other participants, and users can also choose to view their own images using a PIP (picture-in-picture). This feature is called Self-View.

VidyoDesktop also enables users to share any window currently displayed on their screens (an Excel spreadsheet or a Keynote slide, for example). We call this application sharing.

While there are different programs for each platform, each installation of an endpoint program consumes one license. Therefore, a user who needs VidyoDesktop on a desktop and VidyoMobile™ on an iPhone would consume two licenses. However, you don't have to predetermine how many of each kind of license you're going to need in advance. There's only one kind of license and it can be used for any device. In other words, our endpoint licensing is device-agnostic.

The optional VidyoGateway server allows interoperability with Legacy conferencing systems that use multi-point control units (MCUs). VidyoGateway also allows people to call into a conference from an ordinary landline or cell phone (that doesn't have VidyoMobile installed) for voice-only participation.

CONVENTIONS USED IN THIS GUIDE

- **Tips** are occasionally provided as helpful information.
- **Notes** are provided as information pertaining to the subject deserving special attention.
- **Cautions** are provided when the information could prevent damaging equipment or result in the loss of data.
- Text you type into an on-screen 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
- In the user interface, a red star (*) denotes a field that cannot be left blank.
- Cross-references to pages are shown in **bold blue**. When viewing this PDF document on-screen, you can click on these page numbers to move to the referenced page.

2. Definitions

This chapter defines the terms used in this guide with which you may not be familiar.

TERMS USED IN THIS GUIDE

Vidyo Concepts and Equipment

Here's a brief introduction to the system's components.

- **Portal** – A single web page¹ (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, which are actually virtual conference rooms. When a user's account is set up, that user is automatically assigned a room. A user can have more than one room (all accessible via his or her portal). An end user uses his or her portal to make direct point-to-point video calls and to set up and use his or her room or rooms.
- **Note:** The UI for the end user in a call or conference is his or her VidyoDesktop software.
- **VidyoDesktop** – The software client that enables users to view other users in point-to-point calls and VidyoConferences. It's easy to use and manage via the VidyoPortal, and it can send and receive in HD. All users are assigned a password-protected personal space, thus making it possible for meetings to be held anytime—whether impromptu or by prior arrangement. It supports standard USB webcams and runs on Macs, PCs, and Linux, providing an unparalleled personalized multipoint collaborative experience.
- **VidyoGateway** – The VidyoGateway allows the VidyoConferencing infrastructure to connect to traditional H.323 and SIP devices. It supports standards, such as H.239 for data collaboration, that are required for those devices to communicate, regardless of whether they are endpoints, MCUs, gatekeepers or gateways. For example, the VidyoGateway can be integrated with SIP PBX. It seamlessly integrates into the network providing the end user with an easy experience regardless of whether they're calling a Vidyo device or traditional H.323/SIP device.
- **VidyoMobile** – A program that allows users of smart phones and tablets to participate in point-to-point calls and VidyoConferences. There are versions for both Android and Apple iOS devices and copies are available from the platforms' respective stores (the Android Market and the App Store).
- **VidyoOne™** – Vidyo's smallest capacity Vidyo Server. It's designed for smaller organizations that don't need the full power of our standard server.
- **VidyoPanorama™ 600** – VidyoPanorama 600 is a multi-screen group solution that allows distributed teams to connect and collaborate easily from desktop, mobile, and room-based systems. While typical room systems limit you to just two screens for people and content, VidyoPanorama 600

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

drives up to six screens. And thanks to the exclusive Multi-Participant Content Sharing feature, content streams from up to six participants can be displayed at the same time.

- **VidyoPortal** – The VidyoPortal provides central management of the Vidyo devices on the network. It's an easy-to-use secure web portal that allows for integration with secure LDAP and Active Directory databases for user authentication, as well as maintaining its own user database. The VidyoPortal allows administrators from any location on the network to control every aspect of the VidyoConferencing solution from a central location. Administrators can control system-wide parameters and policies, establish end-user and association privileges, and customize user conferencing capabilities.

The VidyoPortal also acts as a web front for all users of the system. Its flexible user interface facilitates everything required to initiate and manage a call. Users have control over adding, disconnecting, and muting/un-muting participants along with many other conference control parameters. The interface allows users to manage and customize their own contacts lists and to initiate reservation-less multipoint conferences as well as point-to-point calls.

- **VidyoProxy** – A software component built into the VidyoRouter that enables authorized endpoints to connect while denying unauthorized connections. It also enables NAT and firewall traversal.
- **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 conference or want to view it again.
- **VidyoRoom** – The VidyoRoom system is a hardware appliance endpoint that uses Vidyo's SVC technology. It can deliver HD Quality at 60 frames per second. Designed specifically for use over converged IP networks, the VidyoRoom can decode and display multiple HD participants at video quality unequaled by systems that require dedicated bandwidth to perform at their best. The VidyoRoom system is simple to use, easy to configure and voice-activated with continuous presence. Flexible conference control options make it simple to manage, using either the VidyoPortal or a remote control device. VidyoRoom interoperates seamlessly with VidyoDesktop clients, making it possible for people to join a conference from their home office or wherever they happen to be.
- **VidyoRouter** – The VidyoRouter is the core infrastructure product for conducting all videoconferencing. It is an intelligent routing appliance that uses patented scalable video packet switching technology to achieve unprecedented performance and features without the need for expensive, time consuming transcoding. All video traffic is managed by the VidyoRouter. Additionally, conferences can span across multiple VidyoRouters, achieving maximized WAN utilization as well as redundancy and efficiency.
- **VidyoRouter Cloud Edition or VidyoCloud** – An enhanced topology that increases network bandwidth efficiency, decreases latency and optimizes how VidyoRouters handle traffic. Because many of our customers don't require the advantages that Vidyo Cloud provides, the feature is turned off by default. A small organization with few locations may not need to use 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.

- **Inter-Portal Communications (IPC)** – This option, which is also known as Vidyo Address Dialing, enables users to join conferences that are taking place in rooms on a third-party VidyoPortal. IPC access control can be set at the tenant level or at the system level.
- **VidyoPortal Hot Standby Redundancy** – This option requires two VidyoPortal servers to be deployed in the same subnet. One of the VidyoPortals acts as the Active VidyoPortal and the other as the Standby VidyoPortal. If the Active VidyoPortal is not reachable, the Standby VidyoPortal automatically takes over within one minute. Upon taking over, the Standby VidyoPortal uses the information it received in the last synchronization with the Active VidyoPortal.

Users

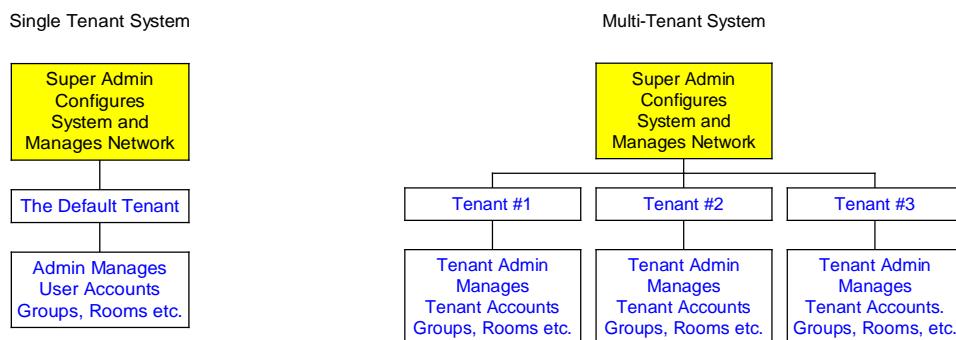
A user is anyone who uses the system. In a small organization, one person might assume the roles of both Super Admin and Admin, when appropriate.

- **The System Console Administrator** – This account configures and maintains the system and the network using the System Console and the Configuration Pages for VidyoRouter, VidyoProxy, and VidyoGateway.
- **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, the Super Admin has full administrative privileges above the tenant admin and all regular tenant admin rights.
- **Tenant Admin** – Has administrative privileges. An Admin can add, delete and manage users, set up public rooms, and set up groups (which define the 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 perform the task. The term Tenant Admin is used for someone who performs the same duties for a tenant in a multi-tenant set-up.
- **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.
- **Normal** – The end user. All users have a portal (Web page) from which they can join meetings (i.e., teleconferences), control their own meetings, and place direct (point-to-point) calls. Users can also change their passwords and optionally set PIN codes required by other users to join meetings.
- **Executive Desktop** – An Executive Desktop is a premium user license that's assigned to a specific user account. An Executive Desktop doesn't require a VidyoLine license to participate in calls or conferences, nor is an Executive Desktop user ever denied service due to lack of shared VidyoLine availability. Executive Desktops are ideal for mission-critical applications such as 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 users, an Executive Desktop user can see each participant's image in full 720p – a capability that no other video conferencing system can match. Executive Desktop user licenses are also used for systems running the VidyoRoom Software Edition (SE).

- **VidyoPanorama** – The VidyoPanorama user type was used for VidyoPanorama 1.0 and included the same rights as a normal user. VidyoPanorama 1.0 had its own *Administrator and User Guide*. VidyoPanorama 1.0 has since been replaced by VidyoPanorama 600.
 - **VidyoRoom** – VidyoRoom is a hardware appliance endpoint that's generally placed in an actual conference room. It has the same rights as a normal user and has its own *VidyoRoom Administrator Guide* and *VidyoRoom Quick User Guide*.
- Note:** VidyoPanorama 600 also uses the VidyoRoom User Type. VidyoPanorama 600 has its own *Administrator Guide*.
- **VidyoRoom SE** – VidyoRoom SE is a software application that allows you to leverage a VidyoRoom system on select hardware. It consumes an Executive Desktop user license and has its own *VidyoRoom SE Deployment Guide*.
 - **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.
 - **Guest Users** – 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, but the Super Admin can customize the text as desired and the Admin or Tenant Admins can edit the text for their tenants. Users can edit each invitation they send (in order to add the date, time, or any other information). The guest user clicks the link in the invitation email, downloads the software (if he or she hasn't before), and then enters a guest user name 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.

Tenants

- **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. 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** – A single organization might also wish to divide up its users into multiple sets of tenants. In the latter case, the Super Admin enables cross-tenant access, so any system user can reach any other regardless of tenant.



This chart illustrates the differences and similarities between Single Tenant and Multi-Tenant systems. Both types of systems 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 being both the Super Admin and Admin at different times, as appropriate. A single person could be the Tenant Admin for more than one tenant. In fact, nothing in the system prohibits one person 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 own 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 or fully qualified domain name (FQDN) that tenants use to access his or her user portals.

Meeting

A meeting is an audio and video connection of a meeting room with two or more users interacting and sharing their media streams and, optionally, the windows of applications running on their machines.

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 for that user.
- **Public** – Common public spaces may also be created by Admins and Operators only. These are the equivalent of conference rooms in the physical world. In addition to his or her automatically created private room, a user can request additional public rooms for his or her account.

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 and Tenant Admins.
- Groups are subsets of Tenants. You don't have to create any groups. However, 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 allowed in a VidyoConference and the maximum bandwidth per participant for the conference.
- 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 maximum number of users in a call and the maximum bandwidth allowed per call can be set for guest users and public rooms by designating a special group with the desired settings and assigning that group to specific users and public rooms as necessary.

For more information, see “Adding a Meeting Room” on page [213](#) and “Adding a New Group” on page [230](#).

- You can change the maximum number of participants allowed in a personal room by simply changing the maximum for the group to which the user belongs.
- The bandwidth limitation is per user, so changing the group to which a user belongs might also affect his or her bandwidth limitation-and the maximum number of participants that can be in his or her rooms. However, a public room can be assigned to a different group than the room owner.

The default group has the following factory configuration:

- 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.

VidyoLines

VidyoLines are a *perpetual* software license for a single logical connection through the VidyoRouter – either point-to-point or multipoint – 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 on a call and releases the license for someone else to use when the call is ended.

VidyoRoom and VidyoGateway connections are effectively free since they don’t consume VidyoLine licenses. Systems running VidyoRoom SE consume an Executive Desktop user license.

Install

An install represents one installation of the VidyoDesktop or VidyoMobile client software. There are VidyoDesktop versions for Windows, Mac OS, and Linux, and VidyoMobile versions for Android and iOS. A guest user also requires an install.

Endpoint

A device, such as a desktop, laptop, Android phone or tablet, iOS phone or tablet, or VidyoRoom that enables a user to participate in direct video calls and video conferences. Two points worth remembering:

- The VidyoRoom is the only endpoint that's also considered a user; however, systems running VidyoRoom SE consume an Executive Desktop user license.
- Even though people can participate in conferences in audio-only mode (if your system has a Vidyo-Gateway) by using cell phones and landlines, they're not considered endpoints if they don't have VidyoMobile software installed. If they have VidyoMobile, they *are* considered endpoints and they can participate via audio *and* video.

3. Upgrading Your VidyoConferencing System

This chapter describes how to upgrade your VidyoConferencing system. If you are installing your system for the first time, skip this chapter and proceed to “Initial Configuration” on page [22](#).

Caution:

- You must refer to the Release Note for your software version before starting the upgrade process. The “Upgrade Notices” section of the Release Note contains important information that you must adhere to in order to successfully perform the upgrade.
- Once a Vidyo Server (VidyoPortal, VidyoRouter, VidyoGateway, or VidyoReplay) has been upgraded, it cannot be reverted back to a previous version.

The following steps reference the procedures you must perform in order to upgrade your VidyoConferencing system. Follow the steps in the order listed.

To upgrade your VidyoConferencing System:

1. **Back Up Your VidyoPortal Database** – The first procedure you must perform when upgrading your VidyoConferencing system is to back up the VidyoPortal database.
For more information, see “Backing Up the Database” on page [73](#).
2. **Upgrade Your VidyoRouters** – Perform this step only if you have any secondary VidyoRouters (along with your VidyoPortal). Otherwise, skip this step.
For more information, see “Upgrading Your VidyoRouter” on page [134](#).
3. **Upgrade Your VidyoGateways** – Perform this step only if you have one or more VidyoGateways as part of your VidyoConferencing System. Otherwise, skip this step.
For more information, refer to the “Upgrading Your VidyoGateway” section of the *VidyoGateway Administrator Guide*.
4. **Upgrade Your VidyoReplays** – Perform this step only if you have one or more VidyoReplays as part of your VidyoConferencing System. Otherwise, skip this step.
For more information, refer to the “Upgrading VidyoReplay” section of the *VidyoReplay Administrator Guide*.
5. **Upgrade Your VidyoPortal** – The procedure used for upgrading your VidyoPortal depends on whether or not you have the Hot Standby software option on your VidyoConferencing System.
 - **Upgrading Your VidyoPortal without Hot Standby** – Upgrades are performed using the System Upgrade Tab in the Super Admin Portal.
For more information, see “Upgrading Your VidyoPortal System Software” on page [78](#).

- **Upgrading Your VidyoPortal with Hot Standby** – The following two methods are available for upgrading your VidyoPortal while running the Hot Standby software option.

- **Upgrading Your Hot Standby VidyoPortals while Keeping One Server Online**

For more information, see “Upgrading Your Hot Standby VidyoPortals while Keeping One Server Online” on page [371](#).

- **Upgrading Your Hot Standby VidyoPortals while Taking Both Servers Offline**

For more information, see “Upgrading Your Hot Standby VidyoPortals while Taking Both Servers Offline” on page [373](#).

Regardless as to how you upgraded your VidyoPortal, you should now confirm that all of your components are upgraded and have a Status of UP on the Components Table. Any external components, VidyoRouters, VidyoGateways, and VidyoReplays that were previously listed as DOWN, NEW, or in Alarm should have automatically updated or cleared. If any component remains with an Alarm, mouse over the Alarm to display the reason for the Alarm. Try rebooting the component in Alarm to clear the Alarm; otherwise, attempt to correct the issue based on the alarm reason presented. For more information, see “Configuring Your Components as the Super Admin” on page [113](#).

If any external components, VidyoRouters, VidyoGateways and/or VidyoReplays were not already upgraded, upgrade them now as described in the steps in this chapter. Once upgraded, ensure that you reboot the VidyoPortal so that each additional component may be automatically updated.

- 6. **Upload the Endpoint Software to the VidyoPortal** – After performing a VidyoPortal upgrade, you typically need to upload new endpoint software as well. For more information, see “Uploading Endpoint Software” on page [68](#).

4. Configuring Your Vidyo Server

Immediately after you have physically installed your Vidyo Server as described in the *Vidyo Server Installation Guide*, you must initially configure your VidyoConferencing system as described in this chapter.

For more information about installing the Vidyo Server and for Vidyo Server specifications, refer to the *Vidyo Server Installation Guide*. You can access this document and other Vidyo product documentation by registering at <https://selfservice.vidyo.com/register/>.

Super Admins are typically network system administrators responsible for management of the VidyoPortal, VidyoRouter, and other Vidyo components.

Note: Vidyo Customer Support may require access to your Vidyo Server via SSH over port 2222 in order to troubleshoot any of your customer issues. You can restrict Vidyo Customer Support SSH access by configuring your firewall to only permit access from authorized networks and users or contact Vidyo Customer Support for alternate options.

As a Super Admin, after the Vidyo server is physically installed (as described in the *Vidyo Server Installation Guide*), you must do the following to initially configure your system:

- When setting up your Vidyo Server, always be sure to configure your firewall to only permit SSH access from authorized networks and users.
- Change your System Administrator Console default password. This must be changed after the first login. For more information, see the following procedure.
- Change the default password of your Super Admin account. For more information, see “Changing Super Account Passwords” on page [87](#).
- Configure the network information.

The network settings are set at the System Console. You can view the settings (read-only) in the Super Admin portal.

- Change the remaining default passwords.
- Configure the VidyoPortal.
- Request Vidyo system licenses and apply the system license keys to your system.
- Select the system language.

All of these tasks are described in this chapter.

Note: Some of these tasks may not be necessary when you first set up your system and are preset at the factory. However, you’ll need to know how to perform them if you want to change the factory defaults.

Besides these tasks, the Super Admin can perform many other tasks, such as configuring the system settings, setting up components such as the VidyoManager, and configuring tenants. System configuration 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 after the initial configuration has been completed. These tasks are explained in the following chapters.

For descriptions of the tasks that Admins and Tenant Admins perform, see the “What Tenant Admins Do” section on page [201](#).

LOGGING IN TO THE SYSTEM CONSOLE OF YOUR VIDYO SERVER AND CHANGING THE DEFAULT PASSWORD

The very first time you log into your Vidyo Server, you are required to change the System Console default password to a more secure one. This procedure must be used to change the default password on all Vidyo Servers including:

- VidyoPortal
- VidyoRouter
- VidyoGateway (an optional component)

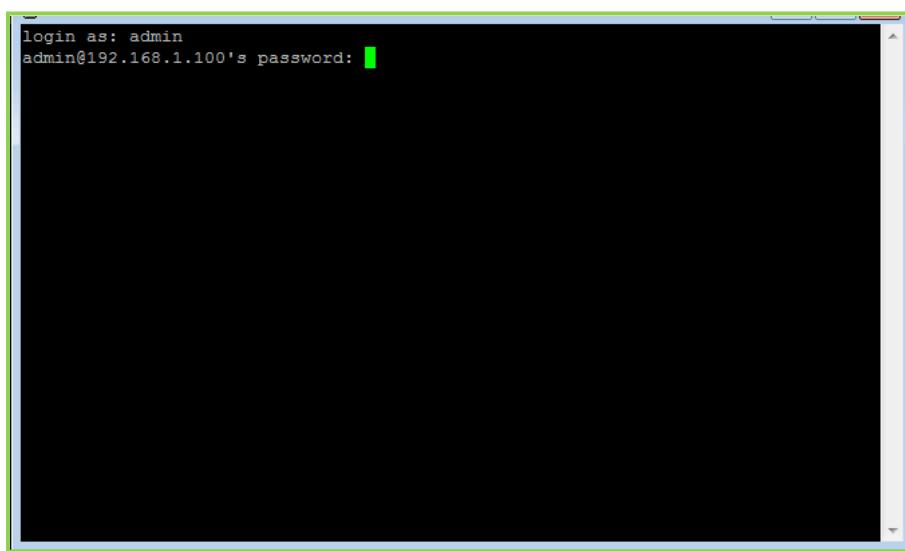
To log in to your Vidyo Server and change the default password:

1. Connect a keyboard and a VGA display directly to your server.
2. Log in using the default Administrator account:

User Name: **admin**

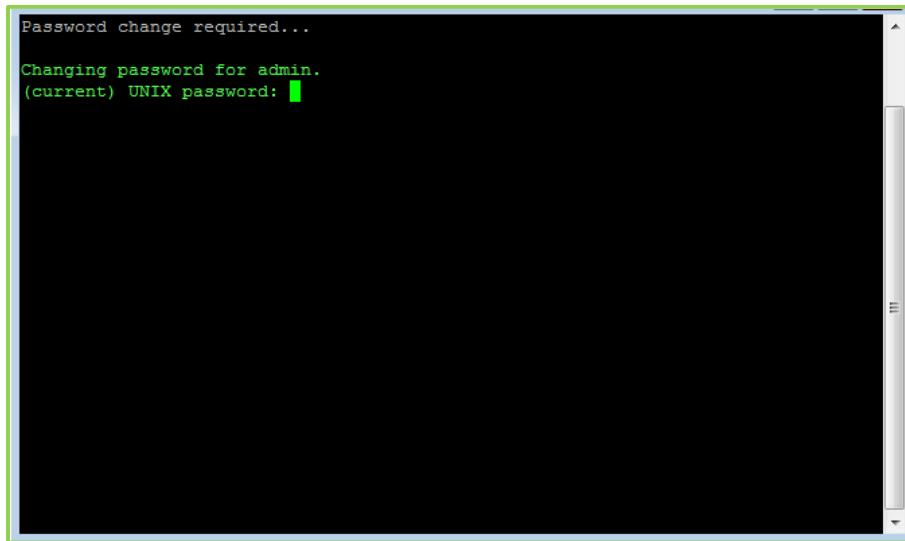
Password: **password** (case sensitive)

3. At the login prompt, enter **admin**.



4. At the (current) UNIX Password prompt, enter **password**.

The password is case sensitive. You'll be prompted to enter a new password and asked to enter it again.



A screenshot of a terminal window titled "Password change required...". The window shows the command "Changing password for admin." followed by "(current) UNIX password: [REDACTED]". The terminal has a green border and a vertical scroll bar on the right side.

5. At the Enter new UNIX password: prompt, type a new password.

When selecting a new password, follow these guidelines:

- **The password should not be based on the dictionary.**
- **The password should not be too similar to the old password.**

The default setting is at least 3 characters should be different from the old password.

- **The password should not be too simple or too short.**

The algorithm here is a point system to satisfy the min password length (the default is length 8 characters). The password gets extra points if it contains “number”, “upper case”, “lower case”, or “special character”. Each point is equivalent to 1 character.

- **The password should not be a case change only of the old password or should not be the reverse of the old password.**

6. At the Retype new UNIX password: prompt, type your new password again.

If the passwords don't match, you'll be prompted to try again. If the passwords match, the System Console menu opens immediately.

```

Local Time: Fri May 10 17:03:54 EDT 2013
Universal Time: Fri May 10 21:03:54 UTC 2013

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           I
7. Display DNS Nameserver
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
m. ... (more options)
x. Exit System Administrator Console

Selection: [ ]

```

7. When you need to reset the password, use 13. Set 'admin' password.

CONFIGURING THE NETWORK SETTINGS AT THE SYSTEM CONSOLE

Each type of Vidyo Server (VidyoPortal, VidyoRouter, VidyoGateway, or VidyoReplay) has a different default IP address and is necessary to perform the steps in this section:

- VidyoPortal: 192.168.1.100
- VidyoRouter: 192.168.1.105 (optional external component)
- VidyoGateway: 192.168.1.110 (optional external component)
- VidyoReplay: 192.168.1.115 (optional external component)

For more information about System Administrator Console Menu Options, see “Understanding System Administrator Console Menu Options” on page [28](#), and “Understanding the More Options System Administrator Console Menu Options” on page [33](#).

Note: The basic network setup for each type of Vidyo Server is basically the same. You must perform a network setup for each of your Vidyo Servers.

To configure the network settings at the System Console:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

The following illustrations show the System Console after you have logged in using a keyboard and VGA monitor plugged directly into the VidyoPortal.

2. Select 1. Configure IP Address.

3. Select the PRODUCTION INTERFACE or MANAGEMENT INTERFACE which contains the IP you want to configure.

```
Select Network Interface to Configure
-----
1. PRODUCTION INTERFACE
2. MANAGEMENT INTERFACE
X. Exit

Enter 1, 2 or x: [REDACTED]
```

Note: The Management Interface should not be used to transfer any media.

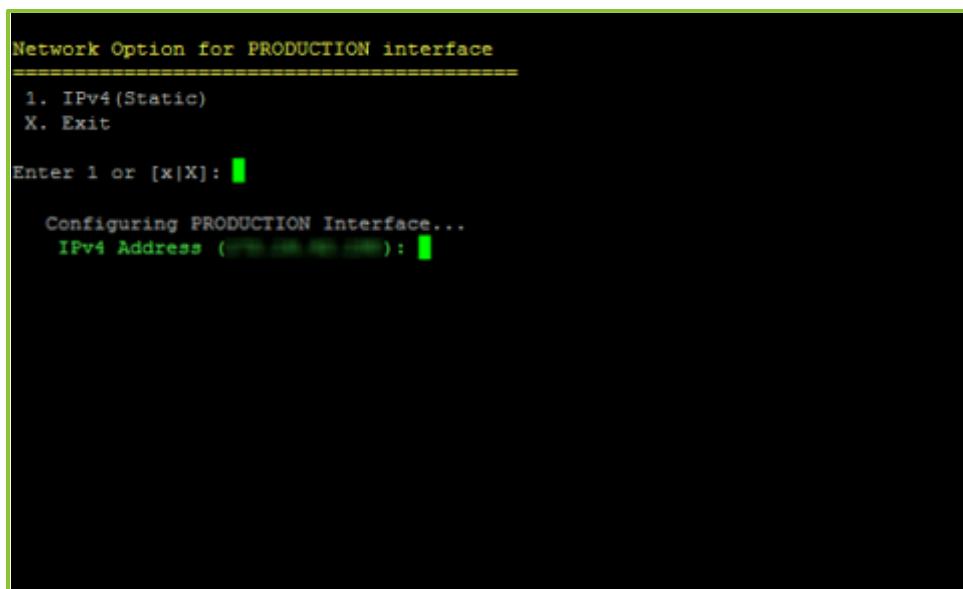
For more information, see “Enabling the Management Interface” on page [57](#).

4. Select the IPv4 (Static) IP address format.

```
Network Option for PRODUCTION interface
-----
1. IPv4(Static)
X. Exit

Enter 1 or [x|X]: [REDACTED]
```

5. Select **1. IPv4(Static)** to set the server IP address, subnet mask, default gateway, and MAC addresses, hostname, domain name, and FQDN. Press **Enter** after entering each setting.

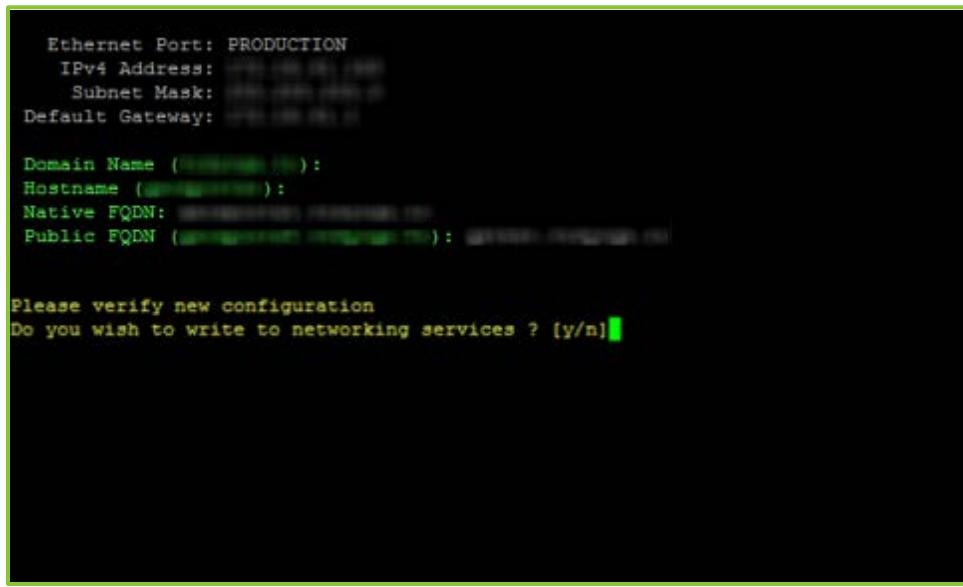


```
Network Option for PRODUCTION interface
=====
1. IPv4(Static)
X. Exit

Enter 1 or [x|X]: 1

Configuring PRODUCTION Interface...
IPv4 Address (192.168.1.100):
```

6. Once you have entered the required information, select **y** and press **Enter**.



```
Ethernet Port: PRODUCTION
IPv4 Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

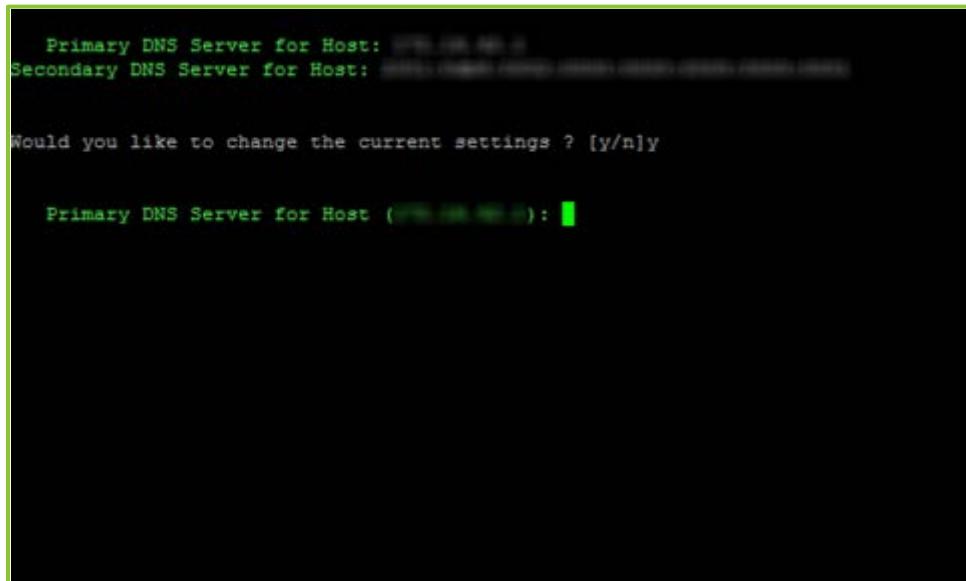
Domain Name (cluster.local.):
Hostname (cluster):
Native FQDN: cluster
Public FQDN (cluster.vidyouser.com): cluster.vidyouser.com

Please verify new configuration
Do you wish to write to networking services ? [y/n] y
```

Note:

1. Unless you're using the Hot Standby software option, the Native FQDN and Public FQDN should be the same.
2. If you are using the Hot Standby software option, the Native FQDN will be the Native FQDN of the Active or Standby VidyoPortal and the Public FQDN will be the same as the Cluster FQDN. For more information, see “Applying System License Keys to Your System Using the Hot Standby Software Option” on page [67](#) and “Hot Standby” on page [342](#).

3. The Public FQDN provided here is the same one you use when requesting your license keys from Vidyo Support. For more information, see “Requesting Vidyo System Licenses and Applying System License Keys” on page [51](#) and “Applying System License Keys to Your System” on page [52](#).
7. Select **2. Configure DNS Nameserver** to set the fully qualified domain name (if it exists) for the VidyoPortal and the IP addresses of the DNS servers:
 - a. Enter two DNS server IP addresses. If you have only one DNS server, use the same one twice.



```

Primary DNS Server for Host: [REDACTED]
Secondary DNS Server for Host: [REDACTED]

Would you like to change the current settings ? [y/n]y

Primary DNS Server for Host ([REDACTED]): [REDACTED]

```

- b. Once you have entered the required information, select **y** and press **Enter**.

The System Console main menu is shown.

8. Enter the remaining network settings for the server as needed, confirming by typing **y** and pressing **Enter** after entering each setting:
 - a. Select **3. Configure NTP Time Servers** to set the NTP (Network Time Protocol) time server.
 - b. Select **4. Configure Time Zone** to specify the time zone you are working in.
 - c. If necessary, select **5. Configure Ethernet Options** to set the MTU (Maximum Transmission Unit) size.
9. Select **14. Reboot system** to restart the server.

When the server restarts, it will have the new network settings. Be sure to record your network settings, as you will need them for further configuration of your system.

CHANGING THE REMAINING DEFAULT PASSWORDS

Besides changing the default password for the Vidyo Server (often referred to as the System Console or Admin Console), you should also change the following additional default passwords to ensure security and prevent unauthorized access:

- VidyoPortal/VidyoOne Super Administrator

To change this password, log into the Super Admin portal as described in “Logging in to the Super Admin Portal” on page [35](#).

- VidyoPortal/VidyoOne Administrator (per tenant)

Change the Administrator login as described in the “Editing a User” section on page [207](#). In a multi-tenant system, you must do this for each Tenant Administrator.

- VidyoRouter Administrator

This password is tied to the System Console password. For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

- VidyoManager Administrator

This password is tied to the System Console password.

- VidyoProxy Administrator

This password is tied to the System Console password.

For more information about System Administrator Console Menu Options, see “Understanding System Administrator Console Menu Options” on page [28](#), and “Understanding the More Options System Administrator Console Menu Options” on page [33](#).

SUPPORTING MULTIPLE SYSTEM CONSOLE ACCOUNTS

System Console accounts can be used on the VidyoPortal, the VidyoRouter, and the VidyoGateway.

The System Console menu allows for the creation of up to ten System Console accounts. These accounts are created from the System Console.

To create System Console accounts:

1. Log in to the System Console of your Vidyo Server.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select m. . . (more options)

3. Select 19. User Administration.

```
Local Time: Fri May 17 16:42:08 EDT 2013
Universal Time: Fri May 17 20:42:08 UTC 2013

17. Configure Adobe Connect plugin
18. Display System ID
19. User Administration
20. Software Versions
  A. Advanced Options
  E. Emergency Admin
  b. ... (back to previous menu)

Selection: [
```

4. The User Maintenance screen provides the following options:

- a. Select A to add a user.

```
-----
User Maintenance
-----
[A] - Add User
[B] - Remove User
[C] - Show User(s)
[x] - Exit
-----
CURRENT USER: admin1
=> [
```

- b. Select B to remove a user.
c. Select C to show all user accounts.
d. Select x to exit.

The current user is also shown on the screen.

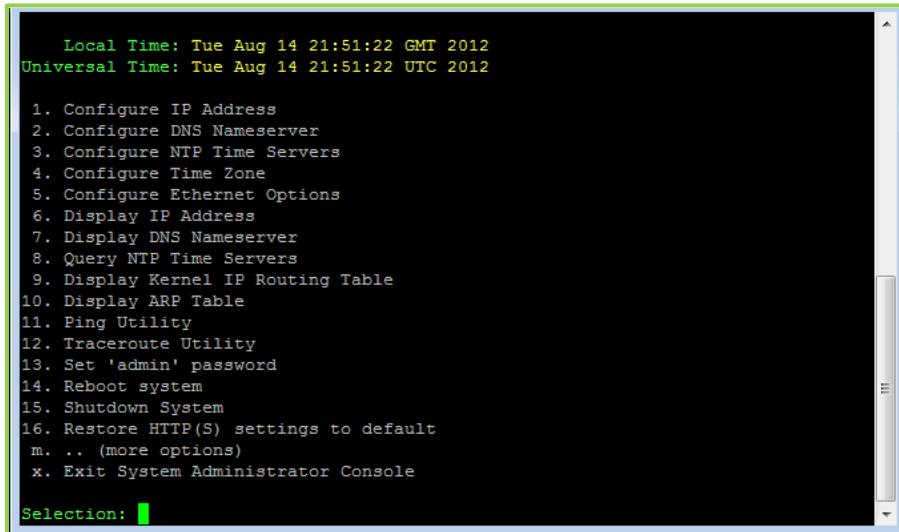
Note:

- In addition to accessing the the System Console menu, the ten System Console accounts can also access the VidyoGateway Admin Pages.

- Each new System Console account has a default password of **password**, which is case sensitive.
- The System Console accounts force a password change on first login. To prevent the use of default passwords, each new System Console user must be present at the local console during account creation. That user must log in and change their password and it must meet JITC password complexity requirements.

UNDERSTANDING SYSTEM ADMINISTRATOR CONSOLE MENU OPTIONS

The following list includes steps taking you through configurations on System Console menu options. Follow along and use the examples as entries to make for various configurations.



The following describes commands on the Main Menu.

1. **Configure IP Address** – Select 1 to configure your server IP address, subnet mask, and default gateway addresses. Initially, information must be configured locally. You can also use this option to configure the domain name, hostname, local FQDN, and public FQDN values.

Examples:

```

IP Address Mode: static
Network Interface: Production
IPv4 Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
Hostname: portal
Domain Name: yourcompany.com
Local FQDN: portal.yourcompany.com
Public FQDN: publicportal.yourcompany.com
  
```

Note: The Public FQDN can match the Local or Native FQDN, if desired.

For more information, see “Configuring Network Settings at the System Console” on page [25](#) and “Enabling the Management Interface” on page [57](#).

Note: The Management Interface should not be used to transfer any media.

- 2. Configure DNS Nameserver** – Select **2** to specify the Domain Nameserver.

Examples:

Primary DNS Server for Host: 192.168.1.10

Secondary DNS Server for Host: 192.168.1.11

- 3. Configure NTP Time Servers** – Select **3** to set the Network Time Protocol (NTP) time server. Change to synchronize the system with a different time server.

Examples:

Primary NTP Server: pool.ntp.org

- 4. Configure Time Zone** – Select **4** to specify the time zone of your server. Change as necessary for accurate billing records.

Examples:

US/Eastern

- 5. Configure Ethernet Options** – Select **5** to set the Maximum Transmission Unit (MTU) size. The default is **1500**. Only change this setting if your network MTU size is less than **1500**. You can also turn autonegotiation on or off. Autonegotiation is on by default.

Examples:

MTU Size: 1500

Autonegotiation: On

Note: When Autonegotiation is set to **Off**, it means **100/Full**.

- 6. Display IP Address** – Select **6** to view your current IP address settings and IP address mode. Also displays the hostname, domain name, and FQDN.

Examples:

IP Address Mode: static

Network Interface: Production

IPv4 Address: 192.168.1.100

Subnet Mask: 255.255.255.0

MAC Address: 00:0c:29:4b:4c:3w

Default Gateway:

default via 192.168.1.1 dev eth0

Hostname: portal

Domain Name: yourcompany.com

Local FQDN: portal.yourcompany.com

Public FQDN: publicportal.yourcompany.com

7. **Display DNS Nameserver** – Select 7 to view the DNS servers.

Examples:

Primary DNS Server for Host: 192.168.1.10

Secondary DNS Server for Host: 192.168.1.11

8. **Query NTP Time Servers** – Select 8 to query NTP servers.

Note: This command doesn't work if the domain name server is not defined.

9. **Display Kernel IP Routing Table** – Select 9 to view how your server is configured for Ethernet routing.

10. **Display ARP Table** – Select 10 to display router and MAC address information. This information is display only.

11. **Ping Utility** – Select 11 to ping network addresses. Use **Ctrl+c** to stop pinging.

12. **Traceroute Utility** – Select 12 to display the trace route to a specified address. You must enter the IP address of the device.

Press enter to return to the Main Menu.

13. **Set ‘admin’ Password** – Select 13 for password menu options including functions to reset the admin password to the default value and change password.

Note: Adhere to the password guidelines explained on page [24](#).

Select x to return to the Main Menu.

14. **Reboot system** – Select 14 to restart your server.

Note: It can take up to a minute for your server to restart.

15. **Shutdown System** – Shuts down your server.

16. **Restore HTTP(S) settings to default** – Select 16 to return HTTP settings to their default values (HTTP and port 80).

Note: This option is not available on the VidyoGateway and VidyoReplay System Console menu.

- m. **.. (more options)** – Select m for a submenu containing additional options.

For more information, see “Understanding the More Options System Administrator Console Menu” on page [33](#).

- x. **Exit System Administrator Console** – Select x to close the SSH session. This command also closes SSH clients, if one is used.

Understanding the More Options System Administrator Console Menu

The following list describes commands on the More Options menu.

17. **Configure Adobe Connect Plugin** – Select 17 to configure your Adobe Connect Server and Adobe Connect Plugin.

- 18. Display System ID** – Select **18** to display system identification data including the Local Time, Universal Time, and the System ID.
- 2. User Administration** – Select **19** to perform user maintenance and create additional System Console accounts.
For more information, see “Supporting Multiple System Console Accounts” on page [29](#).
- 4. Hot Standby** – This menu item only appears if you have the Hot Standby option applied on your system. Select **H** to access the Hot Standby menu.
For more information, see Hot Standby on page [342](#).
- 2. Advanced Options** – Select **A** to access advanced options.
For more information, see “Understanding the Advanced Options System Administrator Console Menu” on page [34](#).
 - 1. Restart Web Services** – Select **W** to restart your Web services.
 - b. .. (back to previous menu)** – Select **b** to return to the Main Menu from More Options.

Understanding the Advanced Options System Administrator Console Menu

The following list describes commands on the Advanced Options menu.

- 1. ** unused ****
- 2. Network Route Management** – Select **2** to for Network Route Management options including functions to Add, Remove, or Remove All (routes); navigate routes using Next or Previous; and Exit the Route Management menu and return to the Advanced Options menu.
For more information, see “Managing Network Routes” on page [35](#).
- 3. OCSP Information** – Select **3** to view OCSP settings and enable or disable OCSP.
For more information, see “Disabling OCSP from the System Console” on page [284](#).
- 4. SNMP Administration** – Select **4** for SNMP menu options including functions to enable or disable SNMP, delete the local user-based security model, or configure traps.
For more information, see “Configuring SNMP” on page [39](#).
- 5. Hostname Management** – Select **5** for Hostname Management menu options including functions to Add, Remove, or Remove All (hostnames); navigate hostnames using Next or Previous; and Exit the Hostname Management menu and return to the Advanced Options menu.
For more information, see “Managing Hostnames” on page [39](#).
- 3. Download Login/Welcome Banner** – Select **R** to download the welcome banner from your configured VidyodaPortal.
- x. Exit Advanced Options** – Select **x** to return to the More Options menu from Advanced Options.

MANAGING NETWORK ROUTES

Static routes are used in deployments where Vidyo servers are in a DMZ between two segregated firewalls with no route for either internal or external traffic. Network Routes are also used when the Management Interface is enabled and you want to route traffic across that network.

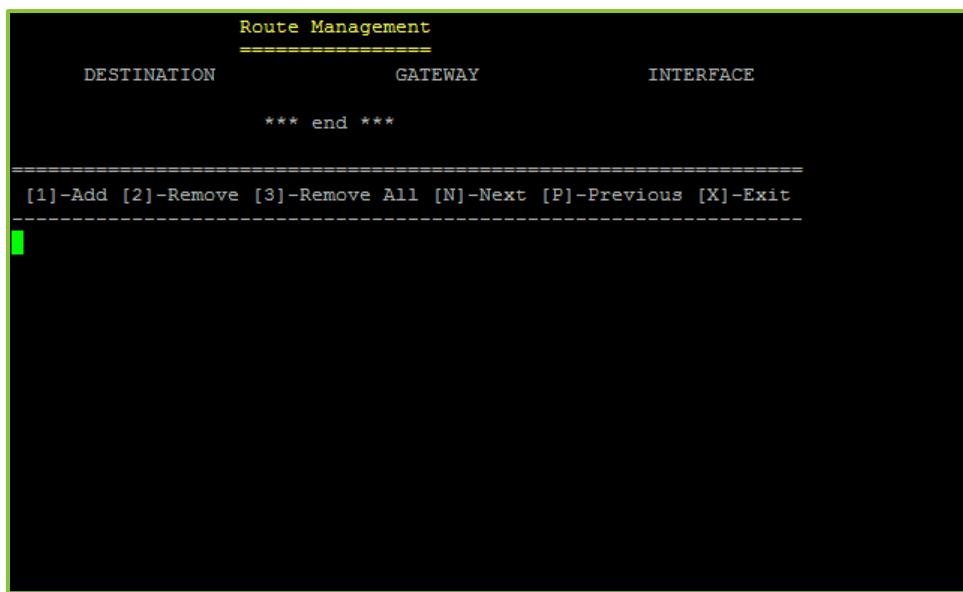
Note:

- Vidyo recommends this feature not replace adding proper network router to your DMZ to handle the proper subnet routes. Static route setup can lead to security vulnerabilities and should only be configured by advanced network administrators. Vidyo is not responsible for any possible security risk resulting from static route configurations.
- You can either add a static route for one host at a time or add a route covering a range of IP addresses using a subnet mask.

For more information, see “Adding a Network Route” on page [36](#).

To manage network routes:

1. Log in to the System Console.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
2. Select **m. ... (more options)**.
 3. Select **A. Advanced Options**.
 4. Select **2. Network Route Management**.



The Route Management screen appears. Use this screen to Add, Remove, or Remove All (routes); navigate routes using Next or Previous; and Exit the Route Management screen.

5. Select **[X]-Exit** to return to the Advanced Options menu.

Adding a Network Route

Note: Currently, you can only add a static route for one host at a time. Adding static routes for a range of IP addresses (or subnet) is not supported at this time.

To add a network route:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select **m. ... (more options)**.
3. Select **A. Advanced Options**.
4. Select **2. Network Route Management**.
5. Select **[1]-Add** to add a Network Route.
6. Enter the following information:

- **Destination** – Enter an IP address of the target machine for your network route.

Note: You can either add a static route for one host at a time or add a route covering a range of IP addresses using a subnet mask. To specify a range for, say, 172.16.1.0 – 172.16.1.255, you would enter **172.16.1.0/24**, where 24 is the subnet mask.

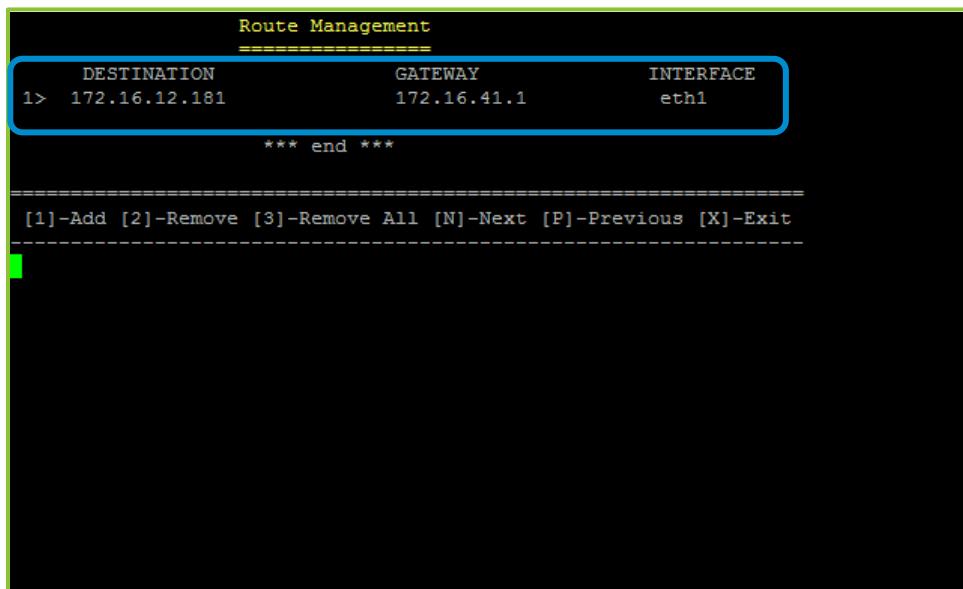
- **Gateway** – Enter the IP address of the Gateway through which your network route will travel.
- **Interface** – Enter the PRODUCTION (eth0) or MANAGEMENT (eth1) interface you want your network route to use.

Note:

If you want to cancel adding your Network Route, press enter while providing no Destination, Gateway, or Interface information. The system tells you that you must provide valid information and to press any key. Press any key to return to the Route Management screen.

7. Select **y** to confirm the change and add your Network Route.

Your Network Route is then listed and numbered on the top of the Route Management screen.



The screenshot shows a terminal window titled "Route Management". It displays a single route entry:

DESTINATION	GATEWAY	INTERFACE
1> 172.16.12.181	172.16.41.1	eth1

Below the table, the text "*** end ***" is displayed. At the bottom of the screen, there is a menu with the following options: [1]-Add [2]-Remove [3]-Remove All [N]-Next [P]-Previous [X]-Exit. A small green square cursor is visible on the left side of the menu.

8. Select [X]-Exit to return to the Advanced Options menu.

Removing a Network Route

To remove a network route:

1. Log in to the System Console.
For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
2. Select m. . .(more options).
3. Select A. Advanced Options.
4. Select 2. Network Route Management.
5. Select [2]-Remove to remove a Network Route.

- Enter the corresponding number of the network route you want to remove.

```

Route Management
=====
1> DESTINATION      GATEWAY      INTERFACE
   172.16.12.181    172.16.41.1  eth1
*** end ***
[1]-Add [2]-Remove [3]-Remove All [N]-Next [P]-Previous [X]-Exit
  
```

- Select **y** to confirm removing the selected Network Route.
- Select **[X]-Exit** to return to the Advanced Options menu.

Removing all of Your Network Routes

To remove all of your network routes:

- Log in to the System Console.
For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Select **m. ... (more options)**.
- Select **A. Advanced Options**.
- Select **2. Network Route Management**.
- Select **[2]-Remove all** to remove all of your Network Routes.
- Select **y** to confirm removing all of your Network Routes.
- Select **[X]-Exit** to return to the Advanced Options menu.

Navigating Your Network Routes

To navigate your network routes:

- Log in to the System Console.
For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Select **m. ... (more options)**.
- Select **A. Advanced Options**.

4. Select **2. Network Route Management**.
 - Select **[N]-Next** to navigate to the next Network Route.
 - Select **[P]-Previous** to navigate to the previous Network Route.
5. Select **[X]-Exit** to return to the Advanced Options menu.

CONFIGURING SNMP

You can use SNMP (Simple Network Management Protocol) to manage and monitor the components over your entire Vidyo network. You can configure notifications or traps and send them to your network management server via SNMPv2 community strings or SNMPv3 users.

Note:

- For more information about Vidyo enterprise Notifications, as well as Get, and Set Polling OIDs, refer to the Vidyo MIB file at <http://www.vidyo.com/services-support/technical-support/product-documentation/administrator-guides/>.
- If your VidyoPortal system uses the Hot Standby option and you are not using your management interface, your SNMP notifications will source from the shared IP address.
- Vidyo recommends configuring your VidyoPortal using a management interface so your SNMP notifications can be sourced from unique management interface IP addresses. In this case, your network management system (NMS) should be accessible over your management network.

For more information, see “Enabling the Management Interface” on page [57](#).

Enabling SNMP

Enable SNMP only after configuring SNMP2 community strings or SNMPv3 users and creating notifications or traps.

To enable SNMP:

1. Log in to the System Console.
For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
2. Select **m. ... (more options)**.
3. Select **A. Advanced Options**.
4. Select **4. SNMP Administration**.
5. Select **A. Enable SNMP**.
Note: The feature toggles between Enable and Disable states.
6. Select **y** to confirm the change and enable or disable SNMP.
7. Select **X. Exit**.
8. Select **x. Exit Advanced Options**.
9. Select **14. Reboot system**.

When your system comes back online, SNMP is then enabled (or disabled).

Configuring an SNMPv2 Community String

You can create two SNMPv2 community strings on your system that can access your network management server. One community string has read-only access and the other has read-write access.

To configure an SNMP community string:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select **m. ... (more options)**.
3. Select **A. Advanced Options**.
4. Select **A. SNMP Administration**.
5. Select **B. Configure SNMPv2 Community String**.

Select from the menu based on the SNMPv2 Community String type desired.

- Select **1. Create ReadOnly Community String** to create a read-only SNMPv2 community string.

- a. Enter a read-only community string.

Note: The user name must be at least 8 characters and contain no spaces.

- Select **y** to confirm.

After the read-only community string is created, the Create ReadOnly Community String option toggles and becomes the Delete ReadOnly Community String option.

- Select **2. Create ReadWrite Community String** to create a read-write SNMPv2 community string.

- a. Enter a read-write community string.

Note: The user name must be at least 8 characters and contain no spaces.

- Select **y** to confirm.

After the read-write community string is created, the Create ReadWrite Community String option toggles and becomes the Delete ReadWrite Community String option.

- Select **x. Exit** to return to the SNMP Administration menu.

Deleting an SNMP Community String

To delete an SNMP community string:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select **m. ... (more options)**.

- 3.** Select **A. Advanced Options**.
- 4.** Select **A. SNMP Administration**.
- 5.** Select **B. Configure SNMPv2 Community String**.

Select from the menu based on the SNMPv2 Community String type desired.

- Select **1. Delete ReadOnly Community String** to delete the read-only SNMPv2 community string.

- a.** Select **y** to confirm.

Note: After the read-only community string is deleted, the Delete ReadOnly Community String option toggles and becomes the Create ReadOnly Community String option.

- Select **2. Delete ReadWrite Community String** to delete a read-write SNMPv2 community string.

- a.** Select **y** to confirm.

Note: After the read-write community string is deleted, the Delete ReadWrite Community String option toggles and becomes the Create ReadWrite Community String option.

- Select **x. Exit** to return to the SNMP Administration menu.

Configuring Local SNMPv3 User (User-based Security Model)

You can create two local SNMPv3 users on your system that can access your network management server. One user can have read-only access and the other can have read-write access.

To configure a local SNMPv3 user:

- 1.** Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

- 2.** Select **m. ... (more options)**.
- 3.** Select **A. Advanced Options**.
- 4.** Select **4. SNMP Administration**.
- 5.** Select **C. Configure Local SNMPv3 User (User-based Security Model)**.

Select from the menu based on the SNMPv3 User type desired.

- Select **1. Create ReadOnly User** to create a local SNMPv3 user with read-only access.

- a.** Enter a user name for your local SNMPv3 user with read-only access.

Note: The user name must be at least 8 characters and contain no spaces.

- b.** Enter and verify an authentication password of your choice.

This password uses SHA authentication.

Note:

- The password must be at least 8 characters.
- Vidyo does not currently support MD5 authentication.

C. Enter and verify a second authentication password of your choice.

This password uses AES encryption.

Note:

- The password must be at least 8 characters.
- Vidyo does not currently support DES encryption.

After the read-only user is created, the Create ReadOnly User option toggles and becomes the Delete ReadOnly User option.

- Select 2. **Create ReadWrite User** to create a local SNMPv3 user with read-write access.

a. Enter a user name for your local SNMPv3 user with read-write access.

Note: The user name must be at least 8 characters and contain no spaces.

b. Enter and verify an authentication password of your choice.

This password uses SHA authentication.

Note:

- The password must be at least 8 characters.
- Vidyo does not currently support MD5 authentication.

C. Enter and verify a second authentication password of your choice.

This password uses AES encryption.

Note:

- The password must be at least 8 characters.
- Vidyo does not currently support DES encryption.

After the read-write user is created, the Create ReadWrite User option toggles and becomes the Delete ReadWrite User option.

- Select x. **Exit** to return to the SNMP Administration menu.

Deleting a Local SNMPv3 User (User-based Security Model)

To delete a local SNMPv3 user:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select **m. ... (more options)**.

3. Select **A. Advanced Options**.

4. Select **4. SNMP Administration**.
5. Select **C. Configure Local SNMPv3 User (User-based Security Model)**.
Select from the menu based on the SNMPv3 User type desired.
 - Select **1. Delete ReadOnly User** to delete the local SNMPv3 user with read-only access.
 - a. Select **y** to confirm.
Note: After the read-only user is deleted, the Delete ReadOnly User option toggles and becomes the Create ReadOnly User option.
 - Select **2. Delete ReadWrite User** to delete the local SNMPv3 user with read-write access.
 - a. Select **y** to confirm.
Note: After the read-write user is deleted, the Delete ReadWrite User option toggles and becomes the Create ReadWrite User option.
 - Select **x. Exit** to return to the SNMP Administration menu.

Configuring an SNMP Notification

You can configure notifications or traps that can be sent to your network management server via SNMPv2 community strings or local SNMPv3 users. Notifications are created as either SNMPv2 or SNMPv3.

Creating an SNMPv2 Notification

To create an SNMPv2 notification:

1. Log in to the System Console.
For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
2. Select **m. ... (more options)**.
3. Select **A. Advanced Options**.
4. Select **4. SNMP Administration**.
5. Select **D. Configure SNMP Notification**.
The SNMP Notification menu appears.
6. Select **1. SNMPv2 Notification**.
The SNMPv2 Notification menu appears.
7. Select **1. SNMPv2 Notification**.
8. Enter the IP or FQDN address of your network management server.
9. Select **I** or **T** to configure an Inform or Trap notification type.
Note: The system asks for the values in the remaining steps if your notification type is Inform or Trap.
10. Enter your community string.
Note: The community string must be at least 8 characters and contain no spaces.

- 11.** Select **y** to confirm.

After SNMPv2 notifications are created, they are listed in the top of the SNMPv2 Notification menu and Delete SNMPv2 Notification option appears as a second option.

- 12.** Select **X. Exit** to return to the SNMP Notification menu.

Deleting an SNMPv2 Notification

To delete an SNMPv2 notification:

- 1.** Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

- 2.** Select **m. ... (more options)**.
- 3.** Select **A. Advanced Options**.
- 4.** Select **4. SNMP Administration**.
- 5.** Select **D. Configure SNMP Notification**.

The SNMP Notification menu appears.

- 6.** Select **1. SNMPv2 Notification**.

The SNMPv2 Notification menu appears.

- 7.** Select **1. SNMPv2 Notification**.
- 8.** Select **2. Delete SNMPv2 Notification**.
- 9.** Select the number of the notification user you wish to delete.
- 10.** Select **y** to confirm.

- 11.** Select **X. Exit** to return to the SNMP Notification menu.

Creating an SNMPv3 Notification

To create an SNMPv3 notification:

- 1.** Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

- 2.** Select **m. ... (more options)**.
- 3.** Select **A. Advanced Options**.
- 4.** Select **4. SNMP Administration**.
- 5.** Select **D. Configure SNMP Notification**.

The SNMP Notification menu appears.

- 6.** Select **2. SNMPv3 Notification**.

The SNMP Notification menu appears.

7. Select **1. SNMPv3 Notification User**.
8. Enter the IP or FQDN address of your network management server.
9. Select **I** or **T** to configure an Inform or Trap notification type.

Note: The system asks for the values in the remaining steps if your notification type is Inform or Trap.

10. Optionally enter your Remote Engine ID.
11. Enter your user name.

Note: The user name must be at least 8 characters and contain no spaces.

12. Enter and verify an authentication password of your choice.

This password uses SHA authentication.

Note:

- The password must be at least 8 characters.
- Vidyo does not currently support MD5 authentication.

13. Enter and verify a second authentication password of your choice.

This password uses AES encryption.

Note:

- The password must be at least 8 characters.
- Vidyo does not currently support DES encryption.

After SNMPv3 notification users are created, they are listed in the top of the SNMPv3 Notification menu and Delete SNMPv3 Notification User appears as a second option.

14. Select **X. Exit** to return to the SNMP Notification menu.

Deleting an SNMPv3 Notification

To delete an SNMPv3 notification:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select **m. . .(more options)**.
 3. Select **A. Advanced Options**.
 4. Select **4. SNMP Administration**.
 5. Select **D. Configure SNMP Notification**.
- The SNMP Notification menu appears.
6. Select **1. SNMPv3 Notification**.
- The SNMPv3 Notification menu appears.
7. Select **1. SNMPv3 Notification**.

8. Select 2. Delete SNMPv3 Notification.
9. Select the number of the notification user you wish to delete.
10. Select **y** to confirm.
11. Select X. **Exit** to return to the SNMP Notification menu.

MANAGING HOSTNAMES

Hostname entries can be added to a single hostfile on your VidyoPortal. These entries are used to map an IP addresses to a specific Hostname or FQDN.

Note:

- Vidyo recommends this feature not replace adding proper records to your internal and external DNS servers. It should only be used to support DMZ deployments where there is no DNS server access from the DMZ and allowing the different servers to properly locate each other.
- The Cluster FQDN of the VidyoPortal can be added to the hostfile to avoid making DNS queries from your VidyoManager, VidyoRouter, and VidyoProxy to the same VidyoPortal on which they reside. If you use the same Public FQDN as your Cluster FQDN, then it is not necessary to add the Cluster FQDN to your hostfile.

To manage hostnames:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select **m. ... (more options)**.
3. Select **A. Advanced Options**.

4. Select 5. Hostname Management.

```

Host Entries
-----
1> 10.10.10.1           example.com
*** end ***
=====
[1]-Add [2]-Remove [3]-Remove All [N]-Next [P]-Previous [X]-Exit
-----
```

The Host Entries screen appears. Use this screen to Add, Remove, or Remove All (hostnames); navigate hostnames using Next or Previous; and Exit the Host Entries screen.

5. Select [X]-Exit to return to the Advanced Options menu.

Adding a Hostname

To add a hostname:

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

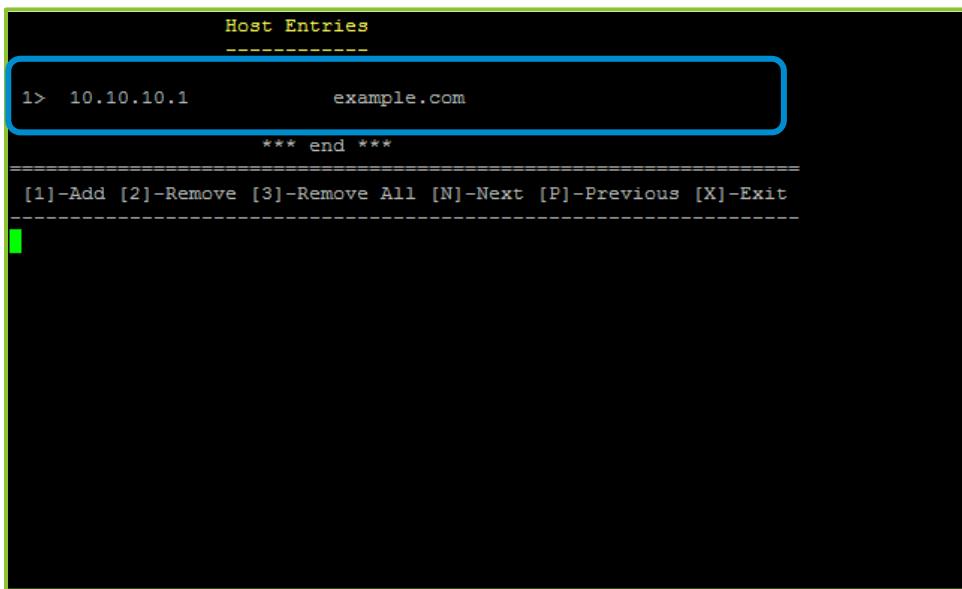
2. Select m. ... (more options).
3. Select A. Advanced Options.
4. Select 5. Hostname Management.
5. Select [1]-Add to add a Hostname.
6. Enter the following information:

- **Hostname/FQDN** – Enter a Hotname or FQDN you want to map to a specific IP address.
- **IP Address** – Enter the IP address you want to map to the specific Hostname or FQDN.

Note: If you want to cancel adding your Hostname, press enter while providing no Hostname/FQDN or IP Address information. The system tells you that you must provide valid information and to press any key. Press any key to return to the Host Entries screen.

7. Select y to confirm the change and add your Hostname.

Your Hostname is then listed and numbered on the top of the Host Entries screen.



The screenshot shows a terminal window titled "Host Entries". It displays one host entry: "1> 10.10.10.1 example.com". Below the entry, it says "*** end ***". At the bottom, there is a menu with options: "[1]-Add [2]-Remove [3]-Remove All [N]-Next [P]-Previous [X]-Exit". A blue rectangle highlights the first two entries of the host list.

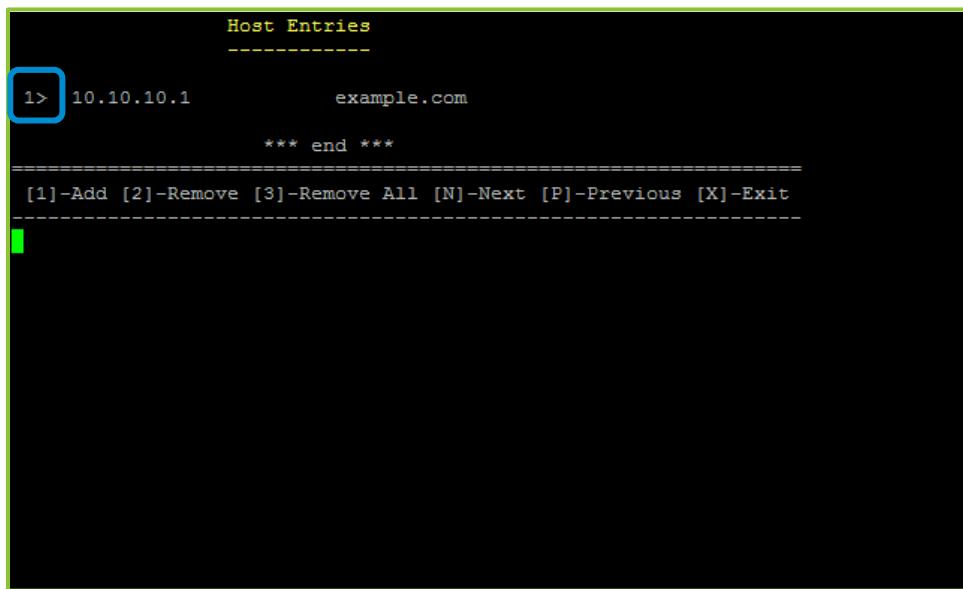
8. Select **[X]-Exit** to return to the Advanced Options menu.

Removing a Hostname

To remove a hostname:

1. Log in to the System Console.
For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
2. Select **m. ... (more options)**.
3. Select **A. Advanced Options**.
4. Select **5. Hostname Management**.
5. Select **[2]-Remove** to remove a Hostname.

- Enter the corresponding number of the Hostname you want to remove.



```

Host Entries
-----
1> 10.10.10.1      example.com
*** end ***
=====
[1]-Add [2]-Remove [3]-Remove All [N]-Next [P]-Previous [X]-Exit
=====
```

- Select **y** to confirm removing the selected Hostname.
- Select **[X]-Exit** to return to the Advanced Options menu.

Removing all of Your Hostnames

To remove all of your hostnames:

- Log in to the System Console.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Select **m. ... (more options)**.
- Select **A. Advanced Options**.
- Select **5. Hostname Management**.
- Select **[2]-Remove all** to remove all of your Hostnames.
- Select **y** to confirm removing all of your Hostnames.
- Select **[X]-Exit** to return to the Advanced Options menu.

Navigating Your Hostnames

To navigate your hostnames:

- Log in to the System Console.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Select **m. ... (more options)**.
- Select **A. Advanced Options**.

4. Select **5. Hostname Management**.
 - a. Select **[N]-Next** to navigate to the next Hostname.
 - b. Select **[P]-Previous** to navigate to the previous Hostname.
5. Select **[X]-Exit** to return to the Advanced Options menu.

LOGGING IN TO THE SUPER ADMIN PORTAL

Now that you have connected your Vidyo Server to the network, you must log in as the Super Admin and configure the VidyoPortal in order to ensure that it can function within your VidyoConferencing system.

To log in as the Super Admin:

1. Enter the IP address or FQDN (Fully Qualified Domain Name) for the VidyoPortal in the address bar of a web browser, followed by a forward slash and the word “super”:
http://<IP or FQDN>/super
2. Log in using the new password that you have set. Otherwise, log in using the default Super Admin user name and password:

User Name: **super**

Password: **password** (case sensitive)

Checking the Status of the Components

To check the status of the components:

1. Log in to the Super Admin portal using your Super Admin account.
 For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.

The Components table appears.

Components							
Component Name:	Type:	All					
Status	Name	Type	IP	Config Version	Software Version	Alarm	
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	24 / 24	TAG_VCS3_1_0_037		
UP	Local VM	VidyoManager	172.20.4.125	4 / 3	TAG_VCS3_1_0_037		
UP	Local VP	VidyoProxy	172.20.4.125	10 / 0	TAG_VCS3_1_0_037		
DOWN	vg484	VidyoGateway	172.16.4.84		3.0.0(96)		

3. Verify that the VidyoManager component has a Status of **UP**.

REQUESTING SYSTEM LICENSES AND APPLYING SYSTEM LICENSE KEYS

The next step in your initial system configuration is to request Vidyo licenses and then apply the license keys to your system.

Requesting Your Vidyo Licenses

After purchasing your license, if you're running VidyoPortal Virtual Edition or the Hot Standby software option, you'll receive Fully Qualified Domain Name (FQDN) licenses (removing license dependency to your Vidyo hardware). Otherwise, you'll receive System ID-based licenses (licenses tied to your Vidyo hardware).

Note:

- By default, you will receive System ID-based license unless you are running VidyoPortal Virtual Edition or using the Hot Standby software option. Using VidyoPortal Virtual Edition or the Hot Standby software option requires an FQDN license.
- Existing customers with System ID-based licenses using VidyoPortal Virtual Edition or the Hot Standby software option can be converted to FQDN license by contacting Vidyo Support.
- System ID-based licenses and FQDN-based licenses were sent to the email address you provided when making your purchase. However, if you do not possess these licenses, you may request them after providing your configured system information and using the procedures in this section.

The Vidyo licensing team usually sends keys out within one business day from the time you submit the required information from the Vidyo website form. Licenses are sent to the email address you provided.

If you have any licensing questions please contact Vidyo's license team with your MAC address, System ID, and Public FQDN at lincenses@vidyo.com.

Requesting Vidyo System ID-Based Licenses

System ID-based licenses and FQDN-based licenses were sent to the email address you provided when making your purchase. However, if you do not possess these licenses, you may request them after providing your configured system information and using the procedures in this section.

To request Vidyo System ID-based licenses:

1. If you did not receive an email containing your System ID-based licenses after order processing, request them from the Vidyo license team with your MAC address, System ID, and Public FQDN at lincenses@vidyo.com.

Otherwise, if you did receive an email containing your System ID-based licenses after order processing, proceed by applying the license keys to your system. For more information, see "Applying System License Keys to your System" on page [64](#).

2. Submit your system information using the form on the Vidyo website.

Requesting Vidyo FQDN-Based Licenses

If you're running the VidyoPortal Virtual Edition or the Hot Standby software option and were able to provide your FQDN at the time of purchase, your FQDN-based licenses were sent to the email address you provided at that time. However, if you do not possess these licenses, you may request them after providing your configured system information and using the procedures in this section.

To request Vidyo FQDN-based licenses:

1. If you were unable to provide an FQDN for your license at the time of purchase, contact the Vidyo license team with your MAC address, System ID, and Public FQDN at licenses@vidyo.com.
Otherwise, if you did provide an FQDN when ordering, your license keys were provided in the email sent to you after order processing. For more information, see "Applying System License Keys to your System" on page [64](#).
2. Submit your system information using the form on the Vidyo website.

Applying the System License Keys to Your System

Your VidyoPortal ships with factory default licensing. You need to apply your full Vidyo system license keys in order to access the license quantities and options purchased. The procedure for doing this varies depending on whether or not you are running the Hot Standby software option. For complete information about applying your licenses, see "Applying System License Keys to Your System" section on page [64](#) and "Applying System License Keys to Your System Using the Hot Standby Software Option" section on page [67](#).

SETTING THE LANGUAGE FOR THE SUPER ADMIN INTERFACE

The VidyoPortal's Super Admin interface is available in these 14 languages:

- English
- Chinese (Simplified)
- Chinese (Traditional)
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish
- Thai

You can set the language of your Super Admin portal in either of these two ways:

- You can use the drop-down on the upper right corner of the Super Admin Login page (before or after logging into the system).
- You can use the Settings > Super Account screen from inside the Super Admin Portal.

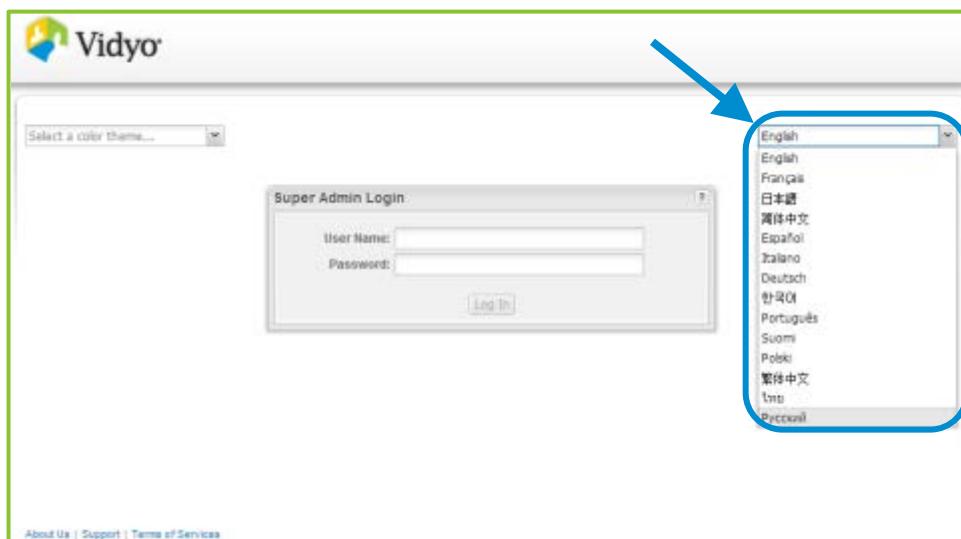
Note:

- You can also change the color scheme of your Super Admin portal using the **Select a color scheme...** drop-down on the upper left corner of the Super Admin Login page before logging into the system.
- Interfaces are immediately modified after selecting your preferred language or color scheme using the drop-downs.
- Preferred language changes to the Super Admin interface have no effect on the Admin and Vidyo-Desktop interfaces.

Setting Your Preferred Language Using the Upper-Right Drop-Down Outside the System

To set your preferred language using the drop-down on the upper-right corner of the Super Admin Login page:

- Select your desired language using the language drop-down on the upper right corner of the Super Admin Login page.

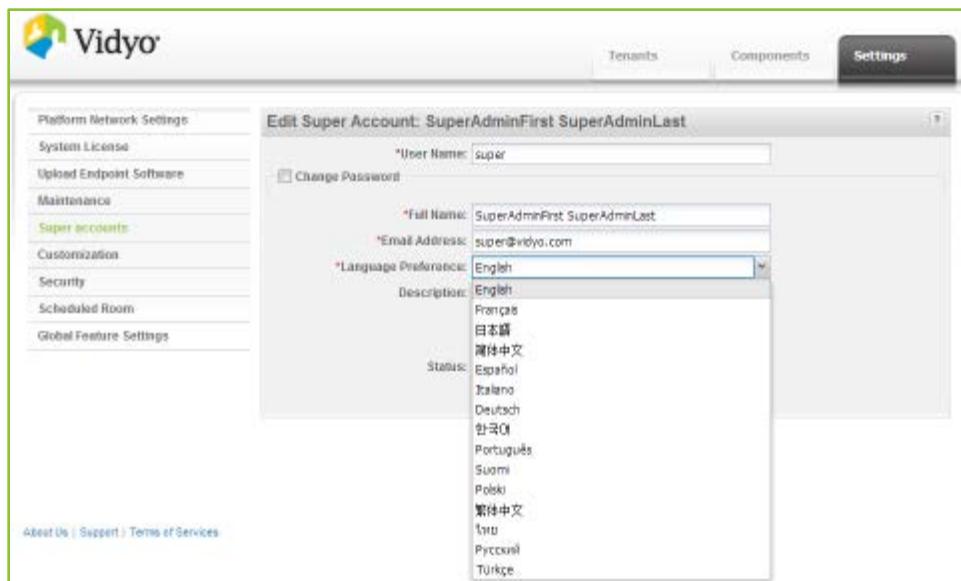


Setting Your Preferred Language from Settings > Super Account Inside the System

To set your preferred language from Settings > Super Account inside the system:

- Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
- Click the **Settings** tab.
- Click **Super Account** on the left menu.

4. Select the Super Admin's language from the Language Preference drop-down menu.



5. Click **Save**.

You are automatically logged out of the Super Admin Portal.

ADDING MULTIPLE SUPER ADMIN ACCOUNTS

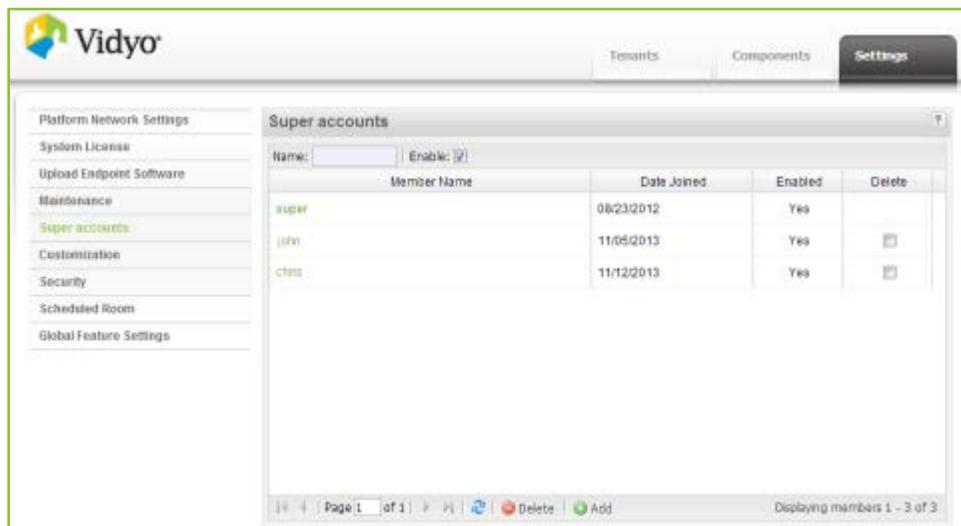
Super Admins can create and delete multiple Super Admin accounts.

To add multiple Super Admin accounts:

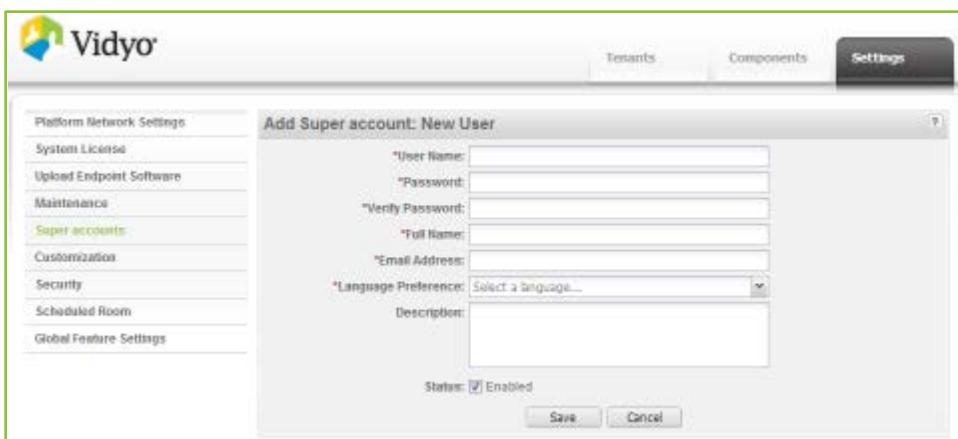
1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page 35.

2. Click the **Settings** tab.
3. Click **Super accounts**.



4. Click the **Add** button to add a new Super Admin account.



5. Enter field values for your new Super Account.

Caution: Each Super Account is required to have a valid, resolvable, email address in order to function properly in your VidyoConferencing system.

Note: Fields marked with an asterisk cannot be left blank.

6. Select the **Enabled** check box to enable the account.

7. Click **Save**.

Note: For information about super accounts, see “Managing Your Super Accounts” on page [86](#).

5. Enabling the Management Interface

VidyoPortal, VidyoRouter, and VidyoGateway allow for the configuration of a secondary Ethernet interface that can be used to access the management capabilities of the system. The secondary Ethernet interface is typically on a segregated network from the main production interface.

You can move the following configuration pages so that they are only accessible over the Management Interface:

- VidyoPortal’s vm2conf
- VidyoPortal and VidyoRouter’s vr2conf
- VidyoPortal and VidyoRouter’s vp2conf
- VidyoPortal’s Super Admin
- VidyoPortal’s Tenant Admin
- VidyoGateway’s Admin

As shown in the following table, the Management Interface is referred to by different names on the physical interface of the server and on the System Console and the Super Admin interface on the Settings > Security > Applications tab:

Physical Interface	The System Console and The Super Admin Applications Tab
GB1	PRODUCTION
GB2	MANAGEMENT

Note:

- If the Management Interface is enabled, SNMP is only available on the Management Interface.
- The Management Interface should not be used to transfer any media. Doing so will result in failed calls.

The following sections show you how to enable the management interface in the system console and then move VidyoPortal, VidyoRouter, and VidyoGateway applications to the Management Interface.

To enable the Management Interface:

1. Log in to the System Console.
For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
2. Enter option 1 to select Configure IP Address.

3. Select **y** to change the current settings.

```
Select Network Interface to Configure
-----
1. PRODUCTION INTERFACE
2. MANAGEMENT INTERFACE
X. Exit

Enter 1, 2 or x: [cursor]
```

4. Select **2. MANAGEMENT INTERFACE**.
5. Enter the IP address and Subnet Mask for the Management Interface.
Note: The Management Interface supports only IPv4 addresses.
6. Select **y** to save the configuration.
7. Select **14** to reboot the server.

MOVING VIDYOPORTAL APPLICATIONS TO THE MANAGEMENT INTERFACE

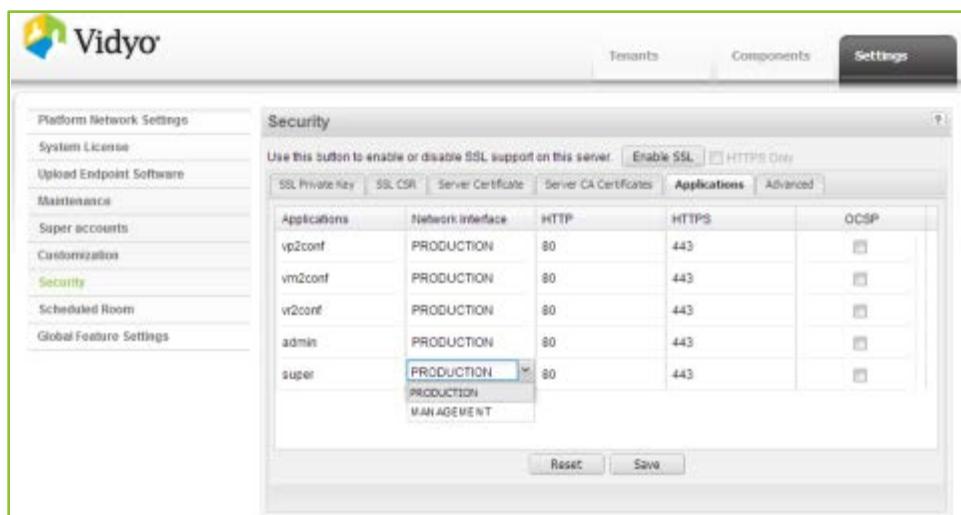
After enabling the Management Interface on a VidyoPortal, all applications will still reside on the Production Interface unless explicitly moved to the Management Interface.

Note: Unlike applications which you must explicitly move to the Management Interface, SNMP will be automatically moved to the Management Interface as soon as the Management Interface is enabled on the VidyoPortal.

To move VidyoPortal applications to the Management Interface:

1. Log in to the Super Admin portal using your Super Admin account.
2. Click the **Settings** tab.
3. Click **Security**.

- Click the Applications tab.



- Look in the Applications column for the application you want to move to your VidyoPortal Management Interface, and then select **MANAGEMENT** from the drop-down.

You can select and move multiple applications at the same time.

Note: The User portal (user application) cannot be moved to the Management Interface; it must remain on the Production Interface (PRODUCTION).

- Optionally, you can also change the Port to which an application is bound.

In the preceding screenshot, some applications are bound to port 443.

- Click **Save**.

Changes are applied immediately; therefore, if the Super application is moved, you are logged out and it is no longer accessible from the Production Interface (PRODUCTION).

THE MANAGEMENT INTERFACE ON VIDYOROUTER AND VIDYOGATEWAY

Moving Your VidyoRouter Applications to the Management Interface

Now you can explicitly move your VidyoRouter applications to the Management Interface.

Note: Unlike applications which you must explicitly move to the Management Interface, SNMP will be automatically moved to the Management Interface as soon as the Management Interface is enabled on the VidyoPortal.

To move your VidyoRouter applications to the Management Interface:

- Log in to your VidyoRouter using your system console account.

The URL of each VidyoRouter is typically a subdomain followed by your domain name and the address of the VidyoRouter Configuration page: <yourVidyoRouter.yourorganization.mil>/vr2conf.

- Click the **Settings** tab.

3. Click **Security**.
4. Click the **Applications** tab.

The screenshot shows the Vidyo Management Interface with the 'Settings' tab selected. Under the 'Security' tab, there is a table listing applications and their network interfaces. One row for the application 'super' has a dropdown menu open, showing 'PRODUCTION' and 'MANAGEMENT' as options. Other applications listed include vp2conf, vm2conf, vr2conf, admin, and super. The 'MANAGEMENT' option is highlighted in the dropdown.

Applications	Network Interface	HTTP	HTTPS	OCSP
vp2conf	PRODUCTION	80	443	<input type="checkbox"/>
vm2conf	PRODUCTION	80	443	<input type="checkbox"/>
vr2conf	PRODUCTION	80	443	<input type="checkbox"/>
admin	PRODUCTION	80	443	<input type="checkbox"/>
super	PRODUCTION	80	443	<input type="checkbox"/>
	MANAGEMENT			<input type="checkbox"/>

5. Look in the Applications column for the application you want to move to your VidyoRouter Management Interface, and then select **MANAGEMENT** from the drop-down.

You can select and move multiple applications at the same time.

Note: The User portal (user application) cannot be moved to the Management Interface; it must remain on the Production Interface (PRODUCTION).

6. Optionally, you can also change the Port to which an application is bound.

In the preceding screenshot, some applications are bound to port 443.

7. Click **Save**.

Changes are applied immediately; therefore, if the Super application is moved, you are logged out and it is no longer accessible from the Production Interface (PRODUCTION).

Moving Your VidyoGateway Application to the Management Interface

Now you can explicitly move your VidyoGateway application to the Management Interface.

Note: Unlike applications which you must explicitly move to the Management Interface, SNMP will be automatically moved to the Management Interface as soon as the Management Interface is enabled on the VidyoPortal.

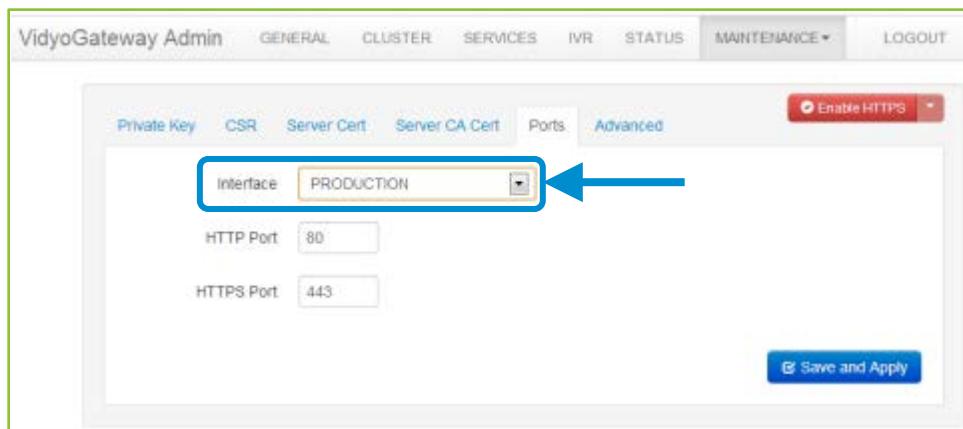
To move a VidyoGateway application to the Management Interface:

1. Log in to your VidyoGateway using your system console account.

The URL of your VidyoGateway is typically a domain name: <somevidyogateway.com>/.

2. Click the **Maintenance** tab.
3. Click **Security**.
4. Click the **Ports** tab.

- Select **MANAGEMENT** from the Interface drop-down.



- Optionally, you can also change the Port to which your VidyoGateway is bound.

In the preceding screenshot, the VidyoGateway is bound to port 443.

- Click **Save and Apply**.

Changes are applied immediately; therefore, if your VidyoGateway Admin is moved, you are logged out and it is no longer accessible from the Production Interface (PRODUCTION).

ADDING STATIC NETWORK ROUTES

With the addition of the Management Interface capability, the System Console allows you to add static network routes to the system.

To add static network routes to the system:

- Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

- Select **m. ... (more options)**.
- Select **A. Advanced Options**.

4. Select 2. Network Route Management.

```
Static Route Configuration
-----
1. Add route
2. Remove route
3. Display route
X. Exit

Enter 1,2,3 or X: [ ]
```

5. Enter **1** to add a new route.
6. Enter the Destination IP or Network (using Slash notation for the subnet mask).
7. Enter the IP address of the route you want to use.

```
Static Route Configuration
-----
1. Add route
2. Remove route
3. Display route
X. Exit

Enter 1,2,3 or X: 1

Create new route
=====

Destination IP: 10.10.10.0/24
Via: 172.16.41.1

Route successfully created.

Confirm changes ? [y/n] [ ]
```

8. Select **y** to confirm your changes.

6. Configuring System Settings as the Super Admin

This chapter explains how the System Administrator configures functions under the Settings tab in the Super Admin Portal. Configurations made by the Super Admin using the Super Admin portal are globally applied to your VidyoConferencing system and are done in a specific order.



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

- System licenses
- Endpoint software
- Maintenance
- Super Account (login)
- Customization
- Inter-Portal Communication
- VidyoMobile access

Hot Standby (only visible once the Hot Standby license is applied and Hot Standby has been configured via the System Console menu)

To make these configurations, you must log in to the Super Admin portal using your Super Admin account. For more information, see “Logging in to the Super Admin Portal” on page [35](#).

CHECKING YOUR PLATFORM NETWORK SETTINGS

You must configure your network settings using the System Console prior to performing your system setup. For more information, see “Configuring the Network Settings at the System Console” on page [25](#). If you haven’t yet configured your network settings, complete that section before proceeding.

Platform Network Settings shows (read only) the settings you made using the System Console. The data is blurred in the following screenshot.



APPLYING SYSTEM LICENSE KEYS TO YOUR SYSTEM

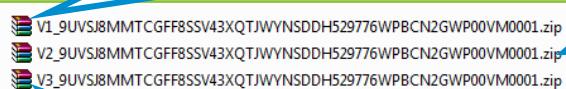
Your VidyoPortal ships with factory default licensing. You need to apply your full Vidyo system license keys in order to access the license quantities and options you purchased.

Note:

1. If you do not possess these licenses, you may request them after providing your configured system information. For more information, see “Requesting Vidyo System Licenses” on page [51](#).
2. The procedure differs for applying system license keys to your system if you are running the Hot Standby software option. For more information, see “Applying System License Keys to Your System Using the Hot Standby Software Option” on page [67](#).
3. System ID-based licenses and FQDN-based licenses were sent to the email address you provided when making your purchase. However, if you do not possess these licenses, you may request them after providing your configured system information. For more information, see “Requesting Your Vidyo Licenses” on page [51](#).

You will receive an email from Vidyo Customer Support to the address you provided with your purchase order from the license request web page. This email contains a single .zip archive containing specific files based on the VidyoPortal version you are running as follows:

Users running VidyoPortal versions earlier than 3.0 are sent a .zip archive prefixed with “v1” containing a **vmlicense.XXXX...** VidyoManager license file and **syslicense.XXXX...** license file.



Users running VidyoPortal version 3.0 or 3.1 are sent a .zip archive prefixed with “v2” containing a **v2.vmlicense.XXXX...** VidyoManager license file and **v2.syslicense.XXXX...** license file.

Users running VidyoPortal version 3.2 or later are sent a .zip archive prefixed with “v3” containing a **v3.license.XXXX...** license file.

6. Configuring System Settings as the Super Admin

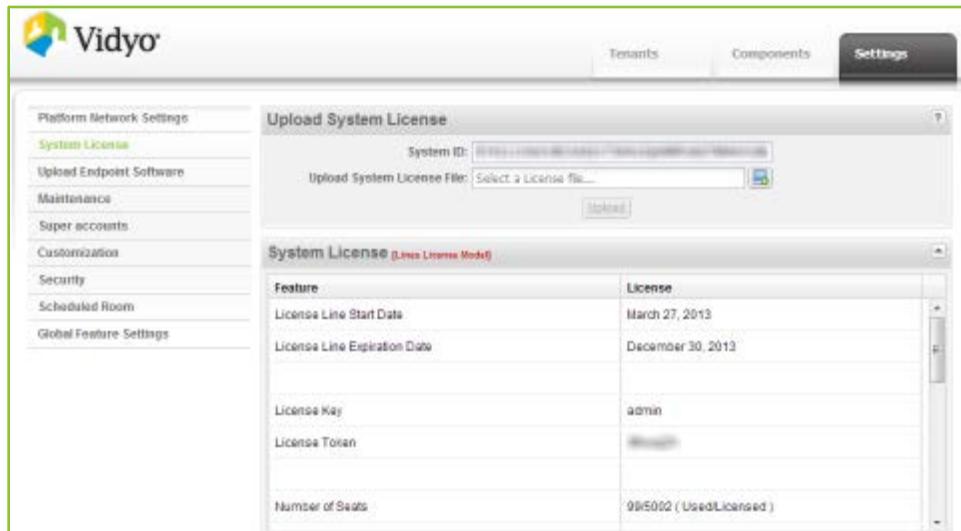
The email also includes a license information text file that includes license information details. This file is prefixed with “LicenseInfo.”.

Your VidyoPortal system-wide license defines the term (length) of your license, the number of VidyoLines and installations available for use as well as whether it is:

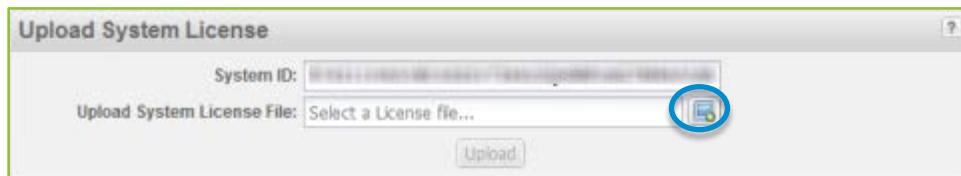
- A single- or multi-tenant system
- Licensed for UC integration, encryption, Hot Standby, Executive lines, and APIs (the API license is also used to enable Adobe Connect integration).

To apply the system license keys to your system:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **System License** on the left menu.



4. Click **Select File**, which is located to the right of the Upload System License File field.



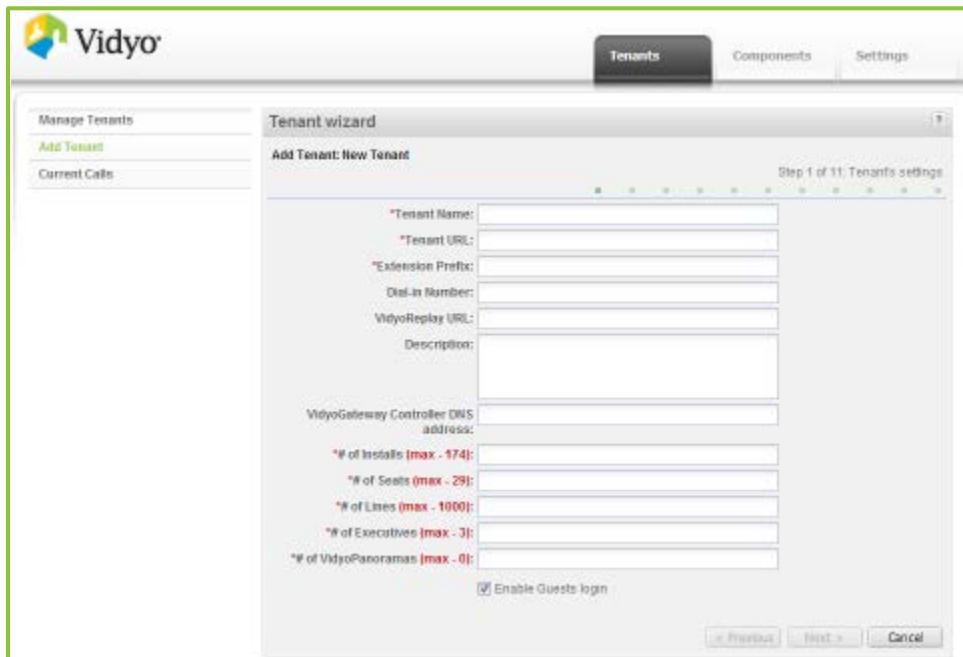
5. If you are running a VidyoPortal version earlier than 3.2, upload your VidyoManager license:
 - a. Select the appropriate VidyoManager license file based on the VidyoPortal version you are running.

Note:

- The VidyoManager license file for users running VidyoPortal version 3.0 or 3.1 is prefixed with “v2” and contains **vmlicense** in the name.

