# TABLE OF CONTENTS

1. **Overview** ........................................................................................................... 1
   Understanding the Different System Accounts .................................................. 1
   The System in Brief .............................................................................................. 2
   Conventions Used ............................................................................................... 2

2. **Definitions** ......................................................................................................... 3
   Vidyo Concepts and Equipment ............................................................................ 3
   Users ....................................................................................................................... 5
   Tenants ................................................................................................................... 6
   Meeting .................................................................................................................. 7
   Meeting Rooms ................................................................................................... 8
   Groups .................................................................................................................... 8
   VidyoLines ........................................................................................................... 9
   Install .................................................................................................................... 9
   Endpoint ............................................................................................................... 9

3. **Upgrading Your VidyoConferencing System** .................................................. 10

4. **Configuring Your Server** .................................................................................. 12
   Logging in to the System Console of Your Server and Changing the Default Password ...... 13
   Configuring the Network Settings at the System Console ...................................... 15
   Changing the Other Default Passwords .................................................................. 18
   Supporting Multiple System Console Accounts ..................................................... 19
   Understanding System Administrator Console Menu Options .................................. 20
   Understanding the More Options System Administrator Console Menu ......................... 23
   Configuring FIPS on Your Vidyo Server .................................................................. 24
   Managing Network Routes ................................................................................... 25
      Adding a Network Route .................................................................................. 26
      Removing a Network Route .............................................................................. 28
      Removing all of Your Network Routes ............................................................... 28
      Navigating Your Network Routes .................................................................... 29
   Configuring SNMP ............................................................................................... 29
      Enabling SNMP ............................................................................................... 32
      Configuring an SNMPv2 Community String ...................................................... 33
      Configuring Local SNMPv3 User (User-based Security Model) .......................... 35
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a SNMP Notification</td>
<td>37</td>
</tr>
<tr>
<td>Managing Hostnames</td>
<td>40</td>
</tr>
<tr>
<td>Adding a Hostname</td>
<td>41</td>
</tr>
<tr>
<td>Removing a Hostname</td>
<td>42</td>
</tr>
<tr>
<td>Removing all of Your Hostnames</td>
<td>43</td>
</tr>
<tr>
<td>Navigating Your Hostnames</td>
<td>44</td>
</tr>
<tr>
<td>Enabling Secure Shell Access on the Management Interface</td>
<td>44</td>
</tr>
<tr>
<td>Enabling an Emergency Admin User</td>
<td>45</td>
</tr>
<tr>
<td>Configuring Your SSH Port</td>
<td>46</td>
</tr>
<tr>
<td>Configuring Your VidyoRouter Media Priority</td>
<td>47</td>
</tr>
<tr>
<td>Configuring Service Accessibility</td>
<td>48</td>
</tr>
<tr>
<td>Logging in to the Super Admin Portal</td>
<td>49</td>
</tr>
<tr>
<td>Checking the Status of the Components</td>
<td>50</td>
</tr>
<tr>
<td>Requesting System Licenses and Applying System License Keys</td>
<td>51</td>
</tr>
<tr>
<td>Requesting Your Vidyo Licenses</td>
<td>51</td>
</tr>
<tr>
<td>Applying the System License Keys to Your System</td>
<td>53</td>
</tr>
<tr>
<td>Setting the Language for the Super Admin Interface</td>
<td>53</td>
</tr>
<tr>
<td>Adding Multiple Super Admin Accounts</td>
<td>55</td>
</tr>
<tr>
<td>5. Configuring RADIUS</td>
<td>58</td>
</tr>
<tr>
<td>Disabling FIPS Mode</td>
<td>58</td>
</tr>
<tr>
<td>Enabling RADIUS</td>
<td>59</td>
</tr>
<tr>
<td>Viewing the Current RADIUS Configuration</td>
<td>61</td>
</tr>
<tr>
<td>Modifying the RADIUS Configuration</td>
<td>62</td>
</tr>
<tr>
<td>Creating a RADIUS-Enabled Account</td>
<td>63</td>
</tr>
<tr>
<td>Viewing a RADIUS-Enabled Account</td>
<td>64</td>
</tr>
<tr>
<td>Removing a RADIUS-Enabled Account</td>
<td>65</td>
</tr>
<tr>
<td>Disabling RADIUS Authentication</td>
<td>65</td>
</tr>
<tr>
<td>Creating a Local System Console Account</td>
<td>66</td>
</tr>
<tr>
<td>6. Enabling the Management Interface</td>
<td>68</td>
</tr>
<tr>
<td>Moving VidyoPortal Applications to the Management Interface</td>
<td>69</td>
</tr>
<tr>
<td>The Management Interface on VidyoRouter and VidyoGateway</td>
<td>70</td>
</tr>
<tr>
<td>Moving Your VidyoRouter Applications to the Management Interface</td>
<td>70</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Moving Your VidyoGateway Application to the Management Interface</td>
<td>72</td>
</tr>
<tr>
<td>Adding Static Network Routes</td>
<td>73</td>
</tr>
<tr>
<td>7. Configuring System Settings as the Super Admin</td>
<td>75</td>
</tr>
<tr>
<td>Applying System License Keys to Your System</td>
<td>76</td>
</tr>
<tr>
<td>Applying System License Keys to Your System Using the Hot Standby Software Option</td>
<td>79</td>
</tr>
<tr>
<td>Understanding Vidyo License Consumption by User Type</td>
<td>80</td>
</tr>
<tr>
<td>Understanding Licensing Notifications</td>
<td>80</td>
</tr>
<tr>
<td>Checking Your Platform Network Settings</td>
<td>80</td>
</tr>
<tr>
<td>Uploading Endpoint Software</td>
<td>81</td>
</tr>
<tr>
<td>Activating an Endpoint Installation File</td>
<td>84</td>
</tr>
<tr>
<td>Deleting an Endpoint Installation File</td>
<td>88</td>
</tr>
<tr>
<td>Performing System Maintenance</td>
<td>88</td>
</tr>
<tr>
<td>Backing Up the Database</td>
<td>88</td>
</tr>
<tr>
<td>Downloading a Backup File</td>
<td>90</td>
</tr>
<tr>
<td>Uploading a Backup File</td>
<td>90</td>
</tr>
<tr>
<td>Restoring a Backup File Located on Your VidyoPortal</td>
<td>91</td>
</tr>
<tr>
<td>Restoring a Backup File No Longer on Your VidyoPortal</td>
<td>92</td>
</tr>
<tr>
<td>Deleting a Backup File Located on Your VidyoPortal</td>
<td>93</td>
</tr>
<tr>
<td>Restoring the Database to the Factory Default</td>
<td>94</td>
</tr>
<tr>
<td>Upgrading Your VidyoPortal System Software</td>
<td>94</td>
</tr>
<tr>
<td>Restarting Your System</td>
<td>96</td>
</tr>
<tr>
<td>Configuring the CDR Database for Remote Access in the Super Admin Portal</td>
<td>97</td>
</tr>
<tr>
<td>Exporting and Purging CDR Files from the Super Admin Portal</td>
<td>98</td>
</tr>
<tr>
<td>Downloading System Logs</td>
<td>100</td>
</tr>
<tr>
<td>Downloading Specific VidyoPortal Installation Logs</td>
<td>102</td>
</tr>
<tr>
<td>Creating a System Diagnostic File</td>
<td>103</td>
</tr>
<tr>
<td>Viewing a System Diagnostic File</td>
<td>104</td>
</tr>
<tr>
<td>Downloading a System Diagnostic File</td>
<td>106</td>
</tr>
<tr>
<td>Enabling Syslogs</td>
<td>106</td>
</tr>
<tr>
<td>Configuring Status Notify</td>
<td>108</td>
</tr>
<tr>
<td>Managing Your Super Accounts</td>
<td>109</td>
</tr>
<tr>
<td>Viewing Your Super Accounts</td>
<td>109</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing Super Account Information and Changing the Password</td>
<td>110</td>
</tr>
<tr>
<td>Customizing the System</td>
<td>112</td>
</tr>
<tr>
<td>Customizing the About Info</td>
<td>112</td>
</tr>
<tr>
<td>Reverting To Default System Text on the About Info Screen</td>
<td>113</td>
</tr>
<tr>
<td>Customizing Support Info</td>
<td>114</td>
</tr>
<tr>
<td>Reverting To Default System Text on the Support Info Screen</td>
<td>115</td>
</tr>
<tr>
<td>Customizing Notification Information</td>
<td>116</td>
</tr>
<tr>
<td>Customizing the Invite Text</td>
<td>118</td>
</tr>
<tr>
<td>Reverting To Default System Text on the Invite Text Screen</td>
<td>121</td>
</tr>
<tr>
<td>Uploading Custom Logos</td>
<td>122</td>
</tr>
<tr>
<td>Changing Where the System Looks for PDF Versions of the Administrator and User Guides</td>
<td>124</td>
</tr>
<tr>
<td>Customizing Your VidyoPortal Login and Welcome Banners</td>
<td>126</td>
</tr>
<tr>
<td>Customizing Room Links</td>
<td>129</td>
</tr>
<tr>
<td>Customizing Your Password Settings</td>
<td>130</td>
</tr>
<tr>
<td>Reverting To Default Password Settings on the Password Screen</td>
<td>132</td>
</tr>
<tr>
<td>Securing Your VidyoConferencing System</td>
<td>133</td>
</tr>
<tr>
<td>Configuring System-Wide Inter-Portal Communication (IPC)</td>
<td>133</td>
</tr>
<tr>
<td>Configuring Endpoint Network Settings</td>
<td>137</td>
</tr>
<tr>
<td>Setting Global Features</td>
<td>139</td>
</tr>
<tr>
<td>Enabling VidyoWeb Access</td>
<td>139</td>
</tr>
<tr>
<td>Enabling Vidyo Neo for WebRTC access</td>
<td>141</td>
</tr>
<tr>
<td>Enabling VidyoMobile Access</td>
<td>142</td>
</tr>
<tr>
<td>Configuring System-Wide Search Options</td>
<td>144</td>
</tr>
<tr>
<td>Configuring Transport Layer Security (TLS) VidyoProxy</td>
<td>145</td>
</tr>
<tr>
<td>Configuring System-Wide Public and Private Chat</td>
<td>146</td>
</tr>
<tr>
<td>Configuring Scheduled and Public Room Settings</td>
<td>147</td>
</tr>
<tr>
<td>Configuring User Attributes</td>
<td>148</td>
</tr>
<tr>
<td>8. Configuring Your Components as the Super Admin</td>
<td>151</td>
</tr>
<tr>
<td>Using the Components Table</td>
<td>152</td>
</tr>
<tr>
<td>Configuring Your VidyoManager Component</td>
<td>154</td>
</tr>
<tr>
<td>Entering General VidyoManager Information</td>
<td>154</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

Configuring Your VidyoRouter Component .......................................................................... 156
Configuring VidyoRouter General Settings ....................................................................... 156
Configuring VidyoRouter SCIP Settings ........................................................................... 158
Configuring VidyoRouter Media Port Range Settings ...................................................... 158
Configuring VidyoRouter Quality of Service (QoS) .......................................................... 159
Configuring VidyoRouter NAT Firewall Settings .............................................................. 159
Accessing Your VidyoRouter Configuration Page ............................................................. 160
Configuring Basic Settings on Your VidyoRouter ............................................................. 161
Configuring Security on Your VidyoRouter ..................................................................... 162
Viewing System Information on Your VidyoRouter ......................................................... 162
Upgrading Your VidyoRouter ............................................................................................ 163
Downloading Your VidyoRouter Installation Logs History .............................................. 166
Restarting Your VidyoRouter ............................................................................................. 170
Logging Out of Your VidyoRouter ...................................................................................... 171
VidyoGateway Configuration ............................................................................................. 171
Making Configurations on Your VidyoGateway ............................................................... 171
Making Configurations on Your VidyoPortal for Your VidyoGateway ................................ 172
Adding a VidyoGateway to Your VidyoPortal .................................................................. 172
Configuring Router Pools ................................................................................................ 175
Creating a VidyoRouter Pool ............................................................................................. 176
Deleting an Entire VidyoRouter Pool .............................................................................. 178
Activating the Router Pool Configuration ...................................................................... 178
Creating User Location Tags ............................................................................................ 180
Creating Priority Lists ....................................................................................................... 181
Creating Endpoint Rules .................................................................................................. 182

9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE) ...................................... 185

Understanding the VE Requirements .............................................................................. 185
VidyoPortal Virtual Machine Provisioning Requirements ................................................. 186
VidyoRouter Virtual Machine Provisioning Requirements ................................................. 187
Example Configurations .................................................................................................. 187
Understanding VMware Best Practices ............................................................................ 188
# TABLE OF CONTENTS

Understanding VidyoPortal and VidyoRouter VE Support of VMware Features ........................................... 188
Installing VidyoPortal VE ............................................................................................................................ 189
Installing VidyoRouter VE ......................................................................................................................... 196

10. Managing Tenants as the Super Admin .................................................................................................. 205
    Using the Tenants Table .......................................................................................................................... 205
    Understanding How to Add a Tenant ....................................................................................................... 206
    Adding a Tenant ........................................................................................................................................ 206
    Adding a Default Tenant or Adding a New Tenant .................................................................................. 207
    Enabling Cross-Tenant Access .............................................................................................................. 210
    Making the VidyoProxy Components Available ..................................................................................... 211
    Making the VidyoGateway Components Available ............................................................................... 212
    Making the VidyoReplay Recorders Available ....................................................................................... 213
    Making the VidyoReplay Components Available ................................................................................... 214
    Assigning Location Tags ......................................................................................................................... 215
    Adding the New Tenant to Your System ................................................................................................. 216
    Deleting a Tenant ...................................................................................................................................... 217
    Viewing Current Calls ............................................................................................................................ 218

11. Managing Users as the Tenant Admin .................................................................................................. 220
    What Tenant Admins Do ......................................................................................................................... 220
    Logging In as a Tenant Admin ................................................................................................................ 221
    Setting the Language for the Admin Interface ....................................................................................... 221
    Using the Manage Users Table ............................................................................................................. 223
    Adding a New User .................................................................................................................................. 223
    Editing a User ........................................................................................................................................... 227
    Deleting a User ........................................................................................................................................ 230
    Adding a Legacy Device .......................................................................................................................... 231
    Exporting Users ....................................................................................................................................... 232
    Exporting .csv Files ............................................................................................................................... 234
    Importing Users ......................................................................................................................................... 235

12. Managing Meeting Rooms as the Tenant Admin .................................................................................. 236
    Using the Manage Meeting Rooms Table ............................................................................................ 236
    Adding a Meeting Room .......................................................................................................................... 237
TABLE OF CONTENTS

Editing a Meeting Room ................................................................. 240
Deleting a Public Meeting Room ....................................................... 241
Viewing Current Calls .................................................................. 243
Understanding Controlling Meetings .............................................. 244
Controlling Meetings ................................................................... 245
  Configuring Conference Settings .................................................. 248
Setting the Moderator PIN on Your Room ..................................... 252
Moderating Another Person’s Room ................................................. 253
Controlling a Meeting from VidyoDesktop ..................................... 254
Controlling a Meeting from a Tablet ................................................. 255
Managing Participants .................................................................. 257
13. Managing Tenant Admin Room Systems .................................... 258
14. Managing Tenant Admin Groups as the Tenant Admin ............. 259
  Using the Manage Groups Table ................................................... 259
  Adding a New Group .................................................................. 260
  Editing a Group ......................................................................... 261
  Deleting a Group ....................................................................... 261
15. Configuring Settings as the Tenant Admin ................................. 263
  Checking Your License Terms .................................................... 263
  Uploading Endpoint Software ..................................................... 263
    Activating an Endpoint Installation File ..................................... 266
    Deleting an Endpoint Installation File ....................................... 267
  Setting the Tenant Language ....................................................... 268
  Configuring Guest’s Settings ...................................................... 270
  Configuring Customization on Your Tenant ............................... 270
    Customizing the About Info ..................................................... 271
    Reverting To Default System Text on the About Info Screen ..... 272
    Customizing Support Information ............................................. 273
    Reverting To Default System Text on the Support Info Screen ... 274
    Customizing Notification Information ..................................... 275
    Customizing the Invite Text ..................................................... 276
    Reverting To Default System Text on the Invite Text Screen ..... 280
# TABLE OF CONTENTS

Uploading Custom Logos on Your Tenant ............................................................... 281  
Configuring Authentication ..................................................................................... 282  
  Configuring Authentication Using LDAP ................................................................. 283  
  Configuring Authentication Using Web Services .................................................. 300  
  Configuring Authentication Using SAML .............................................................. 302  
Managing Location Tags ......................................................................................... 317  
Exporting CDR Files from the Admin Portal ......................................................... 319  
Configuring Endpoint Network Settings on Your Tenant ....................................... 321  
Configuring Feature Settings on Your Tenant ....................................................... 323  
  Configuring VidyoWeb on Your Tenant ................................................................. 323  
  Configuring Public and Private Chat on Your Tenant ........................................... 325  
  Configuring Room Attributes on Your Tenant ...................................................... 326  
  Configuring User Attributes ................................................................................. 329  
16. Auditing ............................................................................................................. 331  
  Downloading Audit Logs from Your VidyoPortal ................................................ 331  
  Downloading Audit Logs from Your VidyoRouter ............................................... 331  
  Downloading Audit Logs From Your VidyoGateway .......................................... 332  
Audit Log Content .................................................................................................. 334  
  Content Captured in the Audit Log. ...................................................................... 334  
  Sample Audit Log Content .................................................................................... 337  
17. Configuring OCSP ............................................................................................. 338  
  Enabling and Configuring OCSP ......................................................................... 338  
    Enabling OCSP in the VidyoPortal and VidyoRouter and Configuring OCSP in the VidyoPortal ................................................................. 338  
    Enabling OCSP in the VidyoGateway ................................................................. 340  
  Disabling OCSP from the System Console ......................................................... 341  
Appendix A. Firewall and Network Address Translations (NAT) Deployments ........ 343  
  NAT Introduction .................................................................................................. 343  
  VidyoConferencing Firewall Ports ..................................................................... 344  
    VidyoDesktop and VidyoRoom Requirements ................................................... 344  
    Vidyo Server Requirements .............................................................................. 345  
  Configuring VidyoConferencing with a Firewall NAT ........................................ 346
TABLE OF CONTENTS

Configuring the Firewall NAT .......................................................................................................................... 347
Configuring DNS and FQDN ............................................................................................................................. 348
Configuring the Vidyo Server ........................................................................................................................... 348
Configuring Tenant URLs ................................................................................................................................. 349
Configuring the VidyoManager ......................................................................................................................... 349
Configuring Each of Your VidyoRouters ............................................................................................................. 350
Testing Your Configuration ............................................................................................................................... 352

Appendix B. VidyoProxy ..................................................................................................................................... 353
VidyoProxy Solution for Traversal of Restricted Networks ............................................................................... 353
Overcoming Deployment Barriers Securely and Effectively ............................................................................. 353
Vidyo Solutions for Firewalled Networks .......................................................................................................... 353
Key Features and Functions of Vidyo’s Proxy Solution .................................................................................... 354

Appendix C. Security .......................................................................................................................................... 356
Securing Your VidyoConferencing System with SSL and HTTPS ................................................................. 357
Importing, Exporting, and Regenerating an SSL Private Key ........................................................................... 358
Regenerating and Viewing an SSL CSR ............................................................................................................ 361
Using a Wildcard Certificate in a Multi-Tenant System .................................................................................... 364
Certificates Received from Your Certificate Authority ................................................................................... 365
Deploying Your Server Certificate .................................................................................................................... 367
Deploying Your Server CA Certificates (Intermediates) .................................................................................. 369
Configuring HTTPS Port Settings on Your Applications .................................................................................. 371
Importing Security Settings from the Advanced Tab ....................................................................................... 372
Enabling SSL and HTTPS Only ......................................................................................................................... 374
Importing and Exporting Certificates from the Advanced Tab ....................................................................... 376
Resetting Your Security Configuration to Factory Defaults ............................................................................ 378
Configuring Client CA Certificates .................................................................................................................. 379
Configuring Your Components to Work with HTTPS ...................................................................................... 379
Setting the Hostname and Domain on Your Vidyo Server ................................................................................ 380
Setting the FQDN on Your VidyoRouter Configuration Pages ....................................................................... 380
Setting the FQDN on Your Tenants ................................................................................................................ 381
Configuring Each VidyoPortal Component to Use Your FQDN ..................................................................... 381
Setting the FQDN in Your VidyoRouter Component Configuration ................................................................. 381
# TABLE OF CONTENTS

Verifying Your VidyoPortal Components are Online (Status: UP) .................................................. 383
Applying VidyoPortal SSL Certificates to VidyoRooms ................................................................. 384
Building the VidyoPortal Full Chain SSL Certificate ................................................................. 385
Implementing Encryption Using the Secured VidyoConferencing Option ................................ 385
Verifying Your VidyoPortal is Licensed for Encryption ............................................................ 386
Enabling Encryption on the VidyoConferencing System ............................................................ 387
Testing the VidyoDesktop and Verifying Encryption ................................................................. 387

**Appendix D. CDR** .......................................................................................................................... 388

Understanding CDR Configuration ............................................................................................... 389
Configuring the CDR Database for Remote Access ..................................................................... 390
Exporting and Purging CDR Files ............................................................................................... 390
CDR Version 2.1 Tables .................................................................................................................. 391
ClientInstallations 2 ....................................................................................................................... 391
ConferenceCall 2 ............................................................................................................................ 391

**Appendix E. Hot Standby** ............................................................................................................ 395

Automatically and Manually Triggering Hot Standby ................................................................. 395
Synchronizing the VidyoPortal Database for Hot Standby .......................................................... 396
Configuring Your Settings in Preparation for Hot Standby ......................................................... 397
Setting IP and DNS Settings on VP1 and VP2 ............................................................................. 397
Verifying Correct Installation of VidyoPortal Licenses with the Hot Standby Option .............. 397
Preparing the System Software and Database ............................................................................ 399
Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster ................................. 399
Ensuring that the Network IP Address Can Be Pinged ............................................................... 403

Configuring Hot Standby ................................................................................................................ 404
Setting Hot Standby Configuration Values on VP1 ..................................................................... 404
Rebooting to Apply the New Hot Standby Configuration Values on VP1 ................................. 409
Verifying VP1 Functionality ......................................................................................................... 410
Setting Hot Standby Configuration Values on VP2 ..................................................................... 410
Generating and Importing the Security Keys .............................................................................. 411
Validating the Security Keys ........................................................................................................ 417
Triggering the First Database Synchronization from VP1 ......................................................... 418
Verifying the Node Status on VP1 and VP2 ............................................................................... 418
# TABLE OF CONTENTS

Checking the Status of the Hot Standby Configuration ......................................................... 419
Forcing the Active VidyoPortal into Standby Mode from the Super Admin Portal .................. 421
Email Notifications .................................................................................................................. 423
Upgrading Hot Standby VidyoPortals ...................................................................................... 423
Upgrading Your Hot Standby VidyoPortals while Keeping One Server Online ..................... 424
Upgrading Your Hot Standby VidyoPortals while Taking Both Servers Offline ...................... 426

Appendix F. Vidyo Support ..................................................................................................... 429
Enabling Vidyo Support ......................................................................................................... 429
Disabling Vidyo Support ....................................................................................................... 430

Appendix G. Reliability .......................................................................................................... 431
Limitations of Reliability Prediction Models ......................................................................... 431
General Prediction Methodology ........................................................................................... 431
Electronic Equipment Procedure .......................................................................................... 431
Component Parameters and Assumptions .............................................................................. 432
Supplier MTBF Data .............................................................................................................. 432
Subsystem MTBF Data Release Policy .................................................................................. 432
MTBF Reliability .................................................................................................................. 432

Appendix H. Licensing ........................................................................................................... 434
Apache License ..................................................................................................................... 434
Curl License .......................................................................................................................... 437
Open SSL License .................................................................................................................. 437
Original Ssleay License ......................................................................................................... 438
X11 License ........................................................................................................................... 439
NSIS License ......................................................................................................................... 439
  zlib/libpng License ............................................................................................................. 440
  bzip2 License .................................................................................................................... 440
Common Public License version 1.0 ..................................................................................... 441
GNU Lesser General Public License ...................................................................................... 445
GNU General Public License ................................................................................................ 448
Ubuntu Linux Source Code Availability .............................................................................. 458
Zend Framework .................................................................................................................. 458
Common Development And Distribution License (CDDL) Ver. 1.0 .................................... 459
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>License Agreement</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Public License (CPL) Ver. 1.0</td>
<td>460</td>
</tr>
<tr>
<td>Binary Code License (BCL) Agreement for the Java SE Runtime Environment (JRE) Ver. 6 and JavaFX Runtime Ver. 1</td>
<td>462</td>
</tr>
<tr>
<td>TeraByte Inc. End User License Agreement</td>
<td>462</td>
</tr>
</tbody>
</table>
1. Overview

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.
1. Overview

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

- Items marked with Tip indicate that the information is useful and practical.
- Items marked with Note indicate that the information deserves special attention.
- Items marked with Caution indicate that not following the information provided may result in unwanted or undesirable outcomes.
- Text you type into an on-screen field or a browser address bar displays in a bold Consolas font. Variables are shown in blue, surrounded by brackets:
  
  http://[IP or FQDN address]

- Cross-references to pages are shown in blue.
- Navigational paths are delimited with greater-than symbols and italicized:
  
  Click Settings > Options
2. Definitions

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

Vidyo Concepts and Equipment

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

- **Portal** – A single web page\(^1\) (for end users) or a series of web pages (for Super Admins, Admins, and Operators) that are used to interact with the system. It’s also how the users access their rooms, 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 their portal to make direct point-to-point video calls and to set up and use their room or rooms.

**Note**  The UI for the end user in a call or conference is their 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).

\(^1\) 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.
2. Definitions

- **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 drives up to six screens. 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 contact 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.
2. Definitions

- **Router Pools** – 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 Router Pools provides, the feature is turned off by default. A small organization with few locations may not need to use of the capabilities of Router Pools 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 setup.

- **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** – A single VidyoPortal system can be set up to host multiple organizations known as 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.
2. Definitions

- **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.

![Multi-Tenant System Diagram]

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 provisioning groups and public rooms. In a multi-tenant system, the Tenant Admin has the exact same duties, but only for their 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 their 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 their 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 their automatically created private room, a user can request additional public rooms for their 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 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.

When users joining a conference are not assigned to the public room’s groups, the maximum bandwidth will be set by the user’s group and not the public room’s assigned group.

For more information, see [Adding a Meeting Room](#) and [Adding a New Group](#).

- 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 their bandwidth limitation—and the maximum number of participants that can be in their rooms. However, a public room can be assigned to a different group than the room owner.
2. Definitions

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 VidyoGateway) 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 4. Configuring Your Server.

Caution

You must refer to the Release Notes for your software version before starting the upgrade process. The "Upgrade Notices" section of the Release Notes 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.

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.

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.
3. Upgrading Your VidyoConferencing System

For more information, see Upgrading Your VidyoPortal System Software.

- **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.
  
  - Upgrading Your Hot Standby VidyoPortals while Taking Both Servers Offline
    
    For more information, see Upgrading Your Hot Standby VidyoPortals while Taking Both Servers Offline.

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 Scheduled and Public Room Settings.

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.
4. Configuring Your Server

Immediately after you have physically installed your Vidyo server, 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 the management of the VidyoPortal, VidyoRouter, and other Vidyo components.

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:

- Vidyo utilizes SSH to provide remote access to the System Administrator Console on your Vidyo server over port 22 or 2222. In addition, Vidyo Customer Support may request access to your Vidyo server over this same port in order to assist in troubleshooting any of your customer issues.

  When setting up your Vidyo server, always be sure to configure your firewall to only permit SSH access from authorized networks and users. Vidyo strongly recommends blocking SSH access from the Internet. You can restrict Vidyo Customer Support SSH access by configuring your firewall or contact Vidyo Customer Support for other options.

- Restrict the access to your management applications (vr2conf, and super) by performing one of the following:
  - Change each management application to an alternate HTTP/HTTPS port and restrict access to them using your firewall.
    For more information, see Configuring HTTPS Port Settings on Your Applications.
  - Move your management applications to the Management Interface (if you have not yet configured your Management Interface, it must be configured at this time).
    For more information, see 5. Configuring RADIUS.

- Change your System Administrator Console default password. This must be changed after the first log in. For more information, see the following procedure.

- Change the default password of your Super Admin account. For more information, see Editing Super Account Information and Changing the Password.

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

Now you can perform additional tasks such as requesting Vidyo system licenses and apply the system license keys to your system, changing the remaining default passwords, selecting the system language, and making other configurations.
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. Administrative tasks are managed by an Admin after the initial configuration has been completed. These tasks are explained in the following chapters.

Logging in to the System Console of Your Server and Changing the Default Password

The very first time you log into your 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)

Note The screenshots in this section show the System Admin Console (also known as the Shell menu) as seen after logging in via the terminal. The menu may look slightly different depending on how you connect and what tool you use for your connection.

To log in to your server and change the default password:

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

Note Press the Enter key after each prompt.

2. Log in using the default Administrator account:
   
   User Name: **admin**
   
   Password: **password** (case sensitive)
4. Configuring Your Server

3. Enter `admin` at the “login as” prompt.

4. Enter `password` at the “(current) UNIX Password” prompt.
   The password is case sensitive. You'll be prompted to enter a new password and asked to enter it again.

5. Enter a new password at the “Enter new UNIX password:” prompt.
   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 three 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 minimum password length (the default is length eight characters). The password gets extra points if it contains number, upper case, lower case, or special character. Each point is equivalent to one 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. Enter your new password again at the “Retype new UNIX password:” prompt.
If the passwords don’t match, you’ll be prompted to try again. If the passwords match, the System Console menu opens immediately.

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)

**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 Server and Changing the Default Password](#).

   The following illustrations show the System Console after you have logged in using a keyboard and VGA monitor plugged directly into the VidyoPortal.
2. Enter 1 to configure IP Address.

3. Press the Enter key.

4. Enter 1 to select the PRODUCTION INTERFACE option or 2 to select the MANAGEMENT INTERFACE option depending on which one contains the IP you want to configure.

5. Press the Enter key.

![Select Network Interface to Configure](image)

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

For more information, see 5. Configuring RADIUS.

6. Enter 1 to select the IPv4 (Static) option to set the server IP address, subnet mask, default gateway, and MAC addresses, hostname, domain name, and FQDN.

7. Press the Enter key on your keyboard after providing each value.

![Network Option for PRODUCTION interface](image)
4. Configuring Your Server

8. Enter `y` and press the `Enter` key after you have entered the required information.

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

Domain Name (optional): 
Hostname (optional):
Native FQDN: 
Public FQDN (optional): 

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

**Note** Unless you’re using the Hot Standby software option, the Native FQDN and Public FQDN should be the same.

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 the System License Keys to Your System* and *Appendix E. Hot Standby*.

The Public FQDN provided here is the same one you use when requesting your license keys from Vidyo Support. For more information, see *Requesting System Licenses and Applying System License Keys* and *Applying the System License Keys to Your System*.

9. Enter `2` to 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: 192.168.1.1
Secondary DNS Server for Host: 192.168.1.2