6. Configuring System Settings as the Super Admin

- The VidyoManager license file for users running VidyoPortal versions earlier than 3.0 contains **vmlicense** in the name and has no “vx” prefix.
 - The **vmlicense** file must be uploaded before the **syslicense**.
- b. Click **Upload** to apply the VidyoManager license.
6. For all VidyoPortal versions, upload the license file:
- a. Select the appropriate license file based on the VidyoPortal version you are running.
- Note:**
- The license file for users running VidyoPortal version 3.2 or later is prefixed with “v3.”
 - The license file for users running VidyoPortal version 3.0 or 3.1 is prefixed with “v2” and contains **syslicense** in the name.
 - The license file for users running VidyoPortal versions earlier than 3.0 contains **syslicense** in the name without a “vx” prefix.
- b. Click **Upload** to apply the license.
7. Click the Tenants tab and edit the Default Tenant by clicking the **Default Tenant Name**. If you are using the MultiTenant Add-on, see the note about MultiTenant License Allocation below the following illustration.
8. Allocate the full set of licenses to the Default Tenant.



9. Click **Next** through the remaining screens and then click **Save**.

10. Restart the VidyoPortal Web Server for the licensing changes to take effect.

For more information, see “Restarting Your System” on page [81](#).

Applying System License Keys to Your System Using the Hot Standby Software Option

Your VidyoPortal ships with factory default licensing. You need to apply your full Vidyo system license keys in order to access the license quantities and options you purchased. If you do not possess these licenses, you may request them after providing your configured system information. For more information, see “Requesting Vidyo System Licenses” on page [51](#).

The way you apply Vidyo FQDN-based licenses vary based on whether they are being applied when you are initially configuring both your system and the Hot Standby software option or you are applying add-on licenses to a system already synchronizing via the Hot Standby software option. The following sections explain both procedures.

Note:

- If you currently have a Vidyo System ID-based license with Hot Standby, and you’re now running VidyoPortal 3.0, you’ll be required to upgrade to a Vidyo FQDN-based license when you make your next license Add-on purchase.
- And all new Hot Standby software option purchases are issued with a single FQDN-based license for both VidyoPortals.

Applying Vidyo FQDN-Based Licenses When Initially Configuring Both Your System and The Hot Standby Software Option

The following procedure should only be used if you are performing an initial system setup with the Hot Standby software option.

To applying Vidyo FQDN-based licenses when performing an initial system setup with the Hot Standby software option:

1. Perform the steps as explained in the previous section on both of your VidyoPortals. For more information, see “Applying System License Keys to Your System” on page [64](#).

Apply the same FQDN-based license on both of your VidyoPortals.

Note: If you have a Vidyo System ID-based license, contact Vidyo Support for a Vidyo FQDN-based license instead.

For more information about Hot Standby, see “Hot Standby” on page [342](#).

Applying Add-on Licenses to a System Already Synchronizing via the Hot Standby Software Option

An add-on license may be additional client installations, features, and extensions.

Note: Make sure you’ve already configured Hot Standby on your system and it’s running properly. For more information, see “Hot Standby” on page [342](#).

To apply add-on licenses to a system already synchronizing via the Hot Standby software option:

1. Log in to the Super Admin portal using your Super Admin account on your Active VidyoPortal.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Perform the steps as explained in the previous section on your Active VidyoPortal. For more information, see Applying System License Keys to Your System” on page [64](#).

The license replicates to your Standby VidyoPortal automatically.

Note: You can also replicate your license immediately by clicking **Sync Now** in the **Settings > Hot Standby > Database Synchronization** tab on your Active VidyoPortal. For more information, see “Scheduling the Database Synchronization” on page [365](#).

Understanding Vidyo License Consumption by User Type

	VidyoLines Licensing Model
User Type	VidyoLines*
Super Admin	–
Admin	✓
Operator	✓
Executive Desktop	–
Normal User	✓
Guest	✓
VidyoRoom (used for Vidyo-Room as well as for VidyoPanorama 600)	–
VidyoGateway	–
VidyoPanorama 1.0	–

* In the VidyoLines licensing model all users with a checkmark consume a line for all calls.

Understanding Licensing Notifications

If you provided one or more licensee addresses when purchasing, they are embedded into your license.

The Super Admin and Admin and Tenant Admins receive a license warning when only 25 installs remain. If you don’t purchase additional installation licenses, you’ll receive additional warnings at 15, and another at five installations left. Your current installs never expire. If you run out, you won’t be able allow any new users who need to install the software until you purchase more.

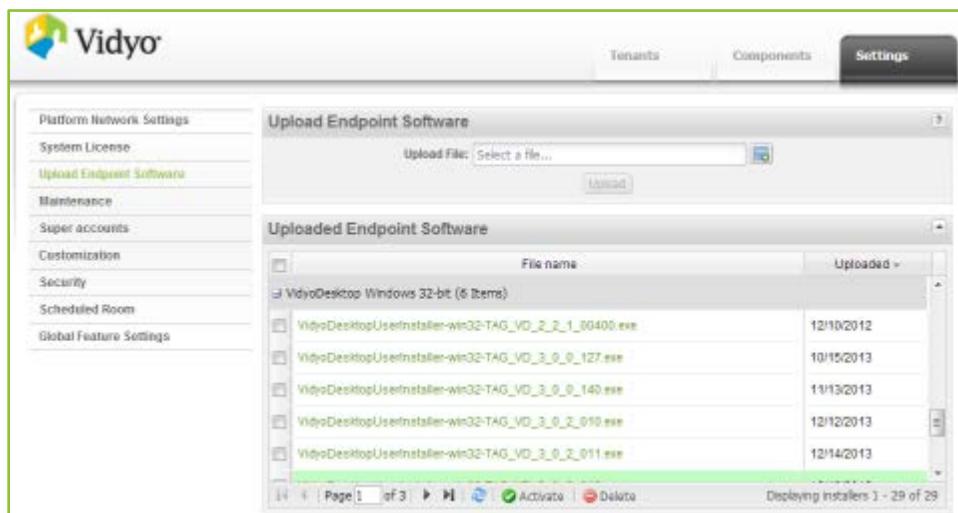
UPLOADING ENDPOINT SOFTWARE

You may choose to perform installations directly on user machines. However, most administrators prefer having users install their VidyoDesktop software by accessing VidyoPortal using the user name and password you assign them.

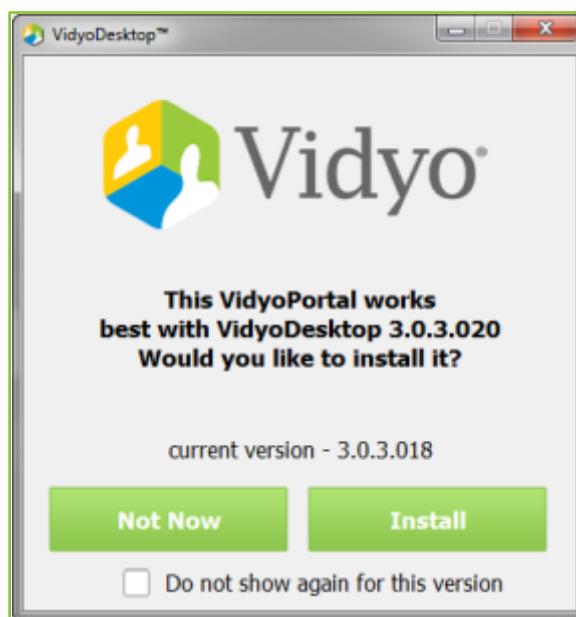
6. Configuring System Settings as the Super Admin

When your users access the VidyoPortal, the VidyoDesktop software is installed even if users do not have administrator privileges. (The Windows installer places the VidyoDesktop-related files in a user-specific directory called “AppData”.)

When new versions of the VidyoDesktop and VidyoRoom client software become available from Vidyo, you can provide this software to your users by uploading the new software to your servers using the Upload Endpoint Software page. A Tenant Admin user can also upload Vidyo client software for users on their own tenant. This helps the Tenant Admin decide when they want to make endpoint software available for their own users.



By doing this, your users are automatically prompted to download the new version the next time they log in. Users can choose to not update their software or install the update, if desired.



Installation files for various client types include the following:

- VidyoDesktop for Windows

- VidyoDesktop for Macintosh OS X
- VidyoDesktop for Linux

There can be up to four active Linux clients. If the bit architecture the distribution is meant for isn't in the name then, it's the 32-bit version. If the distribution is meant for 64-bit machines, the file is named accordingly.

- VidyoRoom

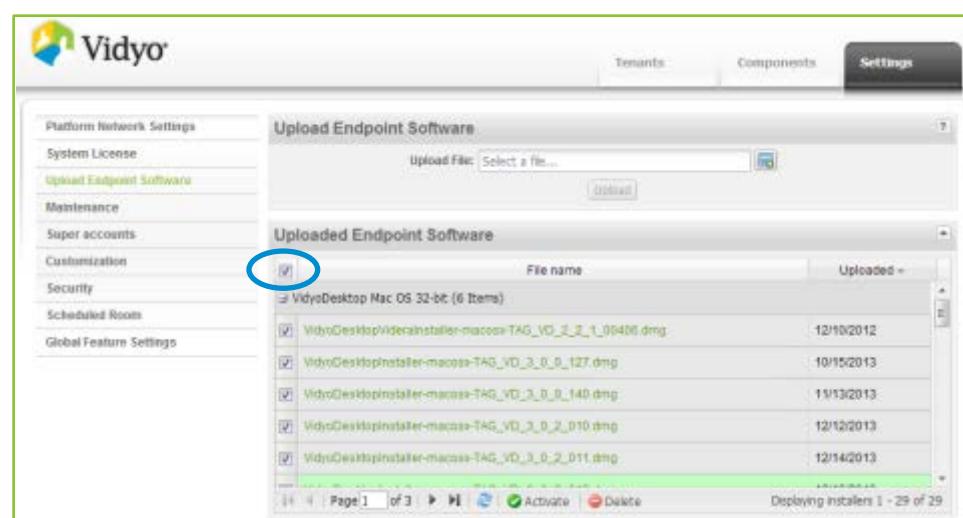
In the Upload Endpoint Software page, you can upload up to four different versions of each type of endpoint software (VidyoDesktop for Macintosh, VidyoDesktop for PC and so on), but for each type you must make just one active. (Again, Linux is the exception. Up to four Linux versions can be active.) 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 endpoint software installation files:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Settings** tab.
3. Click **Upload Endpoint Software** on the left menu.
4. Click the **System Upgrade** tab.
5. Remove any previously uploaded clients, if needed:
 - a. Select all the previously uploaded clients by selecting the check box to the left of “File name”.



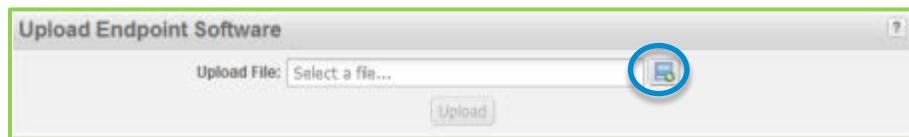
- b. Click **Delete**.

Note: If you uploaded any client software via the Tenant Admin portal, remove those clients via the Tenant Admin portal by going to <http://<Tenant FQDN>/admin> and selecting **Settings > Upload Endpoint Software**.

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

The link is provided to you by your reseller or by Vidyo Customer Support.

7. Click Select File.



8. Select the installation file and click Upload to import it.

Note:

- To avoid failure messages, make sure you are uploading Vidyo software only. The software file name ends with an .exe extension for Windows and VidyoRoom and .dmg for Macintosh.
- Vidyo recommends 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.

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.

	File name	Uploaded
<input checked="" type="checkbox"/>	Installer-HD50/100/220 (4 Items)	
<input checked="" type="checkbox"/>	Installer-Win32 (3 Items)	
<input type="checkbox"/>	VidyoDesktopDoDInstaller-win32-TAG_VD_2_1_0_00383.exe	10/01/2012
<input type="checkbox"/>	VidyoDesktopDoDInstaller-win32-TAG_VD_2_2_3_00424.exe	04/21/2013
<input type="checkbox"/>	VidyoDesktopDoDInstaller-win32-TAG_VD_2_2_3_00427.exe	05/29/2013

From the Uploaded Endpoint Software table, you can Activate an installer for your users or Delete installers from the list.

Activating an Endpoint Installation File

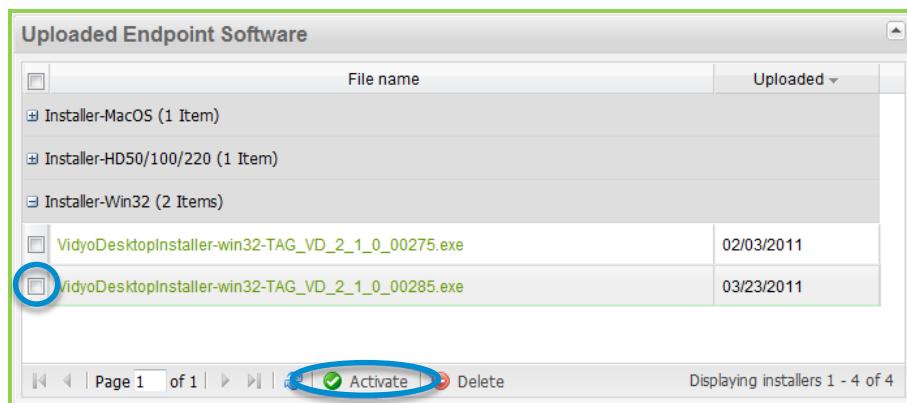
To activate an endpoint installation file:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Upload Endpoint Software** on the left menu.
4. Select the check box to the left of the file name you wish to activate.

Tip: Use the top-left check box to select or clear all of the software file check boxes.

5. Click **Activate** at the bottom of the list.

The file name appears highlighted in green.



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. (Again, Linux is the exception. Up to four Linux versions can be active.) It is the active version that downloads automatically for VidyoPortal users when they first use the system or upgrade to a new version.

Deleting an Endpoint Installation File

To delete an endpoint installation file:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Settings** tab.
3. Click **Upload Endpoint Software** on the left menu.
4. Select the check box to the left of the file name you wish to delete.

Tip: Use the top-left check box to select or clear all of the software file check boxes.

5. Click **Delete**.

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.

PERFORMING SYSTEM MAINTENANCE

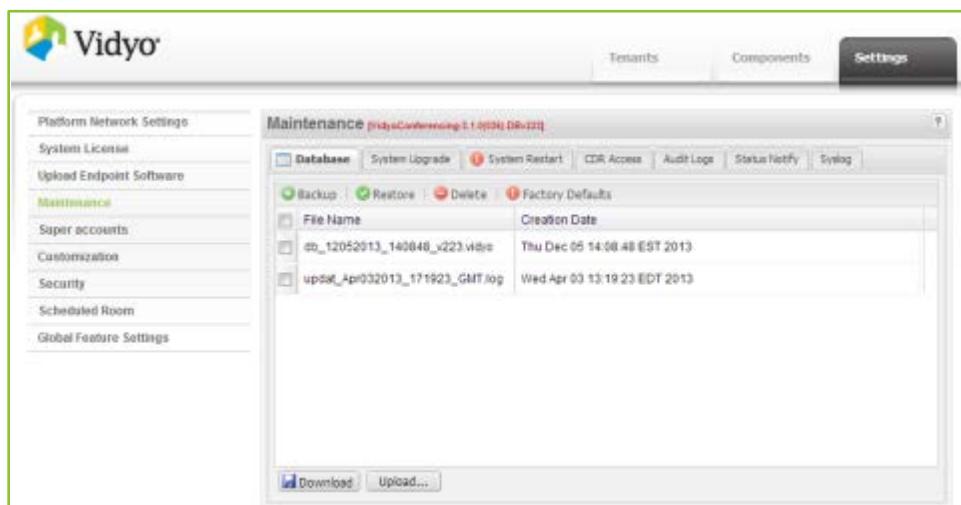
The VidyoPortal database contains everything but the basic network settings of the system (IP, DNS, host-name, NTP), the SSL security certificates loaded and CSR information, and the license keys (each of these would need to be reset separately should a unit need to be replaced/rebuilt). For more information about the CDR database, see “CDR” on page [336](#).

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

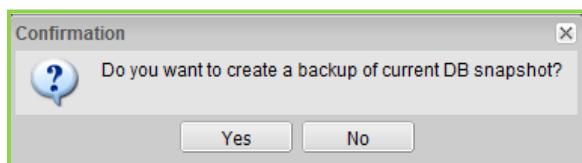
Backing Up the Database

To back up the database:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. Click **Backup** at the top of the database list.

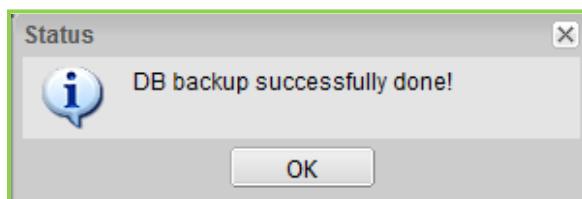


A confirmation dialog box appears.



5. Click **Yes**.

A backup copy of the database is made on the VidyoPortal. A Status dialog box appears confirming a successful backup.



6. Click **OK**.

Caution: 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. Therefore, you should download backups to an offsite computer as described in the following section.

Downloading a Backup File

To download a backup file:

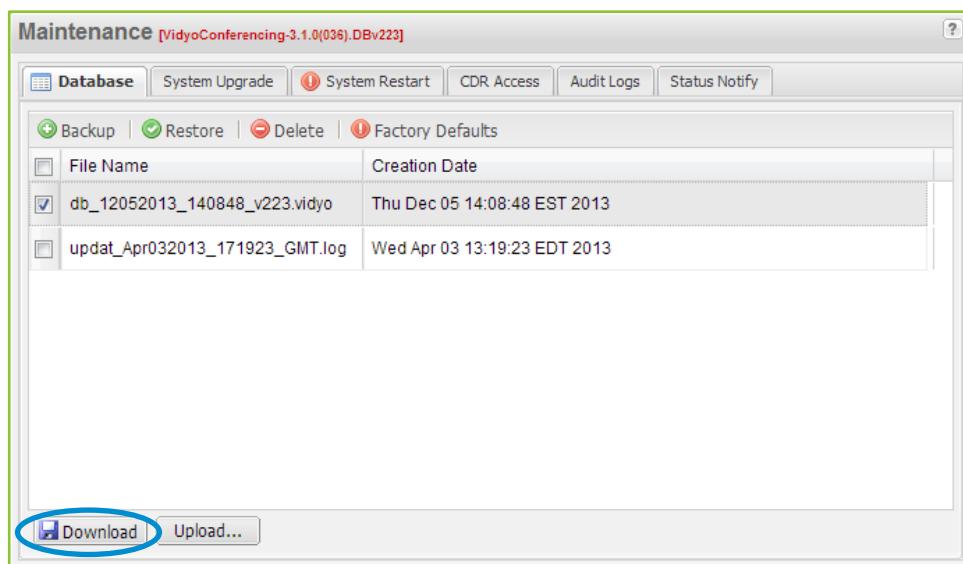
1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

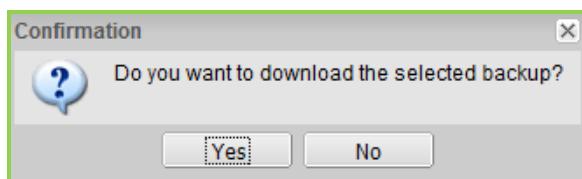
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. Select the check box to the left of the file name you wish to download.

Tip: Use the top-left check box to select or clear all of the software file check boxes.

5. Click **Download**.

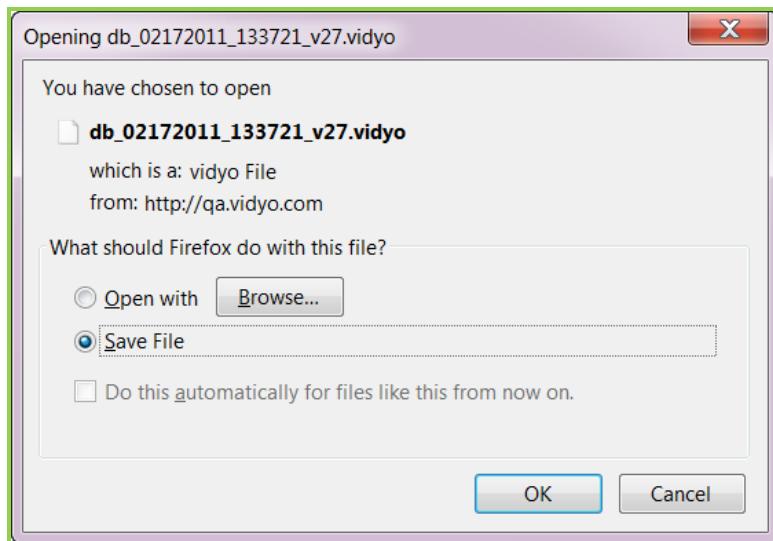


A Confirmation dialog box appears.



6. Click **Yes**.

Your browser's standard Open and Save File dialog box appears.



7. Select **Save File**.
8. Click **OK** to save the database to the location you've set your browser to save files.

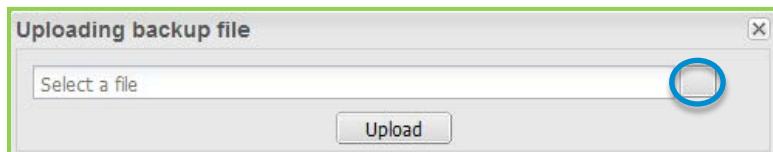
Now that you've downloaded the database, you have a true backup.

Uploading a Backup File

To upload a backup file:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. Click **Upload** beneath the database table.

The Uploading backup file dialog box appears.



5. Click **Select File**.
Your OS's standard File Upload dialog box appears.
6. Locate the file on your computer or other computer on your network.
7. Click **Open** in the File Upload dialog box.

8. Click **Upload** on the Uploading backup file dialog box.

The file uploads and is listed in the Database table.

Restoring a Backup File Located on Your VidyoPortal

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

Note:

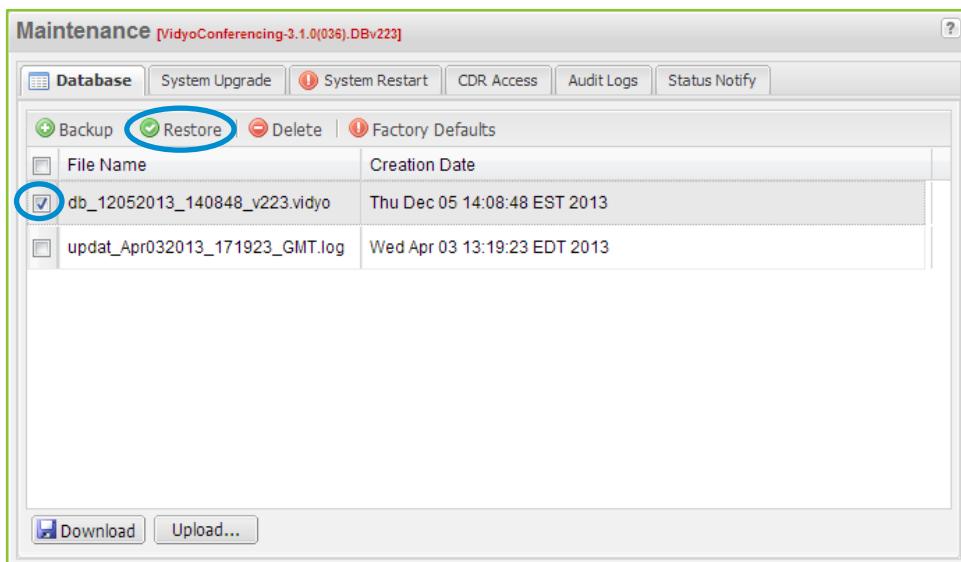
- Vidyo strongly suggests rebooting your VidyoPortal as the final step when restoring a backup database. Make sure you are able to reboot your VidyoPortal before starting to restore a backup database.
- The system license of the database you're restoring must be equal to or greater than the number of Lines allocated to a tenant or.

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

To restore a backup file located on your VidyoPortal:

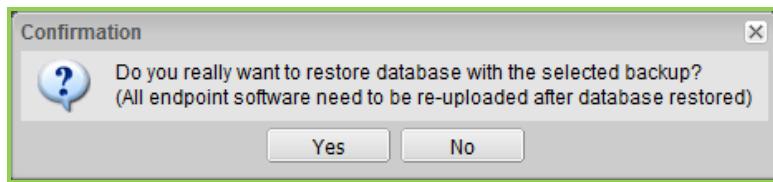
1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. Select the check box to the left of the file name you wish to restore.

Tip: Use the top-left check box to select or clear all of the software file check boxes.



5. Click **Restore**.

A Confirmation dialog box appears.



6. Click **Yes**.
7. Reboot your VidyoPortal.

For steps to reboot your VidyoPortal, see “Restarting the System” on page [80](#).

Restoring a Backup File No Longer on Your VidyoPortal

Note:

- Vidyo strongly suggests rebooting your VidyoPortal as the final step when restoring a backup database. Make sure you are able to reboot your VidyoPortal before starting to restore a backup database.
- The system license of the database you’re restoring must be equal to or greater than the number of Lines allocated to a tenant or.

Caution: The following task destroys the current database file. It’s best to make a backup of the current database file before restoring a prior version.

To restore a backup file no longer on your VidyoPortal:

1. With the desired version of the database on your local machine, follow the “Uploading a Backup File” procedure on page [75](#) to put the file back on the VidyoPortal.
2. Follow the “Restoring a Backup File Located on Your VidyoPortal” procedure on page [76](#).

Deleting a Backup File That’s on the VidyoPortal

Caution: The following task cannot be undone.

To delete unnecessary or outdated versions of the database:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. On the Backup tab, select the check box next to the version you wish to delete.
5. Click **Delete** at the top of the database table.
6. Confirm the action in the dialog box that opens.

Restoring The Database to the Factory Default

Caution: The following task cannot be undone.

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

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. On the Backup tab, click **Factory Defaults** above the database table.
5. Confirm the action in the dialog box that appears.

Upgrading Your VidyoPortal System Software

The System Upgrade tab is used for upgrading the VidyoPortal and VidyoOne software version as well for downloading installation logs history and applying system add-ons (such as SNMP or Hot Standby) or patches.

Before you perform a system upgrade, Vidyo highly recommends that you read the Release Note that pertain to your upgrade version.

The Vidyo upgrade filenames contain the server product abbreviation, version number and/or Add-on/Patch name, and have a **.vidyo** extension (example: **TAG_VC_3_0_0_x.vidyo**).

Caution: Once the VidyoPortal is upgraded, it cannot be reverted back to the previous version or other versions.

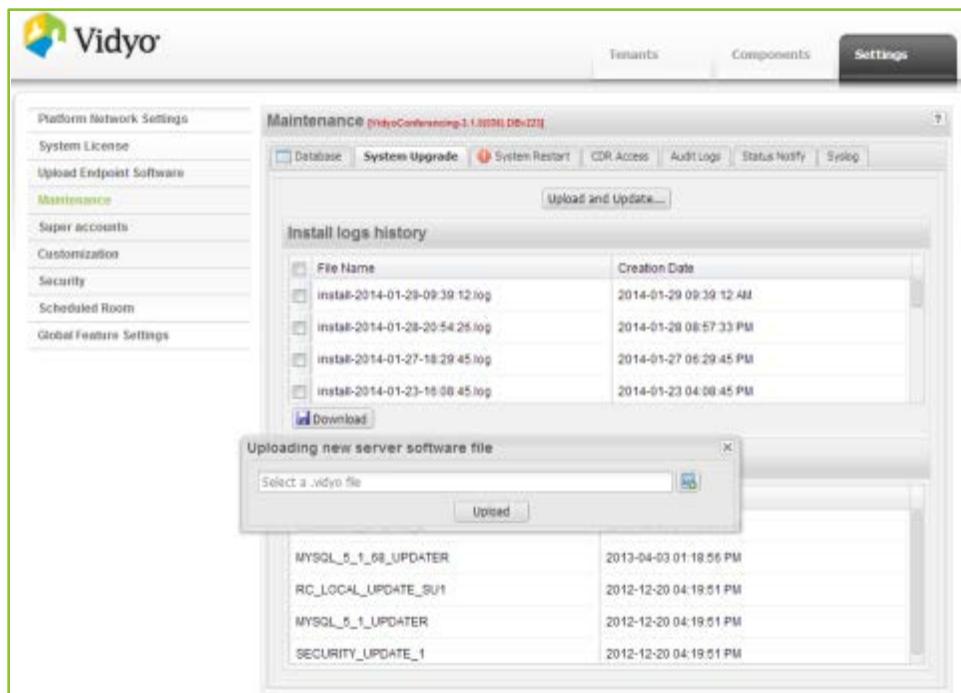
Note:

- The system doesn’t accept a file that’s versioned earlier than the version currently being used on the VidyoPortal, preventing you from accidentally downgrading your software.
- The system only accepts **.vidyo** files signed by Vidyo, protecting you from non-genuine files.
- 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.

To upgrade the VidyoPortal:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.

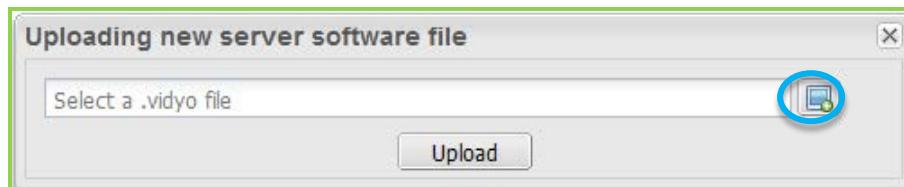
- Click the **System Upgrade** tab.



- Click **Upload and Update**.

The Uploading new server software file dialog box appears.

- Click **Select File**.



Your OS's standard File Upload dialog box appears.

- Locate the **.vidyo** file on your computer or other computer on your network.
- Click **Open** in the File Upload dialog box.
- Click **Upload** in the Uploading new server software file dialog box.

The upload process may take five to fifteen minutes or more depending on the bandwidth available between the upload file location and the VidyoPortal.

Once the upload completes, the VidyoPortal will reboot. Wait two to five minutes before proceeding to the next step.

Caution: Do not reboot the server manually during this process; doing so may interrupt the upgrade process and corrupt the data. Vidyo recommends running a continuous ping to the server to monitor the reboot process status.

When performing a VidyoPortal upgrade, you also typically need to upload new endpoint software as well. For more information, see “Uploading Endpoint Software” on page [68](#).

Downloading Your VidyoPortal Installation Logs History

You can download your VidyoPortal installation logs history from the System Upgrade tab.

To download your VidyoPortal installation logs history:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. Click the **System Upgrade** tab.

The screenshot shows the Vidyo Portal maintenance interface. On the left, there's a sidebar with options like Platform Network Settings, System License, Upload Endpoint Software, Maintenance (which is selected), Super accounts, Customization, Security, Scheduled Room, and Global Feature Settings. The main area has tabs for Database, System Upgrade (which is active), System Restart, CDR Access, Audit Log, Status Notify, and Syslog. Under the System Upgrade tab, there's a section titled 'Install logs history' with a table showing log files and their creation dates. One file, 'install-2014-01-29-09:39:12.log', is checked. Below this is a 'Download' button. Another section titled 'Installed patches' shows a list of patches with their names and creation dates.

File Name	Creation Date
install-2014-01-29-09:39:12.log	2014-01-29 09:39:12 AM
install-2014-01-28-20:54:26.log	2014-01-28 08:57:33 PM
install-2014-01-27-18:29:45.log	2014-01-27 06:29:45 PM
install-2014-01-23-16:08:45.log	2014-01-23 04:08:45 PM

Patch Name	Creation Date
SECURITY_UPDATE_2	2013-04-03 01:18:56 PM
MYSQL_5_1_88_UPDATER	2013-04-03 01:18:56 PM
RC_LOCAL_UPDATE_SU1	2012-12-20 04:19:51 PM
MYSQL_5_1_UPDATER	2012-12-20 04:19:51 PM
SECURITY_UPDATE_1	2012-12-20 04:19:51 PM

5. Select the check box to the left of the file name you wish to download.
6. Click **Download**.

Your selected .log file or files then download through your Web browser.

Viewing Your VidyoPortal Installed Patches

You can view your VidyoPortal installed patches from the System Upgrade tab.

To view your VidyoPortal installed patches:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).

- 2.** Click the **Settings** tab.
- 3.** Click **Maintenance** on the left menu.
- 4.** Click the **System Upgrade** tab.

The screenshot shows the Vidyo Portal's Maintenance interface. At the top, there are tabs for Database, System Upgrade (which is selected), System Restart, CDR Access, Audit Log, Status Notify, and Syslog. Below the tabs, there is a section titled "Install logs history" containing a table of log files with their creation dates. Underneath is a section titled "Installed patches" containing a table of patches with their creation dates. A "Download..." button is located at the bottom of the patch table.

File Name	Creation Date
Install-2014-01-29-09-39-12.log	2014-01-29 09:39:12 AM
Install-2014-01-28-20-54-26.log	2014-01-28 08:57:33 PM
Install-2014-01-27-18-29-45.log	2014-01-27 06:29:45 PM
Install-2014-01-23-16-08-45.log	2014-01-23 04:08:45 PM

Patch Name	Creation Date
SECURITY_UPDATE_2	2013-04-03 01:18:56 PM
MYSQL_5_1_58_UPDATER	2013-04-03 01:18:56 PM
RC_LOCAL_UPDATE_SUI	2012-12-20 04:18:51 PM
MYSQL_5_1_UPDATER	2012-12-20 04:18:51 PM
SECURITY_UPDATE_1	2012-12-20 04:18:51 PM

All of the patches you have installed on your VidyoPortal appear on the Installed Patches section of the screen.

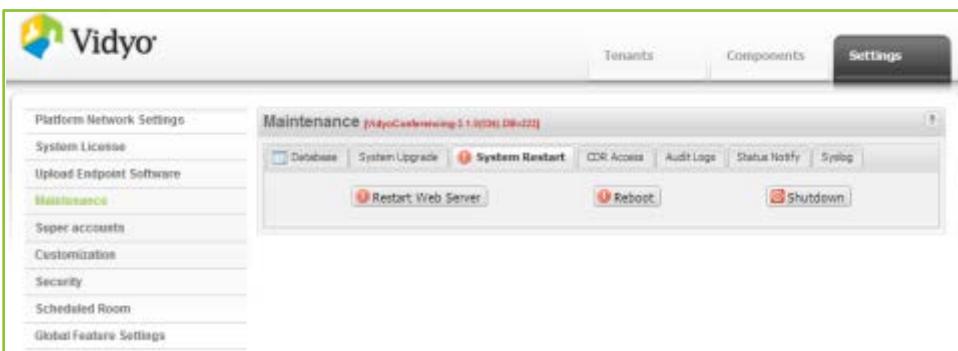
Restarting Your System

The System Restart tab is used to restart or shutdown the VidyoPortal. You can also restart the web server.

To restart your VidyoPortal:

- 1.** Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
- 2.** Click the **Settings** tab.
- 3.** Click **Maintenance** on the left menu.
- 4.** Click the **System Restart** tab.
- 5.** Click the desired button from the following choices:
 - Click **Restart Web Server** to restart the web server application (Tomcat) service on your VidyoPortal.
 - Click **Reboot** to reboot your VidyoPortal.

- Click **Shutdown** to shut down your VidyoPortal.



6. A dialog box appears asking you to confirm the action.
7. Click **Yes**.

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

Caution: When the system is restarted or shut down all calls in progress are ended. Therefore, you may want to email users ahead of time and perform the upgrade when system usage is lowest.

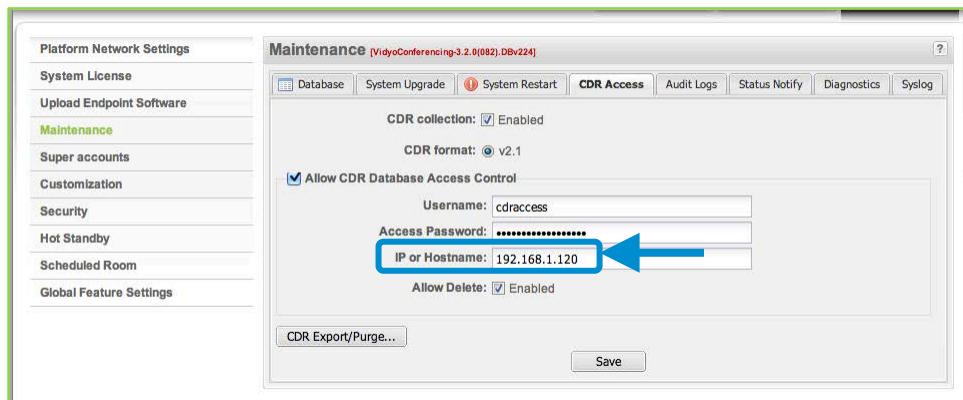
Configuring the CDR Database for Remote Access in the Super Admin Portal

For more information, see the “CDR” appendix on page [336](#).

To configure VidyoPortal to grant remote access to CDR data:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. Click **CDR Access** tab.
5. Select **Allow CDR Database Access Control** and enter the following information:
 - Enter your **Username** as cdraccess (limited to read and delete privileges).
 - Enter your **Password**, which is configured using the VidyoPortal Admin portal.

- Enter your VidyoDashboard IP or Hostname.



Note:

- Providing the IP or Hostname on this page provides remote access to your CDR data on the VidyoPortal. The VidyoDashboard virtual server may be used for this remote access. For more information about remotely accessing CDR data using VidyoDashboard, refer to the *VidyoDashboard Installation Guide*.
 - You can use the wildcard character “%” in the IP or Hostname. For example, **192.168.1.%** or **%.vidyo.com**.
- Select **Allow Delete**, if desired.
 - Click **Save**.

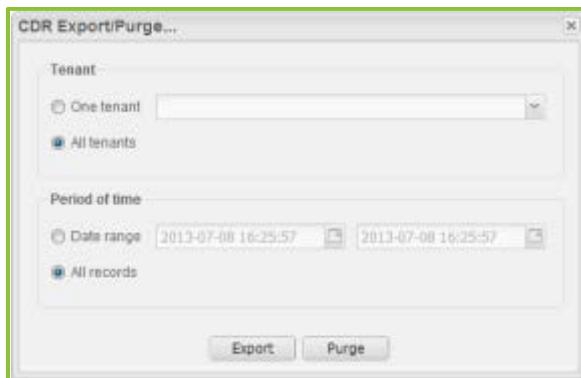
Exporting and Purging CDR Files from the Super Admin Portal

For more information about the CDR, see the “CDR” appendix on page [336](#).

To export and purge CDR records from the Super Admin Portal:

- Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
- Click the **Settings** tab.
- Click **Maintenance** on the left menu.
- Click **CDR Access** tab.
- Select **Allow CDR Database Access Control** and enter your username, password, and IP hostname.
- Select **Allow Delete**, if desired.
- Click **CDR Export and Purge**.

- In the CDR Export and Purge window, specify one or all tenants and a period of time for your CDR record Export or Purge.



- Click **Export** or **Purge**, as desired.

Note:

- The export record limit is 65,000 records. If the export contains more than 65,000 records, a message appears warning you to restrict the range before proceeding with the download.
- The export data provided matches the fields and descriptions explained in the ConferenceCall2 table on page [338](#).

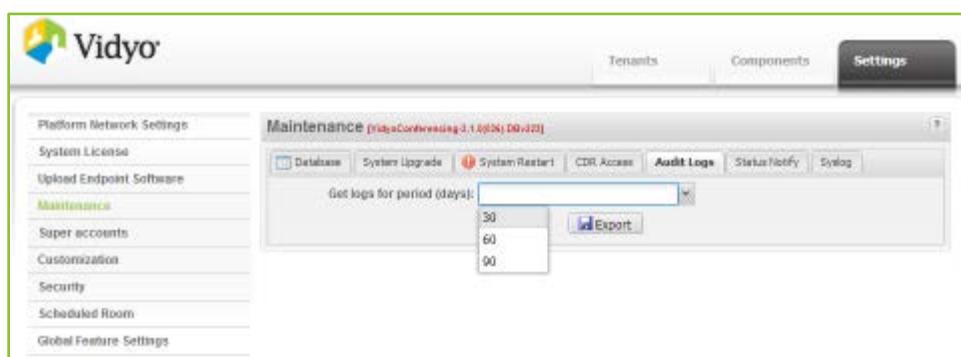
Downloading Audit Logs

The system logs all activity on the VidyoPortal. The information logged includes Record ID, User Name, Tenant Name, Activity (Log In, Log Out, Add Room), Status (Success or Failure), Date & Time, IP Address the user comes from, Event Details and so on. For more information, see “Auditing” on page [272](#).

Note: VidyoPortal audit logs can be generated using either a Super Admin or the Audit user account.

To download the Audit Logs:

- Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
- Click the **Settings** tab.
- Click **Maintenance** on the left menu.
- Click the **Audit Logs** tab.

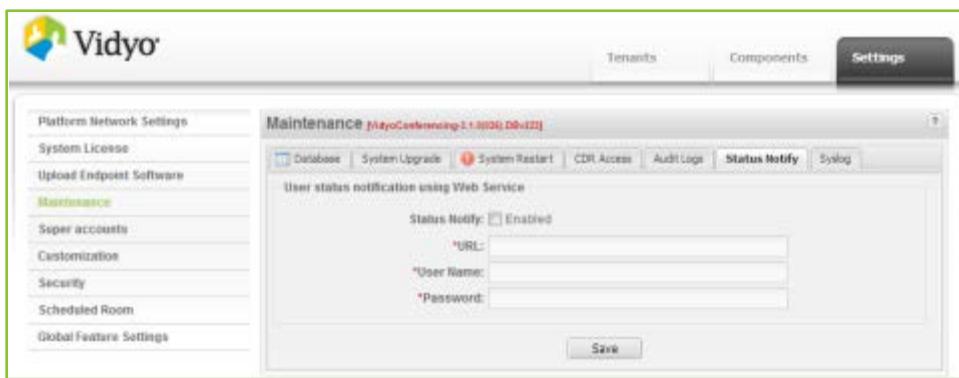


5. From the drop-down menu select 30, 60 or 90 days.
6. Click **Export**.

Configuring Status Notify

To set up Status Notify:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.
4. Click the **Status Notify** tab.



5. Select **Enable**.

Note: When enabled, URL, User Name and Password information is required.

6. Enter a URL.
7. Enter a User Name.
8. Enter a Password.
9. Click **Save**.

Enabling Syslog

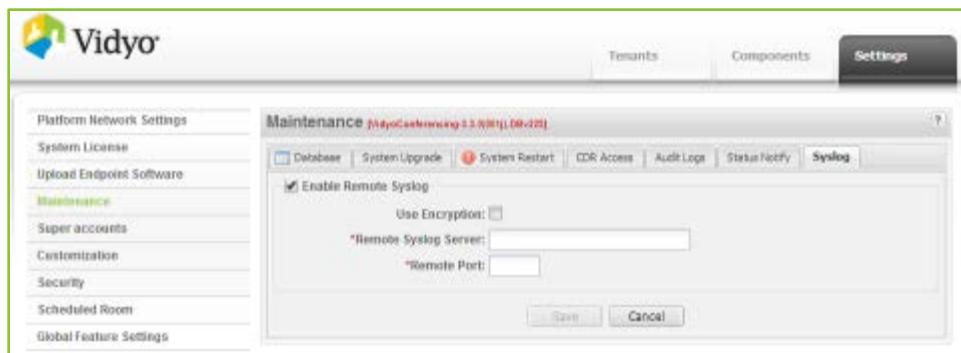
You can enable the use of a Syslog server for syslog message data storage in to a separate server of your choice.

Note: This feature is not available on the Linux Ubuntu 8.04 platform.

To enable Syslog:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Maintenance** on the left menu.

- Click the **Syslog** tab.



- Select **Enable Remote Syslog**.

When enabled, Use Encryption, Remote Syslog Server, and Remote Port fields appear.

- Select **Use Encryption**, if desired.
- Enter the Remote Syslog Server location.
- Enter the Remote Port for your syslog server.
- Click **Save**.

MANAGING YOUR SUPER ACCOUNTS

The Super accounts tab allows you to create and change Super Accounts.

For more information, see “Adding Multiple Super Admin Accounts” on page [55](#).

Caution: Each Super Account is required to have a valid, resolvable, email address in order to function properly in your VidyoConferencing system.

Viewing Your Super Accounts

To view your super accounts:

- Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
- Click the **Settings** tab.

3. Click Super accounts.

Name	Member Name	Date Joined	Enabled	Delete
super		08/23/2012	Yes	<input type="checkbox"/>
john		11/05/2013	Yes	<input type="checkbox"/>
chris		11/12/2013	Yes	<input type="checkbox"/>

4. Click an existing account Member Name to access its details. You can also click Add below the Super Accounts list. Adding or Editing account details show the same screen with different headings. Fields marked with an asterisk cannot be left blank.

Edit Super Account

*User Name:

*Full Name:

*Email Address:

*Language Preference:

Description: Default Super Admin

Change Password

Save Cancel

Note:

- Change the default Super Account email address so you receive important system notifications.
- For security purposes, you should change the password for Super Admin access as soon as possible (as described in the next procedure).

5. Modify field values for your Super Account as desired.

6. Click Save.

Note: For information about adding multiple super accounts, see page [55](#).

Editing Super Account Information and Changing the Password

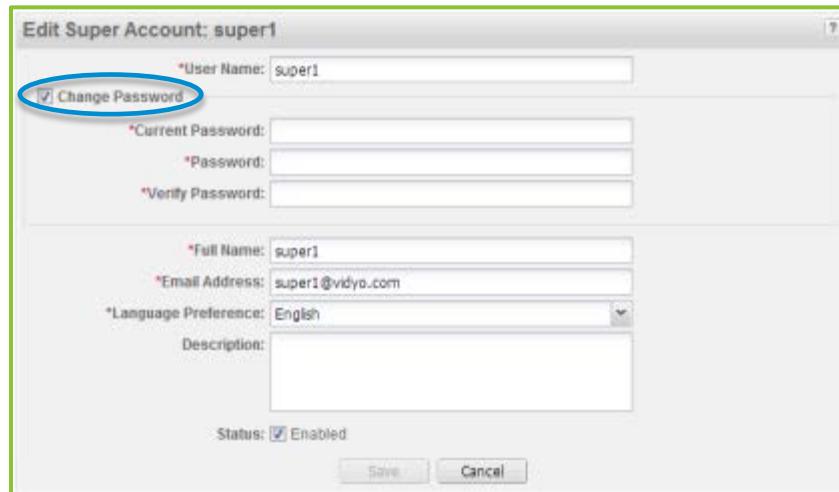
To edit super account information and change the password:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Settings** tab.
3. Click **Super accounts**.
4. Click an existing account Member Name to access its details. You can also click Add below the Super Accounts list. Adding or Editing account details show the same screen with different headings. Fields marked with an asterisk cannot be left blank.
5. Select the **Change Password** check box.

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



6. Enter your new password in the New Password field.
7. Enter your new password again in the Verify New Password field.
8. Assuming the system doesn't complain about a failure to match, when you're done typing, click **Save** to complete the password change.

The system indicates a password mismatch until the last letter is typed in Verify New Password.

CUSTOMIZING THE SYSTEM

The Customization left menu item allows you to customize information that end users see as well as perform other system customization.

Customizing the About Info

The About Info page enables you to create and format an About Us page that appears when users click About Us at the bottom of the VidyoPortal home page and the VidyoPortal Admin and Super Admin Portal.

Note:

- Because of the limitations of Adobe Flash, URLs and other markup information can be inserted into the text but must conform to HTML 1.1 specifications.

6. Configuring System Settings as the Super Admin

- About us customizations created at the Super Admin level can be overridden at the Tenant level by Tenant Admins.

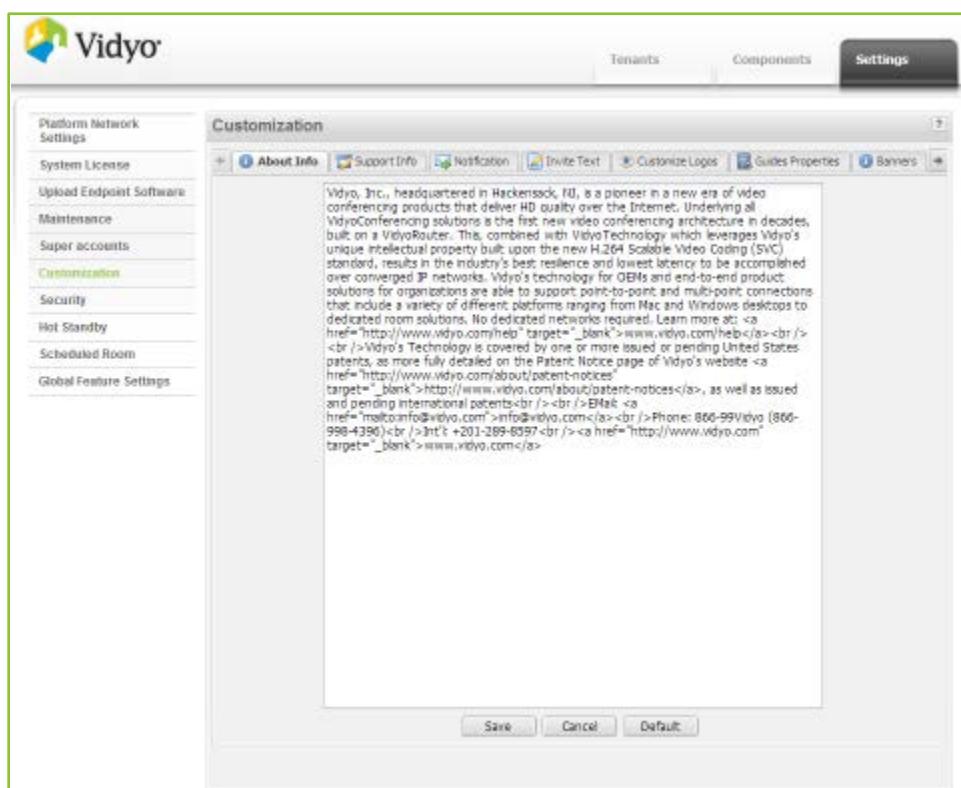
For more information, see “Configuring Customization on Your Tenant” on page 240.

To customize the About Us information:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page 35.

2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click **About Info**.



5. Enter text or paste text you have copied from another application.
6. Apply any formatting desired.
7. Click **Save**.

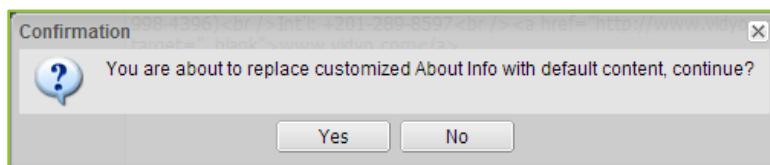
Reverting To Default System Text on The About Info Screen

Note: About us customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.

For more information, see “Configuring Customization on Your Tenant” on page 240.

To revert to default system text on the About Info screen:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page 35.
2. Click the **Settings** tab.
4. Click **Customization** on the left menu.
5. Click **About Info**.
6. To remove any previously saved customized text and revert to the default system text provided by Vidyo, click **Default**.
7. A confirmation dialog box appears.



8. Click **Yes**.

Customizing Support Info

It's easy to keep your support contact information up to date. The Support Info page enables you to create and format a support page that appears when users click Support Info at the bottom of the VidyoPortal home page, the VidyoPortal admin and Super Admin Portal, and the login page. This is information your users need to contact the VidyoPortal Super Administrator.

A screenshot of the Vidyo Customization interface. The top navigation bar includes "Tenants", "Components", and "Settings". The left sidebar has a "Customization" section with several tabs: "About Info", "Support Info" (which is selected and highlighted in blue), "Notification", "Invite Text", "Customize Logos", "Guides Properties", and "Banners". The main content area shows a rich text editor with the following text:

```
For useful tips and video clips on how to get started and make the most out of your Vidyo experience, please check the Vidyo Knowledge Center: <br><br><u><font color="#ffcc00" size="2">Trebuchet MS</font><a href="http://www.vidyo.com/knowledge-center" target="_blank">www.vidyo.com/knowledge-center</a></font></u><br><br>For other support issues, please contact your system administrator<br><br>
```

At the bottom of the editor are "Save", "Cancel", and "Default" buttons.

Note:

- Because of the limitations of Adobe Flash, URLs can be inserted into the text but they must conform to HTML 1.1 specifications.
- Support customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.

For more information, see “Configuring Customization on Your Tenant” on page [240](#).

To add and edit Support Info:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click **Support Info**.
5. Enter text or paste text you have copied from another application.
6. Apply any formatting desired.
7. Click **Save**.

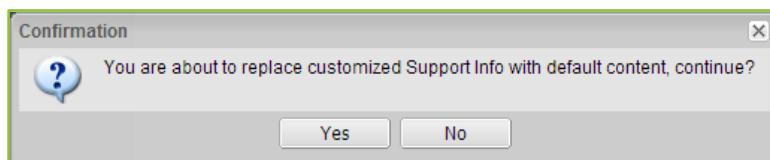
Reverting To Default System Text on The Support Info Screen

Note: Support customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.

For more information, see “Configuring Customization on Your Tenant” on page [240](#).

To revert to default system text on the Support Info screen:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click **Support Info**.
5. To remove any previously saved customized text and revert to the default system text provided by Vidyo, click **Default**.
6. A confirmation dialog box appears.



7. Click **Yes**.

Customizing Notification Information

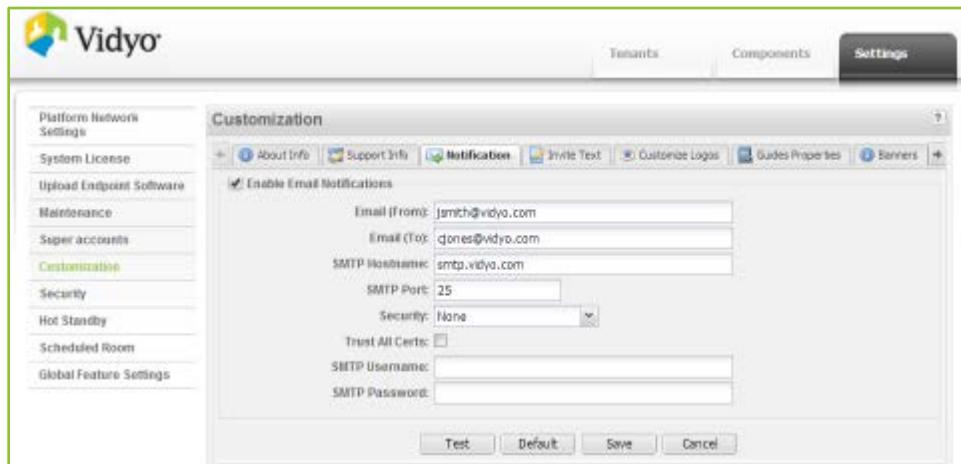
The Notification page enables you to enter From and To email information that's used by the VidyoPortal for automated emails. The From address you enter is used for automated emails sent out by the VidyoPortal, such as confirmations to new users that their accounts are activated, and other correspondence.

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 VidyoPortal. Configure SMTP and Security information as desired.

Note:

- Be sure to provide a From address. Not doing so can result in SMTP servers blocking emails or changing email headers.
- Notification customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.

For more information, see “Configuring Customization on Your Tenant” on page [240](#).



To customize Notification information:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Notification** tab.
5. Select the **Enable Email Notifications** check box to activate the addresses and settings you configure.
6. Enter valid email addresses in the From and To fields and provide the following SMTP and Security information:
 - a. Enter the SMTP Hostname.
 - b. Enter the SMTP Port.

- c. Select either STARTTLS or TLS Security.
 - d. Select Trust All Certs, if desired.
 - e. Enter the SMTP Username.
 - f. Enter the SMTP Password.
- 7. Click **Save**.**

Note: You can use the Test button to confirm your Notification customizations.

Customizing the Invite Text

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

There are three kinds of invitations.

- Email Content text is sent for VidyoConferences.
- Voice Only text is sent to those participating in voice-only mode via telephone.
- Webcast text is sent to participants accessing your webcast.

As with the other informational text boxes on the Customization pages, 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 green buttons in the upper right hand corner of the page.

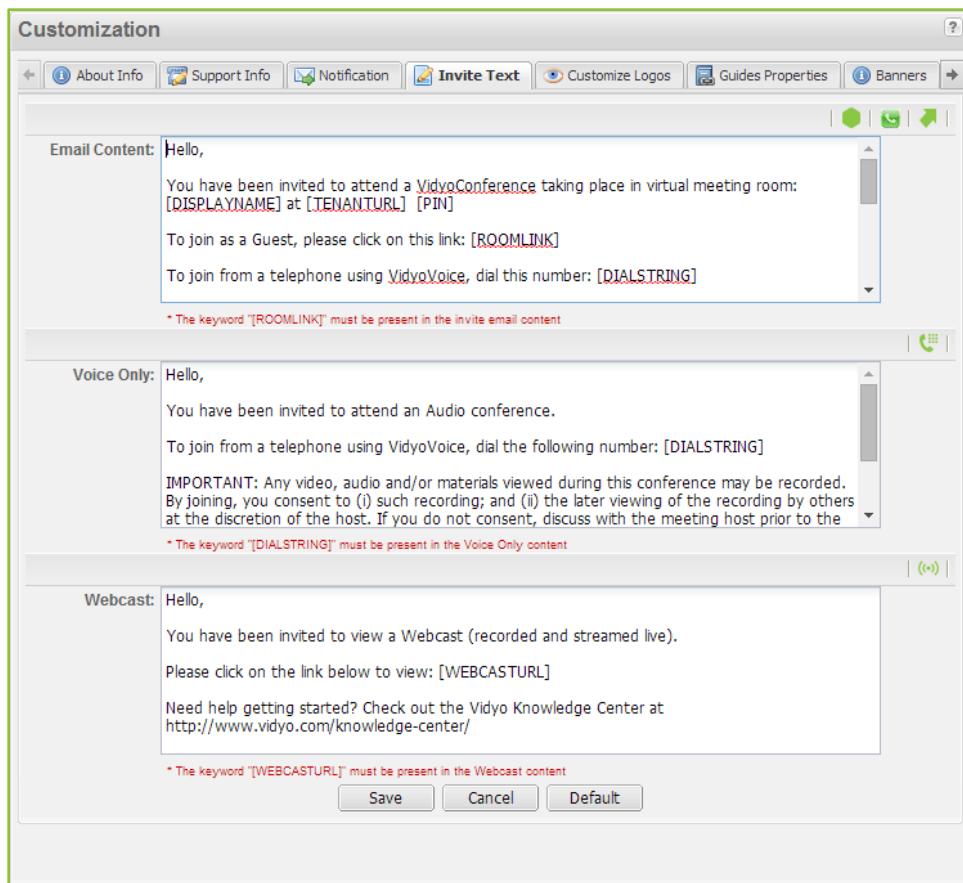
Note: Invite text customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.

For more information, see “Configuring Customization on Your Tenant” on page [240](#).

To customize Invite Text:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.

4. Click the **Invite Text** tab.



5. Change the text from the Email Content, Voice Only, and Webcast sections, as desired.

Some common changes to the messages that you may want to make include the following:

- If your organization has disabled guest access, delete the line about joining as a first-time user from your desktop or mobile device, or to annotate with VidyoSlate on your iPad: Click [ROOMLINK] from the Email Content section.

Note: When accessed from a tablet, roomlinks may be used to join a conference, annotate, or manage a meeting.

- If your system includes a VidyoGateway, add the following sentence as part of your email content:

To join from a non-Vidyo conferencing endpoint: Connect through a VidyoGateway <enter your VidyoGateway IP here> using H.323 or SIP and enter meeting ID [EXTENSION].

Note: Modify the <enter your VidyoGateway IP here> portion with your VidyoGateway IP address.

- If your organization doesn't use IPC, delete the line about joining from another VidyoPortal using IPC: Enter [ROOMNAME]@[TENANTURL] from the Email Content section.
- If your organization doesn't use VidyoVoice, delete the line about using VidyoVoice in the Voice Only section.

- If your organization uses more than one VidyoVoice number, add the additional number or numbers in the Voice Only section.

Note: Keep in mind that due to some browsers' limitations, the message cannot contain more than 1300 characters.

6. The following variables are available when providing text for the Email Content section:

When your email invitations are created, the VidyoPortal automatically passes the specific data to the variable.

- Click  to insert a [ROOMLINK] placeholder for the link to the user's room.
This variable is required in your Email Content section.
Note: When accessed from a tablet, roomlinks may be used to join a conference, annotate, or manage a meeting.
- Click  to insert a [VIDYOROOMLINK] placeholder for the link to the conference for sending to a VidyoRoom.
- Click  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. Optionally, you can enter a PIN if you want to require a PIN to enter the room.
- Click  to insert a [LEGACY_URI] placeholder for the URI used by participants accessing your conference from a specific Legacy endpoint.
- The [DISPLAYNAME] variable used in the default text to show the specific user's display name as it was entered in to the system.
- The [TENANTURL] variable used in the default text shows the name of the tenant.
- The [PIN] variable used in the default text shows the room PIN (if one has been set).
- The [ROOMNAME] variable used in the default text shows the name of the room for which the invite was issued.

Note: If applicable, modify the default text in the Email Content section with your VidyoGateway IP address for your participants accessing your conference from Legacy endpoints.

7. Click  to insert a [DIALSTRING] placeholder for the phone number used by participants accessing your conference from a voice-only telephone.
8. Click  to insert a [WEBCASTURL] placeholder for the URL used by participants to access your webcast.
9. Click **Save** to save the invitations.

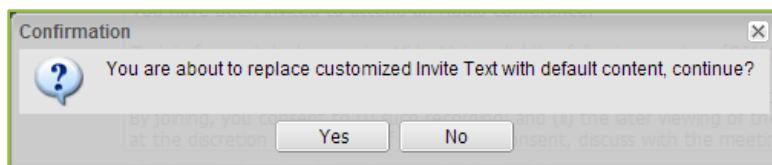
Reverting To Default System Text on The Invite Text Screen

Note: Invite text customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.

For more information, see “Configuring Customization on Your Tenant” on page [240](#).

To revert to default system text on the Invite Text screen:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Invite Text** tab.
5. To remove all custom invitations and revert to the default text supplied by Vidyo, click **Default**.
6. A confirmation dialog box appears.



7. Click **Yes**.

Uploading Custom Logos

You can upload your organization’s logo to customize and brand your Super and Admin portal, your User portal, and your VidyoDesktop download page for a more cohesive company branding of your VidyoConferencing system.

You can upload a User portal Logo, which becomes the default logo for each Tenant User portal page. However, logos can also be individually customized by Tenant Admins on their respective tenants.

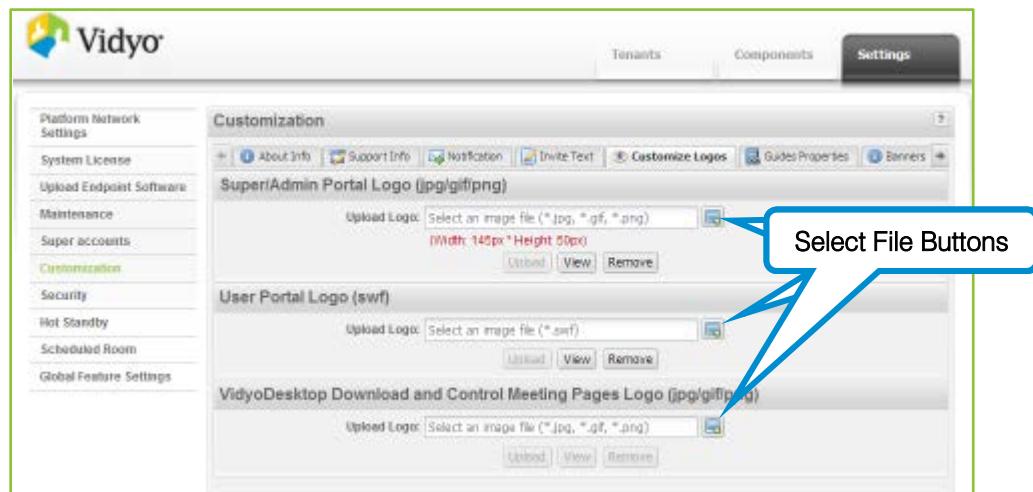
Note:

- Logo customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.
For more information, see “Configuring Customization on Your Tenant” on page [240](#).
- The customized logos per tenant appear on the HTML-based Control Meeting screen.
For more information, see "Controlling a Meeting Room" on page [219](#).

To upload your custom logos:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.

3. Click **Customization** on the left menu.
4. Click the **Customize Logos** tab.
5. Click the **Select File** buttons for the corresponding logo you wish to upload.



Logos can be uploaded for the following system locations:

- The Super and Admin Portal Logo updates the logo used on both the Super Admin portal and the Tenant Admin portal, replacing the Vidyo logo in the top-left corner of the page.
Note: The Super and Admin Portal logo must be 145 x 50 pixels and can be in the .gif, .jpg or .png formats
- The User Portal Logo updates the logo used on your tenant User portal. Each Tenant Admin can upload a different logo for each User portal which replaces the Vidyo logo in the top-left corner of the page and a VidyoPower™ logo appears in the bottom-right corner.
Note: The uploaded User Portal Logo should be 150 x 50 pixels and in the .swf format. 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. Therefore, the exact size of the logo is less important than the aspect ratio. No matter what size your logo image is, make sure it has a 3:2 aspect ratio. Logos with different proportions will be stretched or squeezed.
- Vidyo provides a service for converting logos to .swf format. Please contact your reseller or Vidyo Customer Support for details.
- The VidyoDesktop Download and Control Meeting Pages Logo updates the logo used on the VidyoDesktop download page shown to users when a software update is performed and the Control Meeting page shown to meeting moderators.
Note: The VidyoDesktop Download and Control Meeting Pages logo must be 145 x 50 pixels and can be in the .gif, .jpg or .png formats.

For more information, see “Controlling a Meeting Room” on page [219](#).

6. Select your logo file and click **Upload**.

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

7. Click **View** to see the logo file currently in use.
- The logo file appears in a new browser tab.
8. Click **Remove** to delete the logo file currently in use.

After removal, your logo file is replaced with the system default Vidyo logo.

Changing Where the System Looks for PDF Versions of the Administrator and User Guides

By default, your system is set to get the Administrator and User Guides from Vidyo's Web servers. These guides are guaranteed to be the most up-to-date versions available.

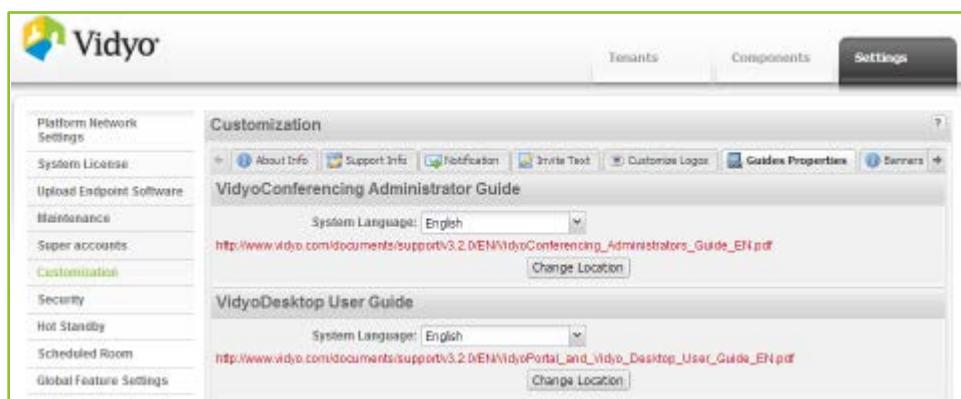
However, if you have a relatively slow Internet connection, it may not be convenient to connect to our server in the US every time you want to look something up. So we give you an option to use the original version that came with your product. Just copy it to the same network your VidyoPortal is on and your users can open it from there.

If you choose to use your local copy, you might want to occasionally check our Web site to see if the Guide you want has been updated. You can tell by the version designator on the title page or in the filename of the Guide; if you have version 2.2-A and you see that our Web site has version 2.2-C, you know some changes have been made. You can then download the latest version from our Web site when it's convenient, and replace your local copy with it.

To change where the system looks for PDF versions of the Administrator and User Guides:

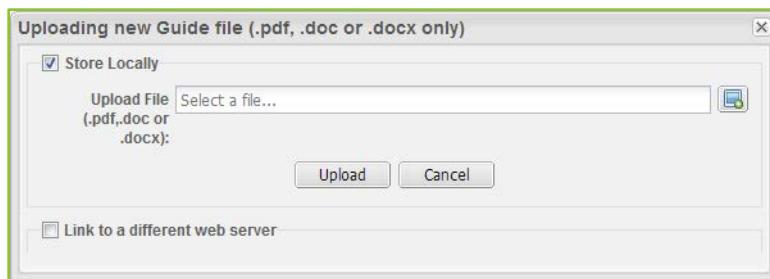
1. Log in to the Super Admin portal using your Super Admin account.
- For more information, see "Logging in to the Super Admin Portal" on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Guides Properties** tab.

The current location of the PDFs appears on the page in red text.



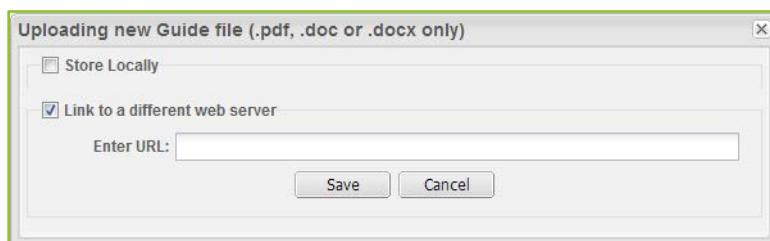
5. In the System Language drop-down, select a language to associate a guide you want to upload or link with the language in which it is written.

6. Click **Change Location** to upload or link a .pdf guide.



The Uploading new Guide file dialog box appears with Store Locally selected by default.

- 7.** Store your selected guide locally on your VidyoPortal using the following steps:
 - a.** Select the **Store Locally** check box.
 - b.** Click **Select File**.
 - c.** After locating and opening your guide, click **Upload** to store it locally.
- 8.** Alternatively, select Link to a different web server to link to a guide located on a different web server using the following steps:
 - a.** Select the **Link to a different web server** check box.



- b.** In the Enter URL field, enter the web server URL file location where your new guide is stored.
- c.** Click **Save**.
- 9.** Repeat the procedure to upload additional versions of the Administrator and User Guides to provide translations for use when you or the tenant admin change the interface language settings.

For more information, see “Setting the Language for the Super Admin Interface” on page 53, “Setting the Language for the Admin Interface” on page 202, and “Setting the Tenant Language” on page 238.

Customizing Your VidyoPortal Login and Welcome Banners

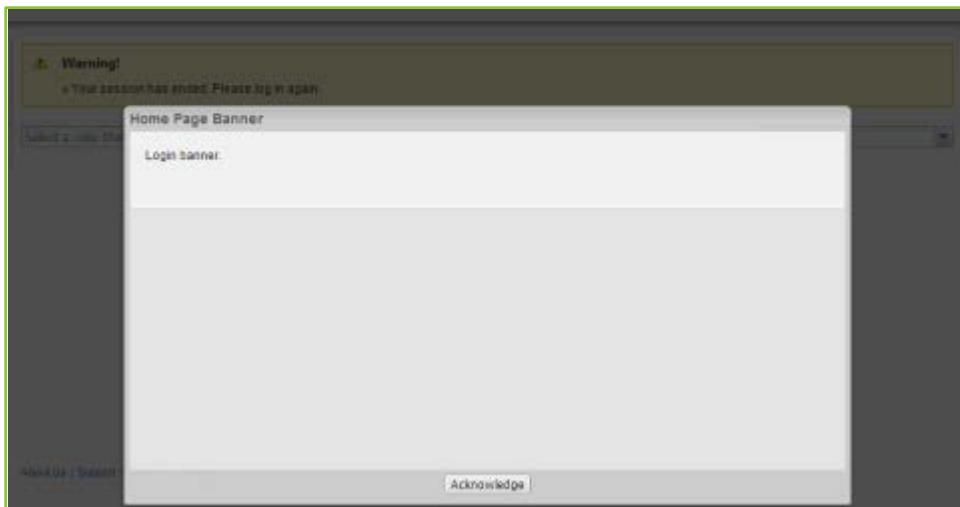
The Login banner is a dialog box that appears every time your users access the login pages of the Super Admin or Tenant Admin portals. The Welcome banner is a dialog box that first appears when your users access the Super Admin or Tenant Admin portals after logging in to the system. Both banners are activated and customized by the Super Administrator.

Viewing and Acknowledging the Login Banner

To view and acknowledge the Login banner:

1. Access the Super Admin portal.

The Login banner appears and displays text customized by your Super or Tenant administrator.



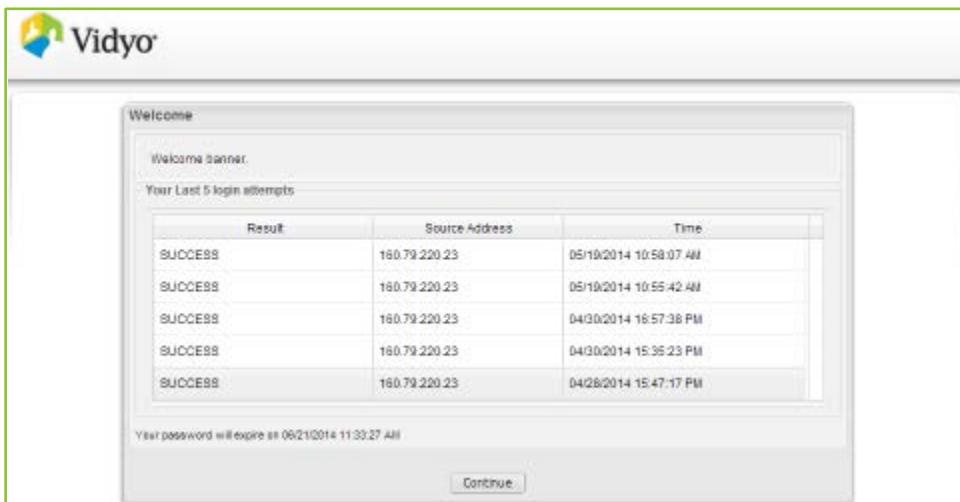
2. Click **Acknowledge**.

Note: You must click the Acknowledge button to close the login banner and continue logging in to the system.

Viewing the Welcome Banner

To view the Welcome banner:

1. Access the Super Admin portal.
 2. Click **Acknowledge** on the Login banner.
 3. Log in to the Super Admin portal using your Super Admin account.
- For more information, see “Logging in to the Super Admin Portal” on page [35](#).
4. The Welcome banner appears and displays text customized by your Super or Tenant administrator and your last 5 login attempts in a table.



The following information is provided as columns in the table showing your last 5 login attempts:

- The result; meaning, whether or not you successfully logged in to the system.
- The source address. This is your IP address when accessing the Super or Admin portal when you logged in to the system.
- The time when you logged in to the system.

5. Click **Continue**.

Customizing Your Login Banner

To customize your login banner:

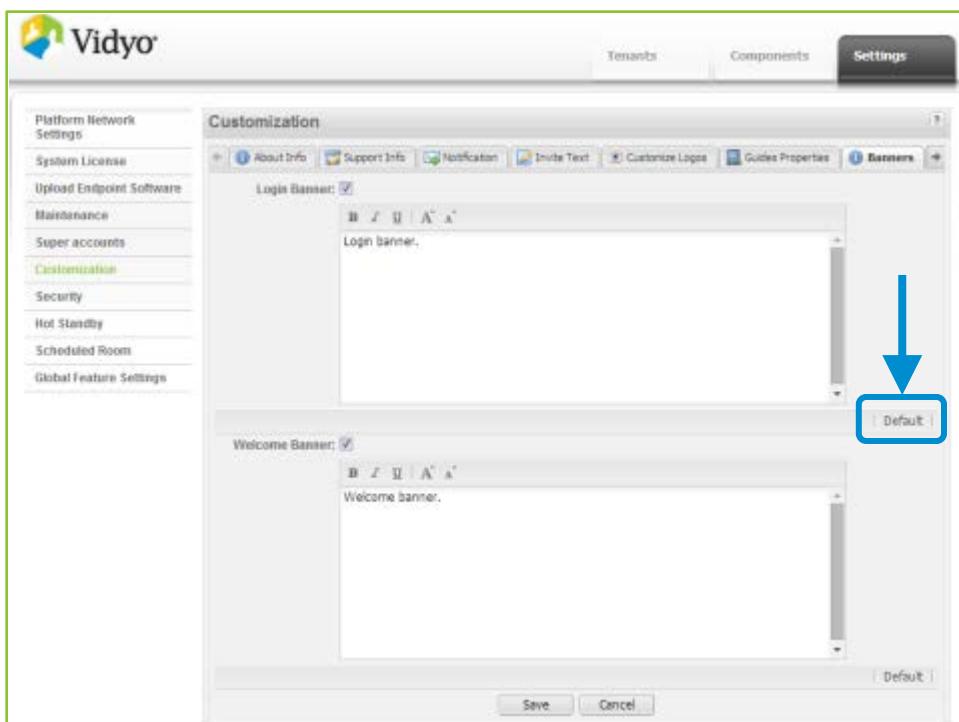
1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Banners** tab.
5. Select the Login Banner check box to activate the login banner.
6. Enter your desired text and formatting for your login banner.
7. Click **Save**.

Reverting Your Login Banner to Default System Text

To revert your login banner to the default system text:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Banners** tab.
5. Select the Login Banner check box to activate the login banner.

6. Click the **Default** button on the lower-right side of the login banner part of the screen.



7. Click **Save**.

Customizing Your Welcome Banner

To customize your welcome banner:

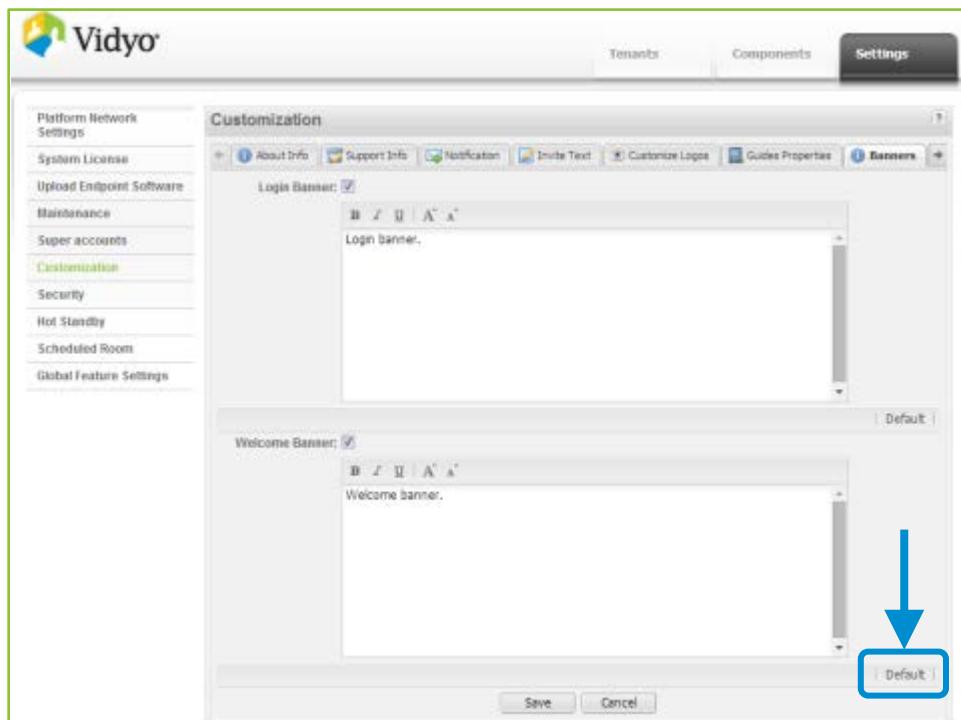
1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Banners** tab.
5. Select the Welcome Banner check box to activate the welcome banner.
6. Enter your desired text and formatting for your welcome banner.
7. Click **Save**.

Reverting Your Welcome Banner to Default System Text

To revert your welcome banner to the default system text:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.

4. Click the **Banners** tab.
5. Select the Welcome Banner check box to activate the welcome banner.
6. Click the **Default** button on the lower-right side of the welcome banner part of the screen.



7. Click **Save**.

Customizing Your Password Settings

You can customize the password settings for users accessing the Super Admin portal.

To customize password settings for users accessing the Super Admin portal:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Passwords** tab.
5. Provide the following information:
 - In the “Number of days before password expires” field, enter the desired number of days.
 - In the “Number of days of inactivity before a password change is forced” field, enter the desired number of days.

Note: The “Number of days before password expires” and “Number of days of inactivity before a password change is forced” do not apply to LDAP auto-provisioned accounts.

- In the “Number of failed login attempts before account is locked” field, enter the desired number of attempts.

Note: When your LDAP auto-provisioned accounts are locked out of the system, they are disabled on the VidyoPortal.

6. Click **Save**.

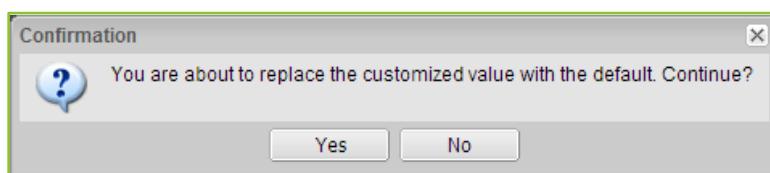
Reverting To Default Password Settings on the Password Screen

To revert to default password settings on the Password screen:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Passwords** tab.
5. To remove all custom password settings and revert to the default values supplied by Vidyo, click **Default**.

Note: Defaults are 0, 0, and 0 (0 meaning infinite) for the “Number of days before password expires,” “Number of days of inactivity before a password change is forced,” and “Number of failed login attempts before account is locked” fields, respectively.

6. A confirmation dialog box appears.



7. Click **Yes**.

SECURING YOUR VIDYOCONFERENCING SYSTEM

Securing your VidyoConferencing system involves securing your VidyoPortal and your various components such as VidyoManager, VidyoRouter, and VidyoGateway. The Security section of the guide shows you how to secure your VidyoPortal.

For more information, see “Security” on page [300](#).

CONFIGURING A SCHEDULED ROOM PREFIX

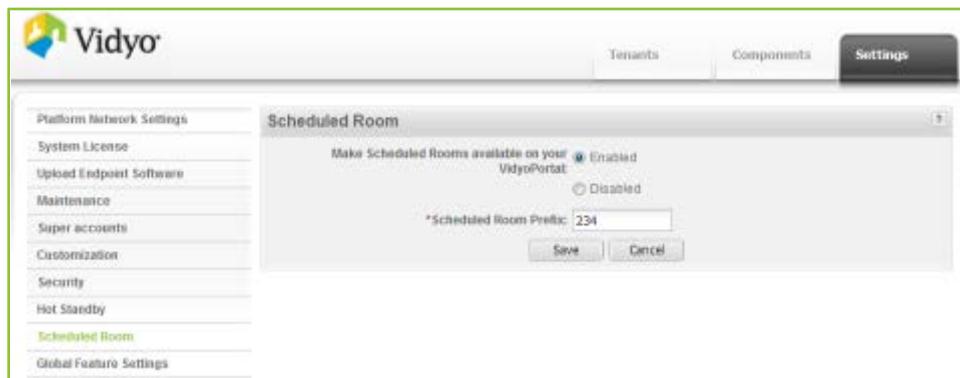
By adding a scheduled room prefix, your users can then create ad-hoc rooms from specific endpoints on your system. The prefix you configure on this screen is used for all scheduled rooms created on your system.

To configure a scheduled room prefix:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page 35.

2. Click the **Settings** tab.
3. Click **Scheduled Room** on the left menu.



4. Select **Enabled** to allow scheduled rooms on your VidyoPortal.
 5. In the Scheduled Room Prefix field, enter a numeric prefix.
- Note:** If you do not provide a scheduled room prefix, no scheduled rooms can be created by your users from specific endpoints on your system.
6. Click **Save**.

SETTING GLOBAL FEATURES

The Global Feature Settings left menu item allows you to control the system-wide behavior of VidyoWeb, VidyoMobile, Search Options, and Inter-Portal Communication on your VidyoPortal.

Enabling VidyoWeb Access

The VidyoWeb browser plug-in makes it easy for guest participants to join conferences from within a web browser on desktop and laptop computers. VidyoWeb is designed especially for guest participants who simply want an easy way to join a conference.

You don't pay extra for VidyoWeb. It's built into your VidyoPortal. However, when a new user connects to your VidyoPortal via VidyoWeb for the first time, one of your licenses is consumed.

Note:

- User licenses apply to either VidyoWeb or VidyoDesktop, but not both at the same time. Therefore, when using VidyoWeb, be sure to close VidyoDesktop if it's open.
- VidyoWeb is brought back to the first installed version when upgrading your VidyoPortal. Remember to upgrade your version of VidyoWeb after upgrading your VidyoPortal.
- After upgrading your VidyoPortal, re-install your version of VidyoWeb if the version bundled in your VidyoPortal upgrade is less current than the installation used prior to your VidyoPortal upgrade.
- Global feature settings made in the Tenant Admin portal override settings made in the Super Admin portal.

For more information about configuring VidyoWeb on tenants, see “Configuring VidyoWeb on Your Tenant” on page [269](#). For more information about administering and using VidyoWeb, refer to the *VidyoWeb Quick Administrator Guide* and the *VidyoWeb Quick User Guide*.

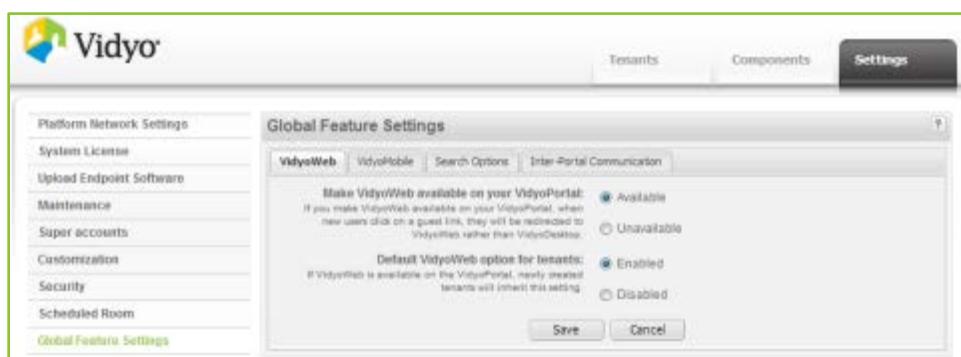
- As the Super Admin, you can configure VidyoWeb to be globally available or unavailable on your entire VidyoPortal. If you choose to make it available, you can control the default VidyoWeb setting (enabled or disabled) on newly created tenants.

To configure VidyoWeb access on your system:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the Settings tab.
3. Click Global Feature Settings on the left menu.
4. Click the VidyoWeb tab.



4. Select one of the following options:

- Select **Available** to give VidyoWeb access to all tenants on your VidyoPortal.

When Available is selected, Enabled and Disabled options appear for newly created tenants:

- Select **Enabled** to enable VidyoWeb on your newly created tenants.
- Select **Disabled** to disable VidyoWeb on your newly created tenants.

- Select **Unavailable** to restrict VidyoWeb access from all tenants on your VidyoPortal.

Enabling VidyoMobile Access

VidyoMobile brings the power of VidyoConferencing to Android and iOS phones and tablets.

You don't pay extra for VidyoMobile. It's built into your VidyoPortal. However, when a new user connects to your VidyoPortal via VidyoMobile for the first time, one of your licenses is consumed.

- Global feature settings made in the Tenant Admin portal override settings made in the Super Admin portal.

For more information about configuring VidyoMobile on tenants, see “Enabling or Disabling VidyoMobile on Your Tenant” on page [196](#). For more information about using VidyoMobile, refer to the *VidyoMobile for iOS User Guide* and the *VidyoMobile for Android Quick User Guide*.

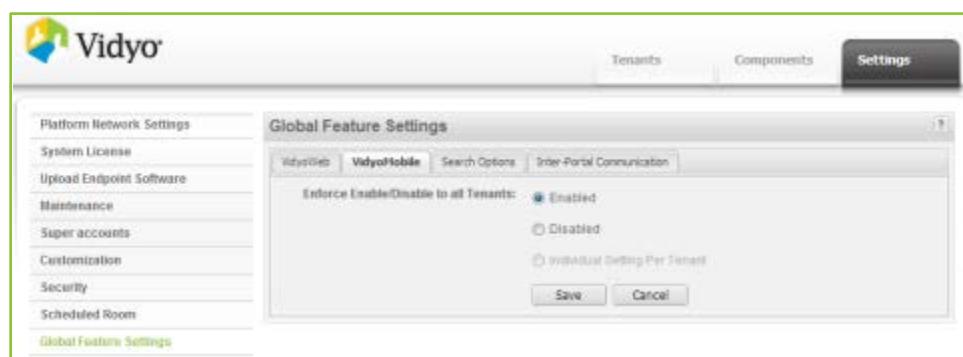
- As the Super Admin, you can configure VidyoMobile to be globally available or unavailable on your entire system. If you choose to make it available, you can control the default VidyoMobile setting (enabled or disabled) on newly created tenants.

To configure VidyoMobile access on your system:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Settings** tab.
3. Click **Global Feature Settings** on the left menu.
4. Click the **VidyoMobile** tab.



5. Select one of the following options:

- Select Enabled to give VidyoMobile access to all tenants.
- Select Disabled to restrict VidyoMobile access from all tenants.
- Regardless of whether VidyoMobile access is Enabled or Disabled here, creating a single tenant with an opposite setting overrides the configuration and Individual Setting Per Tenant is selected here. The following examples provide clarification:
 - With Disabled selected, and at some point later VidyoMobile access is enabled for even one tenant (as described in the “Enabling or Disabling VidyoMobile” section on page [196](#)), Individual Setting Per Tenant is then enabled.
 - Similarly, if at some later point in time after selecting Enabled, VidyoMobile access is disabled for a specific tenant, the next time you look at this screen, Individual Setting Per Tenant will be selected.

Note:

- Along with VidyoMobile access, guest logins must also be enabled on your tenant or tenants if you want to use VidyoSlate. For more information about enabling guest logins on tenants, see page [96](#).

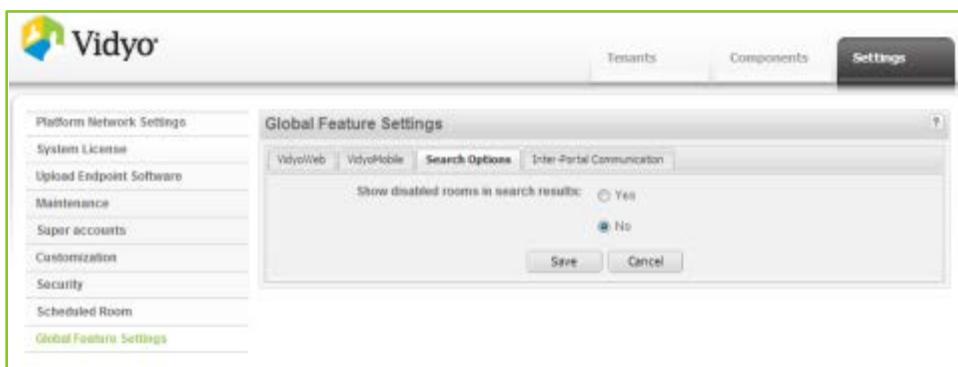
- For more information on VidyoMobile and VidyoSlate you can download the user guides from <http://www.vidyo.com/support/documentation/>. VidyoMobile guides are available for both iOS and Android versions of the application. VidyoSlate is compatible with iPad 2 and later and the iPad Mini.

Configuring System-Wide Search Options

You can control whether or not disabled rooms appear in search results on your VidyoPortal by using Search Options.

To configure whether or not disabled rooms appear in search results:

- Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
- Click the **Settings** tab.
- Click **Global Feature Settings** on the left menu.
- Click the **Search Options** tab.



- Select the **Yes** or **No** radio button to determine whether or not you want disabled rooms to appear in search results on your VidyoPortal.
- Click **Save**.

Configuring System-Wide Inter-Portal Communication (IPC)

Inter-Portal Communication (IPC) allows users to join VidyoConferences with someone on a different VidyoPortal. IPC also supports conferencing between tenants on the same VidyoPortal.

IPC is built into all Vidyo systems running VidyoPortal version 2.2 or later. Users can also use IPC with version 1.1 and later of VidyoMobile for iOS and VidyoMobile for Android (as long as they’re also using VidyoPortal version 2.2 or later).

Note:

- Global feature settings made in the Tenant Admin portal override settings made in the Super Admin portal.

For more information about configuring Inter-Portal Communication (IPC) on tenants, see “Configuring Inter-Portal Communication (IPC) on Your Tenant” on page [268](#).

- As the Super Admin, you can configure IPC to be globally available or unavailable on your entire system.

If you do control system-wide IPC from this interface, you then create a list of either Allowed or Blocked Domains and Addresses that work as follows:

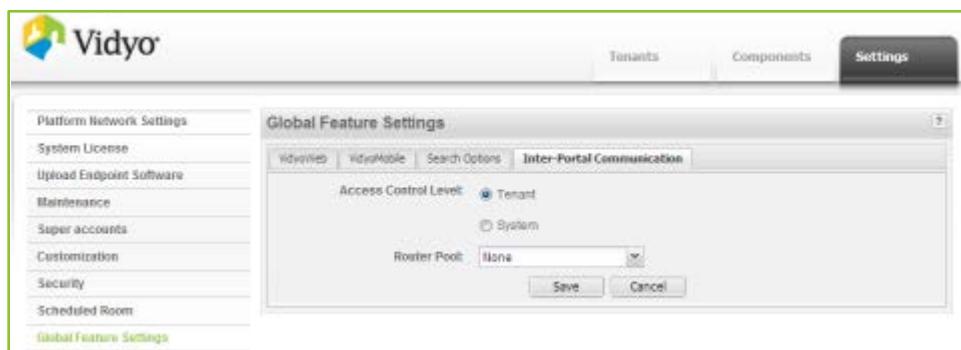
- An Allowed List only permits domains and addresses included on your list to interoperate on your domain. This type of list is often referred to as a whitelist.
- A Blocked List specifically disallows all domains and addresses included on your list from interoperating on your domain. This type of list is often referred to as a blacklist.

To configure system-wide IPC:

- Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

- Click the **Settings** tab.
- Click **Global Feature Settings** on the left menu.
- Click the **Inter-Portal Communication** tab.

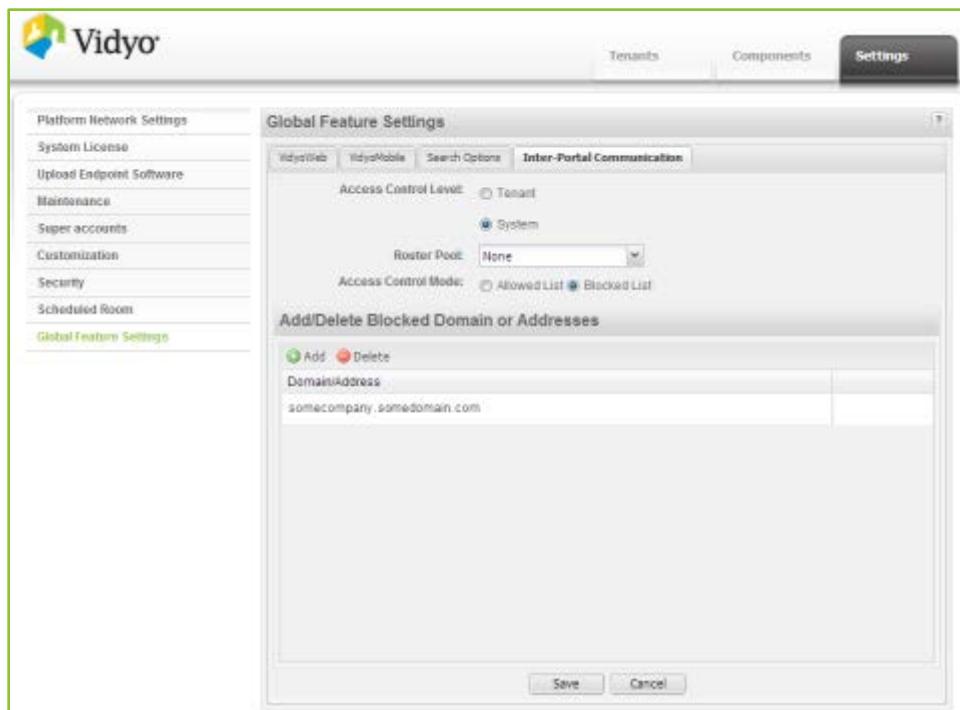


- Select **Tenant** to give Tenant Admins control over IPC.

For more information, see “Configuring Inter-Portal Communication (IPC) on Your Tenant” on page [267](#).