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

Primary DNS Server for Host (optional): 
```

b. Enter `y` and press the `Enter` key once you have entered the required information.

The System Console main menu displays.
4. Configuring Your Server

10. Enter the remaining network settings for the server as needed, confirming by typing `y` and pressing **Enter** after entering each prompt:

   a. Enter **3** to configure NTP Time Servers to set the NTP (Network Time Protocol) time server.
   
   b. Enter **4** to configure Time Zone to specify the time zone you are working in.
   
   c. Enter **5** to configure Ethernet Options to set the MTU (Maximum Transmission Unit) size if necessary.

11. Enter **14** to restart the server.

12. Press the **Enter** key.

   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 Other 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](#).

- **VidyoPortal/VidyoOne Administrator (per tenant)**
  
  Change the Administrator login as described in [Editing a User](#). 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 Server and Changing the Default Password](#).

- **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](#) and [Understanding the More Options System Administrator Console Menu](#).
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 Server and Changing the Default Password.

   **Note** Press the Enter key after each prompt.

2. Enter m for more options.

3. Enter 19 to access the User Maintenance menu.

   ![User Maintenance Menu]

   The User Maintenance screen provides the following options:

   a. Enter A to add a user.

   ![Add User]

   b. Enter B to remove a user.
4. Configuring Your Server

c. Enter C to show all user accounts.

d. Enter x to exit.

The current user is also shown on the User Maintenance menu.

---

**Note**

In addition to accessing 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 satisfy the password complexity requirements.

---

Understanding System Administrator Console Menu Options

The following list takes you through configurations on the System Console menu options.

The following describes the options on the Main Menu.

1. **Configure IP Address** – Enter 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.
4. Configuring Your Server

Configuration Example:

- **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:** example.com
- **Local FQDN:** vidyoportal.example.com
- **Public FQDN:** publicvidyoportal.example.com

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

For more information, see Configuring the Network Settings at the System Console and 5. Configuring RADIUS.

2. **Configure DNS Nameserver** – Enter 2 to specify the Domain Nameserver.

   Configuration Example:
   
   - **Primary DNS Server for Host:** 192.168.1.10
   - **Secondary DNS Server for Host:** 192.168.1.11

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

   Configuration Example:
   
   - **Primary NTP Server:** pool.ntp.org

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

   Configuration Example:
   
   - **US/Eastern**

5. **Configure Ethernet Options** – Enter 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.

   Configuration Example:
   
   - **MTU Size:** 1500
   - **Autonegotiation:** On
4. Configuring Your Server

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

6. **Display IP Address** – Enter 6 to view the IP address.

7. **Display DNS Nameserver** – Enter 7 to view the DNS servers.
   
   Configuration Example:

   **Primary DNS Server for Host:** 192.168.1.10
   
   **Secondary DNS Server for Host:** 192.168.1.11

8. **Query NTP Time Servers** – Enter 8 to query NTP server.
   
   This command doesn’t work if the domain name server is not defined.

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

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

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

12. **Traceroute Utility** – Enter 12 to run the utility.
   
   The system then prompts you for an IP address and port:

   - If you provide an IP address but do not provide the port, the system will display the trace route to the IP address you specified.
   
   - If you provide an IP address and also provide the port, the system will check if any ports in the firewall are blocking access to your Vidyo server, and then display them.

   Press **Enter** without providing an IP address to return to the Main Menu.

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

   Adhere to the password guidelines explained on page 14.

14. **Reboot system** – Enter 14 to restart your server.
   
   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** – Enter 16 to return HTTP settings to their default values (HTTP and port 80).

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

17. **... (more options)** – Enter m for a submenu containing additional options.

   For more information, see [Understanding the More Options System Administrator Console Menu](#).
4. Configuring Your Server

18. Exit System Administrator Console – Enter 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.

1. **Configure IP Address** – Enter 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.

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

3. **Display System ID** – Enter 18 to display system identification data including the Local Time, Universal Time, and the System ID.

4. **User Administration** – Enter 19 to perform user maintenance and create additional System Console accounts.
   
   For more information, see [Supporting Multiple System Console Accounts](#).

5. **Hot Standby** – This menu item only displays if you have the Hot Standby option applied on your system. Select H to access the Hot Standby menu.
   
   For more information, see [Appendix E. Hot Standby](#).

6. **Vidyo Support** – This menu enables a two-stage authentication process for the Vidyo Customer Support team that enables them to remotely SSH into the VidyoGateway for troubleshooting purposes.

7. **Advanced Options** – Enter A to access advanced options.

   For more information, see [Understanding the Advanced Options System Administrator Console Menu](#).

8. **Restart Web Services** – Enter W to restart your Web services.

9. **... (back to previous menu)** – Enter 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. **Enable FIPS-mode** – Enter 1 to enable or disable FIPS-validated security.

   For more information, see [Configuring FIPS on Your Vidyo Server](#).
2. **Network Route Management** – Enter 2 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](#).

3. **OCSP Information** – Enter 3 to view OCSP settings and enable or disable OCSP.

   For more information, see [Disabling OCSP from the System Console](#).

4. **SNMP Administration** – Enter 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](#).

5. **Hostname Management** – Enter 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](#).

6. **SSH Configuration** – Enter 6 for SSH Configuration menu options.

   For more information, see [Enabling Secure Shell Access on the Management Interface](#).

7. **Media Priority** – Enter M for Media Priority menu options including functions to add, remove, or remove all; navigate hostnames using Next or Previous; and exit the Hostname Management menu and return to the Advanced Options menu.

   For more information, see [Configuring Your VidyoRouter Media Priority](#).

8. **Download Login/Welcome Banner** – Enter R to download the welcome banner from your configured VidyoPortal.

9. **Configuration Service Accessibility** – Enter S to configure whether or not you will allow VidyoRouters to register to the VidyoPortal on your production or your production and management interfaces.

   For more information, see [Configuring Service Accessibility](#).

10. **Web Server Mode** – Enter W to access the Vidyo Web Server Mode menu, which allows you to enable or disable Privileged Mode.

11. **Exit Advanced Options** – Enter x to return to the More Options menu from Advanced Options.

---

**Configuring FIPS on Your Vidyo Server**

FIPS is the Federal Information Processing Standard 140-2. By default, FIPS mode is enabled on your Vidyo server.
4. Configuring Your Server

FIPS Certified Modules include the following:

- Vidyo’s SDK has been FIPS 140-2 validated:
- Third party applications, such as Apache, Net-SNMP, OpenSSH, and OpenSSL, have been built using the FIPS-validated OpenSSL module.

The following steps show you how to enable or disable FIPS mode from the System Console.

**To disable or enable FIPS mode:**

1. Log in to the System Console.
   
   For more information, see [Logging in to the System Console of Your Server and Changing the Default Password](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm).

2. Enter `m` for more options.

3. Enter `A` for Advanced Options.

4. Enter `1` to disable FIPS-mode.
   
   This setting toggles between disable and enable states.

5. Enter `y` to verify disabling (or enabling) the FIPS-mode change.

6. Enter `x` to exit Advanced Options.

7. Enter `14` to reboot the system.
   
   When your system comes back online, FIPS is then disabled (or enabled) on your Vidyo server.

**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.
4. Configuring Your Server

For more information, see Adding a Network Route.

To manage network routes:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter A for Advanced Options.
4. Enter 2 to select the Network Route Management option.

The *Route Management* screen displays. Use this screen to add, remove, or remove all routes, navigate routes using Next or Previous, and exit the *Route Management* screen.

5. Enter X to return to the Advanced Options menu.

Adding a Network Route

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 Server and Changing the Default Password.

   **Note** Press the Enter key after each prompt

2. Enter m for more options.
3. Enter A for Advanced Options.
4. Enter 2 to select the Network Route Management option.

5. Enter 1 to add a Network Route.

6. Enter the following information:

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

8. Enter X to return to the Advanced Options menu.
4. Configuring Your Server

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 Server and Changing the Default Password](#).

   **Note** Press the **Enter** key after each prompt.

2. Enter **m** for more options.
3. Enter **A** for Advanced Options.
4. Enter **2** to select the Network Route Management option.
5. Enter **2** to remove a Network Route.

![Route Management](image)

6. Select **y** to confirm removing the selected Network Route.
7. Select **X** to return to the Advanced Options menu.

Removing all of Your Network Routes

To remove all of your network routes:

1. Log in to the System Console.
   
   For more information, see [Logging in to the System Console of Your Server and Changing the Default Password](#).

   **Note** Press the **Enter** key after each prompt.

2. Enter **m** for more options.
3. Enter **A** for Advanced Options.
4. Configuring Your Server

4. Enter 2 to select the Network Route Management option.
5. Enter 2 to remove all of your Network Routes.
6. Enter y to confirm removing all of your Network Routes.
7. Enter X to return to the Advanced Options menu.

Navigating Your Network Routes

To navigate your network routes:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the Enter key after each prompt.

   2. Enter m for more options.
   3. Enter A for Advanced Options.
   4. Enter 2 to select the Network Route Management option.
      - Enter N to navigate to the next Network Route.
      - Enter P to navigate to the previous Network Route.
   5. Enter X 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.

The VidyoPortal traps include the following object identifiers (OIDs):

- **vidyoPortalManagerDown**
  - This trap indicates that the VidyoManager is not operational.
  - Triggered when the VidyoManager goes down, this trap can be turned on or off by setting the notification in the System Console.
  - This trap’s clearing notification is **vidyoPortalManagerUp**.

- **vidyoPortalRouterDown**
  - This trap indicates that the VidyoRouter is not operational.
4. Configuring Your Server

- Triggered when the VidyoRouter goes down, this trap can be turned on or off by setting the notification in the System Console.
- This trap’s clearing notification is `vidyoPortalRouterUp`.

**vidyoPortalVidyoProxyDown**
- This trap indicates that the VidyoProxy is not operational.
- Triggered when the VidyoProxy goes down, this trap can be turned on or off by setting the notification in the System Console.
- This trap’s clearing notification is `vidyoPortalVidyoProxyUp`.

**vidyoPortalGatewayDown**
- This trap indicates that the VidyoGateway component is not operational.
- Triggered when a VidyoGateway component goes down, this trap can be turned on or off by setting the notification in the System Console.
- This trap’s clearing notification is `vidyoPortalGatewayUp`.

**vidyoPortalReplayDown**
- This trap indicates that the VidyoReplay component is not operational.
- Triggered when a VidyoReplay component goes down, this trap can be turned on or off by setting the notification in the System Console.
- This trap’s clearing notification is `vidyoPortalReplayUp`.

**VidyoPortalDown**
- This trap indicates when the Tomcat or Apache web servers are not operational in your VidyoPortal.
- Triggered when the VidyoPortal goes down, this trap can be turned on or off by setting the notification in the System Console.
- This trap’s clearing notification is `vidyoPortalUp`.

**vidyoRouterVmConnLosAlert**
- This trap provides an indication that the VidyoRouter has lost contact with the VidyoManager.
- Triggered when the VidyoRouter is unable to contact the VidyoManager, this trap can be turned on or off by setting the notification in the System Console.
- This trap’s clearing notification is `vidyoRouterVmConnEstablishedAlert`.

**vidyoRouterCascadeBrokenAlert**
- This trap provides an indication that a conference cascade has been broken.
- Triggered when a conference cascade is broken, this trap can be turned on or off by setting the notification in the System Console.
This trap’s clearing notification is `vidyoRouterCascadeFixedAlert`.

**`vidyoRouterCascadeMediaQualityAlert`**

- This trap provides an indication that a conference cascade is having a problem with packet loss or jitter that may be affecting media quality in a conference.
- Triggered when a conference cascade is having a problem with packet loss or jitter, this trap can be turned on or off by setting the notification in the System Console.
- Specific threshold settings can be set for this trap via the SNMP manager as follows:
  - `vidyoRouterCascadeMediaAlertEnabled = TRUE`  
    This value is enabled by default.
  - `vidyoRouterCascadeMediaJitterThreshold: 10000 (in µs)`  
    The default value is 10 ms.
  - `vidyoRouterCascadeMediaLossThreshold: 100 (1 = .01%)`  
    The default value is 1%.
- This trap repeats every 30 seconds as long as the condition persists.

**`vidyoRouterParticipantMediaQualityAlert`**

- This trap provides an indication that a participant is having a problem with packet loss or jitter that may be affecting their media quality in a conference.
- Triggered when a participant is having a problem with packet loss or jitter, this trap can be turned on or off by setting the notification in the System Console.
- Specific threshold settings can be set for this trap via the SNMP manager as follows:
  - `vidyoRouterParticipantMediaAlertEnabled = FALSE`  
    This value is disabled by default.
  - `vidyoRouterParticipantMediaJitterThreshold: 10000 (in µs)`  
    The default value is 10 ms.
  - `vidyoRouterParticipantMediaLossThreshold: 100 (1 = .01%)`  
    The default value is 1%.
- This trap repeats every 30 seconds as long as the condition persists.

**`vidyoPortalFailoverOccurred`**

- This trap provides an indication that a VidyoPortal failover occurred.
- Triggered when a VidyoPortal failover occurs, this trap can be turned on or off by setting the notification in the System Console.
- This trap does not have a clearing notification.
4. Configuring Your Server

- **vidyoPortalLineConsumptionThresholdExceeded**
  - This trap provides an indication that the Lines license consumption threshold has been exceeded.
  - Triggered when the Lines license consumption threshold has been exceeded, this trap can be turned on or off by setting the notification in the System Console.
  - Specific threshold settings can be set for this trap via the SNMP manager. Measured as a percent, the default value is 0.
  - This trap’s clearing notification is **vidyoPortalLineConsumptionNormal**.

- **vidyoPortalInstallConsumptionThresholdExceeded**
  - This trap provides an indication that the installation license consumption threshold has been exceeded.
  - Triggered when the installation license consumption threshold has been exceeded, this trap can be turned on or off by setting the notification in the System Console.
  - Specific threshold settings can be set for this trap via the SNMP manager. Measured as a percent, the default value is 0.
  - This trap does not have a clearing notification.

**Note**

Some un-configurable object identifiers (OIDs) are standard on all Vidyo servers. With SNMP traps enabled, they provide notifications if the CPU, disk or memory utilization has reached its threshold (~80% utilization). The specific OIDs are cpuLoadReachedThreshold, diskReachedThreshold, and memoryReachedThreshold.


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 5. Configuring RADIUS.

**Enabling SNMP**

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

To enable SNMP:

1. Log in to the System Console.
   For more information, see [Logging in to the System Console of Your Server and Changing the Default Password](#).

   **Note** Press the **Enter** key after each prompt.

2. Enter `m` for more options.
3. Enter `A` for Advanced Options.
4. Enter `4` to select the SNMP Administration option.
5. Enter `A` to enable SNMP.
   The feature toggles between Enable and Disable states.
6. Enter `y` to confirm the change and enable or disable SNMP.
7. Enter `x` to exit the SNMP Administration menu.
8. Enter `x` to exit Advanced Options.
9. Enter `14` to reboot the 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 Server and Changing the Default Password](#).

   **Note** Press the **Enter** key after each prompt.

2. Enter `m` for more options.
3. Enter `A` for Advanced Options.
4. Enter `A` to select the SNMP Administration option.
5. Enter `B` to configure SNMPv2 Community String.
6. Select from the menu based on the SNMPv2 Community String type desired:
   a. Enter 1 to create a read-only SNMPv2 community string, and then enter the read-only community string.
      The user name must be at least eight characters and contain no spaces.
      After the read-only community string is created, the Create ReadOnly Community String option toggles and becomes the Delete ReadOnly Community String option.
   b. Enter 2 to create a read-write SNMPv2 community string, and then enter a read-write community string.
      The user name must be at least eight characters and contain no spaces.
   c. Enter 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.
   d. Enter x 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 Server and Changing the Default Password.

Note Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter A for Advanced Options.
4. Enter A to select the SNMP Administration option.
5. Enter B to configure SNMPv2 Community String.
6. Select from the menu based on the SNMPv2 Community String type desired:
   a. Enter 1 to delete the read-only SNMPv2 community string, and then enter y to confirm.
      After the read-only community string is deleted, the Delete ReadOnly Community String option toggles and becomes the Create ReadOnly Community String option.
   b. Enter 2 to delete a read-write SNMPv2 community string, and then enter y to confirm.
      After the read-write community string is deleted, the Delete ReadWrite Community String option toggles and becomes the Create ReadWrite Community String option.
   c. Enter x 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 Server and Changing the Default Password.

   Note Press the Enter key after each prompt.

2. Enter m for more options.
3. Select A for Advanced Options.
4. Select 4 to select the SNMP Administration option.
5. Select c to configure Local SNMPv3 User (User-based Security Model).
6. Select from the menu based on the SNMPv3 User type desired.
   a. Enter 1 to create a local SNMPv3 user with read-only access, and then enter a user name for your local SNMPv3 user with read-only access.
      The user name must be at least eight characters and contain no spaces.
   b. Enter and verify an authentication password of your choice.
      ▪ This password uses SHA authentication.
      ▪ The password must be at least eight characters.
      ▪ Vidyo does not currently support MD5 authentication.
   c. Enter and verify a second authentication password of your choice.
      ▪ This password uses AES encryption.
      ▪ The password must be at least eight 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.
   d. Select 2 to create a local SNMPv3 user with read-write access, and then enter a user name for your local SNMPv3 user with read-write access.
      The user name must be at least eight characters and contain no spaces.
4. Configuring Your Server

- Enter and verify an authentication password of your choice.
  - This password uses SHA authentication.
  - The password must be at least eight characters.
  - Vidyo does not currently support MD5 authentication.

- Enter and verify a second authentication password of your choice.
  - This password uses AES encryption.
  - The password must be at least eight 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.

- Enter x 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 Server and Changing the Default Password.

   - Press the Enter key after each prompt.

2. Select m for more options.

3. Select A for Advanced Options.

4. Select 4 to select the SNMP Administration option.

5. Select C to configure Local SNMPv3 User (User-based Security Model).

6. Select from the menu based on the SNMPv3 User type desired.
   - Select 1 to delete the local SNMPv3 user with read-only access.
   - Select y to confirm.
     - After the read-only user is deleted, the DeleteReadOnly User option toggles and becomes the Create ReadOnly User option.
   - Select 2 to delete the local SNMPv3 user with read-write access.
   - Select y to confirm.
     - After the read-write user is deleted, the Delete ReadWrite User option toggles and becomes the Create ReadWrite User option.
   - Select x to return to the SNMP Administration menu.
Configuring a 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 a SNMPv2 notification:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

Note Press the Enter key after each prompt.

2. Enter \textit{m} for more options.
3. Enter \textit{A} for Advanced Options.
4. Enter \textit{4} to select the SNMP Administration option.
5. Enter \textit{D} to configure SNMP Notification.
   The SNMP Notification menu displays.
6. Enter \textit{1} to select the SNMPv2 Notification option.
   The SNMPv2 Notification menu displays.
7. Enter \textit{1} to select the SNMPv2 Notification option.
8. Enter the IP or FQDN address of your network management server.
9. Enter \textit{I} or \textit{T} to configure an Inform or Trap notification type.
   The system asks for the values in the remaining steps if your notification type is Inform or Trap.
10. Enter your community string.
    The community string must be at least eight characters and contain no spaces.
11. Enter \textit{y} to confirm.
    After SNMPv2 notifications are created, they are listed in the top of the SNMPv2 Notification menu and Delete SNMPv2 Notification option displays as a second option.
12. Enter \textit{X} to return to the SNMP Notification menu.
Deleting a SNMPv2 Notification

To delete a SNMPv2 notification:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the **Enter** key after each prompt.

   2. Enter **m** for more options.
   3. Enter **A** for Advanced Options.
   4. Enter **4** to select the SNMP Administration option.
   5. Enter **D** to configure SNMP Notification.
      The SNMP Notification menu displays.
   6. Enter **1** to select the SNMPv2 Notification option.
      The SNMPv2 Notification menu displays.
   7. Enter **1** to select the SNMPv2 Notification option.
   8. Enter **2** to select the Delete SNMPv2 Notification option.
   9. Enter the number of the notification user you wish to delete.
   10. Select **y** to confirm.
   11. Select **X** to return to the SNMP Notification menu.

Creating a SNMPv3 Notification

To create a SNMPv3 notification:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the **Enter** key after each prompt.

   2. Enter **m** for more options.
   3. Enter **A** for Advanced Options.
   4. Enter **4** to select the SNMP Administration option.
   5. Enter **D** to configure SNMP Notification.
The SNMP Notification menu displays.

6. Enter 2 to select the SNMPv3 Notification option.
   The SNMP Notification menu displays.

7. Enter 1 to select the SNMPv3 Notification User option.

8. Enter the IP or FQDN address of your network management server.

9. Enter I or T to configure an Inform or Trap notification type.
   The system asks for the values in the remaining steps if your notification type is Inform or Trap.

10. Enter your Remote Engine ID if necessary.

11. Enter your user name.
    The user name must be at least eight characters and contain no spaces.

12. Enter and verify an authentication password of your choice.
    - This password uses SHA authentication.
    - The password must be at least eight characters.
    - Vidyo does not currently support MD5 authentication.

13. Enter and verify a second authentication password of your choice.
    - This password uses AES encryption.
    - The password must be at least eight 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 displays as a second option.

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

Deleting a SNMPv3 Notification

To delete a SNMPv3 notification:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the Enter key after each prompt.

2. Enter m for more options.

3. Enter A for Advanced Options.
4. Configuring Your Server

4. Enter 4 to select the SNMP Administration option.

5. Enter d to configure SNMP Notification.
   The SNMP Notification menu displays.

6. Enter 1 to select the SNMPv3 Notification option.
   The SNMPv3 Notification menu displays.

7. Enter 1 to select the SNMPv3 Notification option.

8. Enter 2 to select the Delete SNMPv3 Notification option.

9. Enter the number of the notification user you wish to delete.

10. Enter y to confirm.

11. Enter X 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 that 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 Server and Changing the Default Password.

Note  Press the Enter key after each prompt.

2. Enter m for more options.

3. Enter A for Advanced Options.
4. Enter 5 to select the Hostname Management option.

The Host Entries screen displays. 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 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 Server and Changing the Default Password.

   Note Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter A for Advanced Options.
4. Enter 5 to select the Hostname Management option.
5. Enter 1 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. Enter y to confirm the change and add your Hostname.
4. Configuring Your Server

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

8. Enter X 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 Server and Changing the Default Password.

   **Note**  Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter A for Advanced Options.
4. Enter 5 to select the Hostname Management option.
5. Enter 2 to remove a Hostname.
4. Configuring Your Server

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

7. Enter y to confirm removing the selected Hostname.

8. Enter X to return to the Advanced Options menu.

Removing all of Your Hostnames

To remove all of your hostnames:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   Note: Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter A for Advanced Options.
4. Enter 5 to select the Hostname Management option.
5. Enter 2 to remove all of your Hostnames.
6. Enter y to confirm removing all of your Hostnames.
7. Enter X to return to the Advanced Options menu.
Navigating Your Hostnames

To navigate your hostnames:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the **Enter** key after each prompt.

2. Enter **m** for more options.
3. Enter **A** for Advanced Options.
4. Enter **5** to select the Hostname Management option.
   a. Enter **N** to navigate to the next Hostname.
   b. Enter **P** to navigate to the previous Hostname.
5. Select **X** to return to the Advanced Options menu.

Enabling Secure Shell Access on the Management Interface

As a System Console Administrator, you can enable secure shell access (SSH) to the Management Interface of your system for you and other System Console Administrator accounts. This option is disabled by default.

**Note** When SSH is enabled on your Vidyo server, it runs on port 2222.

Secure shell access (SSH) is only permitted on the Management interface. If you enable SSH, be sure to setup whitelist IP filters to ensure access is only granted to specific machines.

**To create System Console accounts:**

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the **Enter** key after each prompt.

2. Enter **m** for more options.
3. Enter **A** for Advanced Options.
4. Configuring Your Server

4. Enter 5 to enable SSH.

5. Enter y to change the current setting.

Enabling an Emergency Admin User

As a System Console Administrator, you can enable a single Emergency Admin user. This option is disabled by default.

Note: The Emergency Admin user can only access the system with a directly connected keyboard and monitor.

The Emergency Admin user can only log in via the System Console and re-enable and reset a System Console Admin user’s password. When enabled, the Emergency Admin user’s default password is password. You should immediately change this password; however, note that this password does not have to adhere to the password guidelines explained on page 14.

In order to reset a System Console Admin user’s password, you must know the username. The user’s password is automatically reset to the default password, which is password.

To enable an emergency admin user:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

Note: Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter A for Advanced Options.
4. Enter 7 to select Emergency User.
The Emergency Account menu provides the following options:

- Enter A to add (or remove) the emergency account.

- Enter B to show the emergency account.

- Enter C to change the password of the emergency account.

Note When enabled, the Emergency Admin user’s default password is password. You should immediately change this password; however, note that this password does not have to adhere to the password guidelines explained on page 14.

- Enter X to exit.

Configuring Your SSH Port

You can configure your SSH port to either 22 or 2222.

To configure your SSH port:

1. Log in to the System Console.

   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

Note Press the Enter key after each prompt.

2. Enter m for more options.

3. Enter A for Advanced Options.
4. Configuring Your Server

4. Enter **6** to select the SSH Configuration option.

![SSH Configuration]

5. Enter **1** to toggle 22 and 2222 options.
6. Enter **y** to confirm.
7. Enter **x** to exit.
8. Enter **x** to exit Advanced Options.
9. Enter **14** to reboot the system.

When your system comes back online, your SSH port is changed.

**Configuring Your VidyoRouter Media Priority**

You can configure the media priority to allow media traffic on your production interface only, or you can allow it on both production and management interfaces but must give priority to either one.

**To configure your VidyoRouter media priority:**

1. Log in to the System Console.
   
   For more information, see [Logging in to the System Console of Your Server and Changing the Default Password](#).

   **Note** Press the **Enter** key after each prompt.

2. Enter **m** for more options.
3. Enter **A** for Advanced Options.
4. Enter **P** to select the Media Priority option.

![VidyoRouter Media Priority](image)

**Note** Confirming any change to your VidyoRouter media priority selection will disrupt active calls on your system.

Select from the menu based on the interface prioritization you want your VidyoRouter to give media in your system:

- Enter **1** to select the PRODUCTION (default) option to only allow media traffic on your production interface, and then enter **y** to confirm.
- Enter **2** to select the PRODUCTION and MANAGEMENT option to allow media traffic on both production and management interfaces, but give priority to production, and then enter **y** to confirm.
- Enter **3** to select the MANAGEMENT and PRODUCTION option to allow media traffic on both production and management interfaces, but give priority to management, and then enter **y** to confirm.

5. Enter **x** to return to the Advanced Options menu.

### Configuring Service Accessibility

You can configure whether or not you will allow VidyoRouters to register to the VidyoPortal on your production interface only, or both your production and management interfaces.

**To configure service accessibility:**

1. Log in to the System Console.
   
   For more information, see [Logging in to the System Console of Your Server and Changing the Default Password](#).

   **Note** Press the Enter key after each prompt.

2. Enter **m** for more options.
4. Configuring Your Server

3. Enter A for Advanced Options.

4. Enter S to select the Service Accessibility option.

![Configuration Service Accessibility]

Note  Confirming any change to your service accessibility selection will disrupt active calls on your system.

Select from the menu based on which interfaces you want to allow your VidyoRouter to register to the VidyoPortal:

- Enter 1 to select the PRODUCTION (default) option to only allow VidyoRouters to register to the VidyoPortal on your production interface, and then enter y to confirm.
- Enter 2 to select the PRODUCTION and MANAGEMENT option to permit media traffic on both production and management interfaces, but give priority to production, and then enter y to confirm.

5. Enter x to exit Advanced Options.

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 or FQDN address (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 address]/super
4. Configuring Your Server

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.
2. Click the *Components* tab.

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).
4. Configuring Your Server

**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 an 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 out keys 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 licenses@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 licenses@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 the System License Keys to Your System](#).

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 the System License Keys to Your System.

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

**Setting the Language for the Super Admin Interface**

The VidyoPortal’s Super Admin interface is available in these 15 languages:

- Chinese (Simplified)
- Chinese (Traditional)
- English
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish
- Thai
- Turkish
- Japanese
**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 VidyoDesktop interfaces.

**To set the language of your Super Admin portal:**

1. You can set the language of your Super Admin portal in either of the following ways:
   - Use the language drop-down on the upper-right corner of the *Super Admin Login* page.
   - Use the *Super Account* screen from inside the Super Admin portal:
     a. Log in to the Super Admin portal using your Super Admin account.
        For more information, see *Logging in to the Super Admin Portal*.
        The *Components* page displays by default.
     b. Click the *Settings* tab.
     c. Click *Super accounts* on the left menu.
2. Select the Super Admin’s language from the **Language** drop-down.

3. 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](#).

2. Click the **Settings** tab. The **Upload System License** page displays by default.

3. Click **Super accounts**.
4. Configuring Your Server

The *Super Accounts* page displays.

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

5. Enter field values for your new Super Account.

   Fields marked with an asterisk cannot be left blank.
Caution: Each Super Account is required to have a valid, resolvable email address in order to function properly in your VidyoConferencing system.

6. Select the **Enable** checkbox to enable the account.

7. Click **Save**.

For information about super accounts, see [Managing Your Super Accounts](#).
5. Configuring RADIUS

The Remote Authentication Dial-In User Service (RADIUS) can be enabled for VidyoPortal, VidyoRouter, and VidyoGateway servers. This configuration is optional and you do not have to install it unless you plan on using RADIUS.

Disabling FIPS Mode

RADIUS configuration is allowed only when the Vidyo server has FIPS disabled. If FIPS is enabled, follow the procedures in this section to disable it. If FIPS is already disabled, then proceed to the Enabling RADIUS section.

To disable FIPS mode:

1. Log in to the System Console.

Note Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter A for Advanced Options.

Advanced Options:

1. Enable FIPS-mode
2. Network Route Management
3. OCSP Information
4. SNMP Administration
5. Hostname Management
6. Disable SSH
7. Emergency User
8. DSCP Configuration
9. Download Login/Welcome Banner
x. Exit Advanced Options

Selection: 

4. Enter 1 to disable FIPS mode.

Note This setting toggles between disable and enable states.

A message displays stating the following: CDR access and RADIUS authentication are allowed with FIPS-mode disabled.
5. Enter y to verify disabling FIPS mode.