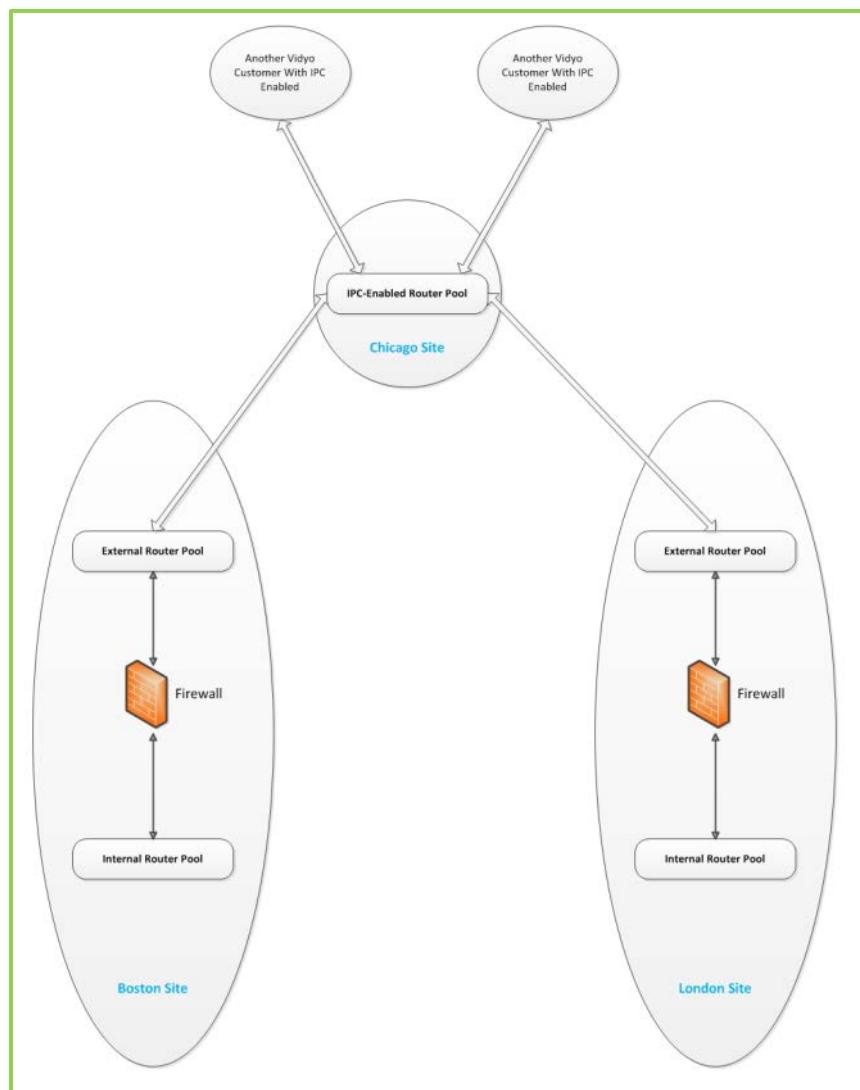
6. Configuring System Settings as the Super Admin

- 6.** In the Router Pool drop-down select a router pool if you have cascaded VidyoRouters.



The IPC-enabled router pool serves as a hub through which all IPC communication is routed.

For example, in the following configuration, this organization designated one of its router pools at the Chicago site to be IPC-enabled. (Chicago could have any number of any other router pools that are not IPC-enabled.)



For more information about router pools, see “VidyoCloud Management” on page [145](#).

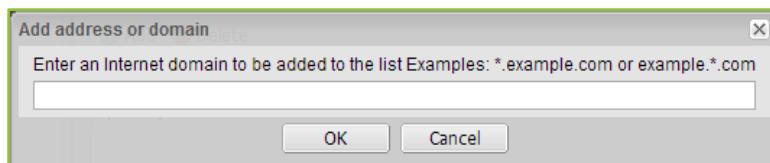
7. Select **System** if you want to control IPC system-wide over all tenants from settings made on this screen.

The Allowed List and Blocked List access control mode options appear:

- Select **Allowed List** to permit domains and addresses you add to interoperate on your domain. This type of list is often referred to as a whitelist.
- Select **Blocked List** to specifically disallow all domains and addresses you add from interoperating on your domain. This type of list is often referred to as a blacklist.

8. Click **Add** to add domains or addresses to your list.

The Add address or domain dialog box appears.



9. Enter the URL or domain name you want to add to the list and click **OK**.
10. Repeat the aforementioned steps to add as many domains or addresses to your list as desired.
11. Click **Save** to save your list.

Note: You can add or delete Domains and Addresses at any time.

Telling Your Users About IPC

The *VidyoPortal and VidyoDesktop User Guide* explain how your end users can take advantage of IPC if your organization has enabled it. However, you should keep them informed of IPC changes by following these suggestions:

- When you first enable IPC, whether upon installation or at some other time, be sure to send out a mass email to all of your users informing them that you have enabled IPC. Refer them to the *VidyoPortal and VidyoDesktop User Guide* for detailed information.
- Be sure to tell them whether they can interoperate with all domains except those on your Block list or if they can interoperate only with those domains on your Allowed list.
- Let them know whenever you add or delete a domain. You might want to include the full list reflecting the change if it's not overly long. You could also keep the list up-to-date on your intranet.
- Although your users should know how to use IPC from reading the *VidyoDesktop Quick User Guide*, it's probably a good idea to recap how to use IPC:

In the Contact Search field, they must enter the Vidyo address of the person they want to call using this format: **user_name@portal_name**.



Remind your users that although this looks like an email address, it's not. Rather, it's a unique Vidyo address. To call the user hhakston (who is on a different VidyoPortal), your users would have to enter his Vidyo user name (**hhakston**), the @ sign, and then the domain name of his VidyoPortal (in this case, it's **vidyo.phu.edu**). Then, they can click **Join Room**.

Remind them also that the **Join Room** button is the only way they can use IPC. The **Call Direct** button is dimmed because IPC can't be used to make a direct call.

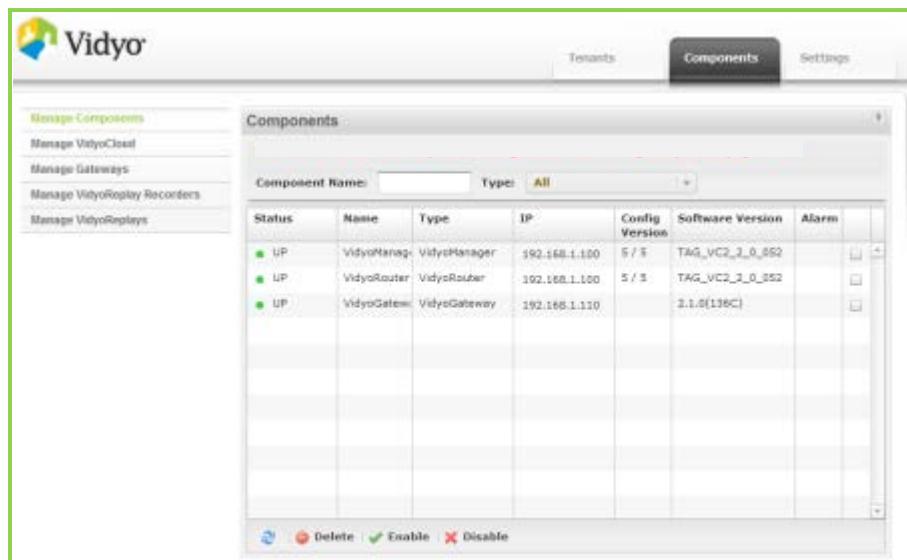
7. Configuring Your Components as the Super Admin

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.
Caution: Do not perform any tasks on the VidyoManager other than those described below. Many VidyoManager tasks including ones indicate in the following section should only be done under specific instruction from Vidyo Customer Support.
- **VidyoRouter** – Routes video and audio streams between endpoints and intelligently identifies and adjusts to bandwidth and network constraints. You can purchase VidyoRouters to increase your call capacity.
- **VidyoProxy** – A software component built into the VidyoRouter that enables authorized endpoints to connect while denying unauthorized connections. It also enables NAT and firewall traversal.
- **VidyoGateway** – An optional component that connects the VidyoPortal to legacy conferencing systems and landlines and cell phones (for voice-only participation). For more information about this component, refer to the *VidyoGateway Administrator Guide*.

USING THE COMPONENTS TABLE

The Manage Components table is used to view, delete, and manage the components in your system.



The screenshot shows the Vidyo Portal interface with a green border around the main content area. At the top, there's a navigation bar with tabs: 'Tenants' (disabled), 'Components' (selected), and 'Settings'. On the left, a sidebar has links: 'Manage Components' (highlighted in green), 'Manage VidyoCloud', 'Manage Gateways', 'Manage VidyoReplay Recorders', and 'Manage VidyoReplays'. The main area is titled 'Components' and contains a table with the following data:

Component Name:	Type:	All				
Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoManager	VidyoManager	192.168.1.100	5 / 5	TAG_VC2_3_0_352	<input type="checkbox"/>
UP	VidyoRouter	VidyoRouter	192.168.1.100	5 / 5	TAG_VC2_3_0_352	<input type="checkbox"/>
UP	VidyoGateway	VidyoGateway	192.168.1.110		3.1.0(138C)	<input type="checkbox"/>

At the bottom of the table are buttons: a blue circular icon, a red circular icon, 'Delete', 'Enable' (with a green checkmark), and 'Disable' (with a red X).

To use the Manage Components table:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Components in your VidyoPortal appear on the table and include component Status, Name, Type, IP, Config Version, Software Version, Alarm, and Delete fields as columns:

- a. The following statuses appear on the Manage Components table.
 - A green dot in the status column means it's installed and operating.
 - A yellow dot means the component is newly installed, but not configured yet.
 - A red dot means the component isn't working. Hover your mouse pointer over the red dot to read its alarm message.
 - A gray dot means the component is disabled, typically when you take a component offline while performing maintenance.
- b. The Name column shows the descriptive name you provided when installing a component.
- c. The type shows the specific type of component as VidyoManager, VidyoProxy, VidyoRouter, or VidyoGateway.
- d. The IP Address column shows the IP address you assigned to the component when you created it.
- e. The Configuration Version column shows a numeric tally on the left side of the slash. The number increases each time you change a component's configuration.

Note:

- Whenever you modify and save a component, the new configuration is assigned an incremental version number to distinguish it from previous component modifications saved on your VidyoPortal.
- Approximately every 15 seconds, your component communicates with your VidyoPortal and reports the configuration it is currently running. This is the number shown on the right side of the slash.
- If a new configuration version is available on your VidyoPortal, it is pushed to your component.
- Configuration version numbers do not appear for the optional VidyoGateway component.
- f. The Software Version column shows the latest software version to which the component has been upgraded.

- g. The Alarm column shows an alarm symbol when the component is not working properly. Hover your mouse pointer over it to read a brief description of the fault.
 - h. The check box column allows you to select one or more components to be deleted, enabled or disabled on your system.
- You can drag and drop the column headings to arrange them in the order you prefer.
4. Search by component name or type using the Component Name field or Type drop-down above the table.
 5. If desired, you can also select the Refresh, Delete, Enable, and Disable buttons:
 - Click **Refresh** to refresh the table.
 - Click **Delete** after selecting one or more components to be deleted from your system.
 - Click **Enable** after selecting one or more components to be enabled on your system.
 - Click **Disable** after selecting one or more components to be disabled on your system.

Note:

- You can access the Configuration Pages of each registered component by double-clicking the Status, Name or Type shown in the Components table.
- You can access the component's own local webpage configuration screen by clicking the IP Address shown in the Components table. The first page shown is the component's login page where you can log in using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

CONFIGURING YOUR VIDYOMANAGER COMPONENT

This section describes how to configure the VidyoManager.

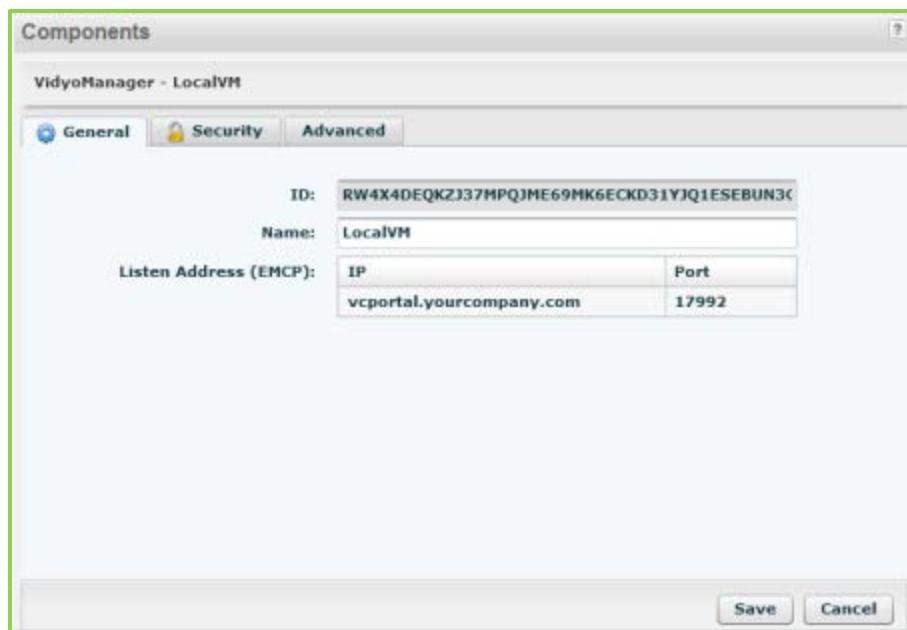
Entering General VidyoManager Information

To enter general VidyoManager information:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.
The Manage Components left menu item is selected by default.
3. Double-click on the VidyoManager line in the Components Table.

Note: To access the VidyoManager Component Configuration, double-click anywhere on the VidyoManager line in the Components Table, except on the IP address.

4. Click the **General** tab.



5. View and enter the following information:

- The ID shows your VidyoManager ID, which is automatically created and set by the system. This value cannot be changed.
- In the Name field, enter a display name or label for your VidyoManager.
- In the Listen Address (EMCP) fields, enter an EMCP address and port.

These address and port values are then used by VidyoDesktop, VidyoRoom and VidyoGateway clients to communicate with your VidyoManager.

Note:

- Do not change the address value unless required for NAT traversal or enabling Security.
- Before editing the EMCP settings, see “Firewall and NAT Deployments” on page [286](#) and “Security” on page [300](#).
- If you’re using FQDN licensing, the EMCP address is read-only.

Enabling VidyoManager Security

To enable VidyoManager security:

- Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

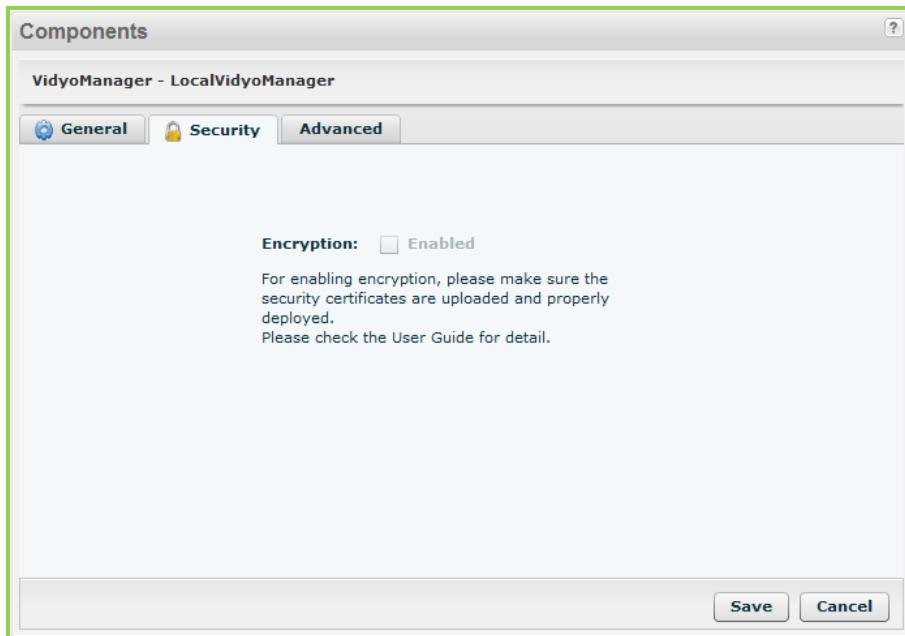
- Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click on the VidyoManager line in the Components Table.

Note: To access the VidyoManager Component Configuration, double-click anywhere on the VidyoManager line in the Components Table, except on the IP address.

4. Click the **Security** tab.



5. Select the **Enabled** check box to enable TLS (Transport Layer Security) security for the VidyoManager. Additional configuration is required. Your VidyoPortal doesn't have the proper encryption if the check box is disabled as shown previously. For information about enabling end-to-end security for your VidyoConferencing system, see "Security" on page [300](#).
6. Click **Save** to keep the setting.

Entering VidyoManager Advanced Information

To enter VidyoManager advanced information:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see "Logging in to the Super Admin Portal" on page [35](#).

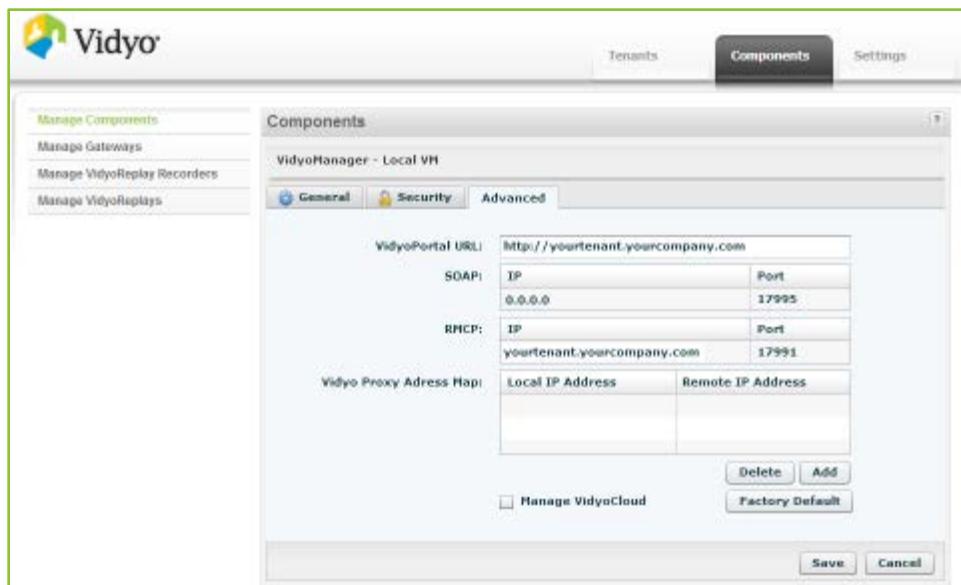
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click on the VidyoManager line in the Components Table.

Note: To access the VidyoManager Component Configuration, double-click anywhere on the VidyoManager line in the Components Table, except on the IP address.

4. Click the **Advanced** tab.



5. Only upon direction from Vidyo Customer Support should the following settings be changed:

Caution: These VidyoManager settings should only be done under specific instruction from Vidyo Customer Support.

- a. The VidyoPortal URL shows the address the VidyoManager uses to communicate with the VidyoPortal.
Note: Do not change this address.
- b. The SOAP IP and Port fields allow your VidyoPortal to communicate with your VidyoManager.
- c. The RMCP IP and Port fields allow your VidyoRouter to connect to the VidyoManager.
- d. Create or remove VidyoProxy address maps with local and remote IP address pairs using the Delete or Add buttons.
- e. Select the Manage VidyoCloud check box to enable the VidyoCloud left-menu.

After selecting the Manage VidyoCloud check box and clicking Save, you can configure VidyoRouter pools, location tags, endpoint rules, and inter-pool references.

For more information, see “Configuring VidyoCloud” on page [148](#).

- f. The Factory Default button returns your VidyoManager to the factory default settings.
6. Click **Save**.

ACCESSING YOUR 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.

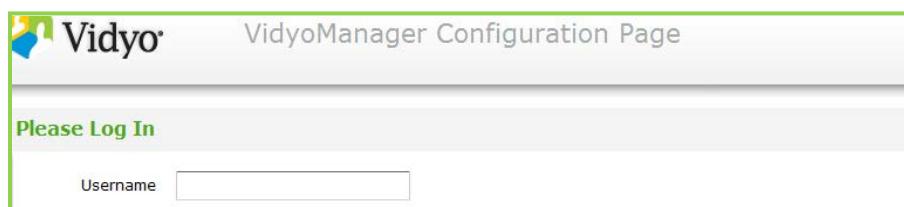
To log in to the VidyoManager Configuration Page:

1. Log in to your VidyoManager Configuration Page using your System Console account.

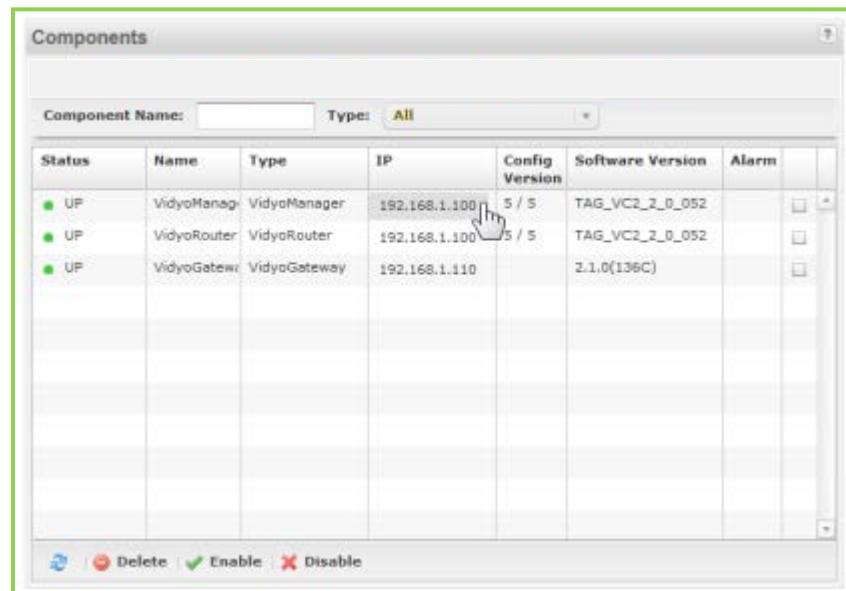
Note:

- The URL of your VidyoManager is your VidyoPortal domain name: <http://<FQDN or IP>/vm2conf/>. You can also click the VidyoManager IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoManager Configuration Page appears.



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



Configuring Basic Settings on Your VidyoManager

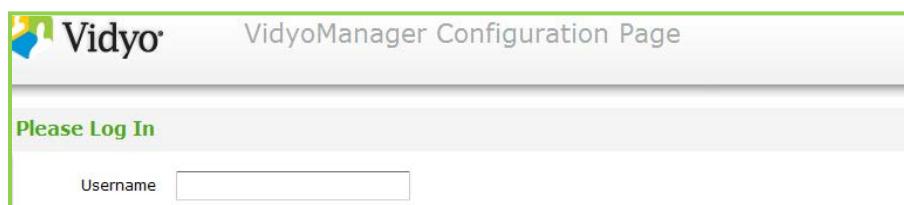
To configure basic settings on your VidyoManager:

1. Log in to your VidyoManager Configuration Page using your System Console account.

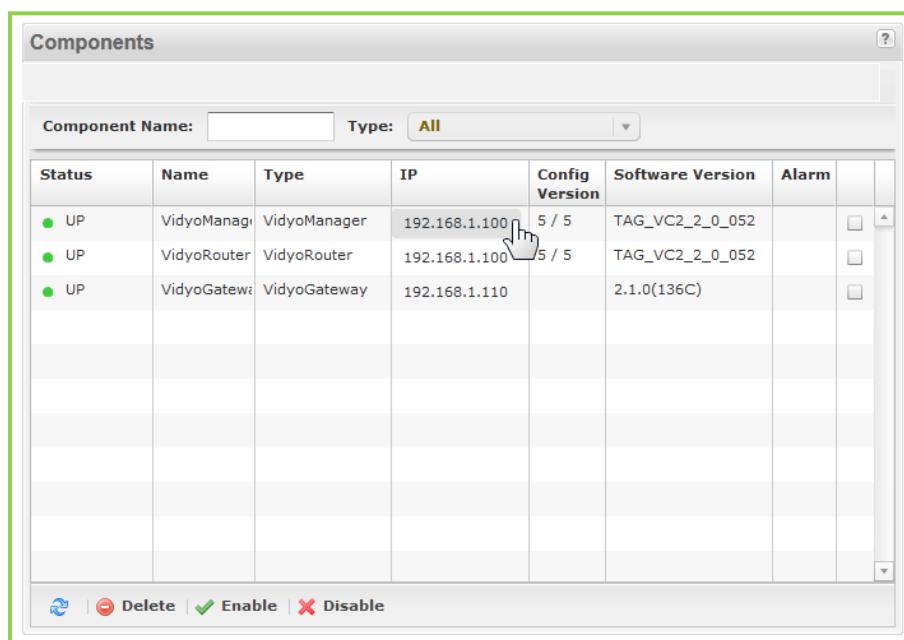
Note:

- The URL of your VidyoManager is your VidyoPortal domain name: <http://<FQDN or IP>/vm2conf/>. You can also click the VidyoManager IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoManager Configuration Page appears.

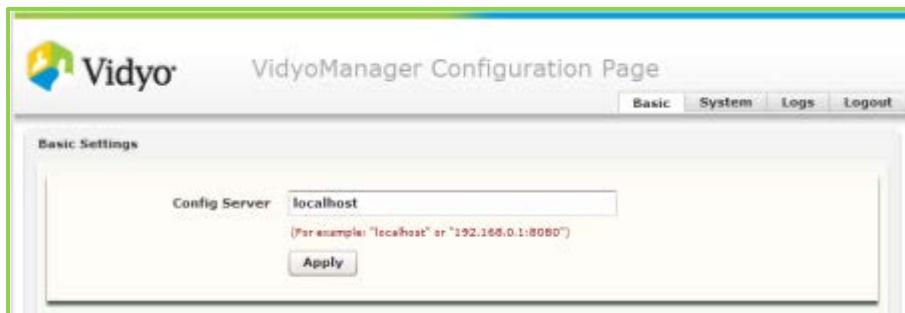


Note: An alternative route to this page is to click on the IP address of the VidyoManager in the Components page.



The Basic tab is shown by default.

2. The Config Server field tells the VidyoManager (and other components) where to look for their configuration information. Generally, “localhost” is entered in this field, although it could also contain the IP address or URL of your VidyoPortal. Do not change this address unless required for NAT traversal or enabling security. Before editing the Config Server settings, see “Firewall and NAT Deployments” on page [286](#) and “Security” on page [300](#).



Viewing System Settings on Your VidyoManager

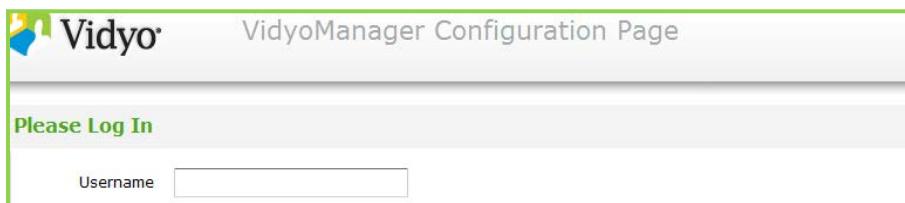
To view system settings on your VidyoManager:

1. Log in to your VidyoManager Configuration Page using your System Console account.

Note:

- The URL of your VidyoManager is your VidyoPortal domain name: <http://<FQDN or IP>/vm2conf/>. You can also click the VidyoManager IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoManager Configuration Page appears.



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

The screenshot shows a software interface titled "Components". At the top, there are search fields for "Component Name" and "Type" (set to "All"). Below is a table with columns: Status, Name, Type, IP, Config Version, Software Version, and Alarm. Three rows are listed:

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoManager	VidyoManager	192.168.1.100	5 / 5	TAG_VC2_2_0_052	<input type="checkbox"/>
UP	VidyoRouter	VidyoRouter	192.168.1.100	5 / 5	TAG_VC2_2_0_052	<input type="checkbox"/>
UP	VidyoGateway	VidyoGateway	192.168.1.110		2.1.0(136C)	<input type="checkbox"/>

At the bottom of the table area are buttons for Refresh, Delete, Enable, and Disable.

The Basic tab is shown by default.

2. Click the **System** tab.

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

The screenshot shows the "VidyoManager Configuration Page" with tabs for Basic, System, Logs, and Logout. The "System configuration" section contains the following fields:

- IP Address: [Input field]
- Subnet Mask: [Input field]
- Default Gateway: [Input field]
- Name Server: [Input field]
- Alt Name Server: [Input field]
- Hostname: [Input field]
- Mac Address: [Input field]
- System ID: [Input field]

Downloading Logs from Your VidyoManager

See the Audit section of this guide which contains “Downloading Audit Logs from Your VidyoManager” on page [273](#).

Logging Out of VidyoManager

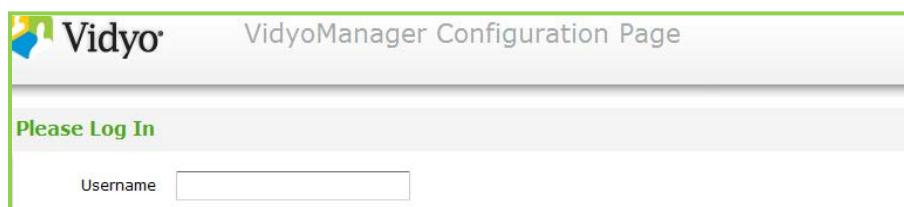
To log out of your VidyoManager:

1. Log in to your VidyoManager Configuration Page using your System Console account.

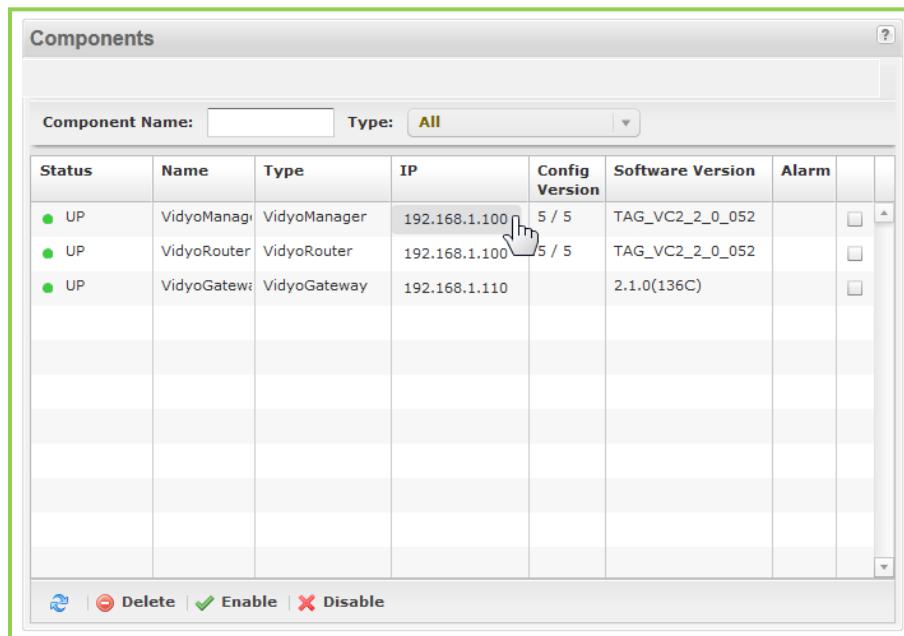
Note:

- The URL of your VidyoManager is your VidyoPortal domain name: <http://<FQDN or IP>/vm2conf/>. You can also click the VidyoManager IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoManager Configuration Page appears.



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



The Basic tab is shown by default.

2. Click the **Logout** tab.

3. Click **Logout**.

A dialog box appears asking to confirm your intent to logout of the VidyoManager.

4. Click **OK**.

CONFIGURING YOUR VIDYOROUTER COMPONENT

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

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	24 / 24	TAG_VC3_1_0_037	
UP	Local VM	VidyoManager	172.20.4.125	4 / 3	TAG_VC3_1_0_037	
UP	Local VP	VidyoProxy	172.20.4.125	20 / 0	TAG_VC3_1_0_037	
DOWN	vg484	VidyoGateway	172.16.4.84		3.0.0(96)	

Configuring VidyoRouter General Settings

To configure VidyoRouter general settings:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

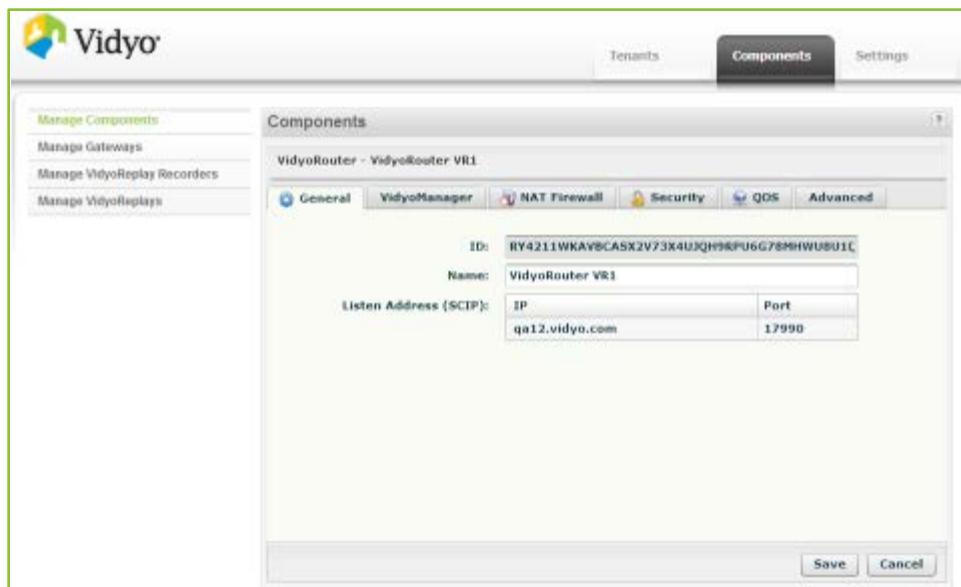
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click on the VidyoRouter line in the Components Table.

Note: To access the Component screen for the VidyoRouter, you must double-click anywhere on the VidyoRouter line in the Components Table, except on its IP address.

4. Click the **General** tab.



5. Enter the following information:
 - a. The ID shows your VidyoRouter ID, which is automatically created and set by the system. This value cannot be changed.
 - b. In the Name field, enter a display name or label for your VidyoRouter.

Note: This is the minimum required to authorize a VidyoRouter. It's a good idea to give your routers names that help you remember their locations, such as NYC VidyoRouter 1 and NYC VidyoRouter 2.

- c. In the SCIP Listen Address fields, enter a SCIP IP and port.

These IP and port values are then used by VidyoDesktop, VidyoRoom, and VidyoGateway clients to communicate with your VidyoRouter using Vidyo's proprietary network protocol. This is the listening address of the VidyoRouter. The default IP setting of o.o.o.o listens on all Ethernet ports.

Note:

- Don't change this address unless required for NAT traversal or enabling Security.
- Before editing SCIP settings, see "Firewall and NAT Deployments" on page [286](#) and "Security" on page [300](#).

Configuring VidyoManager Settings from the VidyoRouter

To configure VidyoManager settings from the VidyoRouter:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see "Logging in to the Super Admin Portal" on page [35](#).

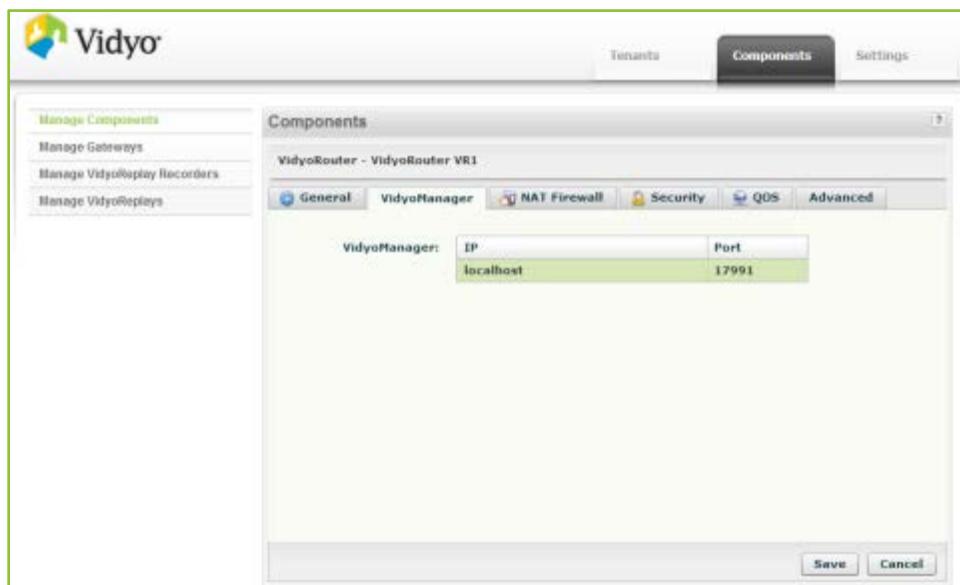
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click on the VidyoRouter line in the Components Table.

Note: To access the Component screen for the VidyoRouter, you must double-click anywhere on the VidyoRouter line in the Components Table, except on its IP address.

4. Click the **VidyoManager** tab.



5. Enter the address the VidyoRouter uses to communicate with the VidyoManager. Change this setting only if you're using full VidyoPortal security as outlined in "Security" on page [300](#).

Configuring VidyoRouter NAT Firewall Settings

This page is used for traversal of a NAT when the VidyoPortal and VidyoRouter are hosted behind a NAT. For more information, see "Firewall and NAT Deployments" on page [286](#).

To configure VidyoRouter NAT Firewall settings:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see "Logging in to the Super Admin Portal" on page [35](#).

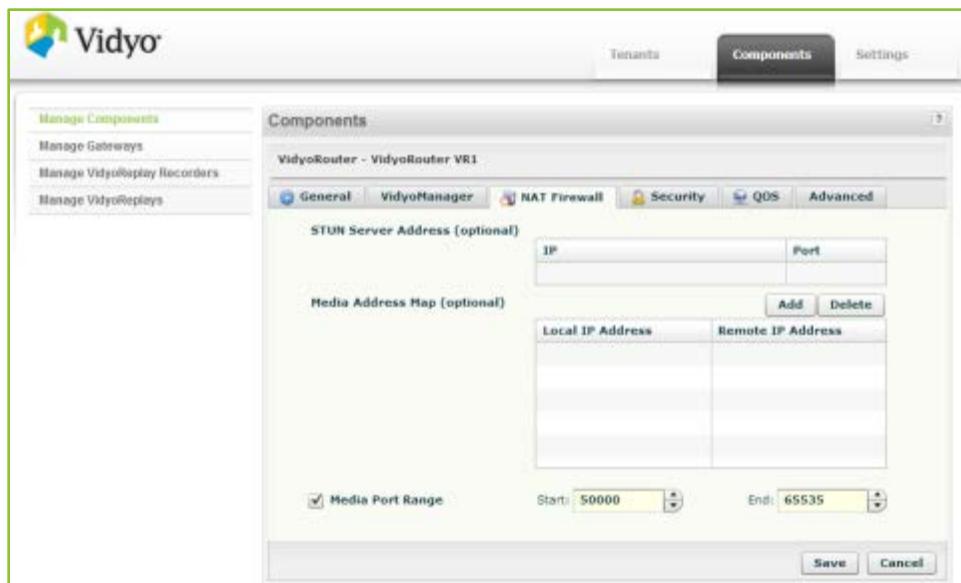
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click on the VidyoRouter line in the Components Table.

Note: To access the Component screen for the VidyoRouter, you must double-click anywhere on the VidyoRouter line in the Components Table, except on its IP address.

4. Click the **NAT Firewall** tab.



5. Enter the following information:

Note: The Media Address Map feature is the preferred configuration option. Only enter values for STUN Server Address fields or Media Address Map fields. Enabling both options, by entering values for each, causes the system to malfunction.

- a. In the STUN Server Address fields, enter an IP and port.

A STUN server generally uses port 3478.

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.

- b. In the Media Address Map fields, enter an IP and port.

If the system is NATed with a 1:1 port mapping, hence no port translation, you can define local \leftrightarrow public address mappings.

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

- c. Select the **Media Port Range** check box and provide Start and End port numbers. If only one port is available, enter the same port number in each Start and End field.

This allows you to define a range of ports available in your firewall.

Enabling VidyoRouter Security

To enable VidyoRouter security:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page 35.

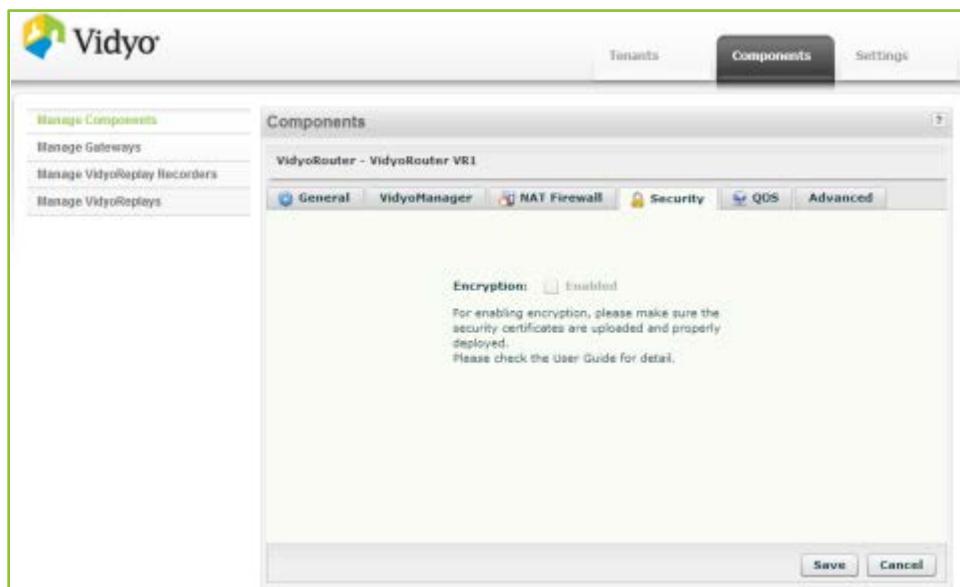
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click on the VidyoRouter line in the Components Table.

Note: To access the Component screen for the VidyoRouter, you must double-click anywhere on the VidyoRouter line in the Components Table, except on its IP address.

4. Click the **Security** tab.



5. Select the **Enabled** check box to enable TLS (Transport Layer Security) security.

Your VidyoPortal doesn't have the proper encryption if the check box is disabled as shown previously. For information about enabling end-to-end security for your VidyoConferencing system, see "Security" on page [300](#).

6. Click **Save** to keep the setting.

Configuring VidyoRouter Quality of Service (QoS)

This page allows you to set differentiated services code point (DSCP) values for audio, video, and content coming from your VidyoRouter to various endpoints. Audio, video, and content data coming from your VidyoRouter is assigned corresponding values you set on this screen.

With these specified values assigned to media types coming from your VidyoRouter, you can then configure your network router or switch to prioritize the packets as desired.

To configure Quality of Service values in your VidyoRouter:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see "Logging in to the Super Admin Portal" on page [35](#).

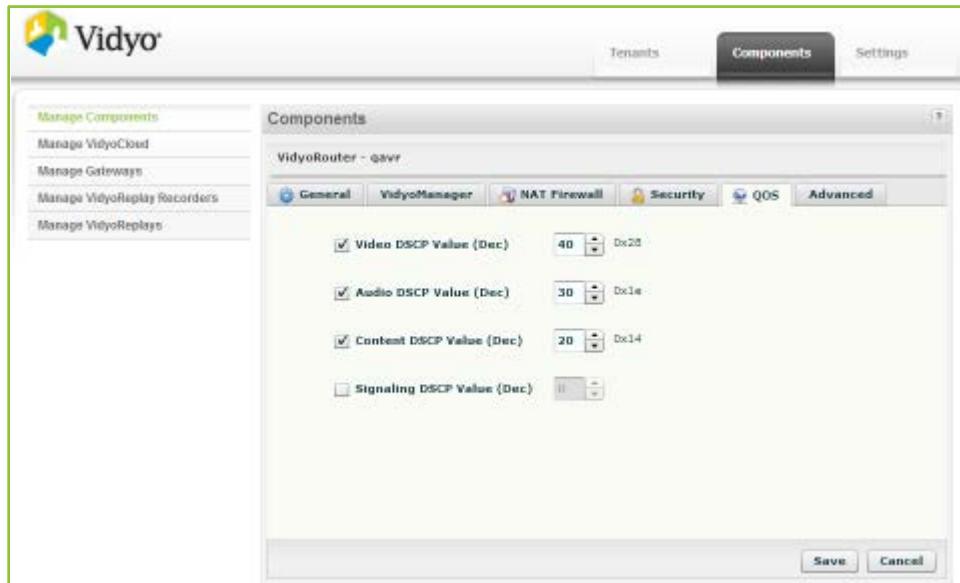
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click on the VidyoRouter line in the Components Table.

Note: To access the Component screen for the VidyoRouter, you must double-click anywhere on the VidyoRouter line in the Components Table, except on its IP address.

4. Click the **QoS** tab.



5. Optionally select Video, Audio, Content, and Signaling DSCP values as desired and provide corresponding decimal values. If no values are provided, they all default to zero.

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

For more information about setting DSCP for endpoints on your tenants, see “Configuring Quality of Service (QoS) on Your Tenant” on page [269](#).

Restoring VidyoRouter to Factory Default Settings

To restore your VidyoRouter to factory default settings:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

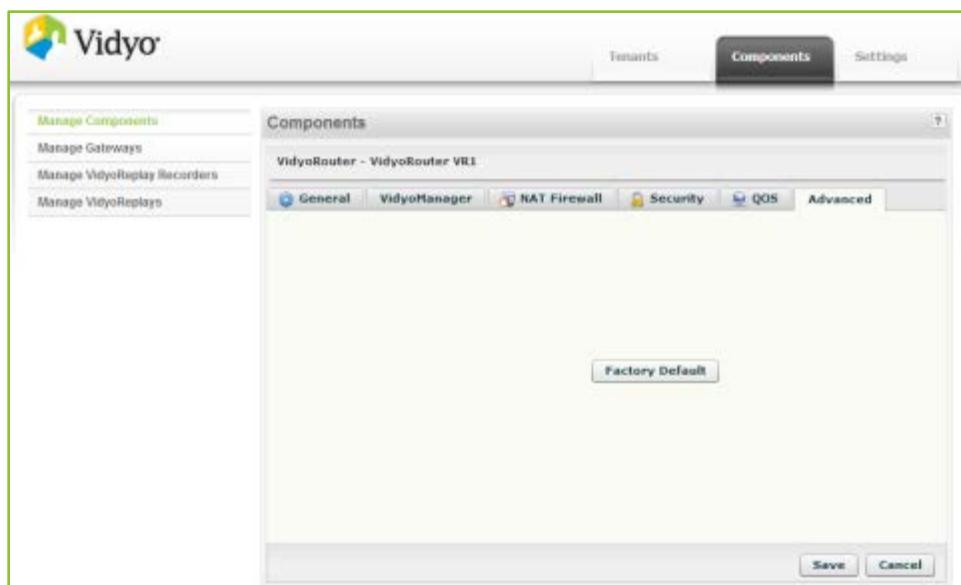
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

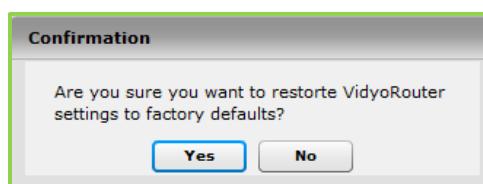
3. Double-click on the VidyoRouter line in the Components Table.

Note: To access the Component screen for the VidyoRouter, you must double-click anywhere on the VidyoRouter line in the Components Table, except on its IP address.

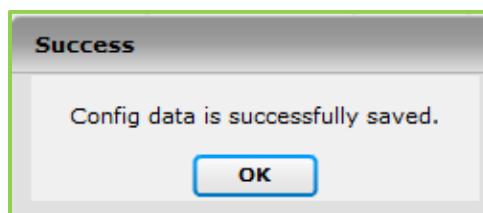
- Click the **Advanced** tab.



- Click **Factory Default** and a dialog box appears asking you to confirm restoring the factory settings. Click **Yes**.



- A second dialog box appears confirming the data was successfully saved. Click **OK**.



ACCESSING YOUR VIDYOROUTER CONFIGURATION PAGE

Configuring Basic Settings on Your VidyoRouter

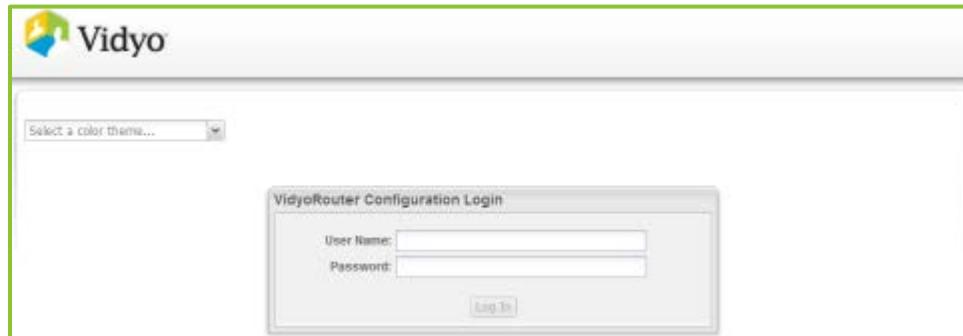
To configure basic settings on your VidyoRouter:

- Log in to your VidyoRouter using your System Console account.

Note:

- The URL of your VidyoRouter is typically a domain name: <http://<FQDN or IP>/vr2conf/>. You can also click the VidyoRouter IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoRouter Component Configuration appears.



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

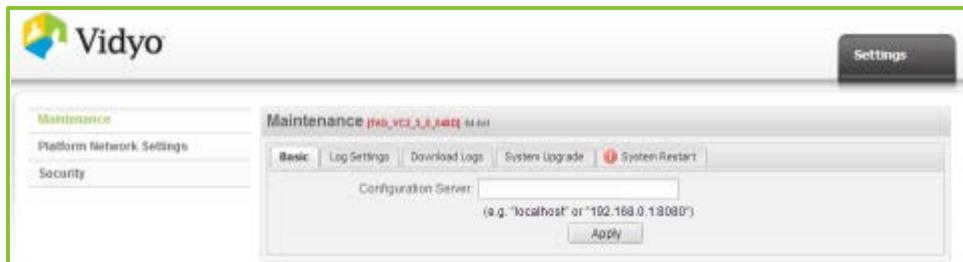
Components								
Component Name:		Type:	All					
Status	Name	Type	IP	Config Version	Software Version	Alarm		
● UP	VidyoManager	VidyoManager	192.168.1.100	5 / 5	TAG_VC2_2_0_052	<input type="checkbox"/>		
● UP	VidyoRouter	VidyoRouter	192.168.1.100	5 / 5	TAG_VC2_2_0_052	<input type="checkbox"/>		
● UP	VidyoGateway	VidyoGateway	192.168.1.110		2.1.0(136C)	<input type="checkbox"/>		

At the bottom of the table, there are four buttons: a refresh icon, a delete icon, an enable icon, and a disable icon.

The Basic tab is shown by default.

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

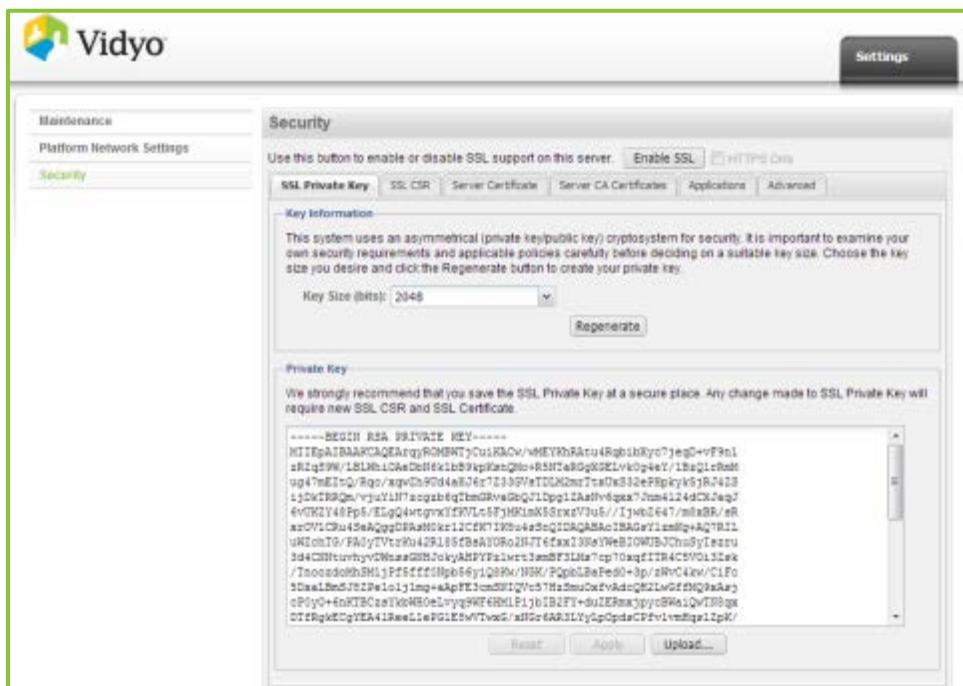
The Configuration Server field tells the VidyoRouter where to look for its configuration information. For VidyoRouters, it's the FQDN or IP of your VidyoPortal.



3. Enter the FQDN or IP address of your VidyoPortal.
4. Click **Apply** for the VidyoRouter to register.

Configuring Security on Your VidyoRouter

Entering information on this tab is optional. For detailed VidyoRouter security information, see “Security” on page [300](#).



Viewing System Information on Your VidyoRouter

To view system information on your VidyoRouter:

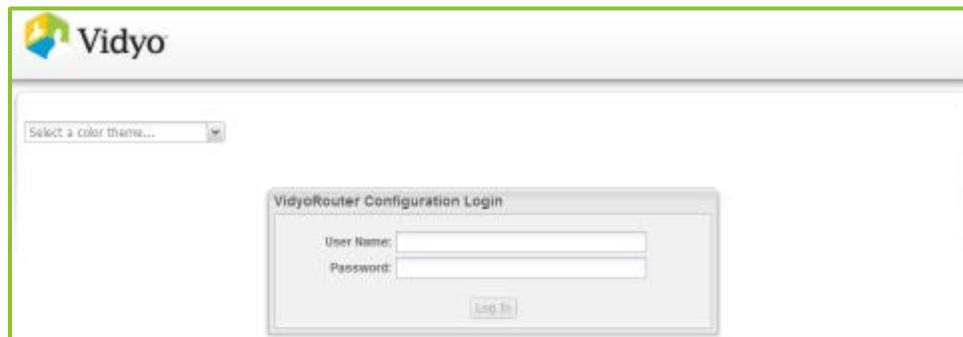
1. Log in to your VidyoRouter using your System Console account.

Note:

- The URL of your VidyoRouter is typically a domain name: <http://<FQDN or IP>/vr2conf/>. You can also click the VidyoRouter IP address on the Components tab in your VidyoPortal.

- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page 23.
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoRouter Configuration Page appears.



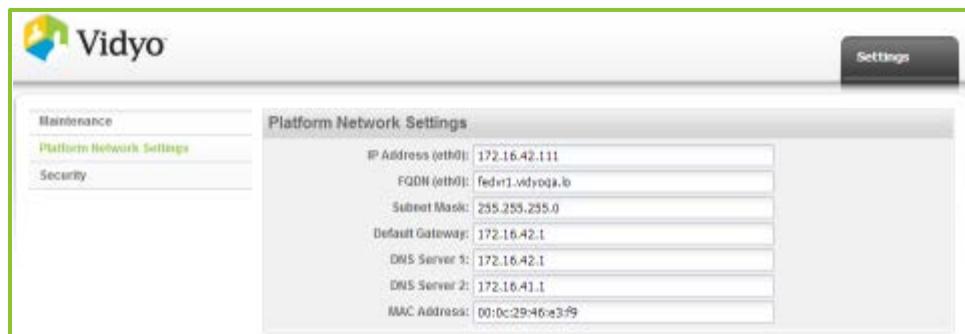
Note: An alternative route to this page is to click on the IP address of the VidyoRouter in the Components page.

Components								
Component Name:		Type:	All					
Status	Name	Type	IP	Config Version	Software Version	Alarm		
● UP	VidyoManager	VidyoManager	192.168.1.100	5 / 5	TAG_VC2_2_0_052		<input type="checkbox"/>	<input type="checkbox"/>
● UP	VidyoRouter	VidyoRouter	192.168.1.100	5 / 5	TAG_VC2_2_0_052		<input type="checkbox"/>	<input type="checkbox"/>
● UP	VidyoGateway	VidyoGateway	192.168.1.110		2.1.0(136C)		<input type="checkbox"/>	<input type="checkbox"/>

The Basic tab is shown by default.

2. Click **Platform Network Settings** on the left menu.

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



Downloading Logs from Your VidyoRouter

See the Audit section of this guide which contains “Downloading Audit Logs from Your VidyoRouter” on page [274](#).

Upgrading Your VidyoRouter

Caution: Upgrades cannot be rolled back. In addition, when the system is restarted or shut down, all calls in progress are ended.

Before you perform a system upgrade, Vidyo highly recommends that you read the Release Notes that pertain to your upgrade version. In addition, you might want to email users ahead of time and perform the upgrade when system usage is lowest.

To upgrade any VidyoRouters:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Click on the VidyoRouter IP address (as shown in the following illustration) or browse to <http://<VidyoRouter Server FQDN or IP>/vr2conf/> to access the VidyoRouter Configuration Page.

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	LocalVM	VidyoManager	192.168.1.201	1 / 1	TAG_VC2_1_4_158	
UP	LocalVR	VidyoRouter	192.168.1.201	1 / 1	TAG_VC1_1_4_158	
UP	LocalProxy	VidyoProxy	192.168.1.201	1 / 1	TAG_VC2_1_4_158	
UP	SA_VR1	VidyoRouter	192.168.1.201	1 / 1	TAG_VC2_1_4_158	
UP	SA_VR1_Pro	VidyoProxy	192.168.1.202	1 / 1	TAG_VC2_1_4_158	

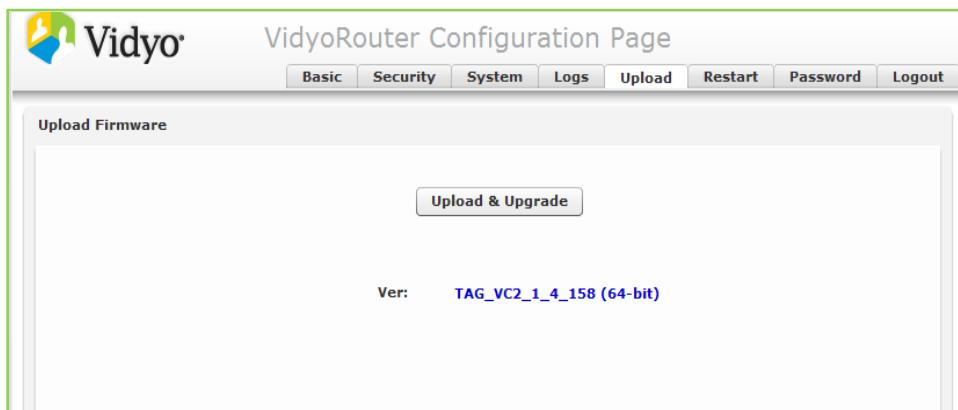
4. Enter your VidyoRouter Administrator username and password.

The default username is **admin** and the default password is **password**.

5. Click **Login**.

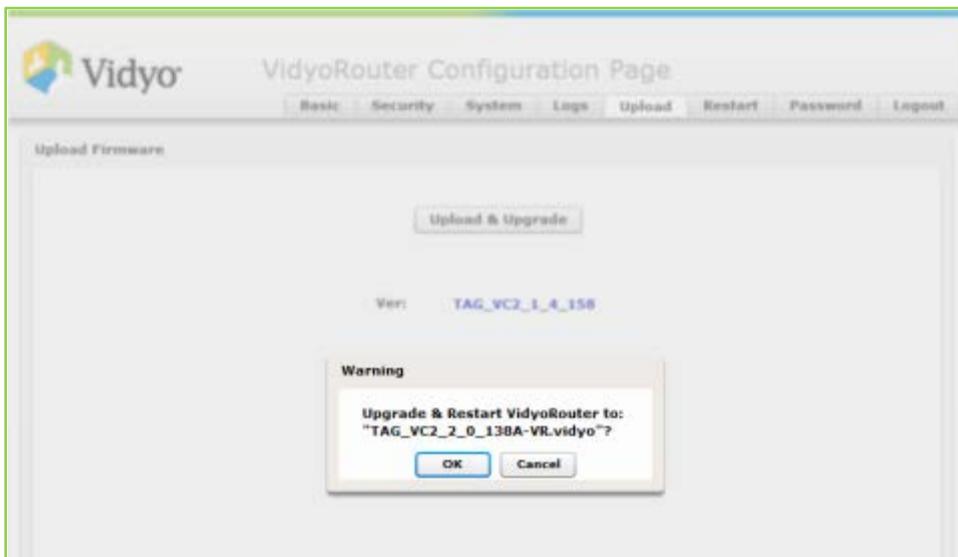
The VidyoRouter Configuration Page appears.

6. Click the **Upload** tab.



Note: You can determine your VidyoRouter type by the Version label (**Ver:**) displayed on the VidyoRouter Configuration Page Upload tab. If the version ends in **(64-bit)**, as shown in the previous illustration, then the VidyoRouter type is 64-bit. Otherwise, the VidyoRouter type is 32-bit as shown in the following illustration.

7. Click **Upload & Upgrade**.



8. Click **OK** to proceed with the upgrade.

Wait for the installation to complete.

9. After the VidyoRouter reboots, return to the Super Admin portal and click the **Components** tab.

Caution: The VidyoRouter (and corresponding VidyoProxy) may both have a Status of DOWN or NEW, or they may show an Alarm (as shown in the following illustration). Do not attempt to reconfigure the NEW or delete the DOWN component, or attempt to clear the Alarm at this time. Each will update or clear automatically once the VidyoPortal is upgraded.

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	25 / 0	TAG_VC3_1_0_03	
UP	Local VM	VidyoManager	172.20.4.125	4 / 4	TAG_VC3_1_0_037	
UP	Local VP	VidyoProxy	172.20.4.125	10 / 0	TAG_VC3_1_0_037	
DOWN	vg484	VidyoGateway	172.16.4.84		3.0.0(96)	

10. Verify that the Software Version displayed is correct for the VidyoRouter that you upgraded.
11. Repeat the steps in this section for each additional VidyoRouter for your VidyoConferencing system.

Restarting Your VidyoRouter

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

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

Logging Out of Your VidyoRouter

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

CONFIGURING VIDYOROUTERS AND VIDYOPROXYS USING THEIR CONFIGURATION PAGES

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

VidyoRouters need to be configured in order to register with the VidyoPortal Configuration Pages. Each VidyoRouter comes bundled with a VidyoProxy component that you must also configure in order for it to register to the Configuration Page.

This section describes how to configure VidyoRouter and VidyoProxy Configuration Page addresses as well as how to configure these new components using the Configuration Server.

Before you configure the VidyoRouter and VidyoProxy, you must configure their Configuration Page addresses. The following procedures show you how.

Setting the Configuration Page Address of Your VidyoRouter

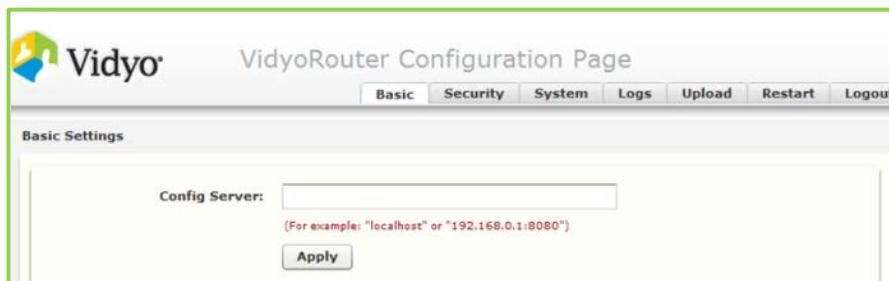
To set the Configuration Page address of your VidyoRouter:

1. Log in to your VidyoRouter using your System Console account.

Note:

- The URL of your VidyoRouter is typically a domain name: <http://<FQDN or IP>/vr2conf/>. You can also click the VidyoRouter IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoRouter Configuration Page appears.



The Config Server field tells the VidyoRouter (and other components) where to register for its configuration information. The Config Server is the IP address or FQDN of the VidyoPortal.

2. Enter the VidyoPortal IP Address or FQDN.
3. Click **Apply** to register the VidyoRouter.

Setting the Configuration Page Address of Your VidyoProxy

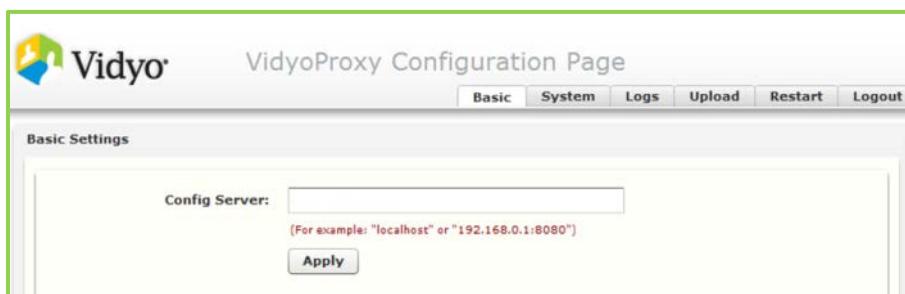
To set the Configuration Page Address of your VidyoProxy:

1. Log in to your VidyoProxy using your System Console account.

Note:

- The URL of your VidyoProxy is typically a domain name: <http://<FQDN or IP>/vp2conf/>. You can also click the VidyoProxy IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoProxy Configuration Page appears.



The Config Server field tells the VidyoProxy, and other components, where to register for their configuration information. For a Standalone VidyoProxy, the Configuration Server is the IP address or URL of the VidyoPortal.

2. Enter the VidyoPortal IP address or FQDN.
3. Click **Apply** to register the VidyoProxy.

If you’re deploying the VidyoRouter and VidyoProxy in a NATed environment and/or with SSL or encryption, each must use the VidyoPortal FQDN as the Config Server address. For more information, see “Firewall and NAT Deployments” on page [286](#) and “Security” on page [300](#). Also, see “VidyoRouter Configuration” on page [163](#) for information about the other tabs on the VidyoRouter and VidyoProxy configuration pages.

Configuring a VidyoRouter using its Configuration Page

After you apply the Configuration Server settings, the component’s Status is shown as **NEW** on the Super Admin Components table. You must now configure each new component to function within the system.

To configure a VidyoRouter using the Configuration Page:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click the word NEW in the Status column of the VidyoRouter you wish to configure.

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	Local VP	VidyoProxy	192.168.1.100	1 / 1	TAG_VC2_1_0_058	
UP	Local VM	VidyoManager	192.168.1.100	1 / 1	TAG_VC2_1_0_058	
UP	Local VR	VidyoRouter	192.168.1.100	1 / 1	TAG_VC2_1_0_058	
NEW		VidyoRouter	192.168.1.105	0 / 0	TAG_VC2_1_0_058	
NEW		VidyoProxy	192.168.1.105	0 / 0	TAG_VC2_1_0_058	

4. In the Name field, enter a name for your VidyoRouter.

For example: VR or VR1.

ID:	RY4211WKAVBCASX2V73X4U3QH98PU6G78MHWU8UIC				
Name:	VidyoRouter VR1				
Listen Address (SCIP):	<table border="1"> <tr> <td>IP</td> <td>Port</td> </tr> <tr> <td>qa12.vidyo.com</td> <td>17990</td> </tr> </table>	IP	Port	qa12.vidyo.com	17990
IP	Port				
qa12.vidyo.com	17990				

5. Do not change the 0.0.0.0 SCIP Listen Address unless you're deploying the router in a NATed environment and with security (SSL and encryption).

For more information, see “Firewall and NAT Deployments” on page [286](#) and “Security” on page [300](#).

6. Click **Save**.

7. Click **OK** in the Confirmation dialog box to confirm the changes.

Configuring a Standalone VidyoProxy using its Configuration Page

To configure a Standalone VidyoProxy using the Configuration Page:

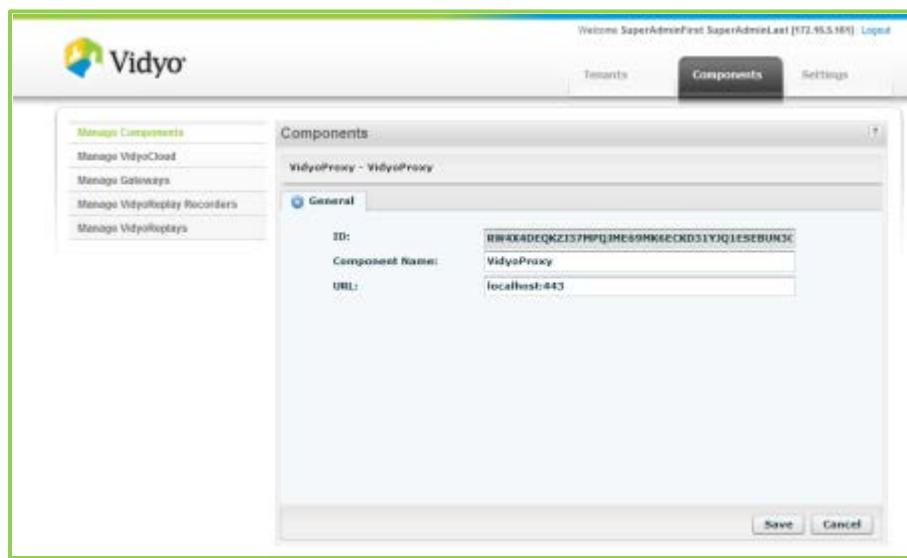
1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.
The Manage Components left menu item is selected by default.
3. Double-click the word **NEW** in the Status column of the VidyoProxy you wish to configure.

Status	Name	Type	IP	Config Version	Software Version	Alarm
DISABLED	VidyoProxy	vidyoProxy	192.168.1.100	1 / 0	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	LocalVN	vidyoManager	192.168.1.100	9 / 9	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	DEFAULT_NU	vidyoRouter	192.168.1.105	3 / 3	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	VidyoGateway	VidyoGateway	192.168.1.110		2.2.0(283)	<input type="checkbox"/>
UP	VidyoRecord	VidyoProxyReco	192.168.1.115		2.2.0(283)	<input type="checkbox"/>
NEW	VidyoRecord	VidyoProxy	192.168.1.108	0 / 0	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	VidyoReplay	VidyoReplay	192.168.1.115		2.2.0.201	<input type="checkbox"/>

Buttons at the bottom: Refresh, Delete, Enable, Disable.

4. In the Name field, enter a name for your VidyoProxy.

For example: **Standalone VP** or **SAVP1**.



5. In the URL field, change **localhost** to the Standalone VidyoProxy server address or FQDN, and then enter a colon and the port you wish the VidyoProxy to use (such as **vp1.yourcompany.com:443**).

Note: Vidyo recommends using port 443 for the VidyoProxy to allow for typical access available for restricted clients.

6. Click **Save**.
7. Click **OK** in the Confirmation dialog box to confirm the changes.

VIDYOGATEWAY CONFIGURATION

A VidyoGateway is the optional component that permits calls from legacy devices that support SIP, H.323, and video conferencing endpoints such as land lines and cell phones, to participate in videoconferences.

Note: Telephones can send and receive only the audio portion of the teleconference.

VidyoGateway configuration requires cumulative steps performed on both the VidyoPortal and the Vidyo-Gateway as described in the following procedures:

Making Initial VidyoGateway Configurations on Your VidyoPortal

To initially configure VidyoGateway on your VidyoPortal:

1. Add the VidyoGateway as a component to the VidyoConferencing system.
For more information, see “Adding a VidyoGateway to Your VidyoPortal” on page [143](#).
2. Assign the VidyoGateway to a tenant. If you are running a multi-tenant system, assign it to appropriate tenants.
For more information, see “Configuring a Tenant” on page [187](#).

Making Initial VidyoGateway Configurations on Your VidyoGateway

To initially configure VidyoGateway on your VidyoGateway:

3. Configure your VidyoGateway to communicate with your VidyoPortal.
For more information, refer to the *VidyoGateway Administrator Guide*.
4. If desired, set up call services to enable dialing between the VidyoGateway and your Legacy system, or use any of the predefined services.
For more information, refer to the *VidyoGateway Administrator Guide*.
5. Perform additional VidyoGateway configuration options as needed, create VidyoGateway clusters if desired, and integrate VoIP phones and IP PBXs as needed.
For more information, refer to the *VidyoGateway Administrator Guide*.

Making Initial VidyoGateway Configurations on Your VidyoPortal (Continued)

To configure VidyoGateway on your VidyoPortal (continued):

6. For convenient access to Legacy systems (if you have them), add your video device in your directory using **Users > Add Legacy Device** in your VidyoConferencing system Admin Portal.
For more information, see “Adding a Legacy Device” on page [208](#).

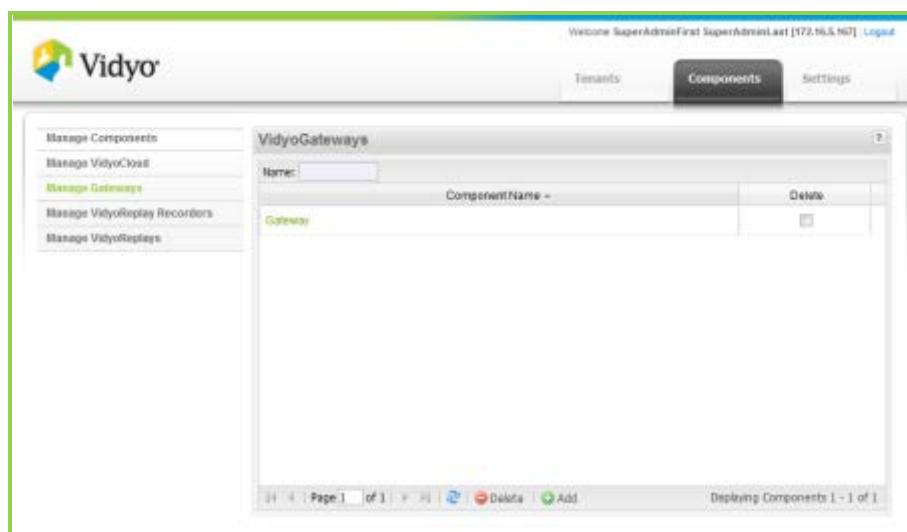
As mentioned previously, if you are performing an initial VidyoGateway setup, you must add the VidyoGateway as a component to the VidyoConferencing system. For more information, see “Adding a VidyoGateway to Your VidyoPortal” on page [143](#).

Adding a VidyoGateway to Your VidyoPortal

To add a VidyoGateway to your VidyoPortal:

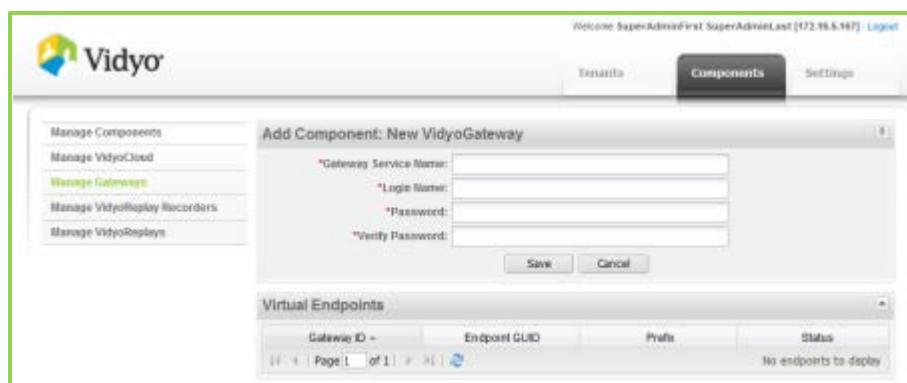
1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.

3. Click **Manage Gateways** on the left menu.



4. Click **Add** at the bottom of the page.

The Add Component: New VidyoGateway page appears.



5. In the **Gateway Service Name** field, enter a descriptive name for the VidyoGateway.
6. In the **Login Name** field, enter the VidyoGateway login name for VidyoPortal registration and authentication.
7. In the **Password** field, enter the VidyoGateway password for VidyoPortal registration and authentication.
8. In **Verify Password**, re-enter the password.
9. Click **Save**.

When the VidyoGateway registers, its list of configured services is shown in the Virtual Endpoints table.

- To refresh the table, click **Refresh**.

- To scroll through any pages of listed services, click the Page direction arrows.
- To delete an existing VidyoGateway, select the check box in the far right column, and then click **Delete** at the bottom of the page.

VIDYOREPLAY RECORDER AND VIDYOREPLAY CONFIGURATION

A VidyoReplay Recorder is the optional component that adds webcast recording, cataloging and replay of VidyoConferences to a VidyoConferencing system. VidyoReplay is the optional component that records VidyoConferences on your VidyoConferencing system.

VidyoReplay Recorder and VidyoReplay configurations require cumulative steps performed on both the VidyoPortal and the VidyoReplay as described in the following procedures. Therefore, you must repeat these procedures on both the VidyoReplay Recorder and VidyoReplay.

Making Initial VidyoReplay Recorder or VidyoReplay Configurations on Your VidyoPortal

To initially configure VidyoReplay Recorder or VidyoReplay on your VidyoPortal:

1. Add the VidyoReplay Recorder or VidyoReplay as a component to the VidyoConferencing system.
For more information, see “Adding a VidyoReplay Recorder to Your VidyoPortal” on page [146](#) and “Adding a VidyoReplay to Your VidyoPortal” on page [147](#).
2. Assign the VidyoReplay Recorder and VidyoReplay Component to a tenant. If you are running a multi-tenant system, assign it to appropriate tenants.
For more information, see “Configuring a Tenant” on page [187](#).

Making Initial VidyoReplay Recorder or VidyoReplay Configurations on Your VidyoReplay

To initially configure VidyoReplay Recorder or VidyoReplay on your VidyoReplay:

3. Setup your VidyoReplay Recorder or VidyoReplay accounts and configure them to communicate with your VidyoPortal.
For more information, refer to the *VidyoReplay Administrator Guide*.

Making Initial VidyoReplay Recorder or VidyoReplay Configurations on Your VidyoPortal (Continued)

To configure VidyoReplay Recorder or VidyoReplay on your VidyoPortal (continued):

4. Configure your Tenant to use your VidyoReplay Recorder and VidyoReplay.
For more information, see “Configuring a Group for VidyoReplay Recorder and VidyoReplay Use” on page [232](#).

Note: If you are performing an initial VidyoReplay Recorder and VidyoReplay setup, you must add both as components in your VidyoConferencing system. For more information, see “Adding a VidyoReplay Recorder to Your VidyoPortal” on page [146](#) and “Adding a VidyoReplay to Your VidyoPortal” on page [147](#).

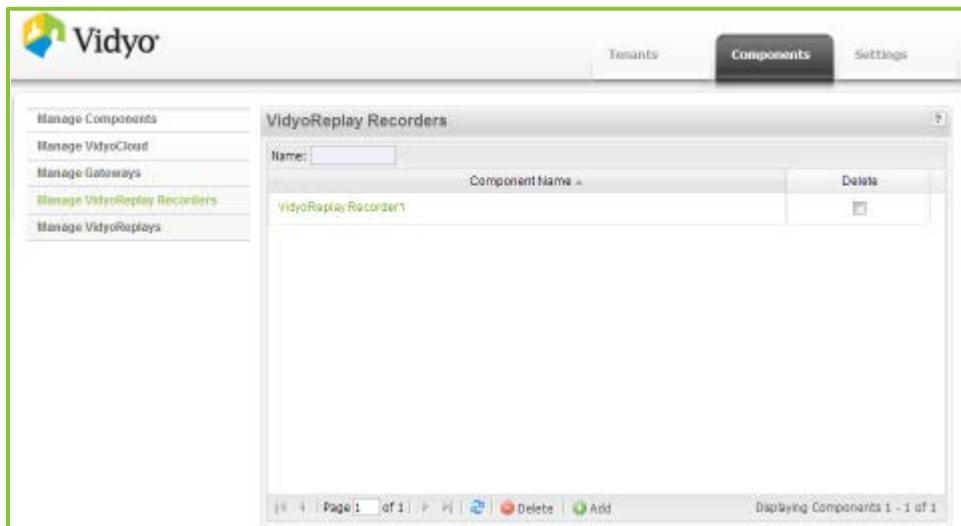
Adding a VidyoReplay Recorder to Your VidyoPortal

To add a VidyoReplay Recorder to your VidyoPortal:

1. Log in to the Super Admin portal using your Super Admin account.

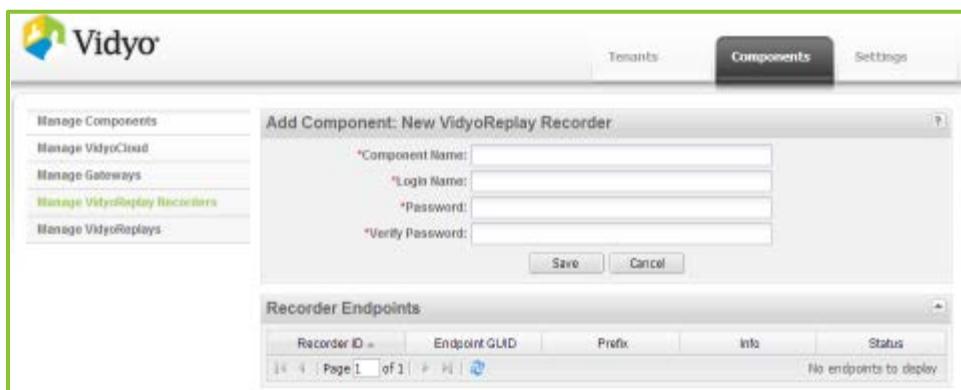
For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.
3. Click **Manage VidyoReplay Recorders** on the left menu.



4. Click **Add** at the bottom of the page.

The Add Component: New VidyoReplay Recorder page appears.



5. In the Component Name field, enter a descriptive name for your VidyoReplay Recorder.
6. In the Login Name field, enter the VidyoReplay Recorder login name for VidyoPortal registration and authentication.
7. In the Password field, enter the VidyoReplay Recorder password for VidyoPortal registration and authentication.
8. In Verify Password, re-enter the password.
9. Click **Save**.

When the VidyoReplay Recorder registers, its list of configured services is shown in the Virtual End-points table.

- To refresh the table, click **Refresh**.
- To scroll through any pages of listed services, click the Page direction arrows.
- To delete an existing VidyoReplay Recorder, select the check box in the far right column, and then click **Delete** at the bottom of the page.

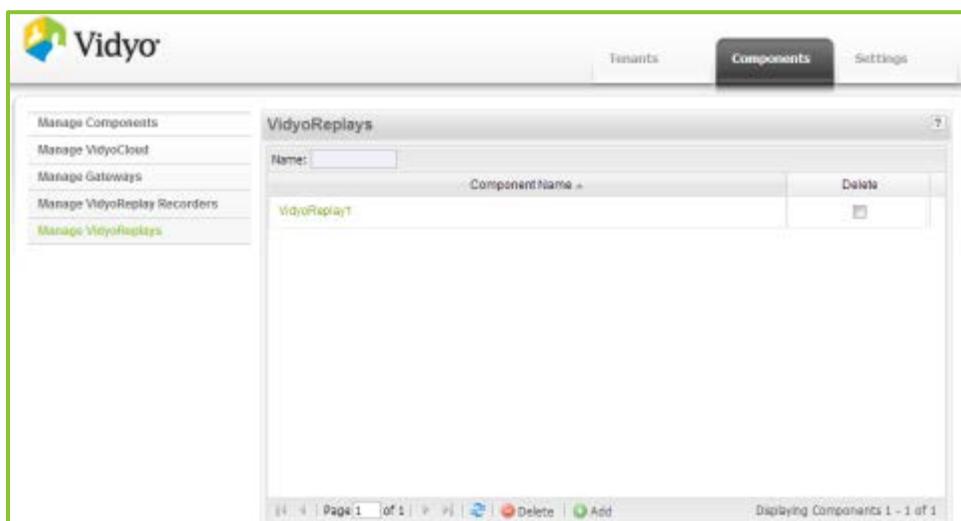
Adding a VidyoReplay to Your VidyoPortal

To add a VidyoReplay to your VidyoPortal:

1. Log in to the Super Admin portal using your Super Admin account.

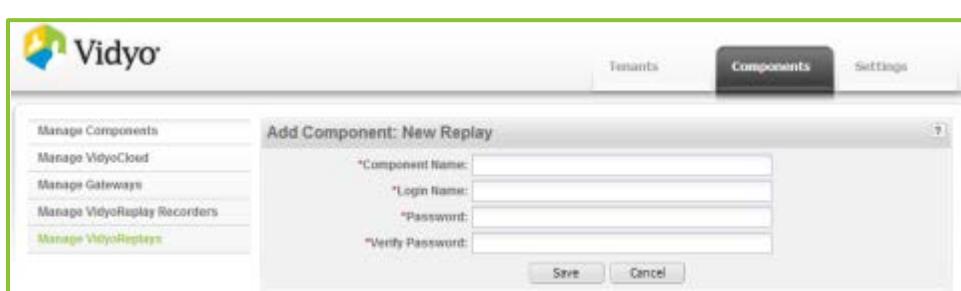
For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.
3. Click **Manage VidyoReplays** on the left menu.



4. Click **Add** at the bottom of the page.

The Add Component: New VidyoReplay page appears.



5. In the Component Name field, enter a descriptive name for your VidyoReplay.

6. In the Login Name field, enter the VidyoReplay login name for VidyoPortal registration and authentication.
7. In the Password field, enter the VidyoReplay password for VidyoPortal registration and authentication.
8. In Verify Password, re-enter the password.
9. Click **Save**.

CONFIGURING VIDYOCLOUD

VidyoCloud is an optional advanced topology for configuring VidyoRouters in the VidyoConferencing system. You can configure VidyoCloud at initial installation or do so at a later date when your organization's network grows. Some of the benefits of VidyoCloud include:

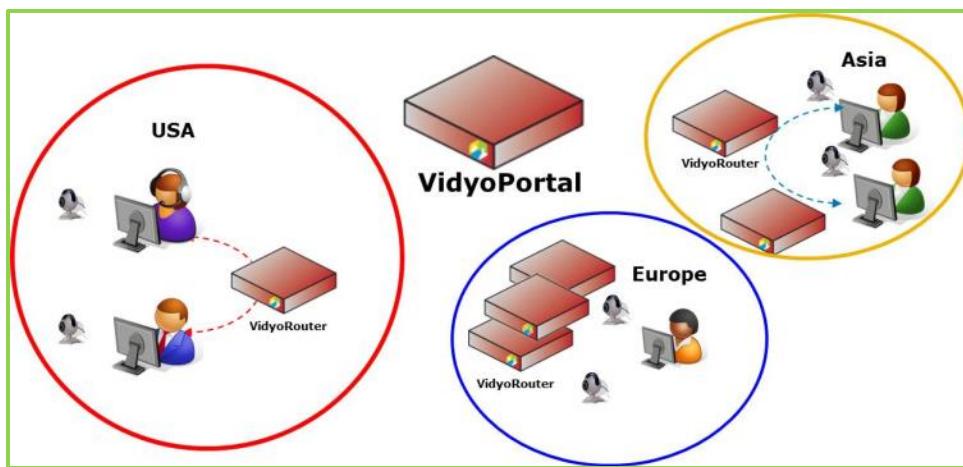
- More efficient network bandwidth utilization.
- Improved latency for conferences by localizing traffic.
- Support for large conferences spanning over multiple VidyoRouters.
- Shared capacity with floating VidyoLine licenses among regions.
- Simplified firewall configurations.

The capacity of a single VidyoRouter is up to 100 concurrent HD lines. If you need additional capacity, you can purchase additional VidyoRouters. If you do, you can group them into pools or VidyoClouds. Typically you might do this to group 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).

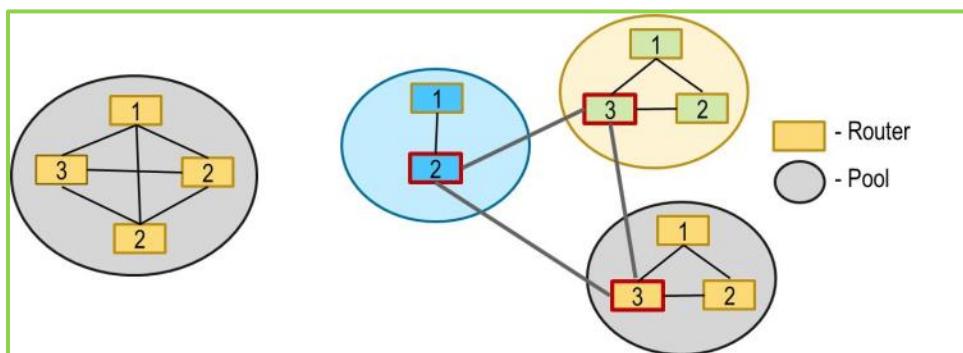
- A VidyoRouter can be in only one pool.
- A pool contains one or more VidyoRouters.
- If you have only one VidyoRouter, it's still in a pool.
- A location may have a number of pools.
- Multiple VidyoRouters in a pool provide failover across the pool.

Before VidyoCloud, if one VidyoRouter reached its saturation point of 100 simultaneous users for a conference, any additional connection attempts were refused, even if a second VidyoRouter was hosting less than 100 users. There was no way the first VidyoRouter could utilize the second VidyoRouter's unused capacity.

However, once a VidyoCloud 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 within a single pool use the Full Mesh topology, whereas pools are cascaded using the DAG (Directed Acyclic Graph) topology. Directed edges of the DAG must be manually specified during system configuration. You must also assign a priority which will decide which two locations will connect when there is more than one choice.



This section describes how to create a VidyoRouter pool, how to remove a VidyoRouter from a pool, and how to delete an entire VidyoRouter pool.

Enabling the VidyoCloud

By default, VidyoCloud is disabled. If your organization wants to use VidyoCloud, you can quickly enable it.

To enable the VidyoCloud:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.

3. Click **Manage Components** on the left menu.

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoManager	VidyoManager	192.168.1.100	5 / 5	TAG_VC2_2_0_052	<input type="checkbox"/>
UP	VidyoRouter	VidyoRouter	192.168.1.100	5 / 3	TAG_VC2_2_0_052	<input type="checkbox"/>
UP	VidyoGateway	VidyoGateway	192.168.1.110		2.1.0(136C)	<input type="checkbox"/>

Buttons: Delete, Enable, Disable

4. Double-click on the VidyoManager.
5. In the VidyoManager table, click the **Advanced** tab.
6. Click the **Manage VidyoCloud** check box.

VidyoManager - Local VM	
<input checked="" type="checkbox"/> General <input type="checkbox"/> Security <input type="checkbox"/> Advanced	
VidyoPortal URL:	http://yourtenant.yourcompany.com
SOAP:	IP: 0.0.0.0 Port: 17995
RHCP:	IP: yourtenant.yourcompany.com Port: 17991
Vidyo Proxy Address Map:	Local IP Address Remote IP Address
<input type="checkbox"/> Manage VidyoCloud <input type="button" value="Delete"/> <input type="button" value="Add"/> <input type="button" value="Factory Default"/>	

7. Click **Save**.

For more information, see “Entering VidyoManager Advanced Information” on page [117](#).

Creating a VidyoRouter Pool

To create a VidyoRouter pool:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page 35.

2. Click the **Components** tab.
3. Click **Manage VidyoCloud** on the left menu.
- Notice the option button labeled **Active** in the upper right-hand corner.
4. Click **Add Pool**.

The VidyoCloud Table opens, with the VidyoRouter Pools tab selected.

Pool Name	VidyoRouter(s)
89C	DEFAULT_NAME [8A9678531C3Y36F8VSPQ0PvAS4A274Q3MBQ3WHKBYQgVUT05v]

The VidyoRouter Pool table opens. All of your available routers are listed in the Available Routers section in the table.

Router Name	IP
DEFAULT_NAME	192.168.1.105

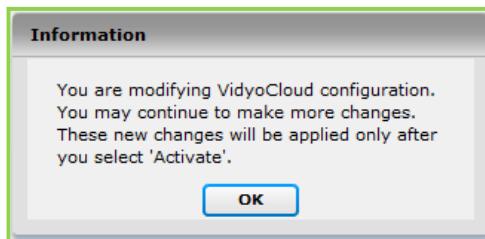
Router Name	IP	Status

5. 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 remind you of the location or purpose, such as New York, Paris, or Board Members.

6. In the Available Routers section, click on a VidyoRouter in the Router Name column and drag and drop it to the Router Name column in the Routers in Pool section.
7. Repeat this process for each VidyoRouter you wish to add to this pool.
8. When you're done, click **Save Pool**.

The Information dialog box appears.



Note that the main image behind the dialog box is blurred and the **Active** button has now been joined by a **Modified** button.



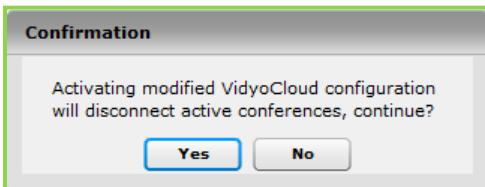
This is to remind you that by starting to change the configuration you are now working on a modified version of the system.

9. Click **OK**.

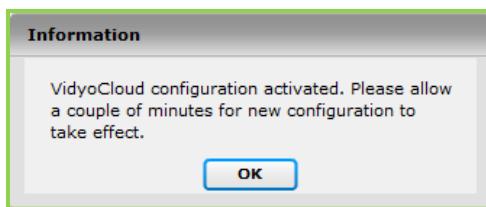
You'll be returned to the VidyoCloud table. The original configuration remains unchanged for now. If you need to interrupt what you're doing, you could click the **Save** button and your modified version is stored, but your current configuration would not be disturbed. You can then come back later and continue working until you are ready to activate your changes.

10. Click **Activate** to activate all of your changes.

The Confirmation dialog box appears.



This dialog box reminds you that modifying the system requires a restart. Warn your users that you're going to restart the system and do it when your system usage is lowest. After you click **OK**, you'll see another Information dialog box.



This reminds 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.

Note: When you want to add additional routers to a pool, open the VidyoCloud table and double-click the pool's name. You add additional routers in the same way you added the first one.

Removing a VidyoRouter from a Pool

To remove a VidyoRouter from a pool:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.

3. Click **Manage VidyoCloud** on the left menu.

Notice the option button labeled **Active** in the upper right-hand corner.

4. Double-click the name of the pool in which your VidyoRouter is located.

This opens the VidyoRouter Pool table.

5. Simply drag and drop the VidyoRouter'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.

Deleting an Entire VidyoRouter Pool

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

To delete an entire VidyoRouter pool:

1. Log in to the Super Admin portal using your Super Admin account.

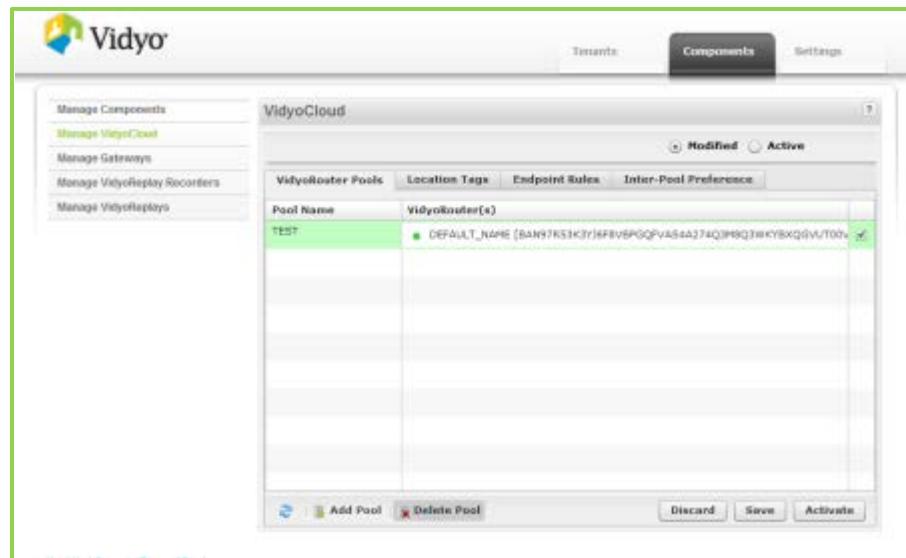
For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.

3. Click **Manage VidyoCloud** on the left menu.

Notice the option button labeled **Active** in the upper right-hand corner

4. Select the check box to the right of the pool or pools you wish to delete.
5. Click **Delete Pool**.



6. Confirm your decision to delete the pool in the confirmation dialog box that appears.

Activating the VidyoCloud Configuration

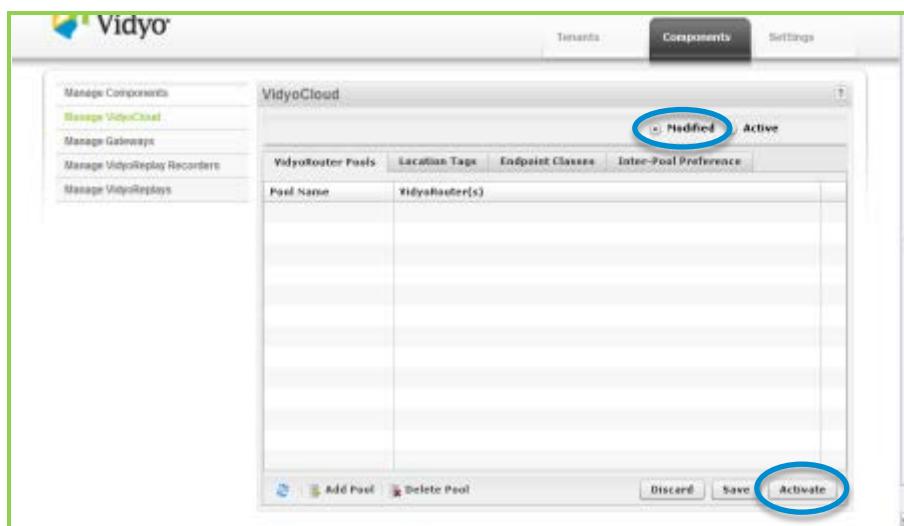
VidyoCloud enables the VidyoConferencing system to cascade conferences across multiple VidyoRouters. The VidyoCloud configuration must be activated for any changes made to the configuration of the VidyoManager or any VidyoRouters. This is due to the underlying default Router Pool and VidyoCloud configuration; even though you may decide not to configure a full VidyoCloud, a default Cloud Pool for any VidyoRouters still exists in the system. If you have multiple VidyoRouters, they cascade by default as needed (even without a full VidyoCloud configuration) to provide for larger conferences and router capacity overflow. Therefore, you need to activate the VidyoCloud configuration upon configuring all the components.