```
Advanced Options:
------------------
1. Disable FIPS mode
2. Network Route Management
3. OCSP Information
4. SNMP Administration
5. Hostname Management
6. Disable SSH
7. Emergency User
8. DSIP Configuration
9. Download Login/Welcome Banner
x. Exit Advanced Options

Selection: 1

CDR access and RADIUS authentication are allowed with FIPS-mode disabled.

Verify FIPS-mode to be disabled [y/n] : y
```

6. Press the Enter key on your keyboard to return to the Advanced Options menu.

Enabling RADIUS

To enable RADIUS:

1. Log in to the System Console.

**Note** Press the Enter key after each prompt.

2. Enter 19 to access the User Maintenance menu.
3. Enter d to select the RADIUS Authentication option.
4. Enter y for the change settings prompt.
5. Enter y for the confirm enable radius prompt.

6. Enter the IP or FQDN of the RADIUS server or leave blank to cancel.

7. Enter the preshared key for the RADIUS server.

8. Enter the IP or FQDN for additional RADIUS servers or leave blank to finish.

Note A maximum of 10 RADIUS servers are supported.

9. Enter the preshared key for the additional RADIUS server.

10. Enter the IP or FQDN for additional RADIUS server or leave blank to finish.

Note In the following screenshot, two RADIUS servers were configured causing this prompt to display. This prompt will only display if two or more RADIUS servers are being configured. If you do not have additional RADIUS servers to configure, leave blank to finish.

RADIUS is enabled.
11. Press any key on your keyboard to return to the User Maintenance menu.

Viewing the Current RADIUS Configuration

You should always review your RADIUS server configurations for accuracy.

To view the current RADIUS configuration:

1. Log in to the System Console.

   **Note** Press the **Enter** key after each prompt.

2. Enter **D** to select the RADIUS Authentication option.

   The RADIUS server configurations display.

3. Enter **n** for the change settings prompt if the configuration does not need to be modified.

   **Note** Enter **y** for the change settings prompt if the configuration needs to be modified, and proceed to step 4 in the **Modifying the RADIUS Configuration** section.
5. Configuring RADIUS

Modifying the RADIUS Configuration

To modify the RADIUS configuration:

1. Log in to the System Console.

Note: Press the Enter key after each prompt.

2. Enter D to select the RADIUS Authentication option.
   The RADIUS server configurations display.

3. Enter y for the change settings prompt if the configuration needs to be modified.

Note: If you enter y for the change settings prompt, then all RADIUS server configurations will need to be re-entered.

4. Re-enter the IP or FQDN of the RADIUS server or leave blank to cancel.

5. Re-enter the preshared key for the RADIUS server.

6. Re-enter the IP or FQDN for additional RADIUS servers or leave blank to finish.

Note: A maximum of 10 RADIUS servers are supported.

7. Re-enter the preshared key for the additional RADIUS server.

8. Re-enter the IP or FQDN for any additional RADIUS server or leave blank to finish.
5. Configuring RADIUS

Note In the following screenshot, two RADIUS servers were configured causing this prompt to display. This prompt will only display if two or more RADIUS servers are being configured. If you do not have additional RADIUS servers to configure, leave blank to finish.

RADIUS is enabled.

9. Press any key on your keyboard to return to the User Maintenance menu.

Creating a RADIUS-Enabled Account

To create a RADIUS-enabled account:

1. Log in to the System Console.

Note Press the Enter key after each prompt.

2. Enter A for Advanced Options.

3. Enter a unique username.
   The username must match your RADIUS User ID.

4. Enter y for the confirm changes prompt.

5. Enter y for the user to be authenticated via RADIUS prompt.

Note Enter n if you do not want the user to be authenticated via RADIUS, and proceed to the Creating a Local System Console Account section.
Viewing a RADIUS-Enabled Account

You should always review the new RADIUS-enabled account for accuracy.

To view a RADIUS-enabled account:

1. Log in to the System Console.

   **Note** Press the **Enter** key after each prompt.

2. Enter **19** to access the User Maintenance menu.

3. Enter **C** to select the Show User(s) option.
   
   A list of current users in the system displays. If the new user is set up incorrectly, then proceed to the **Removing a RADIUS-Enabled Account** section.

4. Press any key on your keyboard to return to the User Maintenance menu.
Removing a RADIUS-Enabled Account

To remove a RADIUS-enabled account:

1. Log in to the System Console.

Note Press the Enter key after each prompt.

2. Enter B to select the Remove User option.
3. Enter the username to be removed.
4. Enter y for the confirm changes prompt.

```
--- User Maintenance ---
[A] - Add User
[B] - Remove User
[C] - Show User(s)
[D] - RADIUS Authentication
[X] - Exit
---
CURRENT USER: vidyoqa
=> b
Please enter username to remove: radius
You are about to remove username (radius)
Confirm changes ? [y/n]y
```

Disabling RADIUS Authentication

To disable RADIUS authentication:

1. Log in to the System Console.

Note Press the Enter key after each prompt.

2. Enter 19 to access the User Maintenance menu.
3. Enter D to select the RADIUS Authentication option.
   Details about the RADIUS server display.
4. Enter y for the change settings prompt.
5. Enter \textbf{n} for the leave RADIUS enabled prompt.  
RADIUS is disabled.

6. Press any key on your keyboard to return to the User Maintenance menu.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{user_maintenance.png}
\caption{User Maintenance Menu}
\end{figure}

Creating a Local System Console Account

\textbf{To create a local System Console account:}

1. Log in to the System Console.

\begin{itemize}
  \item \textbf{Note} Press the \textbf{Enter} key after each prompt.
\end{itemize}

2. Enter \textbf{A} for Advanced Options.
3. Enter a unique username.
4. Enter \textbf{y} for the confirm changes prompt.
5. Enter \textbf{n} for the user to be authenticated via RADIUS prompt.
6. Enter \textbf{password} for the current UNIX password.

Enter a unique password that follows these password complexity requirements:

- 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 three characters should be different from the old password.
- The password should not be too simple or too short.
5. Configuring RADIUS

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

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

7. Re-enter your new password for the retype new UNIX password prompt.

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

**Note** When you need to reset the password, use **13. Set 'admin' password**. However, if you are logged in with a RADIUS-enabled account and need to use this option, then your account will be converted back to a local System Console account with the standard default password at the next login.

In addition, when using the emergency user functionality with a RADIUS-enabled account, the account will be converted back to a local System Console account as well.
6. 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 and VidyoRouter’s vr2conf
- 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, in the System Console, and in the Applications page of the Super Admin interface:

<table>
<thead>
<tr>
<th>Physical Interface</th>
<th>System Console and Super Admin Applications Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1</td>
<td>PRODUCTION</td>
</tr>
<tr>
<td>G2</td>
<td>MANAGEMENT</td>
</tr>
</tbody>
</table>

**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.

**Note**

Press the Enter key after each prompt.

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

2. Enter option 1 to configure IP Address.
3. Enter `y` to change the current settings.

![Select Network Interface to Configure](image)

4. Enter `2` to select the MANAGEMENT INTERFACE option.

5. Enter the IP address and Subnet Mask for the Management Interface.

**Note** The Management Interface supports only IPv4 addresses.

6. Enter `y` to save the configuration.

7. Enter `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.

   The *Upload System License* page displays by default.

3. Click + to the left of *Security* on the left menu.
6. Enabling the Management Interface

4. Click *Applications* from the submenu.

5. 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 in the Network Interface column.
   
   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.

6. 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.
6. Enabling 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:

1. 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 Pages:
   
   `[yourVidyoRouter.yourorganization.com]/vr2conf`

2. Click the *Settings* tab.
   The *Upload System License* page displays by default.

3. Click + to the left of *Security* on the left menu.

4. Click *Applications* from the submenu.

5. Look in the Applications column for the application that you want to move to your VidyoRouter Management Interface, and then select *MANAGEMENT* from the drop-down in the Network Interface column.
   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.
6. 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: `vidyogateway.example.com`.

2. Navigate to **Maintenance > Security**.

3. Click the **Ports** subtab.

4. 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.

5. 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:

1. Log in to the System Console. For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   Note Press the Enter key after each prompt.

2. Enter m for more options.

3. Enter A for Advanced Options.

4. Select 2 to select the Network Route Management option.

5. Enter 1 to add a new route.

6. Enter the Destination IP or Network (using Slash notation for the subnet mask).
6. Enabling the Management Interface

7. Enter the IP address of the route you want to use.

8. Select y to confirm your changes.
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 License
- Platform Network Settings
- Upload Endpoint Software
- Maintenance
- Super accounts
- Customization
- Security
- Inter-Portal Communication
- Endpoint Network Settings
- Feature Settings

*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](#).
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** 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](#).

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](#).

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.

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:

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 currently being used:

- 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.
7. Configuring System Settings as the Super Admin

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

The Components page displays by default.

2. Click the Settings tab.

The Upload System License page displays by default.

![Upload System License](image)

3. Click Browse.

![Browse Button](image)

4. 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.

   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.

5. Upload the license file for all VidyoPortal versions:
   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.

6. Click **Upload** to apply the license.

7. Click the **Tenants** tab and edit the Default Tenant by clicking the **Default Tenant Name**.

8. Allocate the full set of licenses to the Default Tenant.

9. Click **Save**.

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

For more information, see [Restarting Your System](#).
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 Your Vidyo Licenses.

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.

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 apply 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 the System License Keys to Your System.
2. 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 Appendix E. Hot Standby.

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 Appendix E. Hot Standby.

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.
2. Perform the steps as explained in the previous section on your Active VidyoPortal. For more information, see Applying the System License Keys to Your System. The license replicates to your Standby VidyoPortal automatically.

Understanding Vidyo License Consumption by User Type

<table>
<thead>
<tr>
<th>VidyoLines Licensing Model</th>
<th>User Type</th>
<th>VidyoLines*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Super Admin</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Admin</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Operator</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Executive Desktop</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Normal User</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Guest</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>VidyoRoom (used for VidyoRoom as well as for VidyoPanorama 600)</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>VidyoGateway</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>VidyoPanorama 1.0</td>
<td>–</td>
</tr>
</tbody>
</table>

* 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, 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 warning when five installations are left. Your current installs never expire. If you run out, you won’t be able to add any new users who need to install the software until you purchase more installation licenses.

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. 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.

![Platform Network Settings](image)

### 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 username 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".)
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 not to 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 that 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](#).

   The *Components* page displays by default.

2. Click the *Settings* tab.

   The *Upload System License* page displays by default.

3. Click *Upload Endpoint Software* on the left menu.

   The *Upload Endpoint Software* page displays.

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

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

5. Click *Browse*.

6. Locate the installation file on your computer and click *Upload* to import it.
7. Configuring System Settings as the Super Admin

**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.

Since Super Admin endpoint software uploads overwrite Tenant Admin uploads, Tenant Admins should always upload files on their tenants after Super Admin uploads are completed.

When the endpoint installation file is uploaded, it displays in the Uploaded Endpoint Software list under its corresponding heading. Scroll through this list to view all available installation files.

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](#).

   The *Components* page displays by default.

2. Click the *Settings* tab.

   The *Upload System License* page displays by default.

3. Click *Upload Endpoint Software* on the left menu.

   The *Upload Endpoint Software* page displays.

4. Select the checkbox to the left of the file name that needs to be activated.

   **Tip**: Use the top-left checkbox to select or clear all of the software file checkboxes.

5. Click *Activate* at the top or bottom of the list.
The file name displays 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.

Depending upon whether the Vidyo Neo or VidyoDesktop client installer file is uploaded and activated, either the Vidyo Neo Client or VidyoDesktop Client is automatically pushed to users who are logged into the system. Users who do not have Vidyo Neo or VidyoDesktop installed will be instructed to download and install either application when clicking a room link or navigating to the VidyoPortal’s FQDN.
7. Configuring System Settings as the Super Admin

Vidyo Neo Client Landing Page

After activating Vidyo Neo on the tenant and clicking a room link to join a conference, an HTML landing page displays. The HTML landing page appears as follows:

Note This page will look different depending upon the browser (e.g., Chrome, Firefox, Internet Explorer, Safari, and Edge) and OS used (e.g., OS X, Windows).

![Vidyo Neo Client Landing Page](image)

- Vidyo Neo will attempt to connect if you already have Vidyo Neo installed. The client does not have to be running in order to launch, but must be installed.

Note Depending on the OS and browser used, a browser pop-up may display and ask for your permission to launch the application. For browsers (e.g., Chrome and Firefox) that display this alert, you are advised to select the **Remember my choice** checkbox so that this alert doesn’t display again.

  This alert is automatic and Vidyo does not control it.

- The **Join via the browser** option displays if the Super Admin has enabled Vidyo Neo for WebRTC access in the Super Admin Portal **Settings > Feature Settings > Vidyo Neo for WebRTC** page.

  For more information, see [Enabling Vidyo Neo for WebRTC access](#).

- If you do not have Vidyo Neo already installed (hence you are not connected to the conference), you are advised to download the client by clicking **Download**.

  You do not need to enter a VidyoPortal FQDN in the **VidyoPortal** field upon logging in, which only displays when you click the **Sign in to a different portal** button, since it will be
auto-populated when downloading Vidyo Neo for Desktop. However, if you want to enter a different VidyoPortal FQDN, click the **Sign in to a different portal** button.

For more information, refer to the latest *Vidyo Neo for Desktop Administrator Guide*.

- You do not need to re-click the room link after downloading the client since the room key is automatically propagated upon clicking the meeting link.

**VidyoDesktop Client Landing Page**

After activating VidyoDesktop on the tenant and clicking a room link to join a conference, an HTML landing page displays. The HTML landing page appears as follows:

**Note** You will only see this page when VidyoDesktop is installed and running.
7. Configuring System Settings as the Super Admin

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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click Upload Endpoint Software on the left menu.
   The Upload Endpoint Software page displays.

4. Select the checkbox to the left of the file name that needs to be deleted.
   Tip: Use the top-left checkbox to select or clear all of the software file checkboxes.

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, hostname, NTP), the SSL security certificates loaded and CSR information, and the license keys (each of these would need to be reset separately should a unit need to be replaced/rebuilt). For more information about the CDR database, see Appendix D. CDR.

The Database page 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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click ☕ to the left of Maintenance on the left menu.
4. Click Database from the submenu. The Database page displays.

5. Click Backup.

A pop-up displays.

6. Enter an encrypted password in the Password field.

7. Re-enter the password in the Confirm Password field to confirm.

8. Click Backup.

A backup copy of the database is made on the VidyoPortal. A pop-up displays confirming a successful backup.

9. 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.
7. Configuring System Settings as the Super Admin

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.
   The Components page displays by default.
2. Click the Settings tab.
   The Upload System License page displays by default.
3. Click ➕ to the left of Maintenance on the left menu.
4. Click Database from the submenu.
   The Database page displays.
5. Select the checkbox to the left of the file name that needs to be downloaded.
6. Click Download.

Your selected .veb file or files then download through your Web browser.
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.
   The Components page displays by default.
2. Click the Settings tab.
   The Upload System License page displays by default.
3. Click ➕ to the left of Maintenance on the left menu.
4. Click Database from the submenu.
   The Database page displays.
5. Click **Upload** at the top of the *Database* page.

The *Uploading backup file* pop-up displays.

6. Click **Browse…**
7. Locate and select the file from the file selection dialog box.
8. Click **Open**.
9. Click **Upload** in the *Uploading backup file* pop-up.
   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.

**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](#).
   The *Components* page displays by default.
2. Click the Settings tab.

The Upload System License page displays by default.

3. Click to the left of Maintenance on the left menu.

4. Click Database from the submenu.

The Database page displays.

5. Select the checkbox to the left of the file name that needs to be restored.

6. Click Restore.

A Confirmation pop-up displays.

7. Click Yes.

8. Reboot your VidyoPortal.

For steps to reboot your VidyoPortal, see Restarting Your System.

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.
7. Configuring System Settings as the Super Admin

**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. Follow the [Uploading a Backup File](#) procedure for the desired version of the database on your local machine to put the file back on the VidyoPortal.

2. Follow the [Restoring a Backup File Located on Your VidyoPortal](#) procedure to restore the backup file.

**Deleting a Backup File Located on Your 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](#).

2. Click the **Settings** tab.

3. Click **Database** from the submenu.

4. Select the checkbox next to the version that needs to be deleted.

5. Click **Delete** at the bottom of the **Database** page.

6. Confirm the action in the pop-up that displays.
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](#).
   
   The Components page displays by default.

2. Click the Settings tab. The Upload System License page displays by default.

3. Click ☰ to the left of Maintenance on the left menu.

4. Click Database from the submenu. The Database page displays.

5. Click Factory Defaults at the top of the Database page.

6. Confirm the action in the pop-up that displays.

Upgrading Your VidyoPortal System Software

The System Upgrade page 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 Notes that pertains 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).
7. Configuring System Settings as the Super Admin

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.

The Components page displays by default.

2. Click the Settings tab.

The Upload System License page displays by default.

3. Click to the left of Maintenance on the left menu.

4. Click the Upgrade from the submenu.

The System Upgrade page displays.

5. Click Browse....

6. Locate and select the .vidyo file from the file selection dialog box.

7. Click Open.
8. Click **Upload**.

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](#).

### Restarting Your System

The *Restart* page 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](#).
   
   The *Components* page displays by default.

2. Click the **Settings** tab.

   The *Upload System License* page displays by default.

3. Click **+** to the left of *Maintenance* on the left menu.

4. Click **Restart** from the submenu.

   The *System Restart* page displays.

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.

A pop-up displays asking you to confirm the action.

6. 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 disconnected. Therefore, you may want to email users ahead of time and perform the upgrade when system usage is at its lowest.

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

For more information, see the [Appendix D. CDR](#).

**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](#).
   The **Components** page displays by default.

2. Click the **Settings** tab.
   The **Upload System License** page displays by default.

3. Click **Maintenance** on the left menu.

4. Click **CDR Access** from the submenu.
   The **CDR Access** page displays.

5. Leave the **CDR Collection** and **CDR Database Access Control** checkboxes selected, and enter the following information:
   - Enter your **Username** as cdraccess (limited to read and delete privileges).
7. Configuring System Settings as the Super Admin

- Enter your **Password**, which is configured using the VidyoPortal Admin portal.
- Enter your VidyoDashboard **IP or Hostname**.

![VidyoPortal Admin Portal](image)

**Note**  Providing the IP or Hostname on this page provides remote access 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`.

6. Leave the **Allow Delete** checkbox selected if desired.

7. Click **Save**.

### Exporting and Purging CDR Files from the Super Admin Portal

For more information about the CDR, see **Appendix D. CDR**.

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

1. Log in to the Super Admin portal using your Super Admin account.
7. Configuring System Settings as the Super Admin

For more information, see Logging in to the Super Admin Portal.

The Components page displays by default.

2. Click the Settings tab.

The Upload System License page displays by default.

3. Click to the left of Maintenance on the left menu.

4. Click CDR Access from the submenu.

The CDR Access page displays by default.

5. Leave the CDR Collection and CDR Database Access Control checkboxes selected, and enter your username, password, and IP hostname.

6. Leave the Allow Delete checkbox selected if desired.

7. Select either the One tenant or All tenants checkbox and a Date Range for your CDR record Export or Purge in the CDR Export/Purge... section.

8. 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 displays 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.
7. Configuring System Settings as the Super Admin

Downloading System Logs

Audit Logs

The system logs all activity on the VidyoPortal. The information logged in the Audit Logs 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 16. Auditing. VidyoPortal audit logs can be generated using either a Super Admin or the Audit user account.

To download Audit Logs:

1. Log in to the Super Admin portal using your Super Admin account. For more information, see Logging in to the Super Admin Portal. The Components page displays by default.

2. Click the Settings tab. The Upload System License page displays by default.

3. Click to the left of Maintenance on the left menu.

4. Click System Logs from the submenu. The System Logs page displays.

5. Enter a Start Date and End Date to retrieve the Audit Logs within that specific time period.
7. Configuring System Settings as the Super Admin

6. Click **Download Audit Logs**.

The browser downloads the `.csv` file.

**VidyoPortal Logs**

The VidyoPortal logs include information that may be used by the Customer Support team to troubleshoot an issue that occurred with the system.

**To download VidyoPortal Logs:**

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

   The **Components** page displays by default.

2. Click the **Settings** tab.

   The **Upload System License** page displays by default.

3. Click 📂 to the left of **Maintenance** on the left menu.

4. Click **System Logs** from the submenu.

   The **System Logs** page displays.

5. Click **Download VidyoPortal Logs**.
7. Configuring System Settings as the Super Admin

The VidyoPortal Logs pop-up displays for the administrator to enter a password for encrypting the data.

6. Enter a password if you want to protect the .zip file of logs.
7. Re-enter the password to confirm if necessary.

Note This password will be required when attempting to unzip the file. Leave the Password and Confirm Password fields blank if you do not wish to protect the .zip file.

8. Click Export.

   The browser downloads the .zip file.

Note The .zip file may take a few minutes to start downloading depending upon the size of the file and/or speed of your Internet connection.

Downloading Specific VidyoPortal Installation Logs

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

To download specific VidyoPortal installation logs:

1. Log in to the Super Admin portal using your Super Admin account.
   For more information, see Logging in to the Super Admin Portal.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click to the left of Maintenance on the left menu.

4. Click System Logs from the submenu.
   The System Logs page displays.
5. Select the checkbox to the left of the VidyoPortal installation patch that needs to be downloaded.

6. Click **Download**.

   ![Image of VidyoPortal installation log]

   The browser downloads the VidyoPortal installation log.

**Creating a System Diagnostic File**

You can analyze your system health by creating a system diagnostic file and viewing the results. Depending on your system, the diagnostic file shows the following information:

- Date
- Tenant Report
- SMTP Configuration Report
- Type of Node
- Status Notification Report
- Ports
- FDQN
- EMCP Report
- License Tokens
- IP Address
- SCIP Report
- Ethernet Hardware Report
- DNS Server Report
- VidyoProxy Report
- Certificate Check

To create a system diagnostic 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](#).

   The **Components** page displays by default.

2. Click the **Settings** tab.

   The **Upload System License** page displays by default.

3. Click **+** to the left of **Maintenance** on the left menu.
4. Click Diagnostics from the submenu.
   
   The Diagnostics page displays.

5. Click Run.

   The Result pop-up displays.

6. Click OK.

7. Refresh your browser.

   Your system diagnostic file now displays in the list.

**Viewing a System Diagnostic File**

You can view a system diagnostic file by viewing it on your VidyoPortal or downloading it for further analysis.

**To view a system diagnostic 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](#).

   The Components page displays by default.

2. Click the Settings tab.

   The Upload System License page displays by default.

3. Click ➩ to the left of Maintenance on the left menu.

4. Click Diagnostics from the submenu.
7. Configuring System Settings as the Super Admin

The Diagnostics page displays.

5. Select the checkbox to the left of the file name you wish to download.
   **Tip**: Use the top-left checkbox to select or clear all of the software file checkboxes.

6. Click View.

The View Diagnostics Report pop-up displays.

7. Click Close.
7. Configuring System Settings as the Super Admin

Downloading a System Diagnostic File

You can download a system diagnostic file for further analysis.

**To download a system diagnostic 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](#).

   The *Components* page displays by default.

2. Click the *Settings* tab.

   The *Upload System License* page displays by default.

3. Click ➔ to the left of *Maintenance* on the left menu.

4. Click *Diagnostics* from the submenu.

   The *Diagnostics* page displays.

5. Select the checkbox to the left of the file name that needs to be downloaded.

6. Click *Download*.

   Your selected .txt file downloads via your Web browser.

Enabling Syslogs

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

**Note**  
Syslog is only supported over TCP.

Syslog information consists of the audit log information. For more information about audit logs, see [16. Auditing](#).
To enable Syslogs:

1. Log in to the Super Admin portal using your Super Admin account. For more information, see Logging in to the Super Admin Portal.
   
   The Components page displays by default.

2. Click the Settings tab.
   
   The Upload System License page displays by default.

3. Click ☰ to the left of Maintenance on the left menu.

4. Click the Syslog from the submenu.
   
   The Syslog page displays.

5. Select the Enabled checkbox.
   
   When enabled, Use Encryption, Remote Syslog Server, and Remote Port fields become active.

6. Select Use Encryption if desired.

7. Enter the Remote Syslog Server location.

8. Enter the Remote Port for your syslog server.

9. Click Save.
7. Configuring System Settings as the Super Admin

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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click ☕ to the left of Maintenance on the left menu.

4. Click Status Notify from the submenu.
   The Status Notify page displays.

5. Select the Enabled checkbox.

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.
7. Configuring System Settings as the Super Admin

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](#).

**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:

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

   The *Components* page displays by default.

2. Click the *Settings* tab.

   The *Upload System License* page displays by default.

3. Click *Super accounts* on the left menu.

   The *Super Accounts* page displays.

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.

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 Adding Multiple Super Admin Accounts.

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.
7. Configuring System Settings as the Super Admin

The *Components* page displays by default.

2. Click the *Settings* tab.
   The *Upload System License* page displays by default.

3. Click *Super accounts* on the left menu.
   The *Super Accounts* page displays.

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* checkbox.
   The *Password* and *Verify Password* fields display.

6. Enter your current password in the *Your Current Password* field.

7. Enter your new password in the *New Password For The User* field.
7. Configuring System Settings as the Super Admin

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

9. Click **Save** to complete the password change.

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

Customizing the System

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

Customizing the About Info

The *About Info* page enables you to create and format an About Us page that displays 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.

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.

**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.

   The *Components* page displays by default.

2. Click the *Settings* tab.

3. The *Upload System License* page displays by default.

4. Click ➕ to the left of *Customization* on the left menu.
7. Configuring System Settings as the Super Admin

The About Info page displays.

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.

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.
   The Components page displays by default.
2. Click the Settings tab.
   The Upload System License page displays by default.
3. Click ☁ to the left of Customization on the left menu.
4. Click the About Info from the submenu.
7. Configuring System Settings as the Super Admin