Note: Far End Camera Control (FECC) for cascaded VidyoRouters is enabled on VidyoPortal 2.2 and later.

To activate the VidyoCloud configuration:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.

3. Click **Manage VidyoCloud** on the left menu.



4. Click the **Modified** radio button.
5. Click **Activate**.
6. Confirm your actions in the dialog boxes that open.

Unless you need to control which particular VidyoRouter your users' access, you don't need to define a VidyoCloud. By leaving everything under Manage VidyoCloud blank, you create a default Cloud, and your VidyoRouters are automatically pooled together and allowed to cascade for larger conferences.

If you do not activate VidyoCloud, a message appears on top of the Components window.

**** You MUST activate VidyoCloud configuration in the Manage VidyoCloud page ****

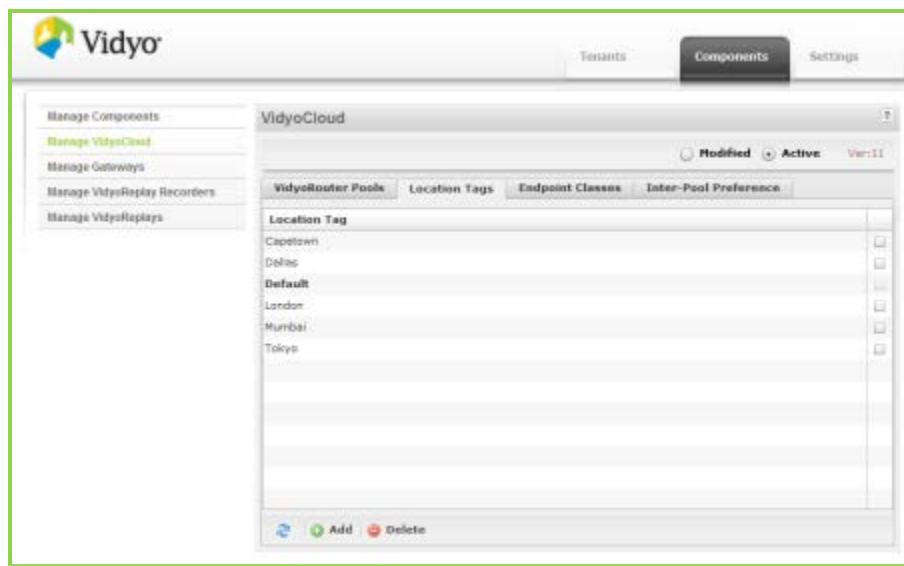
Creating User Location Tags

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 on the Add User page. For more information, see “Adding a New User” on page 204. 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.

To create a user location tag:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page 35.
2. Click the **Components** tab.
3. Click **Manage VidyoCloud** on the left menu.

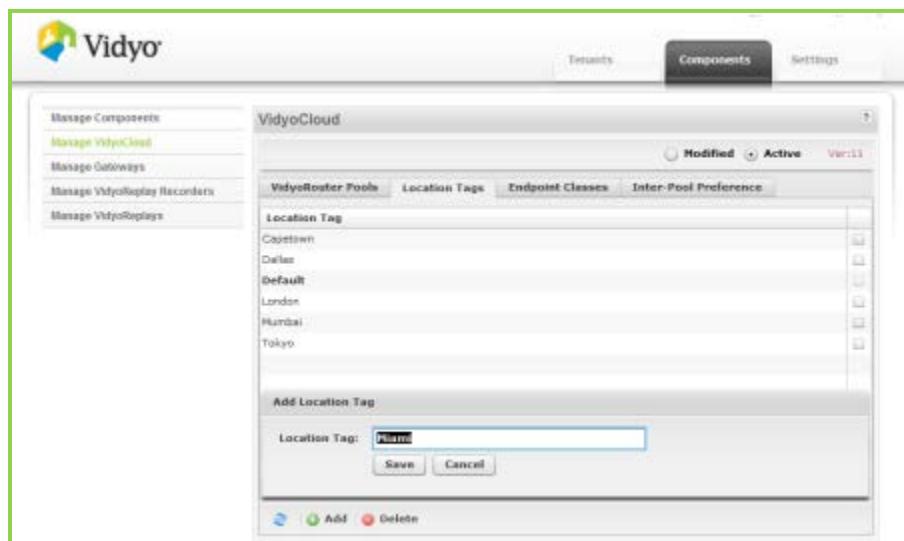
4. Click the **Location Tags** tab.



The screenshot shows the VidyoCloud management interface. The left sidebar has links for Manage Components, Manage VidyoCloud (which is selected), Manage Gateways, Manage VidyoReplay Recorders, and Manage VidyoReplays. The main area is titled 'VidyoCloud' and shows a table of 'Location Tag' entries. The table includes columns for Name and several checkboxes. The entries listed are CapeTown, Dallas, Default, London, Mumbai, and Tokyo. At the bottom of the table are buttons for Refresh, Add, and Delete.

5. Click **Add**.

A pop-up appears where you can add a location.

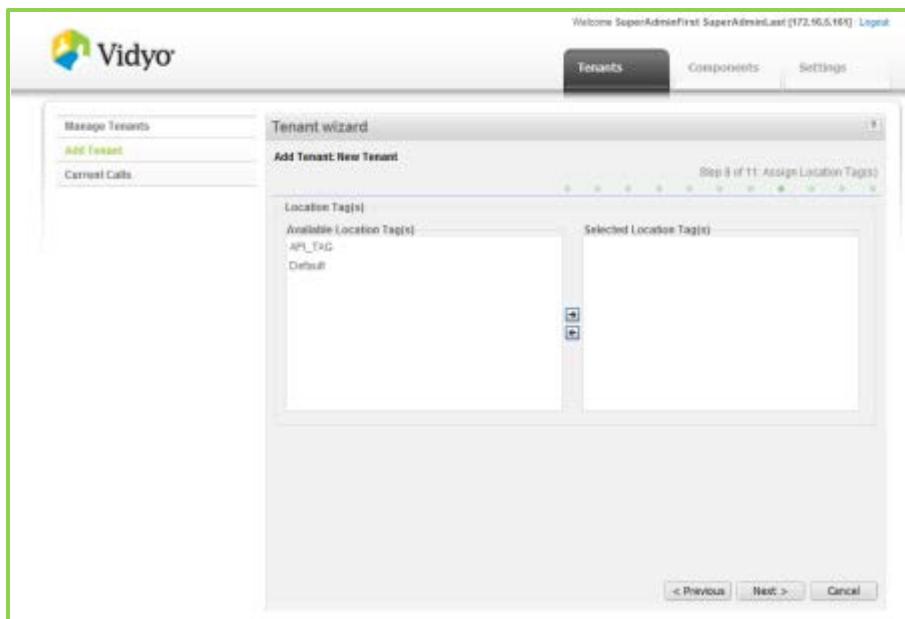


The screenshot shows the same VidyoCloud interface as above, but with a modal dialog box open over it. The dialog is titled 'Add Location Tag' and contains a single input field labeled 'Name' with the placeholder 'Name'. Below the input field are 'Save' and 'Cancel' buttons. The rest of the interface, including the sidebar and the main table, are visible in the background.

6. Enter the name of the location tag you wish to create.

7. Click **Save**.

For information about how to assign location tags to tenants, see “Assigning Location Tags” on page [195](#).



Creating Endpoint Rules

An endpoint is any device that can be used to participate in a point-to-point call or a conference (such as VidyoDesktop, VidyoRoom, a VidyoMobile device, and VidyoGateway).

Endpoint Rules determine which VidyoRouter pool a given endpoint is assigned to. Remember that you can create Endpoint Rules only after you have set up your VidyoRouter pools.

As Super Admin, you determine the order in which Endpoint Rules are applied. The first rule that matches the endpoint’s characteristics (IP address, location tag, or Endpoint ID) is the rule that’s applied.

You can have as many as 1,000 rules. 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.

Note: The default rule is always selected and applied to all of the pools you have configured to keep you from having to configure large sets of rules for simple configurations.

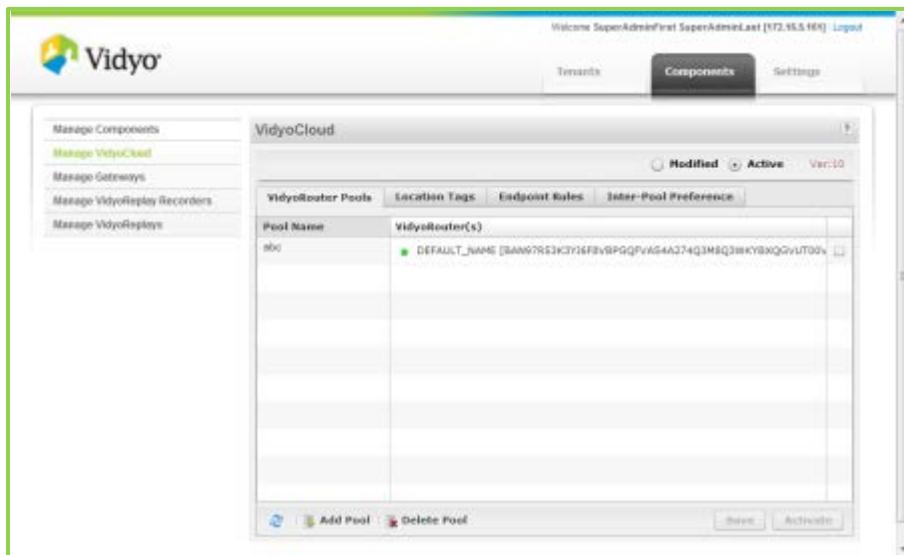
As part of the process of setting up rules, we recommend that you set up a catch-all rule accepting all endpoints that do not match any of the endpoints previously created. The catch-all can be a rule that uses IP o.o.o/o.

To create an endpoint rule:

1. Log in to the Super Admin portal using your Super Admin account

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.
3. Click **Manage VidyoCloud** on the left menu.
4. In the VidyoCloud table, click the **Endpoint Rules** tab.

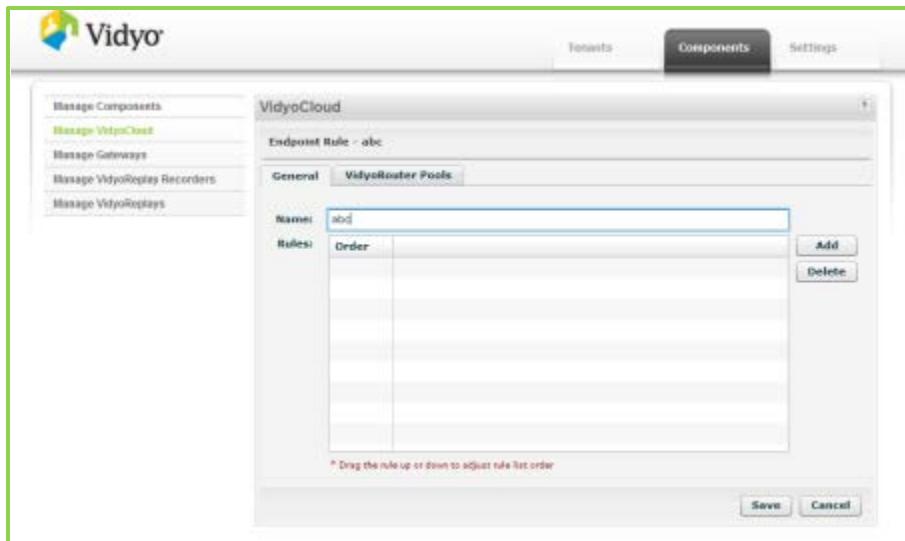


5. Click the **Modified** option button to start editing the active configuration.

The very first time you do this the Modified button will not appear. For more information, see “Creating a Router Pool” on page [149](#).

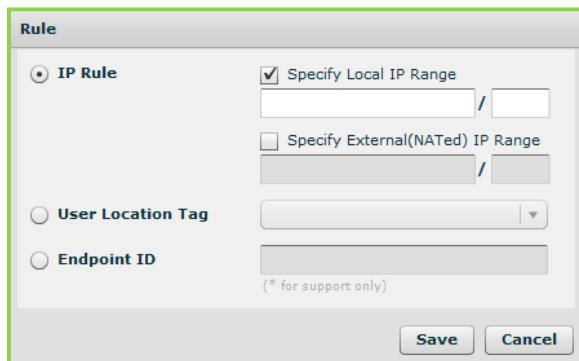
6. In the Name field, enter a name for your endpoint rule.

Note that as soon as you begin typing the name it appears as the title of the Endpoint Rule above the name field.



- Click **Add** to create a rule.

The Rule dialog box appears.



You can set only one rule at a time in the Rule dialog box.

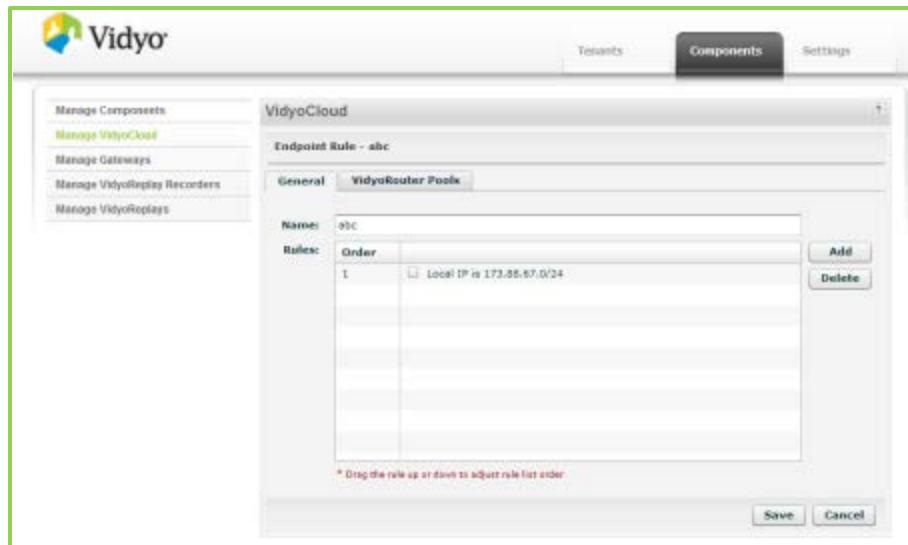
- Select from the following rules:

- Select IP Rule and select the corresponding Specify Local IP Range and Specify External(NATed) IP Range to specify a range of local and external IP addresses.
- Select User Location Tag to select from location tags you have already configured in the system.

Note: Location tags must first be created in order to select them for your rule. For more information, see “Creating User Location Tags” on page [155](#).

- The Endpoint ID is selected to provide a unique identifier for an endpoint.

Caution: This Endpoint ID field should only be set under specific instruction from Vidyo Customer Support.



9. Click **Save**.

The Save button is enabled after you create one or more rules.

10. You can now use the General screen to perform the following:

- To add another rule, click **Add**.
- To delete a rule, select its check box, and then click **Delete**.
- If you have multiple rules, you can change the order in which they're applied by dragging and dropping them in this list. The rules are applied in order, from top to bottom.

Configuring 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 wouldn't want your Sydney pool to cascade to your New York pool. You'd probably want your Sydney pool to cascade to your Tokyo pool and as a second choice maybe your New York pool. Alternatively, 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.

To configure Inter-Pool Preferences:

- 1.** Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

- 2.** Click the **Components** tab.

- 3.** Click **Manage VidyoCloud** on the left menu.

- Click the **Inter-Pool Preference** tab in the VidyoCloud table.

The screenshot shows the VidyoCloud management interface. The left sidebar has links for Manage Components, Manage VidyoCloud, Manage Gateways, Manage VidyoReplay Recorders, and Manage VidyoReplays. The main area is titled 'VidyoCloud' and has tabs for Active and Pending. Below is a table with columns: From / To, QoSvr1, QoSvr2, TestVr, local_SA, local_VR, and D210VR. The table lists several pools: QA5vr1, QA1vr, TestVr, local_SA, local_VR, D210VR3, and abc. The 'From / To' column lists all pools, while the other columns show specific settings like 'High', 'Medium', or 'None'.

From / To	QoSvr1	QoSvr2	TestVr	local_SA	local_VR	D210VR
QA5vr1	High	High	High	None	None	Medium
QA1vr	High	High	High	None	None	Medium
TestVr	High	High	High	None	None	Medium
local_SA	None	None	None	High	None	Medium
local_VR	None	None	None	None	High	Medium
D210VR3	Medium	Medium	Medium	Medium	Medium	High
abc	Medium	Medium	Medium	Medium	Medium	Medium

Note that the table lists all of the VidyoRouter pools in the same order along *both* the vertical left-hand side of the table *and* across the top of the table.

- Click the word inside the intersecting cells of your VidyoRouter pools.

When you click a word inside the intersecting cell, a drop-down menu appears with the following options:

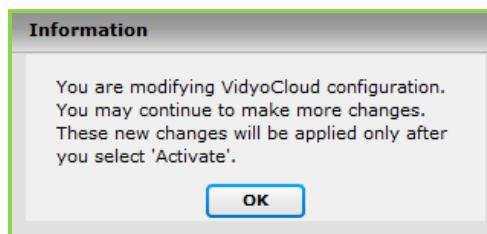
- High
- Medium (the default)
- Low
- None (to bypass)

- Select the option for the cascading priority you want to set between the two VidyoRouter pools.

When performing this task, consider the physical locations of your pools and your existing and projected bandwidth and usage patterns.

- As you work your way through the matrix, click **Save** often.

The first time you click **Save**, the Information dialog box appears.

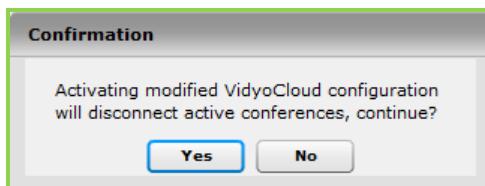


- Click **OK**.

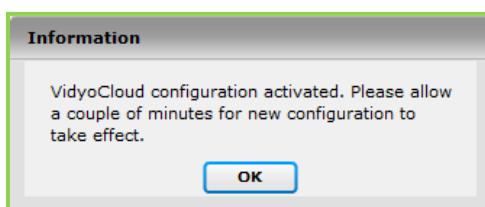
Note that a Discard button is also available if you want to discard your changes.

- When you're all done, click **Activate** to activate your changes.

When you click **Activate**, the Confirmation dialog box appears to remind you that enabling your changes disconnects everyone currently using the system.



- Click **Yes**.

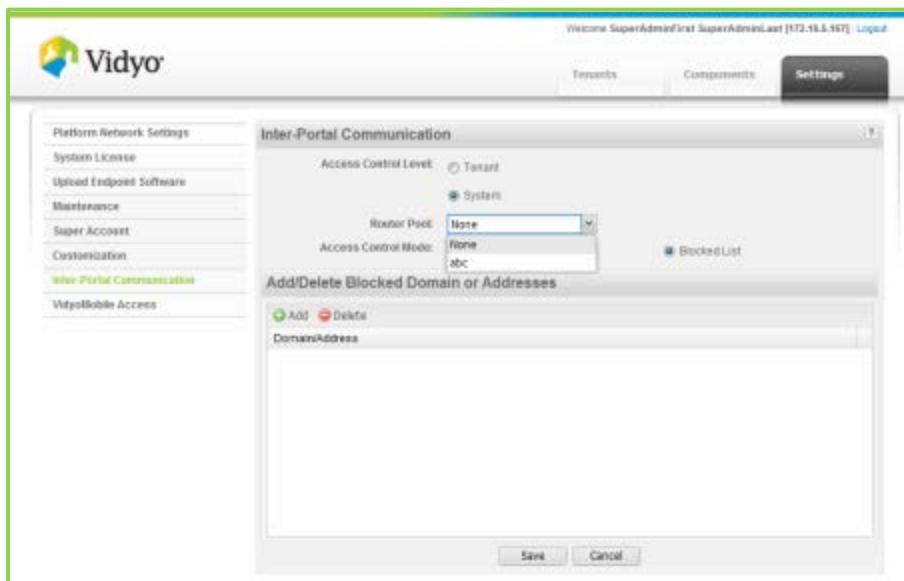


You must restart the system for your changes to take effect.

- Click **OK**.

Configuring Inter-Portal Communication When Using VidyoCloud

To configure IPC when using VidyoCloud, you must select the router pool from the Router Pool drop-down list on the Inter-Portal Communication page. For more information, see “Configuring System-Wide Inter-Portal Communication” on page [108](#).



The IPC-enabled router pool serves as a hub through which all IPC communication is routed.

8.Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

Vidyo's virtual appliances – the VidyoPortal Virtual Edition (VE), the VidyoRouter VE, and the VidyoGateway VE – allow you to enjoy the benefits of the VidyoPortal, VidyoRouter, and VidyoGateway within a virtual environment. The advantages of using virtual appliances include:

- All the features and functionality of the physical appliance.
- The simplicity and efficiency of a software-based virtual appliance.
- Leveraging your investment in VMware vSphere infrastructure.

This chapter describes how to configure the VidyoPortal VE and the VidyoRouter VE. For information about how to configure the VidyoGateway VE, refer to the *VidyoGateway Administrator Guide*.

UNDERSTANDING THE VE REQUIREMENTS

To run VidyoPortal or VidyoRouter VE, the following requirements must be met:

- Hypervisor: VMware vSphere ESXi Hypervisor software version 5.0 or later.
- Must be compliant with the VMware qualified hardware list
<http://www.vmware.com/resources/compatibility/search.php>.
- Requires Intel-based servers with a minimum Xeon 56xx Series at 2.4 GHz or faster, supporting Intel Westmere architecture, with AES-NI and hyper-threading enabled.
- NIC: At least 1Gbps vNICs.
- The BIOS settings of the host machine must be set for maximum performance, including both CPU and memory settings. For example, memory should be the highest rated speed specified by the host CPU, and all memory lanes of the CPUs should be populated with identical size and speed DIMMs.
- Ensure that the BIOS settings enable the Hyperthreading, Virtualization Technology (VT), and Extended Page Tables (EPT) options on all ESX hosts.

VidyoPortal Virtual Machine Provisioning Requirements

VidyoPortal VE is designed to be a **standalone appliance**.

VE Model	Resource Allocation
VidyoPortal VE Capacity: 10,000 registered users, 2,500 active users	Number of vCPUs: 8 RAM: 4 GB Disk: 50 GB

Note: VidyoPortal VE can be configured to use the Hot Standby software option. For more information, see “Hot Standby” on page [342](#).

VidyoRouter Virtual Machine Provisioning Requirements

Subject to the resource requirements specified in this chapter, Vidyo supports running a Virtual VidyoPortal simultaneously with a single Virtual VidyoRouter on the same physical machine. Other configurations, such as running multiple Virtual VidyoRouters on the same physical machine, running multiple Virtual VidyoGateways on the same physical machine, running a mix of Virtual VidyoRouters and Virtual VidyoGateways on the same physical machine, or running a Virtual VidyoPortal and Virtual VidyoGateway on the same physical machine are not supported.

VidyoRouter VE Model	Resource Allocation	Resource Reservation
VidyoRouter VE 100	Number of vCPUs: 8 RAM: 8 GB	CPU: 18 GHz RAM: 5 GB
VidyoRouter VE 25	Number of vCPUs: 4 RAM: 4 GB	CPU: 9 GHz RAM: 4 GB

Note:

- Number of Connections: 100 for the VidyoRouter VE 100; 25 for the VidyoRouter VE 25.
- Use a dedicated virtual switch to connect the VidyoRouter VE appliance to the physical NIC.

UNDERSTANDING VMWARE BEST PRACTICES

The following VMware best practices should be followed when running Vidyo VE appliances:

- The overall CPU utilization should not exceed that of a typical production server (that is, 70% utilization). Add CPU resources or move one or more VidyoPortal VE machines if the host CPU utilization exceeds the recommended threshold.
- Vidyo recommends that at least 1 vCPU with 2 GHz and 2 GB of RAM is left idle for the hypervisor.

UNDERSTANDING VIDYOPORTAL AND VIDYOROUTER VE SUPPORT OF VMWARE FEATURES

The following list includes VMware features and explains if and how they are currently supported by VidyoPortal and VidyoRouter VE:

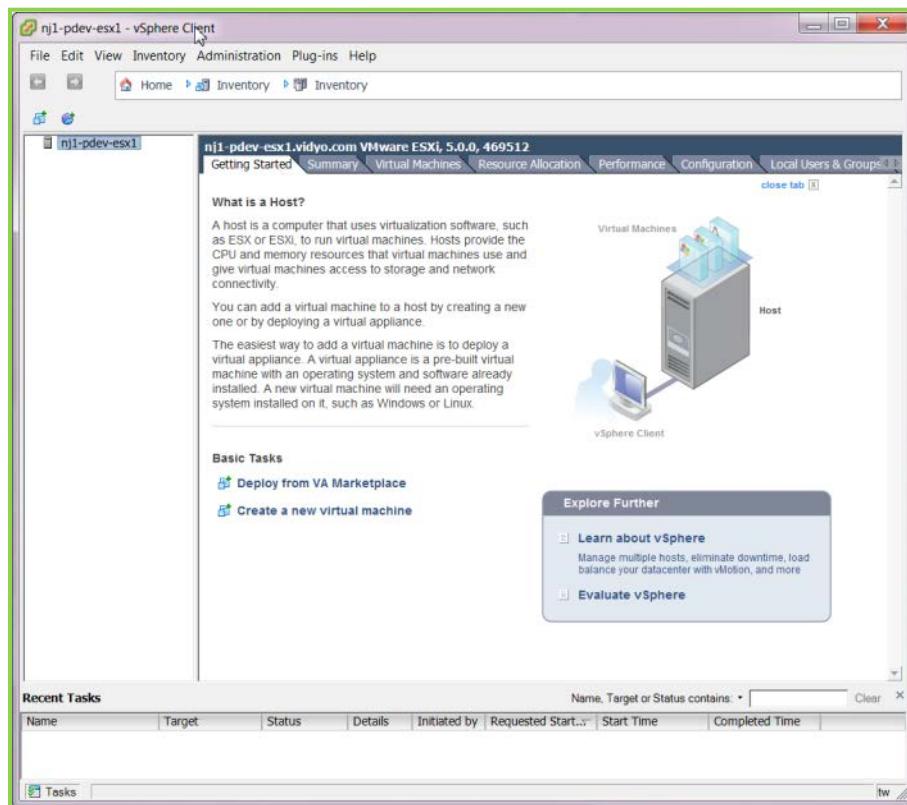
- You can store backup copies of your VidyoPortal or VidyoRouter VE appliance using vSphere's export feature. You can then re-deploy the backup copy using vSphere's import feature.
- While your VidyoPortal or VidyoRouter VE appliance is powered off, it may be moved (cold migration) or copied (cloned) from one host or storage location to another.
- You can resize your virtual machine and add vCPUs and vRAM; however, removing virtual hardware resources are not currently supported.
- VidyoPortal software updates are managed in the same manner as the regular appliance. Always take snapshots (while your VidyoPortal VE appliance is powered off) before updating. The snapshot can be used to downgrade the software version if needed. For more information see "Upgrading Your VidyoPortal System Software" on page [78](#).

- Advanced features, such as vMotion, high availability, fault tolerance, and distributed resource manager are not currently supported.

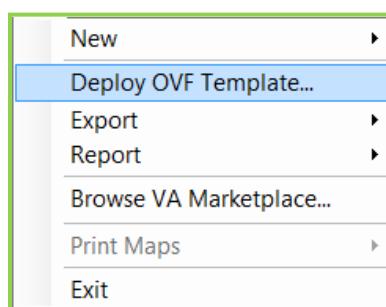
INSTALLING VIDYOPORTAL VE

To install VidyoPortal VE:

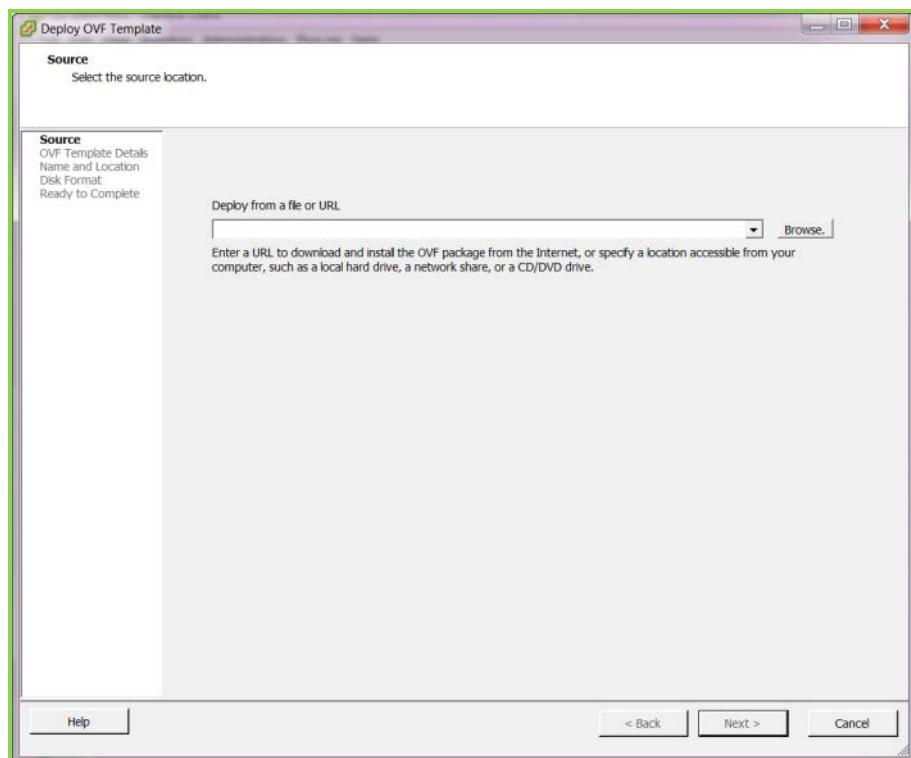
1. Log in to the vSphere client.



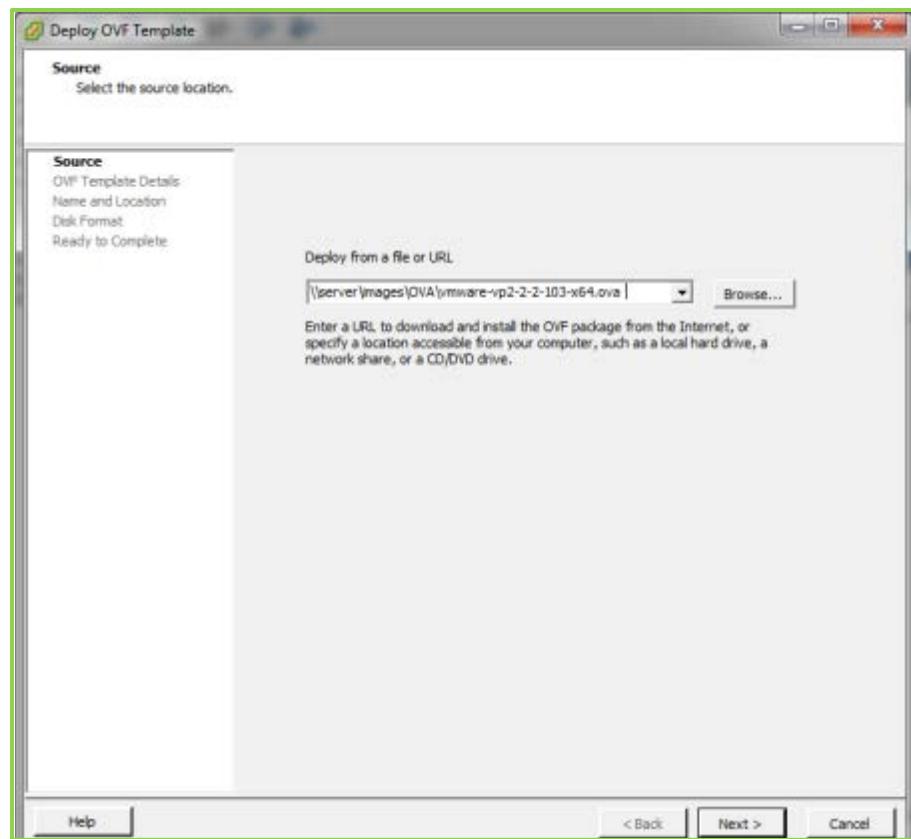
2. From the File menu, select **Deploy OVF Template**.



The Source dialog box appears:

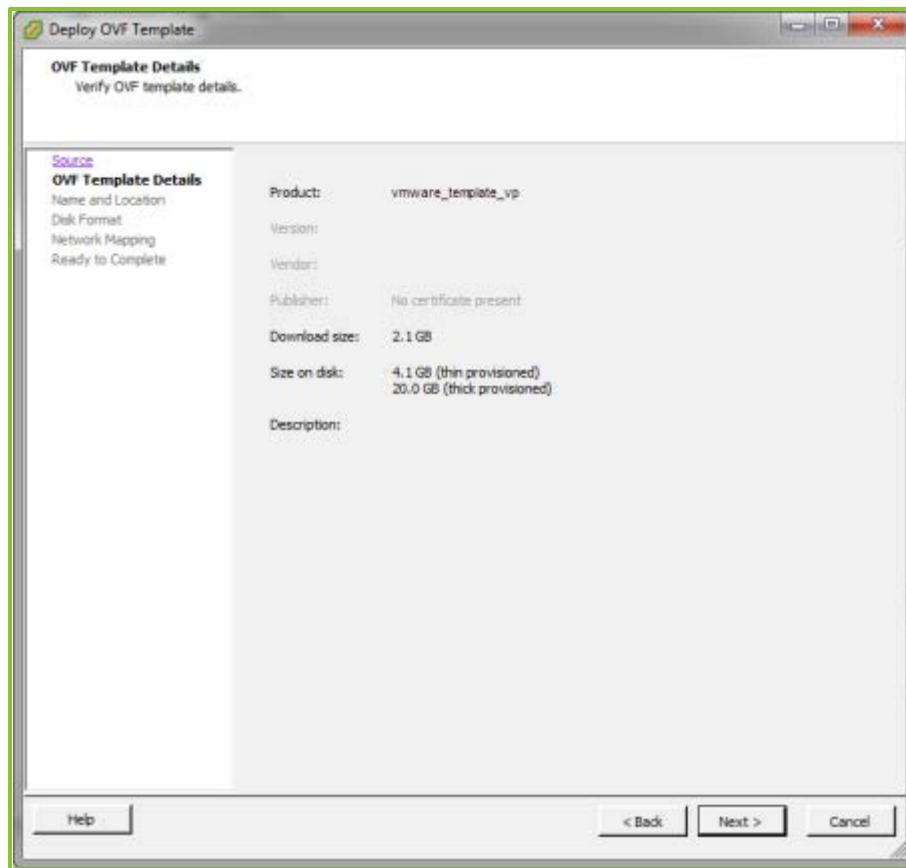


3. Click **Browse** and select the OVA file from your file system.



4. Click Next.

The dialog box changes to OVF Template Details.

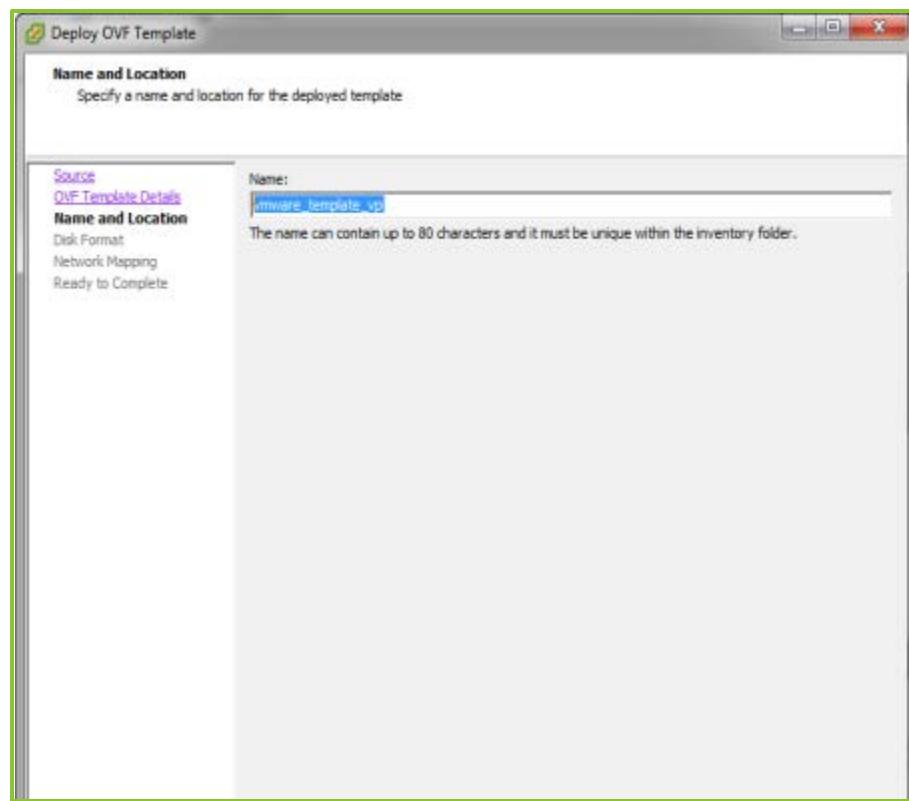


This screen is read-only. If you need to change anything, use the **Back** button.

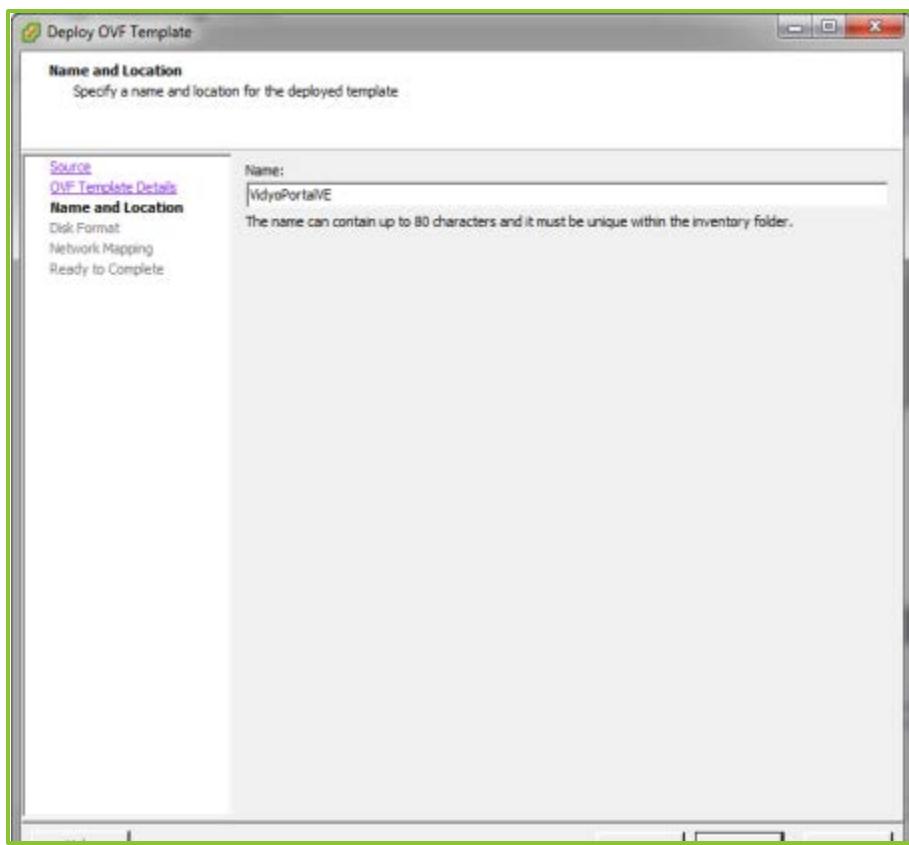
5. Click Next.

The dialog box changes to Name and Location.

The name displayed is the vSphere default.



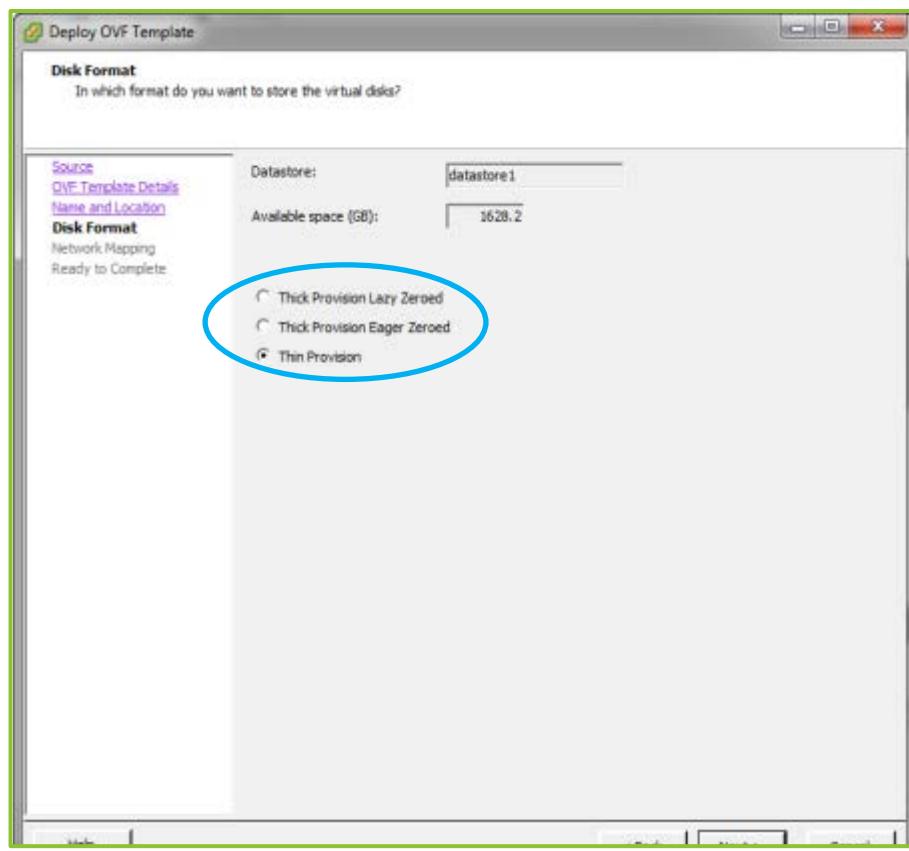
- 6.** Type in a more descriptive name if you want to.



- 7.** Click **Next**.

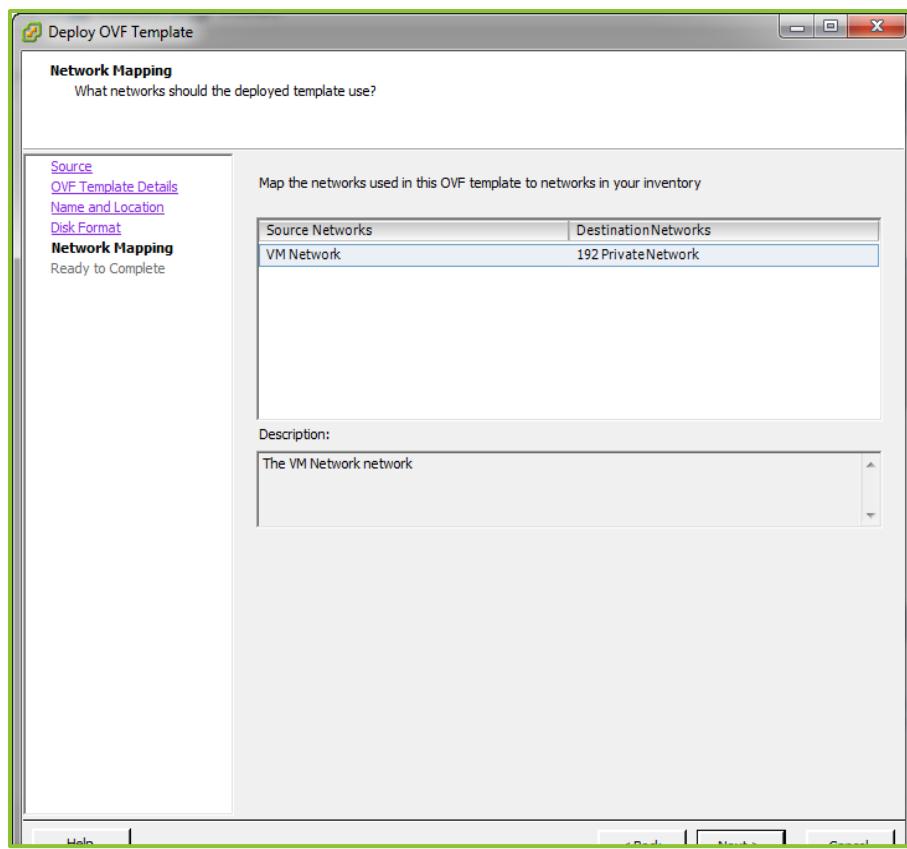
The dialog box changes to Disk Format.

- 8.** Be sure to select **Thin Provision**.



- 9.** Click **Next**.

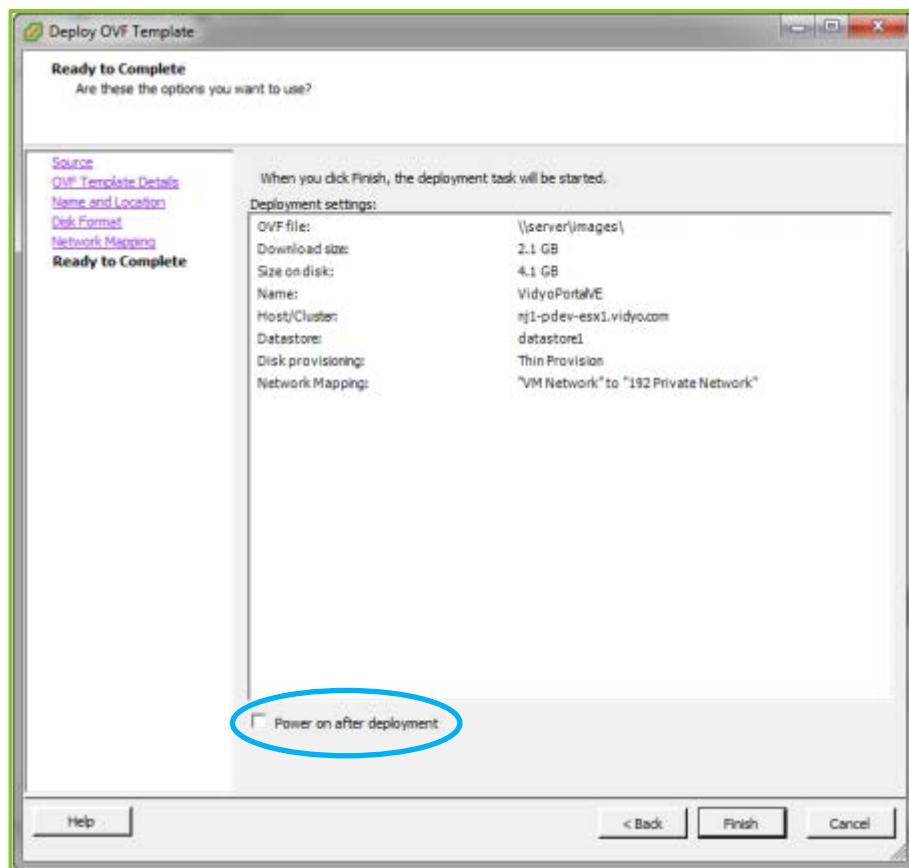
The dialog box changes to Network Mapping.



10. Select the network you want the VidyoPortal VE to use.

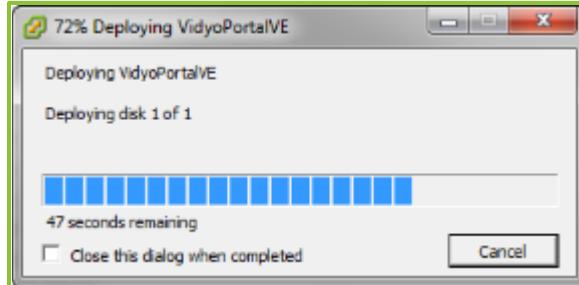
11. Click **Next**.

The dialog box changes to Ready to Complete.

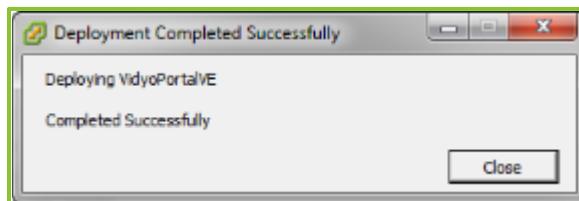


12. Select the **Power on after deployment** checkbox to start your VidyoPortal immediately after you take the next step.
13. Click **Finish**.

The Deploying VidyoPortal VE dialog box appears.

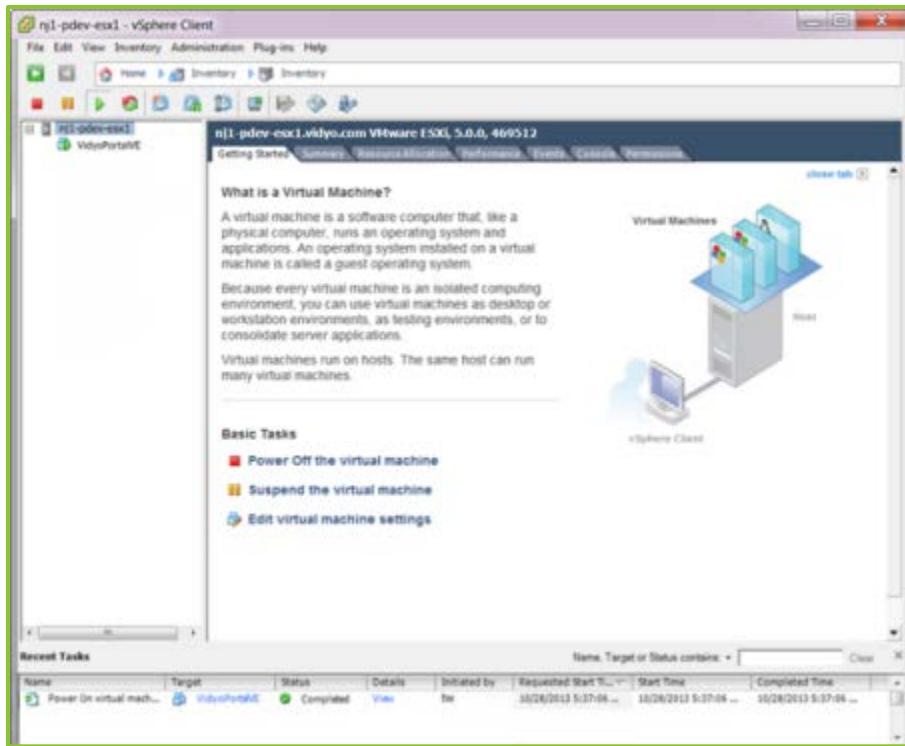


The Deployment Completed Successfully dialog box appears.



14. Click Close.

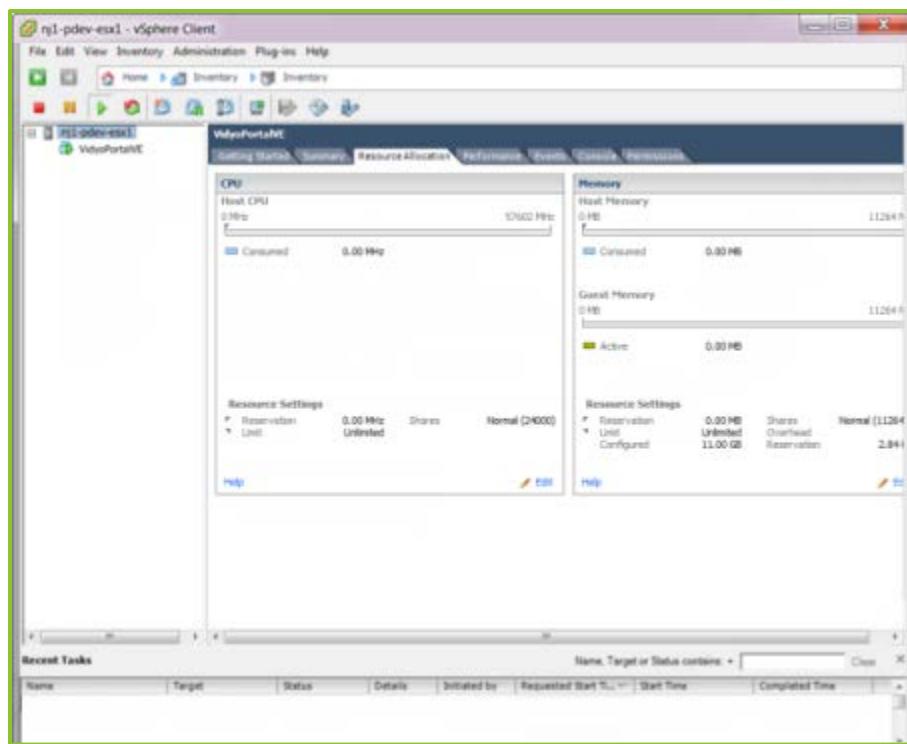
The vSphere Client window appears.



15. Click the + sign in the left side pane.

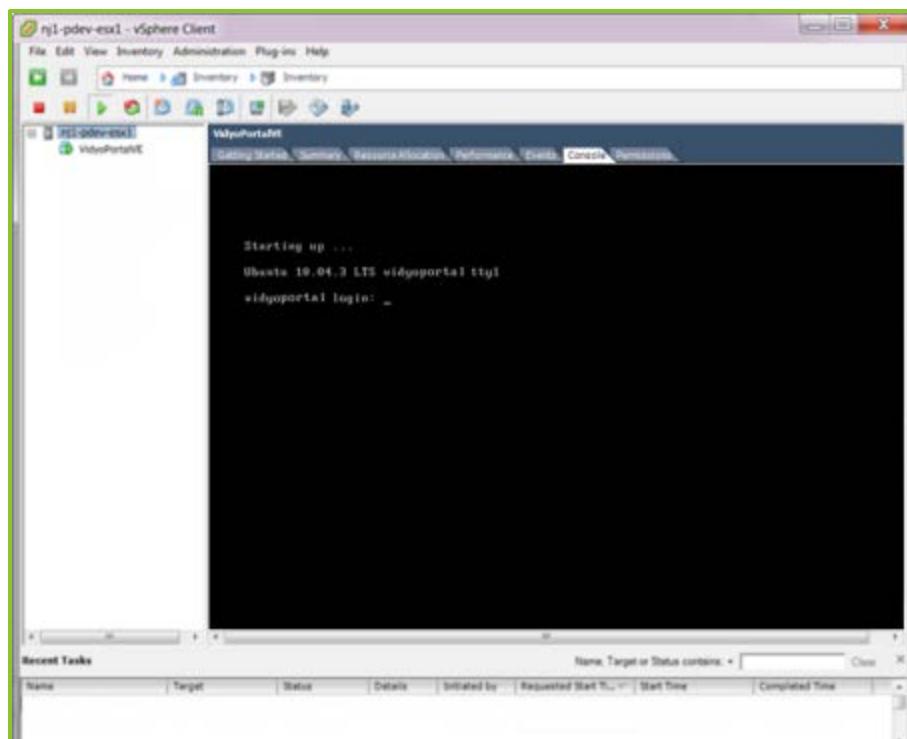
16. Click VidyoPortal VE in the left-side pane.

The tabs change.



- 17.** Click the **Console** tab.

You're at your VidyoPortal VE's Admin console.



- 18.** Log in as Admin.

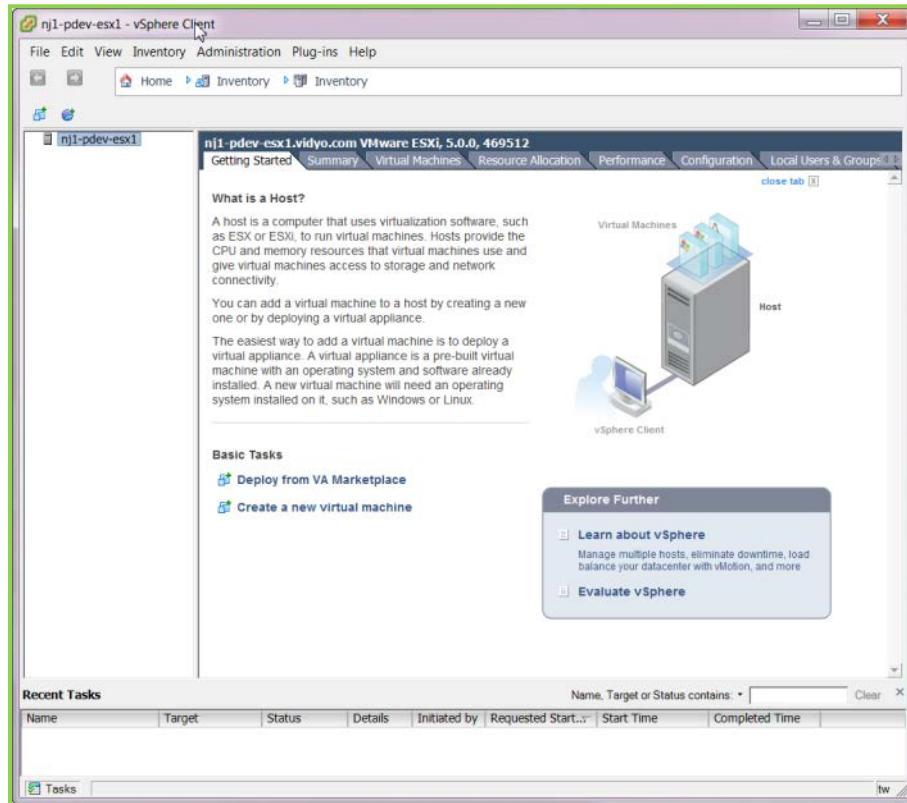
If you haven't changed your password yet, use the default password we have provided for you.

You can now configure your VidyoPortal VE.

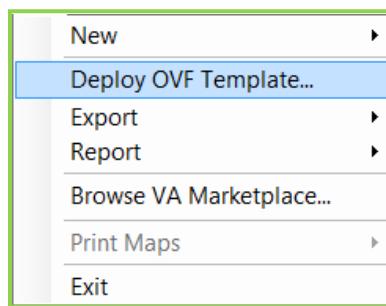
INSTALLING VIDYOROUTER VE

To install VidyoRouter VE:

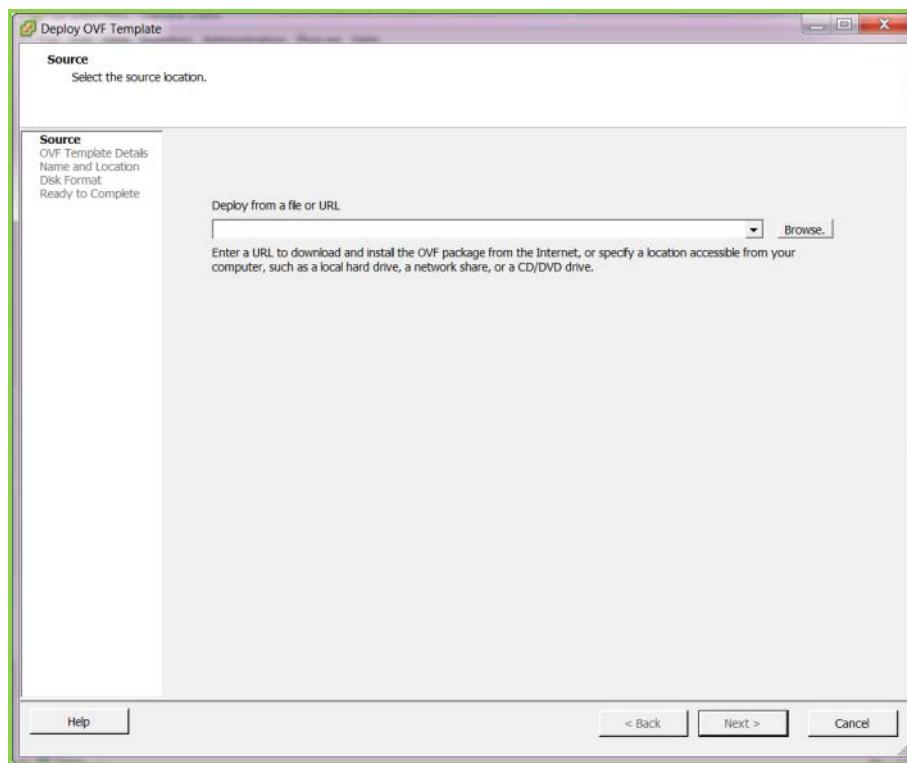
1. Log in to the vSphere client.



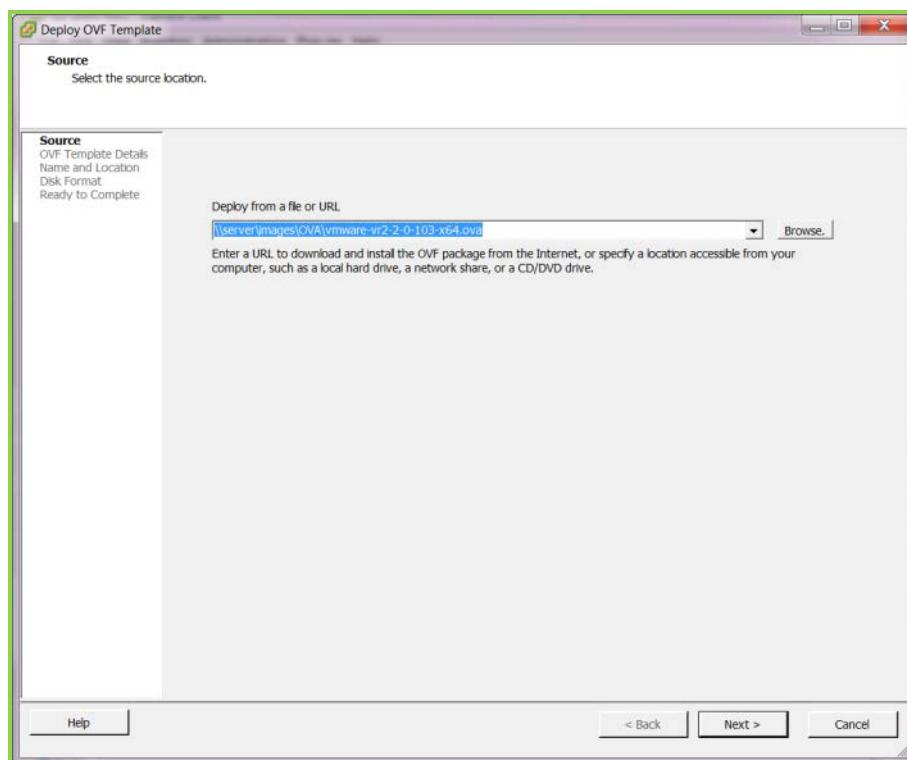
2. From the File menu, select **Deploy OVF Template**.



The Source dialog box appears:

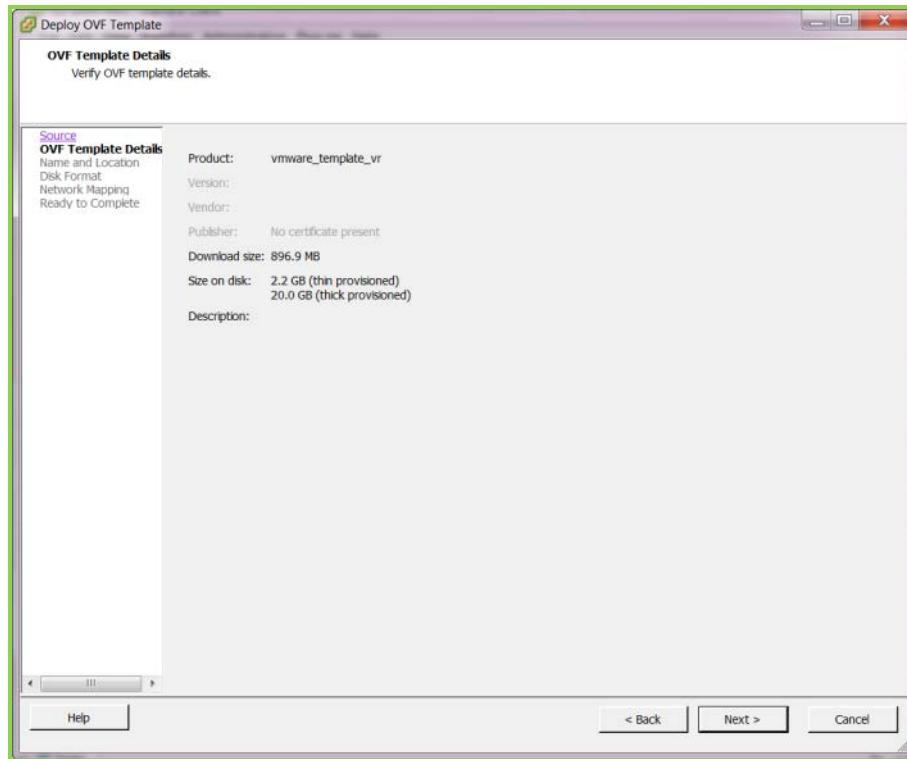


- 3.** Click **Browse** and select the OVA file from your file system.



4. Click Next.

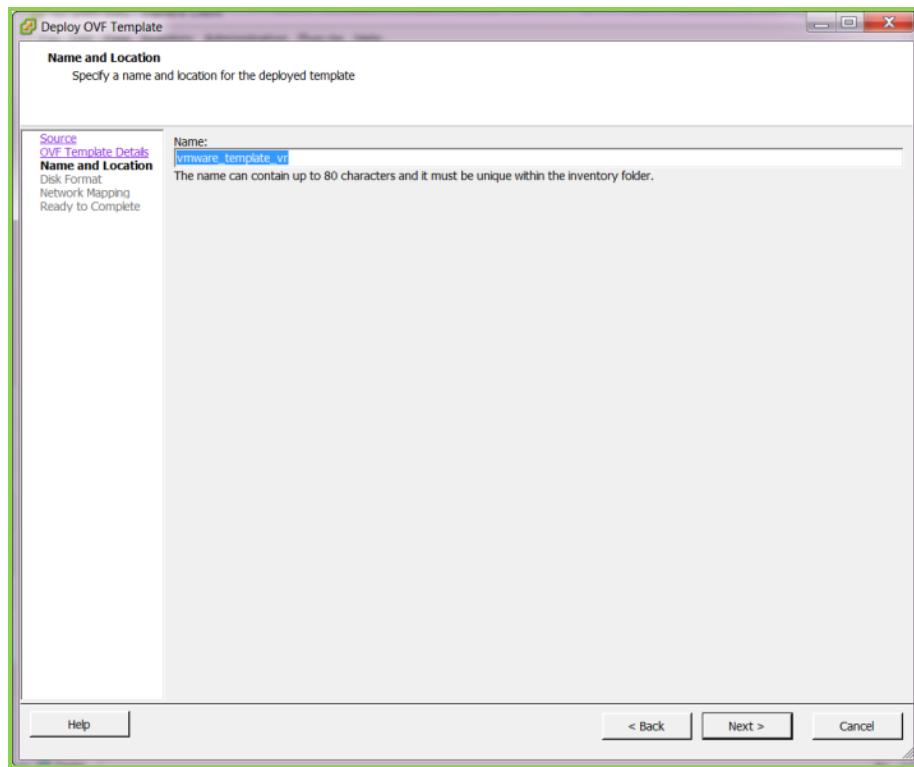
The dialog box changes to OVF Template Details.



This screen is read-only. If you need to change anything, use the **Back** button.

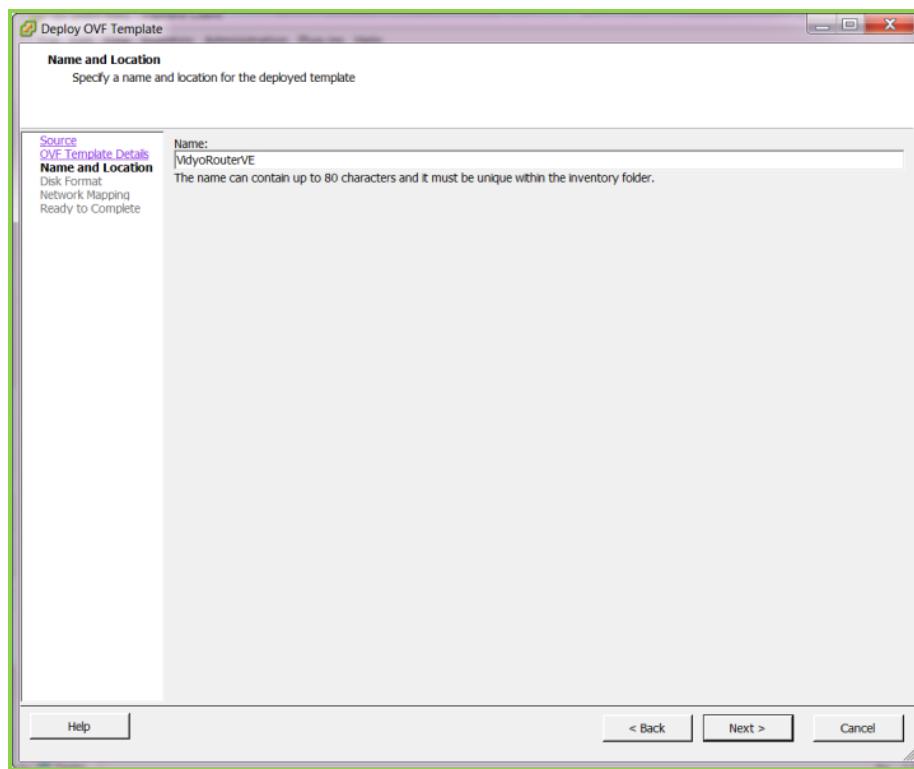
5. Click Next.

The dialog box changes to Name and Location.



The name displayed is the vSphere default.

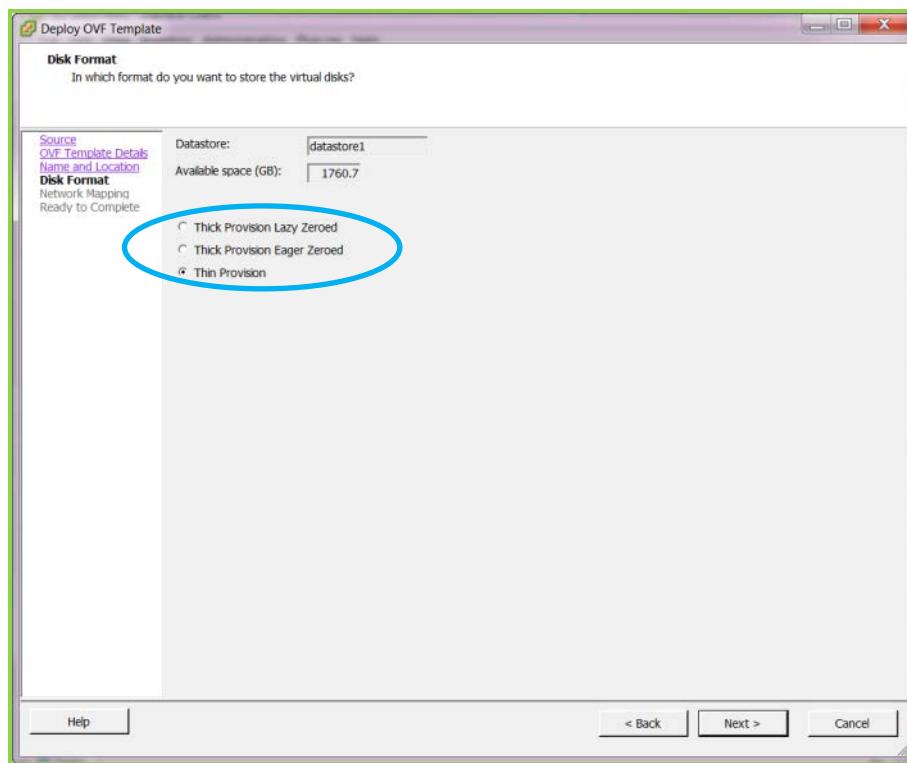
- 6.** Type in a more descriptive name if you want to.



- 7.** Click **Next**.

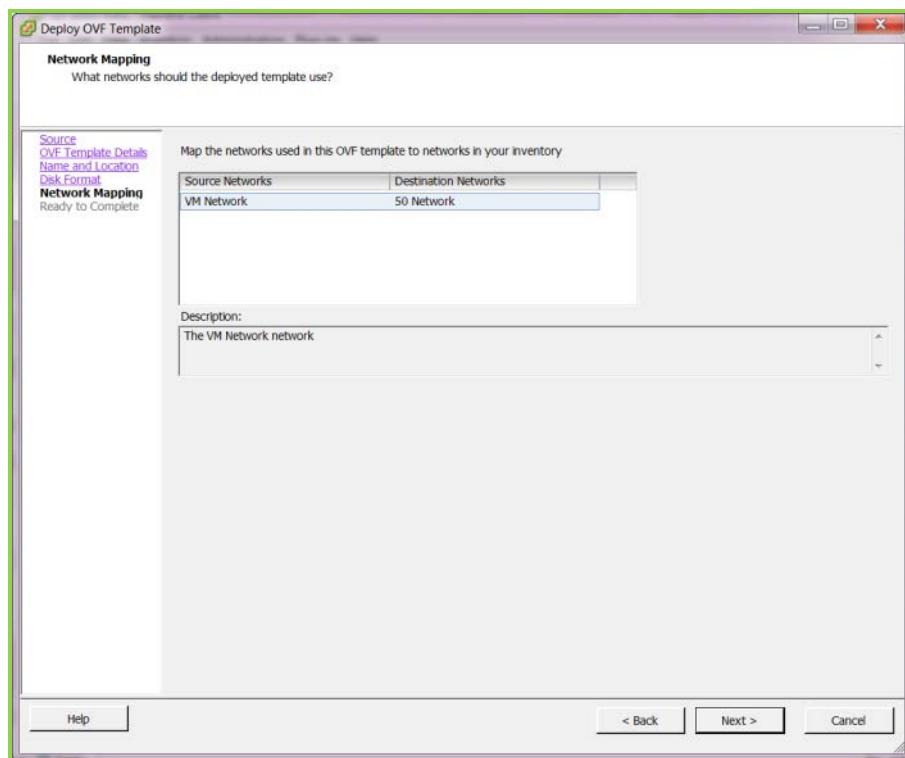
The dialog box changes to Disk Format.

8. Be sure to select Thin Provision.



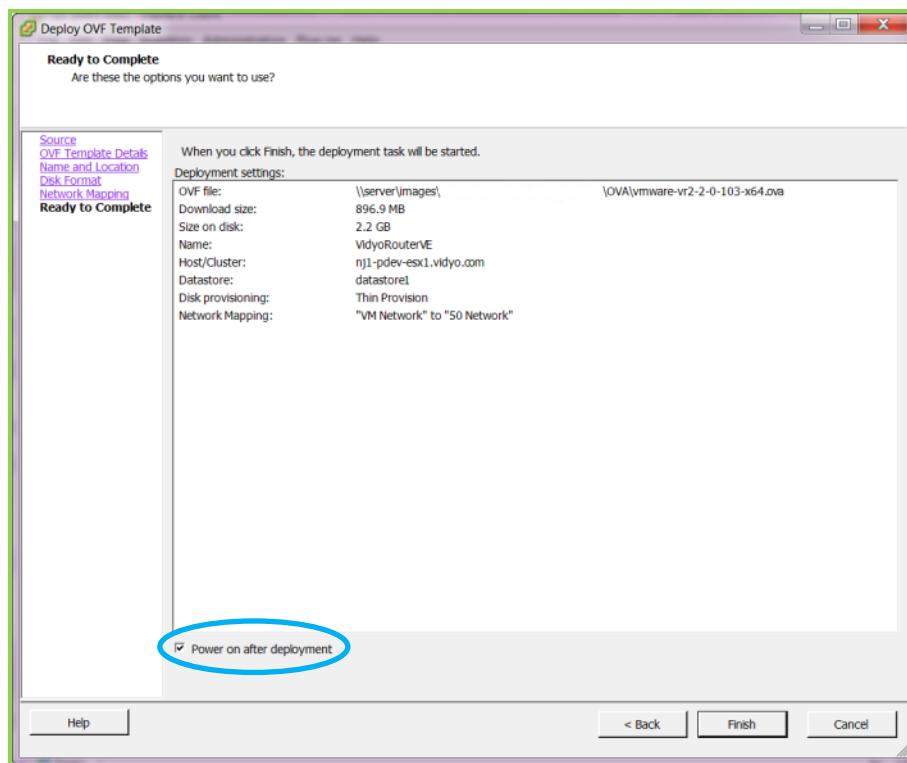
9. Click Next.

The dialog box changes to Network Mapping.



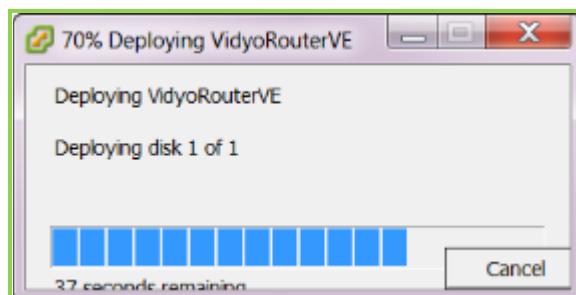
- 10.** Select the network you want the VidyoRouter VE to use.
- 11.** Click **Next**.

The dialog box changes to Ready to Complete.

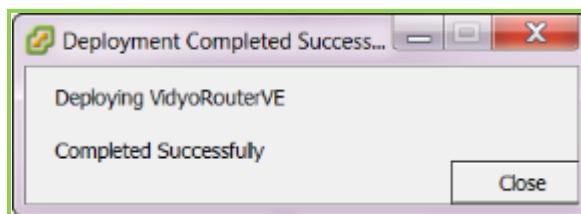


12. Select the **Power on after deployment** checkbox to start your VidyoRouter immediately after you take the next step.
13. Click **Finish**.

The Deploying VidyoRouterVE dialog box appears.

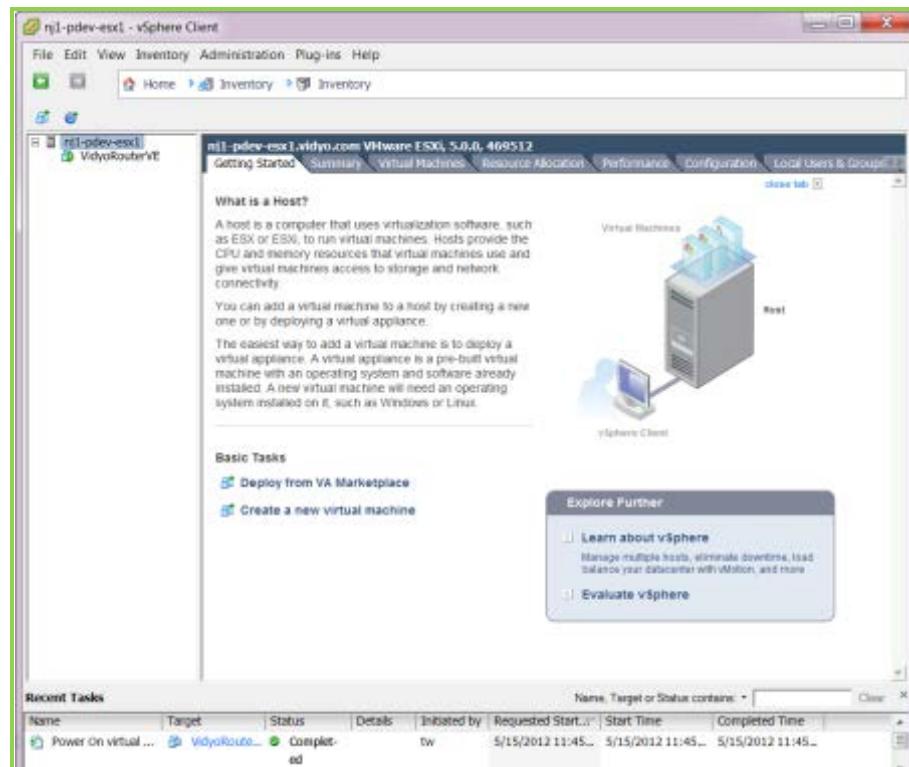


The Deployment Completed Successfully dialog box appears.

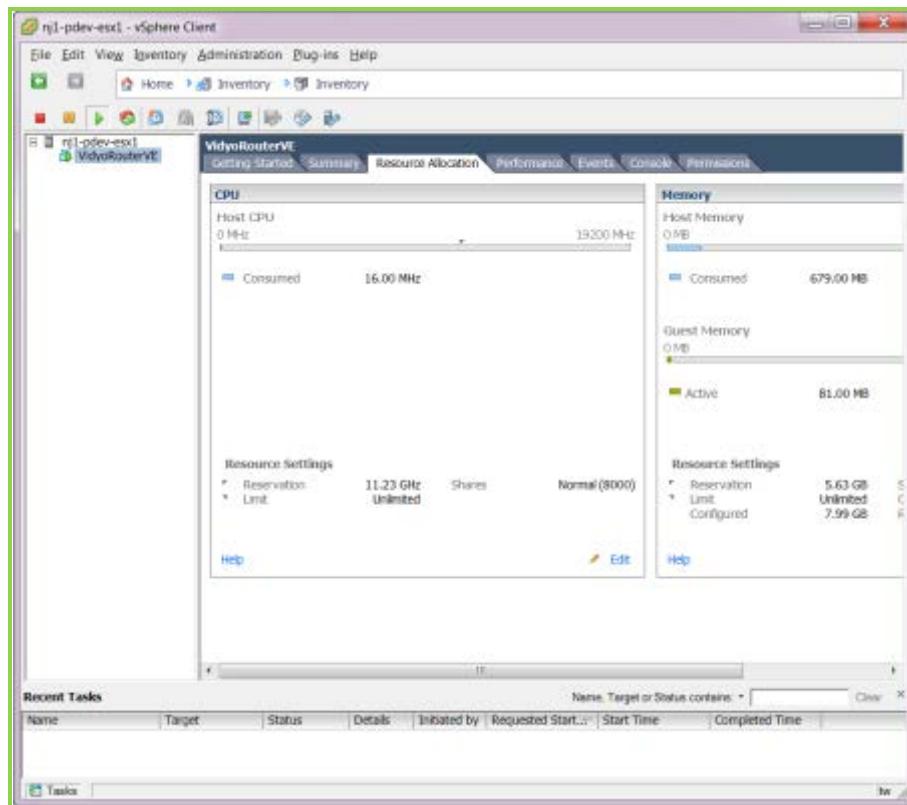


14. Click Close.

The vSphere Client window appears.

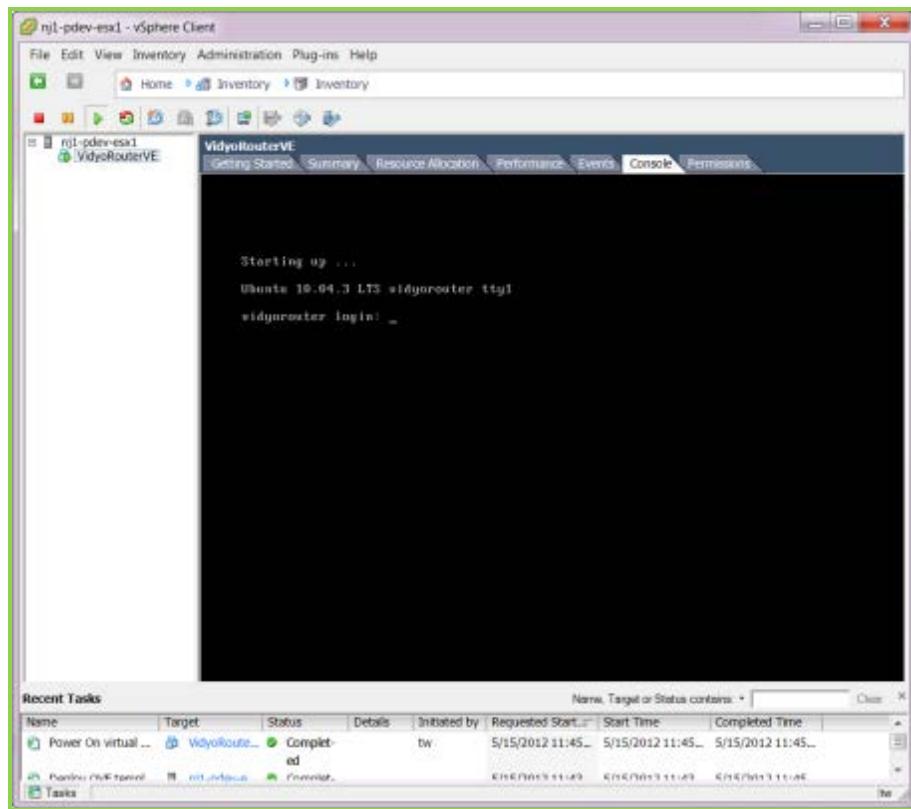
**15.** Click on the + sign to the left of the ESXi host name.**16.** Click on **VidyoRouter VE** in the left-side pane.

The tabs change.



- 17.** Click the **Console** tab.

You're at your VidyoRouter VE's System Console.



18. Log in as Admin.

If you haven't changed your password yet, use the default password we have provided for you.

You can now configure your VidyoRouter VE.

9. Managing Tenants as the Super Admin

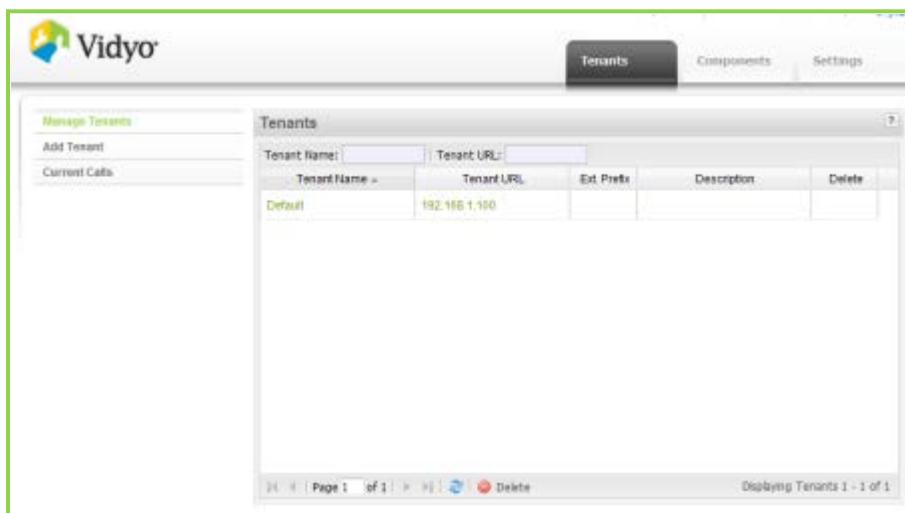
Every Vidyo system has at least one tenant, called the default tenant. If your VidyoConferencing system is licensed for multi-tenant mode, you can create multiple tenants.

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.

USING THE TENANTS TABLE

The Manage Tenants table is used to view, delete, and manage the tenants in your system.

A screenshot of the Vidyo Super Admin Portal. The top navigation bar includes the Vidyo logo, a search bar, and tabs for 'Tenants' (which is selected), 'Components', and 'Settings'. On the left, a sidebar menu shows 'Manage Tenants' as the active item, along with 'Add Tenant' and 'Current Calls'. The main content area is titled 'Tenants' and contains a table with columns: Tenant Name, Tenant URL, Ext. Prefix, Description, and Delete. A single row is visible for 'Default' with the value '192.168.1.100' in the Tenant URL column. At the bottom of the table are buttons for 'Page 1 of 1', 'Refresh', and 'Delete', and a status message 'Displaying Tenants 1 - 1 of 1'.

To use the Manage Tenants table:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Tenants** tab.

The Manage Tenants left menu item is selected by default.

3. Tenants in your VidyoPortal appear on the table and include Tenant Name, Tenant URL, Ext. Prefix, Description, and Delete fields as columns.

You can drag and drop the column headings to arrange them in the order you prefer.

4. Search by tenant name or tenant URL using the Tenant Name or Tenant URL search boxes above the table.
5. The lower part of the table includes the following functions:
 - Click **Refresh** to refresh the table.

- Click the First Page, Previous Page, Next Page, and Last Page direction arrows to scroll through multiple pages of results in the table.
- Enter a page number to access a specific page of results in the table.

UNDERSTANDING HOW TO ADD A TENANT

Use the following steps to add or configure a tenant. Some steps can be skipped if your installation or the tenant you're configuring has not licensed certain capabilities.

1. Configure 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.
9. Enable or disable VidyoMobile access (skip if VidyoMobile is not being used).
10. Allow inbound and/or outbound Inter-Portal Communication.
11. Save the tenant configuration.

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: 

ADDING A TENANT

This is step 1 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

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.

Note: A password change is required when your tenant admin first logs in to a newly configured tenant.

Adding a Default Tenant or Adding a New Tenant

To add a default tenant or a new tenant:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Tenants** tab.

The Manage Tenants left menu item is selected by default.

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

Alternatively, if your system is licensed for multi-tenant mode, in the Tenants tab, click **Add Tenant** to display the first of ten pages of the Tenant wizard.

The screenshot shows the 'Add Tenant: New Tenant' step of the Tenant wizard. It includes fields for Tenant Name, Tenant URL, Extension Prefix, Dial-in Number, VidyoReplay URL, and a Description. Below these are usage statistics: # of installs (0, max: 8964), # of Seats (0, max: 72439), # of Lines (0, max: 1080), # of Executives (0, max: 0), and # of VidyoPanaramas (0, max: 0). There are checkboxes for 'Enable Guests login' and 'Enable Scheduled Room'. At the bottom are 'Previous' and 'Next >' buttons, and a 'Cancel' button.

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

- In the Tenant Name field, enter 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.

- In the Tenant URL, enter the IP or FQDN used by this tenant's users to access the VidyoPortal.

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 portal. You can also use your server's IP if it does not have a URL.
- Your tenants should be configured to use an FQDN and not an IP address in order to secure your VidyoConferencing system with HTTPS and optionally encryption (using the Secured VidyoConferencing Option).

- In the Ext. Prefix field, enter a desired prefix to be added to extension numbers. This allows multiple tenants to use the same extension numbers.

An extension prefix 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.

- In the Dial-in Number field, enter the phone number dialed for voice-only participants when accessing conferences.
- In the VidyoReplay URL enter the URL the tenant's users will use in order to access VidyoReplay. If the VidyoReplay option has not been licensed on your system, entering information in this field has no effect. This is also the case for Vidyo's Federal implementation.
- In the Description field, enter a short description of the tenant for informational purposes.
- In the Tenant VidyoGateway SIP/H.323 SRV record FQDN field, enter tenant support for inbound URI dialing from the VidyoGateway using SIP and H.323 protocols.

Note: This feature is only compatible with VidyoGateway 3.0.

For more information, refer to “Understanding Call Types and Service Examples” in the *Vidyo-Gateway Administrator Guide*.

- In the # of Installs field, enter 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.
- In the # of Users field, enter 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.
- In the # of Lines field, enter the maximum number of lines allocated to the tenant.
Lines are pooled among all tenants.

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

- In the # of Executives field, enter the number of maximum number of Executive Desktop users allocated to the tenant.

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.

- Select the **Enable Guests login** check box to allow guest logins on the tenant.

Note:

- Along with enabling guest logins on your tenant or tenants, VidyoMobile access must also be enabled if you want to use VidyoSlate. For more information about VidyoMobile access, see page [56](#).
- For more information on VidyoMobile and VidyoSlate you can download the user guides from <http://www.vidyo.com/support/documentation/>. VidyoMobile guides are available for both iOS and Android versions of the application. VidyoSlate is compatible with iPad 2 and later and the iPad Mini.

Enabling Cross-Tenant Access

This is step 2 of the 11 steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

To enable cross-tenant access:

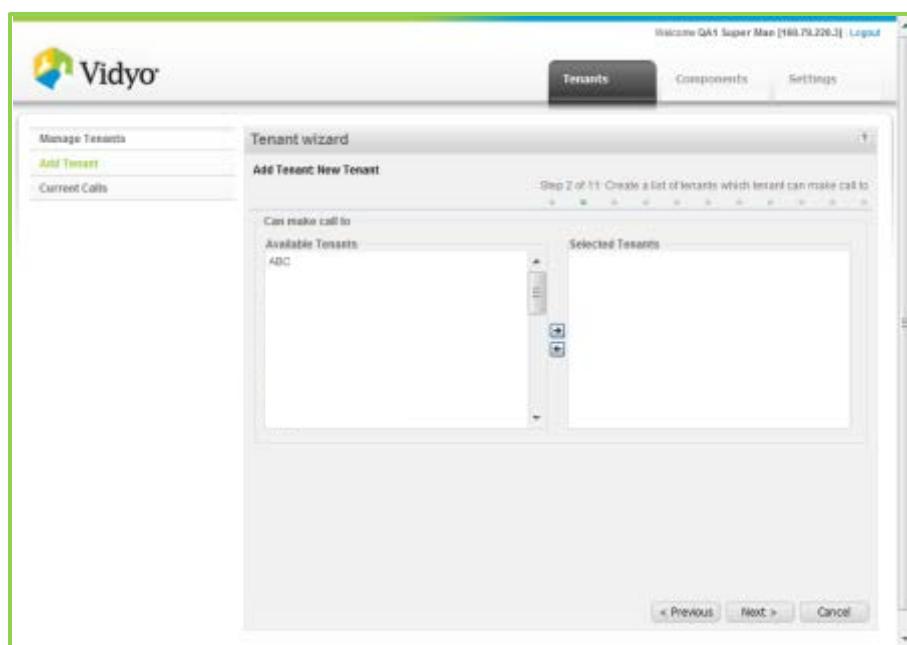
1. Click **Next** to proceed to Step 2.

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.

2. To enable cross-tenant access, select one or more tenants in the Available Tenants list and click the **Right Arrow** to move the tenant or tenants 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.

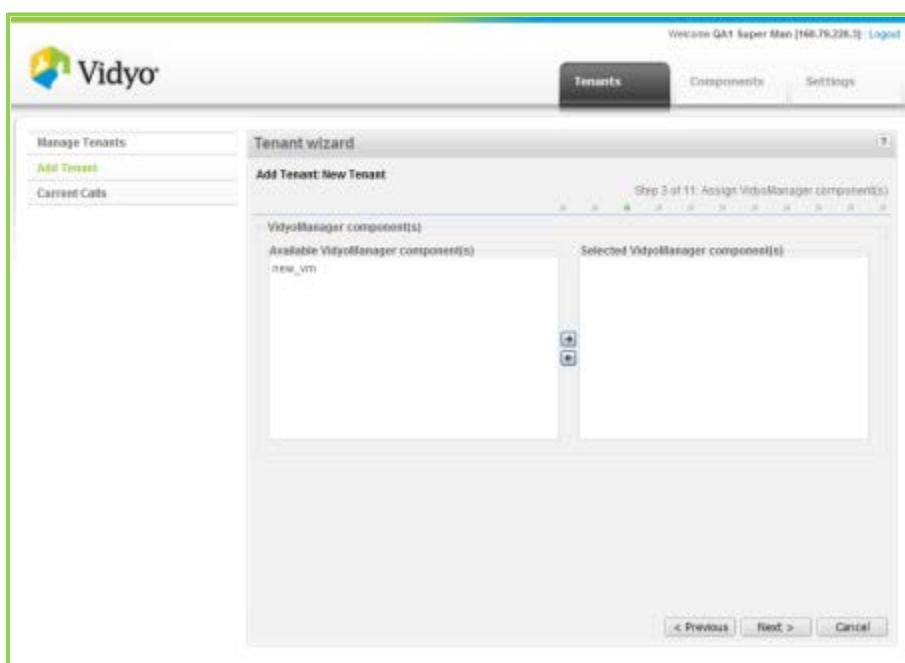
You can also click **Previous** at any point and as many times as necessary to go back and change any of the data you entered.

Making the VidyoManager Component Available

This is step 3 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

To make the VidyoManager component available:

1. Click **Next** to proceed to Step 3.



On 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** to move them to the Selected VidyoManager component(s) list.