The About Info page displays.

5. Click Default to remove any previously saved customized text and revert to the default system text provided by Vidyo.

A Confirmation pop-up displays.

6. 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 displays 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.
7. Configuring System Settings as the Super Admin

**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](#).

**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](#).
   The *Components* page displays by default.
2. Click the *Settings* tab. 
   The *Upload System License* page displays by default.
3. Click + to the left of *Customization* on the left menu.
4. Click the *Support Info* from the submenu. 
   The *Support Info* page displays.
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](#).

**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](#).
   The *Components* page displays by default.
2. Click the *Settings* tab. 
   The *Upload System License* page displays by default.
3. Click + to the left of *Customization* on the left menu.
4. Click *Support Info* from the submenu.
7. Configuring System Settings as the Super Admin

The Support Info page displays.

5. Click Default to remove any previously saved customized text and revert to the default system text provided by Vidyo.

A Confirmation pop-up displays.

6. 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** If a From address is not provided, SMTP servers may block emails or change email headers.

Notification customizations completed at the Super Admin level can be overridden at the Tenant level by Tenant Admins.
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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click ➕ to the left of Customization on the left menu.

4. Click Notification from the submenu.
   The Notification page displays.

5. Select the Enable Email Notifications checkbox to activate the addresses and settings you configured.

6. Enter valid email addresses in the Email (From) and Email (To) fields.

7. Provide the following SMTP and Security information:
   a. Enter the SMTP Hostname.
   b. Enter the SMTP Port.
   c. Select either NONE, STARTTLS, or SSL/TLS from the Security drop-down.
7. Configuring System Settings as the Super Admin

d. Select the Trust All Certs checkbox if desired.
e. Enter the SMTP Username.
f. Enter the SMTP Password.

8. 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 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.

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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click + to the left of Customization on the left menu.

4. Click the Invite Text from the submenu.
7. Configuring System Settings as the Super Admin

The *Invite Text* page displays.

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

The following system variables (uppercase text inside of brackets) display and can be inserted in sections of your invite text using the following buttons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Available in the Email Content and Voice Only sections, the <code>[DIALIN_NUMBER]</code> variable inserts the dial-in number of your room into your invite text.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Available in the Email Content and Voice Only sections, the <code>[PIN_ONLY]</code> variable inserts the PIN (if one is configured) of your room into your invite text.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Available in the Email Content and Voice Only sections, the <code>[EXTENSION_ONLY]</code> variable inserts the room extension (if one is configured) into your invite text.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>Required in the Email Content section, the <code>[ROOMLINK]</code> variable inserts a hyperlink to your room into your invite text. When accessed from a tablet, roomlinks may be used to join a conference, annotate, or manage a meeting.</td>
</tr>
</tbody>
</table>
7. Configuring System Settings as the Super Admin

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Available in the Email Content section, the [LEGACY_URI] variable inserts the URI participants will use to access your room from Legacy endpoints.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Available in the Email Content section, the [DIALSTRING] variable inserts the phone number participants will use to access your room voice-only telephones.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Required in the Webcast section, the [WEBCASTURL] variable inserts the URL participants can use to access your webcast.</td>
</tr>
</tbody>
</table>

Some additional variables (ones that do not have buttons or icons) and display in sections of your invite text include:

- The [DISPLAYNAME] variable inserts the specific user’s display name as it was entered in to the system in the Email Content section.
- The [EXTENSION] variable inserts the room extension (if one is configured) along with the room PIN (if one is configured) into your invite text.
- The [PIN] variable inserts the room PIN (if one is configured) in the Email Content section.
- The [ROOMNAME] variable inserts name of the room for which the invite was issued.
- The [TENANTURL] variable inserts the name of the tenant in the Email Content section.

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.

6. Click **Save** to save the invitations.

### Making Common Invite Text Changes

You can make the following common changes to invite text:

- If your organization uses mobile devices that support a tap-to-connect functionality, you can add the following template to your invite: Voice only users can tap-to-connect: "[DIALIN_NUMBER], [EXTENSION]#".
- 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**  Some browsers may not support email invitation generation due to a limitation on the number of characters in the invite text. Vidyo recommends that you generate the email invitation prior to making that text the default, and reduce the number of characters if needed.

## Reverting To Default System Text on the Invite Text Screen

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](#).

**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](#).

   The **Components** page displays by default.

2. Click the **Settings** tab.

   The **Upload System License** page displays by default.

3. Click **Customization** to the left of **Customization** on the left menu.

4. Click the **Invite Text** from the submenu.

   The **Invite Text** page displays.

5. Click **Default** to remove all custom invitations and revert to the default text supplied by Vidyo.
7. Configuring System Settings as the Super Admin

A Confirmation pop-up displays.

6. 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.

The customized logos per tenant display on the HTML-based Control Meeting screen.

For more information, see Controlling Meetings.

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.

   The Components page displays by default.

2. Click the Settings tab.
   
   The Upload System License page displays by default.

3. Click + to the left of Customization on the left menu.

4. Click the Customize Logos from the submenu.
   
   The Customize Logos page displays.
5. Click the Select File icons for the corresponding logo you wish to upload.

Logos can be uploaded for the following system locations:

- The *Super and Admin Portal Logo* section 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 *VidyoDesktop Download and Control Meeting Pages Logo* section updates the logo used for your VidyoDesktop Download page shown to users when a software update is performed and the Control Meeting page shown to meeting moderators.

  **Note** The uploaded 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 Meetings](#).

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 displays 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]

   The *Components* page displays by default.

2. Click the *Settings* tab.
   
   The *Upload System License* page displays by default.

3. Click ![arrow] to the left of *Customization* on the left menu.
   
   The *VidyoConferencing Administrator Guide* page displays.

4. Click *Guides Properties* from the submenu.
5. Select a language from the **System Language** drop-down 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 *Upload file for new guide (.pdf, .doc, or .docx)* pop-up displays with the **Store Locally** checkbox selected by default.

7. Store your selected guide locally on your VidyoPortal using the following steps:
   a. Select the **Store Locally** radio button.
   b. Click the **Select File** icon.
   c. Locate your guide and click **Open**.
   d. Click **Upload** to store it locally.
7. Configuring System Settings as the Super Admin

8. Select the **Link to a different web server** radio button to link to a guide located on a different web server using the following steps as an alternative:
   a. Select the **Link to a different web server** radio button.
   
   ![Upload file for new guide (pdf, .doc, or .docx)](image)
   
   b. Enter the web server URL file location where your new guide is stored in the **Enter URL** field.
   
   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](#), [Setting the Language for the Admin Interface](#), and [Setting the Tenant Language](#).

**Customizing Your VidyoPortal Login and Welcome Banners**

The *Login banner* is a dialog box that displays 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 displays 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.
7. Configuring System Settings as the Super Admin

The *Login banner* displays with text customized by your Super or Tenant administrator.

![Home Page Banner](image)

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](#).
The *Welcome banner* displays with text customized by your Super or Tenant administrator and your last 5 login attempts in a table.

<table>
<thead>
<tr>
<th>Result</th>
<th>Source Address</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>123.45.67.89</td>
<td>02/09/2016 10:57:52 AM</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>123.45.67.89</td>
<td>02/09/2016 10:41:02 AM</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>123.45.67.89</td>
<td>02/08/2016 17:19:03 PM</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>123.45.67.89</td>
<td>02/08/2016 15:50:24 PM</td>
</tr>
<tr>
<td>SUCCESS</td>
<td>123.45.67.89</td>
<td>02/08/2016 15:27:10 PM</td>
</tr>
</tbody>
</table>

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

- The result; refers to 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.

4. Click **Continue**.

The *Components* page displays by default.

**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](#).
   
   The *Components* page displays by default.

2. Click the **Settings** tab.
   
   The *Upload System License* page displays by default.

3. Click **+** to the left of *Customization* on the left menu.

4. Click **Banners** from the submenu.
7. Configuring System Settings as the Super Admin

The Banners page displays.

5. Select the Login Banner checkbox to activate the login banner.
6. Enter your desired text and formatting for your login banner.
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.
   The Components page displays by default.
2. Click the Settings tab.
   The Upload System License page displays by default.
3. Click to the left of Customization on the left menu.
4. Click Banners from the submenu.
   The Banners page displays.
5. Select the Welcome Banner checkbox to activate the welcome banner.
6. Enter your desired text and formatting for your welcome banner.
7. Click Save.

Customizing Room Links

You can customize the key length and format for guest room meeting links.

To customize room links:

1. Log in to the Super Admin portal using your Super Admin account.
   For more information, see Logging in to the Super Admin Portal.
   The Components page displays by default.
2. Click the Settings tab.
   The Upload System License page displays by default.
3. Click to the left of Customization on the left menu.
4. Click Room Link from the submenu.
5. Enter a value between 8 and 25 in the **Room Key Length** field.

6. Select the appropriate **Room Link format** radio button.

   The first format is the traditional format and the second format is a new simplified format. The selected room format will appear in all meeting invitations. Regardless of selection, both formats will always work.

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](#).

   The **Components** page displays by default.

2. Click the **Settings** tab.

   The **Upload System License** page displays by default.

3. Click 📦 to the left of **Security** on the left menu.

4. Click **Passwords** from the submenu.
5. Provide the following information:

- Enter the desired number of days in the **Number of days before password expires** field.

**Note** The Number of days before password expires and Number of days of inactivity before a password change is forced settings do not apply to LDAP or SAML auto-provisioned accounts.

- 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 attempts in the Number of failed login attempts before account is locked field.

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

- Select the **Enforce password complexity rules** checkbox if necessary.
  - Passwords must be at least 15 characters long.
  - Passwords must contain at least two uppercase alphabetic characters.
  - Passwords must contain at least two lowercase alphabetic characters.
  - Passwords must contain at least two numeric characters.
  - Passwords must contain at least two non-alphanumeric (special) characters.
  - Password must contain no more than two consecutive repeating characters.
7. Configuring System Settings as the Super Admin

**Note** When password complexity is enabled on a system with user accounts already configured, only Admin and Super Admin users are forced to change their passwords on their next login attempt. Normal users will not be prompted to change their passwords; however, if they choose to subsequently change their passwords, the complexity rules are enforced. The complexity rules are also enforced on any newly created VidyoPortal accounts.

- Select the **Disable password recovery for Super Accounts** checkbox if necessary. When checked, the **Forgot Your Password** link will not be available for Super users and they will not have the option recover their password.

- Enter the desired number of hours for keeping the client session active in the **Client Session Expiration Period (Hours)** field. When the period expires, the clients will be automatically logged off and requested to re-enter their credentials.

- Enter the desired minimum length for the user configured PINs including Personal, Public, Webcast, and Moderator PINs in the **Minimum Length for User Configurable PINs (Personal, Public, Webcast Moderator)** field.

**Note** The Minimum PIN Length does not apply to PINs for Scheduled Meeting Rooms.

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](#).

   The **Components** page displays by default.

2. Click the **Settings** tab.

   The **Upload System License** page displays by default.

3. Click **Security** to the left of **Security** on the left menu.

4. Click **Passwords** from the submenu.

   The **Passwords** page displays.

5. Click **Default** to remove all custom password settings and revert to the default values supplied by Vidyo.

**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.
7. Configuring System Settings as the Super Admin

A Confirmation pop-up displays.

6. 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 Appendix C. Security.

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 Adding a Default Tenant or Adding a New Tenant.

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, 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.
7. Configuring System Settings as the Super Admin

To configure system-wide IPC:

1. Log in to the Super Admin portal using your Super Admin account.
   For more information, see Logging in to the Super Admin Portal.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click Inter-Portal Communication on the left menu.
   The Inter-Portal Communication page displays.

4. Select Tenant to give Tenant Admins control over IPC.
   For more information, see Adding a Default Tenant or Adding a New Tenant.

5. Select System to configure system-wide IPC settings by adding or deleting allowed or blocked domains or addresses.

6. Select the router pool from the Router Pool drop-down.
   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 Configuring Router Pools.

7. Select your desired access control mode to add or delete domains or addresses from allowed or blocked lists as follows:

- Select **Allowed List** from the Access Control Mode options to add or delete a permitted domain or address as follows:
  - If you want to add an allowed domain:
    a. Click **Add**.
    b. Enter the Internet domain to be added to the list.
    c. Click **OK**.
  - If you want to delete an allowed domain:
    a. Click the existing domain you want to delete from the list.
    b. Click **Delete**.
7. Configuring System Settings as the Super Admin

- Select **Blocked List** from the Access Control Mode options to add or delete a restricted domain or address as follows:
  - If you want to add a blocked domain:
    a. Click **Add**.
    b. Enter the Internet domain to be added to the list.
    c. Click **OK**.
  - If you want to delete a blocked domain:
    a. Click the existing domain you want to delete from the list.
    b. Click **Delete**.

8. Click **Save** to save your list.

---

**Note**

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

- It’s a good idea to advise your users that you have enabled IPC and they can use the VidyoDesktop search box to place external calls to users on a different VidyoPortal and other domains (unless you have restricted them).

- Use the following syntax as a guide for making an IPC call on different VidyoPortals:
  
  `[Username on other VidyoPortal]@[IP or FQDN address of other VidyoPortal].com`

  For more information, refer to the *VidyoDesktop Quick User Guide*.

---

**Telling Your Users About IPC**

The *VidyoDesktop Quick User Guide* explains 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 *VidyoDesktop Quick 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 the 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 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 **vido.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.

### Configuring Endpoint Network Settings

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 are assigned corresponding values that 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.

You may tag packets as a non-Administrative user, if desired, using Windows Group Policy settings. Sites may be able to establish domain policy rules implementing these settings.


**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.
7. Configuring System Settings as the Super Admin

You can also configure the media port range and enable use of the VidyProxy on the *Endpoint Network Settings* page.

**To configure quality of service values for endpoints**

1. Log in to the Super Admin portal using your Super Admin account. For more information, see [Logging in to the Super Admin Portal](#).
   The *Components* page displays by default.

2. Click the *Settings* tab.
   The *Upload System License* page displays by default.

3. Click *Endpoint Network Settings* on the left menu.
   The *Endpoint Network Settings* page displays.

![Endpoint Network Settings](image)

4. Enter DSCP values for Video, Audio, Content, and Signaling. Values provided must be decimals from 0 to 63. The values default to 0.

5. Enter the appropriate values in the fields in the Media Port Range section.

6. Click *Save*.
   A *Confirmation* pop-up displays.
7. Configuring System Settings as the Super Admin

7. Click Yes.

A message displays stating that 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.

![Message]

Setting Global Features

The Feature Settings left menu item allows you to control the system-wide behavior of VidyoWeb, VidyoMobile, Search Options, VidyoProxy, Chat, and Scheduled Rooms on your VidyoPortal.

Enabling VidyoWeb Access

The VidyoWeb browser extension 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.


For more information about configuring VidyoWeb on tenants, see Configuring VidyoWeb on Your Tenant. 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 enable 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. The Components page displays by default.

2. Click the Settings tab. The Upload System License page displays by default.

3. Click ☐ to the left of Feature Settings on the left menu.

4. Click VidyoWeb from the submenu. The VidyoWeb page displays.

The current version of VidyoWeb displays in the Version field.

5. Deselect the Make VidyoWeb available on your VidyoPortal checkbox to restrict VidyoWeb use on your system or leave selected.

6. Select the Default VidyoWeb option for tenants checkbox to configure whether or not VidyoWeb will be used as the default setting for new tenants in your system or leave deselected.

7. Click Save.
Enabling Vidyo Neo for WebRTC access

Vidyo Neo™ for WebRTC Server allows you to use desktop and mobile browsers that support WebRTC to join conferences on VidyoPortal without installing browser plugins or extensions. For more information, refer to the Vidyo Neo for WebRTC Server Administrator Guide.

To enable Vidyo Neo for WebRTC access:

1. Log in to the Super Admin portal using your Super Admin account. For more information, see Logging in to the Super Admin Portal.
   
   The Components page displays by default.

2. Click the Settings tab.
   
   The Upload System License page displays by default.

3. Click 🔄 to the left of Feature Settings on the left menu.

4. Click Vidyo Neo for WebRTC from the submenu.
   
   The Vidyo Neo for WebRTC page displays.

5. Select the Enable Vidyo Neo for WebRTC for guests checkbox if you want to allow invited guests to join calls via Vidyo Neo for WebRTC.

6. Select the Enable Vidyo Neo for WebRTC for users checkbox if you want to allow users to join calls via Vidyo Neo for WebRTC.

7. Click Save.
8. Configure the URL of the Vidyo Neo for WebRTC Server for each tenant that will use Vidyo Neo for WebRTC.

See Adding a Default Tenant or Adding a New Tenant.

---

**Note**

Enabling Vidyo Neo for WebRTC for users is useful if you have users on platforms for which there is not currently a Vidyo Neo Desktop client, such as Chromebooks and Linux desktops. However, users that are currently logged in will reserve the same resources on the Vidyo Neo for WebRTC Server whether or not they are on a call.

Once the Super Admin has enabled Vidyo Neo for WebRTC, the tenant Admin may enable or disable the feature for their tenant.

---

**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.


  For more information about configuring VidyoMobile on tenants, see Adding a Default Tenant or Adding a New Tenant. 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 enable 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.

   The Components page displays by default.

2. Click the Settings tab.

   The Upload System License page displays by default.

3. Click ☑️ to the left of Feature Settings on the left menu.

4. Click VidyoMobile from the submenu.
The *VidyoMobile* page displays.

5. Select one of the following options:
   - Select the **Enabled** radio button to give VidyoMobile access to all tenants.
   - Select the **Disabled** radio button 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 the **Individual Setting Per Tenant** radio button is selected here. The following examples provide clarification:
     - With the **Disabled** radio button selected, and at some point later VidyoMobile access is enabled for even one tenant (as described in Adding a Default Tenant or Adding a New Tenant), **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, the **Individual Setting Per Tenant** radio button will be selected.
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 Adding a Default Tenant or Adding a New Tenant.

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 display in search results on your VidyoPortal by using Search Options.

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

1. Log in to the Super Admin portal using your Super Admin account.
   For more information, see Logging in to the Super Admin Portal.
   The Components page displays by default.
2. Click the Settings tab.
   The Upload System License page displays by default.
3. Click ‹ to the left of Feature Settings on the left menu.
4. Click Search Options from the submenu.
5. Select the **Show disabled rooms in search results** checkbox to allow disabled rooms to display in search results on your VidyoPortal or leave deselected.

6. Click **Save**.

**Configuring Transport Layer Security (TLS) VidyoProxy**

You can enable or disable TLS for VidyoProxy on your VidyoPortal. Establishing a TLS tunnel between the VidyoProxy and the VidyoPortal significantly increases connectivity success rates as most firewalls block non-TLS traffic on port 443. This feature is disabled by default.

**Note** When turned on, only endpoints supporting this feature can connect via VidyoProxy. For more information, refer to the documentation for your Vidyo endpoints.

**To configure the TLS VidyoProxy:**

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

   The **Components** page displays by default.

2. Click the **Settings** tab.

   The **Upload System License** page displays by default.

3. Click **+** to the left of **Feature Settings** on the left menu.
4. Click VidyoProxy from the submenu.

The VidyoProxy page displays.

5. Select the Enabled or Disabled radio button to enable or disable TLS VidyoProxy on your VidyoPortal.

6. Click Save.

All of your VidyoProxies automatically restart.

Configuring System-Wide Public and Private Chat

You can configure system-wide public and private chat.

To configure system-wide public and private chat:

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

   For more information, see Logging in to the Super Admin Portal.

   The Components page displays by default.

2. Click the Settings tab.

   The Upload System License page displays by default.

3. Click + to the left of Feature Settings on the left menu.

4. Click Chat from the submenu.
The Chat page displays.

5. Deselect the Make chat available on your VidyoPortal checkbox to deny the availability of chat on your VidyoPortal or leave selected.

6. Deselect the Public chat default option checkbox to deny public chat on newly created tenants or leave selected.

7. Deselect the Private chat default option checkbox to deny private chat on newly created tenants or leave selected.

8. Click Save.

Configuring Scheduled and Public Room Settings

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 scheduled and public room 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.

   The Components page displays by default.

2. Click the Settings tab.

   The Upload System License page displays by default.
3. Click ‌to the left of *Feature Settings* on the left menu.

4. Click *Room* from the submenu.

The *Room Attributes* page displays.

5. Deselect the *Make Scheduled Rooms available on your VidyoPortal* checkbox to allow scheduled rooms on your VidyoPortal or leave selected.

6. Enter a numeric prefix in the *Scheduled Room Prefix* field.

**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.

7. Deselect the *Allow Public Room creation by users* checkbox to deny users the ability to create public rooms or leave selected.

8. Enter the maximum number of public rooms that the user can create in the *Maximum number of rooms per User* field.

9. Enter the minimum number of digits for auto-generated extensions in the *Minimum number of digits for auto-generated extensions* field.

10. Click *Save*.

**Configuring User Attributes**

You can allow or restrict tenants from uploading their own thumbnail photos.
7. Configuring System Settings as the Super Admin

**Note** In order to use this feature, the Vidyo endpoint must also support it.

If the tenant uploads a thumbnail photo, it will override LDAP and SAML provided images. When the tenant authenticates, the LDAP or SAML thumbnail photo is retrieved only if they have not uploaded a photo.

To configure user attributes:

1. Log in to the Super Admin portal using your Super Admin account. For more information, see [Logging in to the Super Admin Portal](#).
   
   The **Components** page displays by default.

2. Click the **Settings** tab.
   
   The **Upload System License** page displays by default.

3. Click **+** to the left of **Feature Settings** on the left menu.

4. Click **User Attributes** from the submenu.
   
   The **User Attributes** page displays.

5. Select the **Enable Thumbnail Photos** checkbox to allow the **User Attributes** menu item to display under **Settings > Feature Settings** in the Admin Portal, giving tenants the option to upload thumbnail photos.
7. Configuring System Settings as the Super Admin

Additional fields display.

![User Attributes](chart)

6. Select the **Allow users to upload their own image** checkbox if you want to give tenants the option to allow their users to upload their own image, which causes the **Allow users to upload their own image** checkbox to display in the tenant’s **Settings > Feature Settings > User Attributes** page.

7. Enter a value in the **Maximum image size in KB** field.
   The default value is 100.

8. Click **Save**.
8. 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 for the functioning of the VidyoPortal.

  **Caution** Do not perform any tasks on the VidyoManager other than those described below. Many VidyoManager tasks including ones indicated in the following section should only be completed 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, 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.

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.

   The Components page displays by default.