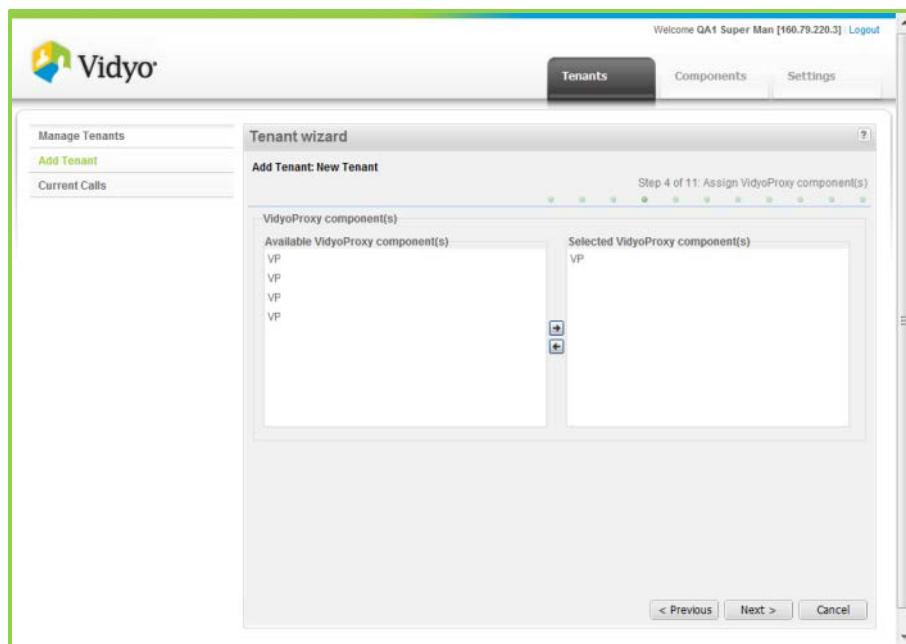
Making the VidyoProxy Components Available

This is step 4 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

This step is needed to assign the VidyoProxy to members of Tenants for VidyoManager (EMCP) proxy access.

To make the VidyoProxy components available:

1. Click **Next** to proceed to Step 4.

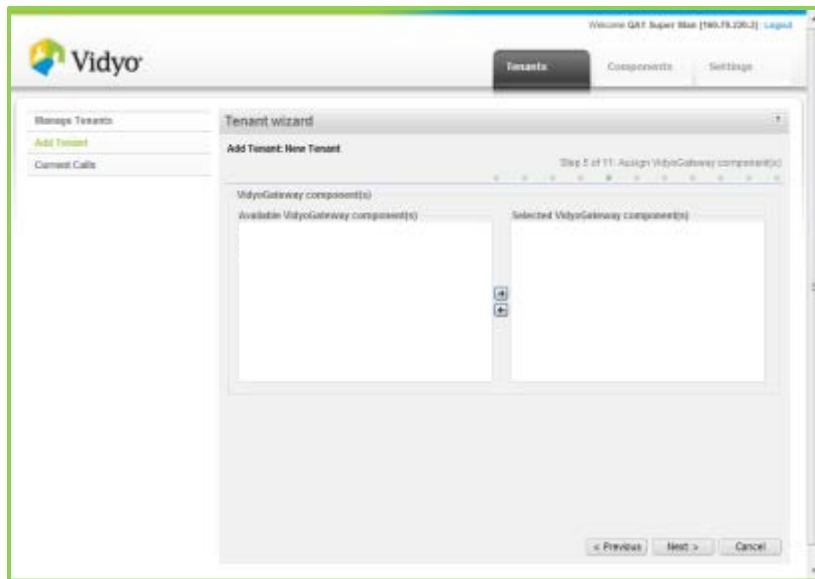


Making the VidyoGateway Components Available

This is step 5 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

To make the VidyoGateway components available:

1. Click **Next** to proceed to Step 5. (If you are not using a VidyoGateway, you can skip this step by clicking the **Next** button.)



On 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.

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** 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.

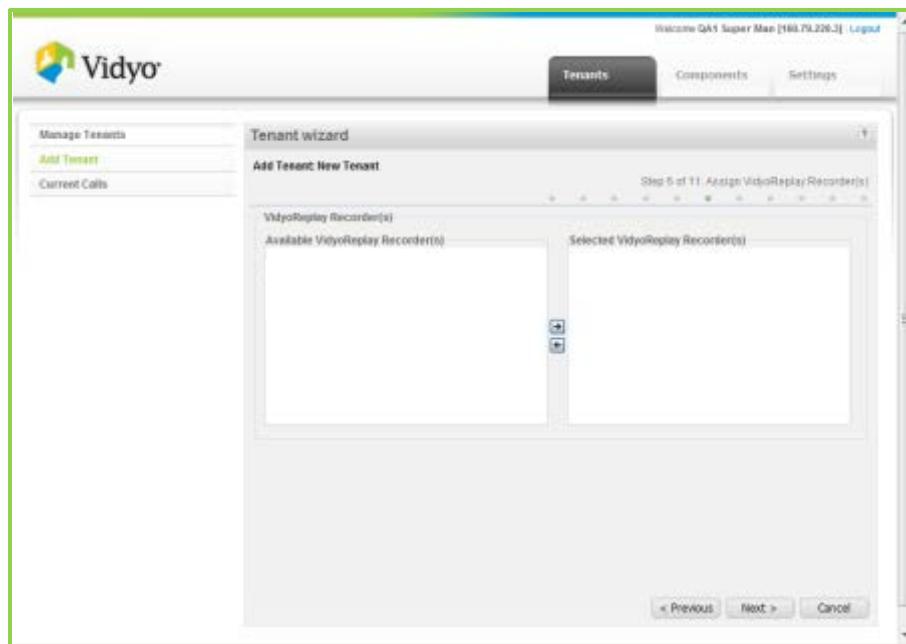
Selecting a VidyoReplay Recorder

This is step 6 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

VidyoReplay is an optional 1U rack mount server that adds webcast recording, cataloging and replay of VidyoConferences to a VidyoConferencing system.

To select a VidyoReplay recorder:

1. Click **Next** to proceed to Step 6. (If you don't have VidyoReplay, you can skip this step by clicking the **Next** button.)



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

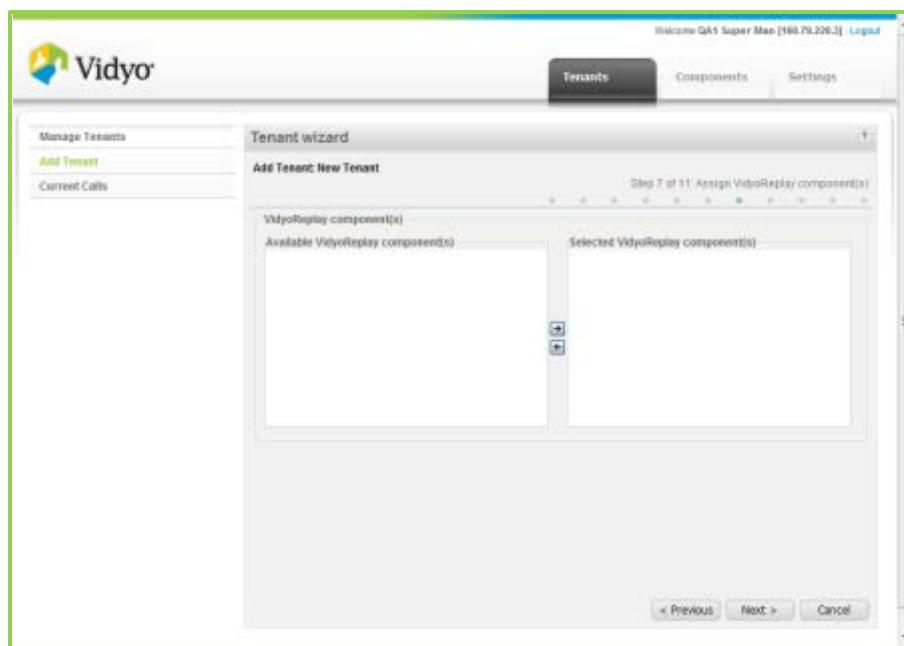
Making the VidyoReplay Components Available

This is step 7 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

To make the VidyoReplay components available:

1. Click **Next** to proceed to Step 7. (If you don't have VidyoReplay, you can skip this step by clicking the **Next** button.)

2. To select a VidyoReplay Component, select one or more in the Available VidyoReplay Recorder components list and click the **Right Arrow** to move them to the Selected VidyoReplay Components list.



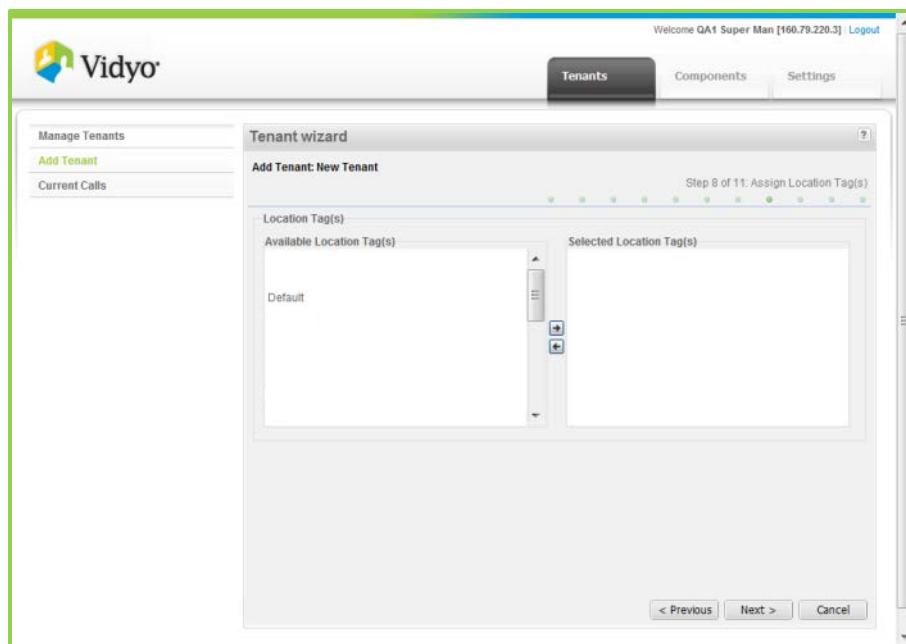
Assigning Location Tags

This is step 8 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

Note: Before you assign location tags, you must create them first. For more information, see “Creating User Location Tags” on page [155](#).

To assign location tags:

1. Click **Next** to proceed to Step 8.



On this page, you can assign location tags to the Tenant. The Super Admin creates the location tags you are able to use. At a minimum you must at least assign the default tag to the tenant.

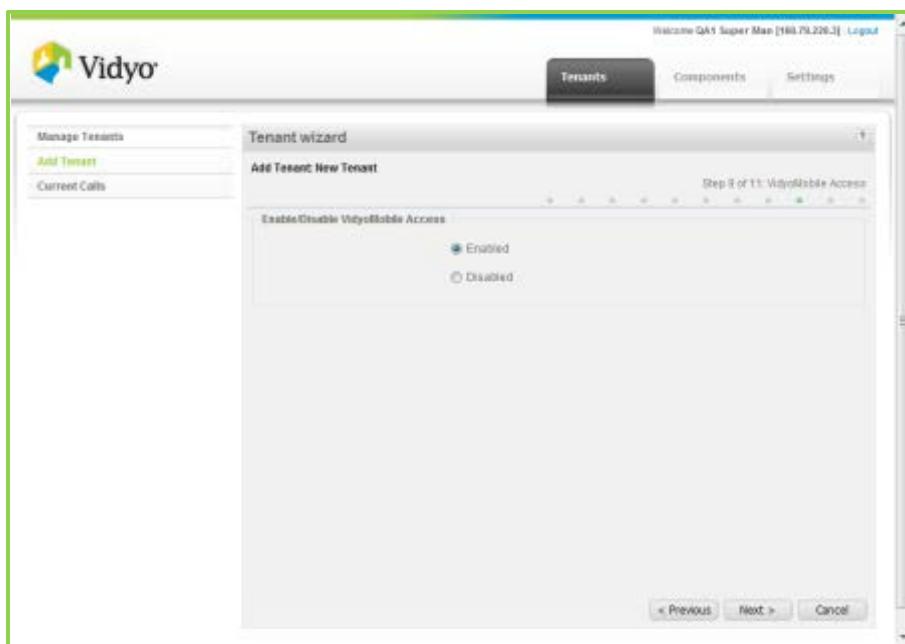
2. To assign a location tag, select one or more in the Available Location Tag list and click the **Right Arrow** to move the Location Tag to the Selected Location Tag list.

Enabling or Disabling VidyoMobile on Your Tenant

This is step 9 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

To enable or disable VidyoMobile:

1. Click **Next** to proceed to Step 9. (If you don't have VidyoMobile, you can skip this step by clicking the **Next** button.)



This page allows you to decide if this tenant has VidyoMobile capability. VidyoMobile is built-in to your VidyoPortal. There are client apps for both Android phones and tablets and iOS iPhones and iPads. You don't have to download the client programs to make them available to your users. End users just download them from the Android Market or the App Store respectively. They don't have to pay anything to download them, but the first time a user logs in to your VidyoPortal, one of your licenses is consumed.

2. Click **Enabled** or **Disabled** choices as desired.

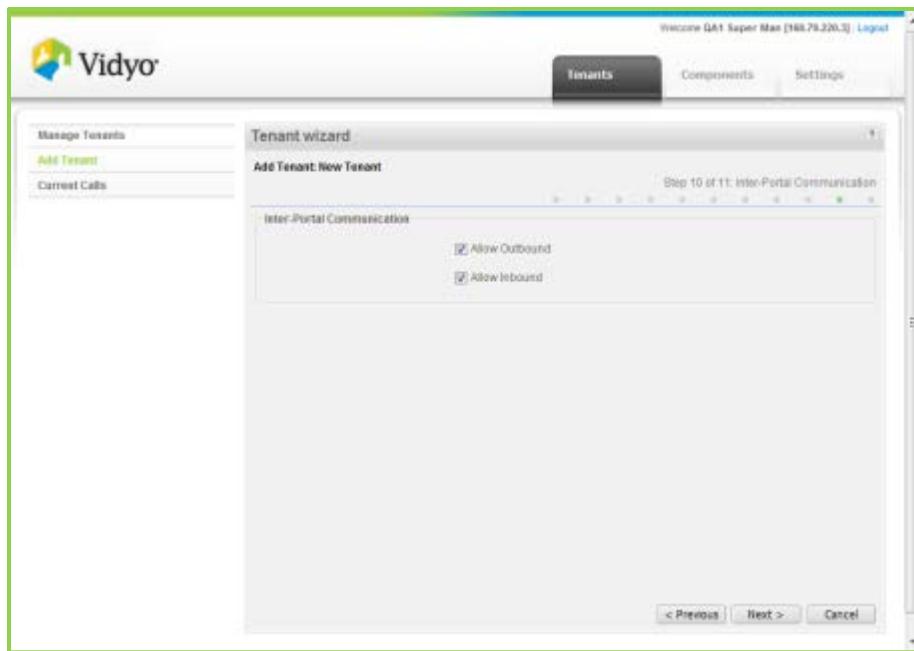
Note: The Super Admin can enable or disable VidyoMobile access for all tenants, or the Super Admin can allow the individual Tenant Admins to control VidyoMobile access (this is the default). Regardless of whether the Super Admin enables or disables VidyoMobile, creating a single tenant with an opposite setting takes precedence for every tenant. For more information on how to enable and disable VidyoMobile access as the Super Admin, see the “Enabling VidyoMobile Access” section on page [104](#).

Allowing Inbound and Outbound Inter-Portal Communication

This is step 10 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

To allow inbound and outbound Inter-Portal Communication:

1. Click **Next** to proceed to Step 10.



2. Decide whether you want to:

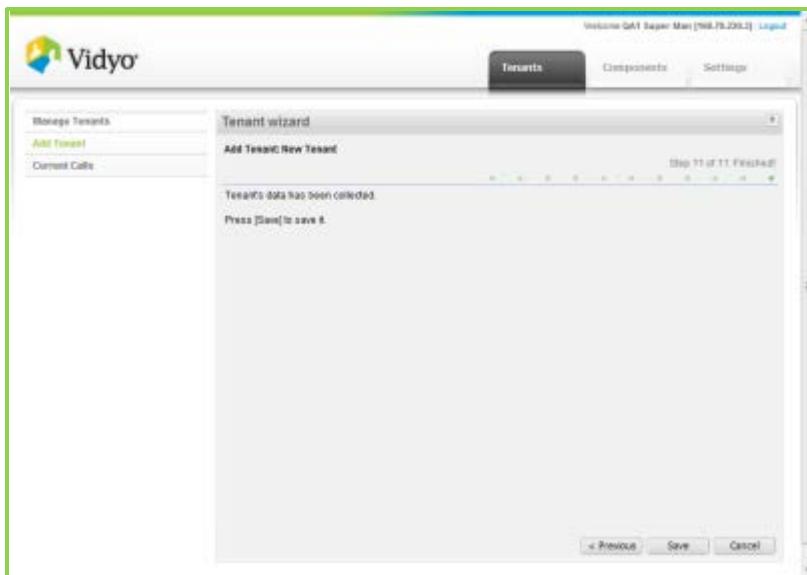
- Only allow calls to other VidyoConferencing systems (Click **Allow Outbound**, keep **Allow Inbound** clear).
- Only allow calls from other VidyoConferencing systems (Keep **Allow Outbound** clear, click **Allow Inbound**).
- Or allow both inbound and outbound calls. (Click both boxes).

Adding the New Tenant to Your System

This is step 11 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see “Overview of the Tenants Table” on page [186](#).

To add the new tenant:

1. Click **Next** to proceed to Step 11.



2. Click **Save** to finish configuring this tenant.

DELETING A TENANT

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

To delete a tenant:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Tenants** tab.
The Manage Tenants left menu item is selected by default
3. Select the check box in the Delete column for the tenant you wish to remove.
4. Click **Delete** at the bottom of the Tenants table.
5. Click **OK** in the Confirmation dialog box that appears.

VIEWING 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 and then click Current Calls on the menu.
- In the Super Admin Portal, click on the Tenants tab on the top navigation bar and then click Current Calls on the menu.

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

- The Name column shows the name of the caller.
- The Extension column shows the extension number of the caller.
- The VidyoRouter column shows the VidyoRouter the caller is using.
- The VidyoRouter Pool column shows the VidyoRouter pool to which the VidyoRouter belongs.

The Current Calls page in the Super Admin displays the same information. In addition, in the left-most column the following information appears:

- The Tenant Name column shows 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 page is for monitoring only. You cannot manage or control calls in the Current Calls page. For information about controlling a meeting, see “Controlling Meetings” on page [218](#).

Name	Extension
gordon@qa1.vidyo.com: 1 (Conference)	
gordon1	11123123123
leo@qa1.vidyo.com: 1 (Conference)	
Linfeng Zhang	10050
linfeng@qa1.vidyo.com: 2 (Conference)	
dean	1139
Linfeng Guo	1110051
utest_share_room@qa1.vidyo.com: 1 (Conference)	
utest_user45	11909145

The Current Calls Table in the Admin Portal

Conference Name	Tenant Name	Name	Extension	VidyoRouter Na...	VidyoRouter Pool
vgv5@qa1.vid...		Conference Room		D210VR3	D210VR3
linfeng@qa1.vid...	Default	dean	1139	D210VR3	D210VR3
gordon@qa1.vi...	Default	gordon1	11123123123	D210VR3	D210VR3
linfeng@qa1.vi...	Default	Linfeng Guo	1110051	D210VR3	D210VR3
leo@qa1.vidyo....	Default	Linfeng Zhang	10050	D210VR3	D210VR3
vgv5@qa1.vid...		Sony PCS-XG80		D210VR3	D210VR3
utest_share_ro...	Default	utest_user45	11909145	D210VR3	D210VR3
vgv5@qa1.vid...	Default	vgv5	11912121	QA5vr1-64bit	QA5vr1
vr31@qa1.vidyo...	Default	vr31 (拓也.たくや...)	11453	D210VR3	D210VR3
vr36@qa1.vidyo...	Default	vr36 (ゆうすけ.ゆう...	11651	D210VR3	D210VR3

The Current Calls Table in the Super Admin Portal

10. Managing Users as the Tenant Admin

WHAT TENANT ADMINS DO

Super Admins configure the system (and create tenants if running a multi-tenant system). Then, they create Tenant Admins who can manage their assigned tenant or tenants.

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.
- Setting up Quality of Service.
- Customize a Contact Us page to enable VidyoConferencing users to contact them for help with the system, customize an About Us page, and set up the boilerplate text for email conference invitations.

If you have a single-tenant system then you need at least 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 in to any tenant using his or her Super Admin credentials.

You use the Users tab to add, delete, and 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.

LOGGING IN AS A TENANT ADMIN

To administer your tenant you must log in to your Tenant Admin Portal, but if you're a Super Admin, you can use your Super Admin credentials.

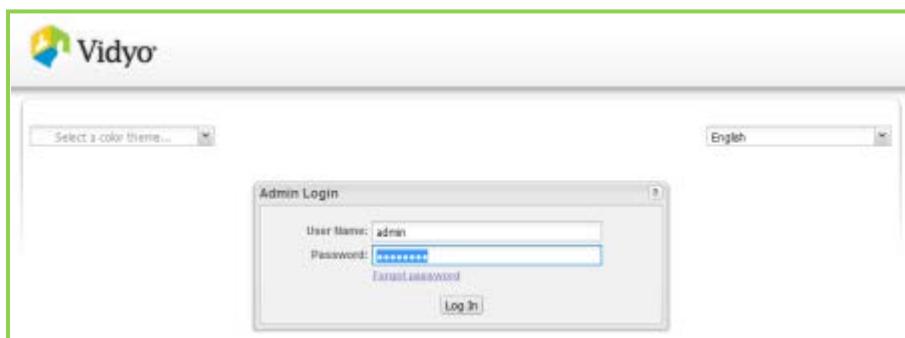
To log in as a Tenant Admin:

1. Log in to the Admin portal using your Admin account.

Enter the FQDN or IP address for the VidyoPortal in the address bar of a web browser, followed by a forward slash and the word "admin":

`http://<FQDN or IP>/admin`

2. Enter the default Admin user name and password.



- User Name: **admin**
- Password: **password** (case sensitive)

Note:

- A password change is required when you first log in to a newly configured tenant.
- For more information, see “Managing Tenant Admin Users” on page [201](#).

SETTING THE LANGUAGE FOR THE ADMIN INTERFACE

The VidyoPortal’s Admin interface is available in these 14 languages:

- | | |
|-------------------------|--------------|
| ■ English | ■ Japanese |
| ■ Chinese (Simplified) | ■ Korean |
| ■ Chinese (Traditional) | ■ Polish |
| ■ Finnish | ■ Portuguese |
| ■ French | ■ Russian |
| ■ German | ■ Spanish |
| ■ Italian | ■ Thai |

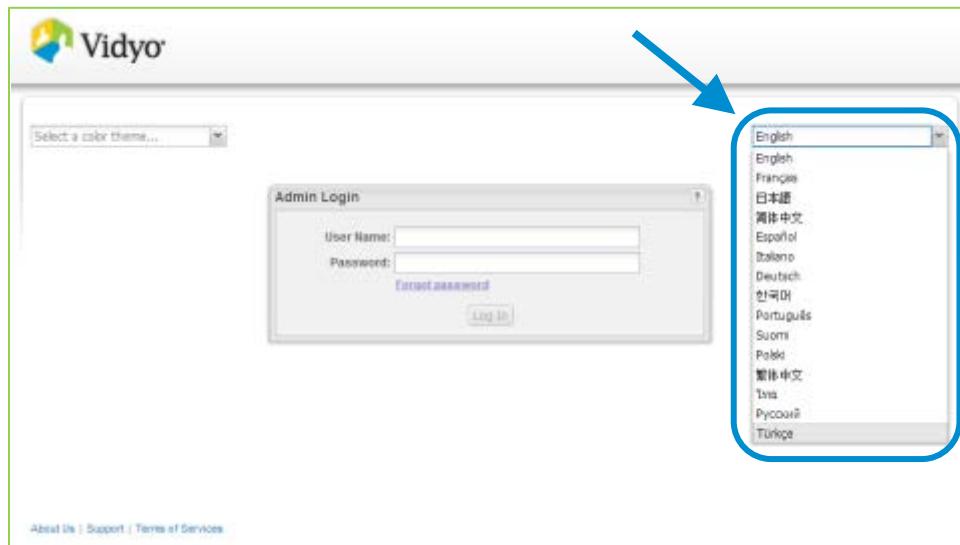
You can set the language of your Admin portal using the drop-down on the upper right corner of the Admin Login page (before or after logging into the system).

Note:

- You can also change the color scheme of your Admin portal using the **Select a color scheme...** drop-down on the upper left corner of the Admin Login page before logging into the system.
- Interfaces are immediately modified after selecting your preferred language or color scheme using the drop-downs.
- Preferred language changes to the Admin interface have no effect on the Super Admin and Vidyo-Desktop interfaces.

To set your preferred language using the drop-down on the upper right corner of the Admin Login page:

- Select your desired language using the language drop-down on the upper right corner of the Admin Login page.



USING THE USERS TABLE

The Manage Users table is used to view, delete, and manage the users in your tenant.

A screenshot of the Vidyo Admin portal. The main navigation bar includes tabs for 'Users', 'Meeting Rooms', 'Groups', and 'Settings'. On the left, there is a sidebar with options: 'Manage Users' (selected), 'Add User', 'Add Legacy Device', 'Import Users', and 'Export Users'. The central area is titled 'Users' and contains a table with the following data:

Member Name	Ext	Type	Group Name	Date Joined	Enabled	Delete
12345678 [12345678]	012234	Normal	Default	10/31/2013	Yes	<input type="checkbox"/>
AdminFirst AdminLast [admin]	012002	Admin	Default	10/18/2013	Yes	<input type="checkbox"/>
jsmith [john]	0122013	Admin	Default	10/30/2013	Yes	<input type="checkbox"/>
cjones [cjones]	012801	Normal	Default	10/30/2013	Yes	<input type="checkbox"/>

At the bottom of the table, there are navigation icons for 'Page 1 of 7', 'Delete', and a message 'Displaying members 1 - 23 of 154'.

To use the Manage Users table:

- Log in to the Admin portal using your Admin account.
- For more information, see “Logging in as a Tenant Admin” on page [201](#).
- Click the Users tab.

The Manage Users left menu item is selected by default.

3. Users in your VidyoPortal appear on the table and include Member Name, Ext, Type, Group Name, Date Joined, Enabled, and Delete fields as columns.

You can drag and drop the column headings to arrange them in the order you prefer.

4. Search by member name, extension, type, group name, and whether or not the user account is enabled using the various fields above the table.

Note: The member name search works for both display name and username. These names are the ones showing in the VidyoPortal and may not necessarily be the user's full name.

5. The lower part of the table includes the following functions:

- Click **Refresh** to refresh the table.
- Click the **First Page**, **Previous Page**, **Next Page**, and **Last Page** direction arrows to scroll through multiple pages of results in the table.
- Enter a page number to access a specific page of results in the table.

ADDING A NEW USER

As the administrator of your tenant, you can add yourself and others as administrative users and also add normal user accounts.

The screenshot shows the Vidyo Admin portal interface. On the left, there's a sidebar with options: Manage Users, Add User (which is selected and highlighted in green), Add Legacy Device, Import Users, and Export Users. The main area is titled "Add User: New User". It contains the following fields:

- User Type: Normal
- User Name: (empty)
- Password: (empty)
- Verify Password: (empty)
- Display Name: (empty)
- E-Mail Address: (empty)
- Extension: 012
- Group: Default
- Proxy: No Proxy
- Location Tag: Default
- Language Preference: System Language
- Description: (empty)

At the bottom of the dialog, there are two checkboxes: "Status: [checkbox] Enabled" and "Allowed to log in to user portal: [checkbox] Enabled". There are also "Save" and "Cancel" buttons at the bottom right.

Alternatively, you can bulk upload users with the Import Users function. For more information, see “Importing Users” on page [209](#).

To add a user:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Users** tab.

The Manage Users left menu item is selected by default.

3. Click the **Add User** on the left menu.
4. Select one of the following User Type options:
 - Select Admin to provide administrative privileges and capabilities as defined in this guide.
 - Select Operator to 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.
 - Select Normal to join meetings, control their own meetings, and place direct calls. Normal users can change their passwords, set their PIN Codes and invite guests, unless the administrator has disabled this capability.
 - Select VidyoRoom to create the account for the physical Vidyo endpoint appliance with the same rights as a normal user.
 - Select Executive to create executive desktop users are a feature of the 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.
5. Enter the following required fields:

All fields marked with a red asterisk * in the UI are required.

- Enter a user name, which is the name the user provides when logging in to the system.

The user name must be alphanumeric and it cannot contain any spaces or punctuation except for the @ sign, periods, underscores, or dashes. The maximum length is 40 characters. If your intended entry has already been taken, you are prompted to select a different name.
- Enter a password.

You must enter the password field identically two times to set the password. Users may change their own passwords later. Like the user name, the password also has a maximum length of 40 characters, but there is no limitation regarding which characters you can use.
- Enter a 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.

You can set VidyoDesktop to show the names of other users (his or her display name value in the system) while in a conference overlaid at the bottom of their images by clicking Settings > Options and selecting the Show Participant Names check box.
- Enter a valid email address for the user.

This is the address to which the new account email is 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.

- Enter the numeric extension you want associated with the user.

This value must be unique for each user. If your intended entry has already been taken, you'll be prompted to select a different extension.

6. 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. You must define groups prior to assigning them.

For more information about managing groups, see "Managing Tenant Admin Groups as the Tenant Admin" on page [230](#).

7. Select either the default proxy or another proxy you have created. You must define a proxies before assigning them.

For more information, see "Configuring a Standalone VidyoProxy Using its Configuration Page" on page [141](#).

8. Select the user's Location Tag from the drop-down list.

For more information about location tags, see the "Managing Location Tags" section on page [265](#) and the "Configuring VidyoCloud" chapter on page [145](#).

9. Select the default language for the specific user you are adding. Use System Language to apply system-wide language settings you chose at installation.

For information, see "Setting the Tenant Language" on page [238](#). Select any other language to change the language for this specific user only.

10. Enter any details or data regarding the person you are adding.

11. Clear the **Enabled** check box to put a user on hold with all of his or her information intact. He or she doesn't show up in searches in the VidyoPortal or are able to log in.

12. Clear **Allowed to log in to user portal** to disable the account's ability to log in to the User portal. Admin and operator accounts may not need to be able to log in to the User portal like a regular user.

13. Click **Save**.

- If some information is missing, incorrect, or already in the system, you 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 is saved to the database, the main table is shown, and a success message is displayed at the top of the page.

EDITING A USER

To edit a user:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Users** tab.

The Manage Users left menu item is selected by default.

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 “Adding a New User” on page [204](#).

The screenshot shows the 'Edit User' interface. The main form has the following data:

- User Type:** Normal
- User Name:** jsmith
- Display Name:** john
- E-Mail Address:** jsmith@yourcompany.com
- Extension:** 012
- Group:** Default
- Proxy:** No Proxy
- Location Tag:** Default
- Language Preference:** English
- Description:** (empty)
- Status:** Enabled (checkbox checked)
- Allowed to log in to user portal:** Enabled (checkbox checked)

6. Click **Save**.

DELETING A USER

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

To delete a user:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Users** tab.

The Manage Users left menu item is selected by default.

3. Select the **Delete** check box at the far right of the user's listing.

You can select multiple users, if desired.

Member Name	Ext	Type	Group Name	Date Joined	Enabled	Delete
12345678 [12345678]	012234	Normal	Default	10/31/2013	Yes	<input type="checkbox"/>
AdminFirst AdminLast [admin]	012002	Admin	Default	10/18/2013	Yes	<input type="checkbox"/>
jsmith (John)	0122013	Admin	Default	10/30/2013	Yes	<input checked="" type="checkbox"/>
cjones (Chris)	012801	Normal	Default	10/30/2013	Yes	<input checked="" type="checkbox"/>

4. Click **Delete** 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 completely and permanently. Once a user is deleted from the system, it cannot be undone.

As an alternative to deleting a user, you can clear **Enabled** on the User's page to changing his or her status to disabled. Disabling a user puts them on hold with all of his or her information intact. He or she doesn't show up in searches in the VidyoPortal or are able to log in. However, you can re-enable them at any time. For more information, see "Editing a User" on page [207](#).

ADDING A LEGACY DEVICE

You can add Legacy systems as if they were users on your VidyoPortal. This feature is used in conjunction with the VidyoGateway to ease dialing from the VidyoPortal to legacy (H.323 and SIP) endpoints and telephones.

For more information, refer to the *VidyoGateway Administrator Guide*.

To add a Legacy device:

1. Log in to the Admin portal using your Admin account.

For more information, see "Logging in as a Tenant Admin" on page [201](#).

2. Click the **Users** tab.

The Manage Users left menu item is selected by default.

3. Click **Add Legacy Device** on the left menu.



4. Enter the Legacy Device Name.
5. Enter the Extension for your Legacy device.
6. Click **Save**.

IMPORTING USERS

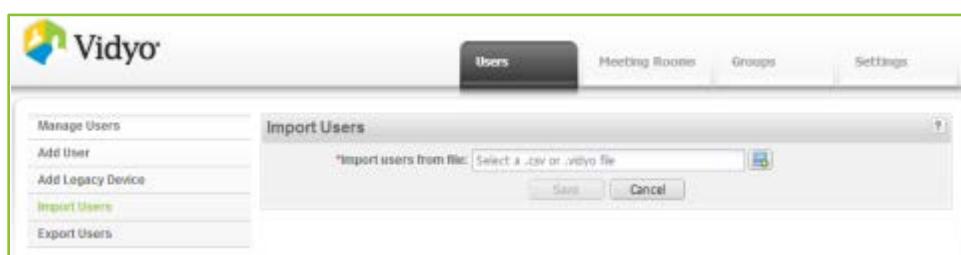
You may import an exported **.csv** or **.vidyo** file (using Exporting Users) containing user information in order to add multiple user accounts. All imported users are created as the normal user type.

Note:

- Except for Proxy and Description, all user account fields are required when importing users.
For more information, see “Exporting Users” on page [210](#).
- The extension values must be numeric values.
For more information, see “Understanding the VidyoPortal User Account Attributes” on page [253](#).

To import users:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Users** tab.
The Manage Users left menu item is selected by default.
3. Click **Import Users** on the left menu.



4. Click **Select File**.
5. After locating and opening your exported **.csv** or **.vidyo** file, click **Save**.

UNDERSTANDING EXPORTING USERS

You may export a **.csv** or **.vidyo** file containing user account data in order to add multiple user accounts using Importing Users on the left menu.

Note: Except for Proxy and Description, all user account fields are required when importing users.

For more information, see “Importing Users” on page [209](#).

The first line of the exported file is considered the header and is not imported as one of the added users. All **.csv** files must use UTF8 encoding. The following image shows the **.csv** data in a spreadsheet.

UserType	Username	Password	Fullname	Email	Extension	Group	Language	Description	Proxy	LocationTag
admin	adm.1	pw	adm.1	test@vidyo.com	101010101	Default	en	Tenant A	No Proxy	Default
admin	adm-2	pw	adm-2	test@vidyo.com	101010102	Default	it	Tenant B	Default	Default
normal	nor@1	pw	nor@1	test@vidyo.com	101010104	Default	fr	Abnormal	Default	Default
normal	qa12	pw	qa12	test@vidyo.com	101010105	Default	ja	So normal it's scary	Default	Default
operator	opr1	pw	opr1	test@vidyo.com	101010107	Default	sc	Smooth	Default	Default
operator	opr-2	pw	opr-2	test@vidyo.com	101010108	default	pt	Heavy equipment	Default	Default
vidyoroom	vrm.1	pw	vrm.1	test@vidyo.com	101010110	Default	fi	Room full of video	Default	Default
vidyoroom	vrm-2	pw	vrm-2	test@vidyo.com	101010111	Default	po	At the monkey house	Default	Default
executive	exe1	pw	exe1	test@vidyo.com	101010113	Default	tc	Privilege	Default	Default
executive	exe_2	pw	exe_2	test@vidyo.com	101010114	Default	en	Action	Default	Default
legacy	leg1	pw	leg1	test@vidyo.com	101010116	Default	es	Subaru	Default	Default
legacy	leg2	pw	leg2	test@vidyo.com	101010117	default	fr	Yet another MCU	Default	Default

The column heading labels (from left to right) include UserType, Username, Password, Fullname, Email, Extension, Group, Language, Description, Proxy, and Location Tag.

Note:

- You can import all types of users including admins, operators, VidyoRooms, executives and legacy devices; however, when imported, they are created with the normal user type.
- The Extension shows the users unique extension.
- The Group shows the provisioned group to which the user belongs. You must define groups before assigning them.

For more information about managing groups, see “Managing Tenant Admin Groups as the Tenant Admin” on page [230](#).

- The Language shows the two-letter language code for the particular user.

For more information about languages, see “Setting the Tenant Language” on page [238](#).

- The Description shows the optional field for any additionally added text (job description, special comments, etc.).

For more information, see “Adding a New User” on page [204](#).

- The Proxy shows the optional proxy to which the user has been assigned.

For more information, see “Adding a New User” on page [204](#).

- The LocationTag shows the location tag to which the user has been assigned.

For more information, see “Adding a New User” on page [204](#) and “Creating User Location Tags” on page [155](#).

EXPORTING USERS

To export users:

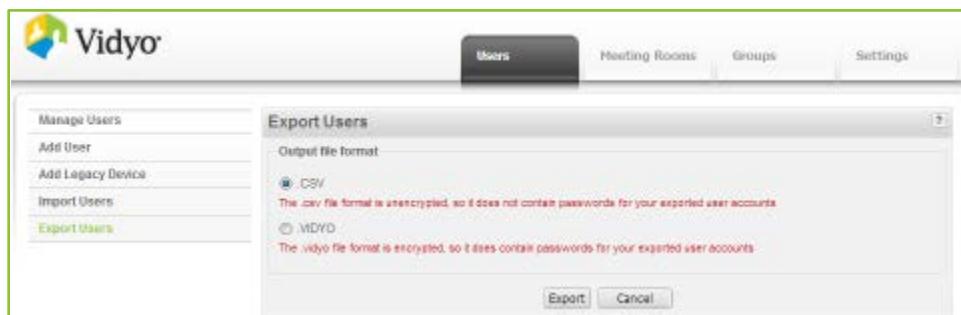
1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Users** tab.

The Manage Users left menu item is selected by default.

3. Click **Export Users** on the left menu.



4. Select the Output file format from the following:

- a. Select .CSV to export your user account data without corresponding passwords in to the standard comma-separated value format.
- b. Select .VIDYO to export your user account data along with corresponding passwords in to the Vidyo encrypted file format.

5. Click **Export**.

11. Managing Meeting Rooms as the Tenant Admin

Every user has a personal room that is automatically assigned to him or her. The admin or operator can also add public rooms that are not associated with a particular user, similar to an actual conference room.

USING THE MANAGE MEETING ROOMS TABLE

The Manage Meeting Rooms table is used to view, delete, and manage the meeting rooms in your tenant.

To use the Manage Meeting Rooms table:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Meeting Rooms** tab.

The Manage Meeting Rooms left menu item is selected by default.

3. Calls taking place in your VidyoPortal appear on the table and include Room Name, Ext, Type, Enabled, Status, Control Meeting, and Delete fields as columns.

You can drag and drop the column headings to arrange them in the order you prefer.

- Status icons indicate the state of the corresponding room as empty, full, locked or PIN protected as follows.

Gary@vidyoqa.io	32502	Personal	Yes		Control Meeting	
-----------------	-------	----------	-----	--	-----------------	--

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 locking and PIN protecting the room.

- Only public rooms can be deleted from the Manage Meeting Rooms table.

For more information, see “Deleting a Public Meeting Room” on page [217](#).

Personal rooms are deleted by deleting the user associated with the personal room.

For more information, see “Deleting a User” on page [207](#).

4. Search fields at the top of the table allow quick and easy searching by room name, extension, type, and whether the room is enabled or disabled.

Room Name	Ext	Type	Enabled	Status	Control Meeting	Delete
12345678	0122342342	Personal	Yes	<input checked="" type="checkbox"/>	Control Meeting	
admin	0120026295	Personal	Yes	<input checked="" type="checkbox"/>	Control Meeting	
John	0122013	Personal	Yes	<input checked="" type="checkbox"/>	Control Meeting	

5. The lower part of the table includes the following functions:
- Click **Refresh** to refresh the table.
 - Click the **First Page**, **Previous Page**, **Next Page**, and **Last Page** direction arrows to scroll through multiple pages of results in the table.
 - Enter a page number to access a specific page of results in the table.

ADDING A MEETING ROOM

Note: Only public rooms can be added here. Personal rooms are automatically generated when you add a new user.

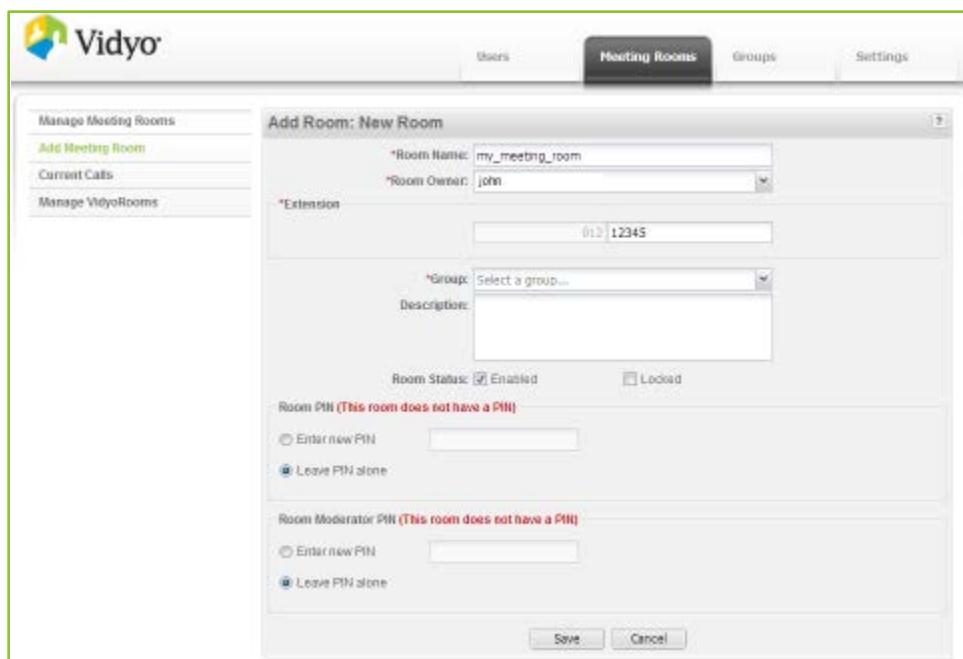
For more information, see “Adding a New User” on page [204](#).

To add a meeting room:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Meeting Rooms** tab.

The Manage Meeting Rooms left menu item is selected by default.

- Click Add Meeting Room on the left menu.



- In the Room Name field, enter the name of your room.

The name must be unique, begin with an alphanumeric character and can't contain spaces. The only other valid characters are periods, underscores, and dashes. The system alerts you provide an existing name.

- In the Room Owner drop-down, select the person to manage and control meetings in the public room.

A list of users is provided on the drop-down for selection. You can also type in the text area of the drop-down to narrow the list.

- In the Extension text field, enter the number used for user's direct calls and speed dial.

The extension value provided must be numeric and unique.

- In the Group drop-down, select the group you want to associate with your new meeting room.

The default group is selected automatically. Remember that groups have special designations of maximum participants and maximum bandwidth privileges.

For more information on groups, see “Managing Tenant Admin Groups as the Tenant Admin” on page [230](#).

- Select the **Enabled** check box to enable your room.

Clearing this check box allows a room to be put on hold with all its information intact. The room also doesn't show up in searches on the User portal.

- Select the **Locked** check box to prevent additional users from accessing your room.

10. Select **Enter new PIN** on the Room PIN section of the screen and enter a four-character PIN in the text box to PIN protect your room.

Participants of this meeting are prompted to enter this PIN before entering meetings in your room. Provide your meeting participants with this PIN prior to meetings you hold in your room.

11. Select **Leave PIN Alone** on the Room PIN section of the screen to not use a PIN or retain the current one (if one is in use) for your room.

12. Select **Enter new PIN** on the Room Moderator PIN section of the screen and enter a four-character PIN in the text box to add a moderator PIN for your room.

The room moderator PIN can be set from this screen, the Edit Room screen, and the Meeting Details screen. You can also set the room moderator PIN from the Room Links screen in the User portal.

13. Select **Leave PIN Alone** on the Room Moderator PIN section of the screen to not use a room moderator PIN or retain the current one (if one is in use) for your room.

14. In the Description field, enter any information that would be useful for the users, such as “This room is used for the weekly sales meeting”.

Note: Room owners can lock the room and configure room and moderator PINs from the User portal.

15. Click **Save** to keep the Meeting Room settings.

- If some information is missing, incorrect, or already in the system, an error message is shown at the top of the screen indicating which fields must be addressed.
- When all required fields are complete and valid, the data is saved to the database and the main table is shown.

EDITING 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 “Adding a Meeting Room ”on page [213](#).

To edit a meeting room:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Meeting Rooms** tab.

The Manage Meeting Rooms left menu item is selected by default.

3. Click the room name you wish to edit.

The room's page appears.

4. Edit field information as necessary.

For more information, see “Adding a Meeting Room” on page 215.

5. Edit or delete the room URL, which is the link participants and guests use to join your room.

- To change the room URL, click  to the right of the Room URL field.
The system automatically generates a new URL.
 - To delete the current room URL, click  to the right of the Room URL field.
6. Click **Save**.
 - If some information is missing, incorrect, or already in the system, an error message is shown at the top of the screen indicating which fields must be addressed.
 - When all required fields are complete and valid, the data is saved to the database, the main table is shown, and a Success message is displayed at the top of the screen.

DELETING A PUBLIC MEETING ROOM

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 the room. If you permanently delete a public room from your system, it cannot be undone. Disabling a room puts it on hold with all its information intact. The room also doesn't show up in searches on the User portal.

For more information about disabling rooms, see “Adding a Meeting Room” on page [213](#).

Note: To delete a personal room associated with a user, you must first delete the user. Deleting the user automatically deletes his or her room.

For more information, see “Deleting a User” on page [207](#).

Room Name	Ext	Type	Enabled	Status	Control Meeting	Delete
12345678	0122342342	Personal	Yes	<input type="checkbox"/>	Control Meeting	<input checked="" type="checkbox"/>
admin	0120026295	Personal	Yes	<input type="checkbox"/>	Control Meeting	<input checked="" type="checkbox"/>
Tam	012987	Public	Yes	<input type="checkbox"/>	Control Meeting	<input checked="" type="checkbox"/>

Note: The Delete check box only appears on the public room on the Meeting Room table.

To delete a public meeting room:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Meeting Rooms** tab.
The Manage Meeting Rooms left menu item is selected by default.
3. Find the public room you wish to delete by using the search filters, sorting on the headers, and pagination.
4. Select a check box or boxes under the Delete column of the room or rooms you want to delete.
5. Click **Delete** at the bottom of the page and answer **Yes** to all prompts.

VIEWING CURRENT CALLS

You can view the calls taking place on your VidyoPortal using the Current Calls screen.

To view current calls on your VidyoPortal:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Meeting Rooms** tab.

The Manage Meeting Rooms left menu item is selected by default.

3. Click **Current Calls** on the left menu.

Calls taking place on your VidyoPortal appear and include the following fields:

- The Conference column
- The Name column
- The Extension column

4. Click the drop-down on the right of each column heading for the following features:

- Select **Sort Ascending** to arrange the current calls appearing on the table in ascending order from top to bottom based on your selected column.
- Select Sort Descending to arrange the current calls appearing on the table in descending order from top to bottom based on your selected column.
- Select or clear Conference, Name, and Extension to control the columns appearing in the table.
- Select Group By This Field.
- Select Show in Groups.

5. The lower part of the table includes the following functions:

- Click **Refresh** to refresh the table.
- Click the **First Page**, **Previous Page**, **Next Page**, and **Last Page** direction arrows to scroll through multiple pages of results in the table.
- Enter a page number to access a specific page of results in the table.

UNDERSTANDING CONTROLLING MEETINGS

Admins and Operator user types have access to the following meeting functions and controls:

- Locking or unlocking the meeting.
- Disconnecting any user.
- Muting any user or disconnecting the video from any user.
- Defining or removing a room PIN.

- Defining or removing a Moderator PIN.
- Creating and deleting a room URL.
- Inviting users to attend the meeting.

Room Name	Ext.	Type	Enabled	Status	Control Meeting	Delete
12345678	012342342	Personal	Yes	<input type="checkbox"/>	Control Meeting	<input type="checkbox"/>
admin	0120026295	Personal	Yes	<input type="checkbox"/>	Control Meeting	<input type="checkbox"/>
Tom	012987	Public	Yes	<input type="checkbox"/>	Control Meeting	<input checked="" type="checkbox"/>

Note:

- The screenshot shown previously shows two personal rooms which have no corresponding check box and therefore cannot be deleted.
- When you delete a user his or her room is deleted with the account.
- You must click a meeting's corresponding Control Meeting link to control the meeting from the Meeting Details screen.
- Admin and Operator user types can control meeting rooms while a meeting is in session.

CONTROLLING A MEETING ROOM

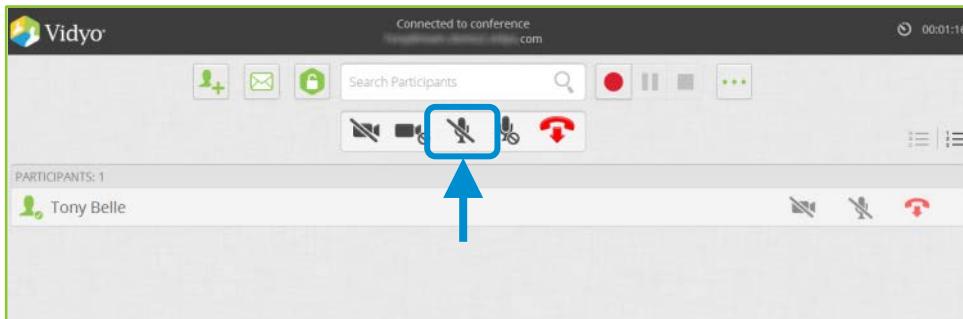
This screen provides certain functions that can apply to all participants in your meeting room or can apply to a selected participant in your meeting room.

For example, you can mute the audio on all participants' microphones without allowing them to re-enable.

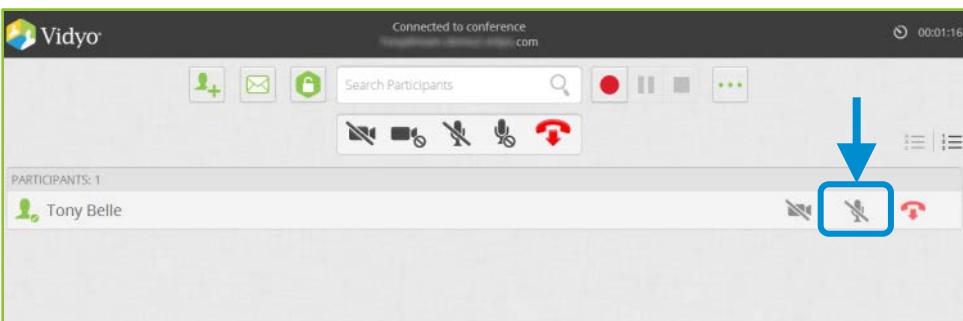
Note:

- When accessed from a tablet, roomlinks may also be used to manage a meeting.
- The HTML-based Control Meeting screen is available when using VidyoDesktop version 3.2 or later.

For more information, see “Customizing the Invite Text” on page [93](#) and “Customizing the Invite Text” on page [243](#).



Or, you can mute the audio of a selected participant’s microphone without allowing that participant to re-enable it.



To control a meeting room:

1. Log in to the Admin portal using your Admin account.

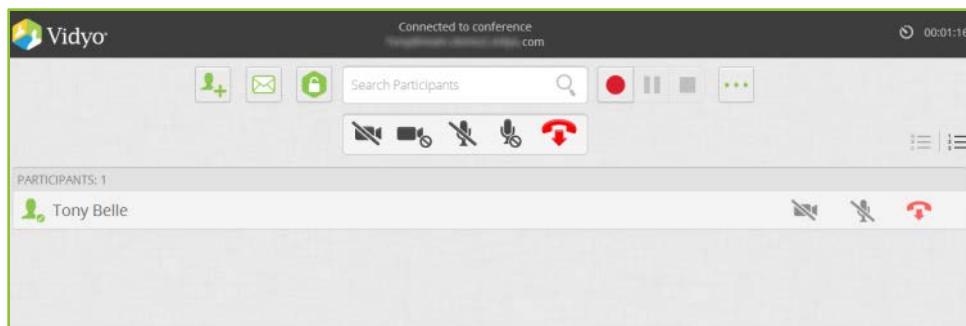
For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Meeting Rooms** tab.

The Manage Meeting Rooms left menu item is selected by default.

3. Click the **Control Meeting** link in the Control Meeting column of the corresponding meeting you want to control.

The HTML-based Control Meeting screen appears.

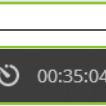


Tip: As you make configurations on the HTML-based Control Meeting screen, notifications appear on the lower part of the screen.

Room is now locked. Additional participants cannot join the conference.

3. Perform any of the following tasks:

Click...	To...
	Add a participant to your room.
	Invite a participant to your room via email.
	Toggle between locking and unlocking your room. Locking prevents additional users from accessing your room.
	Record or record and webcast a meeting using a selected VidyoReplay Record profile. This option only appears if your system includes VidyoReplay.
	Pause a recording or webcast. This option only appears if your system includes VidyoReplay.

Click...	To...
	Stop a recording or webcast. This option only appears if your system includes VidyoReplay.
	Set a moderator PIN, create or remove a room link, and set a room PIN. See “Configuring Moderator PIN, Room Link, and Room PIN Features” on page 222 .
	Disable video on all participants’ cameras without allowing them to re-enable. Or, disable video on a selected participant’s camera without allowing that participant to re-enable it.
	Disable video on all participants’ cameras and allow them to re-enable.
	Mute audio on all participants’ microphones without allowing them to re-enable. Or, mute audio on a single participant’s microphone without allowing that participant to re-enable it.
	Mute audio on all participants’ microphones and allow them to re-enable.
	Disconnect all participants from your meeting room. Or, disconnect a single participant from your meeting room.
	Alphabetically sort the list of your participants.
	Sort the list of your participants in attendance order.
	Toggle between viewing the current conference duration and viewing the current time of day. The conference timer is the default view.

Configuring Moderator PIN, Room Link, and Room PIN Features

To configuring moderator PIN, room link, and room PIN features:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Meeting Rooms** tab.

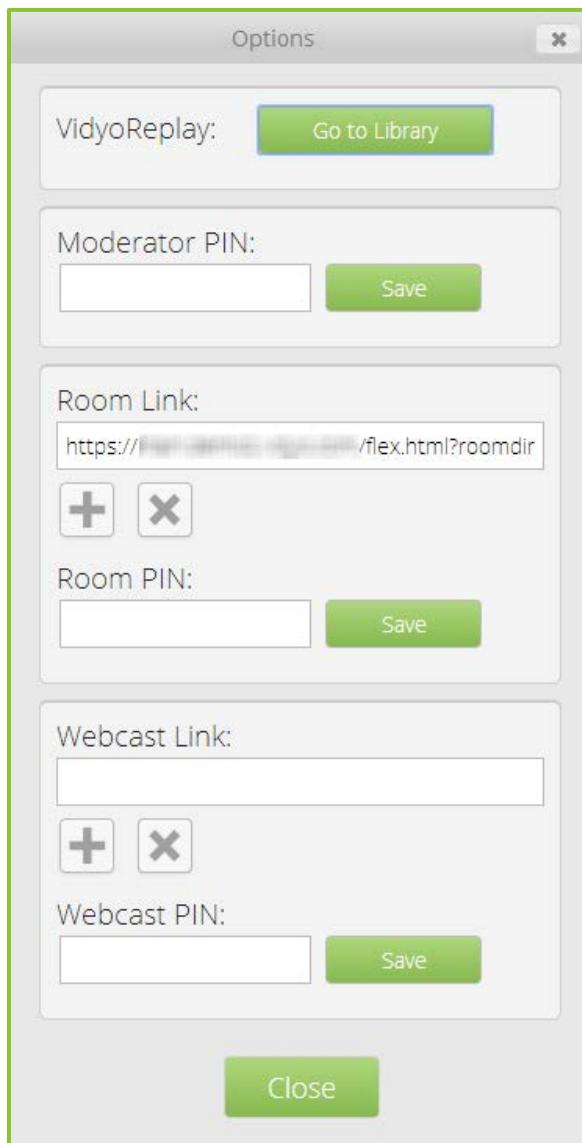
The Manage Meeting Rooms left menu item is selected by default.

3. Click the **Control Meeting** link in the Control Meeting column of the corresponding meeting you want to control.

The HTML-based Control Meeting screen appears.

4. Click **Settings**.

The Options dialog box appears.



5. Click **Go to Library** if your system includes VidyoReplay and you want to access your VidyoReplay library.

For more information about VidyoReplay, refer to the *VidyoReplay Administrator Guide* in the Vidyo Support Center at <http://support.vidyo.com>.

6. If you want to set a moderator PIN, enter four characters in the Moderator PIN text box.

7. Click **Save**.
8. If you want to change the room URL, click the “Create new room link” button beneath the Room Link URL.

The system automatically generates a new URL.

9. If you want to delete the current room URL, click the “Remove room link” button beneath the Room Link field.

The room link URL is the link used by participants and guests to join your room.

10. If you want to set a room PIN, enter four characters in the Room PIN field.

Participants of your room are prompted to enter this PIN before entering. Provide your participants with this PIN prior to meetings you hold in your room.

11. If you want to change the webcast link URL, click the “Create new webcast link” button beneath the Webcast Link field.

The system automatically generates a new URL.

12. If you want to delete the current webcast link URL, click the “Remove webcast link” button beneath the Webcast Link field.

The webcast link URL is the link used by participants and guests to access your webcast.

13. If you want to set a webcast PIN, enter four characters in the Webcast PIN field.

Users accessing your webcast are prompted to enter this PIN before viewing. Provide your participants with this PIN when notifying them about your webcast.

14. Click **Save**.

15. Click **Close**.

SETTING THE MODERATOR PIN ON YOUR ROOM

You can set your own room moderator PIN for rooms you can control in the VidyoPortal without administrator access. When you give this PIN to another user, they can control your room.

For more information, refer to the *VidyoDesktop Quick User Guide* and the *VidyoRoom Quick User Guide*.

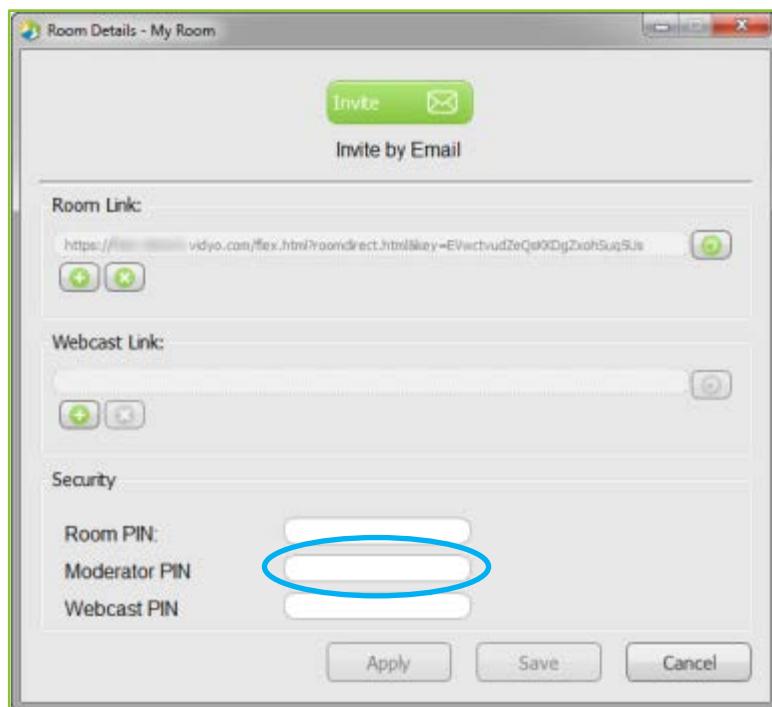
To set the room moderator PIN on your room in the VidyoPortal:

1. Log in to VidyoDesktop.
2. Click the room in which you want to set the moderator PIN from the contacts list.

3. Click **Room Settings** in the upper-right corner of the room dialog box.



4. Enter your new PIN in the **Moderator PIN** field.



5. Click **Save**.

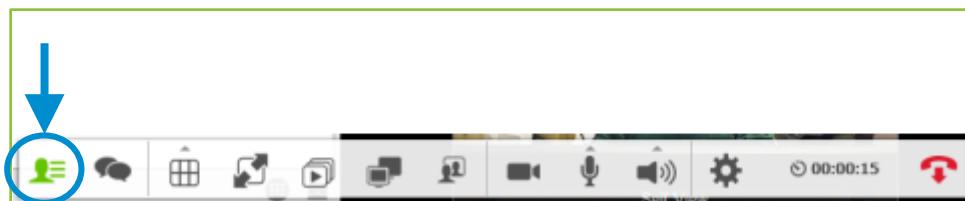
MODERATING ANOTHER PERSON'S ROOM

If someone gives you a moderator PIN, you can use it to control that person's room during a conference.

To moderate another person's Room from VidyoDesktop version 3.2 or later:

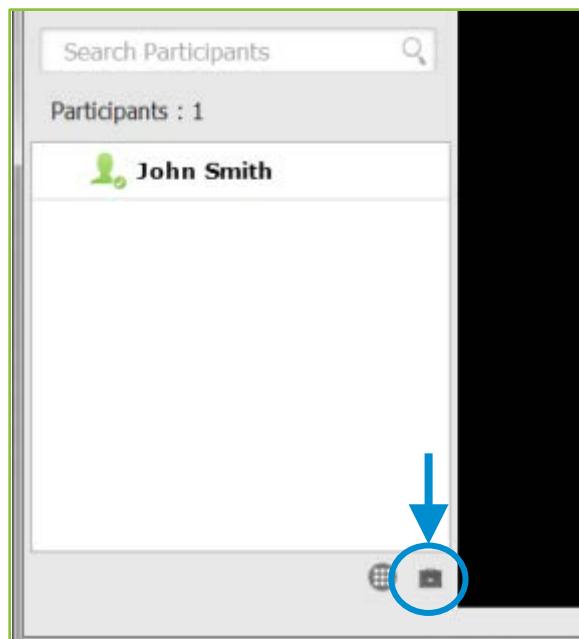
1. Log in to VidyoDesktop.
2. Join a conference in another person's room which you want to moderate.

3. Click **Show Participants**.



The Participants list appears on the left side of the screen.

4. Click **Launch Control Meeting Panel**.



5. Enter the Room Moderator PIN (provided to you by the room owner) in the prompt.



6. Click **OK**.

The HTML-based Control Meeting screen appears.

7. The Control Meeting screen allows you to control the meeting using the Add Participants, Connect All, Disconnect All, Mute All, Unmute All, Silence All, and Remove All buttons.

For more information, see “Controlling a Meeting Room” on page [219](#).

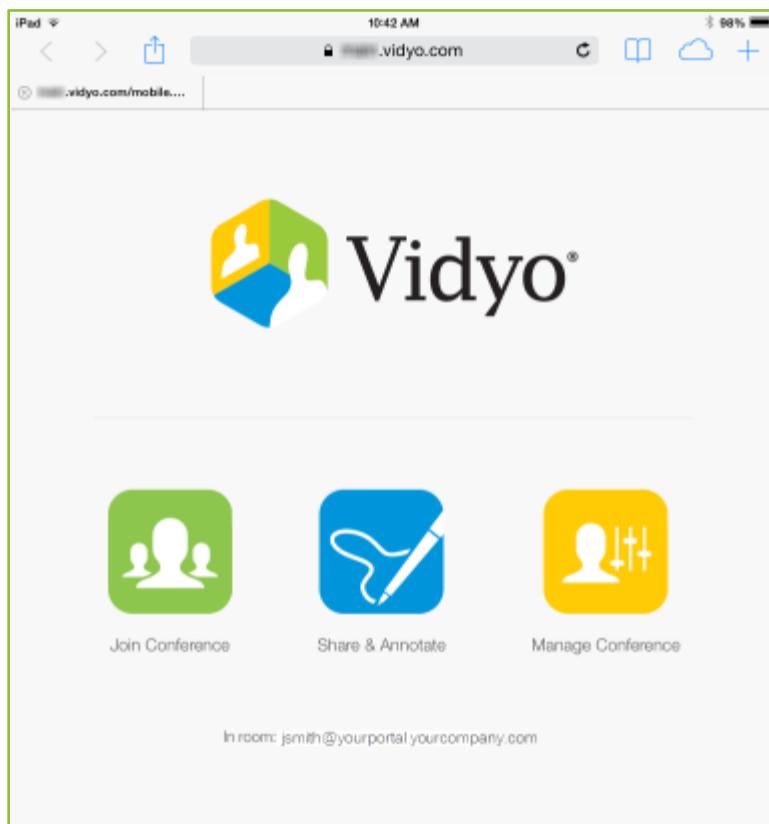
MODERATING ROOMS USING A TABLET

Clicking a guest link from a tablet provides an option to moderate a conference. This can be done either in your own room or in another person's room using a moderator PIN.

To moderate rooms using a tablet:

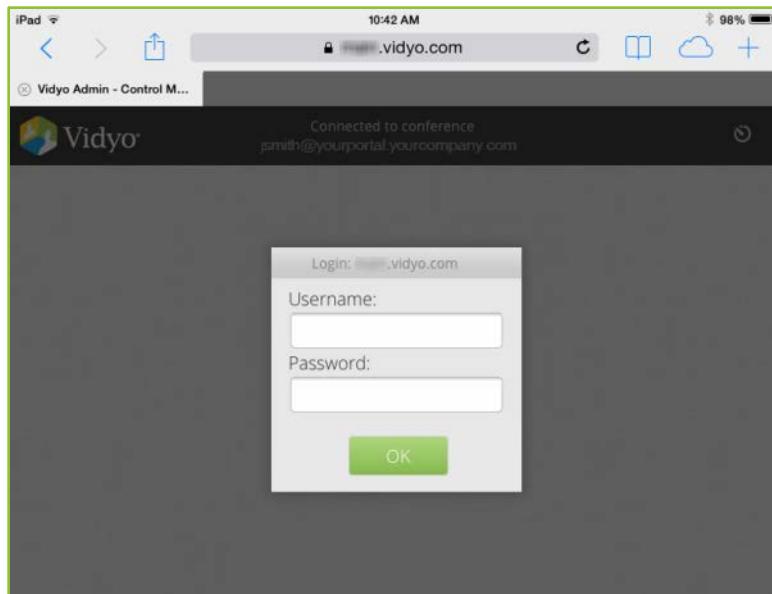
1. Launch your email application on your tablet.
2. Open your VidyoConference meeting invitation.
3. Tap the room link in your meeting invitation.

The Vidyo screen appears.



4. Tap **Manage Conference**.

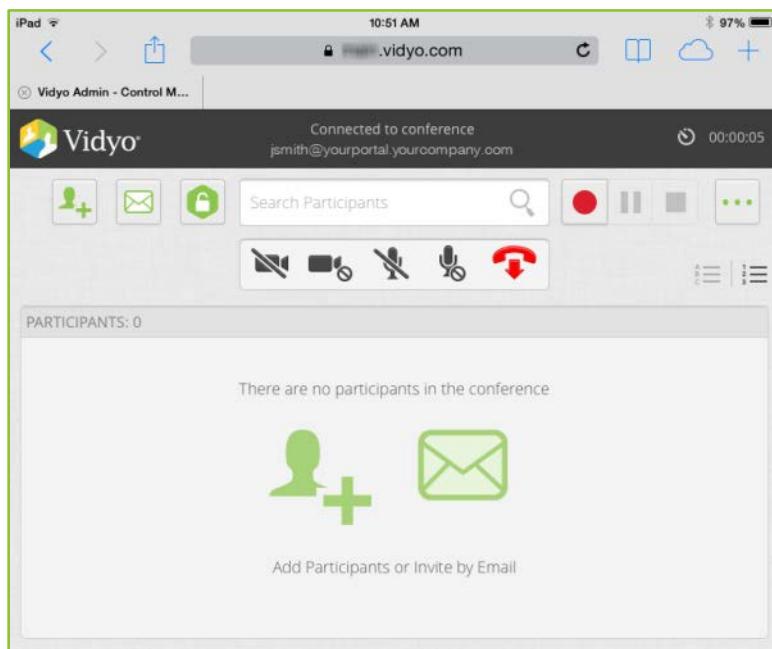
The Control Meeting Login dialog box appears.



5. Enter your username and password.

6. Tap OK.

- If the conference is being held in your own room, the Control Meeting screen appears.



- If the conference is in another person's room you must first provide the moderator PIN.

- a. In the Moderator PIN dialog box, enter the moderator PIN provided by the room owner.

Note: The room must be configured with a moderator PIN provided in the invitation by the room owner.

- b. Tap **OK**.

For more information, see “Controlling a Meeting Room” on page [219](#).

MANAGING PARTICIPANTS

To manage participants:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Meeting Rooms** tab.

The Manage Meeting Rooms left menu item is selected by default.

3. Click **Control Meeting** for the meeting room containing participants you want to manage.

The HTML-based Control Meeting screen appears.

For more information, see “Controlling a Meeting Room” on page [219](#).

12. Managing Tenant Admin Groups as the Tenant Admin

Groups are special designations of users who have the common attributes such as maximum number of users in a call and the maximum bandwidth allowed per call. Users are assigned to the default group automatically unless a new group is created by the Tenant Admin or Operator and the user is assigned to the created group. For additional information about groups, see the definition of Groups on page [18](#).

You may choose to create groups based on specific employee needs or departmental divisions. Changing the group settings for maximum number of users in a call and the maximum bandwidth allowed per call affects the personal meeting room for each user in the group. However, public rooms may be created and can be assigned to a different group than the public room owner.

For more information, see “Adding a Meeting Room” on page [213](#).

USING THE MANAGE GROUPS TABLE

The Manage Groups table is used to view, delete, and manage the groups in your tenant.

To use the Manage Groups table:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Groups** tab.

The Manage Groups left menu item is selected by default.

3. Groups on VidyoPortal appear on the table and include Group Name, Max Participants, Max Bandwidth Out, Max Bandwidth In, and Delete fields as columns.

You can drag and drop the column headings to arrange them in the order you prefer.

4. Search by group name using the Group Name search box above the table.

5. The lower part of the table includes the following functions:

- Click **Refresh** to refresh the table.
- Click the **First Page**, **Previous Page**, **Next Page**, and **Last Page** direction arrows to scroll through multiple pages of results in the table.
- Enter a page number to access a specific page of results in the table.

ADDING A NEW GROUP

To add a new group:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

- 2.** Click the **Groups** tab.

The Manage Groups left menu item is selected by default.

- 3.** Click **Add Group** on the left menu.

- 4.** Enter the following required fields on the New Group screen:

- In the Group Name field, enter the name of the group. The system checks to ensure it is unique.
- In the Max Transmit Bandwidth field, enter the maximum transmit bandwidth in kbps per user. Enter a numeric value for the maximum transmit bandwidth.

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

- 6.** Click **Save** to keep the group settings.

- If some information is missing, incorrect, or already in the system, an error message is shown at the top of the screen indicating which fields must be addressed.
- When all required fields are complete and valid, the data is saved to the database, the main table is shown, and a Success message is displayed at the top of the screen.

EDITING A GROUP

You can edit the settings for any group.

To edit the settings for a group:

- 1.** Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

- 2.** Click the **Groups** tab.

The Manage Groups left menu item is selected by default.

- 3.** Click the group name link for the group you want to edit.

- 4.** Edit the settings as needed.

For information about settings, see “Adding a New Group” on page [230](#).

- 5.** Click **Save** to keep the group settings.

DELETING A GROUP

If you permanently delete a group from your system, it cannot be undone.

To delete a group:

- 1.** Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

- 2.** Click the **Groups** tab.

The Manage Groups left menu item is selected by default.

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

Group Name	Max Participants	Max Bandwidth Out	Max Bandwidth In	Delete
Default	100	10000	10000	<input type="checkbox"/>
Executive Committee	5	100000	100000	<input checked="" type="checkbox"/>
Secret Agents	10	100000	100000	<input type="checkbox"/>

Once the group has been found, select the check box in the Delete column for the group.

4. Click **Delete** at the bottom of the Groups table.
5. Select the **Yes** check box in the Confirmation dialog box that opens.
6. Repeat for all groups that you wish to delete.

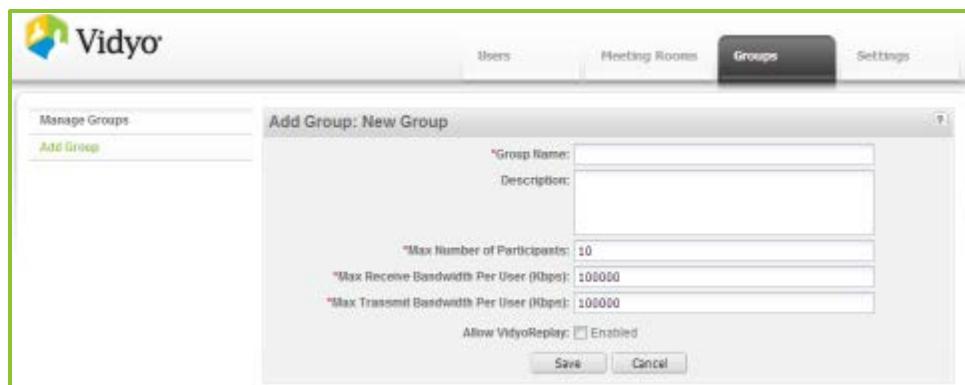
CONFIGURING A GROUP FOR VIDYOREPLAY RECORDER AND VIDYOREPLAY USE

To configure a group for VidyoReplay use:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Groups** tab.
The Manage Groups left menu item is selected by default.
3. You can either create a group for VidyoReplay use or edit an existing one before proceeding to the next step.

For more information, see “Adding a New Group” on page [230](#) and “Editing a Group” on page [231](#).

4. Select **Allow VidyoReplay**.



Note: the Add Group screen is shown here. However, the Allow VidyoReplay Enabled field is also appears on the Edit Group screen as well.

5. Click **Save** to keep the group settings.
- If some information is missing, incorrect, or already in the system, an error message is shown at the top of the screen indicating which fields must be addressed.
6. When all required fields are complete and valid, the data is saved to the database, the main table is shown, and a Success message is displayed at the top of the screen.

13. Configuring Settings as the Tenant Admin

CHECKING YOUR LICENSE TERMS

The License page under the Settings tab provides you with a report of:

- 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).

To check your license terms:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Settings** tab.

3. The License left menu item is selected by default.

Review your license terms shown on the License screen.

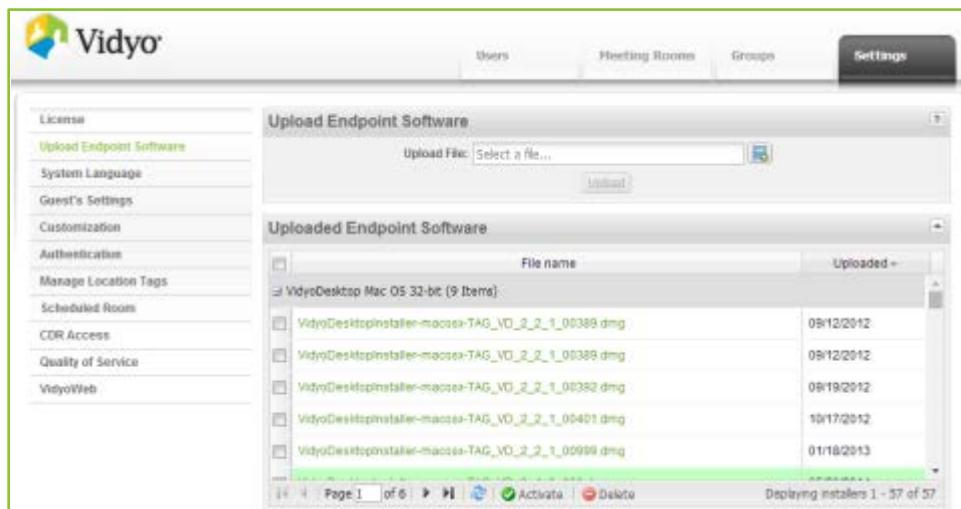
Feature	License
Number of Seats	13310/18500 (Used/Licensed)
Number of Lines	0/400 (Used/Licensed)
Number of Installs	252/400 (Used/Licensed)
Number of Executive Systems	5/10 (Used/Licensed)
Number of VidyoPanorama Systems	2/10 (Used/Licensed)

UPLOADING ENDPOINT SOFTWARE

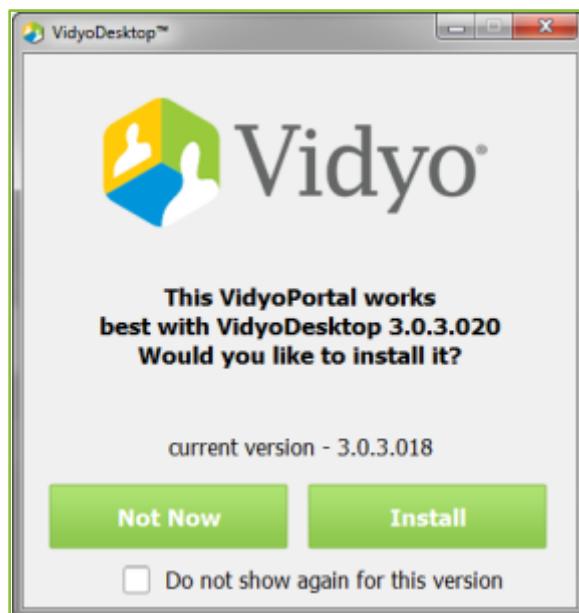
You may choose to perform installations directly on user machines. However, most administrators prefer having users install their VidyoDesktop software by accessing VidyoPortal when provided a user name and password you assign them.

When your users access the VidyoPortal, the VidyoDesktop software is installed even if users do not have administrator privileges. (The Windows installer places the VidyoDesktop-related files in a user-specific directory called “AppData”.)

You provide this software to your users when new versions of the VidyoDesktop and VidyoRoom client software become available from Vidyo by uploading the new software to your servers using the Upload Endpoint Software page.



This way, your users are automatically prompted to download the new version the next time they log in. Users can choose to update their software or skip the update, if desired.



Installation files for various client types include the following:

- VidyoDesktop for Windows
- VidyoDesktop for Macintosh OS X
- VidyoDesktop for Linux

There can be up to four active Linux clients. If the bit architecture the distribution is meant for isn't in the name then it's the 32-bit version. If the distribution is meant for 64-bit machines, the file is named accordingly.

- VidyoRoom

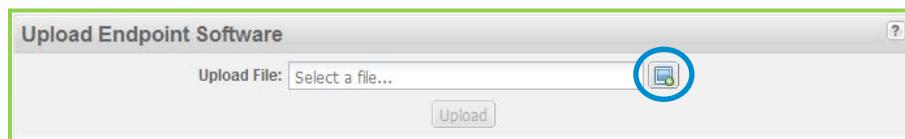
The Super Admin user uploads the latest version of Vidyo client software and makes it available to all users of the VidyoConferencing System. A Tenant Admin user can also upload Vidyo client software for users on their own tenant. This helps the Tenant Admin decide when they want to make endpoint software available for their own users.

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. (Again, Linux is the exception. Up to four Linux versions can be active.) It is the active version that downloads automatically for VidyoPortal users when they first use the system or upgrade to a new version.

Note: Download the latest version of the software to your computer. The link is provided to you by your reseller or by Vidyo Customer Support.

To upload endpoint software installation files:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Upload Endpoint Software** on the left menu.
4. Click **Select File**.



5. After selecting the installation file, click **Upload** to import it.

Note:

- To avoid failure messages, make sure you are uploading Vidyo software only. The software file name ends with 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.

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.

File name	Uploaded
VidyoDesktopDoDInstaller-win32-TAG_VD_2_1_0_00383.exe	10/01/2012
VidyoDesktopDoDInstaller-win32-TAG_VD_2_2_3_00424.exe	04/21/2013
VidyoDesktopDoDInstaller-win32-TAG_VD_2_2_3_00427.exe	05/29/2013

From the Uploaded Endpoint Software list, you can Activate an installer for your users or Delete installers from the list.

Activating an Endpoint Installation File

To activate an endpoint installation file:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Upload Endpoint Software** on the left menu.
4. Click **Activate** at the bottom of the list.

The file name appears highlighted in green.

File name	Uploaded
VidyoDesktopInstaller-win32-TAG_VD_2_1_0_00275.exe	02/03/2011
VidyoDesktopInstaller-win32-TAG_VD_2_1_0_00285.exe	03/23/2011

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. (Again, Linux is the exception. Up to four Linux versions can be active.) It is the active version that downloads automatically for VidyoPortal users when they first use the system or upgrade to a new version.

Deleting an Endpoint Installation File

To delete an endpoint installation file:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Upload Endpoint Software** on the left menu.
4. Select the check boxes for the files you wish to delete.
5. Click **Delete**.

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.

SETTING THE TENANT LANGUAGE

Set the system language of your tenants to one of these 14 languages:

- English
- Chinese (Simplified)
- Chinese (Traditional)
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish
- Thai

To set the system language of your tenants to one of the 14 available languages:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **System Language** on the left menu.

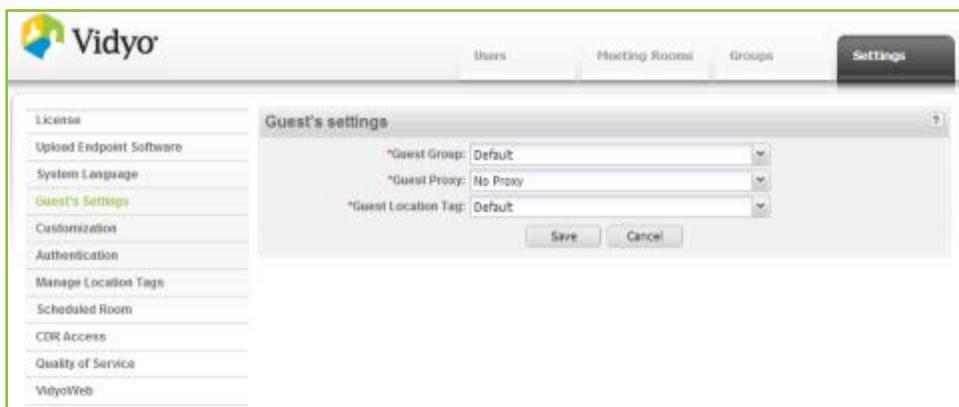
4. Select the System Language from the Default System Language drop-down menu.



Note: This overrides the language set by the Super Admin. Once selected, the page immediately shows your chosen language. It also then becomes the system or tenants default language.

5. Click **Save**.

CONFIGURING GUEST'S SETTINGS



The Guest's Settings page enables you to assign guest users to a group and specify a Location Tag for all guest users. A guest user is an unregistered user of the VidyoConferencing System, but can join meetings to which they are invited by a registered user. In the Settings tab, select Guest's Settings and perform the following:

To provide guest users with group assignments and location tags:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Guest's Settings** on the left menu.
4. Assign guest users to a group by selecting one from the Guest Group list.
5. Assign guest users to a proxy by selecting one from the Guest Proxy list.
6. Assign guest users a location tag by selecting one from the Location Tag list.

7. Click **Save**.

CONFIGURING CUSTOMIZATION ON YOUR TENANT

The Customization left menu item provides additional tabs for making a variety of settings on your tenant.

Customizing the About Info

The About Info page enables you to create and format an About Us page that appears when users click About Us at the bottom of the VidyoPortal home page and the VidyoPortal Admin and Super Admin Portal.

Note:

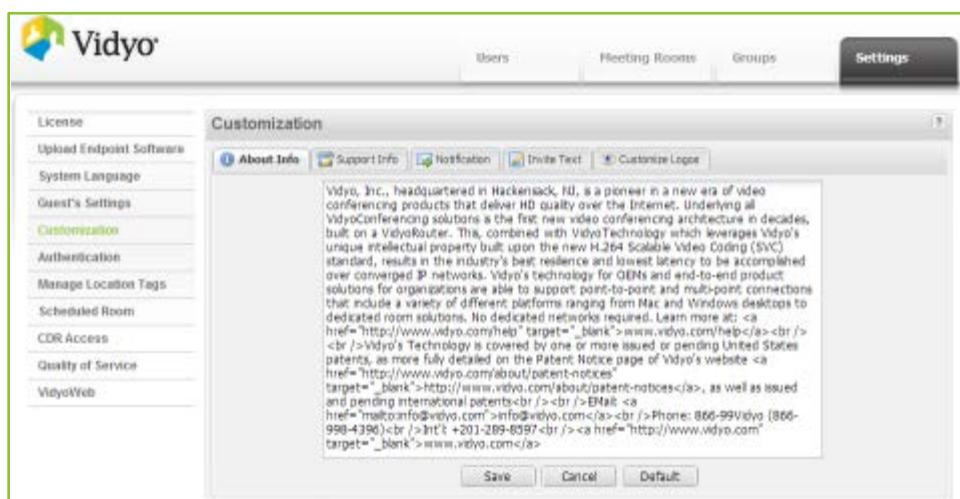
- Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.
- Because of the limitations of Adobe Flash, URLs and other markup information can be inserted into the text but must conform to HTML 1.1 specifications.

To customize the About Us information:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **About Info** tab.



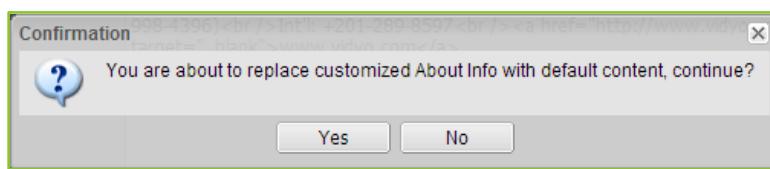
5. Enter text or paste text you have copied from another application.
6. Apply any formatting desired.
7. Click **Save**.

Reverting To Default System Text on The About Info Screen

Note: Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.

To revert to default system text on the About Info screen:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **About Info** tab.
5. To remove any previously saved customized text and revert to the default system text provided by Vidyo, click **Default**.
6. A confirmation dialog box appears.



7. Click **Yes**.

Customizing Support Information

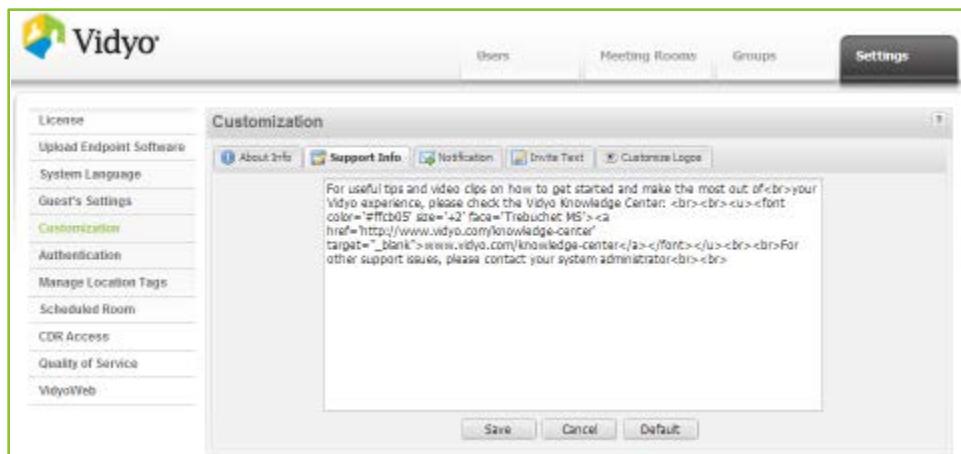
The Support Info page enables you to create and format a contact page that appears when users click Support at the bottom of the VidyoPortal home page as well as the Login page. This is information your users need to contact you, the Tenant Admin. This page is inherited from the Super Admin, but you can customize it here per Tenant.

Note: Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.

To customize the Support Information:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.

- Click the **Support Info** tab.



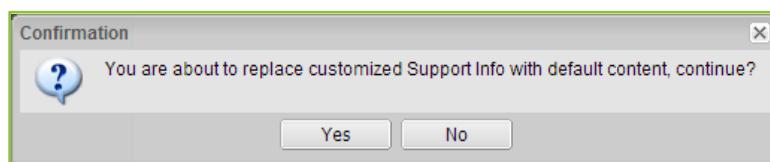
- Enter text or paste text you have copied from another application.
- Apply any formatting desired.
- Click **Save**.

Reverting To Default System Text on The Support Info Screen

Note: Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.

To revert to default system text on the Support Info screen:

- Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
- Click the **Settings** tab.
- Click **Customization** on the left menu.
- Click the **Support Info** tab.
- To remove any previously saved customized text and revert to the default system text provided by Vidyo, click **Default**.
- A confirmation dialog box appears.



- Click **Yes**.

Customizing Notification Information

The Notification page enables you to enter From and To email information that’s used by the VidyoPortal for automated emails. The From address you enter is used for automated emails sent out by the VidyoPortal, such as confirmations to new users that their accounts are activated, and other correspondence.

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 VidyoPortal. Configure SMTP and Security information as desired.

Note:

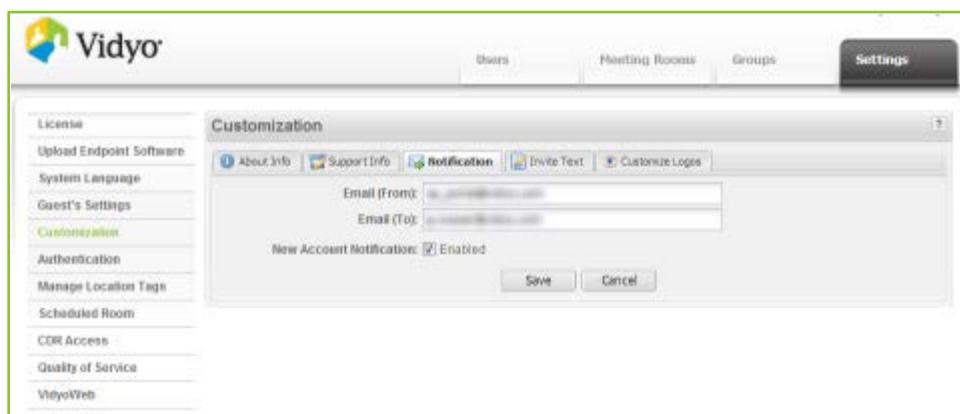
- Be sure to provide a From address. Not doing so can result in SMTP servers blocking emails or changing email headers.
- Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.

To customize Notification information:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Notification** tab.



5. Enter the Email (From) and Email (To) email addresses.
6. Select the New Account Notification check box to have the system send a welcome email to each new account created.

Customizing the Invite Text

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

There are three kinds of invitations.

- Email Content text is sent for VidyoConferences.
- Voice Only text is sent to those participating in voice-only mode via telephone.
- Webcast text is sent to participants accessing your webcast.

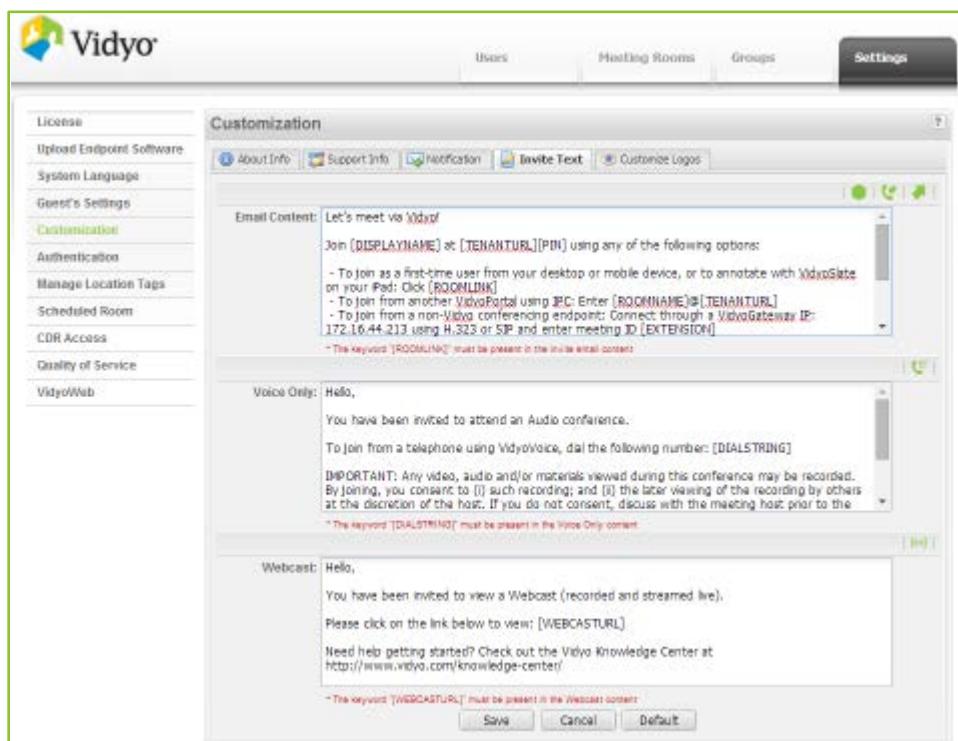
As with the other informational text boxes on the Customization pages, you can use the text as is or modify it as you wish. If you decide to delete the default text and replace it with new text, it's important for you to understand how to use the green buttons in the upper right hand corner of the page.

Note: Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.

For more information, see “Customizing the Invite Text” on page [93](#).

To customize Invite Text:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Invite Text** tab.



5. Change the text from the Email Content, Voice Only, and Webcast sections, as desired.

Some common changes to the messages that you may want to make include the following:

- If your organization has disabled guest access, delete the line about joining as a first-time user from your desktop or mobile device, or to annotate with VidyoSlate on your iPad: Click [ROOMLINK] from the Email Content section.

Note: When accessed from a tablet, roomlinks may be used to join a conference, annotate, or manage a meeting.

- If your system includes a VidyoGateway, add the following sentence as part of your email content:

To join from a non-Vidyo conferencing endpoint: Connect through a VidyoGateway <enter your VidyoGateway IP here> using H.323 or SIP and enter meeting ID [EXTENSION].

Note: Modify the <enter your VidyoGateway IP here> portion with your VidyoGateway IP address.

- If your organization doesn't use IPC, delete the line about joining from another VidyoPortal using IPC: Enter [ROOMNAME]@[TENANTURL] from the Email Content section.
- If your organization doesn't use VidyoVoice, delete the line about using VidyoVoice in the Voice Only section.
- If your organization uses more than one VidyoVoice number, add the additional number or numbers in the Voice Only section.

Note: Keep in mind that due to some browsers' limitations, the message cannot contain more than 1300 characters.

6. The following variables are available when providing text for the Email Content section:

When your email invitations are created, the VidyoPortal automatically passes the specific data to the variable.

- Click  to insert a [ROOMLINK] placeholder for the link to the user's room.
This variable is required your Email Content section.

Note: When accessed from a tablet, roomlinks may be used to join a conference, annotate, or manage a meeting.
- Click  to insert a [VIDYOROOMLINK] placeholder for the link to the conference for sending to a VidyoRoom.
- Click  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. Optionally, you can enter a PIN if you want to require a PIN to enter the room.
- Click  to insert a [LEGACY_URI] placeholder for the URI used by participants accessing your conference from a specific Legacy endpoint.
- The [DISPLAYNAME] variable used in the default text to show the specific user's display name as it was entered in to the system.
- The [TENANTURL] variable used in the default text shows the name of the tenant.
- The [PIN] variable used in the default text shows the room PIN (if one has been set).
- The [ROOMNAME] variable used in the default text shows the name of the room for which the invite was issued.

Note: If applicable, modify the default text in the Email Content section with your VidyoGateway IP address for your participants accessing your conference from Legacy endpoints.

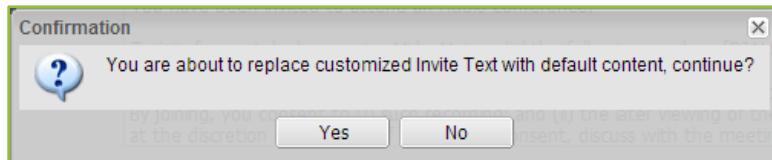
7. Click  to insert a [DIALSTRING] placeholder for the phone number used by participants accessing your conference from a voice-only telephone.
8. Click  to insert a [WEBCASTURL] placeholder for the URL used by participants to access your webcast.
9. Click **Save** to save the invitations.

Reverting To Default System Text on The Invite Text Screen

Note: Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.

To revert to the default system text on the Invite Text screen:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Invite Text** tab.
5. To remove any previously saved customized text and revert to the default system text provided by Vidyo, click **Default**.
6. A confirmation dialog box appears.



7. Click **Yes**.

Uploading Custom Logos on Your Tenant

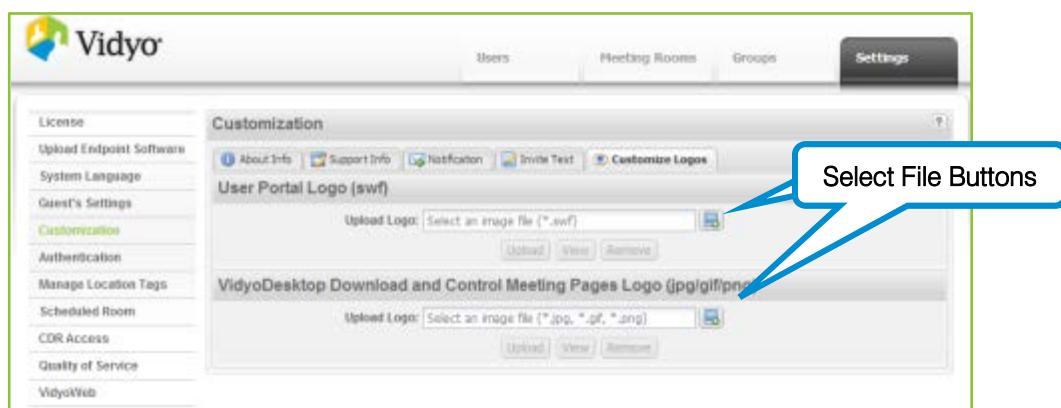
The Super Admin may upload a default User portal and Download Page logo on your tenant. You can then customize these logos on your tenant as desired.

Note:

- Logo customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.
For more information, see “Uploading Custom Logos” on page [96](#).
- The customized logos per tenant appear on the HTML-based Control Meeting screen.
For more information, see “Controlling a Meeting Room” on page [219](#).

To upload your custom logos:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Customization** on the left menu.
4. Click the **Customize Logos** tab.
5. Click **Select File** buttons for the corresponding logo you wish to upload.



Logos can be uploaded for the following system locations:

- The User Portal Logo updates the logo used on your tenant User portal. Each Tenant Admin can upload a different logo for each User portal which replaces the Vidyo logo in the top-left corner of the page and a VidyoPower™ logo appears in the bottom-right corner.
- The User Portal Logo updates the logo used on your tenant User portal. Each Tenant Admin can upload a different logo for each User portal which replaces the Vidyo logo in the top-left corner of the page and a VidyoPower™ logo appears in the bottom-right corner.

Note: The uploaded User Portal Logo should be 150 x 50 pixels and in the **.swf** format. 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. Therefore, the exact size of the logo is less important than the aspect ratio. No matter what size your logo image is, make sure it has a 3:2 aspect ratio. Logos with different proportions will be stretched or squeezed.

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

- The VidyoDesktop Download and Control Meeting Pages Logo updates the logo used on the VidyoDesktop download page shown to users when a software update is performed and the Control Meeting page shown to meeting moderators.

Note: The VidyoDesktop download page logo must be 145 x 50 pixels and can be in the **.gif**, **.jpg** or **.png** formats.

For more information, see “Controlling a Meeting Room” on page [219](#).

- Select your logo file and click **Upload**.

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

- Click **View** to see the logo file currently in use.

The logo file appears in a new browser tab.

- Click **Remove** to delete the logo file currently in use.

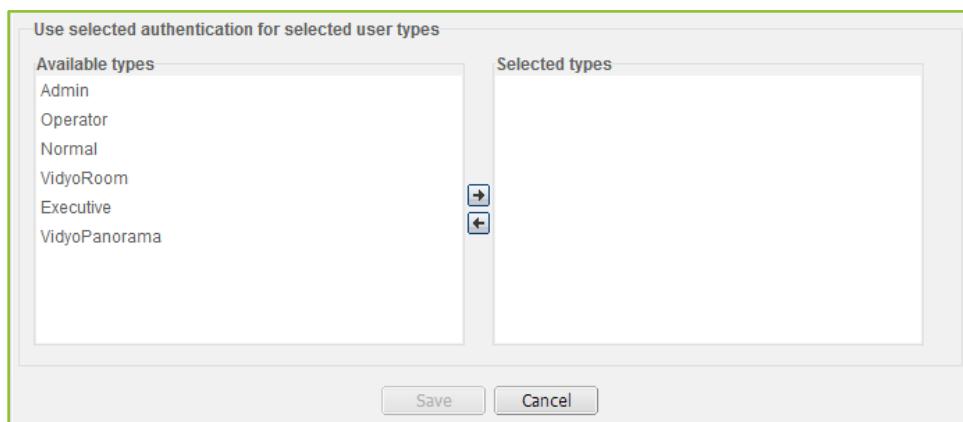
After removal, your logo file is replaced with the system default Vidyo logo.

CONFIGURING AUTHENTICATION

If you do not want to use the local VidyoPortal database to authenticate your users, you can configure your tenant to use LDAP or Web Services authentication.

For more information, see “Configuring Authentication Using Web Services” on page [263](#).

For LDAP and Web Service authentication, you can then apply settings to specific user types.



Configuring Authentication Using LDAP

LDAP Authentication can be used two ways: LDAP Authentication with Manual User Creation and LDAP Authentication with Auto-Provisioning.

Regardless of which LDAP Authentication method you use, your LDAP server must be set up first.

Configuring Your VidyoPortal to Use Your LDAP Server

When you configure your VidyoPortal to use your LDAP Server, you can set it to use a directory system, such as Microsoft Active Directory or Oracle Directory Server, to authenticate your users. When LDAP authentication is enabled on your tenant, your VidyoPortal uses the LDAP protocol to pass your user logins to your directory system for authentication.

Any Vidyo user type (except for the Super Admin and System Console accounts) can be authenticated by LDAP (Normal, Operator, Admin, VidyoRoom, etc.). For more information, see “Understanding the Different System Accounts” on page [11](#).

Note:

- To use secured LDAP, upload your LDAP certificate chain (intermediates and root) from your certification authority using the Security tab before enabling LDAP. For more information, see “Securing Your VidyoConferencing System with SSL and HTTPS” on page [301](#).
- When LDAP authentication is enabled, the User and Admin Portals do not show Change or Reset Password options.

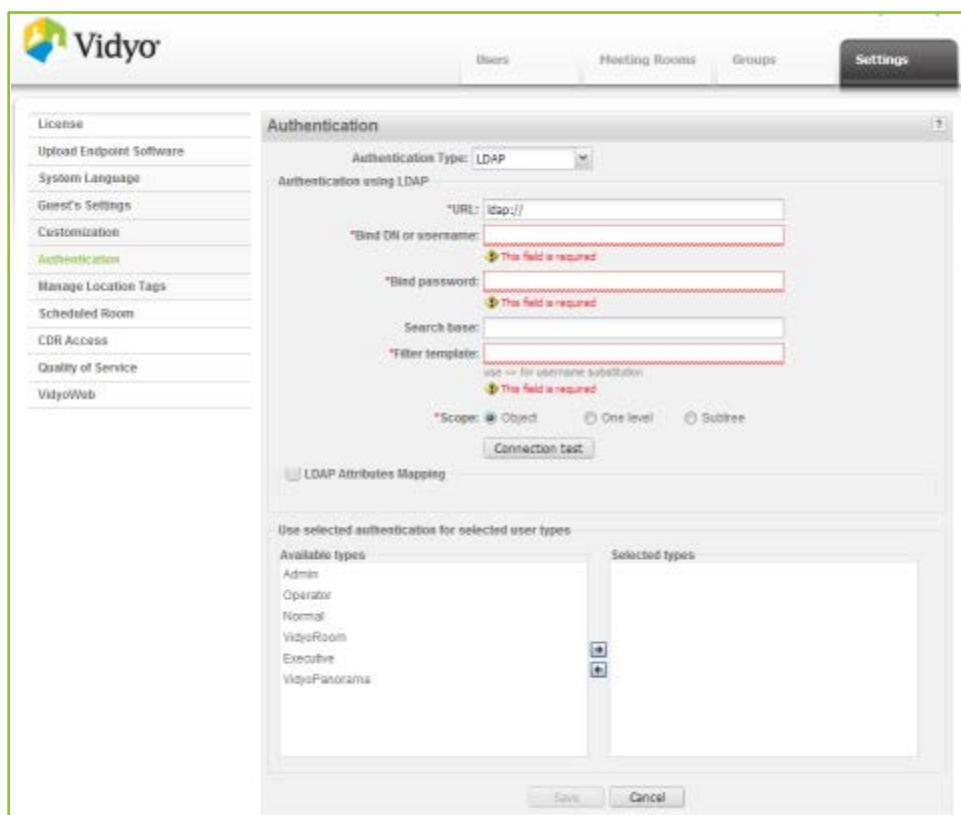
To configure your VidyoPortal to use your LDAP server:

1. Log in to the Admin portal using your Admin account.

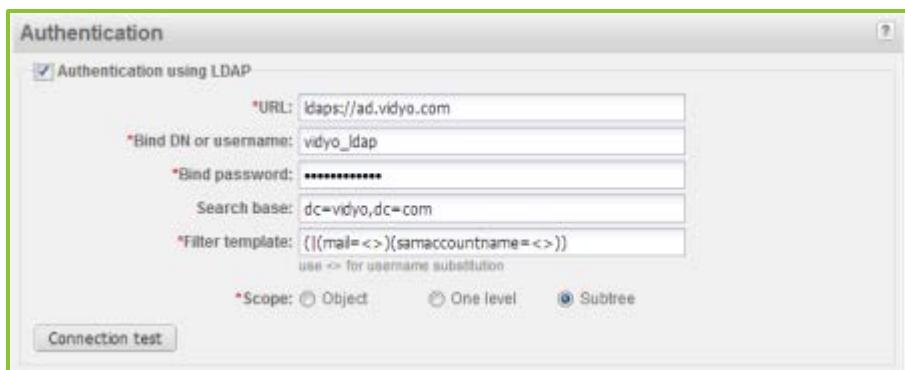
For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Settings** tab.
3. Click **Authentication** on the left menu.
4. Select **LDAP** from the Authentication Type drop-down.

The Authentication screen expands and shows additional fields as follows:



The following screenshot shows a typical LDAP configuration:



5. Enter the following information:

- In the URL field, enter the LDAP server URL.

The format is **ldaps:// <IP or FQDN>/:389**

Note: To use secure LDAP (LDAPS), use an “ldaps” prefix:

ldaps:// <IP or FQDN>/:636

- In the Bind DN or username field, enter the bind DN or user name to log in to the LDAP server.

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

Note: The user must be able to search the LDAP tree.

- In the Bind password field, enter the password needed to bind with the LDAP server.
 - In the optional Search base field, enter the base object (baseObject) used for searching.
- For example: ou=employees, dc=vidyo, dc=com.

- In the Filter template field, enter the configuration string to return the LDAP Distinguished Name (DN).

For example: uid=<> where <> is replaced by the VidyoPortal user name during authentication.

- In the Scope options, select the base object (baseObject) to search:
 - Select **Object** to search the named entry; typically used to read just one entry.
 - Select **One level** to search the entries immediately below the base DN.
 - Select **Subtree** to search the entire subtree starting at the base DN.

6. Click the **Connection Test** button.

The Connection Test dialog box appears.

7. Enter your LDAP user name and password.

- If validation is successful and the LDAP settings are working, click **Save** to save your LDAP settings.

Note: A successful connection test is required to enable the Save button on the lower part of the screen.

- 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 determines whether or not your LDAP settings are correct.

8. Configure authentication on your tenants using your desired method: LDAP Authentication with Manual User Creation or LDAP Authentication with Auto-Provisioning.

For more information see “Configuring LDAP Authentication with Manual User Creation” on page [248](#) or “Configuring LDAP Authentication with Auto-Provisioning” on page [261](#).

9. Apply authentication to specific user types.

For more information see “Applying Authentication (LDAP or Web Service) to Specific User Types” on page [264](#).

10. Click **Save**.

Configuring LDAP Authentication with Manual User Creation

This LDAP Authentication method requires you to manually create user accounts on your tenant. The user attributes can be manually changed and configured; however, only the password is verified against your LDAP server configured in the previous section.

To configure LDAP authentication with manual user creation:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Settings** tab.

3. Click **Authentication** on the left menu.

4. Configure your VidyoPortal to user your LDAP server.

For more information, see “Configuring Your VidyoPortal to Use Your LDAP Server” on page [248](#).

5. Manually create user accounts on your tenant. User accounts can be added at any time.

For more information, see “Adding a New User” on page [204](#) or “Importing Users” on page [209](#).

Note:

- When you create a new user with LDAP authentication enabled, the user name must match the user name configured on your LDAP server. For more information, see the Filter template field explained in the previous section.
- When creating new users, passwords are mandatory; however, when you enable LDAP, the password in the local database is not used to authenticate the user.

- When LDAP authentication is enabled, the User and Admin portals do not provide Change or Reset Password options.
6. Apply authentication to specific user types.
For more information see “Applying Authentication (LDAP or Web Service) to Specific User Types” on page [264](#).
 7. Click **Save**.

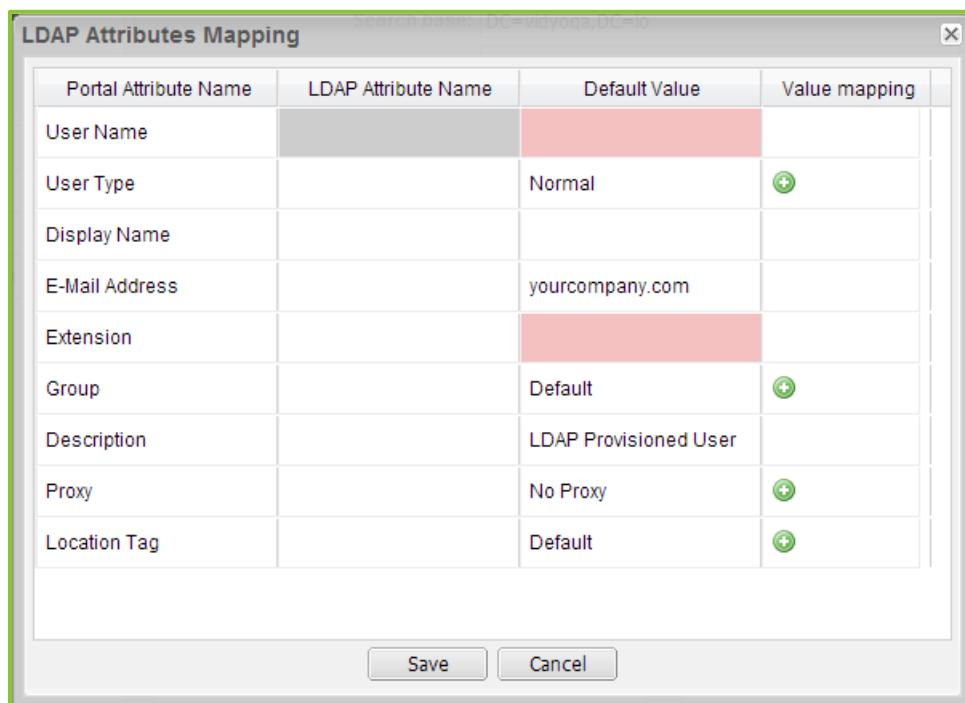
Understanding LDAP Authentication with Auto-Provisioning

This LDAP Authentication method automatically creates user accounts on your tenant based on mapping configurations. When your users log in to the User or Admin portals, the following takes place:

1. The user name and password is validated against the LDAP server.
For more information, see “Configuring Your VidyoPortal to Use Your LDAP Server” on page [248](#).
2. If authentication succeeds, the LDAP server returns the user’s attributes as you have specified using the LDAP Attributes Mapping dialog box.
3. The VidyoPortal then uses the set of attributes returned from the LDAP server to create a new user account in the system.

Note: Before enabling LDAP Authentication with auto-provisioning, it is highly recommended that you first decide which LDAP attributes you want to map to your VidyoPortal user account attributes. These mapping decisions become your LDAP auto-provisioning scheme during the Edit Attributes Mapping step in the following procedure.

The LDAP Attributes Mapping dialog box looks like the following:



Each row on the LDAP Attributes Mapping dialog box represents an attribute. For each attribute, there is an associated Portal Attribute Name, LDAP Attribute Name, Value mapping (where applicable), and Default Value. These configurations become the rules telling the system what values to populate in specific user account fields when the new account is created.

Understanding the VidyoPortal User Account Attributes

When a user is created manually in the VidyoPortal, there is a specific set of attributes required to create an account. The following list of Portal Attributes can be mapped based on LDAP Attributes in order to create accounts automatically.

Note: When you provision users with LDAP, user data is read-only in the Edit User screen after clicking a member name from **Users > Manage Users** in the Admin portal.

The following list explains VidyoPortal attributes (Portal Attribute Names) that can be mapped to LDAP Attribute Names. Default Values for the attributes and Value mapping selection criteria (where applicable) are also explained here.

- User Name is the name of this specific LDAP attribute in the VidyoPortal.
 - In the LDAP Attribute Name, enter a value to map to the VidyoPortal User Name in your LDAP schema.

Many users choose to enter **userPrincipalName** as the LDAP Attribute Name when using a Microsoft Active Directory LDAP server. This is a required attribute.

Note: The LDAP Attribute you associate with the User Name must be specified as part of your Filter template. For more information see “Configuring Your VidyoPortal to Use Your LDAP Server” on page [248](#).

- No Default Value is entered for User Name.

Note: Default Value may not be configured because this is a mandatory, unique attribute.

- No Value mapping configurations are made for the User Name.
- User Type is the name of this specific LDAP attribute in the VidyoPortal.
 - In the LDAP Attribute Name, enter a value to map to the User Type in your LDAP schema.

Many users choose to enter **memberOf** as the LDAP Attribute Name. The **memberOf** value returns a list of groups of which the particular user is a member. This list is then used for Value mapping selection criteria.

 - The Default Value you enter here is used as the default User Type when the LDAP Attribute Name does not exist or returns an invalid attribute value or no Value mapping criteria is met.

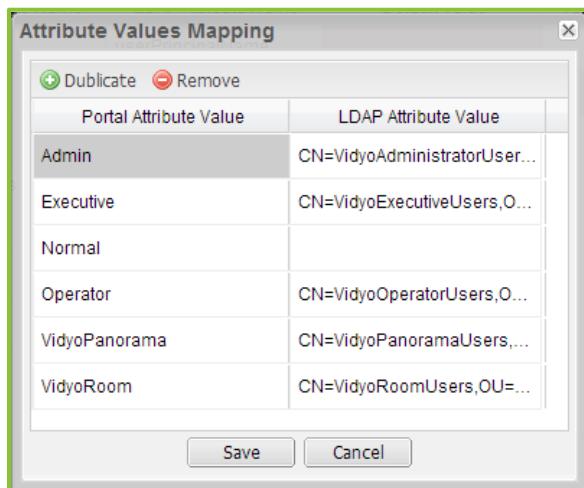
You can select from Admin, Operator, Normal, VidyoRoom, Executive, and VidyoPanorama options. For more information, see “Users” on page [15](#).

 - The Value mapping is used to make specific associations between exact Portal Attribute Values and LDAP Attribute Values based on the LDAP Attribute Name selected for your User Type.

Different users return different LDAP Attribute Values. The Attribute Values Mapping dialog box allows you to map specific associations for all possible values returned.

If desired, select the Duplicate or Remove buttons to create or delete rows in the Attribute Values Mapping dialog box.

The following screenshot provides an example of a Value mapping configuration where the **memberOf** LDAP Attribute Name is used.



For example, using the screenshot shown here, you can see that when a user is a member of the VidyoAdministratorUser group and logs in to the User or Admin portal, the account is created with the Admin User Type.

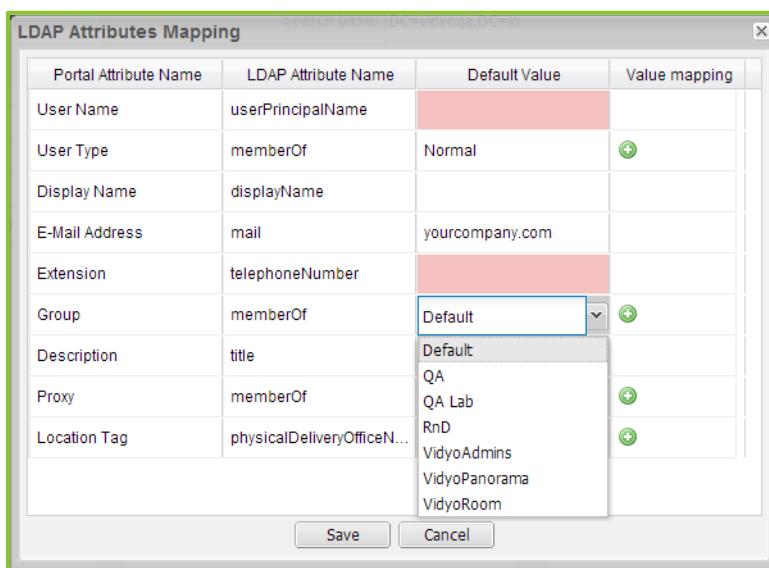
Note: In order to create these Portal User Type mapping associations, Vidyo recommends your LDAP administrator creates specific security groups on your LDAP server in advance.

- Display Name is the name of this specific LDAP attribute in the VidyoPortal.

- In the LDAP Attribute Name, enter a value to map to the Display Name in your LDAP schema.
Many users choose to enter **DisplayName** as the LDAP Attribute Name.
 - In the Default Value, enter a value for the Display Name in this cell for use when a value is somehow missing for any reason.
Note: If you do not type a Default Value for the Display Name in this cell, the system uses the User Name as the default.
 - No Value mapping configurations are made for the Display Name.
- E-Mail Address is the name of this specific LDAP attribute in the VidyoPortal.
- In the LDAP Attribute Name, enter a value to map to the Email Address in your LDAP schema.
Many users choose to enter **mail** as the LDAP Attribute Name. When a user logs in to the User or Admin portal, the system validates that the LDAP Attribute Name value is actually an email address. Otherwise, the system uses the Default Value.
 - The Default Value you enter here is the domain portion of the automatically created email address for the account. When a user logs in to the User or Admin portal and an invalid email address is provided as the LDAP Attribute Name, the system constructs an email address for the account by taking the User Name provided, combining it with what you type as the Default Value, and inserts an @ symbol in between them.
For example, if you log in as **jsmith** and your Default Value is **Vidyo.com**, the system will automatically construct an email address of **jsmith@vidyo.com**.
 - No Value mapping configurations are made for the E-Mail Address.
- Extension is the name of this specific LDAP attribute in the VidyoPortal.
- In the LDAP Attribute Name, enter a value to map the Extension in your LDAP schema.
You may choose to enter **telephoneNumber** as the LDAP Attribute Name when using a Microsoft Active Directory LDAP server.
 - No Default Value is entered for Extension.
When a user logs in to the User or Admin portal and an empty or invalid LDAP Attribute Name is retrieved from your LDAP server, the system randomly auto-generates an extension value for the new account.
Note: If you do not wish to map extensions for new accounts, leave the LDAP Attribute Name blank and the system will use the Default Value to randomly auto-generate extension values for new accounts.
 - No Value mapping configurations are made for the Extension.
Note: When choosing an LDAP Attribute to map to the Extension attribute in the VidyoPortal, if the value retrieved from LDAP contains any special characters, such as dashes and parentheses, your VidyoPortal will reject the mapped extension and auto-generate one using the Default Value.

The following two examples show unacceptable and acceptable LDAP Attribute Values when mapped to the Extension attribute in the VidyoPortal:

- **Unacceptable: (123) 456-7890**
 - **Acceptable: 1234567890**
 - Group is the name of this specific LDAP attribute in the VidyoPortal.
 - In the LDAP Attribute Name enter a value to map the Group in your LDAP schema.
- Many users choose to enter **memberOf** as the LDAP Attribute Name. The **memberOf** value returns a list of groups of which the particular user is a member. This list is then used for Value mapping selection criteria.
- The Default Value you enter here is used as the default User Type when the LDAP Attribute Name does not exist or returns an invalid attribute value or no Value mapping criteria is met.
- The VidyoPortal tenant used in this example has Groups configured as QA, QA Lab, RnD , VidyoAdmins, VidyoPanorama, and VidyoRoom values, from which you can select. Map these groups using the Attribute Value Mapping dialog box.

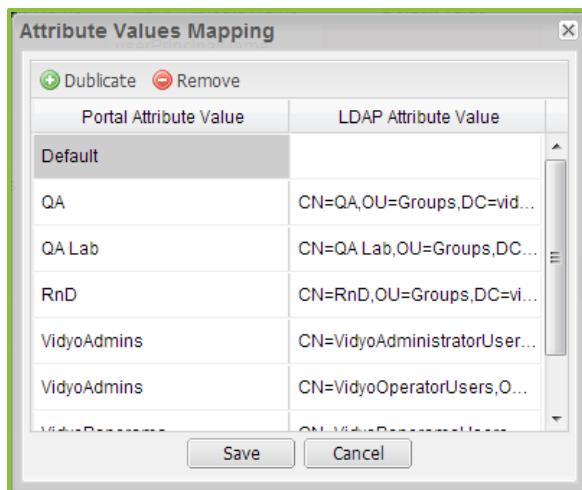


- The Value mapping is used to make specific associations between exact Portal Attribute Values and LDAP Attribute Values based on the LDAP Attribute Name selected for your User Type.

Different users return different LDAP Attribute Values. The Attribute Values Mapping dialog box allows you to map specific associations for all possible values returned.

If desired, select the Duplicate or Remove buttons to create or delete rows in the Attribute Values Mapping dialog box.

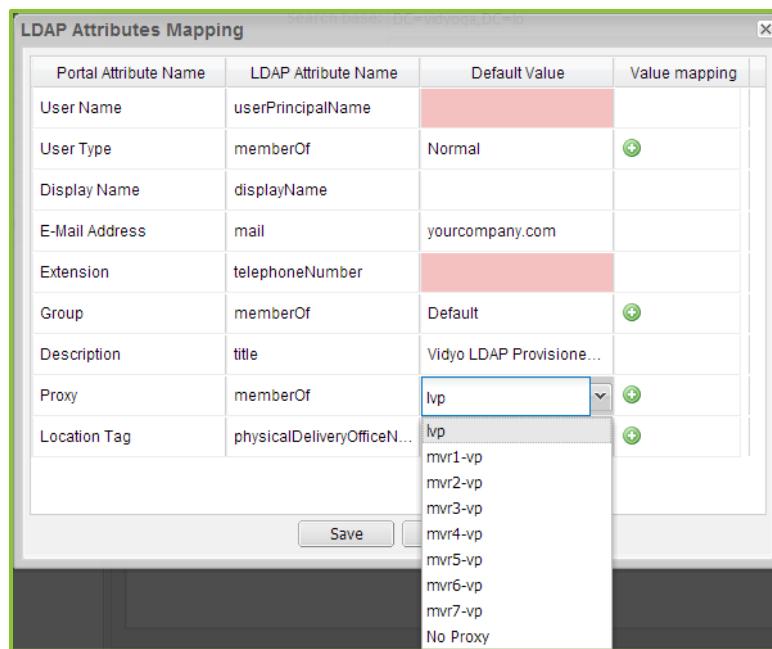
The following screenshot provides an example of a value mapping configuration where the **memberOf** LDAP Attribute Name is used.



For example, using the screenshot shown here, you can see that when a user is a member of the QA group and logs in to the User or Admin portal, the account is created with the QA Group.

- Description is the name of this specific LDAP attribute in the VidyoPortal.
 - In the LDAP Attribute Name, enter a value to map the Description in your LDAP schema.
You may choose to enter **title** as the LDAP Attribute Name.
 - The Default Value you enter here is used as the default User Type when the LDAP Attribute Name does not exist or returns an invalid attribute value or no Value mapping criteria is met.
You can select from Admin, Operator, Normal, VidyoRoom, Executive, and VidyoPanorama options.
For more information, see “Users” on page [15](#).
 - The Default Value you enter here is used as the default Description when the LDAP Attribute Name does not exist or returns an invalid attribute value or no Value mapping criteria is met.
 - No Value mapping configurations are made for the Description.
- Proxy is the name of this specific LDAP attribute in the VidyoPortal.
 - In the LDAP Attribute Name, enter a value to map to the Group in your LDAP schema.
Many users choose to enter **memberOf** as the LDAP Attribute Name. The **memberOf** value returns a list of groups of which the particular user is a member. This list is then used for Value mapping selection criteria.
 - The Default Value you enter here is used as the default Proxy when the LDAP Attribute Name does not exist or returns an invalid attribute value or no Value mapping criteria is met.

The VidyoPortal tenant used in this example has Proxies configured as lvp, mvr1-vp, mvr2-vp, mvr3-vp, mvr4-vp, mvr5-vp, mvr6-vp, and mvr7-vp, from which you can select. Map these groups using the Attribute Value Mapping dialog box.



- The Value mapping is used to make specific associations between exact Portal Attribute Values and LDAP Attribute Values based on the LDAP Attribute Name selected for your User Type.

Different users return different LDAP Attribute Values. The Attribute Values Mapping dialog box allows you to map specific associations for all possible values returned.

You can use the Duplicate and Remove buttons to create or delete rows in the Attribute Values Mapping dialog box.

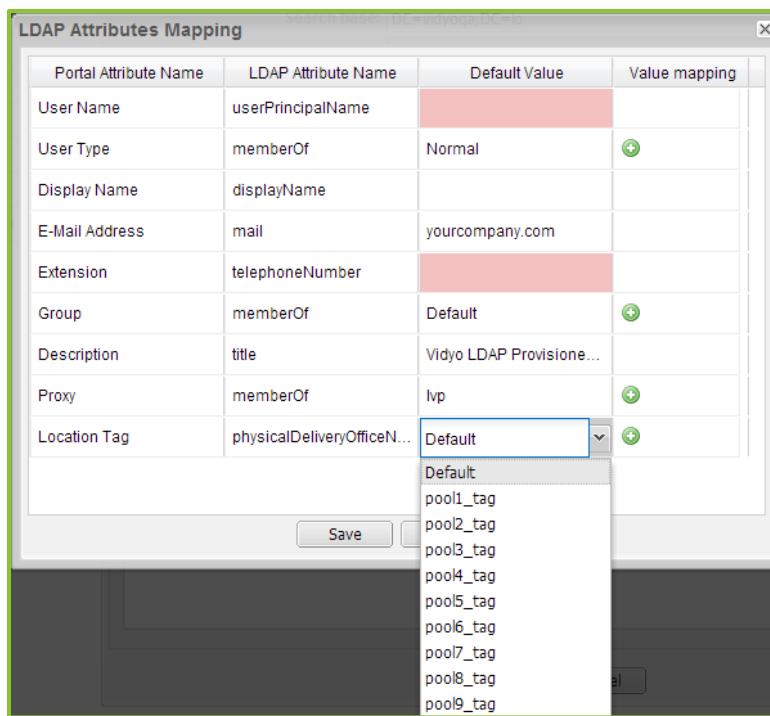
The following screenshot provides an example of a Value mapping configuration where the **memberOf** LDAP Attribute Name is used.

Attribute Values Mapping	
Portal Attribute Value	LDAP Attribute Value
lvp	
mvr1-vp	cn=vidyo-location1,ou=vidyo...
mvr2-vp	cn=vidyo-location2,ou=vidyo...
mvr3-vp	cn=vidyo-location3,ou=vidyo...
mvr4-vp	cn=vidyo-location4,ou=vidyo...
mvr5-vp	cn=vidyo-location5,ou=vidyo...

For example, using the screenshot shown here, you can see that when a user is a member of the **vidyo-location1** VidyoProxy and logs in to the User or Admin portal, the account is created with the **mvr1-vp** VidyoProxy.

- Location Tag is the name of this specific LDAP attribute in the VidyoPortal.
 - In the LDAP Attribute Name, enter a value to map to the Location Tag in your LDAP schema. Many users choose to enter **physicalDeliveryOfficeName** as the LDAP Attribute Name. The **physicalDeliveryOfficeName** attribute returns the user's office location. This value is then used for Value mapping selection criteria.
 - The Default Value you enter here is used as the default Location Tag when the LDAP Attribute Name does not exist or returns an invalid attribute value or no Value mapping criteria is met.

The VidyoPortal tenant used in this example has Location Tags configured as Default, pool1_tag, pool2_tag, pool3_tag, pool4_tag, pool5_tag, pool6_tag, pool7_tag, pool8_tag, and pool9_tag values, from which you can select.

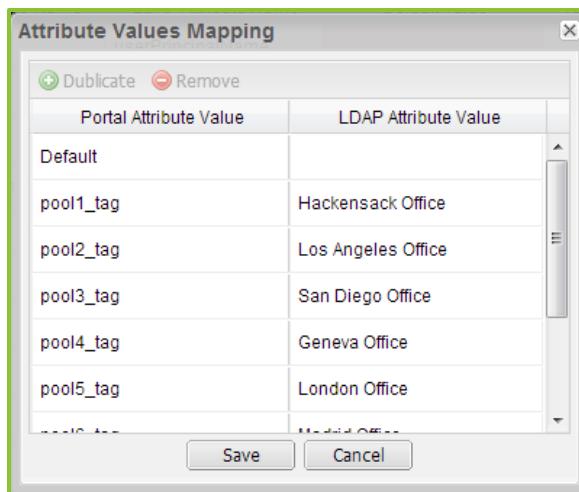


- The Value mapping is used to make specific associations between exact Portal Attribute Values and LDAP Attribute Values based on the LDAP Attribute Name selected for your User Type.

Different users return different LDAP Attribute Values. The Attribute Values Mapping dialog box allows you to map specific associations for all possible values returned.

You can use the Duplicate and Remove buttons to create or delete rows in the Attribute Values Mapping dialog box.

The following screenshot provides an example of a Value mapping configuration where the `physicalDeliveryOfficeName` LDAP Attribute Name is used.



The dialog box has a title bar 'Attribute Values Mapping'. Below it is a toolbar with 'Duplicate' and 'Remove' buttons. A table lists the mappings:

Portal Attribute Value	LDAP Attribute Value
Default	
pool1_tag	Hackensack Office
pool2_tag	Los Angeles Office
pool3_tag	San Diego Office
pool4_tag	Geneva Office
pool5_tag	London Office

At the bottom are 'Save' and 'Cancel' buttons.

For example, using the screenshot shown here, you can see that when a user is a member of the **Hackensack Office** group and logs in to the User or Admin portal, the account is created with the **pool1_tag** Location Tag.

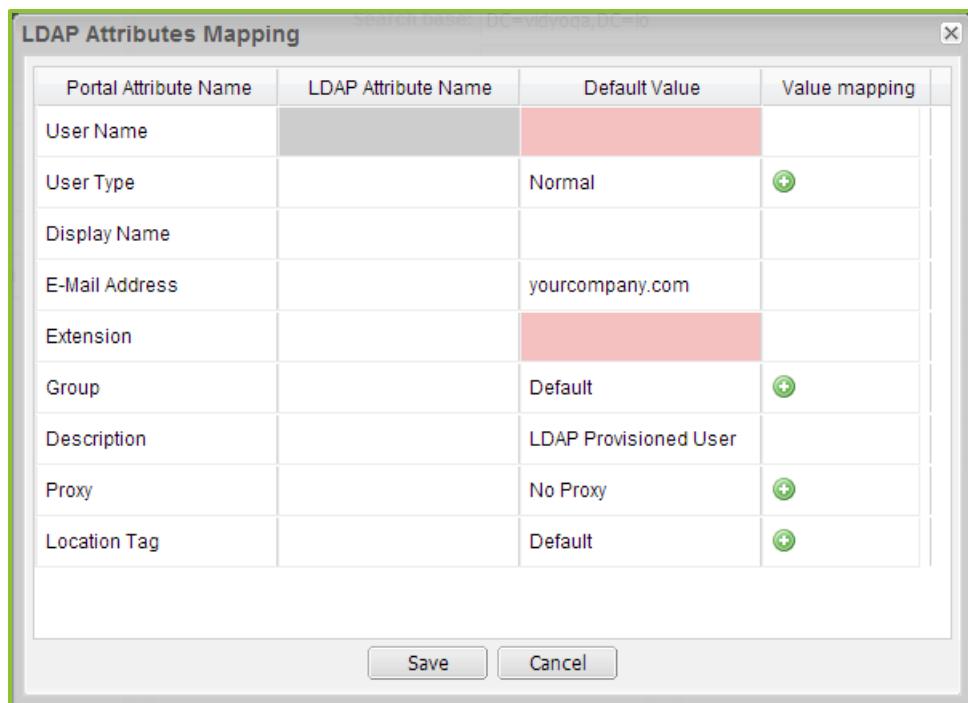
Configuring LDAP Authentication with Auto-Provisioning

Before configuring LDAP Authentication with auto-provisioning, it is highly recommended that you first decide which LDAP attributes you want to map to your VidyoPortal user account attributes. These mapping decisions become your LDAP auto-provisioning scheme during the Edit Attributes Mapping step in the following procedure. For more information, see “Understanding LDAP Authentication with Auto-Provisioning” on page [252](#) and “Explaining the VidyoPortal User Account Attributes” on page [253](#).

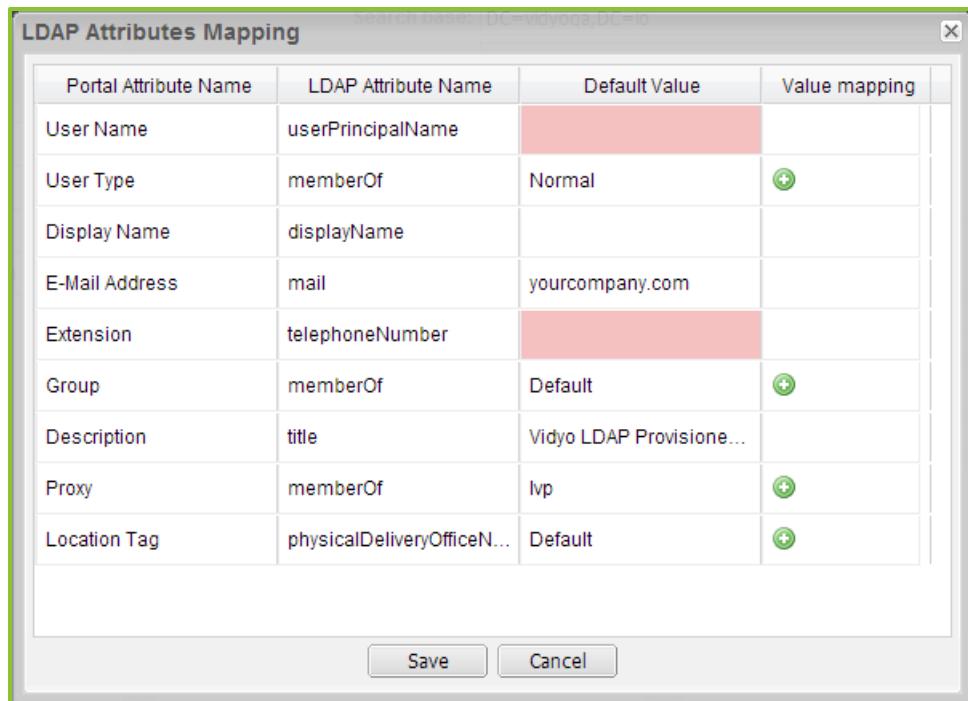
To configure LDAP authentication with auto-provisioning:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Authentication** on the left menu.
4. Configure your VidyoPortal to user your LDAP server.
For more information, see “Configuring Your VidyoPortal to Use Your LDAP Server” on page [248](#).
5. Select **LDAP Attributes Mapping**.
The Edit Attributes Mapping and Test Attributes Mapping buttons appear.
6. Click **Edit Attributes Mapping**.

The LDAP Attributes Mapping dialog box appears.



An example of the LDAP Attributes Mapping dialog box with data looks like the following:



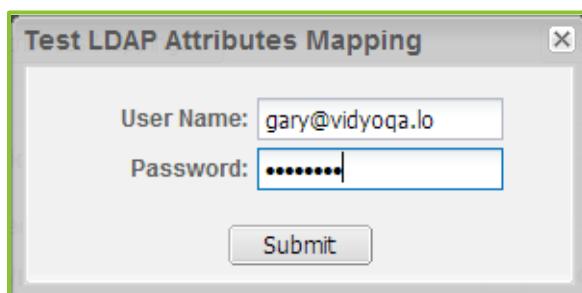
Note: You should spend some time analyzing your VidyoPortal user account attributes in order to decide which LDAP attributes you want to associate with them before you actually making the configurations on the LDAP Attributes Mapping dialog box. For more information, see “Understanding

“LDAP Authentication with Auto-Provisioning” on page 252 and “Explaining the VidyoPortal User Account Attributes” on page 253.

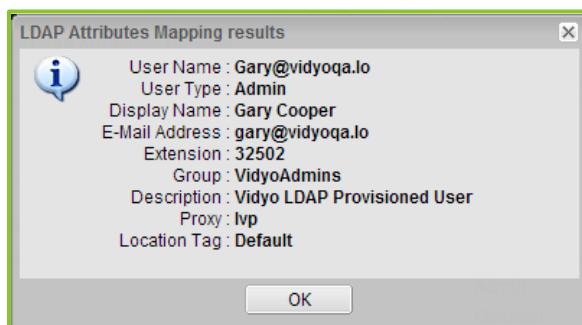
Each row on the LDAP Attributes Mapping dialog box represents an attribute. For each attribute, there is an associated Portal Attribute Name, LDAP Attribute Name, Value mapping (where applicable), and Default Value. These configurations become the rules telling the system what values to populate in specific user account fields when the new account is created.

7. Only after configuring your LDAP Attributes Mapping, click **Test Attributes Mapping** and provide the user account credentials for the account you wish to test as follows:

- a. Type the User Name for the account you wish to test.
- b. Type the Password for the account you wish to test.
- c. Click **Submit**.



If successful, the LDAP Attributes Mapping results dialog box is shown for the account you wish to test.



8. Apply authentication to specific user types.

For more information see “Applying Authentication (LDAP or Web Service) to Specific User Types” on page 264.

Configuring Authentication Using Web Services

Using Web Service Authentication requires an enabled Vidyo API license.

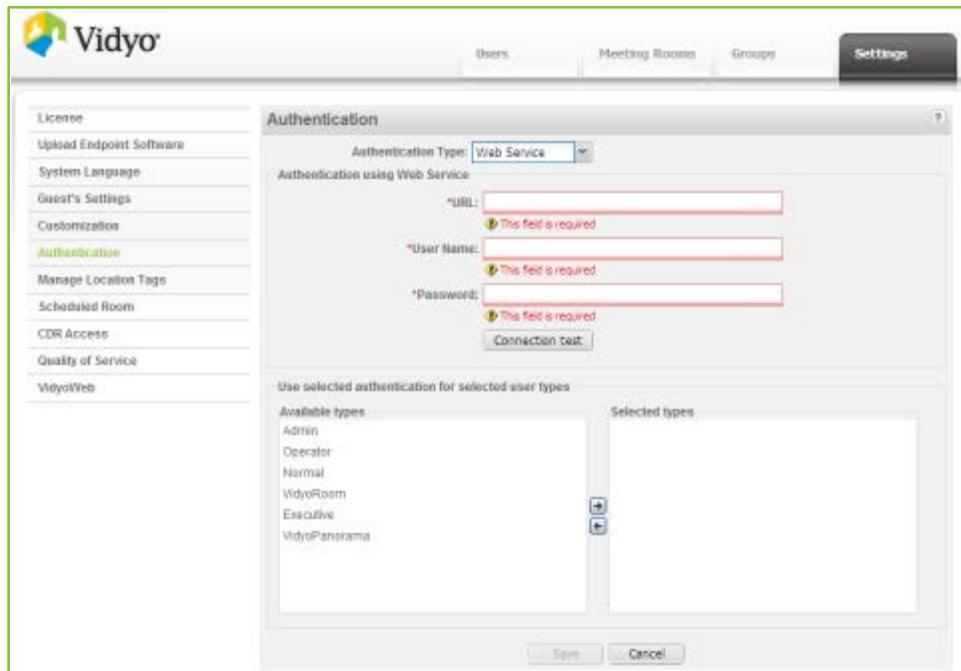
To configure Web Service Authentication:

Note: The Authentication page only allows you to configure Web Service Authentication if you have the API license enabled.

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Settings** tab.
3. Click **Authentication** on the left menu.
4. Configure your VidyoPortal to user your LDAP server.
For more information, see “Configuring Your VidyoPortal to Use Your LDAP Server” on page [248](#).
5. Select **Web Service** from the Authentication Type drop-down.



6. In the URL field, enter the URL of your authentication server.
7. Enter the user name and password for your web service.
8. Click **Connection test**.

If your connection test fails:

- Verify that the user name and password are correct.
- Verify the connection to your Web Service.

Normal users cannot log in to the VidyoPortal until Web Service connectivity is restored. For security reasons, there is no fallback to the VidyoPortal database.

Note: A successful connection test is required to enable the Save button on the lower part of the screen.

9. Apply authentication to specific user types using the following section.
10. Click **Save**.

Applying Authentication (LDAP or Web Service) to Specific User Types

The lower portion of the Authentication screen allows you to apply the authentication you configured (LDAP or Web Service) to specific user types.

To apply the configured authentication (LDAP or Web Service) to specific user types:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Authentication** on the left menu.
4. Configure your VidyoPortal to use your LDAP server.
For more information, see “Configuring Your VidyoPortal to Use Your LDAP Server” on page [248](#).
5. Configure authentication on your tenants using your desired method: LDAP Authentication with Manual User Creation, LDAP Authentication with Auto-Provisioning, or Web Services.
For more information see “Configuring LDAP Authentication with Manual User Creation” on page [248](#), “Configuring LDAP Authentication with Auto-Provisioning” on page [261](#), or “Configuring Web Service Authentication” on page [263](#).
6. From the Available types list, select one or more user types to validate by LDAP.
7. Click the **Right Arrow** button to transfer your selection or selections to the Selected types list.
8. Click **Save**.
9. Verify the selected user types are configured with the authentication you selected (LDAP or Web Service) by logging in to your User portal.

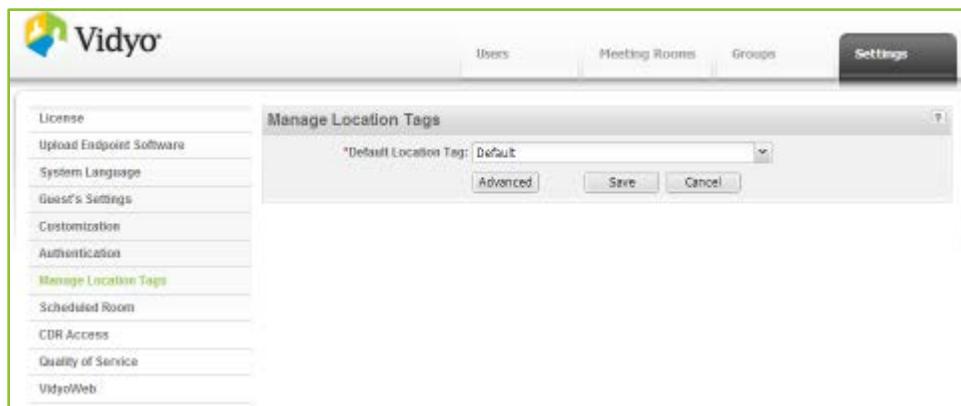
MANAGING LOCATION TAGS

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. Location tags are a feature of the VidyoCloud architecture. For more information, see “Configuring VidyoCloud” on page [145](#).

To manage location tags:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.

- Click **Manage Location Tags** from the left menu.

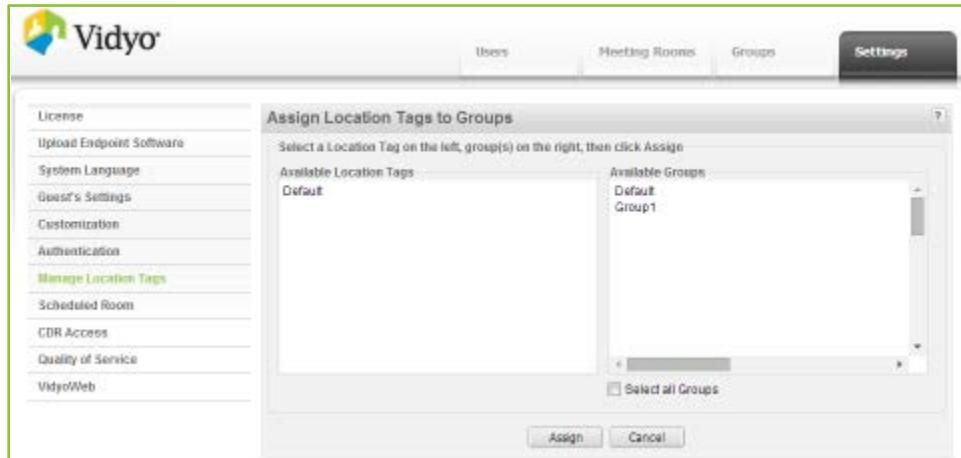


- In the Default Location Tag field, select the location tag that will be used by default on the Add User page.

For more information about the Location Tag field on the Add User page, see “Adding a New User” on page [204](#).

- Click **Advanced**.

The Assign Location Tags to Groups table opens which allows you to assign a location tag to existing users of selected groups.



- Select a location tag from the Available Location Tags list and then select the group you want to assign it to from the Available Groups list (or select all the Groups by selecting the **Select all Groups** check box).
- Click **Assign**.

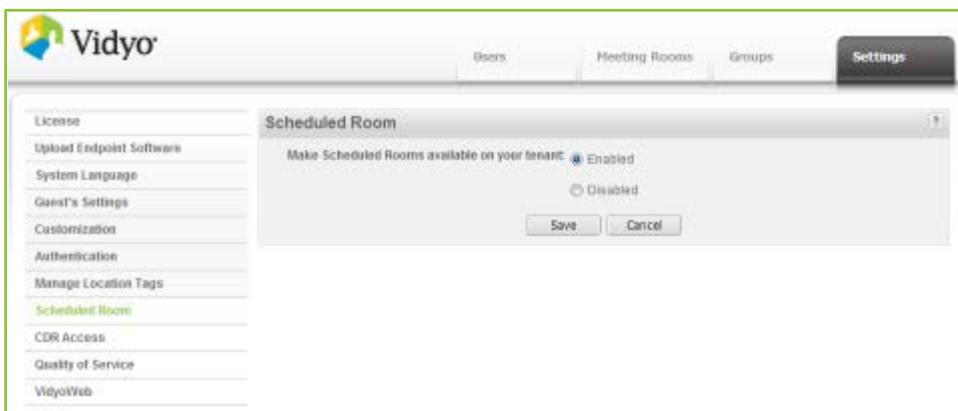
All existing users within the selected Group or Groups will now have this location tag assigned to them.

DISABLING SCHEDULED ROOMS ON YOUR TENANT

Scheduled rooms allow your users to create ad-hoc rooms from specific endpoints on your system. Scheduled rooms are enabled on your tenant by default and can be disabled, if necessary.

To disable scheduled rooms on your tenant:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **Scheduled Room** on the left menu.



4. Select **Enabled**.
5. Click **Save**.

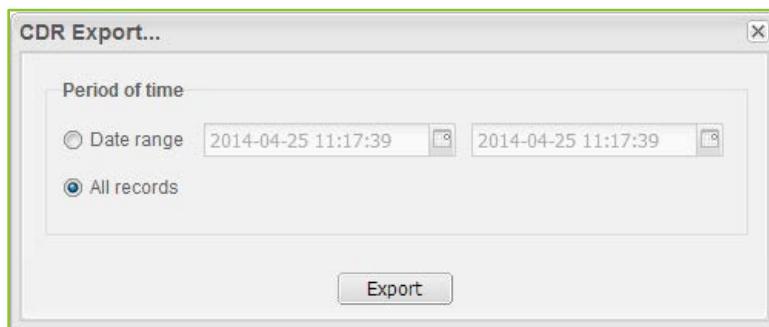
EXPORTING CDR FILES FROM THE ADMIN PORTAL

You can export specific CDR records from your VidyoPortal as necessary.

To export CDR records from the Admin Portal:

1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.
3. Click **CDR Access** on the left menu.
4. Click **CDR Export**.

5. In the CDR Export dialog box, specify a date range or all records for your CDR record Export.



6. Click **Export**.

Note:

- The export record limit is 65,000 records. If the export contains more than 65,000 records, a message appears warning you to restrict the range before proceeding with the download.
- The export data provided match the fields and descriptions explained in the ConferenceCall2 table on page [338](#).

CONFIGURING INTER-PORTAL COMMUNICATION (IPC) ON YOUR TENANT

Inter-Portal Communication (IPC) allows users to join VidyoConferences with someone on a different VidyoPortal. IPC also supports conferencing between tenants on the same VidyoPortal.

If the IPC function is shown on the left menu, your System Administrator is allowing you to control which Domains and Addresses are Allowed or Blocked on your tenant. You create a list of either Allowed or Blocked Domains and Addresses. The lists work in the following manner:

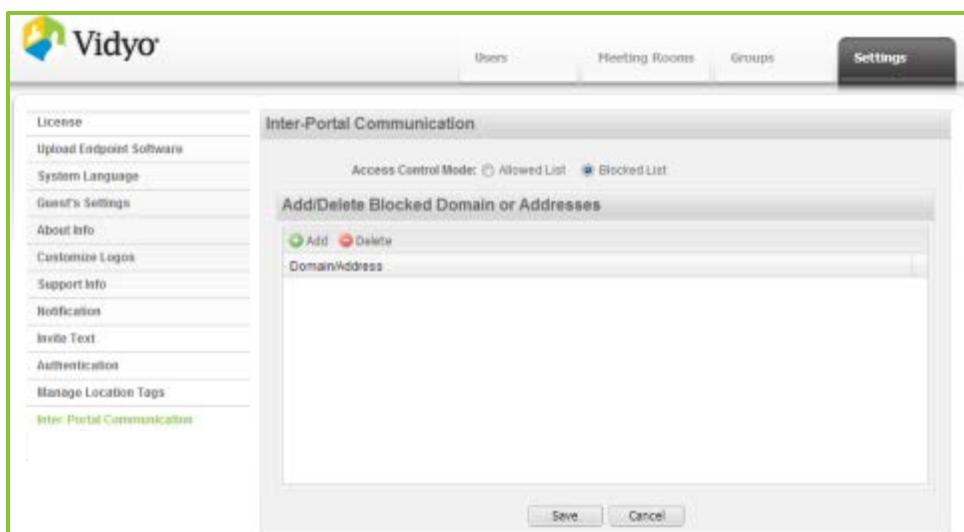
- An Allowed List only permits domains and addresses included on your list to interoperate on your domain. This type of list is often referred to as a whitelist.
- A Blocked List specifically disallows all domains and addresses included on your list from interoperating on your domain. This type of list is often referred to as a blacklist.

Note: The Inter-Portal Communication (IPC) function does not appear on the left menu if your Super Admin has decided they want system-wide IPC control over all tenants.

To configure tenant-level IPC:

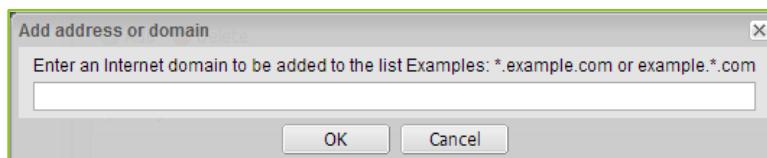
1. Log in to the Admin portal using your Admin account.
For more information, see “Logging in as a Tenant Admin” on page [201](#).
2. Click the **Settings** tab.

3. Click **Inter-Portal Communication** on the left menu.



4. Decide whether to create an Allowed List (whitelist) or a Blocked List (blacklist):
 - An Allowed List only permits domains and addresses included on your list to interoperate on your domain. This type of list is often referred to as a whitelist.
 - A Blocked List specifically disallows all domains and addresses included on your list from interoperating on your domain. This type of list is often referred to as a blacklist.
5. Click **Add** to add domains or addresses to your list.

The Add address or domain dialog box appears.



6. Enter the URL or domain name you want to add to the list and click **OK**.
7. Repeat steps 6 and 7 to add as many domains or addresses to your list as desired.
8. Click **Save** to save your list.

For more information, see “Telling Your Users About IPC” on page [112](#).

Note: You can add or delete Domains and Addresses at any time.

CONFIGURING QUALITY OF SERVICE (QOS) ON YOUR TENANT

This page allows you to set differentiated services code point (DSCP) values for audio, video, content, and signaling coming from your VidyoDesktop and VidyoRoom endpoints to your VidyoRouter. Audio, video, content data, and signaling coming from your VidyoDesktop and VidyoRoom endpoints is assigned corresponding values you set on this screen.

With these specified values assigned to media types coming from your VidyoDesktop and VidyoRoom endpoints, you can then configure your network router or switch to prioritize the packets as desired.

Note: For VidyoDesktop, QoS tagging is currently only supported on Windows platforms. The following operating systems restrict QoS value tagging in the following manner:

- **Windows 7**

- When VidyoDesktop is running as a standard user (not Administrative), the only DSCP values that may be tagged are 0, 8, 40, and 56.
- When VidyoDesktop is running as a user with Administrative permissions, all DSCP values (0 – 63) may be tagged.

- **Windows Vista**

- When VidyoDesktop is running as either a standard user or a user with Administrative permissions, the only DSCP values that may be tagged are 0, 8, 40, and 56.

- **Windows XP**

- When VidyoDesktop is running as a standard user or a user with Administrative permissions, no DSCP values may be tagged. The default value = 0 is the only value that may be used.
- When the `HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > TcpIp > Parameters > DisableUserTOSSetting` key is added to your system registry and you restart your machine, all DSCP values may be tagged. This registry key value is not set by default in Windows XP.

To configure quality of service values for endpoints on your tenant:

1. Log in to the Admin Portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page [201](#).

2. Click the **Settings** tab.

3. Click **Quality of Service** on the left menu.

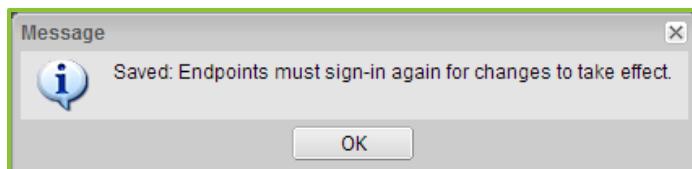


4. Enter DSCP values for Audio, Video, Content, and Signaling.

Values provided must be decimals from 0 to 63. The values default to 0.

5. Click **Save.**

All endpoints using your tenant must sign in to the system again before values are tagged to corresponding media packets based on your saved changes.



CONFIGURING VIDYOWEB ON YOUR TENANT

The VidyoWeb function does not appear on the left menu if your Super Admin has decided to make it unavailable. For more information, see “Enabling VidyoWeb Access” on page 105. Provided your Super Admin has made VidyoWeb available on your tenant, you can then decide to enable or disable it for your users.

The VidyoWeb browser plug-in makes it easy for guest participants to join conferences from within a web browser on desktop and laptop computers. VidyoWeb is designed especially for guest participants who simply want an easy way to join a conference.

You don’t pay extra for VidyoWeb. It’s built into your VidyoPortal. However, when a new user connects to your VidyoPortal via VidyoWeb for the first time, one of your licenses is consumed.

Note: User licenses apply to either VidyoWeb or VidyoDesktop, but not both at the same time. Therefore, when using VidyoWeb, be sure to close VidyoDesktop if it’s open.

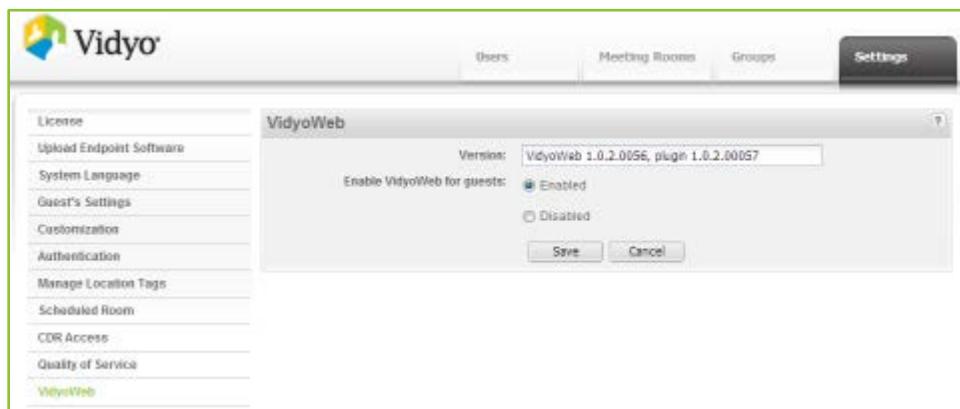
To enable or disable VidyoWeb on your tenant:

1. Log in to the Admin portal using your Admin account.

For more information, see “Logging in as a Tenant Admin” on page 201.

2. Click the **Settings** tab.

3. Click **VidyoWeb** on the left menu.



Note: The Version field displays the current version of the VidyoWeb plugin.

4. Select Enabled or Disabled to grant or deny VidyoWeb use on your tenant.
5. Click **Save**.

14. Auditing

Auditing for administrative functions is enabled on these components:

- VidyoPortal (.csv format)
- VidyoManager (plain text format in a .tar.gz file)
- VidyoRouter (plain text format in a .tar.gz file)
- VidyoGateway (plain text format in a .tar.gz file)

The sections below describe how to download the Audit logs for each component.

For information about using a separate syslog server, see “Enabling Remote Syslog” on page [85](#).

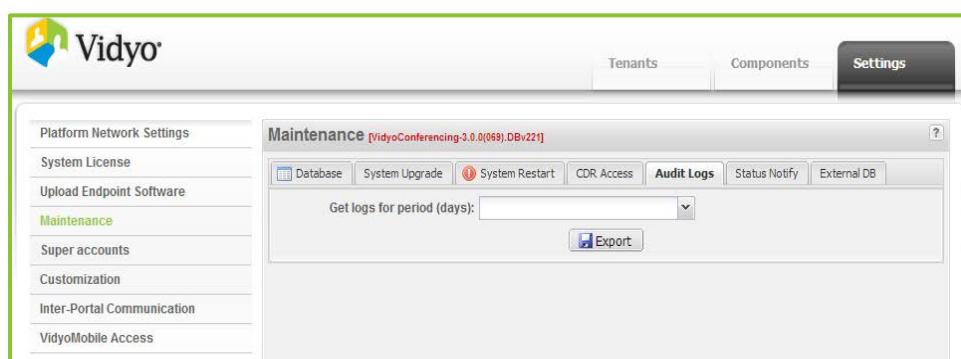
DOWNLOADING AUDIT LOGS FROM YOUR VIDYOPORTAL

Note: VidyoPortal audit logs can be generated using either the System Console or Audit user accounts. The following procedure shows the steps from an Audit user account. The steps are similar enough for the System Console account as well.

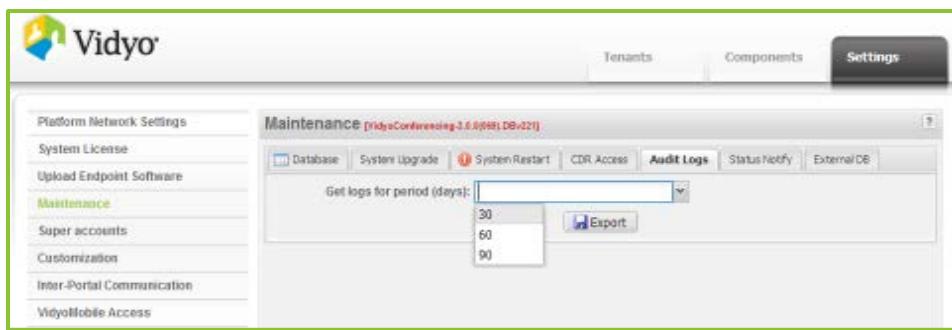
The Super Admin can create Audit user accounts on the default tenant. Audit accounts only have access to Audit logs.

To download audit logs from your VidyoPortal:

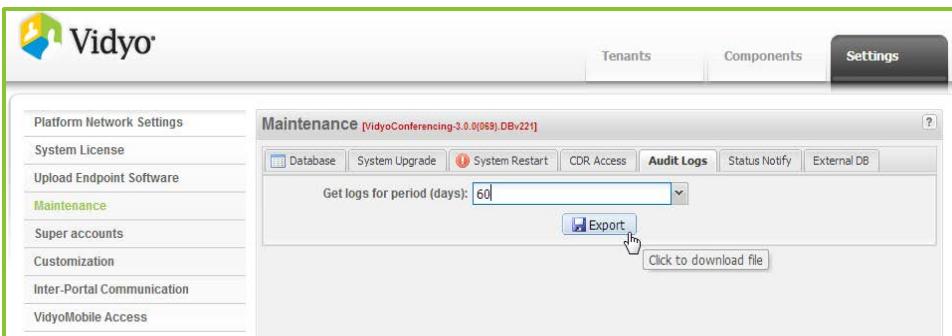
1. Log in to the Super Admin portal using your Super Admin account on your Active VidyoPortal.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click **Settings**.
3. Click **Maintenance** on the left menu.
4. Click the **Audit Logs** tab.



- From the drop-down menu, select either 30, 60 or 90 (days of records).



- Click the **Export** button to download the Audit logs.



- Save the file on your PC.

DOWNLOADING AUDIT LOGS FROM YOUR VIDYOMANAGER

To download audit logs from your VidyoManager:

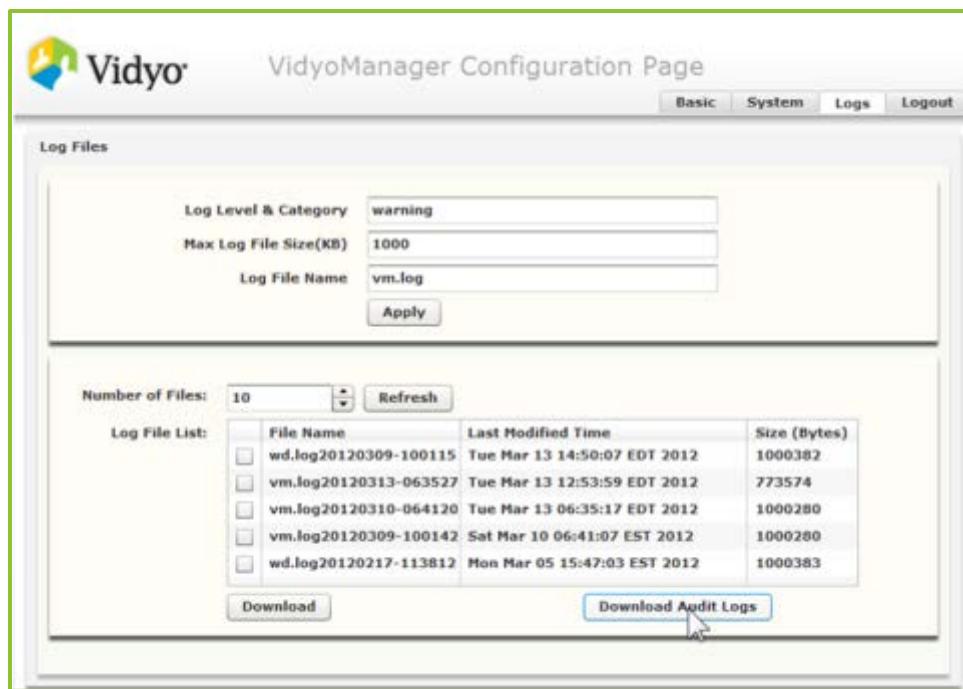
- Log in to your VidyoManager Configuration Page using your System Console account.

Note:

- The URL of your VidyoManager is your VidyoPortal domain name: <http://<FQDN or IP>/vm2conf/>. You can also click the VidyoManager IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

- The Settings tab appears by default.
- The Maintenance left menu item appears by default.

- Click the **Logs** tab.



- Click the **Download Audit Logs** button to download the file.

Note: The Download Audit Logs button downloads the single application logs file for auditing purposes, whereas the Download button is used to download specific user activity log files.

DOWNLOADING AUDIT LOGS FROM YOUR VIDYOROUTER

To download the Audit logs from your VidyoRouter:

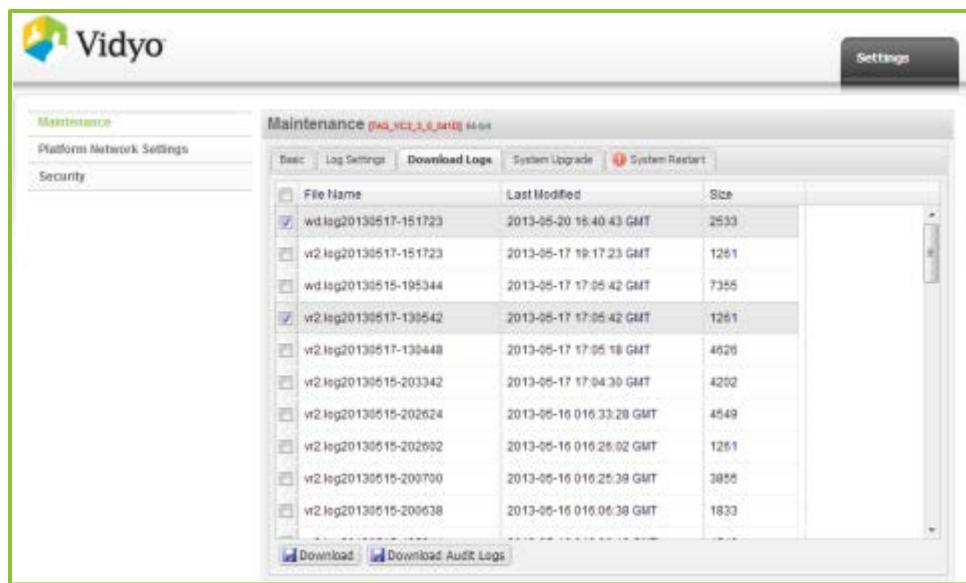
- Log in to your VidyoRouter Configuration Page using your System Console account.

Note:

- The URL of your VidyoRouter is typically a domain name: <http://<FQDN or IP>/vr2conf/>. You can also click the VidyoManager IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page 23.
- Although the default username for this page is admin, only the Super Admin accesses these pages.

- The Settings tab appears by default.
- The Maintenance left menu item appears by default.

- Click the **Download Logs** tab.



- Select corresponding check boxes for the logs you want to download.
- Click the **Download Audit Logs** button to download the file.

Note: The Download Audit Logs button downloads the single application logs file for auditing purposes, whereas the Download button is used to download specific user activity log files.

DOWNLOADING AUDIT LOGS FROM YOUR VIDYOGATEWAY

To download audit logs from your VidyoGateway:

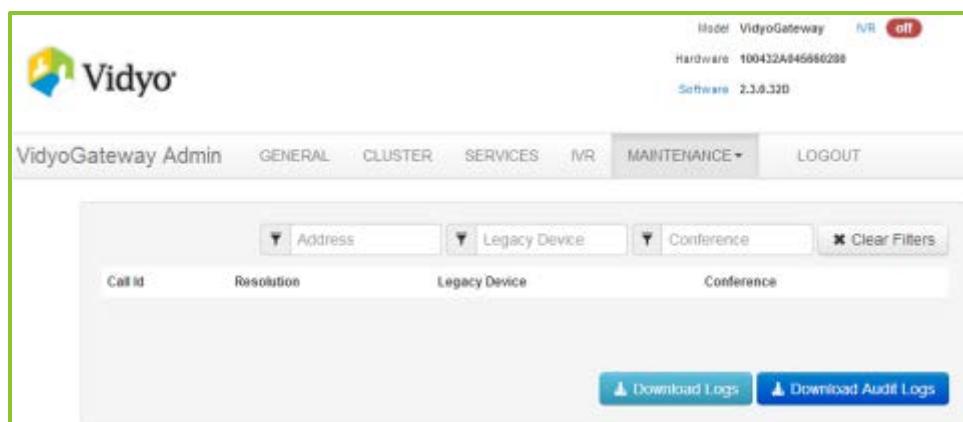
- Log in to your VidyoGateway using your System Console account.

Note:

- The URL of your VidyoGateway is typically a domain name: <http://<somevidyogateway.mil>>. You can also click the VidyoGateway IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page 23.

- Click the **Maintenance** tab.

3. Click Status.



4. Click the Download Audit Logs button to download the file.

Note: The Download Audit Logs button downloads the single application logs file for auditing purposes, whereas the Download button is used to download specific user activity log files.

AUDIT LOG CONTENT

Content Captured in the Audit Log

The following content is captured in the Audit log:

Super

- Login
 - Login Successful
 - Login unsuccessful
 - Logoff
- Tenants
 - Add Tenant
 - Modify Tenant
 - Delete Tenant
- Components
 - Component Updated
 - Component Enabled
 - Component Deleted
 - Component Disabled
 - Vidyo Cloud Activated
 - Gateway added
- Gateway modified
- Gateway deleted
- Settings
 - System License Updated
 - Software updated
 - Database Backup
 - Database Upload
 - Database Download
 - System Upgrade
 - System Restart
 - Ports Apply
 - Generate CSR
 - Upload CSR
 - Clear CSR
 - Certs Uploaded

Admin

- Login
 - Login Successful
 - Login Unsuccessful
 - Logoff
- Users
 - Add User
 - Delete User
 - Modify user
 - Add Legacy
- Meeting Rooms
 - Add Meeting Room
- Modify Meeting Room
- Delete Meeting Room
- Groups
 - Add Groups
 - Modify Groups
 - Delete Groups
- Settings
 - Upload Software
 - Authentication
 - LDAP Save

VidyoManager

- Login
 - Login Successful
 - Login Unsuccessful
 - Logoff
- Basic
 - Apply Config Server
- Restart
 - Restart
 - Shutdown

VidyoRouter

- Login
 - Login Successful
 - Login Unsuccessful
 - Logoff
- Basic
 - Apply Config Server
- Security
 - Ports Apply
 - Generate CSR
 - Upload CSR
 - Clear CSR
- Upload
 - Upload and Upgrade
 - Restart
 - Shutdown

VidyoGateway

- Login
 - Login Successful
 - Login Unsuccessful
 - Logoff
- Config
 - Save
 - Save and Apply
- Services
 - Add Service
 - Delete Service
 - Modify Service
- Upgrade Gateway
 - Upload and install
- Certificate
 - Upload
- Restart
 - Restart
 - Shutdown

Sample Audit Log Content

This is how an Audit log for the VidyoRouter, VidyoGateway, and VidyoManager in .txt format looks as viewed in a text editor after being decompressed. From left to right the data logged are: Timestamp, User ID, IP Address, and Description.

```
2011-09-13 10:46:43 | admin | 172.16.5.209 | New Session / Session is reset / Page refreshed / Logout
2011-09-13 10:46:51 | admin | 172.16.5.209 | Login with correct userid/password
2011-09-13 10:47:07 | admin | 172.16.5.209 | Downloaded audit history files
2011-09-13 10:48:06 | admin | 172.16.5.209 | Downloaded audit history files
```

The following illustration shows how a VidyoPortal Audit log in .csv format looks as viewed in a spreadsheet program. From left to right the data logged are: Action ID, User ID, Tenant Name, Action, Action Result, Timestamp, IP Address, and Action Description.

	A	B	C	D	E	F	G	H
1	144	admin	DOD	Login	FAILURE	18:10.0	172.16.2.219	Username=admin
2	145	super1	DOD	Login	FAILURE	18:31.0	172.16.2.219	Username=super1
3	146	admin1	DOD	Login	FAILURE	18:54.0	172.16.2.219	Username=admin1
4	147	super	DOD	Login	FAILURE	19:02.0	172.16.2.219	Username=super
5	148	superdod	DOD	Login	SUCCESS	37:23.0	172.16.2.146	Username=superdisa
6	149	superdod	DOD	Login	SUCCESS	37:57.0	172.16.2.146	Username=superdisa
7	150	superdod	DOD	Login	SUCCESS	40:13.0	172.16.5.209	Username=superdisa
8	151	superdod	DOD	Login	FAILURE	50:23.0	172.16.5.209	Username=disasuper
9	152	superdod	DOD	Login	SUCCESS	50:33.0	172.16.5.209	Username=superdisa

The following are lines taken from actual Syslog content.

```
<14>1 2013-06-05T14:51:02.389340-04:00 federalvp java - - - VidyoPortal [audit  
timestamp="Wed Jun 05 14:51:02 EDT 2013" result="SUCCESS" tenant="LOCAL" ac-  
tion="Login" params="Username=superuser1" user="superuser1" ip="192.168.0.100"]
```

```
<14>1 2013-06-05T14:51:28.397257-04:00 federalvp java - - - VidyoPortal [audit  
timestamp="Wed Jun 05 14:51:28 EDT 2013" result="SUCCESS" tenant="LOCAL" ac-  
tion="Delete Tenant" params="TenantID = 7;TenantName=TEST" user="superuser1"  
ip="192.168.0.100"]
```

Note: The format used for the Syslog content complies with RFC-5424 standards.

15. Configuring OCSP

The VidyoPortal, VidyoRouter, and VidyoGateway support Online Certificate Status Protocol (OCSP) verification. OCSP verification can be enabled on the following pages:

- VidyoPortal vm2conf
- VidyoPortal and VidyoRouter vr2conf
- VidyoPortal and VidyoRouter vp2conf
- VidyoPortal Super Admin
- VidyoPortal User portal (only supported in an environment with no VidyoRooms)
- VidyoPortal Tenant Admin
- VidyoGateway Admin

Before enabling OCSP, you must do the following:

- Ensure that the Apache version is 2.4.2 or later. Please contact Customer Support if the server has an earlier version.
- Ensure that HTTPS is configured and enabled.
- Ensure that a valid CA Root has been uploaded. All Certificate Authorities and Intermediates for the certificates presented must be present in the CA Root.
- Ensure that a valid Certificate Bundle has been uploaded.

Note: For a Certificate to be verified, its entire Certificate Authority Chain must be verifiable via the configured OCSP responder. If it is not, verification will fail even if the certificate is valid.

ENABLING AND CONFIGURING OCSP

OCSP must be enabled in the VidyoGateway, VidyoPortal, and VidyoRouter. Then, OCSP must be enabled for each application (VidyoGateway and VidyoRouter) on the VidyoPortal.

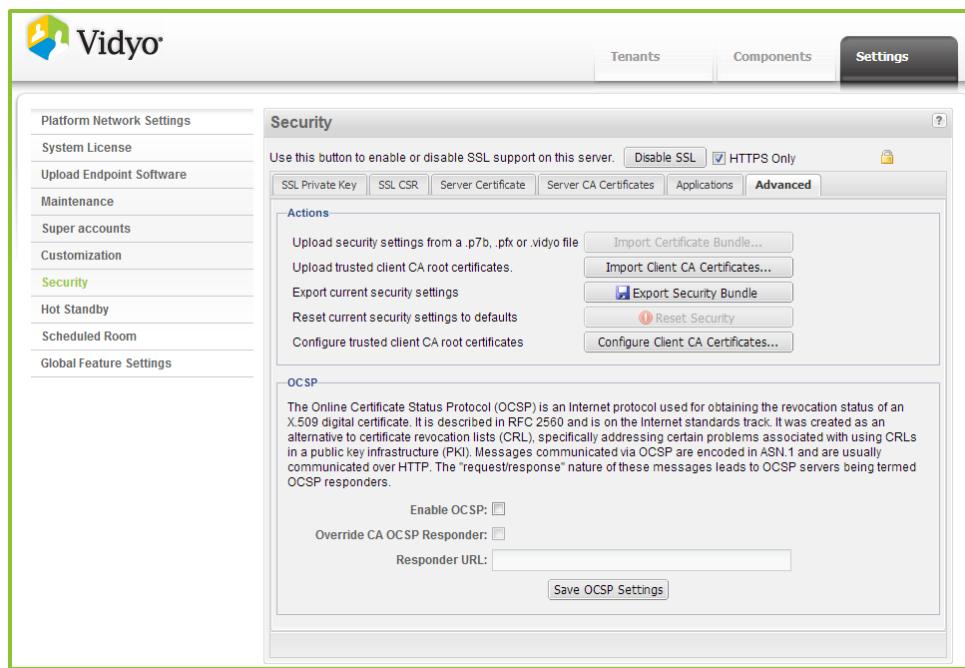
Enabling OCSP in the VidyoPortal and VidyoRouter and Configuring OCSP in the VidyoPortal

Enabling OCSP is done the same way for VidyoPortal and VidyoRouter. For the VidyoPortal, you must enable OCSP and then perform some additional configuration to enable OCSP for each application (VidyoGateway and VidyoRouter).

To enable OCSP in the VidyoPortal or VidyoRouter:

1. Log in to the Super Admin portal or your VidyoRouter.
2. Click the **Settings** tab.
3. Click **Security**.

4. Click the **Advanced** tab.



5. Select the **Enable OCSP** check box.
6. If you want to override the OCSP responders specified in the Client, Intermediate, and Root certificate, select the **Override CA OCSP Responder** check box and enter the **IP address or FQDN** of the new responder in the Responder URL.
7. Click **Save OCSP Settings**.

Note: The server must have access to the OCSP Responders specified in the certificates or the overridden Responder. Also, be sure that the configured DNS server can resolve the FQDNs of all the OCSP Responders.

To configure OCSP for your applications in the VidyoPortal:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page 35.
2. Click the **Settings** tab.
3. Click **Security** on the left menu.

4. Click the **Applications** tab.

The screenshot shows the Vidyo web interface with a green border around the main content area. At the top, there's a navigation bar with tabs: 'Tenants', 'Components', and 'Settings' (which is highlighted). Below the navigation is a sidebar with links like 'Platform Network Settings', 'System License', 'Upload Endpoint Software', 'Maintenance', 'Super accounts', 'Customization', 'Inter-Portal Communication', 'VidyoMobile Access', and 'Security' (which is also highlighted). The main content area is titled 'Security' and contains a sub-section for 'OCSP'. It has a table with columns: Applications, Network Interface, HTTP, HTTPS, and OCSP. There are five rows in the table:

Applications	Network Interface	HTTP	HTTPS	OCSP
super	PRODUCTION	80	443	<input type="checkbox"/>
vm2conf	MANAGEMENT	80	443	<input checked="" type="checkbox"/>
vr2conf	MANAGEMENT	80	443	<input checked="" type="checkbox"/>
admin	PRODUCTION	80	443	<input type="checkbox"/>
vg2conf	MANAGEMENT	80	443	<input checked="" type="checkbox"/>

At the bottom of the table are 'Reset' and 'Save' buttons.

5. Look in the Applications column for the application for which you want to enable OCSP, and then select the check box in the OCSP column for that application.

Note: OCSP should not be enabled for the User portal. If it is enabled, VidyoRooms will no longer function correctly.

6. Click **Save**.

Changes are applied immediately; therefore, if OCSP verification is required for the Super application, you will be immediately prompted for your client certificate.

Enabling OCSP in the VidyoGateway

To enable OCSP in the VidyoGateway:

1. Log in to the VidyoGateway.
2. Click **Maintenance > Security**.

3. Click the **Advanced** tab.

The screenshot shows the VidyoGateway Admin interface with the following details:

- Header:** Model: VidyoGateway, NVR: off, Hardware: 199432A048669260, Software: 2.3.0.320.
- Navigation:** VidyoGateway Admin, GENERAL, CLUSTER, SERVICES, NVR, MAINTENANCE (selected), LOGOUT.
- Sub-Header:** Private Key, CSR, Server Cert, Server CA Cert, Ports, Advanced (selected).
- Client CA Cert:**
 - Upload Client CA Cert: Choose File (No file chosen).
 - Action: append to existing (dropdown menu).
 - Buttons: Import CA Cert File.
- Security Bundle (.p7b / .pfx / .vidyo):**
 - Upload Bundle: Choose File (No file chosen).
 - Password (if any): [Input field].
 - Buttons: Import Bundle, Export All, Reset All.
- Online Certificate Status Protocol (OCSP) Configuration:**
 - Status: disabled (dropdown menu).
 - Override Responder: disabled (dropdown menu).
 - Default Responder: [Input field].
 - Buttons: Save.

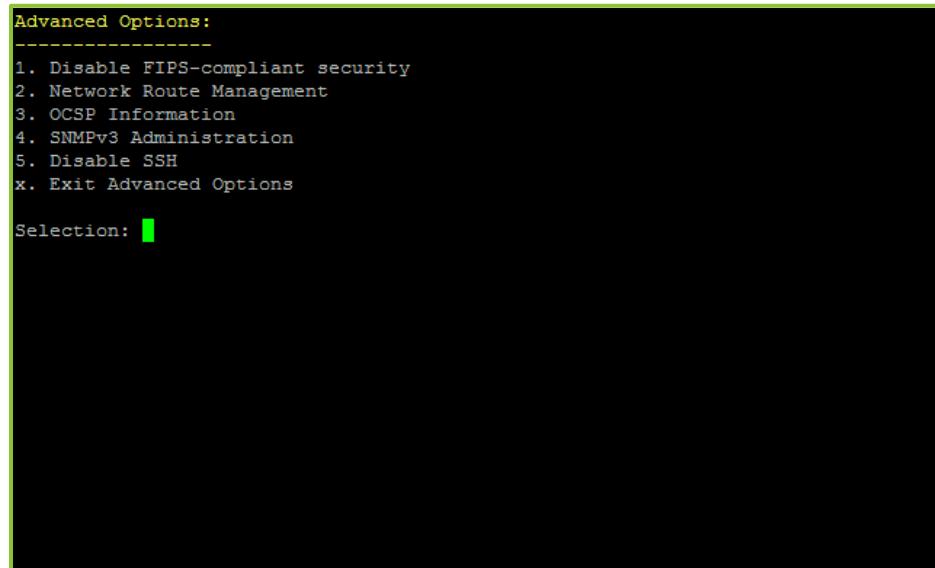
4. Select **disabled** on the Status drop-down.
5. If you want to override the OCSP responders specified in the Client, Intermediate, and Root certificate, select **enabled** on the Override Responder drop-down and enter the **IP address** or **FQDN** of the new responder in Default Responder.
6. Click **Save**.

For VidyoRouter and VidyoGateway, this will immediately require OCSP certificate verification for the vr2conf, vp2conf, and VidyoGateway Admin portal.

Note: The server must have access to the OCSP Responders specified in the certificates or the overridden Responder. Also, be sure that the configured DNS server can resolve the FQDNs of all the OCSP Responders.

Disabling OCSP from the System Console

Only when at least one application (VidyoGateway, VidyoPortal, or VidyoRouter) is enabled for OCSP are you then able to globally disable OCSP from the System Console. Otherwise, the menu option only shows “3. OCSP Information” allowing you to view configuration data.



To disable OCSP from the System Console:

Note: Only when at least one application (VidyoGateway, VidyoPortal, or VidyoRouter) is enabled for OCSP are you then able to globally disable OCSP from the System Console.

1. Log in to the System Console.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

2. Select **m. ... (more options)**.
3. Select **A. Advanced Options**.

4. Select 3. Disable OCSP.

```
OCSP Configuration
=====
SSLOCSPResponderTimeout 10
SSLOCSPEnable on
SSLOCSPOverrideResponder off

Do you want to disable OCSP (y/n) ? y

OCSP Authentication will now be disabled.

Confirm changes ? [y/n]
```

5. Select **y** to save the configuration.

Note: OCSP can be disabled using the System Console option **0** if it was not set up correctly.

Appendix A. Firewall and Network Address Translations (NAT) Deployments

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 is transparent 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 uses 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 and 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:

1. Place the VidyoPortal and VidyoRouter on a public Static IP address.
2. Place the VidyoPortal and VidyoRouter in a private network having a private Static IP address within the organization.
3. Place the VidyoPortal and VidyoRouter within the DMZ with a private Static IP address.

When deployed with a public IP address and no server side firewall or NAT, the VidyoPortal 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 most often permits any connection initiated 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 VidyoPortal and place calls, the client side connection must be open to the VidyoPortal on these TCP and UDP ports:

VidyoDesktop and VidyoRoom Connectivity to VidyoPortal and VidyoRouter		
TCP Port 80	HTTP – Outbound to VidyoPortal	Client to VidyoPortal authentication and GUI
TCP Port 443	TCP – Outbound to VidyoProxy (running on a VidyoRouter - optional)	Optional for TCP signaling and media proxy connections from endpoints
TCP Port 8443	HTTPS – Outbound to VidyoRouter (optional)	Optional for SSL connection to VidyoRouter configuration pages
TCP Port 443	HTTPS – Outbound to VidyoPortal (optional)	Optional for SSL connection to VidyoPortal
TCP Port 17992	EMCP – Outbound to VidyoPortal	Client connection to VidyoManager
TCP Port 17990	SCIP – Outbound to VidyoPortal/ VidyoRouter Note: If you are using a VidyoRouter, the VidyoPortal does not apply.	Client connection to VidyoRouter
UDP Ports 50,000 – 65,535	RTP, sRTP, RTCP – Bi-Directional to and from the 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

Note:

- Some Firewalls have a UDP default timeout. On the Cisco PIX Firewall, for example, if the UDP timeout is not changed, then the call drops in exactly two minutes and the Vidyo client or clients must reconnect.
- Many newer consumer home firewalls have SPI (Stateful Packet Inspection) active by default. This may need to be disabled for better performance.

- For VidyoConferencing clients, who are behind restricted firewalls where the ports above cannot be opened, Vidyo provides the VidyoProxy to address these users. For more information, see “VidyoProxy” on page [298](#).

Vidyo Server Requirements

To enable remote management access to the Vidyo servers, the following TCP and 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
TCP Port 2222	SSH – Inbound to Server	SSH access to the VidyoPortal and VidyoRouter

The following services outline the ports required for Vidyo Cloud cascading.

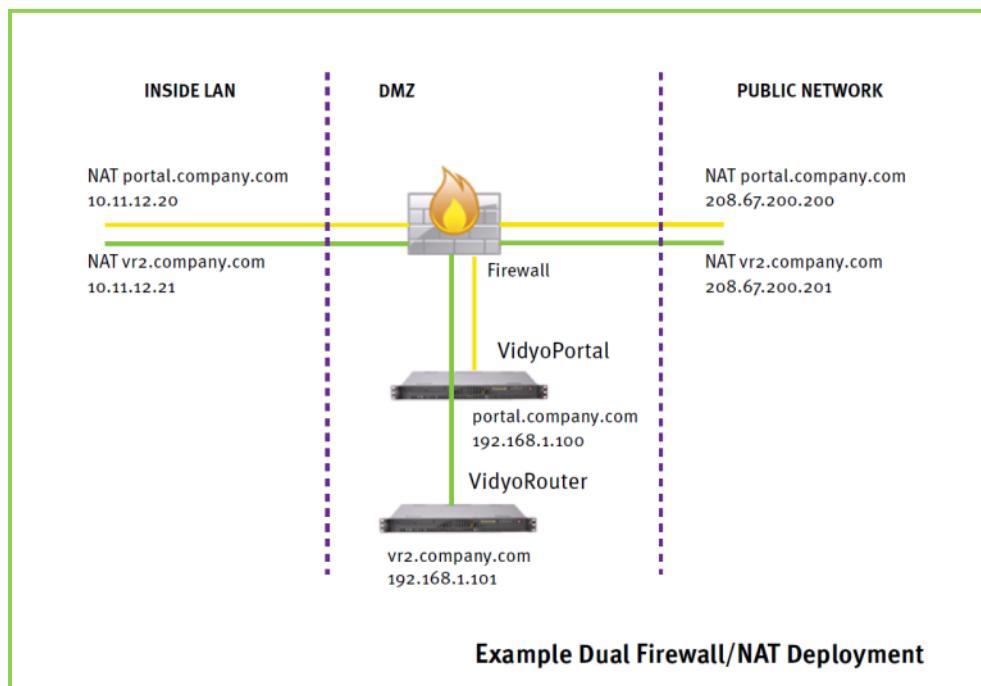
Vidyo Cloud Connectivity to VidyoPortal and VidyoRouter to VidyoRouter		
TCP Port 80	HTTP – Router to VidyoPortal	Client to VidyoPortal authentication and GUI
TCP Port 443	HTTPS – Router to VidyoPortal (optional)	Optional for SSL connection to VidyoPortal
TCP Port 17991	RMCP – Router to VidyoPortal	Router connection to VidyoManager
TCP Port 17990	SCIP – Bi-Directional to and from VidyoRouters	Signaling connections between VidyoRouters
UDP Ports 50,000 – 65,535	RTP, sRTP, RTCP – Bi-Directional to and from VidyoRouters	<ul style="list-style-type: none"> 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 and 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 and Active Directory.
TCP Port 636	LDAPS – Outbound from Server	Secure LDAP. Optional authentication to LDAP and Active Directory
UDP Port 161 – 162	SNMP – Inbound to Server	Basic SNMP functions
TCP and UDP 3478	STUN – Bi-directional to and from Server	Optional, only if using STUN for NAT traversal

CONFIGURING 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.



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 vary based on the Firewall NAT and DNS servers used. This appendix focuses on conceptual information.

Configuring the Firewall NAT

Allocate an external, public static IP address to use for the VidyoPortal and VidyoRouters 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 VidyoPortal 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 and VidyoPortal (configurable)
- Inbound TCP Port 17990 – SCIP protocol client connection to VidyoRouter (configurable)
- Bi-Directional UDP Port 50000 – 65535 – RTP and SRTP media, one RTP and 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 limit the duration of UDP port openings, and this may cause the calls to terminate prematurely.

Configuring DNS and FQDN

For the firewall NAT traversal to properly communicate between servers and clients through the IP address translations, DNS must be configured 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) must 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 yourportal.yourcompany.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.

Configuring the Vidyo Server

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.

This is done by selecting System Console menu option **2. Configure DNS Nameserver**. For more information, see “Configuring the Network Settings at the System Console” on page [25](#).

Note:

- When configuring your DNS Nameserver, set the server local hostname and domain name as well as the working DNS server address.
- It's very important to note that the IP address shown in the System Console (127.0.1.1) must remain intact for proper communications.

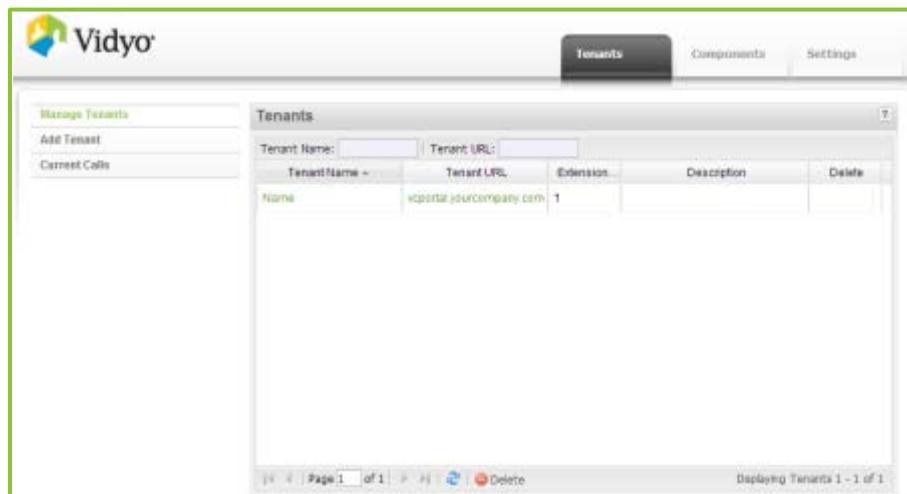
- In a firewalled installation, the VidyoManager and VidyoRouters need to be configured to use the server FQDN instead of the IP addresses.

Configuring Tenant URLs

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Tenants** tab.
3. Select **Manage Tenants**.



4. Ensure that each Tenant (including the Default Tenant) is using a FQDN for Tenant URL.

Configuring the VidyoManager

To configure the VidyoManager to be addressed by its FQDN:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.

3. Click **Manage Component** on the left menu.

The screenshot shows the Vidyo Management interface with the 'Components' tab selected. On the left, there's a sidebar with options like 'Manage Components', 'Manage VidyoCloud', 'Manage Gateways', 'Manage VidyoReplay Recorders', and 'Manage VidyoReplays'. The main area displays a table of components:

Status	Name	Type	IP	Config Version	Software Version	Alarm
DISABLED	VidyoProxy	VidyoProxy	192.168.1.100	1 / D	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	LocalVM	VidyoManager	192.168.1.100	9 / 9	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	DEFAULT_NF	VidyoRouter	192.168.1.105	3 / 3	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	VidyoGateway	VidyoGateway	192.168.1.110		2.2.0(283)	<input type="checkbox"/>
UP	VidyoRecord	VidyoReplayRmc	192.168.1.119		2.2.0(281)	<input type="checkbox"/>
NEW		VidyoProxy	192.168.1.103	D / D	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	VidyoReplay	VidyoReplay	192.168.1.115		2.2.0.281	<input type="checkbox"/>

At the bottom of the table are buttons for 'Delete', 'Enable', and 'Disable'.

4. Double-Click the **Status** of the VidyoManager entry.
5. 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 screenshot shows the configuration dialog for the 'Local VM' component. The 'General' tab is selected. The 'Listen Address (EMCP)' section contains the following fields:

ID:	2FUH2WPSWW3NS0HGNZIA762HJWIC1WQ8C2YC2R	
Name:	Local VM	
Listen Address (EMCP):	IP	Port
	server.yourcompany.com	17992

At the bottom right are 'Save' and 'Cancel' buttons.

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.

6. Edit the port according your needs and firewall rules.
7. Click **Save**.

Configuring Each of Your VidyoRouters

To configure each VidyoRouter to be addressed by its FQDN:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.
3. Click **Manage Components** on the left menu.

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	24 / 24	TAG_VC3_1_0_037	
UP	Local VM	VidyoManager	172.20.4.125	4 / 3	TAG_VC3_1_0_037	
UP	Local VP	VidyoProxy	172.20.4.125	10 / 0	TAG_VC3_1_0_037	
DOWN	vg484	VidyoGateway	172.16.4.84	3.0.0(96)		

4. Double-click the **Status** of the VidyoRouter entry.

ID:	[REDACTED]	
Name:	VidyoRouter VR1	
Listen Address (SCIP):	IP:	Port:
	.vidyo.com	17990

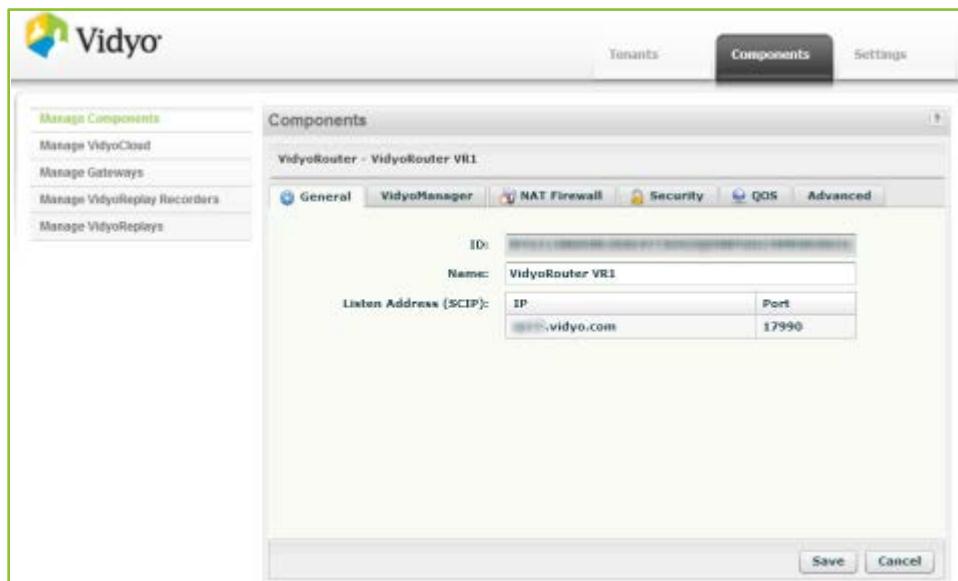
5. Under Listen Address (SCIP), edit the SCIP address. (VidyoRouter signaling address) by clicking the text in the IP column, and enter the server FQDN here, e.g., `yourrouter.yourcompany.com`.

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.

6. Edit the port according your needs and firewall rules.

Each VidyoRouter server requires a unique and separate FQDN to your VidyoPortal server. Use each server's unique FQDN for the SCIP address on each VidyoRouter configuration.

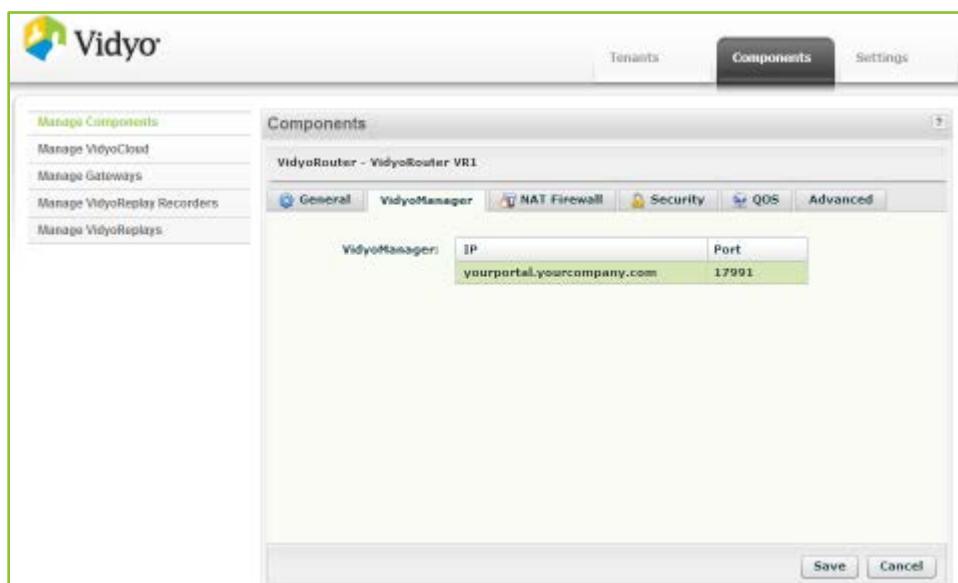
For example: vr1.company.com, vr2.company.com, etc.



To configure the VidyoRouter to address its VidyoManager by FQDN:

Now you must configure the VidyoRouter to address its corresponding VidyoManager by FQDN.

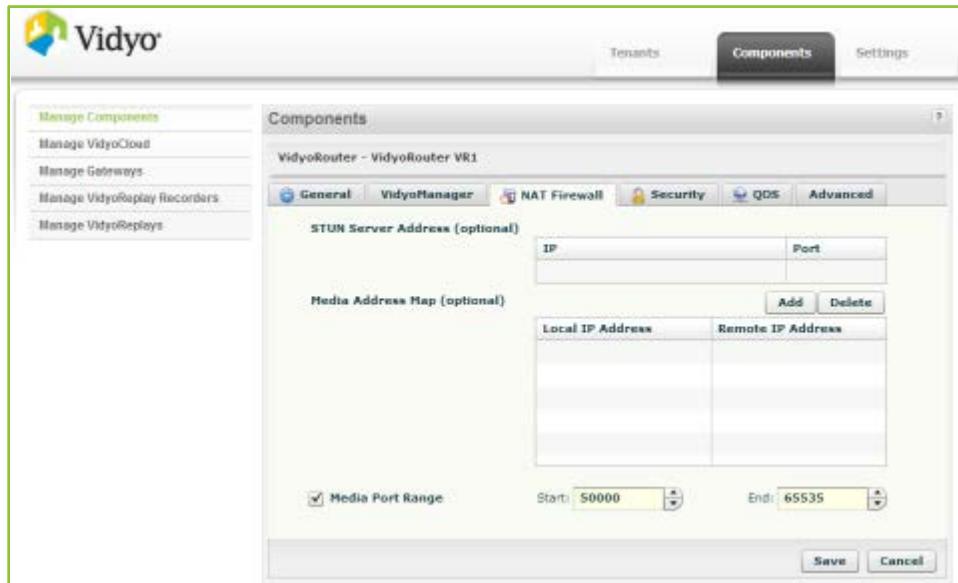
1. In the VidyoRouter Component pages, select the VidyoManager tab.



2. Under VidyoManagers, edit the IP address by clicking the text in the IP column, and enter the server FQDN here, e.g., yourportal.yourcompany.com.

Next, you'll need to configure the VidyoRouter Media Mapping from private to public addresses.

3. In the VidyoRouter Component pages, select the NAT Firewall tab.



4. Under Media Address Map, click **Add** and enter each NAT translation required.
5. For each NAT map, enter the Local IP Address (private) and Remote IP Address (public); the inside and outside NAT addresses needed.

If there is a NAT from the private LAN towards the DMZ, a corresponding media map rule is required.

6. Click **Save**.

In deployments where there is a dual NAT; meaning one NAT from the public network to the server, and one from the private LAN to the server, two Media Map statements are required.

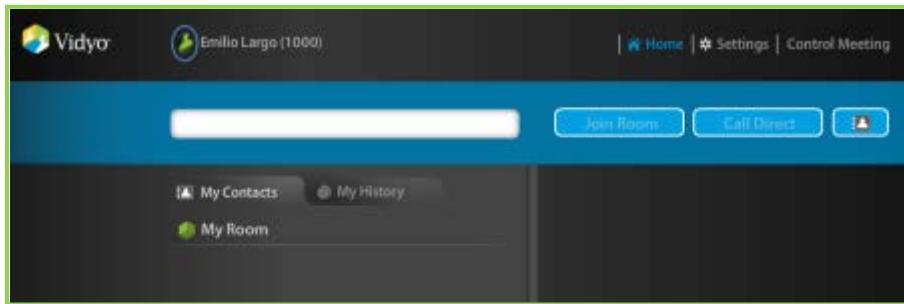
As an alternative method to Media Address Mapping, you can choose to use a public STUN server. To use a STUN server, enter the IP or URL and Port of the public STUN server you wish to use. The default STUN port is 3478. Vidyo hosts a public STUN server at: stunusa.vidyo.com. Using a STUN server instead 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 causes your system to malfunction.

Repeat these steps for each additional VidyoRouter in your VidyoConferencing system.

Testing Your Configuration

From both sides of the firewall NAT, you must attempt to log in to the VidyoPortal as a Normal user. If the EMCP is traversing properly, the person icon in the upper left of the User portal turns 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 you are successfully logged in to the VidyoPortal, 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 VidyoPortal 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.

Appendix B. VidyoProxy

VIDYOPROXY SOLUTION FOR TRAVERSAL OF RESTRICTED NETWORKS

Overcoming Deployment Barriers Securely and Effectively

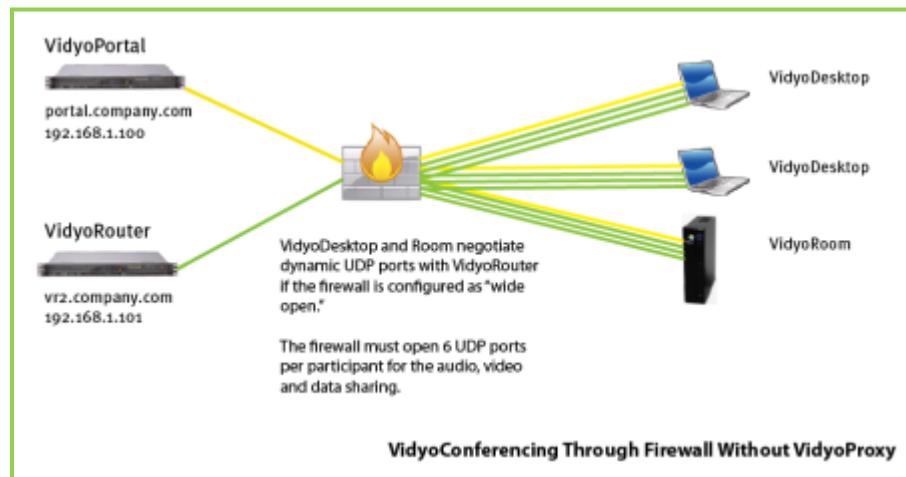
Utilizing the Internet to gain cost efficiencies is a significant advantage of the VidyoConferencing solution. Traversing company firewalls, NATs and web proxies can pose a challenge, particularly if you don't have control over the firewall, or your company policy prevents you from opening the necessary ports for VidyoConferencing signaling and traffic. The VidyoProxy solution was developed to address this challenge, securely and effectively.

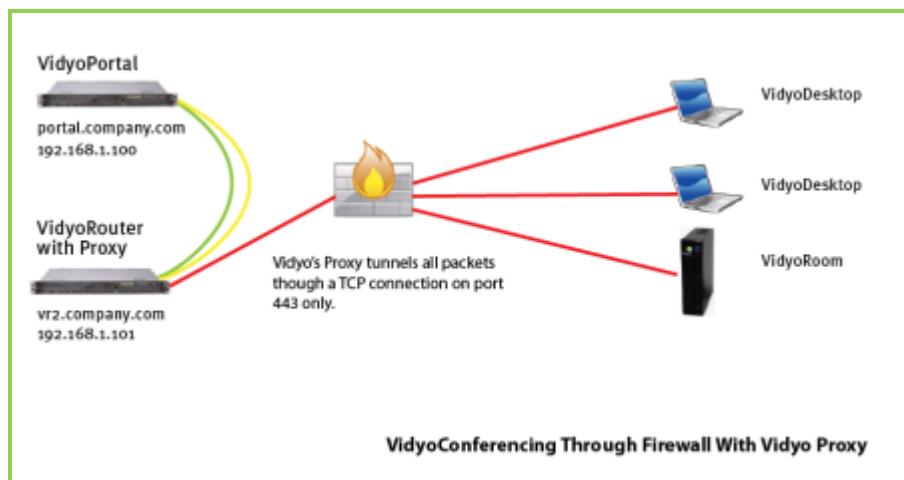
The VidyoProxy solution comprises both client and server software components. The server component resides on the VidyoRouter appliance and is included with the purchase of the VidyoRouter. The client component is included with the VidyoDesktop purchase and resides in VidyoDesktop as an optionally configured component.

Vidyo Solutions for Firewallled Networks

The actual steps to configure the Firewall NAT and DNS environments are outside the scope of this chapter, and varies based on the Firewall NAT and DNS servers used. This section focuses on the configuration of the VidyoProxy solution.

Note: This appendix assumes that HTTPS and SSL are not configured for the VidyoPortal or VidyoRouter.





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 VidyoPortal 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 overridden. 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.

CONFIGURING 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. For information on how to initially configure your VidyoProxy, see the “Configuring VidyoRouters and VidyoProxys via the Configuration Server” on page [138](#). The rest of the tabs on the VidyoProxy Configuration page are very similar to the VidyoRouter. For more information, see “Configuring the VidyoRouter Component” on page [163](#).

Appendix C. Security

Securing your VidyoConferencing system involves securing your VidyoPortal and your various components such as VidyoManager, VidyoRouter, and VidyoGateway. This section of the guide shows you how to secure your VidyoPortal. For specific information about securing VidyoGateway and VidyoReplay, refer to the security sections in the *VidyoGateway* and *VidyoReplay Administrator Guides* in the Vidyo Support Center at <http://support.vidyo.com>.

Before we secure the VidyoPortal, it's important to understand there are two security layers available for your VidyoConferencing system:

- **HTTPS** – The web standard involves setting up HTTPS and using Secure Socket Layer (SSL). This ensures secure browsing on VidyoPortal or VidyoOne.

While support for HTTPS is standardly included in Vidyo products, it does require the purchase and acquisition of SSL certificate or certificates from a valid CA (Certificate Authority). You may implement HTTPS without enabling Vidyo's Encryption to implement secure browsing only.

Enabling HTTPS secure browsing establishes secure connections between:

- The desktop user's browser (also, the VidyoRoom System's browser) and the Vidyo User portal.
- The browser connection to the Admin and Super Admin web pages.
- The VidyoManager, VidyoRouter, and VidyoProxy Configuration Pages.

HTTPS uses standard SSL certification to provide secured browsing to these web pages, protecting usernames and passwords, and actions performed on the pages. Confidential information shared during a VidyoConference browsing session is protected from phishing and hacking attempts.

- **Encryption** – This is an additionally purchased Vidyo licensed feature (referred to as the Secured VidyoConferencing Option) which provides encrypted endpoint management, signaling and media for end-to-end security for your entire VidyoConferencing system. Encryption is meant to be implemented in addition to (and not in place of) HTTPS.

This software option still requires the implementation of HTTPS including the purchase and acquisition of an SSL certificate or certificates 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 (for licensing and management) and VidyoRouters (for signaling and media).
- Connections between all VidyoPortal components: VidyoPortal, VidyoManager, VidyoRouters, VidyoProxy, VidyoGateways and VidyoReplays.

Confidential information shared during a VidyoConference is protected from hijacking and eavesdropping attempts.

Note:

- To configure the Secured VidyoConferencing Option in your VidyoConferencing system, you must have a valid System Console account in order to access the VidyoManager, VidyoRouter, VidyoProxy, and VidyoGateway, Configuration Pages.
- For VidyoReplay, you must access the VidyoReplay Super Admin portal using your VidyoReplay Super Admin Account. For more information, refer to the *VidyoReplay Administrator Guide*.

The overall procedure involves performing the following sections in order:

1. “Securing Your VidyoConferencing System with SSL and HTTPS” on page [301](#).
2. “Configuring Your Components to Work with HTTPS” on page [321](#).
3. “Configuring Each VidyoPortal Component to Use Your FQDN” on page [325](#).
4. “Applying VidyoPortal SSL Certificates to VidyoRooms, and VidyoGateways” on page [330](#).
5. “Implementing Encryption Using the Secured VidyoConferencing Option” on page [331](#) (optional).

SECURING YOUR VIDYOCONFERENCING SYSTEM WITH SSL AND HTTPS

To secure your VidyoConferencing system by Enabling SSL and HTTPS Only, you must complete specific configurations done on six sequential tabs from left to right in the Security section of the Super Admin Portal.

The tabs include:

1. SSL Private Key Tab – This tab is for Generating or Uploading an SSL Private Key.
2. SSL CSR Tab – This tab is for Generating an SSL Certificate Signing Request (CSR).
3. Server Certificate Tab – This tab is for Deploying Your Server Certificate.
4. Server CA Certificates Tab – This tab is for Deploying Your Server Certification Authority (CA) Certificates.
5. Applications Tab – Regarding Security, this tab is used to correctly configure HTTPS Port settings to 443.

Note: This tab is also used for Management Interface configurations. For more information, see “Enabling the Management Interface” on page [57](#).

6. Advanced Tab – This tab is for deploying your Client Root CA Certificates.

Note: The Advanced tab is also used to Upload and Import Security Settings, and Reset Security Settings. For more information, see “Uploading and Exporting Certificates from the Advanced Tab” on page [317](#), and “Resetting Security Settings to Factory Defaults” on page [319](#).

7. Enabling SSL and HTTPS Only

Note: Do not use the Enable SSL button and HTTPS Only check box until you’ve completed the steps for securing your VidyoConferencing system.

The following ordered sections explain these steps in detail.

Note: When configuring a VidyoRouter for security, access your VidyoRouter at <http://<FQDN or IP>/vr2conf/> and use the exact same procedures for VidyoPortal SSL and HTTPS configuration described in “Configuring Your Components to Work with HTTPS” on page 321 and “Configuring Each VidyoPortal Component to Use Your FQDN” on page 325.

- The URL of your VidyoRouter is typically a domain name: <http://<FQDN or IP>/vr2conf/>. You can also click the VidyoRouter IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page 23.
- Although the default username for this page is admin, only the Super Admin accesses these pages.

Generating or Uploading an SSL Private Key

You can generate a new SSL Private Key. Or you can upload or paste an existing SSL Private Key. When generating, examine your own security requirements and applicable policies carefully before deciding on a suitable key size. An initial key is automatically generated when you first set up your system. This initial key has a 2048 key size.

Generating an SSL Private Key

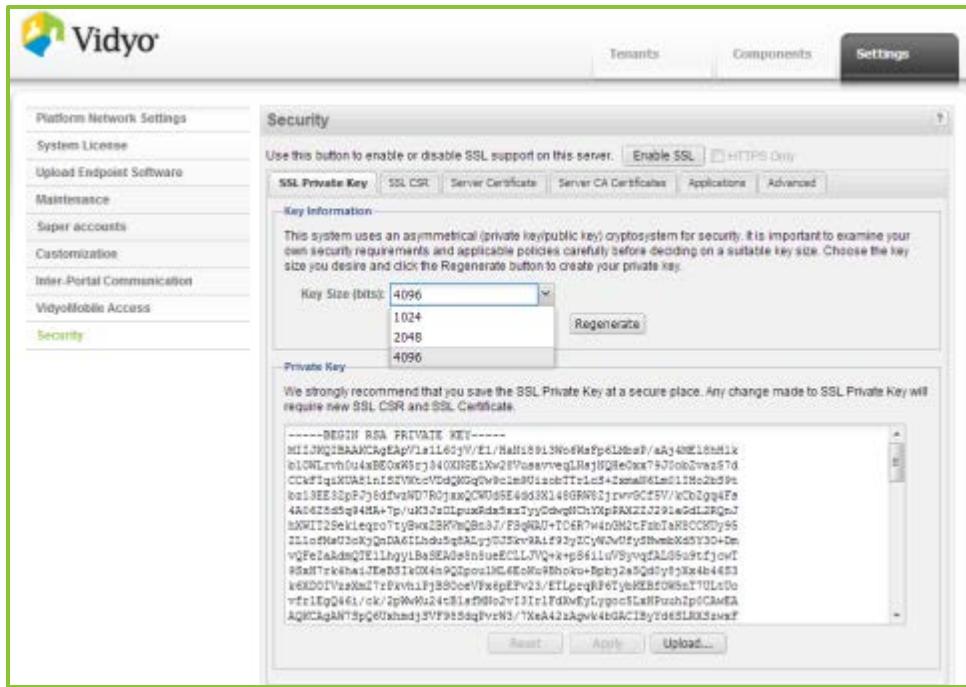
This system uses an asymmetrical (private key and public key) cryptosystem for security. Choose the key size you desire and click the Regenerate button to create your private key.

Note: Changes made to an SSL Private Key require a new CSR and SSL Server Certificate. This includes regenerated keys and uploading existing keys.

To generate an SSL Private Key:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page 35.
2. Click the **Settings** tab.
3. Click **Security** on the left menu.

- Click the **SSL Private Key** tab.



- In the Key Size field, specify a 1024, 2048, or 4096 key size.

Note: Some countries or CAs limit the key size. Observe the limitations in effect in your country. Check with your CA for Key Size requirements.

- Click **Generate** or **Regenerate**.

The key is then shown on the Private Key area of the screen.

Uploading an SSL Private Key

Private keys can be copied from or generated on other machines for use on your server using this and the next section. For more information, see “Pasting an SSL Private Key” on page [304](#).

Note:

- Changes made to an SSL Private Key require a new CSR and SSL Server Certificate. This includes re-generated keys and uploading existing keys.
- Private Keys are replaced if you choose to import from .p7b, .pfx, or .vidyo bundle formats. For more information, see “Importing Certificates from a Certificate Bundle” on page [317](#).

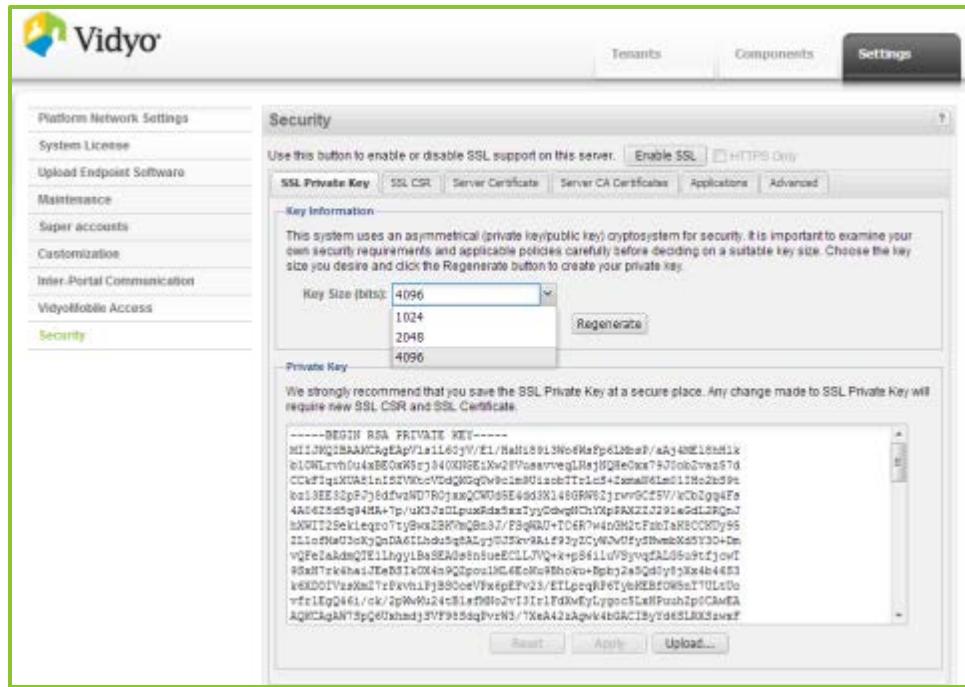
To upload a private key:

- Log in to the Super Admin portal using your Super Admin account.

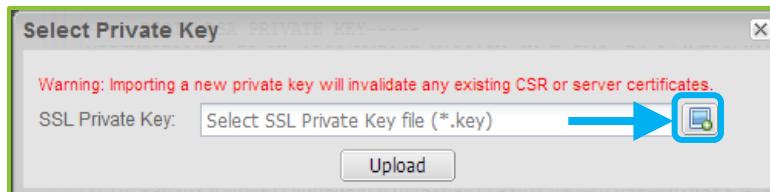
For more information, see “Logging in to the Super Admin Portal” on page [35](#).

- Click the **Settings** tab.
- Click **Security** on the left menu.

- Click the **SSL Private Key** tab.



- Click **Upload**.
- In the Select Private Key dialog box, click **Select File**.



- Select your private key file and click **Upload**.
If the upload is successful, the File Upload Success dialog box appears.
- The tab then loads the Private Key information in the lower part of the screen.

Pasting an SSL Private Key

Private keys can be copied from or generated on other machines for use on your server. Carefully copy your desired SSL Private Key in its entirety before starting this procedure.

Note:

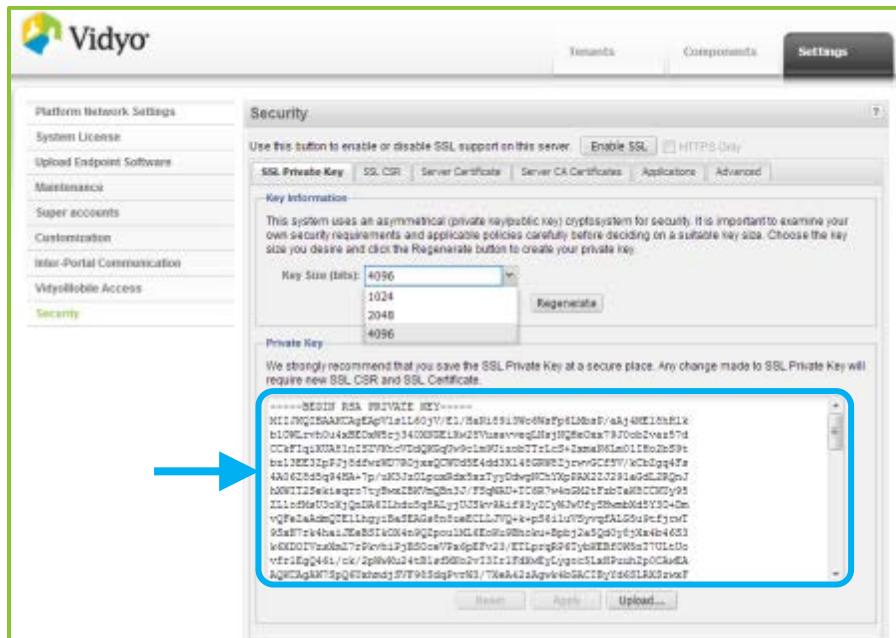
- Changes made to an SSL Private Key require a new CSR and SSL Server Certificate. This includes regenerated keys and uploading existing keys.
- Private Keys are replaced if you choose to import from .p7b, .pfx, or .vidyo bundle formats. For more information, see "Importing Certificates from a Certificate Bundle" on page [317](#).

To paste a private key:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page 35.

2. Click the **Settings** tab.
3. Click **Security** on the left menu.
4. Click the **SSL Private Key** tab.
5. Paste the Private Key you copied from or generated on another machine for use on your server in the Private Key part of the screen.



6. Click **Upload**.

If the upload is successful, the File Upload Success dialog box appears.

Generating an SSL CSR

A Certificate Signing Request (CSR) is a message sent to a certification authority (CA) to request a public key certificate for a person or web server. The majority of public key certificates issued are SSL certificates, which are used to secure communications with web sites. The CA examines the CSR, which it considers to be a wish list from the requesting entity. If the request is in line with the CA's policy or it can be modified to bring it in line, the CA issues a certificate for the requesting entity.

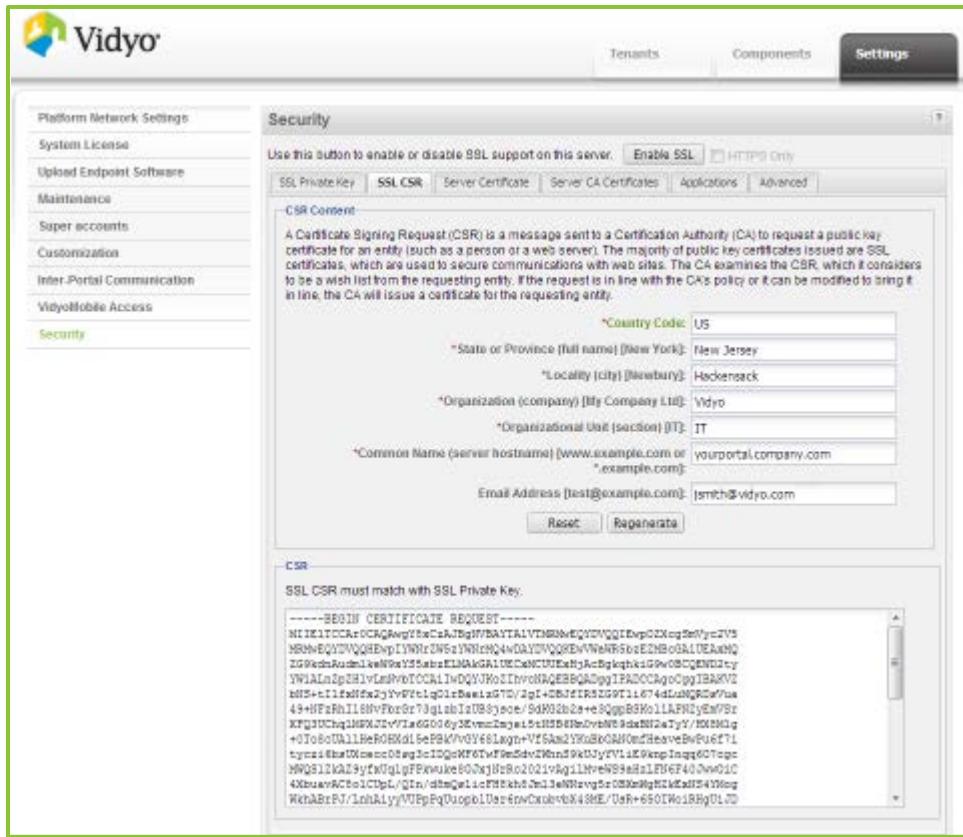
To generate an SSL CSR:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page 35.

2. Click the **Settings** tab.

3. Click **Security** on the left menu.
4. Click the **SSL CSR** tab.



The screenshot shows the Vidyo Platform Network Settings interface with the 'Security' tab selected. Under the 'CSR Content' section, there is a large text area containing a certificate signing request (CSR) string. The string starts with '-----BEGIN CERTIFICATE REQUEST-----' and ends with '-----END CERTIFICATE REQUEST-----'. It includes various fields such as country code (US), state or province (New Jersey), locality (Hackensack), organization (Vidyo), organizational unit (IT), common name (www.example.com or example.com), and email address (smith@example.com).

5. Check with your CA and carefully enter correct values for the following:
 - Country Code (the 2 character ISO 3166 country code)
 - State or Province Name
 - Locality
 - Organization Name
 - Organization Unit
 - Common Name (the FQDN of the server)
 - Email Address

Note: If using a Subject Alternate Name (SAN) certificate, the alternate names are added by the Certificate Authority when a certificate is ordered and the Common Name you're providing here in the Certificate Details portion of the screen is used to provide your base Common Name (CN) for your SAN certificate. For more information, see “Using a Wildcard Certificate in a Multi-Tenant System” on page [307](#).

6. Provide all field information exactly as you registered it with your domain registration provider. You should consider all information on this screen mandatory before you click **Generate** or **Regenerate CSR**.

Note:

- Click **Reset** to reload any previously saved field information.
- Your SSL CSR is generated based on the SSL Private Key you entered during “Generating or Uploading an SSL Private Key” on page [302](#).

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 then also use a wildcard or SAN SSL certificate. For a wildcard 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 automatically matches the fully qualified domain name (FQDN) for the certificate.

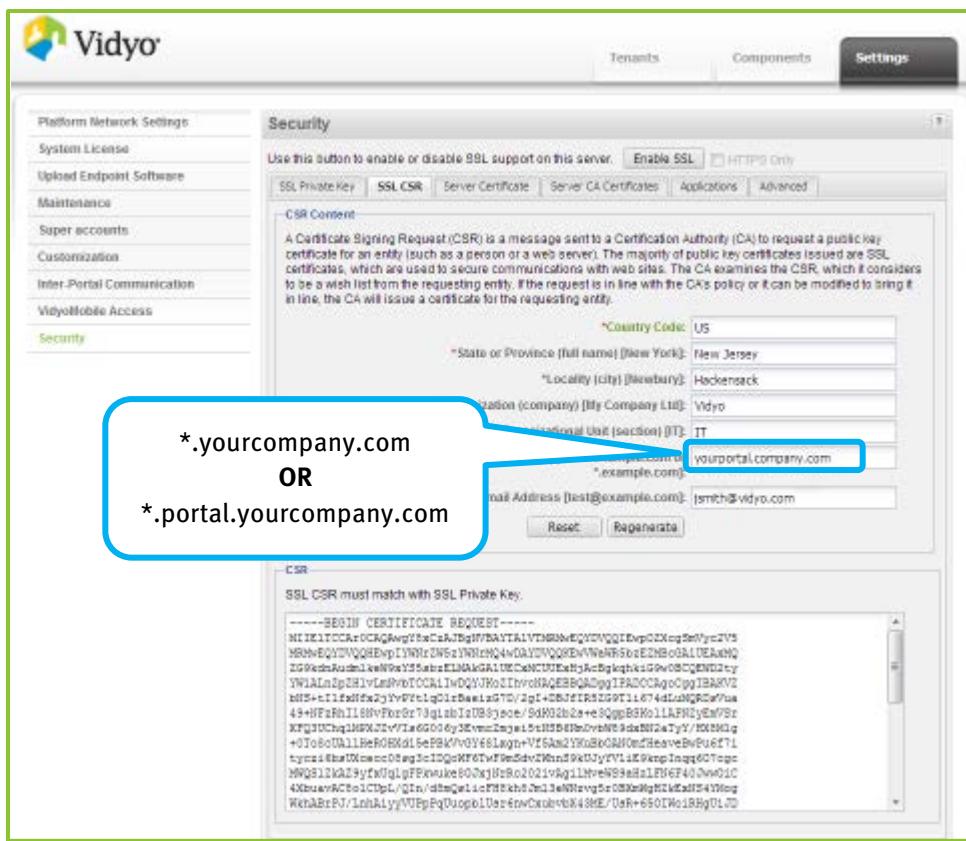
For example: ***.company.com** or ***.portal.company.com**.

Note:

- If using a Subject Alternate Name (SAN) certificate, the alternate names are added by the Certificate Authority when a certificate is ordered and the Common Name you’re providing here in the Certificate Details portion of the screen is used to provide your base Common Name (CN) for your SAN certificate.
- Microsoft refers to their own version of SAN certificates as Unified Communications (UC) certificates.

Vidyo recommends 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 following screenshot shows wildcard certificate entry examples:



Certificates Received from Your Certificate Authority

Most CAs instantly send certificates and returns at least a domain (server) certificate and may return a root and one or more intermediate certificates in separate files. However, some authorities may provide the certificate data in a single email. You must copy the certificate data from the email into separate, respective files.

Note: When selecting the certificate type from your CA, be sure to select Apache2 or Tomcat.

Your certificate authority may provide three types of files:

1. The domain certificate file. This is often named or titled server certificate.
2. One or more intermediate certificate files. This is optional.
3. The root certificate file.

Again, 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.

As mentioned, 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 doesn't append carriage returns at the end of each line.

Vidyo recommends the following guidelines to identify certificate files from your CA:

- 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 intermediate certificates need to be located, and manually downloaded from the CA's website.

If the root and intermediate certificates were not provided to you, the VidyoPortal includes a default bundle of common CA root and intermediate certificates. If you are using a mainstream CA, the root and intermediate certificates may not be needed.

Note: Some CAs have several root and intermediate certificates available depending on the type of certificate you have ordered. Be sure to locate the appropriate matching root and intermediate certificates for your domain certificate. Contact your CA for assistance if you're not sure.

CAs provide different kinds of certificate files to customers. Regardless, the following certificates should be a part of what your CA provides to you:

- Domain Certificate (may have a `.domain`, `.crt`, or `.cer` extension).
- Intermediate Certificate(s) (optional, may be one or more, and may have an `.inter`, `.crt`, or `.cer` extension).
- A Root Certificate (may have a `.root`, `.crt`, or `.cer` extension).

Certificate Files versus Bundles

Your CA may instead provide you with a `.p7b` file, which may contain Root and Intermediate or Root, Intermediate, and Server Certificate content. Check with your CA to find out exactly where each certificate is located. VidyoPortal accepts the `.pem`, `.crt`, `.cer`, `.der`, `.p7b`, and `.pfx` formats. The `.pfx` format additionally includes the private key which may be password protected.

- Certificate Files (`.pem`, `.crt`, `.cer`, and `.der`) are imported using the Server Certificate, Server CA Certificates, and Advanced Tabs. For more information, see “Deploying Your Server Certificate” on page [309](#), “Deploying Your Server CA Certificates (Intermediates)” on page [311](#), and “Importing Client Root CA Certificates from the Advanced Tab” on page [313](#).
- Bundles (`.p7b`, `.pfx`, and `.vidyo`) are imported and exported (only `.vidyo` files can be exported) from the Advanced Tab. For more information, see “Importing Client Root CA Certificates from the Advanced Tab” on page [313](#).

Deploying Your Server Certificate

Note:

- Perform the steps in this procedure after you receive certificate files back from your certification authority.

- An unsigned (self-issued) certificate does not provide a guarantee of security to your users.
- Your Vidyo server checks certificates for validity based on the certificates issued date range. Therefore, make sure that the time zone of your server is configured correctly prior to applying your certificate.

For more information about setting the time zone of your server, see “Configuring Network Settings at the System Console” on page [25](#).

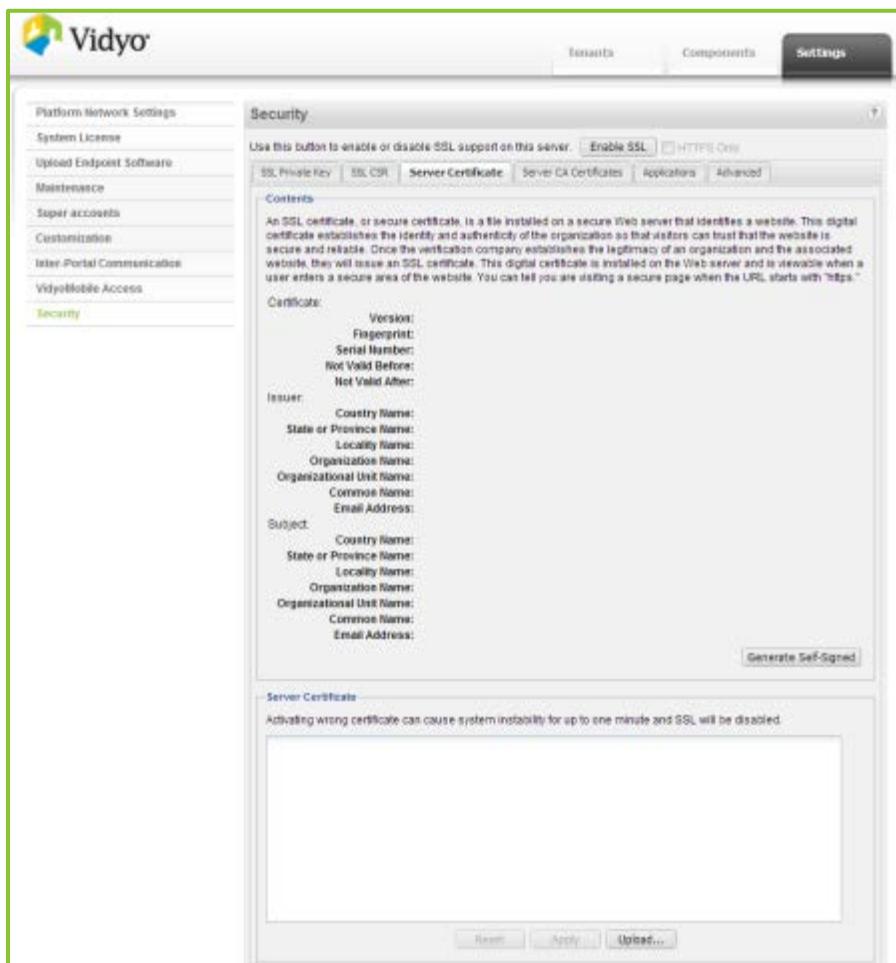
- If you instead plan on using self-signed certificates, you can click **Generate Self-Signed** to have the server sign its own certificate (self-signed). Clicking Generate Self-Signed and confirming removes your currently implemented server certificate.

To upload your server certificate file:

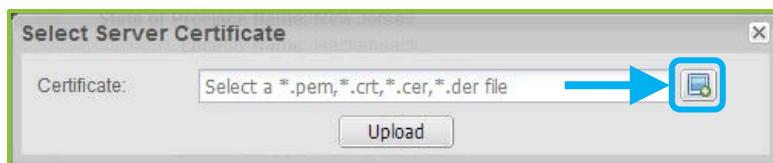
1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Settings** tab.
3. Click **Security** on the left menu.
4. Click the **Server Certificate** tab.



5. Click **Upload**.
6. In the Select Server Certificate dialog box, click **Select File**.



7. Select your server certificate file on your computer (may also be referred to as the Domain Certificate by your Certificate Authority) or local network and click **Upload**.

If the upload is successful, the File Upload Success dialog box appears.

1. The tab then loads the Certificate Information, Issuer, Subject, and the Certificate itself in the screen.

Receiving Certificate Expiration Notifications

The system watches your certificate’s “Not Valid After” value and can warn you when it’s about to expire via System Admin email.

- Advance warnings are provided in the following daily increment order: 60, 45, 30, 15, 7, 6, 5, 4, 3, 2, 1. Verify that the email addresses on your System Admin accounts are configured correctly.
- For more information, see “Managing Your Super Accounts” on page [86](#).
- Contact your Certificate Authority to renew your certificate.

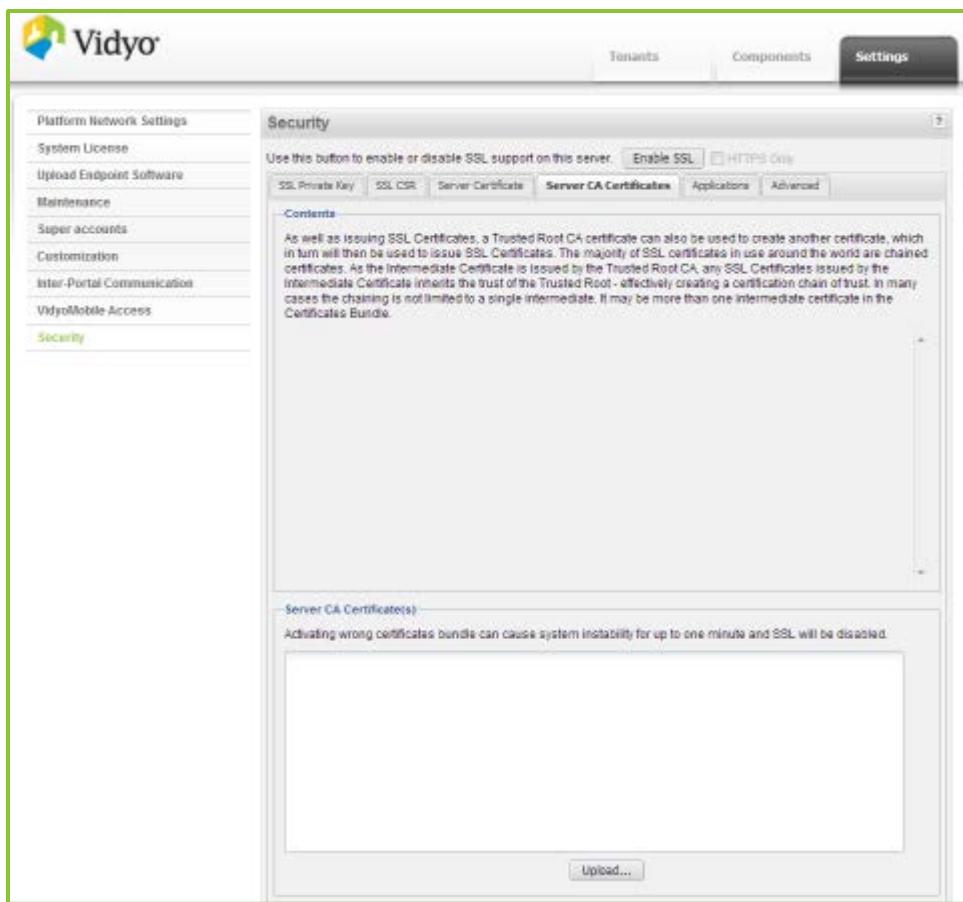
Deploying Your Server CA Certificates (Intermediates)

In addition to issuing SSL Certificates, a Trusted Root CA certificate can also be used to create another certificate, which in turn can be used to issue SSL Certificates. The majority of SSL certificates in use around the world are chained certificates of this type. As the Intermediate Certificate is issued by the Trusted Root CA, any SSL Certificates issued by the Intermediate Certificate inherits the trust of the Trusted Root – effectively creating a certification chain of trust. In many cases the chaining is not limited to a single intermediate. More than one intermediate certificate may be part of a Certificates Bundle.

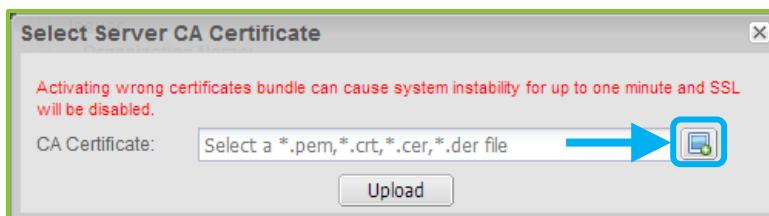
To upload your server CA certificates (intermediates) files:

1. Log in to the Super Admin portal using your Super Admin account.
- For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
 3. Click **Security** on the left menu.

- Click the **Server CA Certificates** tab.



- Click **Upload**.
- In the Select Server CA Certificate dialog box, click **Select File**.



- Select your server CA certificate file on your computer (may also be referred to as the Intermediate Certificate by your Certificate Authority) or local network and click **Upload**.

Note:

- A single file may contain multiple intermediate certificates.
- You can additionally upload the Root CA in this location in order to present the certificate to your clients along with the certificate chain. However, this is not recommended as standard security practice.

If the upload is successful, the File Upload Success dialog box appears.

8. The tab then loads the Certificate Information, Issuer, Subject, and the Certificates in the screen.

Configuring HTTPS Port Settings on Your Applications

Note: The Applications tab is also used for Management Interface settings. For more information, see “Enabling the Management Interface” on page [57](#).

Configuring HTTPS port settings on your Applications:

The HTTPS port should remain 443 (the default) on a VidyoPortal. If you set the HTTPS port to anything other than 443, users have to manually add the port to their URL requests in their browsers.

Note: If you’re using a VidyoRouter, the default HTTPS port is 8443. VidyoProxy runs on port 443.

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Security** on the left menu.
4. Click the **Applications** tab.

Applications	Network Interface	HTTP	HTTPS	OCSP
super	PRODUCTION	80	443	<input type="checkbox"/>
vm2conf	MANAGEMENT	80	443	<input checked="" type="checkbox"/>
vr2conf	MANAGEMENT	80	443	<input checked="" type="checkbox"/>
admin	PRODUCTION	80	443	<input type="checkbox"/>
vp2conf	MANAGEMENT	80	443	<input checked="" type="checkbox"/>

5. Click HTTPS values under the HTTPS column to make them writeable and modify, if desired.
Note: HTTPS will not enable if you have any other applications running on your configured port. This includes VidyoProxy.
6. Click **Save**.

Importing Client Root CA Certificates from the Advanced Tab

The Advanced tab is used to upload trusted Client Root CA Certificates. This includes all Intermediate and Root Certificates.

Note:

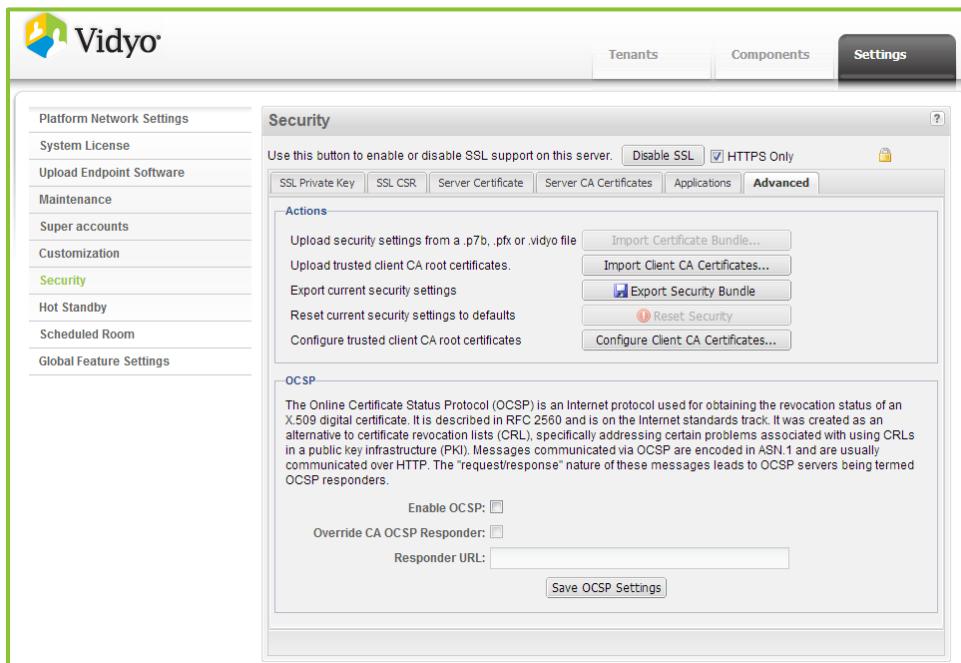
- If your system requires trusting other secure systems such as LDAPS, Secure SMTP Server, and an OCSP Responder, their certificates must also be uploaded in this tab.
- The Advanced tab is also used to Upload and Import Security Settings, Reset Security Settings, and to Enable and Configure OCSP. For more information, see “Uploading and Exporting Certificates from the Advanced Tab” on page 317, “Resetting Security Settings to Factory Defaults” on page 319, “Configuring Client CA Certificates” on page 320, and “Configuring OCSP” on page 280.

To upload Client Root CA Certificates from the Advanced tab:

1. Log in to the Super Admin portal using your Super Admin account.

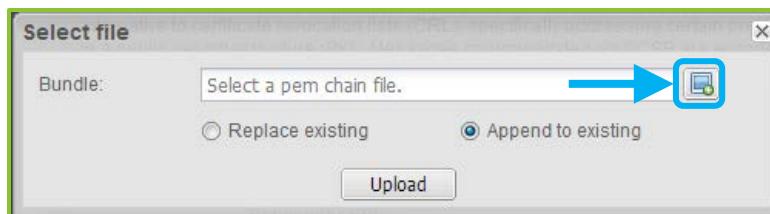
For more information, see “Logging in to the Super Admin Portal” on page 35.

2. Click the **Settings** tab.
3. Click **Security** on the left menu.
4. Click the **Advanced** tab.



5. Click **Import Client CA Certificates**.
6. In the Select file dialog box, choose **Replace existing** or **Append to existing**.
 - Replace existing – Replaces any previously uploaded Client Root CA Certificates.
 - Append to existing – Any uploaded Client Root CA Certificates are added to your existing ones.

7. Click **Select File** to locate the server certificate file on your computer (may also be referred to as the Domain Certificate by your Certificate Authority) or local network.



Note: A single file may contain multiple Client Root CA Certificates.

8. Click **Upload** to upload the client root CA certificate file.

An Uploading file progress bar is shown while the system applies your certificates.

If the upload is successful, a Confirmation dialog box appears indicating that your “Upload successful. Do you want to reboot the server now?”

9. Click **Yes**.

Enabling SSL and HTTPS Only

Note:

- Before Enabling SSL and HTTPS Only, ensure that your VidyoProxy is not running on the same port on which your applications are running. For more information, see “Configuring HTTPS Port Settings on Your Applications” on page [313](#).
- Do not use the Enable SSL button and HTTPS Only check box until you’ve completed the steps for securing your VidyoConferencing system. Do not Enable HTTPS Only mode until you are certain HTTPS is working properly. For more information, see “Securing Your VidyoConferencing System” on page [301](#).

Enabling SSL

To enable SSL:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Settings** tab.

3. Click **Security** on the left menu.

4. Click **Enable SSL** on the Security screen, above the tabs.

A confirmation dialog appears.

5. Click **Yes** to confirm you want to enable SSL.

A success dialog appears.

6. Click **OK**.

You can now browse your VidyoConferencing system over HTTPS.

7. Browse to any of your VidyoPortal Admin portal to confirm that HTTPS is working properly and that the browser does not post any security errors. Be sure to include the HTTPS header in the URL (e.g., **https://<FQDN>**). 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.

Note:

- 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.
- If your browser generates a root certificate error, first check that your operating system has the latest root certificates update applied.

8. If you are successful browsing to your VidyoPortal using HTTPS and you do not receive any browser errors, continue with the next procedure.

Note: If you are unable to connect to your VidyoPortal over HTTPS, see “Recovering from an HTTPS Failure” on page [317](#).

Enabling HTTPS Only

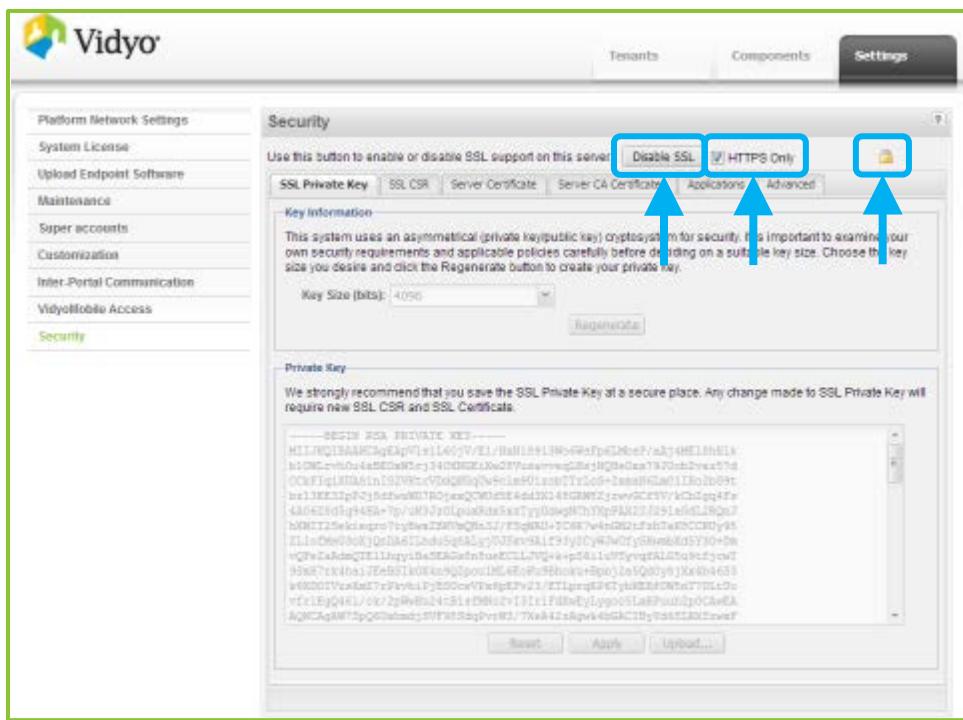
Before you Enable HTTPS Only, you must configure your components to work with HTTPS. For more information see “Configuring Your Components to Work with HTTPS” on page [321](#).

If you don’t configure your components to work with HTTPS first, you can still enable HTTPS Only, however, this may result in “DOWN” component statuses.

To enable HTTPS Only:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Security** on the left menu.
4. Select **HTTPS Only** on the Security screen, above the tabs.
A confirmation dialog appears.
5. Click **Yes** to confirm you want to enable HTTPS only.
A success dialog appears.
6. Click **OK**.
A confirmation dialog appears indicating that your “SSL settings have been reset. Do you want to reboot the server now?”
7. Click **Yes**.

Your sever reboots and the next time you access the system and return to the Security page, Enable SSL now shows as Disable SSL, the HTTPS Only check box is selected, and a padlock icon appears, all confirming your correct SSL and HTTPS implementation.



Recovering from an 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 using the System Console menu and selecting **Option 16**.

For more information, see “Understanding System Administrator Console Menu Options” on page [31](#).

Importing and Exporting Certificates from the Advanced Tab

You can also import or export certificate bundles using the Advanced tab.

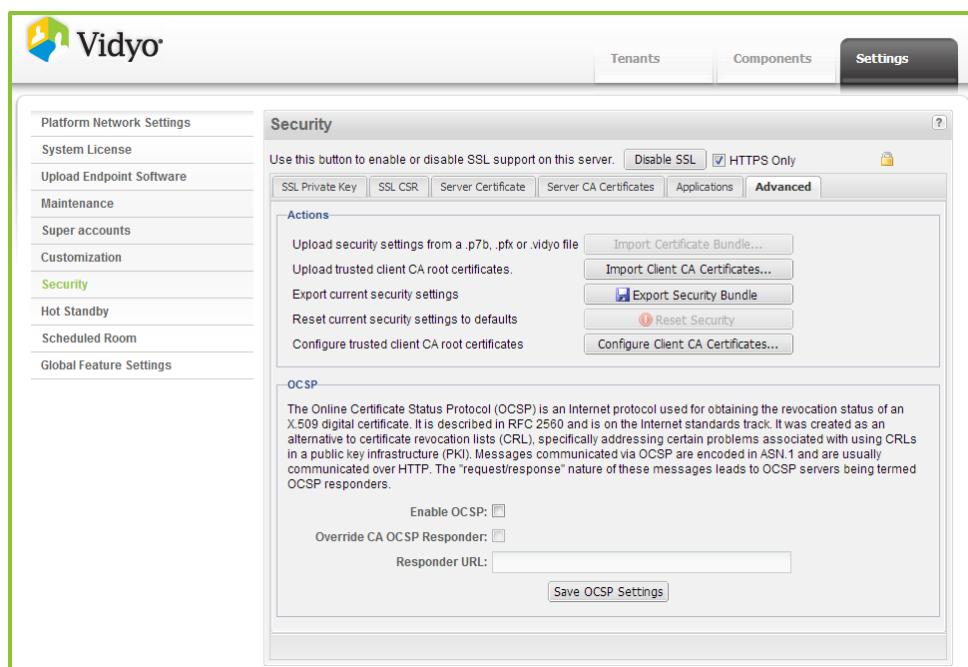
Importing Certificates from a Certificate Bundle

You can import from **.p7b** and **.pfx** standard formats. In addition, the **.vidyo** bundle format is available for importing certificates from other Vidyo servers.

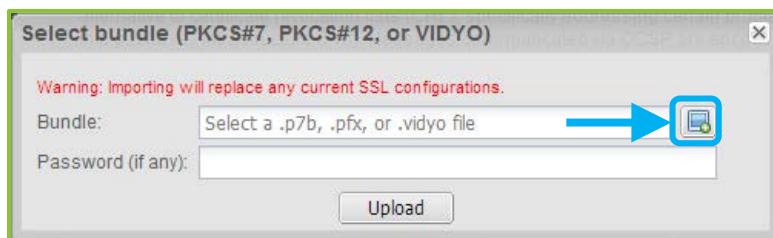
To upload security settings from a certificate bundle:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Security** on the left menu.

4. Click the **Advanced** tab.



5. Click **Import Certificates Bundle**.
6. In the Select bundle dialog box, click **Select File** to locate the bundle file.
7. If using the **.pfx** format, enter the password.



8. Click **Upload** to upload the bundle file.

If the upload is successful, the File Upload Success dialog box appears.

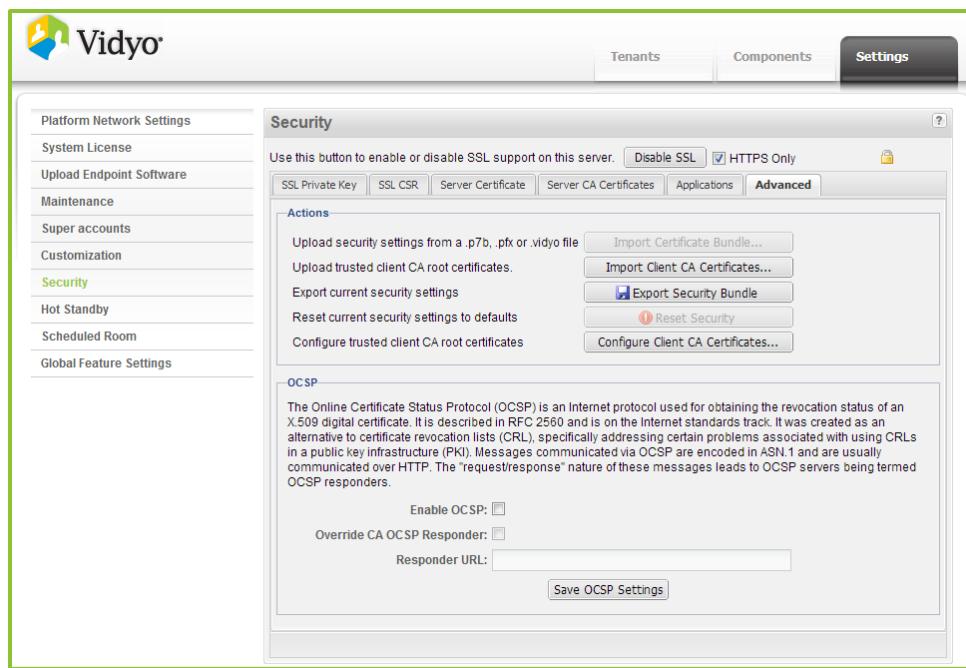
Note: Depending on which bundle format you used, the appropriate Private Key, Server Certificate, Server CA Certificates, and Client Root CA Certificates data is loaded in to your Vidyo Server.

Exporting a Security Bundle Containing Your Certificate Configuration

To export a security bundle containing your certificate configuration:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Security** on the left menu.

4. Click the **Advanced** tab.



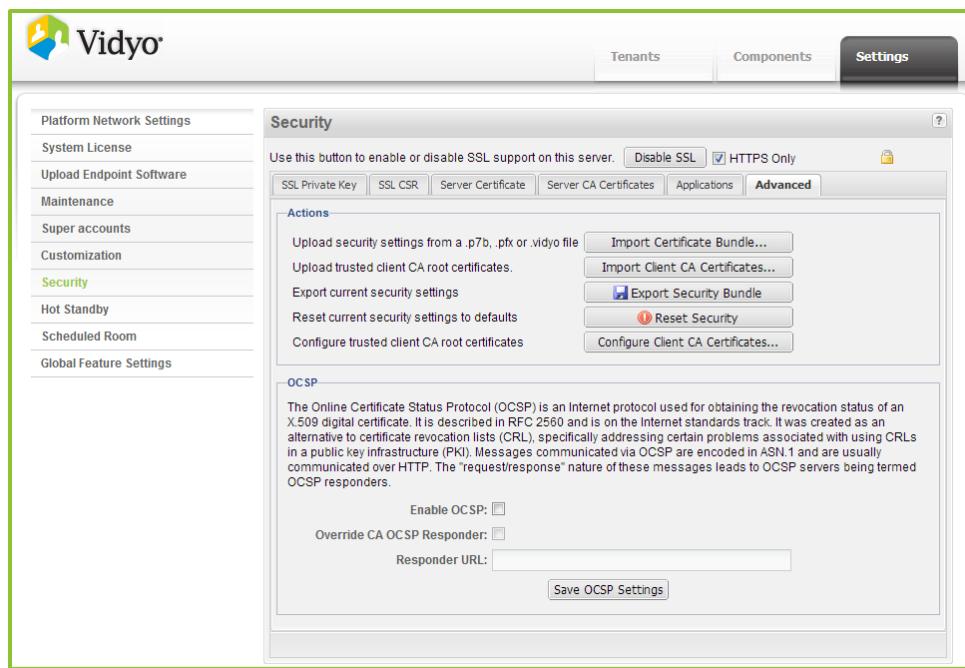
5. Click **Export Security Bundle**.
6. Your browser then downloads **security_bundle.vidyo** file to your computer which contains your security configuration for transfer or backup purposes.

Resetting Your Security Configuration to Factory Defaults

To reset your security configuration to the factory defaults:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Security** on the left menu.

4. Click the **Advanced** tab.



5. Click **Reset Security**.

Your security configuration is then restored to the factory default settings.

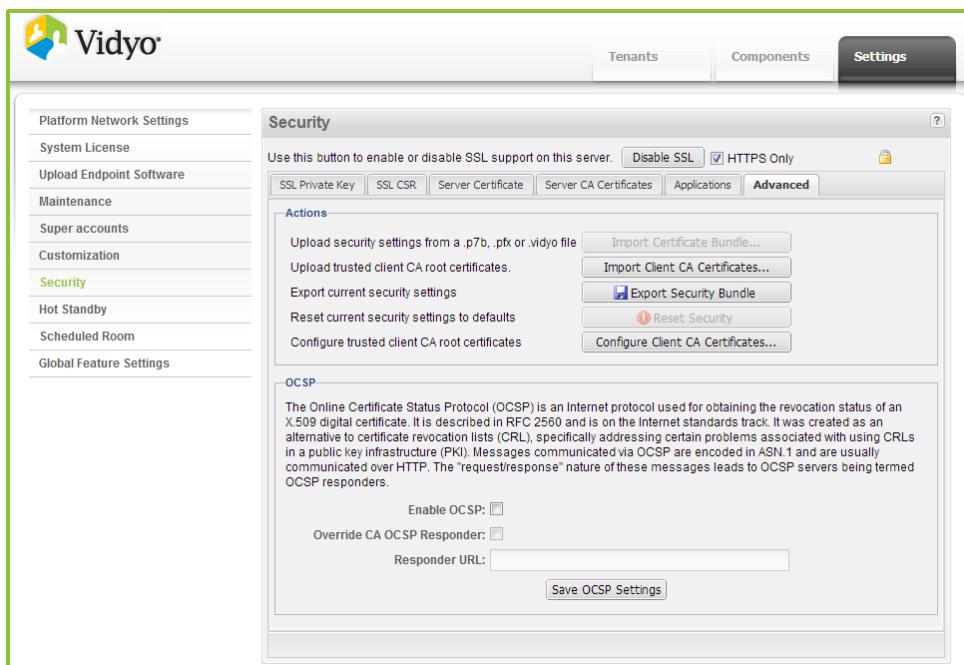
Configuring Client CA Certificates

Vidyo Servers ship with a default trusted CA list and is enabled by default. This Advanced tab function allows you to enable or disable the use of this list.

To configure client CA certificates:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **Security** on the left menu.

4. Click the **Advanced** tab.



5. Click **Configure Client CA Certificates**.

The Configure Client CA Certificates dialog box appears.



6. Click **Save**.

After rebooting your system, your CA root certificates are applied.

For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).

CONFIGURING YOUR COMPONENTS TO WORK WITH HTTPS

After implementing SSL and enabling HTTPS on your VidyoPortal, each component must be set up to listen on and address each other using a valid FQDN (URL or Common Name) as defined in the certificate applied.

After setting the FQDN address on your VidyoPortal and VidyoRouter(s) as described in the first section, be sure to continue and set the FQDN on all of your system components as explained in the following cumulative sections:

1. “Setting the Hostname and Domain on Your Vidyo Server” on page [322](#).
2. “Setting the FQDN on Your VidyoManager Configuration Page” on page [322](#).
3. “Setting the FQDN on Your VidyoRouter Configuration Page” on page [322](#).

4. “Setting the FQDN on Your VidyoProxy Configuration Page” on page [323](#).
5. “Setting the FQDN on Your Tenants” on page [324](#).

Setting the Hostname and Domain on Your Vidyo Server

Your VidyoPortal and VidyoRouter must be configured to be aware of their DNS hostnames. This is done when configuring your network settings at the System Console. For more information, see “Configuring the Network Settings at the System Console” on page [25](#).

Setting the FQDN on Your VidyoManager Configuration Page

To set the FQDN on your VidyoManager Configuration Page:

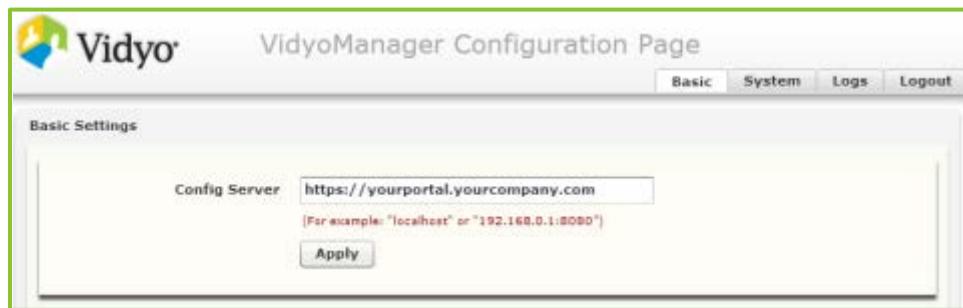
1. Log in to your VidyoManager Configuration Page using your System Console account.

Note:

- The URL of your VidyoManager is your VidyoPortal: <http://<FQDN or IP>/vm2conf/>. You can also click the VidyoManager IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoManager Configuration Page appears.

2. On the Basic tab, set the Configuration Server to a valid FQDN of the VidyoPortal as defined by the applied certificate:



Note: Best practice is to provide a full URL for your Config Server value beginning with **https://**, using your [FQDN or IP](#), and even a port reference, if desired.

3. Click **Apply**.
4. Click **OK** to restart the VidyoManager.
5. Proceed and set the FQDN on your VidyoRouter.

Setting the FQDN on Your VidyoRouter Configuration Page

The FQDN on your VidyoRouter is set up using the following procedure.

To set the FQDN on your VidyoRouter Configuration page:

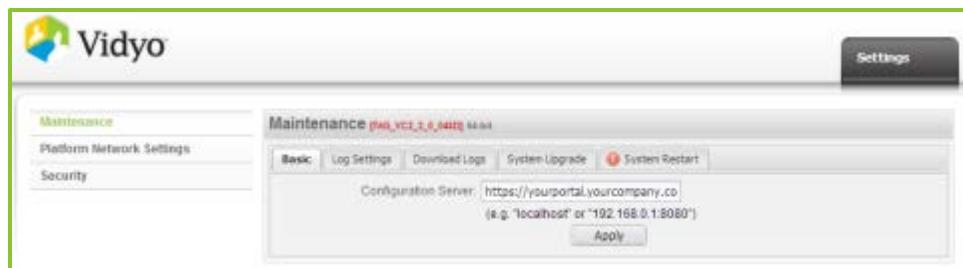
1. Log in to your VidyoRouter using your System Console account.

Note:

- The URL of your VidyoRouter is typically a domain name: **http://<FQDN or IP>/vr2conf/**. You can also click the VidyoRouter IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoRouter Configuration Page appears.

2. On the Basic tab, set the Configuration Server to a valid FQDN of the VidyoPortal as defined by the applied certificate:



Note: Best practice is to provide a full URL for your Config Server value beginning with **https://**, using your **FQDN or IP**, and even a port reference, if desired.

3. Click **Apply**.
4. Click **OK** to restart the VidyoRouter.
5. Proceed and set the FQDN on your VidyoProxy.

Setting the FQDN on Your VidyoProxy Configuration Page

To set the FQDN on Your VidyoProxy Configuration Page:

1. Log in to your VidyoProxy using your System Console account.

Note:

- The URL of your VidyoProxy is typically a domain name: **http://<FQDN or IP>/vp2conf/**. You can also click the VidyoProxy IP address on the Components tab in your VidyoPortal.
- For more information, see “Logging in to the System Console of Your Vidyo Server and Changing the Default Password” on page [23](#).
- Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoProxy Configuration Page appears.

2. On the Basic tab, set the Configuration Server to a valid FQDN for your VidyoPortal as defined by the applied certificate:



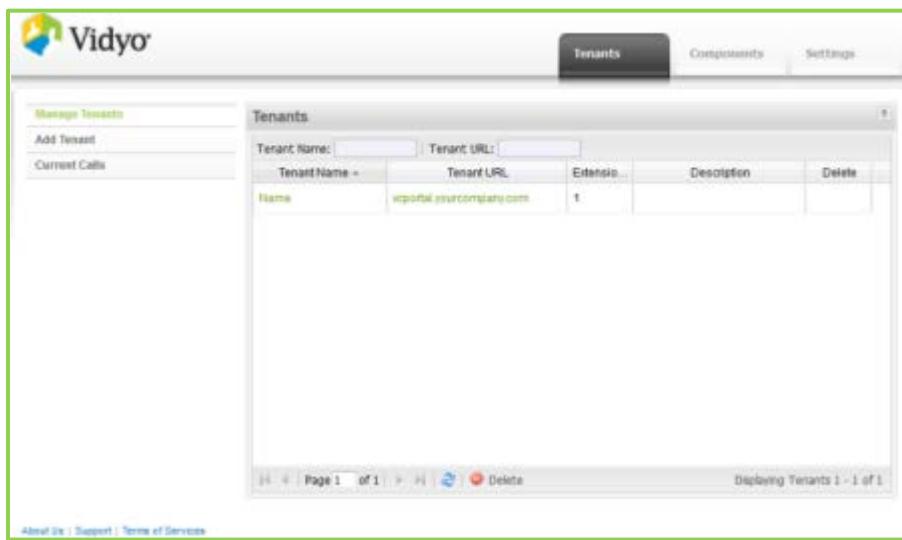
Note: Best practice is to provide a full URL for your Config Server value beginning with **https://**, using your **FQDN or IP**, and even a port reference, if desired.

3. Click **Apply**.
4. Click **OK** to restart the VidyoProxy.

Setting the FQDN on Your Tenants

To configure your tenants to use FQDNs:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Tenants** tab.
3. Click **Manage Tenants** on the left menu.



4. Ensure that each Tenant (including the Default Tenant) is using a valid FQDN for Tenant URL as defined by the certificate applied.

For more information, see “Configuring a Default Tenant or Adding a New Tenant” on page [187](#).

CONFIGURING EACH VIDYOPORTAL COMPONENT TO USE YOUR FQDN

Now, you must use the VidyoPortal Super Admin portal to configure each component to use the FQDN as defined in the certificate applied. This is done from the Component Configuration of your VidyoManager and VidyoRouter.

Setting the FQDN in Your VidyoManager Component Configuration

To set your FQDN in your VidyoManager Component Configuration:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.

Status	Name	Type	IP	Config Version	Software Version	Alarm
DISABLED	VidyoProxy	VidyoProxy	192.168.1.100	1 / 0	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	LocalVM	VidyoManager	192.168.1.100	9 / 9	TAG_VC2_2_0_119	<input type="checkbox"/>
NEW		VidyoRouter	192.168.1.105	0 / 1	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	VidyoGateway	VidyoGateway	192.168.1.110		2.2.0(283)	<input type="checkbox"/>
UP	VidyoRecord	VidyoReplay/Recs	192.168.1.115		2.2.0(281)	<input type="checkbox"/>
UP	SA Proxy	VidyoProxy	192.168.1.105	2 / 2	TAG_VC2_2_0_119	<input type="checkbox"/>
UP	VidyoReplay	VidyoReplay	192.168.1.115		2.2.0(281)	<input type="checkbox"/>

3. Double-click the **Status** on the VidyoManager row.

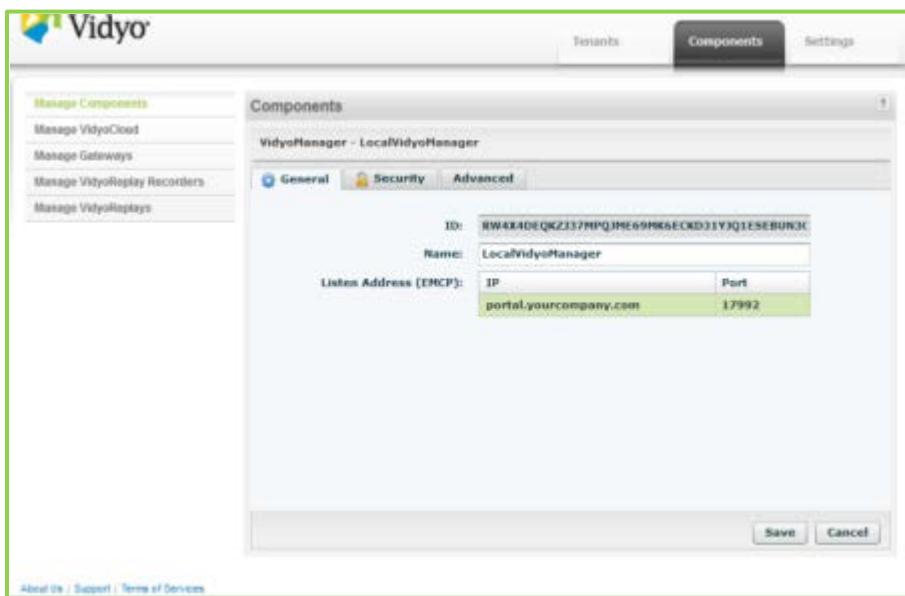
The VidyoManager Component Configuration is shown.

4. Select the **General** tab.

5. In the Listen Address (EMCP) field:

- a. Edit the EMCP address (VidyoManager address) by clicking the text in the IP column.

- b. Enter a valid FQDN as defined in the certificate applied by clicking in the Port column.



Note: If you're using FQDN licensing, the EMCP address is read-only.

6. Click **Save**.
7. Click **OK** to confirm your changes.
8. Return to the Manage Components screen and proceed by configuring your VidyoRouter to use your FQDN.

Setting the FQDN in Your VidyoRouter Component Configuration

Note: This procedure must be completed for each VidyoRouter in your VidyoConferencing system.

To set the FQDN in your VidyoRouter Component Configuration:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

- Click the **Components** tab.

The screenshot shows the Vidyo Components management interface. The main window title is "Components". The table lists the following components:

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	24 / 24	TAG_VC3_1_0_037	<input type="checkbox"/>
UP	Local VM	VidyoManager	172.20.4.125	4 / 3	TAG_VC3_1_0_037	<input type="checkbox"/>
UP	Local VP	VidyoProxy	172.20.4.125	10 / 0	TAG_VC3_1_0_037	<input type="checkbox"/>
DOWN	vg484	VidyoGateway	172.16.4.84		3.0.0(96)	<input type="checkbox"/>

Buttons at the bottom include: Delete, Enable, and Disable.

- Double-click the **Status** on the VidyoRouter row.
- In the Listen Address (SCIP) field:
 - Edit the SCIP address (VidyoRouter signaling address) by clicking the text in the IP field.
 - Enter a valid FQDN as defined by the certificate applied by clicking in the Port column.

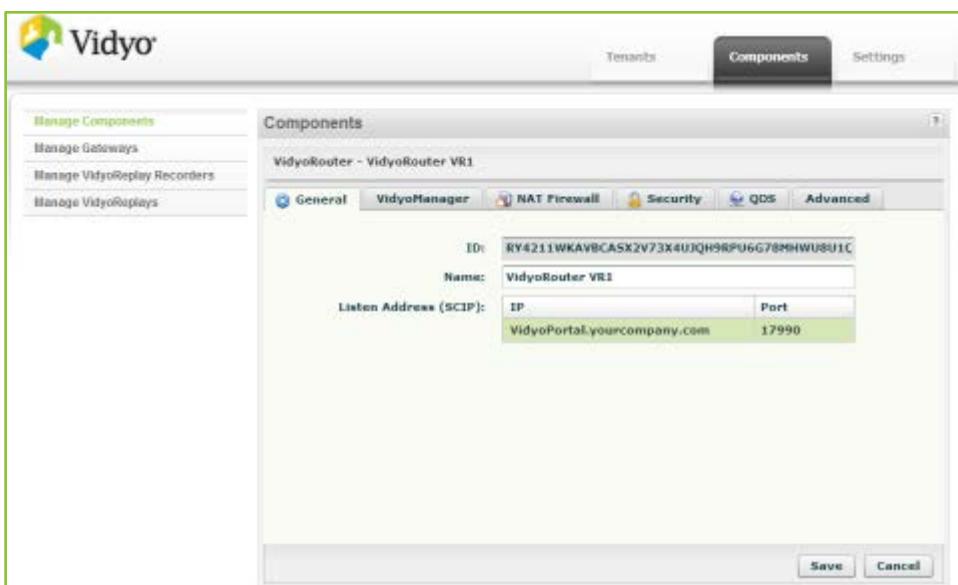
The screenshot shows the configuration dialog for the VidyoRouter - VidyoRouter VR1. The "VidyoManager" tab is selected. The "Listen Address (SCIP)" section contains the following fields:

ID:	RY4211WKAYBCASX2V73X4UJQH9RPU6G78MHWUBU1C	
Name:	VidyoRouter VR1	
Listen Address (SCIP):	IP	Port
	qa12.vidyo.com	17990

Buttons at the bottom include: Save and Cancel.

- Click the **VidyoManager** tab.
- In the VidyoManager field:
 - Edit the IP address by clicking the text in the IP column.

- b. Enter a valid FQDN as defined by the certificate applied.



7. Click **Save**.
8. Click **OK** to confirm your changes.
9. Return to the Manage Components screen and proceed by configuring your VidyoProxy to use your FQDN.

Setting the FQDN in Your VidyoProxy Component Configuration

To set your FQDN in your VidyoProxy Component Configuration:

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

- Click the **Components** tab.

The screenshot shows the Vidyo Components management interface. The left sidebar has links for Manage Components, Manage Gateways, Manage VidyoDisplay Recorders, and Manage VidyoReplays. The main area is titled 'Components' and lists the following components:

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	24 / 24	TAG_VC3_1_0_037	
UP	Local VM	VidyoManager	172.20.4.125	4 / 3	TAG_VC3_1_0_037	
UP	Local VP	VidyoProxy	172.20.4.125	10 / 0	TAG_VC3_1_0_037	
DOWN	vg484	VidyoGateway	172.16.4.84		3.0.0(96)	

At the bottom are buttons for Delete, Enable, and Disable.

- Double-click the **Status** on the VidyoProxy row.

The VidyoProxy Component Configuration is shown.

- Select the **General** tab.

- In the URL field:

- Enter a valid FQDN of the Vidyo Server on which the VidyoProxy is running.

The screenshot shows the Vidyo Components management interface with the 'General' tab selected for the VidyoProxy component. The component name is 'lvp'. The configuration fields are:

ID:	U7YH77X2RA5ZYFPAYPD7S9E5NTRP5W1XH71D52HW
Component Name:	lvp
URL:	yourrouter.yourcompany.com:443

At the bottom are 'Save' and 'Cancel' buttons.

- Click **Save**.

- Click **OK** to confirm your changes.

Verifying Your VidyoPortal Components are Online (Status: UP)

To verify your VidyoPortal components are Online (Status: UP):

1. Log in to the Super Admin portal using your Super Admin account.

For more information, see “Logging in to the Super Admin Portal” on page [35](#).

2. Click the **Components** tab.
3. Verify that all components are Online (Status UP) and have no alarms.

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	24 / 24	TAG_VC3_1_0_037	
UP	Local VM	VidyoManager	172.20.4.125	4 / 3	TAG_VC3_1_0_037	
UP	Local VP	VidyoProxy	172.20.4.125	10 / 0	TAG_VC3_1_0_037	
DOWN	vg484	VidyoGateway	172.16.4.84		3.0.0(96)	

4. Login to a User portal and place test calls to verify the VidyoPortal and components are functional.

Note:

- If your system includes VidyoRouters see “Enabling VidyoRouter Security” on page [127](#).
- For enabling HTTPS on your VidyoGateway and VidyoReplay, refer to respective security sections in *VidyoGateway* and *VidyoReplay Administrator Guides* available from the Vidyo Support Center at <http://support.vidyo.com>.

APPLYING VIDYOPORTAL SSL CERTIFICATES TO VIDYOROOMS

You may need to apply the VidyoPortal’s SSL root or full chain certificate to any VidyoRoom connected to the VidyoPortal.

Your VidyoRoom included a default bundle of common CA root and intermediate certificates. If you’re using a mainstream CA, the root and intermediate certificates may not be required to be uploaded to VidyoRoom systems you may have. Test each first to see if they connect successfully to the HTTPS only enabled VidyoPortal using the default bundled certificates.

If they do not connect, follow the steps in the next section to build the VidyoPortal full chain SSL certificate and apply it to your VidyoRoom.

Note: For VidyoGateways or VidyoReplays to connect using HTTPS, they each must also be configured to connect to the VidyoPortal via HTTPS. For more information, refer to the security sections in the *VidyoGateway* and *VidyoReplay Administrator Guides* in the Vidyo Support Center at <http://support.vidyo.com>.

Building the VidyoPortal Full Chain SSL Certificate

If your VidyoPortal SSL chain includes intermediates, you may need to create and upload the full chain certificate to the VidyoRoom, VidyoReplay and VidyoReplay Recorder.

An easy method to create the VidyoPortal 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 VidyoPortal using the Firefox browser using an HTTPS request:

https://<FQDN or IP>

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 to the left of the URL or the lower right corner of the Firefox window.
3. Click **View Certificate**.
4. Click the **Details** tab.
5. Click **Export**.
6. Browse to the location you wish to save the exported certificate.
7. From the Save as Type drop-down, select ‘X.509 Certificate with chain (PEM)’.
8. Enter a name for the file in the File Name field and click **Save**.
9. Rename the file as desired, save it with a **.crt** extension, and upload as necessary to your VidyoRoom and VidyoReplay Recorder accordingly.

IMPLEMENTING ENCRYPTION USING THE SECURED VIDYOCONFERENCING OPTION

Before configuring encryption using the Secured VidyoConferencing Option, you must first secure your VidyoPortal browsing by implementing SSL and enabling HTTPS.

For more information, see “Securing Your VidyoConferencing System with SSL and HTTPS” on page [301](#).

You also must secure the connections between the VidyoDesktop, VidyoRoom, VidyoManager, and VidyoRouters as explained in the component configuration procedures “Configuring Your Components to Work with HTTPS” on page [321](#) and “Configuring Each VidyoPortal Component to Use Your FQDN” on page [325](#) to fully encrypt and secure your VidyoConferencing system.

With all of these items completed, this section shows you how to verify your VidyoPortal is licensed for Encryption (as having the Secured VidyoConferencing Option), how to enable it on your VidyoConferencing system, and how to test it.

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 Your 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. Your VidyoPortal license must include the encryption option in order to be implemented.

To verify that the VidyoPortal is licensed for encryption:

1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Settings** tab.
3. Click **System License** on the left menu.
4. Scroll down to the Encryption line in the System License information section.

Feature	License
Encryption	128 Bits
MultiTenant	Enable
Allow UC Clients	Enable
License Serial Number	XXXXXXXXXX
Licensee Email	admin@vidyo.com

5. If Encryption is enabled in the VidyoPortal License, the setting reads **128 Bits**, otherwise it shows Disable.

Enabling Encryption on the VidyoConferencing System

Before configuring the encryption option (referred to as the Secured VidyoConferencing Option), you must first secure your VidyoPortal browsing by implementing SSL and enabling HTTPS in addition to other prerequisites mentioned at the beginning of this section. 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 VidyoPortal, please do so before using the following steps.

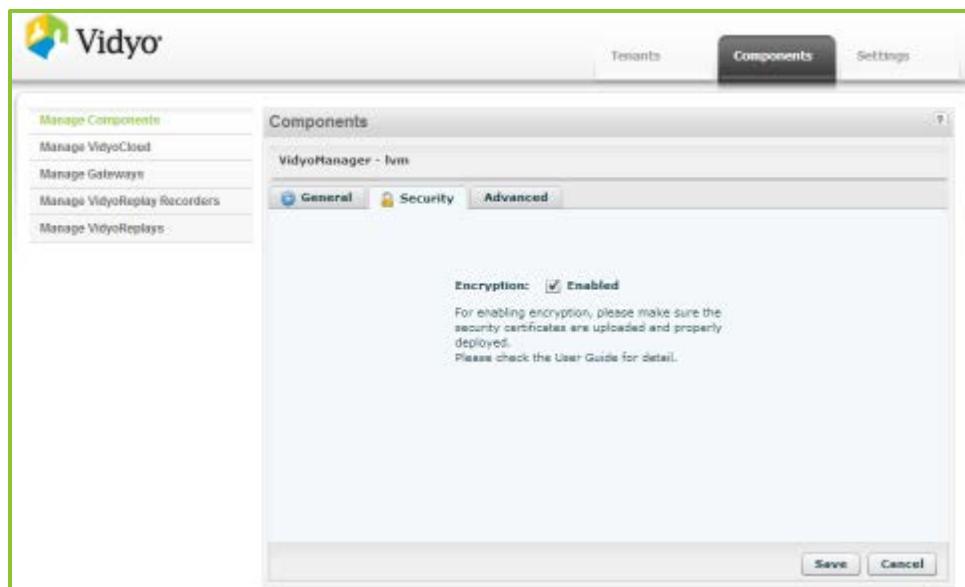
For more information, see “Implementing Encryption Using the Secured VidyoConferencing Option” on page [331](#).

To enable encryption for full signaling and media security:

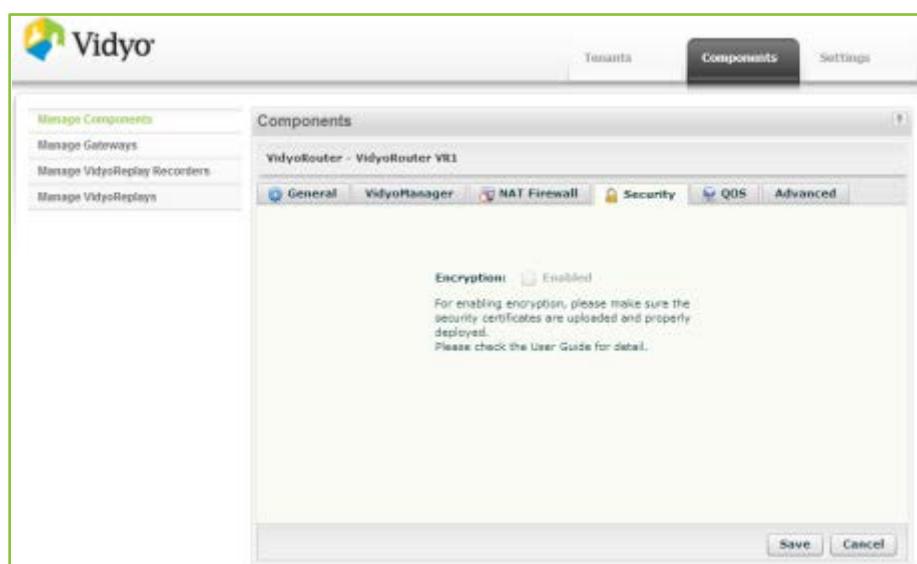
1. Log in to the Super Admin portal using your Super Admin account.
For more information, see “Logging in to the Super Admin Portal” on page [35](#).
2. Click the **Components** tab.

The Manage Components left menu item is selected by default.

3. Double-click **Status** on the VidyoManager entry.
4. Click the **Security** tab.
5. In the Encryption field, select the **Enabled** check box.



6. Click **Save**.
7. Click **OK** to confirm.
8. After returning to the Manage Components screen, double-click **Status** on the VidyoRouter entry.
9. Click the **Security** tab.
10. In the Encryption field, select the **Enabled** check box.



11. Click **Save**.

12. Click **OK** to confirm.
13. 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 clear alarms.)

Status	Name	Type	IP	Config Version	Software Version	Alarm
UP	VidyoRouter VR1	VidyoRouter	172.20.4.125	24 / 24	TAG_VC3_1_0_037	<input type="checkbox"/>
UP	Local VM	VidyoManager	172.20.4.125	4 / 3	TAG_VC3_1_0_037	<input type="checkbox"/>
UP	Local VP	VidyoProxy	172.20.4.125	10 / 0	TAG_VC3_1_0_037	<input type="checkbox"/>
DOWN	vg484	VidyoGateway	172.16.4.84		3.0.0(96)	<input type="checkbox"/>

Note:

- If your system includes VidyoRouters see “Enabling VidyoRouter Security” on page [127](#).
- For using HTTPS with VidyoGateway and VidyoReplay, refer to respective security sections in *Vidyo-Gateway* and *VidyoReplay Administrator Guides* available from the Vidyo Support Center at <http://support.vidyo.com>.
- For using encryption (referred to as the Secured VidyoConferencing Option) with VidyoGateway and VidyoReplay, refer to respective security sections in *VidyoGateway* and *VidyoReplay Administrator Guides* available from the Vidyo Support Center at <http://support.vidyo.com>.

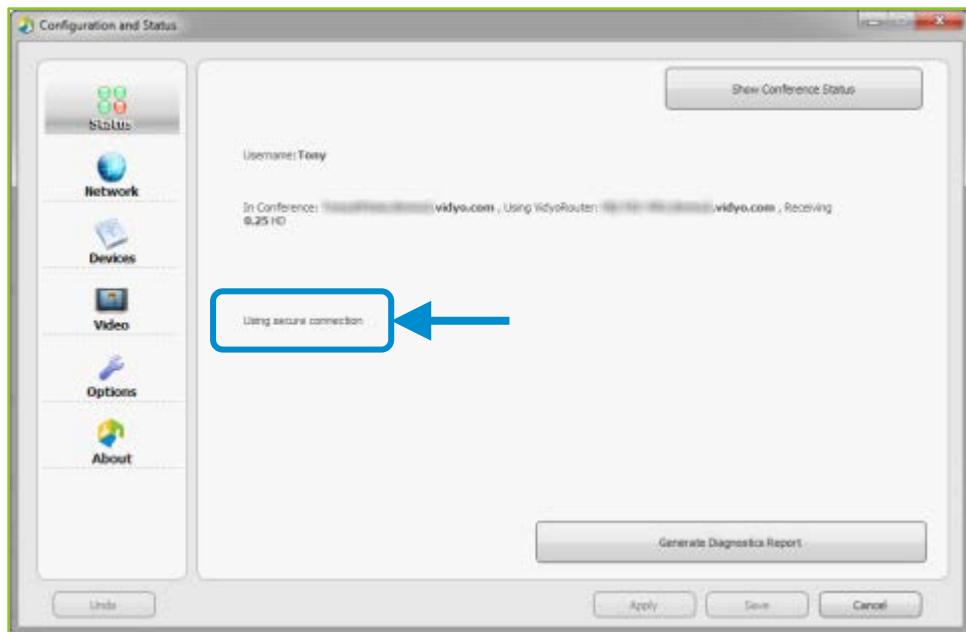
Testing the VidyoDesktop and Verifying Encryption

When you have finished configuring encryption (referred to as the Secured VidyoConferencing Option), you can confirm that you have a secure connection by performing the following steps.

To test the VidyoDesktop and verify encryption:

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 Configuration and Status page:



Appendix D. CDR

This appendix explains how to remotely access the CDR database, how to export and purge CDR files, and describes the schema, configuration, and access mechanisms for call detail records.

Before VidyoPortal version 2.2, the VidyoConferencing system saved call details records (CDRs) on installations, conferences, and point-to-point calls in three separate tables in CDRv1:

- The Client Installation Table (**ClientInstallation**) (Client installations).
- The Conference Call Table (**ConferenceCall**) (Every time a user joins or leaves a conference).
- The Point-to-Point Call Table (**PointToPoint**) (Every time a user makes a point-to-point call).

Version 2.2 and later uses CDRv2 or CDRv2.1, and maintains more information in just two tables:

- **ConferenceCall2**

The Conference Call Table and Point-to-Point Call Table were combined in a single table. Some fields were added, some deleted, and some changed.

- **ClientInstallations2**

The Client Installation Table also has new or changed fields.

In addition, the following features exist in the CDRv2 and CDRv2.1 tables:

- Recording CDR data is optional. It's turned off by default. If you've been recording it, you'll need to enable it after you upgrade to VidyoPortal version 2.2 or later.
- There's an option to purge CDR based on filter criteria. (This option is not available with CDRv1 and is, therefore, disabled on the CDR Access page of the Super Portal.)
- There's an option to export CDRs in CSV format based on filter criteria. (This option is not available with CDRv1 and is, therefore, disabled on the CDR Access page of the Super Portal.)
- Your filter can be based on Tenant Name or From or To date.
- 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 and Canada).
- You can change the time zone in the System Console. (You must be a Shell Admin user.)

As with the earlier tables, the call detail records are stored in a MySQL database on the VidyoPortal server. You need an SQL client to use the CDR database. Please refer to the SQL documentation for information on how to configure it.

Note: VidyoPortal version 2.3 and later does not support CDRv1. If you are using CDRv1 and VidyoPortal version 2.1 and earlier, you are advised to make changes to your CDR collection programs to migrate to CDRv2 or CDRv2 prior to upgrading to VidyoPortal version 2.3 or later. If you do not do so, you will no longer be able to collect CDR information from the VidyoPortal. If you are a Vidyo Reseller or Vidyo End User with "Plus" coverage, please feel free to contact the Vidyo Customer Support team via email with any questions or if you need assistance. If you are a Vidyo End User without "Plus" coverage, please contact your Vidyo Reseller for further details.

UNDERSTANDING CDR CONFIGURATION

The Call Detail Records (CDR) database resides on the same server as your VidyoPortal. Version 2.2 and later maintains more information than earlier versions in just two tables:

- **ConferenceCall2**

The Conference Call Table and Point-to-Point Call Table have been combined in a new single table. Some fields have been added, some deleted and some changed.

- **ClientInstallations2**

The new Client Installation Table also has new or changed fields.

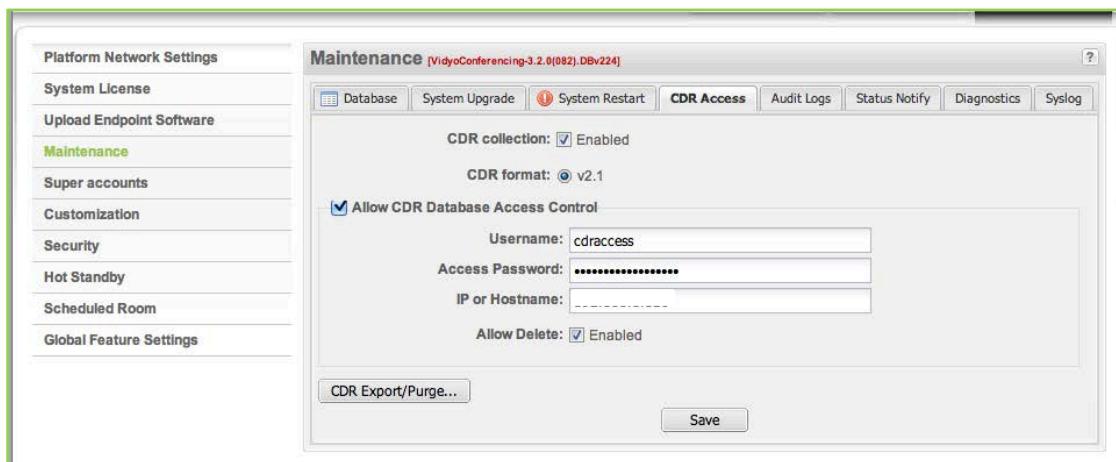
The VidyoPortal has been configured to allow remote MySQL clients to read and delete the details from all the tables within the CDR database.

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 VidyoConferencing 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.

The CDR access tab enables you to grant permission via the access password and host IP or hostname for the cdraccess user.



Configuring the CDR Database for Remote Access

You can configure the CDR database for remote access as the Super Admin.

For more information see “Configuring the CDR Database for Remote Access in the Super Admin Portal” on page [82](#).

Exporting and Purging CDR Files

The Super Admin may export and purge specific CDR records from the Super Admin portal while Admins may export CDR records from their specific tenant or tenants.

The export record limit is 65,000 records. If the export contains more than 65,000 records, a message appears warning you to restrict the range before proceeding with the download.

For more information, see “Exporting and Purging CDR Files from the Super Admin Portal” on page [83](#) and “Exporting CDR Files from the Admin Portal” on page [267](#).

CDR VERSION2.1 TABLES

ClientInstallations2

This table is used to record software installation.

Field	Description
Username	Login Name of user installing client software
DisplayName	Display name
TenantName	The Endpoint ID of a user’s host machine
EID	Endpoint identifier of a user’s host machine
ipAddress	IP address of machine where client software is installed
HostName	Host name of machine where client software is installed
RoomName	This field is populated for guest users and indicates which room they were trying to join that started the client software installation
RoomOwner	Room owner
TimeInstalled	Time of installation

ConferenceCall2

Note: Refer to this table when working with exported CDR file data.

Field	Description
CallID	Auto increment

Field	Description
UniqueCallID	A newly-created conference receives a new, unique call id so the customer can track all conference participants. For example, a conference “green” starting at 10 AM and ending at 11 AM has a different unique call ID from a conference “green” starting at 3 PM and ending at 4 PM.
ConferenceName	Name of the conference
TenantName	Name of the Tenant
ConferenceType	D – Direct Call (two party) C – Conference Call ID – Inter-portal Direct Call IC – Inter-portal Conference Call
EndpointType	R – VidyoRoom D – VidyoDesktop G – Guest L – Call to Legacy via VidyoGateway C – Call Recorded via VidyoReplay and Recorder (if applicable)
CallerID	Caller identifier [Login name of the caller] For Legacy Calls, this is the extension number used.
CallerName	Display Name of the Caller or name of the legacy device
JoinTime	Join time
LeaveTime	Leave time

Field	Description
Call State	<p>Current state of the call:</p> <ul style="list-style-type: none"> ■ RINGING – The status of the side initiating the call (P2P or conference). ■ RING ACCEPTED – This status indicates to the initiating side that the callee has accepted the call. It will switch to “in progress” once the conference begins. ■ RING REJECTED – This status indicates to the initiating side that the alert was not accepted. ■ RING NO ANSWER – This status indicates to the initiating side that the call timed out. ■ RING CANCELLED – This status indicates to the initiating side that the call was aborted from the initiating side. ■ ALERTING – The status indicates to the callee side that there is an incoming call (P2P or conference). ■ ALERT CANCELLED – This status indicates to the callee side that the initiating side cancelled the call. ■ IN PROGRESS – This status indicates to both sides that the call is in progress. ■ COMPLETED – This status indicates to both sides that the call was completed.
Direction	<p>I – Inbound Call</p> <p>O – Outbound Call</p>
RouterID	VidyoRouter used for this call.
GwPrefix	Service prefix used. This applies only to calls that involve a VidyoGateway or VidyoRecorder. For other calls it is set to NULL .
GwID	Gateway ID used for this call. Set to NULL otherwise.
ReferenceNumber	This is a numeric string identifier passed by the endpoint to the VidyoPortal at conference join time. This field is a placeholder for Client lib based apps implementation.

Field	Description
ApplicationName*	<p>This field identifies VidyoConference usage from different endpoint types. The information is reported by endpoints when connecting to the VidyoPortal.</p> <p>Usage is reported from the following endpoint types:</p> <ul style="list-style-type: none"> ■ VidyoWeb ■ VidyoMobile ■ VidyoSlate ■ Lync Plug-in ■ Jabber Plug-in ■ Bott client ■ VidyoMonitoring App ■ VidyoDesktop ■ VidyoRoom ■ VidyoGW ■ VidyoReplay ■ VDI
ApplicationVersion*	This field identifies the endpoint software version.
DeviceModel*	This field identifies the endpoint device model.
EndpointPublicIPAddress	This field identifies the IP address of an endpoint that has joined a conference.
AccessType	<p>U – Registered User</p> <p>G – Guest</p> <p>L – Call to Legacy via VidyoGateway</p> <p>R – Call Recorded via VidyoReplay and Recorder (if applicable)</p>
RoomType	<p>M – Private room belonging to a registered member on the VidyoPortal</p> <p>P – Public room</p> <p>S – Scheduled room</p>
RoomOwner	The logged in username of the room owner.

Field	Description
ApplicationOS*	This field identifies the operating system on which a Vidyo client is running. All VidyoClients (and Client lib based apps) are required to provide this information, if requested. The following operating systems are supported: <ul style="list-style-type: none"> ■ Windows XP ■ Windows7 ■ Windows8 ■ Mac OS ■ Linux ■ iOS ■ Android
CallCompletionCode	This field provides one of the following call completion codes: <p>0 – The call completion reason is not available</p> <p>1 – The user disconnected the call</p> <p>2 – The call was disconnected by the admin, operator, or room owner</p> <p>3 – The call was disconnected due to a network failure on the VidyoManager.</p>
EndpointGUID	This field captures the endpoint's GUID in the conference.

Note: Fields marked with an asterisk* on this table will be released and announced during upcoming endpoint releases.

Appendix E. Hot Standby

The Hot Standby feature is a Vidyo software option that must be purchased separately. To purchase the Hot Standby option, talk to your Vidyo sales representative.

The way you apply Vidyo FQDN-based licenses vary based on whether they are being applied when you are initially configuring both your system and the Hot Standby software option or you are applying add-on licenses to a system already synchronizing via the Hot Standby software option. For more information, see “Applying Add-on Licenses to a System Already Synchronizing via the Hot Standby Software Option” on page [67](#).

The Hot Standby option allows you to have a second VidyoPortal configured to take over in case your primary VidyoPortal is unreachable. The primary VidyoPortal is referred to as the Active VidyoPortal, and the other VidyoPortal is referred to as the Standby VidyoPortal.



Users who already have a VidyoPortal purchase an additional VidyoPortal and add it to their setup in order to leverage the Hot Standby option. Those who do not have an existing VidyoPortal install a brand new set-up consisting of two new VidyoPortals.

The two VidyoPortals should be physically close to each other. If not in the same server room, they should certainly be on the same subnet in the same hosting facility.

Note: Your Hot Standby software option may be used on a Virtual Vidyo Portal. For more information, see “Using the VidyoPortal and VidyoRouter Virtual Editions (VE)” on page [163](#).

AUTOMATICALLY AND MANUALLY TRIGGERING HOT STANDBY

When the Hot Standby feature is implemented correctly, the Standby VidyoPortal (VidyoPortal 1) becomes Active and the Active VidyoPortal (VidyoPortal 2) becomes the Standby when Hot Standby is triggered.



Hot Standby is triggered for the following reasons:

- **Manual Hot Standby** – You can force a Hot Standby from the Hot Standby > Operation screen in the Super Admin Portal.
- **Automatic Hot Standby** – A Hot Standby automatically takes place when the Active VidyoPortal is unreachable for 20 seconds.

Some additional reasons Hot Standby is automatically triggered include:

- An IP network failure of 30 seconds or more.
- A restart or shutdown of the Active VidyoPortal.
- A VidyoManager failure.
- A Web services failure.

Some reasons Hot Standby is not automatically triggered include:

- If a previously unreachable Standby VidyoPortal suddenly becomes reachable and operational, Hot Standby is not triggered and the currently Active VidyoPortal remains in service.
- Restarting Web services from the Super Admin Portal.

Note:

- A manual or automatic Hot Standby disconnects all conferences while switching between the Active and Standby VidyoPortals.
- In most cases, the manual and automatic Hot Standby switching process between VidyoPortals takes up to four minutes.

Synchronizing the VidyoPortal Database for Hot Standby

Since the Hot Standby option has your two VidyoPortals alternating between which one is Active and which one becomes the Standby, database information on each VidyoPortal must be kept synchronized.



Note:

- Whenever Hot Standby changes which VidyoPortal is Active and which one becomes the Standby, all database and Call Detail Records (CDR) changes since the last successful synchronization are lost. Therefore, Vidyo highly recommends setting automatic synchronizations and regular manual synchronizations in advance of Hot Standby triggers.
- If you are using the CDR database, do not let CDR entries accumulate. Instead, periodically access the CDR, collect the records, and then purge the database in order to optimize synchronizations. For more information about CDRs, see “CDR” on page [336](#).

CONFIGURING YOUR SETTINGS IN PREPARATION FOR HOT STANDBY

In order to prepare for Hot Standby, you must configure (or reconfigure) your VidyoPortal IP addresses and perhaps make some DNS settings as described in this section. When this is complete, you can then move on to setting the specific Hot Standby configuration values as explained in “Configuring Hot Standby” on page [350](#).

Setting IP and DNS Settings on VP1 and VP2

You must configure your IP Addresses and DNS settings for VP1 and VP2 (new or existing) using the System Console as described in “Configuring the Network Settings Using the System Console” on page [25](#).

Note:

- Remember that if you are adding a VidyoPortal to your existing setup in order to leverage the Hot Standby option, Vidyo strongly recommends that you change your VidyoPortal's existing, Native IP address and FQDN to new ones so the existing ones can be used as the Cluster IP address and FQDN.
- Always reboot machines after making any IP address and DNS changes.

Tip: As you proceed, print the page containing the title “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#) and write down specific IP address and FQDN values you designate for your VP1, VP2, and Cluster. Having this information handy makes the entire process easier.

Verifying Correct Installation of VidyoPortal Licenses with the Hot Standby Option

To use the Hot Standby feature, your organization must have a Hot Standby license. No third-party software is required.

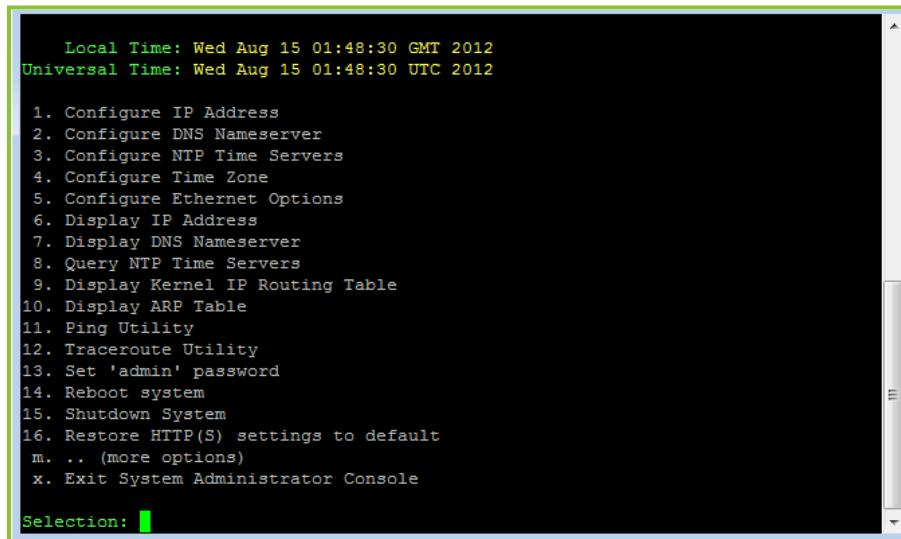
Your Hot Standby option comes with a license for each of your VidyoPortals. These two licenses are tied to specific system IDs and must be installed on the correct VidyoPortal based on the license file name (system ID). For more information, see “Requesting Vidyo System Licenses” on page [51](#) and “Applying the System License Keys to Your System” on page [52](#).

Use the following procedure to make sure you have correctly applied the VidyoPortal licenses with the Hot Standby option.

Note: You should plan in advance to perform the licensing and configuring of your VidyoPortals at the same time because uploading Hot Standby licenses on your VidyoPortals reduces the number of system licenses by 50% until the configuration is complete.

To verify correct installation of VidyoPortal licenses with the Hot Standby option:

1. Open a new System Console for VP1 using the Native IP address or FQDN.



```

Local Time: Wed Aug 15 01:48:30 GMT 2012
Universal Time: Wed Aug 15 01:48:30 UTC 2012

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 DNS Nameserver
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
m. ... (more options)
x. Exit System Administrator Console

Selection: 

```

2. Select **m. ... (more options)**.

```

System Administrator Console [TAG_VC2_2_0_138A]

Local Time: Wed Aug 15 01:49:52 GMT 2012
Universal Time: Wed Aug 15 01:49:52 UTC 2012

17. Configure Adobe Connect plugin
18. Display System ID
H. Hot Standby
b. ... (back to previous menu)

Selection: █

```

Note: System Console menu options are not case sensitive.

3. Verify that **H. Hot Standby** is displayed on the menu. If it is, the license for your Hot Standby option is applied correctly on VP1.

If desired, you may leave the VP1 System Console open.

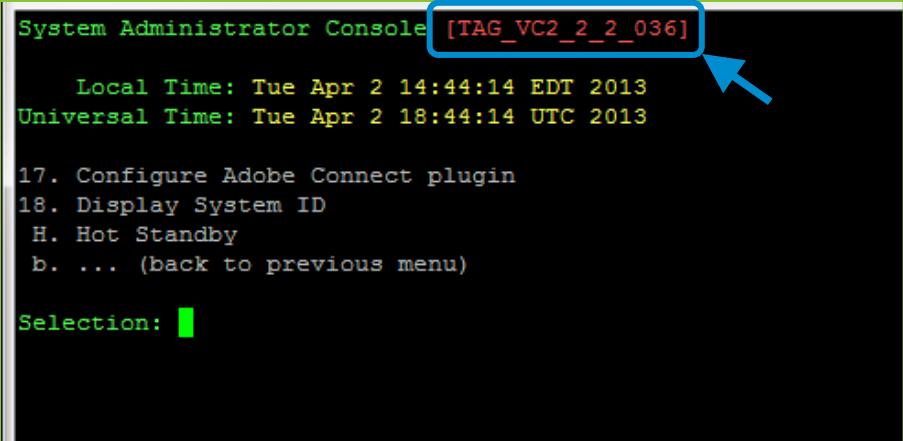
Note: If you do not see option H, review the steps for applying system license keys. For more information, see “Requesting Vidyo System Licenses” on page [51](#) and “Applying the System License Keys to Your System” on page [52](#).

Preparing the System Software and Database

After verifying your licenses, you must do the following to prepare for Hot Standby:

- Verify that the VidyoPortal software on VP1 and VP2 has the latest version and the same security patches applied.
 1. Open a new (or return to an already open) System Console for VP1 using the Native IP address or FQDN you designated for VP.
 2. From the main menu, select **m. ... (more options)**.

The software version is shown in red at the top of the System Console.



```
System Administrator Console [TAG_VC2_2_2_036]

Local Time: Tue Apr 2 14:44:14 EDT 2013
Universal Time: Tue Apr 2 18:44:14 UTC 2013

17. Configure Adobe Connect plugin
18. Display System ID
H. Hot Standby
b. ... (back to previous menu)

Selection: [
```

3. Confirm both of your machines are running the same software version.

If desired, you may leave the VP1 System Console open.

- Backup and download the database on the machine you're using as VP1. For more information, see "Performing System Maintenance" on page [72](#).

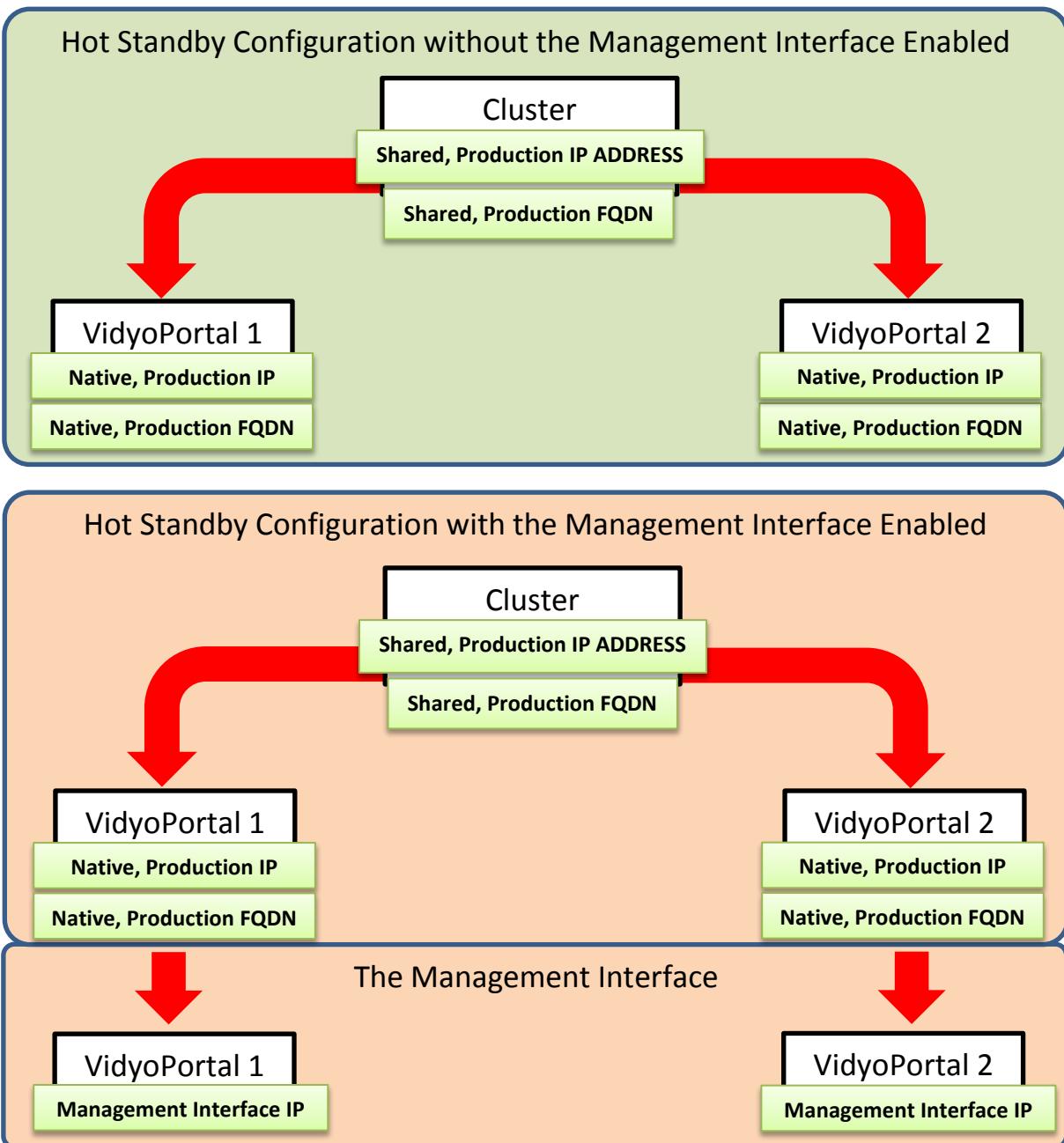
Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster

In order to implement Hot Standby, you need an IP address and FQDN for each of your VidyoPortals. You also need an IP address and FQDN for the Cluster.



When the Hot Standby option is used correctly, the Cluster IP and FQDN always direct traffic to the Active VidyoPortal. The Active VidyoPortal takes the Cluster IP and FQDN during Hot Standby activation.

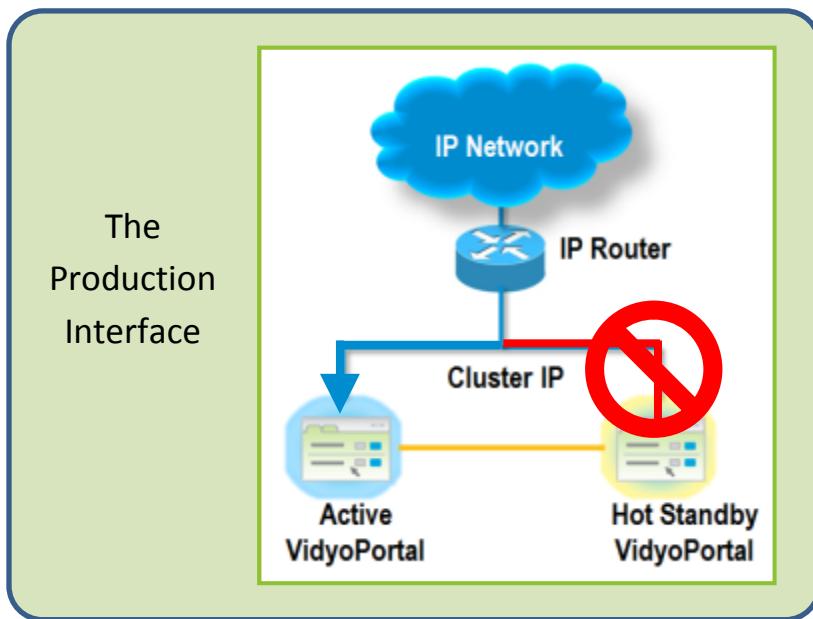
The following diagrams show Hot Standby system configurations both without and with the Management Interface enabled on your system:



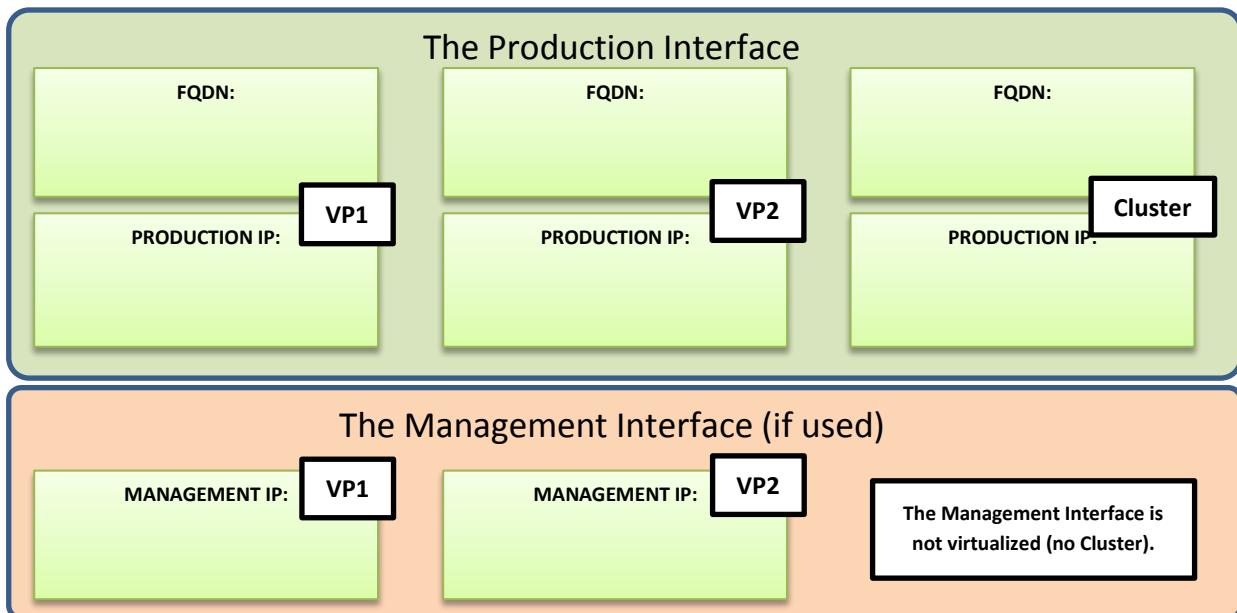
Note:

- The Management Interface IPs remain static and always accessible. There is no virtualization applied to them as done with the Cluster IP.
- The Management Interface is not virtualized; meaning, when using the Management Interface and Hot Standby changes which VidyoPortal is Active and which one becomes the Standby, no IP address virtualization takes place and respective Management Interface IPs remain unchanged.

The following diagram illustrates how your Hot Standby Cluster relates to the Active VidyoPortal:

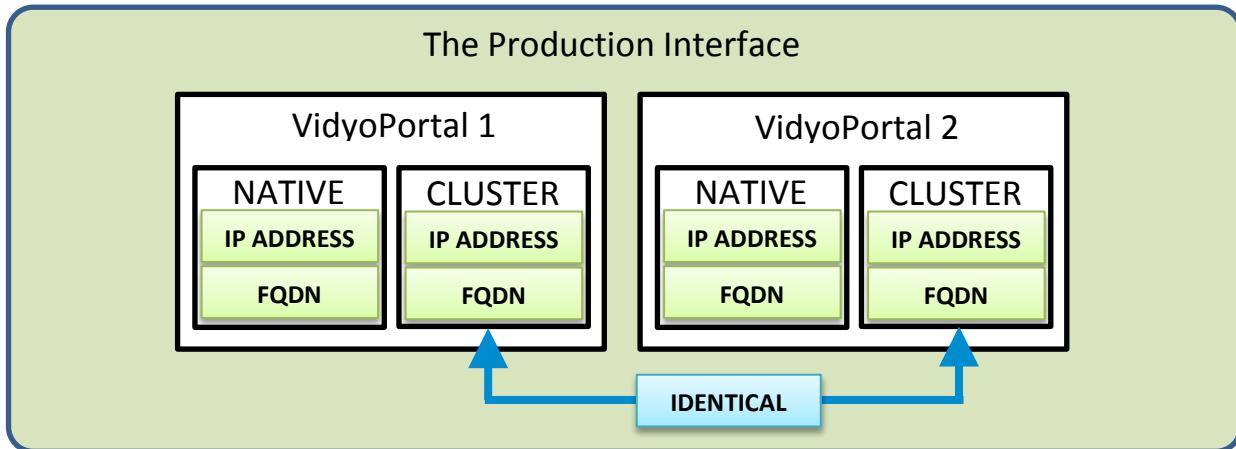


Tip: Prepare for configuring your Hot Standby setup by printing this page and writing down the specific IP and FQDN values you want for your VP1, VP2, and Cluster. You will need this information during various Hot Standby configuration procedures.



Note: If you are upgrading from VidyoPortal 2.x to 3.x and are now using FQDN licensing, your Public FQDNs and Cluster FQDNs on both of your VidyoPortals must be identical before upgrading.

The Hot Standby option creates the mechanism that allows for storing of both a Native IP address and FQDN and a Cluster IP address and FQDN on each of your VidyoPortals in the following manner:



Note:

- The Cluster IP address and FQDN are stored on both machines and are ready for use when the VidyoPortal is designated as the Active VidyoPortal.
- Remember if you are adding a VidyoPortal to your existing setup in order to leverage the Hot Standby option, Vidyo strongly recommends that you change your VidyoPortal's existing, Native IP address and FQDN to new ones so the existing ones can be used as the Cluster IP address and FQDN.
- Always reboot machines after making any IP address and DNS changes.

Ensuring that the Network IP Address Can Be Pinged

The network gateway or router IP address is also used during Hot Standby. Therefore, you must be able to ping this address from both the VP1 and VP2 VidyoPortals. For more information, see the Configure IP Address section of the "Configuring the Network Settings using the System Console" on page [25](#).

If you don't have a pool of existing IP addresses, you can purchase more from your ISP if you are using public IPs. In a NAT environment, you need one public IP address and three private IP addresses.

CONFIGURING HOT STANDBY

This section explains how to completely configure Hot Standby after you already read and completed the steps in all the subsection of the "Configuring Your Settings in Preparation for Hot Standby" section on page [344](#). In particular, ensure that you have configured your IP addresses and possibly DNS settings for VP1 and VP2 (new or existing) using the System Console as described in "Setting IP and DNS Settings on VP1, VP2" on page [344](#).

In addition, you should be familiar with this terminology:

- **VP1** – Generically refers to the VidyoPortal machine you are designating as VP1 and configuring for Hot Standby use. This is regardless as to whether you're using an existing VidyoPortal as VP1 for

your Hot Standby configuration and you purchased a second VidyoPortal to use as VP2, or if you purchased two new VidyoPortals to use for Hot Standby.

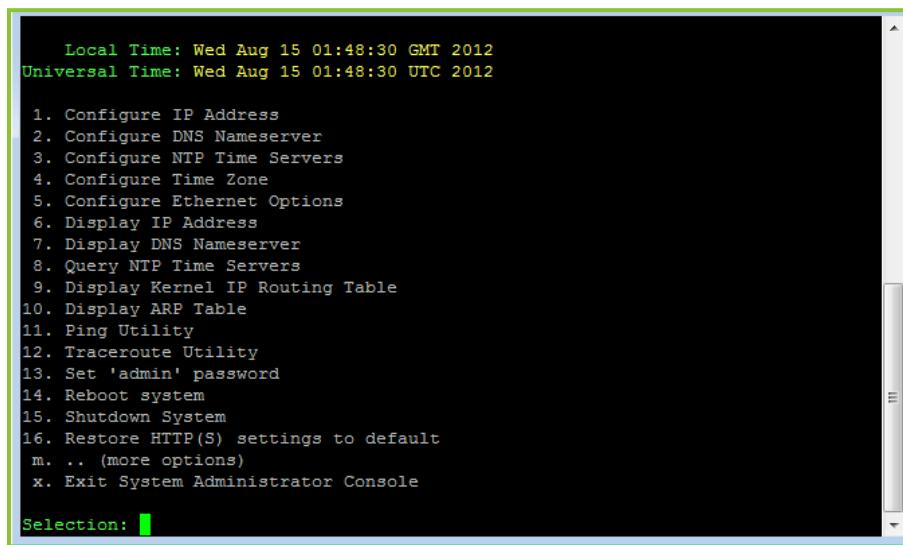
- **VP2** – Generically refers to the VidyoPortal machine you are designating as VP2 and configuring for Hot Standby use.
- **Cluster** – Refers to the Cluster IP and FQDN, which always will direct traffic to the Active VidyoPortal.
- **Active VidyoPortal or Standby VidyoPortal** – For procedures where the status of the VidyoPortal with respect to Hot Standby is the main focus, references may simply indicate the Active VidyoPortal or the Standby VidyoPortal where necessary.

Setting Hot Standby Configuration Values on VP1

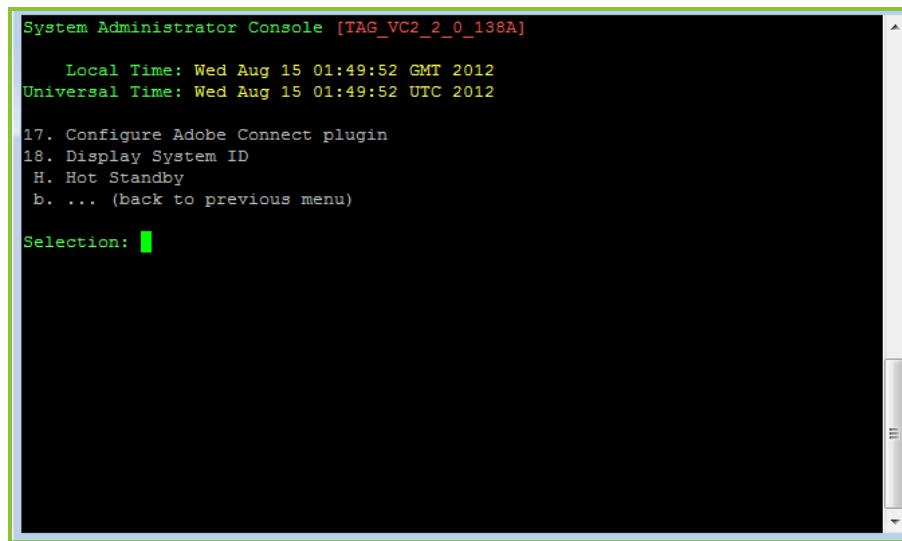
To set the Hot Standby configuration values on VP1:

1. Open a new System Console for VP1 using the Native IP address or FQDN.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).



2. From the main menu, select **m. . . (more options)**.



```
System Administrator Console [TAG_VC2_2_0_138A]

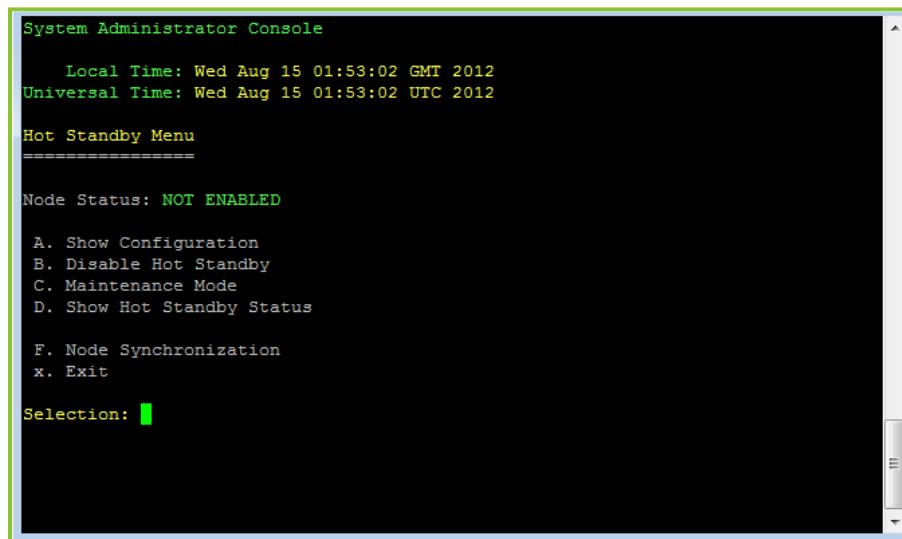
Local Time: Wed Aug 15 01:49:52 GMT 2012
Universal Time: Wed Aug 15 01:49:52 UTC 2012

17. Configure Adobe Connect plugin
18. Display System ID
H. Hot Standby
b. ... (back to previous menu)

Selection: █
```

Note: System Console menu options are not case sensitive.

3. Select **H. Hot Standby**.



```
System Administrator Console

Local Time: Wed Aug 15 01:53:02 GMT 2012
Universal Time: Wed Aug 15 01:53:02 UTC 2012

Hot Standby Menu
=====

Node Status: NOT ENABLED

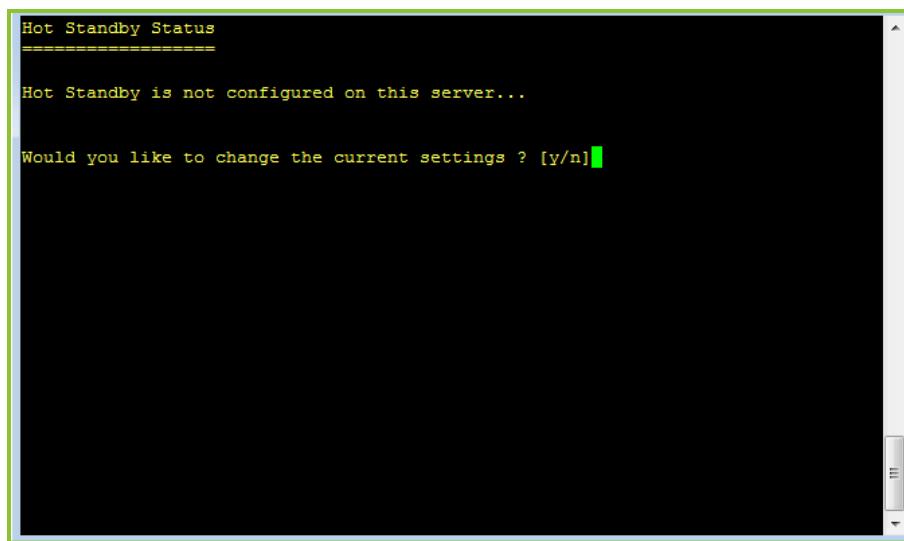
A. Show Configuration
B. Disable Hot Standby
C. Maintenance Mode
D. Show Hot Standby Status

F. Node Synchronization
x. Exit

Selection: █
```

4. Select **A. Show Configuration**.

The Hot Standby Status screen appears.

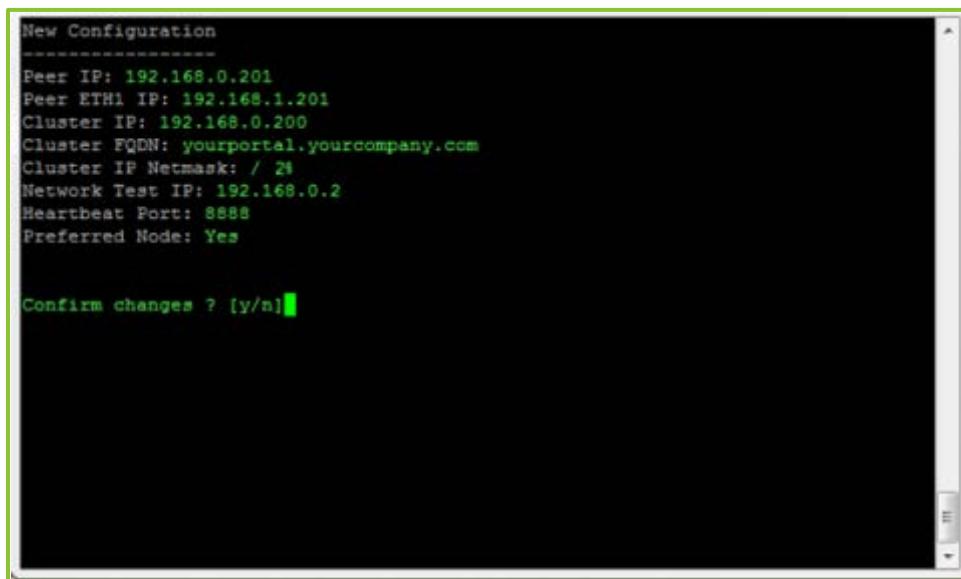


```
Hot Standby Status
=====
Hot Standby is not configured on this server...

Would you like to change the current settings ? [y/n]
```

5. Select **y**.

The New Configuration screen appears.



```
New Configuration
-----
Peer IP: 192.168.0.201
Peer ETH1 IP: 192.168.1.201
Cluster IP: 192.168.0.200
Cluster FQDN: yourportal.yourcompany.com
Cluster IP Netmask: / 24
Network Test IP: 192.168.0.2
Heartbeat Port: 8888
Preferred Node: Yes

Confirm changes ? [y/n]
```

Using the IP and FQDN values you designated for your VP1, VP2, and Cluster in the “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#), enter the following information on the System Console New Configuration screen:

- **Peer IP** – The IP address of the other VidyoPortal (sometimes referred to as the “peer” or “partner” VidyoPortal). Enter VP2’s IP address.

Note: The Peer IP, Cluster IP, and IP address of VP1 must be unique.

- **Peer ETH1 IP** – If your Management Interface is configured, you are prompted for your Peer ETH1 IP. This is the IP of the VP2 Management Interface.

- **Cluster IP** – This is a shared IP address used for the VidyoPortal (VP1 or VP2) activated by Hot Standby. Configure your Cluster IP value for VP1 based on the following:
 - If you are adding a VidyoPortal to your existing setup in order to leverage the Hot Standby option, you are strongly urged to change your VidyoPortal's existing, Native IP address to a new one so the existing one can be used as the Cluster IP. Having the Cluster IP address match the one on your current VidyoPortal keeps you from having to change your DNS and other network configuration settings. Vidyo specifically recommends this method if you are adding a VidyoPortal to your existing setup in order to leverage the Hot Standby option.
 - When configuring both VidyoPortals, one must be selected as the preferred server. This preferred machine initially assumes the Cluster IP address.

Note: When one of your VidyoPortals (VP1 or VP2) becomes the Active VidyoPortal, Hot Standby automatically has that machine use the Cluster IP address and makes the Native IP address unreachable.

- **Cluster FQDN** – The shared FQDN used for the VidyoPortal (VP1 or VP2) activated by Hot Standby.

Note: This is the same value as your Public FQDN as set when you select **1. Configure IP Address**. For more information, see “Configuring the Network Settings at the System Console” on page [25](#).

Configure your Cluster IP value for VP1 based on the following:

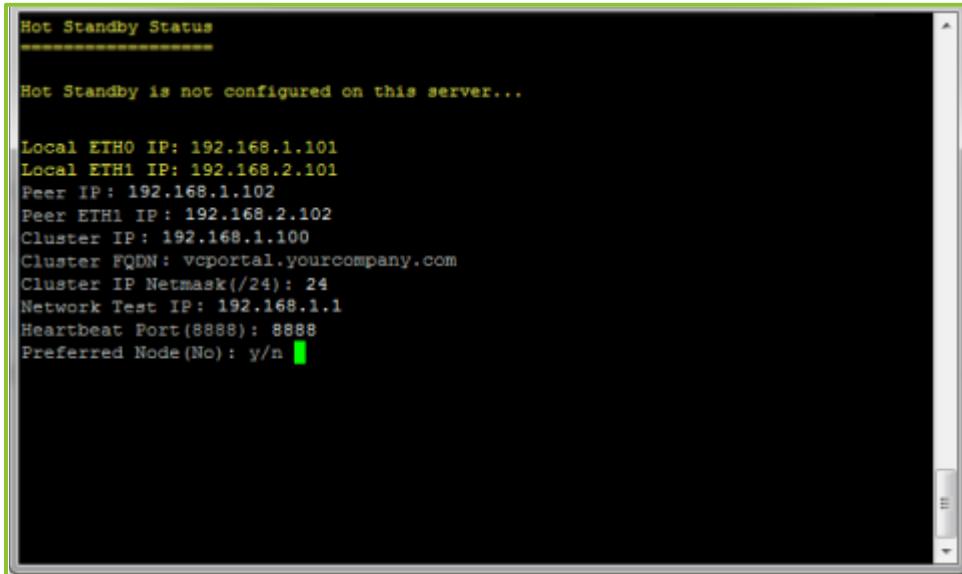
- If you are adding a VidyoPortal to your existing setup in order to leverage the Hot Standby option, you are strongly urged to change your VidyoPortal's existing, Native FQDN to a new one so the existing one can be used as the Cluster FQDN. Having the Cluster FQDN match the one on your current VidyoPortal keeps you from having to change your DNS and other network configuration settings. Vidyo specifically recommends this method if you are adding a VidyoPortal to your existing setup in order to leverage the Hot Standby option.
- When configuring both VidyoPortals, one must be selected as the preferred server. This preferred machine initially assumes the Cluster FQDN address.
- **Cluster IP Netmask** – The netmask for the subnet. You must enter this in the slash format; however, you don't have to enter the slash. For example, if the cluster IP netmask is 255.255.255.0, you should enter **24**, but onscreen you'll see **/24**.
- **Network Test IP** – The external IP address for validating IP connectivity. You should be able to ping this IP address. Vidyo recommends using the VidyoPortal's network gateway IP address. For more information, see the Configure IP Address section of the “Configuring the Network Settings using the System Console” on page [25](#).
- **Heartbeat Port** – This is a port used by both of your VidyoPortal machines (VP1 and VP2) to check each other's availability and check if services are running in order to know when it's necessary to assume the role of the Active VidyoPortal. Any available port may be used, but Vidyo recommends using port 8888.

Note: You must make sure port 8888 (or whichever port decided to use) is open between your VidyoPortal machines (VP1 and VP2).

- **Preferred Node** – This configuration determines which VidyoPortal (VP1 or VP2) becomes the Active one when both machines are initialized. The setting on one machine should be **Yes** and the other should be **No**.

Note:

- Upon subsequent rebooting of VidyoPortal machines, the status is based on this Preferred Node setting and assumes the Active for **Yes** and Standby for **No**.
- If you already had one VidyoPortal and you purchased a second one to use for Hot Standby, you should answer **Yes** for the VidyoPortal you already have and are upgrading, and **No** for the new one. If, on the other hand, you purchased two new VidyoPortals, you can answer **Yes** or **No** for either VidyoPortal as long as you have one of each.



```

Hot Standby Status
-----
Hot Standby is not configured on this server...

Local ETH0 IP: 192.168.1.101
Local ETH1 IP: 192.168.2.101
Peer IP : 192.168.1.102
Peer ETH1 IP : 192.168.2.102
Cluster IP : 192.168.1.100
Cluster FQDN: vcportal.yourcompany.com
Cluster IP Netmask(/24): 24
Network Test IP: 192.168.1.1
Heartbeat Port(8888): 8888
Preferred Node(No) : y/n

```

6. Select **y** to confirm the changes.

If desired, you may leave the VP1 System Console open as you continue to the next procedure.

Rebooting to Apply the New Hot Standby Configuration Values on VP1

To apply the new Hot Standby configuration values on VP1, reboot the machine using the following steps:

1. Open a new (or return to an already open) System Console for VP1 using the Native IP address or FQDN you designated for VP.
2. From the main menu, select **14. Reboot System**.

Note: Wait until the machine has completely rebooted before proceeding.

If desired, you may leave the VP1 System Console open as you continue to the next procedure.

Verifying VP1 Functionality

To verify VP1 functionality:

1. Access the Super Admin portal of your Active VidyoPortal using the Cluster IP address or FQDN. For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

Note:

- You must use the Cluster IP address or FQDN to access VP1 because its Active status deactivates the native IP address.
 - Refer to the specific IP address and FQDN values you designated for your VP1, VP2, and Cluster in the “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).
2. Verify that the appropriate Vidyo components and licenses appear.
 3. Place a test call.

If desired, you may leave the Super Admin portal for your Active VidyoPortal open.

Setting Hot Standby Configuration Values on VP2

Perform the steps from the following sections to set Hot Standby configuration values on VP2.

To set the Hot Standby configuration values on VP2:

1. “Setting Hot Standby Configuration Values on VP1” on page [351](#).
2. “Rebooting to Apply the New Hot Standby Configuration Values on VP1” on page [355](#).
3. After rebooting VP2, the machine will be in Standby mode. You must then do the following:
 - a. Generate and import the security keys on VP1 and VP2.
For more information, see “Generating and Importing the Security Keys” on page [357](#).
 - b. Perform a database synchronization on VP1.
For more information, see “Triggering the First Database Synchronization from VP1” on page [363](#).
 - c. Force VP2 in to Active mode by accessing VP1 and forcing it in to Standby mode.
For more information, see “Forcing the Active VidyoPortal into Standby Mode from the Super Admin Portal” on page [368](#) or “Forcing a Hot Standby from the System Console on Your Active VidyoPortal” on page [372](#).

Note: If you put your Standby VidyoPortal in to Maintenance mode, the Settings > Hot Standby screens do not appear when accessed via the Internet Explorer Web browser.
4. “Verifying VP1 Functionality” on page [356](#).

Note:

- Verify your VP2 functionality by performing a controlled test where you force a Hot Standby, make your VP2 the Active VidyoPortal, and place a test call. You can force a Hot Standby from the Super Admin portal using “Forcing the Active VidyoPortal into Standby Mode” on page [368](#) or from the System Console using “Forcing a Hot Standby on your Active VidyoPortal” on page [372](#).
- For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).
- Proceed only after you’ve configured both VP1 and VP2 and rebooted both machines. One machine has an Active status while the other has a Standby status.

Generating and Importing the Security Keys

Each VidyoPortal generates its own unique security key (unrelated to CA certificates) for sharing with the other VidyoPortal in your Hot Standby setup. This section shows you how use the System Console to generate this key for copying and pasting to your other VidyoPortal.

Alternatively, you can generate the key using the System Console and import it using the Super Admin Portal. For more information, see “Importing a Security Key” on page [369](#).

To generate and import the security keys:

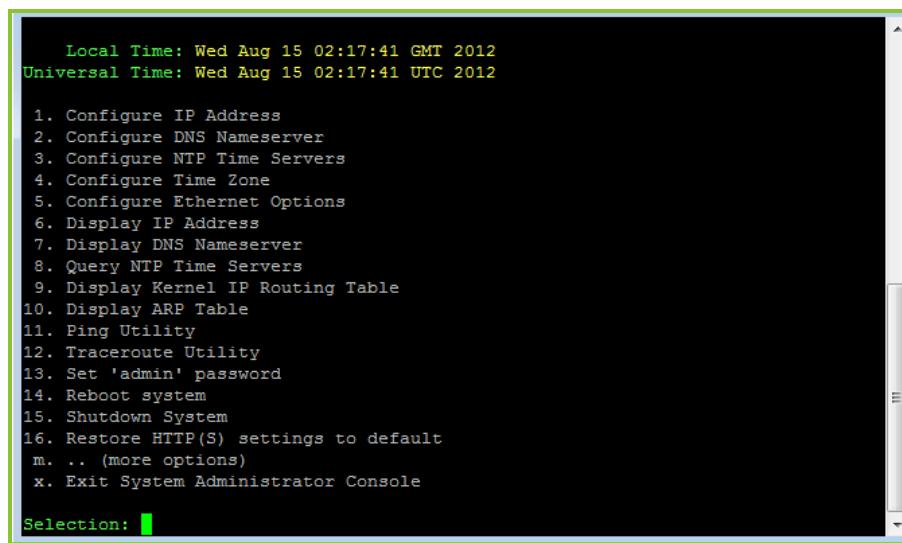
1. Open a new (or return to an already open) System Console and access VP1 using the Cluster IP address or FQDN you designated for VP1.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

Note:

- You must use the Cluster IP address or FQDN to access the Active Vidyo Portal. Its Active status disables the native IP address.
- Refer to the specific IP address and FQDN values you designated for your VP1, VP2, and Cluster in the “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

2. From the main menu, select **m. . . (more options)**.



```
Local Time: Wed Aug 15 02:17:41 GMT 2012
Universal Time: Wed Aug 15 02:17:41 UTC 2012

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 DNS Nameserver
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
m. . . (more options)
x. Exit System Administrator Console

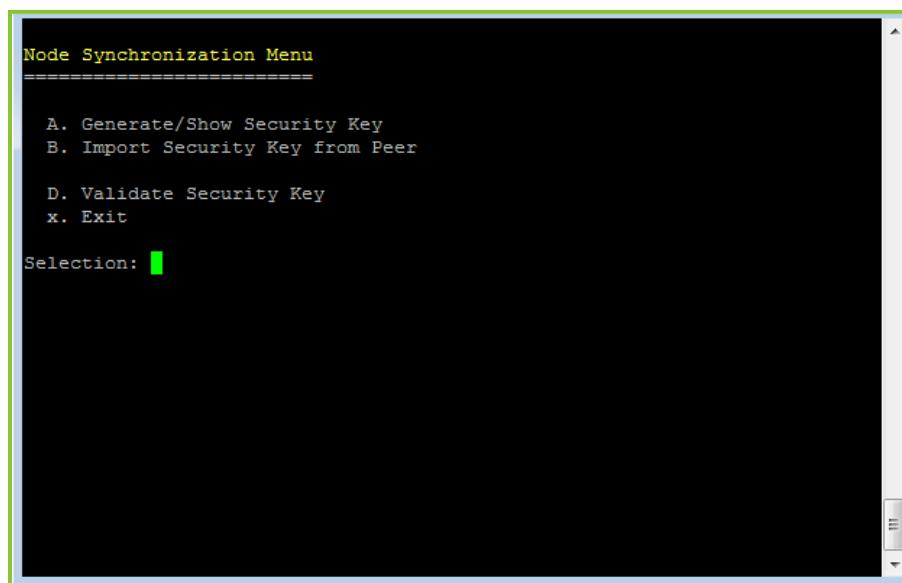
Selection: [
```

3. Select **H. Hot Standby**.

Note: Even though it's not visible on the main menu, you can select **H. Hot Standby**.

4. Select **F. Node Synchronization**.

The Node Synchronization Menu appears.



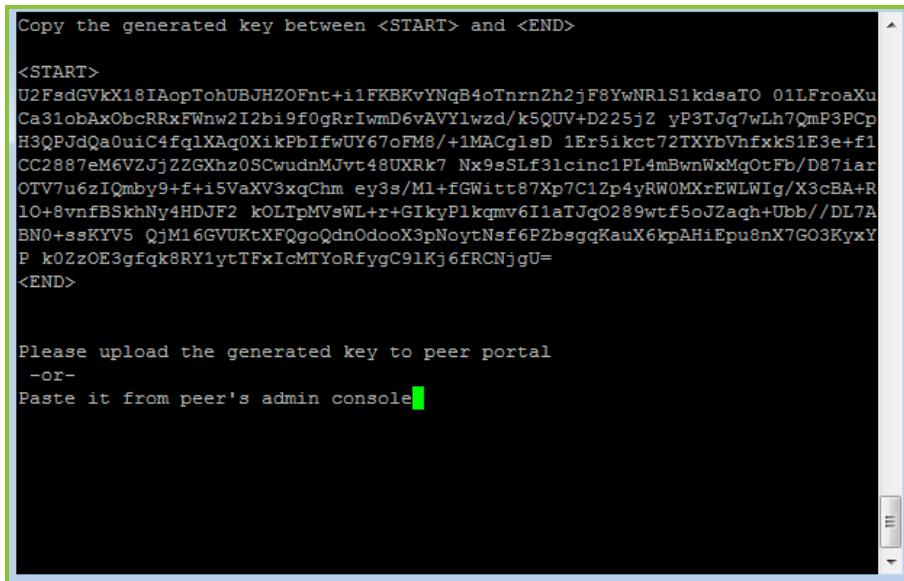
```
Node Synchronization Menu
=====
A. Generate>Show Security Key
B. Import Security Key from Peer
D. Validate Security Key
x. Exit

Selection: [
```

5. Select **A. Generate>Show Security Key**.

6. Select **y** to confirm the key generation.

The system generates a security key for VP2.



```

Copy the generated key between <START> and <END>

<START>
U2FsdGVkX18IAopTohUBJHZOFnt+i1FKBKvYNqB4oTnrvZn2jF8YwNRlS1kdsTO 01LFroaXu
Ca31obAxObcRRxFWnw2I2bi9f0gRrIwmD6vAVYlwzD/k5QUV+D225jZ yP3TJq7wLh7QmP3PCp
H3QPJdQa0uiC4fq1XAq0XikPbIfwUY67oFM8/+1MACglsD 1Er5ikct72TXYbVhfxkS1E3e+f1
CC2887eM6VZJjZZGXhz0SCwudnMjvt48UXRk7 Nx9sSLf3lcinc1PL4mBwnWxMqOtFb/D87iar
OTV7u6zIQmby9+f+i5VaXV3xqChm ey3s/M1+fGWitt87Xp7C1Zp4yRWOMXrEWLWig/X3cBA+R
1O+8vnfBSkhNy4HDJF2 k0LTpMVsWL+r+GIkyPlkqmv6IIiaTJq0289wtf5oJZagh+Ubb//DL7A
BN0+ssKYV5 QjM16GVUKtXFQgoQdn0dooX3pNoytNsf6PZbsggKauX6kpAHiEpu8nX7GO3Kyxy
P k0ZzOE3gfqk8RY1ytTFxIcMTYoRfygC91Kj6fRCNjgU=
<END>

Please upload the generated key to peer portal
-or-
Paste it from peer's admin console

```

7. Copy the key.

Note:

- Use your mouse to highlight the key text shown in the System Console. This automatically copies the selection to your clipboard.
- Exclude the words <START> and <END> when copying the key.

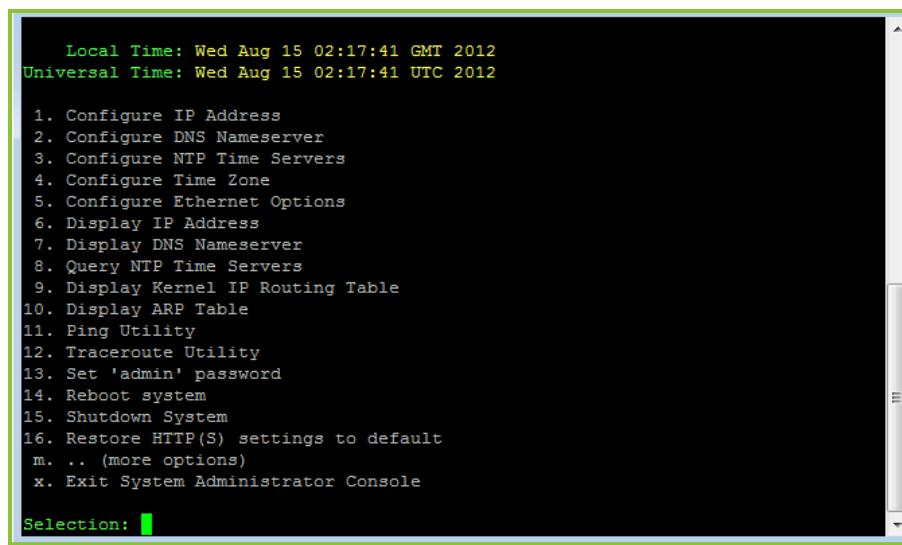
8. Press **Enter** to stop viewing the key.

9. Select **x** and exit the VP1 System Console.

10. Open a new (or return to an already open) System Console for VP2 using the native IP address or FQDN you designated for VP2.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

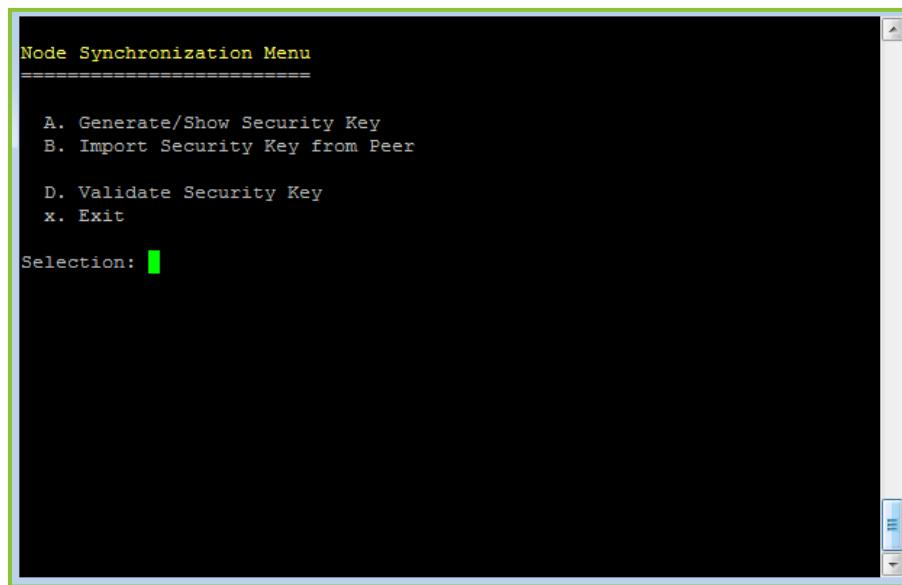
11. From the main menu, select m. . . (more options).



12. Select H. Hot Standby.

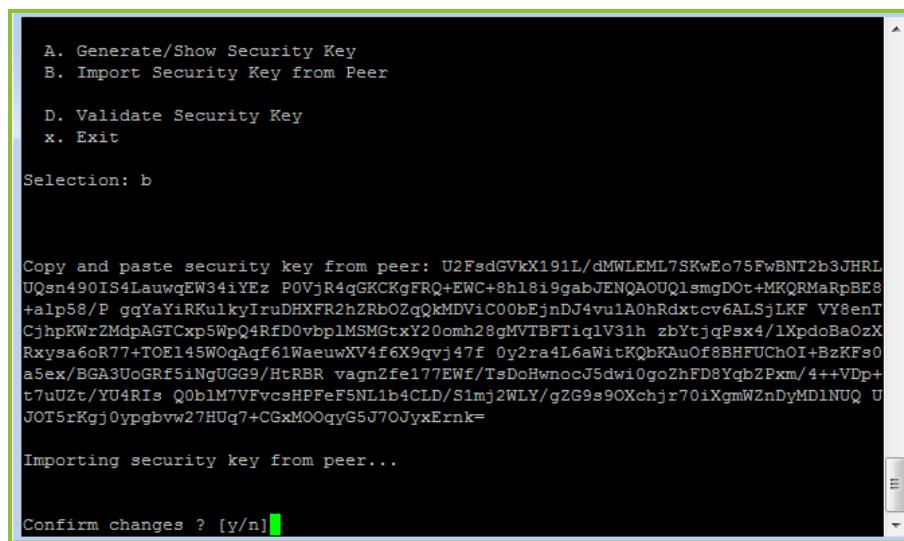
Note: Even though it's not visible on the main menu, you can select H. Hot Standby.

13. Select F. Node Synchronization.



14. Select B. Import Security Key from Peer.

- 15.** Paste the key (generated from VP1) here on VP2.



The screenshot shows a command-line interface in a System Console window. The menu bar includes 'File', 'Edit', 'View', 'Help', and 'System'. The main area displays a list of options:

- A. Generate/Show Security Key
- B. Import Security Key from Peer
- D. Validate Security Key
- x. Exit

Below the menu, the text 'Selection: b' is displayed. The console output shows the following text:

```
Copy and paste security key from peer: U2FsdGVkX191L/dMWLEMl7SKwEo75FwBNT2b3JHRL
UQsn490IS4LauwgEW34iYEz POVjR4qGKCKgFRQ+EWC+8h18i9gabJENQAOUQ1smgD0t+MKQRMaRpBE8
+alp58/P gqYaYiRKulkyIruDHXR2hZRbOZqQkMDViC00bEjnDj4vu1A0hRdxtcv6ALSjLKF VY8enT
CjhpKWrZMdpAGTCxp5WpQ4rfD0vbplMSMGtxY20cmh28gMVIBFTlqlV31h zBYtjqPsx4/lXpdoBaOzX
Rxysa6oR77+TOE145WOqAqf61WaeuwXV4f6X9qvj47f 0y2ra4L6aWitKQbKAuOf8BFUChOI+BzKFs0
a5ex/BGA3UcGRF5iNgUGG9/HtRBR vagnZfe177EWf/TsDohwnocJ5dw10gozhFD8YqbZPxm/4++VDp+
t7uUzt/YU4RIs Q0b1M7VFvcsHPFeF5NL1b4CLD/S1mj2WLY/gZG9s9OXchjr70iXgmWZnDyMD1NUQ U
JOT5rKgj0ypgbvw27HUq7+CGxMOOqyG5J70JyxErnk=
```

Below the output, the text 'Importing security key from peer...' is shown. At the bottom of the window, the prompt 'Confirm changes ? [y/n]' is visible.

- 16.** Select **y** to confirm your changes.

So far you've copied VP1's key to VP2. While you're here in VP2, generate a key for copying to VP1 before validating both keys.

- 17.** Select **A. Generate/Show Security Key**.

- 18.** Copy the key.

Note:

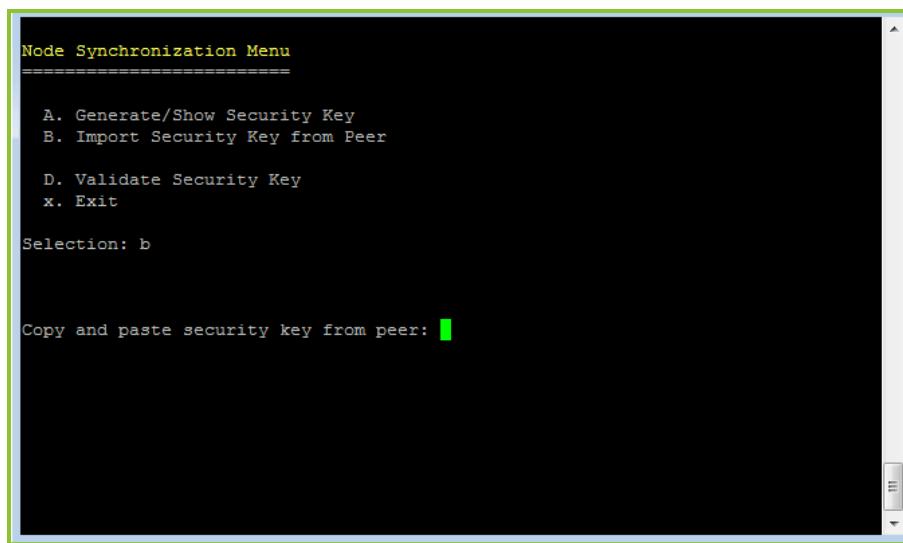
- ▀ Use your mouse to highlight the key text shown in the System Console. This automatically copies the selection to your clipboard.
- ▀ Exclude the words <START> and <END> when copying the key.

If desired, you may leave the VP2 System Console open as you continue to the next procedure.

- 19.** Open a new (or return to an already open) System Console for VP1 using the native IP address or FQDN you designated for VP1.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

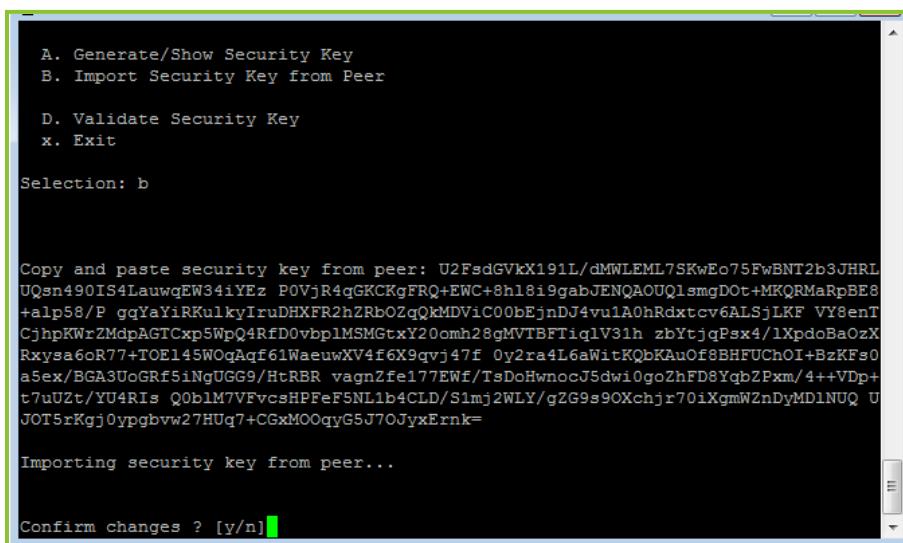
- 20.** Select menu choices **m > H > F** to access VP1's Node Synchronization Menu.



- 21.** Select **B. Import Security Key from Peer**.

- 22.** Paste the key (generated from VP2) here on VP1.

Note: Use your mouse to right-click and paste the key text in to the VP1 System Console.



- 23.** Select **y** to confirm your changes.

- 24.** Press any key.

If desired, you may leave the VP1 System Console open as you continue to the next procedure.

Validating the Security Keys

Continue your Hot Standby configuration by validating the security keys on VP1 and VP2.

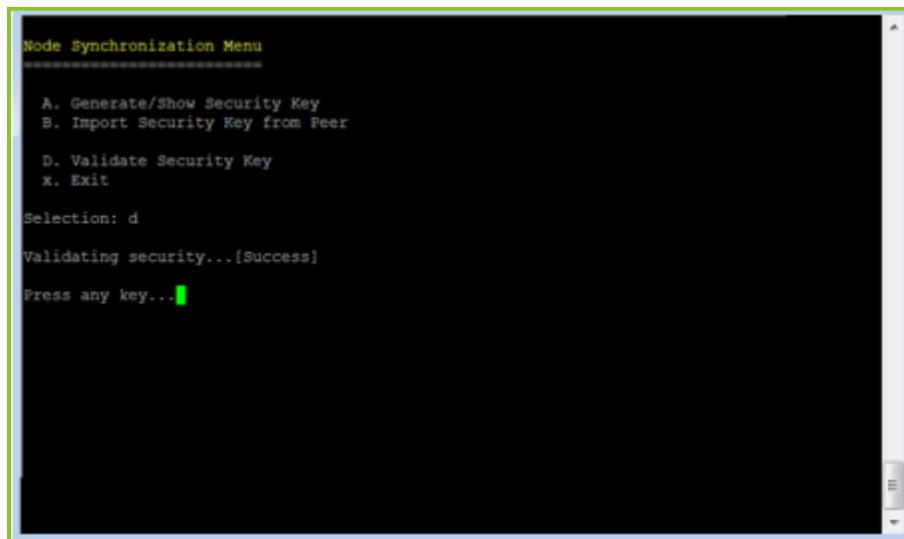
To validate the security keys:

1. Open a new (or return to an already open) System Console for VP1 using the Cluster IP address or FQDN.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

2. From the System Console Node Synchronization menu on VP1, select **D. Validate Security Key**.

The message **Validating security...[Success]** appears indicating that VP1 has validated the security key from VP2.



3. Press any key.

If desired, you may leave the VP1 System Console open as you continue to the next step.

4. Open a new (or return to an already open) System Console for VP2 using the Native IP address or FQDN.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

5. From the main menu, select choices **m > H > F** to access VP2’s Node Synchronization Menu.
6. Select **D. Validate Security Key**.

The message **Validating security...[Success]** appears indicating that VP2 has validated the security key from VP1.

If desired, you may leave the VP2 System Console open as you continue to the next procedure.

Triggering the First Database Synchronization from VP1

Continue your Hot Standby configuration by triggering the first database synchronization from VP1.

To trigger the first database synchronization from VP1:

1. Open a new (or return to an already open) System Console for VP1 using the Cluster IP address or FQDN.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

2. From the main menu, select choices **m > H > F** to access VP1’s Node Synchronization Menu.
3. On the Node Synchronization Menu, select **C. Create DB Snapshot**.

This triggers the initial database synchronization from VP1.

If desired, you may leave the VP1 System Console open as you continue to the next procedure.

Verifying the Node Status on VP1 and VP2

Continue your Hot Standby configuration by verifying the status of each node on VP1 and VP2.

To verify the node status on VP1 and VP2:

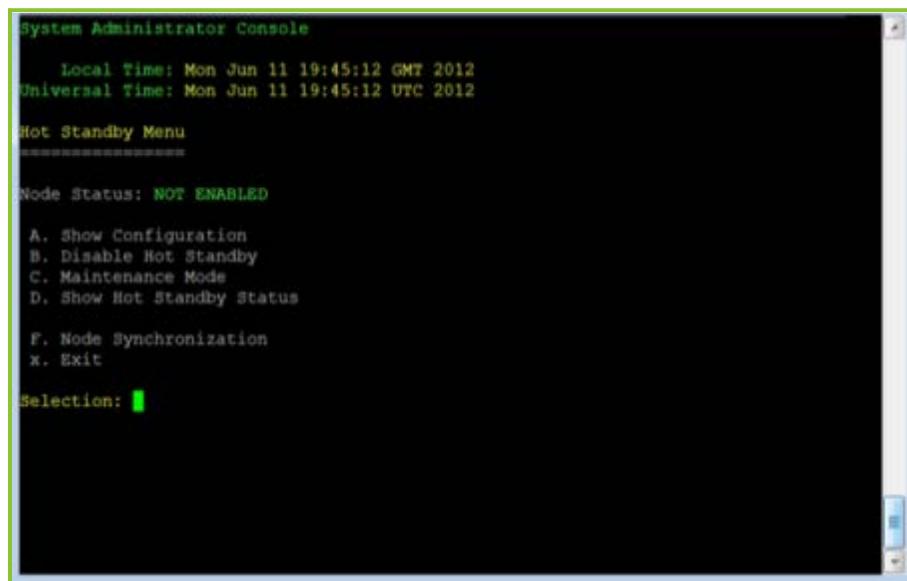
1. Open a new (or return to an already open) System Console for VP1 using the Cluster IP address or FQDN.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

2. From the main menu, select choices **m > H** to access VP1’s Hot Standby Menu.
3. Select **D. Show Hot Standby Status**.

Note:

- One server must show as ACTIVE and the other as STANDBY in your Hot Standby configuration.
- Other statuses include NOT ENABLED and MAINTENANCE.



4. Select **x** and exit the VP1 System Console.
5. Open a new (or return to an already open) System Console for VP2 using the Native IP address or FQDN.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

6. From the main menu, select **m > H** to access VP2’s Hot Standby Menu.
7. Select **D. Show Hot Standby Status**.

Note:

- One server must show as ACTIVE and the other as STANDBY in your Hot Standby configuration.
- Other statuses include NOT ENABLED and MAINTENANCE.

8. Select **x** and exit the VP2 System Console.

Scheduling the Database Synchronization

By scheduling the database synchronization, you are selecting the window of time during which the synchronization takes place and how often it occurs during that time span. You also have the option of synchronizing databases immediately by clicking **Sync Now**.

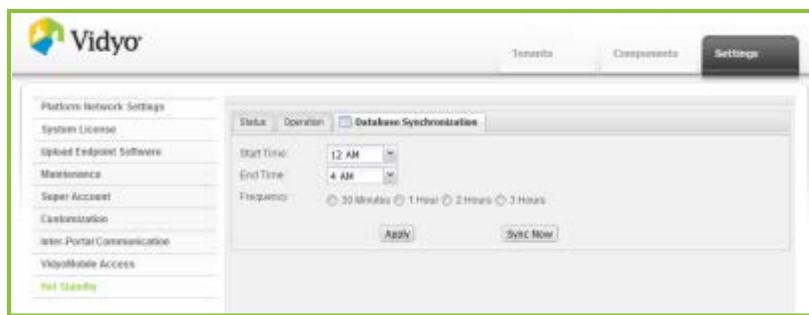
- Database software versions must match, otherwise the content synchronization fails.
- Whenever Hot Standby changes which VidyoPortal is Activated and which one becomes the Standby, all database and Call Detail Records (CDR) changes since the last successful synchronization are lost. Therefore, Vidyo highly recommends setting automatic synchronizations and regular manual synchronizations and in advance of Hot Standby triggers.
- If either VidyoPortal in your Hot Standby setup is replaced, synchronization intervals must be reconfigured as explained in the following section.
- If you are using the CDR database, do not let CDR entries accumulate. Instead, periodically access the CDR, collect the records, and then purge the database in order to optimize synchronizations. For more information about CDRs, see “CDR” on page [336](#).

Synchronizing VidyoPortal Database Information Automatically

To schedule automatic database synchronization:

1. Access the Super Admin portal of your Active VidyoPortal using the Cluster IP address or FQDN. For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).
2. Click **Settings**.
3. Click **Hot Standby** on the left menu.

4. Click the **Database Synchronization** tab.



5. For **Start Time** and **End Time**, select the window of time during which the databases are synchronized.
6. For the **Frequency**, click the radio button that corresponds to how often (during the synchronization window) you want the database to be backed up.

Note:

- The default time and frequency is 12 to 4 AM, once per hour. You may want to keep these early morning hours or choose others when your usage is likely to be lowest. Alternatively, you can synchronize the databases immediately by clicking the **Sync Now** button.
- Synchronization does not drop calls, but users may notice a slight reduction in responsiveness during synchronization.

If desired, you may leave the Super Admin portal for your Active VidyoPortal open as you continue to the next procedure.

Checking the Status of the Hot Standby Configuration

Note: The database status is not shown until you perform the initial Hot Standby database synchronization using either “Triggering the First Database Synchronization from VP1” on page [363](#) or “Synchronizing VidyoPortal Database Information Automatically” on page [365](#).

To check the status of the Hot Standby configuration:

1. Access the Super Admin portal of the Active VidyoPortal using the Cluster IP address or FQDN. For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).
2. Click **Settings**.
3. Click **Hot Standby** on the left menu.
4. Click the **Status** tab.

Note: The following screenshot does not actually show the database synchronization taking place.

Current Role	ACTIVE
Cluster IP	172.16.43.185
Server IP	172.16.43.195
Network Status	ACTIVE
Preferred Primary	Yes
Peer Status	ONLINE
Peer Server IP	172.16.43.194

The Status table appears. This is a read-only table that contains the following Hot Standby information:

- **Current Role** – UNKNOWN appears if the VidyoPortal is in Maintenance mode; otherwise, ACTIVE appears.
- **Cluster IP** – The IP address of the VidyoPortal.
- **Server IP** – The native IP address of the VidyoPortal. This IP address is used during Maintenance mode or when Hot Standby is disabled.
- **Network Status** – ACTIVE appears if the VidyoPortal is reachable; UNKNOWN appears if the VidyoPortal is in Maintenance mode.
- **Preferred Primary** – When both VidyoPortals initialize at the same moment, the Preferred Primary becomes the Active VidyoPortal. (You select the Preferred Primary in the Preferred Node field when you configure VP1 and VP2 using the System Console.)
- **Database Backup** – The last time the database snapshot was taken for synchronization.
- **Peer Status** – The status (either ONLINE or OFFLINE) of the partner VidyoPortal.
- **IP Address** – The configured IP address of the peer VidyoPortal.
- **Sync** – The time the database was last synchronized:

Note:

- If the VidyoPortal can communicate with its peer or partner, the two database times are the same and “In Sync” is shown in the field.
- If the VidyoPortal cannot communicate with its peer or partner or if the database sync failed, this field displays the time of the last sync and “Out of Sync” is shown.
- Statuses generally correspond to the ones shown when using the System Console during “Verifying the Node Status on VP1 and VP2” on page [364](#).

If desired, you may leave the Super Admin portal for your Active VidyoPortal open.

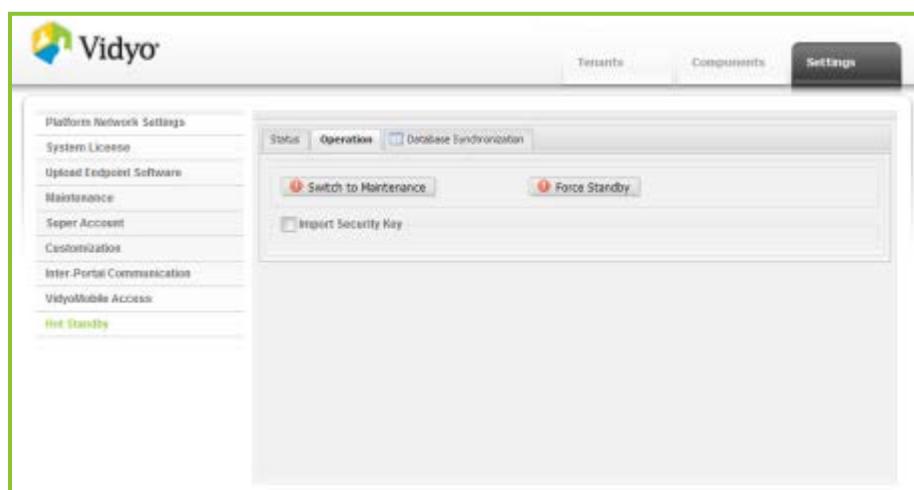
Forcing the Active VidyoPortal into Standby Mode from the Super Admin Portal

Note:

- When a VidyoPortal is in Standby mode, you cannot access corresponding Super Admin or Admin portals; however, the machine is still accessible from the System Console.
- For more information, see “Forcing a Hot Standby from the System Console on Your Active VidyoPortal” on page [372](#).
- If you put your Standby VidyoPortal in to Maintenance mode, the Settings > Hot Standby screens do not appear when accessed via the Internet Explorer Web browser.

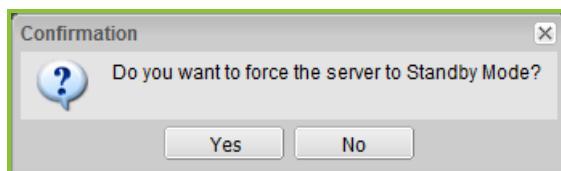
To force the Active VidyoPortal into Standby mode from the Super Admin portal:

1. Verify that the databases are synchronized and backed up using the following steps:
 - a. Access the Super Admin portal of your Active VidyoPortal using the Cluster IP address or FQDN. For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).
 - b. Click **Settings**.
 - c. Click **Hot Standby** on the left menu.
 - d. Click the **Database Synchronization** tab.
 - e. Click **Sync Now**.
 - f. Click the **Status** tab.
 - g. Verify that the sync has completed by ensuring that the Sync field displays that the databases are “In Sync”.
2. Click the **Operation** tab.



3. Click Force Standby.

A Confirmation dialog box appears.



4. Click Yes to force the Active VidyoPortal into Standby mode.

Note:

- At this point, the peer VidyoPortal becomes the Active VidyoPortal and assumes the Cluster IP address and FQDN. This means that the Standby VidyoPortal no longer receives traffic from the Cluster IP address, and instead assumes its Native IP address and FQDN.
- Once a VidyoPortal becomes the Active VidyoPortal, its Native IP address and FQDN are temporarily disabled.
- As a safety measure, you cannot bring down the currently Active VidyoPortal unless its peer VidyoPortal is online and ready to take over. If the peer is offline, the message **Warning!!! Standby Node (xxx.xxx.x.xxx) is OFFLINE** appears, and you are unable to force the currently Active VidyoPortal into Standby mode.

Importing a Security Key

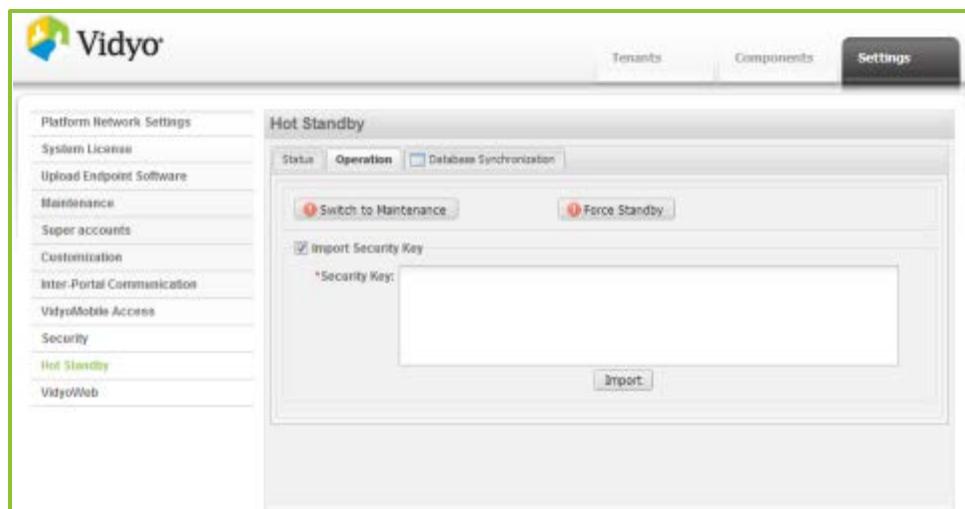
To import a Security Key:

1. Generate and validate a security key for importing using the System Console. For more information, see “Generating and Importing the Security Keys” on page [357](#) and “Validating the Security Keys” on page [362](#).

Note: Set aside the key copied to your clipboard during the “Generating and Importing the Security Keys” on page [357](#). You will use this key during the following procedure.

2. Access the Super Admin portal of the VidyoPortal on which you want to import the key.
3. Click **Settings**.
4. Click **Hot Standby** on the left menu.
5. Click the **Operation** tab.

6. Select Import Security Key.



7. Paste the key copied to your clipboard during the “Generating and Importing the Security Keys” on page [357](#) in the Security Key field.
8. Click **Import**.

Email Notifications

When you change the status of the VidyoPortals in the Hot Standby configuration, you receive email notifications of the changes. The following table lists some of these emails.

Cause	Email or Emails Sent
Active VidyoPortal switches over to Standby VidyoPortal	Two emails: <ul style="list-style-type: none">■ [VidyoPortal] is now the ACTIVE node.■ Standby Node is ONLINE.
Active VidyoPortal switches over to Maintenance mode and Standby VidyoPortal takes over	Two emails: <ul style="list-style-type: none">■ [VidyoPortal] is now the ACTIVE node.■ Standby Node is OFFLINE.
VidyoPortal switches from Maintenance mode to Standby	Standby Node is ONLINE.
VidyoPortal switches from Maintenance mode to Active without Standby	Two emails: <ul style="list-style-type: none">■ [VidyoPortal] is now the ACTIVE node.■ Standby Node is OFFLINE.
Standby VidyoPortal reboots	Two emails: <ul style="list-style-type: none">■ Standby Node OFFLINE.■ Standby Node ONLINE. (This email is sent when it comes back online.)

Cause	Email or Emails Sent
Standby VidyoPortal IP connectivity was lost and restored	<p>Two emails:</p> <ul style="list-style-type: none"> ■ Standby Node OFFLINE. ■ Standby Node ONLINE. (This email is sent when it comes back online.)

UPGRADING HOT STANDBY VIDYOPORTALS

You have two main options for upgrading your Hot Standby VidyoPortals:

1. Upgrading Hot Standby VidyoPortals while Keeping One Server Online
2. Upgrading Hot Standby VidyoPortals while Both Servers are Offline

Upgrading Your Hot Standby VidyoPortals while Keeping One Server Online

This section describes how to upgrade both the Active and the Standby VidyoPortals by forcing your Standby VidyoPortal into Maintenance mode, performing the upgrade, forcing a Hot Standby, and then repeating the process on the previously Active VidyoPortal.

When performing this procedure, refer to the specific IP and FQDN values you designated for your VP1, VP2, and Cluster in the “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

Note: Prior to doing these upgrades, Vidyo recommends performing a database synchronization. For more information, see “Synchronizing VidyoPortal Database Information Automatically” on page [365](#).

Switching to Maintenance Mode and Upgrading Your Standby VidyoPortal

Note: If you put your Standby VidyoPortal in to Maintenance mode, the Settings > Hot Standby screens do not appear when accessed via the Internet Explorer Web browser.

To switch to Maintenance mode and upgrade your Standby VidyoPortal:

1. Open a new System Console and access the Standby VidyoPortal using the Native IP address or FQDN.
For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).
2. Put the Standby VidyoPortal into Maintenance mode using the following steps:
 - a. From the main menu, select **m > H** to access the Standby VidyoPortal’s Hot Standby Menu.
 - b. Select **C** to choose **Maintenance Mode**.

- c. Select **y** to confirm putting your Standby VidyoPortal into Maintenance mode.

```

System Administrator Console

Local Time: Thu Oct 24 16:05:24 EDT 2013
Universal Time: Thu Oct 24 20:05:24 UTC 2013

Hot Standby Menu
=====

Node Status: MAINTENANCE
A. Show Configuration
B. Disable Hot Standby
C. Maintenance Mode
D. Show Hot Standby Status

F. Node Synchronization
x. Exit

Selection: █

```

3. Upgrade the Standby VidyoPortal as described in the “Upgrading Your VidyoPortal System Software” section on page [78](#).

The VidyoPortal automatically reboots.

Note: Wait until the machine has completely rebooted before proceeding.

4. Open a new System Console and return to the Standby VidyoPortal using the Native IP address or FQDN.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#). Take the Standby VidyoPortal out of Maintenance mode using the following steps:

- a. From the main menu, select **m > H** to access the Standby VidyoPortal’s Hot Standby Menu.
- b. Select **C** to choose **Maintenance Mode**.
- c. Select **y** to confirm putting your VidyoPortal back into Standby mode.

If desired, you may leave the System Console for your Standby VidyoPortal open as you continue to the next procedure.

Forcing a Hot Standby from the System Console on Your Active VidyoPortal

To force a Hot Standby on your Active VidyoPortal:

1. Open a new System Console for your Active VidyoPortal using the Cluster IP address or FQDN. For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#). Force a Hot Standby using the following steps:
 - a. From the main menu, select **m > H** to access the Standby VidyoPortal’s Hot Standby Menu.
 - b. Select **E** to choose **Force Standby**.

- C. Select **y** to confirm forcing your Active VidyoPortal into Standby mode.

```

System Administrator Console

Local Time: Tue Apr 2 19:54:03 GMT 2013
Universal Time: Tue Apr 2 19:54:03 UTC 2013

Hot Standby Menu
=====

Node Status: ACTIVE

A. Show Configuration
B. Disable Hot Standby
C. Maintenance Mode
D. Show Hot Standby Status
E. Force Standby
F. Node Synchronization
x. Exit

Selection: e

Warning!!! You are about to set this node to STANDBY

Confirm changes ? [y/n]

```

Your System Console session is automatically disconnected from your VidyoPortal while it is forced into Standby mode.

Note: Alternatively, a Force Standby can be done via the Super Admin portal using “Forcing the Active VidyoPortal into Standby Mode” on page [368](#).

2. Close the System Console which is now disconnected from your VidyoPortal.

Repeat the previous procedures starting with “Switching to Maintenance Mode and Upgrading your Standby VidyoPortal” on page [371](#) for the Standby VidyoPortal – which was just the Active machine before you forced the Standby during the previous step – to complete upgrades on both of your VidyoPortal machines.

Upgrading Your Hot Standby VidyoPortals while Taking Both Servers Offline

This method for upgrading your VidyoPortals requires more time because you must take the system completely offline for full maintenance. However, no CDR records are lost.

With this option, you place both servers into Maintenance mode, upgrade both and then return them to their original Active and Standby modes.

To upgrade Hot Standby VidyoPortals while taking both servers offline:

1. Open a new System Console and access the Standby VidyoPortal using the Native IP address or FQDN to put your Standby VidyoPortal into Maintenance mode.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

- a. From the main menu, select **m** > **H** to access the Standby VidyoPortal’s Hot Standby Menu.
- b. Select **C** to choose **Maintenance Mode**.

- C. Select **y** to confirm putting your Standby VidyoPortal into Maintenance mode.

```

System Administrator Console

Local Time: Tue Apr 2 19:54:03 GMT 2013
Universal Time: Tue Apr 2 19:54:03 UTC 2013

Hot Standby Menu
=====

Node Status: ACTIVE

A. Show Configuration
B. Disable Hot Standby
C. Maintenance Mode
D. Show Hot Standby Status
E. Force Standby
F. Node Synchronization
x. Exit

Selection: e

Warning!!! You are about to set this node to STANDBY

Confirm changes ? [y/n]

```

2. Open a new System Console and access the Active VidyoPortal using the Native IP address or FQDN to put your Active VidyoPortal into Maintenance mode.

For more information, see “Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster” on page [347](#).

- From the main menu, select **m** > **H** to access the Active VidyoPortal’s Hot Standby Menu.
- Select **C** to choose **Maintenance Mode**.
- Select **y** to confirm putting your Standby VidyoPortal into Maintenance mode.

```

System Administrator Console

Local Time: Tue Apr 2 19:54:03 GMT 2013
Universal Time: Tue Apr 2 19:54:03 UTC 2013

Hot Standby Menu
=====

Node Status: ACTIVE

A. Show Configuration
B. Disable Hot Standby
C. Maintenance Mode
D. Show Hot Standby Status
E. Force Standby
F. Node Synchronization
x. Exit

Selection: e

Warning!!! You are about to set this node to STANDBY

Confirm changes ? [y/n]

```

Both of your VidyoPortals should now be offline and in Maintenance Mode.

3. Upgrade both VidyoPortals as described in the “Performing a System Upgrade” section on page [78](#).

4. After the upgrades are complete and the servers are restarted, return the VidyoPortal that was originally your Active VidyoPortal using the Native IP address or FQDN. Put this machine in to Active mode first using the following steps:

Note: The first VidyoPortal server you take out of Maintenance Mode is made the Active VidyoPortal just by removing it from Maintenance Mode.

- a. From the main menu, select **m > H** to access the Standby VidyoPortal's Hot Standby Menu.
- b. Select **C** to choose **Maintenance Mode**.
- c. Select **y** to confirm putting your VidyoPortal back into Active mode.

5. Return the VidyoPortal that was originally your Standby VidyoPortal using the Native IP address or FQDN. Put this machine in to Standby mode using the following steps:

Note: The second VidyoPortal server you take out of Maintenance Mode is made the Standby VidyoPortal just by removing it from Maintenance Mode.

- a. From the main menu, select **m > H** to access the Standby VidyoPortal's Hot Standby Menu.
- b. Select **C** to choose **Maintenance Mode**.
6. Select **y** to confirm putting your VidyoPortal back into Standby mode.

Appendix F. Reliability

THE VIDYO INFORMATION OR THIRD PARTY VENDOR DATA CONTAINED HEREIN IS PROVIDED STRICTLY "AS IS", WITHOUT WARRANTY, AND VIDYO EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE OR FITNESS FOR A PARTICULAR PURPOSE REGARDING SAID INFORMATION OR DATA, EVEN IN THE EVENT VIDYO HAS KNOWLEDGE OF DEFICIENCIES IN SAID INFORMATION OR DATA. VIDYO DOES NOT ENSURE OR GUARANTEE THE ACCURACY OF ANY SUCH VIDYO INFORMATION OR THIRD PARTY VENDOR DATA AND SUCH INFORMATION AND/OR DATA IS UTILIZED BY RECIPIENT SOLELY AT ITS OWN RISK AND EXPENSE. VIDYO DISCLAIMS LIABILITY FOR ANY AND ALL CLAIMS, DAMAGES, COSTS OR EXPENSES, INCLUDING SPECIFICALLY BUT WITHOUT LIMITATION, LOST PROFITS, LOST DATA OR LOST BUSINESS EXPECTANCY, COMPENSATORY, INCIDENTAL AND OTHER CONSEQUENTIAL DAMAGES, ARISING OUT OF OR IN ANY WAY RELATING TO RECIPIENT'S RECEIPT, USE OF, RELIANCE OR ALLEGED RELIANCE UPON THE INFORMATION OR DATA, OR VIDYO'S ACTS OR OMISSIONS REGARDING SUCH INFORMATION OR DATA, EVEN IF RECIPIENT INFORMS VIDYO, WHETHER EXPRESSLY OR BY IMPLICATION, OF ITS RECEIPT, USE OR RELIANCE UPON SUCH INFORMATION, AND EVEN IF SUCH LOSSES ARE DUE OR ALLEGED TO BE DUE IN WHOLE OR IN PART TO VIDYO'S NEGLIGENCE, CONCURRENT NEGLIGENCE OR OTHER FAULT, BREACH OF CONTRACT OR WARRANTY, VIOLATION OF DECEPTIVE TRADE PRACTICES LAWS OR STRICT LIABILITY WITHOUT REGARD TO FAULT. RECEIPT OF THE INFORMATION HEREIN IS DEEMED ACCEPTANCE OF THE TERMS HEREOF.

LIMITATIONS OF RELIABILITY PREDICTION MODELS

- Reliability prediction models provide MTBF point estimates. Model inputs include base component failure rates, environmental, quality, and stress factors.
- Base failure rates use failure data from multiple sources, including industry field data, research lab test results, and government labs.
- Environmental, quality and stress factors may differ from field conditions.
- Predictions assume a constant failure rate which does not account for failures due to early life quality issues or wearout phenomena.

GENERAL PREDICTION METHODOLOGY

- VIDYO's default prediction methodology is Telcordia SR332, Reliability Prediction.

Electronic Equipment Procedure

- Other methods may be used to estimate the reliability of certain products and/or subsystems.
- System reliability predictions take into account the impact of redundant components.

Component Parameters and Assumptions

- The default methodology for MTBF predictions is Telcordia method 1, case 3.

- Assumptions include 250° C system inlet air temperature, quality level II components, ground-based, fixed, controlled environment, and 100% duty cycle. Components internal to the system are generally assumed to be operating at 400° C ambient and 50% electrical stress.

Supplier MTBF Data

- In developing system MTBF predictions, VIDYO uses MTBF data provided by suppliers.
- Apart from using industry standard prediction methodologies, suppliers may derive MTBF data from reliability demonstration testing, life testing, actual field failure rate, or specification and datasheets.
- Supplier data is provided as is to VIDYO, and VIDYO generally does not verify the accuracy of Supplier data.

Subsystem MTBF Data Release Policy

VIDYO does not release MTBF data below the system level.

The reasons for this policy are:

- VIDYO considers internally designed subsystem MTBF data to be confidential intellectual property.
- VIDYO obtains supplier subsystem MTBF data under NDA and is prohibited from sharing such data outside of VIDYO.

MTBF RELIABILITY

The MTBF prediction is calculated using component and subassembly random failure rates. The calculation is based on the Telcordia SR-332 Issue 2, Method I, Case 3.

Product	Part Number	MTBF
HD-40	DEV-RM-HD40-SA-oA	71,537 hours
HD-40B	DEV-RM-HD40-B-SA-oA	66,640 hours
HD-100	DEV-RM-HD100-P4-oA	187,952 hours
HD-100D	DEV-RM-HD100-D9020-SA-oA and DEV-RM-HD100-D-NTPM-SA-oA	75,400 hours
HD-230	DEV-RM-HD230-NTPM-SA-oA and DEV-RM-HD230-SA-oA	80,520 hours
VidyoGateway	DEV-SRV-GW-N2-oB	29,900 hours
VidyoGateway XL	DEV-SRV-GW-XL-N3-oA	121,400 hours
VidyoH2o for Google+ Hangouts	DEV-SRV-H2o-XL-N3-oA	121,400 hours
VidyoOne	DEV-SRV-ONE-N2-oB	29,900 hours
VidyoPanorama 600	DEV-SRV-PAN600-N2-oA	109,186 hours
VidyoPortal	DEV-SRV-PT-N2-oB	29,900 hours
VidyoPortal XL	DEV-SRV-PT-XL-N3-oA	116,700 hours
VidyoReplay	DEV-SRV-REP-N3-0A	116,700 hours
VidyoRouter	DEV-SRV-RTR-N2-0B	29,900 hours
VidyoRouter XL	DEV-SRV-RTR-XL-N3-0A	103,600 hours

Appendix G. Licensing

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, sublicense, 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 hereby 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 patent 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 infringement, 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, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices 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 within 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 complies with the conditions stated in this License.

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.

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.

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 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 SSLEY 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, Ihash, 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 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.

The license 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 license [including the GNU Public License.]

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

ING 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.

1. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “**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.

2. 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.

3. 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.

4. 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.

5. 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 4do, 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.)

6. 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.

7. 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 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.

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

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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. Regardless 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.

8. 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.

9. 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 license, 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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 Modifications

- “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.

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.