   Components in your VidyoPortal display in the table and include component Status, Name, Type, IP, Version, Config Version, ID, and Management URL as columns:

   a. The following statuses display on the Manage Components table.
      
      - A green arrow in the status column means it’s installed and operating.
      - A yellow arrow means the component is newly installed, but not configured yet.
      - A red arrow means the component isn’t working. Hover your mouse pointer over the red arrow to read its alarm message.
      - A gray arrow means the component is disabled, typically when you take a component offline while performing maintenance.

   b. The Name column displays the descriptive name you provided when installing a component.
c. The Type column displays the specific type of component as VidyoManager, VidyoRouter, or VidyoGateway.

d. The IP Address column displays the IP address you assigned to the component when you created it.

e. The Version column displays the specific software version of the component.

f. The Config Version column displays a numeric tally on the left side of the slash. The number increases each time you change a component’s configuration.

g. The ID column displays the identification assigned to the component when you created it.

h. The Management URL column displays the linked URL that takes you to the component’s console page.

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 display for the optional VidyoGateway component.

An alarm symbol displays next to the component’s status when the component is not working properly. Hover your mouse pointer over it to read a brief description of the fault.

The checkbox 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.

2. Search by component name or type using the Component Name field or Type drop-down above the table.

If desired, you can also select the Delete, Enable, and Disable buttons.

The table automatically refreshes.

- 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.
8. Configuring Your Components as the Super Admin

**Note** Deleting a VidyoGateway or VidyoReplay component from the Manage Components table does not disable or delete the component itself. Disabling or deleting the VidyoGateway or VidyoReplay components, must be done from their respective Configuration pages.

You can access the Configuration pages of each registered component by clicking the Name shown in the Components table.

You can access the component’s own local webpage configuration screen by clicking the Management URL 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](#).

---

**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](#).
   
   The Components page displays by default.

2. Double-click on the blue link in the Name column for the VidyoManager component.
The *VidyoManager* pop-up displays.

![VidyoManager pop-up](image)

**3.** View and enter the following information:

a. The **ID** shows your VidyoManager ID, which is automatically created and set by the system. This value cannot be changed.

b. Enter a display name or label for your VidyoManager in the **Display Name** field. These address and port values are then used by VidyoDesktop, VidyoRoom, and VidyoGateway clients to communicate with your VidyoManager.

c. The **Management URL** shows the address the VidyoManager uses to communicate with the VidyoPortal.

**Note** Do not change this address.

d. Enter the appropriate port in the **EMCP Port** field.

**Note** Do not change the address value unless required for NAT traversal or enabling Security.

Before editing the EMCP settings, see Appendix A. Firewall and Network Address Translations (NAT) Deployments and Appendix C. Security.

If you’re using FQDN licensing, the EMCP address is read-only.
8. Configuring Your Components as the Super Admin

   e. The **SOAP Port** field allows your VidyoPortal to communicate with your VidyoManager.
   f. The **RMCP Port** field allows your VidyoRouter to connect to the VidyoManager.
   g. Enter the appropriate FQDN in the **FQDN** field.
   h. The **DSCP** value will be used for VidyoManager connections.

4. Click **Save**.

Configuring Your VidyoRouter Component

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

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](#).

   The **Components** page displays by default.

2. Double-click on the blue link in the Name column for the VidyoRouter component.
3. Enter the following information:

   The ID shows your **VidyoRouter ID**, which is automatically created and set by the system. This value cannot be changed.

   a. Enter a display name or label for your VidyoRouter in the **Name** field.
8. Configuring Your Components as the Super Admin

The Management URL shows the address the VidyoManager uses to communicate with the VidyoPortal.

---

**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.

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

---

**Configuring VidyoRouter SCIP Settings**

Before editing SCIP settings, see Appendix A. Firewall and Network Address Translations (NAT) Deployments and Appendix C. Security.

To configure VidyoRouter SCIP 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](#).
   
   The Components page displays by default.

2. Double-click on the blue link in the Name column for the VidyoRouter component.
   
   The VidyoRouter pop-up displays.

3. Enter a FQDN and Port in the SCIP section.
   
   These FQDN 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.

---

**Configuring VidyoRouter Media Port Range Settings**

To configure VidyoRouter media port range 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](#).
   
   The Components page displays by default.

2. Double-click on the blue link in the Name column for the VidyoRouter component.
   
   The VidyoRouter pop-up displays.

3. Enter a value in the Start and End fields in the Media Port Range section.
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.
   The Components page displays by default.

2. Double-click on the blue link in the Name column for the VidyoRouter component.
   The VidyoRouter pop-up displays.

3. 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 Endpoint Network Settings on Your Tenant.

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 Appendix A. Firewall and Network Address Translations (NAT) Deployments.

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.
   The Components page displays by default.

2. Double-click on the blue link in the Name column for the VidyoRouter component.
   The VidyoRouter pop-up displays.
8. Configuring Your Components as the Super Admin

3. Enter the following information:

**Note**  The Media Address Map feature is the preferred configuration option. Only enter values for NAT Firewall fields or Media Address Map fields. Enabling both options and by entering values for each causes the system to malfunction.

a. Enter an IP and port of a STUN server in the NAT Firewall fields.
   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. Enter an IP and port in the Media Address Map fields.
   If the system is NATed with a 1:1 port mapping, hence no port translation, you can define local <-> 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** checkbox 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.

**Accessing Your VidyoRouter Configuration Page**

The URL of your VidyoRouter is typically a domain name: `http://[IP or FQDN address]/vr2conf`. You can also click the **Management URL** link for the VidyoRouter on the **Components** tab in your VidyoPortal.
8. Configuring Your Components as the Super Admin

For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

Although the default username for this page is admin, only the Super Admin accesses these pages.

**Configuring Basic Settings on Your VidyoRouter**

To configure basic settings on your VidyoRouter:

1. Log in to your VidyoRouter using your System Console account.

2. Enter the IP or FQDN address of your VidyoPortal.

3. Click Apply for the VidyoRouter to register.
8. Configuring Your Components as the Super Admin

Configuring Security on Your VidyoRouter

Entering information on this tab is optional. For detailed VidyoRouter security information, see Appendix C. Security.

![Security Configuration on VidyoRouter](image)

Viewing System Information on Your VidyoRouter

To view system information on your VidyoRouter:

1. Log in to your VidyoRouter using your System Console account.

![System Information Login on VidyoRouter](image)

The Maintenance > Basic page displays by default.

2. Click Platform Network Settings on the left menu.
8. Configuring Your Components as the Super Admin

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

![Vidyo Router System Information](image)

**Upgrading Your VidyoRouter**

The *System Upgrade* tab is used for upgrading your VidyoRouter software version, downloading installation logs history, and viewing installed patches.

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 VidyoRouter 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 VidyoRouter, 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 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](#).

   The *Components* page displays by default.
2. Click on the Management URL link for the VidyoRouter (as shown in the following illustration) or navigate to http://[VidyoRouter Server IP or FQDN address]/vr2conf to access the VidyoRouter Configuration Pages.

3. Enter your VidyoRouter Administrator username and password. The default username is admin and the default password is password.

4. Click Login. The Maintenance > Basic page is selected by default.
8. Configuring Your Components as the Super Admin

5. Click the *System Upgrade* subtab.

![System Upgrade Subtab](image)

**Note** You can determine your VidyoRouter type by viewing the version label displayed to the right of the Maintenance title. The version number also ends with either 64-bit or 32-bit.

The *Uploading new server software file* pop-up displays.

6. Click the *Select File* (곧) icon.

7. Locate and select the *.vidyo* file from the file selection dialog box.

8. Click *Open*.

9. Click *Upload* from the *Uploading new server software file* pop-up.

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

Once the upload completes, your VidyoRouter 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.

10. Return to the Super Admin portal and click the Components tab after the VidyoRouter reboots.

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, delete the DOWN component, or attempt to clear the Alarm at this time. Each will update or clear automatically once the VidyoPortal is upgraded.

11. Verify that the Software Version displayed is correct for the VidyoRouter that you upgraded.

12. Repeat the steps in this section for each additional VidyoRouter in your VidyoConferencing system.

Downloading Your VidyoRouter Installation Logs History

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

To download VidyoRouter 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.
8. Configuring Your Components as the Super Admin

The *Components* page displays by default.

2. Click on the Management URL link for the VidyoRouter or navigate to http://[VidyoRouter Server IP or FQDN address]/vr2conf to access the VidyoRouter Configuration Pages.

3. Enter your VidyoRouter Administrator username and password.
   The default username is *admin* and the default password is *password*.

4. Click Login.
   The *Maintenance > Basic* page displays by default.
5. Click the **System Upgrade** subtab.

![System Upgrade Subtab](image)

6. Select the checkbox to the left of the file name you wish to download.

7. Click **Download**.

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

---

**Viewing Installed Patches in Your VidyoRouter**

You can view the installed patches in your VidyoRouter from the **System Upgrade** tab.

**To view installed patches 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](#).

2. Click the **Components** tab.
   
   The **Manage Components** left menu item is selected by default.
8. Configuring Your Components as the Super Admin

3. Click on the VidyoRouter IP address (as shown in the following illustration) or browse to http://[VidyoRouter Server IP or FQDN address]/vr2conf to access the VidyoRouter Configuration Pages.

4. Enter your VidyoRouter Administrator username and password. The default username is admin and the default password is password.

5. Click Login.
   The Maintenance > Basic page displays.
6. Click the *System Upgrade* subtab.

All of the patches you have installed on your VidyoRouter display on the Installed Patches section of the screen.

**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 will end.

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 pop-up that asks you to confirm your intent to log out of the VidyoRouter.

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 landlines and cell phones, to participate in videoconferences.

VidyoGateway configuration requires cumulative steps performed on both the VidyoGateway and the VidyoPortal as described in the following procedures. Complete all of the following steps on your VidyoGateway and VidyoPortal in the order that they display.

Note  If you are clustering VidyoGateways, the entire procedure should be done for each VidyoGateway in your cluster.

Telephones can send and receive only the audio portion of the teleconference.

Making Configurations on Your VidyoGateway

To make configurations on your VidyoGateway:

1. Configure your network interface settings in the VidyoGateway System Console. The following criteria should be met:
   a. Set your production and management interfaces with IP addresses.
b. Rack your machine properly.

c. Successfully Ping your server before proceeding.

For more information, see “Configuring Network Settings at the System Console” in the VidyoGateway Administrator Guide.

2. Secure your VidyoGateway server (if applicable).

For more information, see “Securing your VidyoGateway System with SSL and HTTPS” in the VidyoGateway Administrator Guide.

3. Register your VidyoGateway to your VidyoPortal by entering your VidyoPortal address in your VidyoGateway.

For more information, see “Configuring the VidyoPortal Settings” in the VidyoGateway Administrator Guide.

Making Configurations on Your VidyoPortal for Your VidyoGateway

To make configurations on your VidyoPortal for your VidyoGateway:

1. Add the VidyoGateway as a component on your VidyoPortal.

Note
If you are performing an initial VidyoGateway setup, you must add the VidyoGateway as a component in your VidyoConferencing system.

For more information, see Adding a VidyoGateway to Your VidyoPortal.

2. Assign the VidyoGateway to a tenant.

If you are running a multi-tenant system, assign it to the appropriate tenant.

For more information, see Making the VidyoGateway Components Available.

Note
Now you can configure additional VidyoGateway features as needed, such as creating VidyoGateway clusters, setting up call services to enable dialing between the VidyoGateway and your Legacy system (or use any of the predefined services), and integrating VoIP phones and IP PBXs.

For more information, refer to the VidyoGateway Administrator Guide.

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.

The Components page displays by default.
2. Log in to the VidyoGateway Console Admin page.

   The General > VidyoPortal subtab is selected by default.

   ![VidyoGateway Admin Console](image.png)

3. Configure the VidyoGateway and ensure that the Address is directed to your VidyoPortal.

   If you need to configure a cluster node, refer to the “Configuring Your Cluster Node” section in the VidyoGateway Administrator Guide.

4. Click Save to complete the configuration.

   For more information, refer to the VidyoGateway Administrator Guide.

   The VidyoGateway appears on the Components tab within the Super Admin portal as "NEW."

5. Navigate back to the Component tab in the Super Admin portal.

6. Click the Name link for the VidyoGateway.
The *VidyoGateway* pop-up displays.

![VidyoGateway pop-up](image)

**Note** The username and password configured in these steps are used when configuring your VidyoPortal settings on your VidyoGateway. For more information, refer to “Configuring the VidyoPortal Settings” in the *VidyoGateway Administrator Guide*.

The username cannot be “admin” or “super.”

When editing existing VidyoGateway components, prefixes from your VidyoGateway are listed on their tables.

7. Enter the VidyoGateway login name for VidyoPortal registration and authentication in the **User Name** field.

8. Enter the VidyoGateway password for VidyoPortal registration and authentication in the **Password** field.

9. Re-enter the password in the **Verify Password** field.

10. Click **Save**.
8. Configuring Your Components as the Super Admin

Configuring Router Pools

Router Pools is an optional advanced topology for configuring VidyoRouters in the VidyoConferencing system. You can configure Router Pools at initial installation or do so at a later date when your organization’s network grows. Some of the benefits of Router Pools 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 Router Pools. 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 setting Router Pools, 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 your Router Pools are 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 that 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.

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.
   The Components page displays by default.

2. Click the Router Pools tab.
   The Router Pools page displays.

3. Click the Modified radio button in the upper right corner.
4. Click **Add Pool** in the Pools List section.

5. Enter a name for the pool you’re creating in the **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. Click **Update**.

![Router Pool Configuration](image)

### 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](#).
   
   The *Components* page displays by default.

2. Click the *Router Pools* tab.
   
   The *Router Pools* page displays.

3. Click the **Modified** radio button in the upper right corner.

4. Select the pool that needs to be deleted from the Pools List section.

5. Click **Delete Pool**.
   
   A **Confirmation** pop-up displays.

6. Click **Yes**.

### Activating the Router Pool Configuration

Router Pools enables the VidyoConferencing system to cascade conferences across multiple VidyoRouters. The Router Pool 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 configuration; even though you may decide not to configure a full Router Pool, a default Router Pool for any VidyoRouters still exists in the system. If you have multiple
8. Configuring Your Components as the Super Admin

VidyoRouters, they cascade by default as needed (even without a full Router Pool configuration) to provide for larger conferences and router capacity overflow. Therefore, you need to activate the Router Pools configuration upon configuring all the components.

To activate the Router Pools 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.
   The Components page displays by default.

2. Click the Router Pools tab.
   The Router Pools page displays.

3. Click the Modified radio button in the upper right corner.

4. Click Activate at the bottom of the page.

   ![](image)
   A Confirmation pop-up displays.

   ![](image)
   Click Yes.

   Unless you need to control which particular VidyoRouter your users’ access, you don’t need to define any Router Pools. By leaving everything under Manage Router Pools blank, you create a default Router Pool, and your VidyoRouters are automatically pooled together and allowed to cascade for larger conferences.
8. Configuring Your Components as the Super Admin

If you do not activate Router Pools, a message displays on top of the Components window.

**You must activate the VidyoRouter configuration in the Router Pool Rules 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 their account is created. It’s a mandatory field on the Add User page. For more information, see Adding a New User. However, using location tags as the basis for a rule is optional, but it’s a good idea to associate a user with their 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.
   The Components page displays by default.
2. Click the Router Pools tab.
   The Router Pools page displays.
3. Click the Location Tags subtab.
4. Select the Modified radio button.
5. Click Add.
6. Enter a name for the location tag in the text field.
7. Click Update.
   A Confirmation pop-up displays stating “Location Tag Saved.”
8. Configuring Your Components as the Super Admin

8. Click OK.

For information about how to assign location tags to tenants, see Assigning Location Tags.

Creating Priority Lists

Priority Lists are priority ordered lists of Router Pools that are used in the Endpoint Rules.

To create a priority list:

1. Log in to the Super Admin portal using your Super Admin account.
   For more information, see Logging in to the Super Admin Portal.
   The Components page displays by default.
2. Click the Router Pools tab.
   The Router Pools page displays.
3. Click the Priority List subtab.
4. Click Add Priority List.
   A new page displays.
5. Enter a name for the priority list in the Priority List Name field.

   Note: Characters are not permitted in the Priority List Name field (e.g., <, >, &, "", ', etc.).

6. Drag and drop pools from the Available Pools list to the Associated Pools list in the order that they should display based on priority level.
7. Click Save Priority List at the top of the page.
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 will use in a call. Remember that you can create Endpoint Rules only after you have set up your VidyoRouter pools and Priority Lists.

As the Super Admin, you determine the order in which Endpoints Rules are applied. The first rule that matches the endpoint’s characteristics (IP address, location tag, or Endpoint ID) is the rule that is 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, known as Endpoint ID, in which it automatically sends to the VidyoManager to identify itself.

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 0.0.0.0/0.

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.
   - The Components page displays by default.
2. Click the Router Pools tab.
   - The Router Pools page displays.
3. Click the Endpoint Rules subtab.
4. Select the **Modified** radio button.

5. Click **Add Rule**.

   A new page displays.

6. Enter a name for your endpoint rule in the **Rule Name** field.
The Add Ruleset pop-up displays.

7. Select from the following radio buttons:
   - Select IP Rule and select the corresponding checkboxes - Specify Local IP Range (Ipv4 or Ipv6) and Specify External (NATed) IP Range (Ipv4 or Ipv6) to specify a range of local and external IP addresses.
   - Select User Location Tag to select from location tags that you have already configured in the system.
   - The Endpoint ID is selected to provide a unique identifier for an endpoint.

Note Location tags must first be created in order to select them for your rule. For more information, see Creating User Location Tags.

Caution This Endpoint ID field should only be set under specific instruction from Vidyo Customer Support.

8. Click Save.
   - To add another rule, click Add Ruleset.
   - To edit a rule, select the corresponding checkbox, and then click Edit Ruleset.
   - To delete a rule, select the corresponding checkbox, and then click Delete Ruleset.
   - You can apply priority lists that were previously created to all rules by selecting the Priority List drop-down.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

The VidyoPortal and VidyoRouter Virtual Editions (VE) allow you to enjoy the benefits of the VidyoPortal and VidyoRouter 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 and VidyoReplay VE, refer to the VidyoGateway Administrator Guide and VidyoReplay Administrator Guide respectively.

Understanding the VE Requirements

You can now run multiple Virtual Edition Vidyo Servers (of any combination) on the same physical host. Virtual Edition Vidyo Servers may be run on hardware that is also running non-Vidyo virtual machines.

If you have an existing Virtual Edition software deployment, you can upgrade to newer software releases using the same hardware and virtual machine configurations. However, in order to be supported under the new guidelines (such as sharing physical hosts with multiple virtual machines), your virtual machines must adhere to the new virtual machine configurations listed in this section.

To run, the following requirements must be met:

- Requires VMware vSphere ESXi Hypervisor software version 5.0 or later; version 5.5 or later recommended.
- Must be compliant with the VMware qualified hardware list at http://www.vmware.com/resources/compatibility/search.php.
- Requires Intel-based servers with a minimum Xeon 56xx Series at 2.0 GHz or faster, supporting Intel Westmere and newer architectures, with AES-NI and hyper-threading enabled. Xeon E5 family with Sandy Bridge architecture or newer are recommended.
- At least 1Gbps vNICs.
- The BIOS settings of the host machine must be set for maximum performance, including both CPU and memory settings.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

- The BIOS settings must enable the Hyperthreading, Virtualization Technology (VT), and Extended Page Tables (EPT) options on all ESX hosts.
- The memory must be the highest rated speed specified by the host CPU, and all memory lanes of the CPUs must be populated with identical size and speed DIMMs.
- For 4+ socket systems, set your CPU affinity to two adjacent packages to ensure that transcoding occurs on memory at most one node away.
- For large memory configurations (64 GB+), ensure that memory access is coalesced from multiple memory channels, e.g., by enabling bank interleaving in the BIOS.
- When running multiple virtual Vidyo Servers:
  - Maintain 15% of the physical hardware CPU capacity as unreserved when deploying multiple virtual machines on a physical host.
  - When deploying multiple VidyoRouters on the same physical host, ensure that you have sufficient network bandwidth. The physical host should have 1 Gbps Ethernet per 100-port VidyoRouter.
  - The physical host must use CPUs with at least 2.0 GHz in all cases, and in some cases higher CPU speeds are required (see the CPU resource reservation guidelines in the following sections for details).
  - Do not co-locate high availability pairs on the same physical host.

VidyoPortal Virtual Machine Provisioning Requirements

VidyoPortal version 3.3 or later is available as a single Virtual Edition that dynamically enforces capacity limits based on the number of vCPU allocated. The following configurations are the only supported configurations:

<table>
<thead>
<tr>
<th>VidyoPortal Capacity</th>
<th>VM Configuration</th>
<th>Resource Reservation</th>
<th>Physical Host</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vCPU</td>
<td>RAM (GB)</td>
<td>Storage (GB)</td>
</tr>
<tr>
<td>10,000 Users; 1,000 Tenants</td>
<td>4</td>
<td>8</td>
<td>50</td>
</tr>
<tr>
<td>10,000 Users; 1,000 Tenants</td>
<td>6</td>
<td>8</td>
<td>50</td>
</tr>
<tr>
<td>1,000 Users; 100 Tenants</td>
<td>2</td>
<td>8</td>
<td>50</td>
</tr>
</tbody>
</table>

VidyoPortal VE may be run together with VidyoRouter VE and/or VidyoGateway VE on the same physical host server for a low-cost solution.
Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

Note VidyoPortal VE can be configured to use the Hot Standby software option. For more information, see Appendix E. Hot Standby.

VidyoRouter Virtual Machine Provisioning Requirements

The VidyoRouter will continue to be offered as a Virtual Edition with the following configurations supported:

<table>
<thead>
<tr>
<th>VidyoRouter Capacity</th>
<th>VM Configuration</th>
<th>Resource Reservation</th>
<th>Physical Host</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vCPU</td>
<td>RAM (GB)</td>
<td>Storage (GB)</td>
</tr>
<tr>
<td>25</td>
<td>4</td>
<td>4</td>
<td>50</td>
</tr>
<tr>
<td>100</td>
<td>8</td>
<td>8</td>
<td>50</td>
</tr>
</tbody>
</table>

Multiple VidyoRouters may be run on the same physical host as long as there is at least 1Gb of Ethernet per 100 ports of VidyoRouter capacity.

Example Configurations

Lab or Demo Configuration:
- One Dell® R220, Intel® Xeon® E3-1286 v3 3.7 GHz 4Core, 16 GB RAM.
- 1 VidyoPortal (1,000 user) + 1 VidyoRouter (25 port) + 1 VidyoGateway (2 HD/4 SD/20 voice).

Small Business Configuration:
- 2 Dell R220, Intel Xeon E3-1286 v3 3.7 GHz 4-Core, 16 GB RAM each with the following installations:
  - 1 VidyoPortal (1,000 user) + 1 VidyoRouter (25 port) + 1 VidyoGateway (2 HD/4 SD/20 voice)
  - VidyoPortals configured with the Hot Standby software option.
  - VidyoGateways clustered to provide an aggregate capacity of 4 HD, 8 SD, and 40 voice.
  - VidyoRouters provide 50 ports of aggregate capacity.

Mid-Size Configuration:
- 2 Dell R420, dual Intel Xeon E5-2470 v2 2.40 GHz 10-Core, 8 GB each with the following installations:
  - 1 VidyoPortal (1,000 user) + 1 VidyoRouter (100 port) + 1 VidyoGateway (4 HD/9 SD/50 voice)
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

- 1 Dell R620, dual Intel Xeon E5-2667 v2 3.30 GHz 8-Core, 32 GB with the following installations:
  - 2 VidyoGateways (8 HD/18 SD/100 voice)
  - VidyoPortals configured with the Hot Standby software option.
  - VidyoGateways clustered to provide an aggregate port capacity 20 HD/45 SD/250 voice
  - VidyoRouters provide 200 ports of aggregate capacity.

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.

- Advanced features, such as vMotion, high availability, fault tolerance, and distributed resource manager are not currently supported.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

Installing VidyoPortal VE

**Note** The virtual appliance's filename reflects the appliance type and the software version. The following screenshots refer to the deployment of a VidyoPortal virtual server appliance with the latest software version at the time of release. Please refer to the VidyoPortal and VidyoRouter Release Notes for more detailed information regarding release versions.

To install VidyoPortal VE:

1. Log in to the vSphere client.

2. Select **Deploy OVF Template** from the File menu.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

The *Source* dialog box displays.

3. Click **Browse** and select the `.ova` file from your file system.

4. Click **Next**.
The dialog box changes to *OVF Template Details*.

![Deploy OVF Template](image)

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 needed.

7. Click Next.
   The dialog box changes to Disk Format.

8. Ensure that either the Thick Provision Lazy Zeroed or Thick Provision Eager Zeroed radio button is selected.
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 displays.

The *Deployment Completed Successfully* dialog box displays.

14. Click **Close**.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

The vSphere Client window displays.

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 System Console.

18. Log in as Admin.
   a. If you haven’t changed your password yet, use the default password we have provided for you.
   b. You can now configure your VidyoPortal VE.

Installing VidyoRouter VE

Note The virtual appliance’s filename reflects the appliance type and the software version. The following screenshots refer to the deployment of a VidyoRouter virtual server appliance with the latest software version at the time of release. Please refer to the VidyoPortal and VidyoRouter Release Notes for more detailed information regarding release versions.
To install VidyoRouter VE:

1. Log in to the vSphere client.

2. Select **Deploy OVF Template** from the File menu.
3. Click **Browse** and select the **.ova** file from your file system.

4. Click **Next**.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

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 needed.

7. Click **Next**.
   The dialog box changes to **Disk Format**.

8. Ensure that either the **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed** radio button is selected.

9. Click **Next**.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

The dialog box changes to \textit{Network Mapping}.

10. Select the network you want the VidyoRouter VE to use.

11. Click \textbf{Next}.

The dialog box changes to \textit{Ready to Complete}.

12. Select the \textbf{Power on after deployment} checkbox to start your VidyoRouter immediately after you take the next step.

13. Click \textbf{Finish}. 

201
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

The *Deploying VidyoRouterVE* dialog box displays.

![Image of Deploying VidyoRouterVE dialog box]

The *Deployment Completed Successfully* dialog box displays.

![Image of Deployment Completed Successfully dialog box]

14. Click **Close**.

The *vSphere Client* window displays.

![Image of vSphere Client window]

15. Click on the + sign to the left of the ESXi host name.

16. Click on **VidyoRouter VE** in the left-side pane.
9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE)

The tabs change.

17. Click the Console tab.

You’re at your VidyoRouter VE’s System Console.
18. Log in as Admin.

a. If you haven’t changed your password yet, use the default password we have provided for you.

b. You can now configure your VidyoRouter VE.
10. 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.

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](#).

   The *Components* page displays by default.

2. Click the *Tenants* tab.

   The *Tenants* page displays. Tenants in your VidyoPortal display in the table and include Tenant Name, Tenant URL, Ext. Prefix, Description, and Delete as columns.

   You can drag and drop the column headings to arrange them in the order you prefer.

3. Search by tenant name or tenant URL using the Tenant Name or Tenant URL search boxes above the table.

4. Use the following buttons at the bottom of the page to change your view of the table.

   - Click *Refresh* to refresh the table.
10. Managing Tenants as the Super Admin

- 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.
- Click **Add** to add a tenant.
- Click **Delete** to delete a tenant.

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 VidyoProxy components.
4. Assign VidyoGateway components (skip if VidyoGateway is not being used).
5. Assign VidyoReplay Recorder components (skip if VidyoRecorder is not being used).
6. Assign VidyoReplay components (skip if VidyoReplay is not being used).
7. Assign location tags.
8. 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 **Using the Tenants Table**.

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.
   The Components page displays by default.

2. Click the Tenants tab.
   The Tenants page displays.

3. Click the Default name and perform the following steps.
   Alternatively, if your system is licensed for multi-tenant mode, click Add at the bottom of the Tenants page.

![Tenant Configuration Form](image-url)
10. Managing Tenants as the Super Admin

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

- Enter a unique name identifying the tenant in the **Tenant Name** field. 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.

- Enter the IP or FQDN address used by this tenant’s users to access the VidyoPortal in the **Tenant URL** field.

  **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).

- Enter a desired prefix in the **Ext. Prefix** field 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.

- Enter the phone number dialed for voice-only participants when accessing conferences in the **Dial-in Number** field.

- Enter the URL the tenant’s users will use in order to access VidyoReplay in the **VidyoReplay URL** field. 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.

- Enter the URL that will resolve to the Vidyo Neo for WebRTC Server to use for this tenant (e.g. https://webrtc.example.com). It may contain the FQDN of the Session Manager or it may be an FQDN that will load balance across several Session Managers.
10. Managing Tenants as the Super Admin

**Note** If a Vidyo Neo for WebRTC Server is configured for a tenant, the tenant Admin will now be able to enable or disable Vidyo Neo for WebRTC. However, the tenant Admin will no longer be able to configure VidyoWeb.

- Enter a short description in the **Description** field for informational purposes.

- Enter tenant support for inbound URI dialing from the VidyoGateway using SIP and H.323 protocols in the **Tenant VidyoGateway SIP/H.323 SRV record FQDN** field.

  For more information, refer to “Understanding Call Types and Service Examples” in the *VidyoGateway Administrator Guide*.

- Enter the number of endpoint software installations in the **# of Installs** field to allocate to the tenant.

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

- Enter the maximum number of seats this tenant can create in the **# of Seats** field.

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

- Enter the maximum number of public rooms this tenant can create in the **# of Public Rooms** field.

  The maximum number of public rooms per tenant cannot exceed 100,000.

- Enter the maximum number of lines allocated to the tenant in the **# of Lines** field.

  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.

- Enter the maximum number of Executive Desktop / VidyoRoom SE users allocated to the tenant in the **# of Executives / VidyoRoom SE** field.

  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. Therefore, 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.

- Enter the maximum number of VidyoPanoramas users allocated to the tenant in the **# of VidyoPanoramas** field.

- Deselect the **Enable Guests login** checkbox if you want to prohibit guest logins on the tenant or leave selected.
10. Managing Tenants as the Super Admin

- Deselect the **Scheduled Room** checkbox if you want to prohibit your tenants from using scheduled rooms or leave selected.

- Enable or disable VidyoMobile Access.
  
  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 via 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.

**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 Vidyo Neo](#) for WebRTC access.

Vidyo Neo™ for WebRTC Server allows you to use desktop and mobile browsers that support WebRTC to join conferences on VidyoPortal without installing browser plugins or extensions. For more information, refer to the *Vidyo Neo for WebRTC Server Administrator Guide*.

**To enable Vidyo Neo for WebRTC access:**

5. Log in to the Super Admin portal using your Super Admin account.
   
   For more information, see [Logging in to the Super Admin Portal](#).
   
   The **Components** page displays by default.

6. Click the **Settings** tab.
   
   The **Upload System License** page displays by default.

7. Click ☑ to the left of **Feature Settings** on the left menu.

8. Click **Vidyo Neo for WebRTC** from the submenu.
10. Managing Tenants as the Super Admin

The *Vidyo Neo for WebRTC* page displays.

9. Select the **Enable Vidyo Neo for WebRTC for guests** checkbox if you want to allow invited guests to join calls via Vidyo Neo for WebRTC.

10. Select the **Enable Vidyo Neo for WebRTC for users** checkbox if you want to allow users to join calls via Vidyo Neo for WebRTC.

11. Click **Save**.

12. Configure the URL of the Vidyo Neo for WebRTC Server for each tenant that will use Vidyo Neo for WebRTC.

See **Adding a Default Tenant or Adding a New Tenant**.

---

**Note** Enabling Vidyo Neo for WebRTC for users is useful if you have users on platforms for which there is not currently a Vidyo Neo Desktop client, such as Chromebooks and Linux desktops. However, users that are currently logged in will reserve the same resources on the Vidyo Neo for WebRTC Server whether or not they are on a call.

Once the Super Admin has enabled Vidyo Neo for WebRTC, the tenant Admin may enable or disable the feature for their tenant.

**Note** Enabling VidyoMobile Access.

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 **Enabling Vidyo Neo** for WebRTC access.
10. Managing Tenants as the Super Admin

Vidyo Neo™ for WebRTC Server allows you to use desktop and mobile browsers that support WebRTC to join conferences on VidyoPortal without installing browser plugins or extensions. For more information, refer to the Vidyo Neo for WebRTC Server Administrator Guide.

To enable Vidyo Neo for WebRTC access:

13. Log in to the Super Admin portal using your Super Admin account. For more information, see Logging in to the Super Admin Portal.

The Components page displays by default.

14. Click the Settings tab.

The Upload System License page displays by default.

15. Click + to the left of Feature Settings on the left menu.

16. Click Vidyo Neo for WebRTC from the submenu.

The Vidyo Neo for WebRTC page displays.

17. Select the Enable Vidyo Neo for WebRTC for guests checkbox if you want to allow invited guests to join calls via Vidyo Neo for WebRTC.

18. Select the Enable Vidyo Neo for WebRTC for users checkbox if you want to allow users to join calls via Vidyo Neo for WebRTC.

19. Click Save.

20. Configure the URL of the Vidyo Neo for WebRTC Server for each tenant that will use Vidyo Neo for WebRTC.
10. Managing Tenants as the Super Admin

See Adding a Default Tenant or Adding a New Tenant.

Note  Enabling Vidyo Neo for WebRTC for users is useful if you have users on platforms for which there is not currently a Vidyo Neo Desktop client, such as Chromebooks and Linux desktops. However, users that are currently logged in will reserve the same resources on the Vidyo Neo for WebRTC Server whether or not they are on a call.

Once the Super Admin has enabled Vidyo Neo for WebRTC, the tenant Admin may enable or disable the feature for their tenant.

Note  Enabling VidyoMobile Access.

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.

- Allow inbound and outbound inter-portal communication by doing any of the following:
  - Select the Allow Outbound checkbox and do not select the Allow Inbound checkbox to only allow calls to other VidyoConferencing systems.
  - Do not select the Allow Outbound checkbox and select Allow Inbound checkbox to only allow calls from other VidyoConferencing systems.
  - Click both checkboxes to allow both inbound and outbound calls.

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 Using the Tenants Table.

To enable cross-tenant access:

1. Click the to expand the Can make call to section.

   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 displays in the Available Tenants list on the left.

2. Select one or more tenants in the Available Tenants list and drag and drop it to the Selected Tenants list.
This allows the users of the tenant that 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 display 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 VidyoProxy Components Available

This is step 3 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see Using the Tenants Table.

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 the + to expand the VidyoProxy component(s) section.

In this section, you can make the VidyoProxy components you set up previously available to the tenant. The Tenant Admin can then choose among these components as necessary. The list of available VidyoProxies displays in the Available VidyoProxy component(s) list on the left.

2. Select one or more VidyoProxies in the Available VidyoProxy component(s) list and drag and drop it to the Selected VidyoProxy component(s) list.

All VidyoProxy components that display in the Selected VidyoProxy component(s) list are available to the tenant. You can move a VidyoProxy from the Selected VidyoProxy component(s) list back to the Available VidyoProxy component(s) list by dragging and dropping.

Making the VidyoGateway Components Available

This is step 4 of the steps needed to configure a tenant. This step is optional. For the full list of steps when configuring a tenant, see Using the Tenants Table.
To make the VidyoGateway components available:

1. Click the **+** to expand the Available VidyoGateway component(s) section.

In this section, you can make the VidyoGateway components you set up previously available to the tenant. The Tenant Admin can then choose among these components as necessary.

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

2. Select one or more VidyoGateways in the Available VidyoGateway component(s) list and drag and drop it to the Selected VidyoGateway component(s) list.

All VidyoGateway components that display 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 dragging and dropping.

**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.

### Making the VidyoReplay Recorders Available

This is step 5 of the steps needed to configure a tenant. This step is optional. For the full list of steps when configuring a tenant, see [Using the Tenants Table](#).
To make the VidyoReplay Recorder available:

1. Click the + to expand the VidyoReplay Recorder(s) section.

In this section, you can make the VidyoReplay Recorders you set up previously available to the tenant. The Tenant Admin can then choose among these components as necessary. The list of available VidyoReplay Recorders displays in the Available VidyoReplay Recorder(s) list on the left.

2. Select one or more VidyoReplay Recorders in the Available VidyoReplay Recorder(s) list and drag and drop it to the Selected VidyoReplay Recorder(s) list.

All VidyoReplay Recorders that display in the Selected VidyoReplay Recorder(s) list are available to the tenant. You can move a VidyoReplay Recorder from the Selected VidyoReplay Recorder(s) list back to the Available VidyoReplay Recorder(s) list by dragging and dropping.

Making the VidyoReplay Components Available

This is step 6 of the steps needed to configure a tenant. This step is optional. For the full list of steps when configuring a tenant, see Using the Tenants Table.
To make the VidyoReplay components available:

1. Click the + to expand the VidyoReplay component(s) section.

   ![VidyoReplay components](image)

In this section, you can make the VidyoReplay components you set up previously available to the tenant. The Tenant Admin can then choose among these components as necessary.

The list of available VidyoReplays displays in the Available VidyoReplay component(s) list on the left.

2. Select one or more VidyoReplays in the Available VidyoReplay component(s) list and drag and drop it to the Selected VidyoReplay component(s) list.

   All VidyoReplay components that display in the Selected VidyoReplay component(s) list are available to the tenant. You can move a VidyoReplay from the Selected VidyoReplay component(s) list back to the Available VidyoReplay component(s) list by dragging and dropping.

### Assigning Location Tags

This is step 7 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see [Using the Tenants Table](#).

**Note** Before you assign location tags, you must create them first. For more information, see [Creating User Location Tags](#).
To assign location tags:

1. Click the + to expand the Location Tag(s) section.

In this section, 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. Select one or more of the location tags in the Available Location Tag list and drag and drop it to the Selected Location Tag list.

Adding the New Tenant to Your System

This is step 8 of the steps needed to configure a tenant. For the full list of steps when configuring a tenant, see Using the Tenants Table.

To add the new tenant:

1. Click the + to expand the *New User section.

2. Enter the following fields:
   - User Name
   - Password
   - Verify Password
   - Display Name
   - E-Mail Address
10. Managing Tenants as the Super Admin

Description (optional)

![Tenant Configuration Screen](image)

3. Click **Save** to finish configuring this tenant.

Deleting a Tenant

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](#).
   
   The *Components* page displays by default.

2. Click the *Tenants* tab.
   
   The *Tenants* page displays.

3. Select the checkbox for the tenant that needs to be removed.

4. Click **Delete** at the bottom of the Tenants table.
5. Click OK in the Confirmation pop-up that displays.

Viewing Current Calls

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

- Click on the Calls tab to view current calls.

The Calls page in the Super Admin portal displays the following information:

- The Conference Name column shows the name of the conference.
- The Tenant Name column shows the name of the owner of the conference.
- The Name column shows the name of the caller.
- The Extension column shows the extension number of the caller.
- The VidyoRouter Name column shows which VidyoRouter the caller is using.
- The VidyoRouter Pool column shows the VidyoRouter pool to which the VidyoRouter belongs.

The Calls page in the Admin portal displays the same information. In addition, in the left-most column the following information displays:

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.
10. Managing Tenants as the Super Admin

The information in this page is for monitoring only. You cannot manage or control calls in the \textit{Calls} page. For information about controlling a meeting, see \textit{Controlling Meetings}.
11. 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 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. Enter the IP or FQDN address for the VidyoPortal in the address bar of a web browser, followed by a forward slash and the word “admin”:

   http://[IP or FQDN address]/admin

   The Login pop-up displays.

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 12. Managing Meeting Rooms as the Tenant Admin.

Setting the Language for the Admin Interface

You can select the language of the VidyoPortal Admin interface before or after you log into the system.
To set the language for the Admin interface:

1. Select your desired language using the language drop-down on the upper right corner of the *Admin Login* page (before or after logging into the system).

The VidyoPortal Admin interface is available in these 15 languages:

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

**Note** The Admin interface is immediately modified once you select your preferred language using the language drop-down.

Any changes you make to the preferred language of the Admin interface have no effect on any other interfaces, such as the VidyoDesktop user interface.
11. Managing Users as the Tenant Admin

Using the Manage Users Table

You can use the Manage Users table is used to view, delete, and manage the users in your tenant.

To use the Manage Users table:

1. Log in to the Admin portal using your Admin account.
   For more information, see Logging In as a Tenant Admin.
   The Users page displays by default. This page lists the users in your VidyoPortal in a table format. You can drag and drop the column headings to arrange them in the order you prefer.

2. 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 the display name and username. These names are the ones showing in the VidyoPortal and may not necessarily be the user's full name.

3. Use the following buttons at the bottom of the page to change your view of the table.
   - 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 you can also add normal user accounts. Alternatively, you can bulk upload users with the Import Users function. For more information, see Importing Users.

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.
   The Users page displays by default.

   Note: The member name search works for both the display name and username. These names are the ones showing in the VidyoPortal and may not necessarily be the user’s full name.

   - 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.
2. Click the **Add User** at the bottom of the page.

The **Add User: New User** pop-up displays.

3. Select one of the following options from the **User Type** drop-down:
   - Select **Admin** to provide the new user with administrative privileges and capabilities.
   - Select **Operator** to provide the user with the ability 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 provide the user with the ability to join meetings, control their own meetings, and place direct calls. Normal users can also change their passwords, set their PIN codes, and invite guests, unless the administrator has disabled these capabilities.
   - Select **VidyoRoom** to create an account for a physical Vidyo endpoint appliance. A VidyoRoom has the same rights as a normal user.
11. Managing Users as the Tenant Admin

- Select **Executive** to create executive desktop users. Executive Desktop licenses 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. Therefore, if you purchase 100 VidyoLines and five Executive Desktops, then even when your system is at full capacity, your five users with Executive Desktop privileges can still make calls.

4. Enter information into the following required fields:

- Enter a user name, which is the name the user provides when logging in to the system, in the **User Name** field.
  
  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 80 characters. If your intended entry has already been taken, you are prompted to select a different name.

- Enter a display name for the user you are adding in the **Display Name** field.
  
  For VidyoRoom systems, the display name is the system name set by the administrator and the name that displays in the top-left corner of the home page. For VidyoDesktop systems, the users’ display names appear below their video images when they are in a conference using VidyoDesktop.

- Enter a password in the **Password** and **Verify Password** fields.
  
  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 valid email address for the user in the **E-Mail Address** field.
  
  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 in the **Extension** field that 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.

- Select either the default group or another group you have created from the **Group** drop-down. 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 14. Managing Tenant Admin Groups as the Tenant Admin.

- Select either the default proxy or another proxy you have created from the **Proxy** drop-down. You must define proxies before assigning them.
11. Managing Users as the Tenant Admin

For more information, see [Making the VidyoProxy Components Available](#).

- Select the user’s Location Tag from the **Location Tag** drop-down.
  For more information about location tags, see [Managing Location Tags](#) and [Configuring Router Pools](#).

- Select the language preference from the **Language Preference** drop-down for the specific user you are adding.
  Select **System Language** to apply the currently selected system-wide language. For more information, see [Setting the Language for the Admin Interface](#). Otherwise, select any other language to change the language for this specific user only.

- Deselect the **Allowed to log in to user portal** checkbox if you want to disable the user’s ability to log in to the User portal, or leave selected.
  Normal users are required to log in, but Administrators and Operators may not be required to log in.

- Leave the **Status** checkbox selected to enable the new user’s room.
  Deselect the **Status** checkbox if you want to put a user on hold with all of their information intact. When this checkbox is selected, the user does not show up in searches in the VidyoPortal and is not able to log in.

5. Select the **Additional Information** checkbox if you want to enter additional information about the new user in the following fields:
11. Managing Users as the Tenant Admin

- Enter a primary phone number for the new user in the **Phone Number 1** field if necessary.
- Enter a secondary phone number for the new user in the **Phone Number 2** field if necessary.
- Enter a tertiary phone number for the new user in the **Phone Number 3** field if necessary.
- Enter the department that the new user is associated with in the **Department** field if necessary.
- Enter the new user’s title in the **Title** field if necessary.
- Enter a primary location (e.g., New York Office) for the new user in the **Location** field if necessary.
- Enter an IM address for the new user in the **IM** field if necessary.
- Enter any details or data regarding the user you are adding in the **Description** field if necessary.

6. Click **Save**.
   - If some information is missing, incorrect, or already in the system, an error message displays at the top of the page 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 page.

7. Repeat the steps in this procedure for every user that you want to add.

**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](#).
   - The **Users** page displays by default.
2. Find the user to edit by using the search filters, sorting on the headers and pagination.
3. Click the name of the user that needs to be edited.
The *Edit User* pop-up displays.
If the *User Attributes* page is available from the *Settings > Feature Settings* submenu and the *Enable Thumbnail Photos* checkbox is selected, the *Edit User* pop-up will display as follows and you will have the option to upload thumbnail photos.

Additionally, if the *User Attributes* page is available from the *Settings > Feature Settings* submenu and the *Allow users to upload their own image* checkbox is selected, your tenants will also have the option to upload their own thumbnail photo from the *Edit User* pop-up.

For more information, see [Configuring User Attributes](#).

- Click ![Image](image) to select and upload a thumbnail photo, and then click *Yes* in the confirmation pop-up that displays.
11. Managing Users as the Tenant Admin

The icon displays.

- Click to remove the uploaded thumbnail photo, and then click Yes in the confirmation pop-up that displays.

4. 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.

5. Click Save.

---

**Note**

If information is missing, incorrect, or already in the system, an error message displays at the top of the page 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 displays.

---

**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.
   
   The Users page displays by default.

2. Find the user to edit by using the search filters, sorting on the headers, or by pagination.
3. Select the one or more checkboxes at the left of the row of the user(s) that needs to be deleted.

![User Management Interface](image)

4. Click **Delete** at the bottom of the page and answer **Yes** to all prompts.

**Note**  Deleting a user also deletes all of the personal, public, and scheduled rooms they created. 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 change their status to disabled. Disabling a user puts them on hold with all of their information intact. That user will not show up in searches in the VidyoPortal and will not be able to log in. However, you can re-enable them at any time. For more information, see [Editing a User](#).

### Adding a Legacy Device

You can add Legacy systems as if they were users on your VidyoPortal. Use this feature in conjunction with the VidyoGateway to make dialing from the VidyoPortal to legacy (H.323 and SIP) endpoints and telephones easier.

For more information, refer to the [VidyoGateway Administrator Guide](#).
11. Managing Users as the Tenant Admin

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.
   The *Users* page displays by default.

2. Click *Add Legacy Device* on the bottom of the page.
   The *Add Legacy Device: New Legacy Device* pop-up displays.

3. Enter the *Legacy Device Name*.

4. Enter the *Extension* for your Legacy device.

5. Click *Save*.

Exporting Users

If you need to add multiple user accounts, you can do so by first exporting a *.csv* or *.veb* file that contains the user information, and then importing that file. This section explains how to export users. For information about how to import users, see Importing 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.
   The *Users* page displays by default.

2. Click *Export Users* on the bottom of the page.
The *Export Users* pop-up displays.

3. Select the output file format from the following:
   a. Select `.csv` to export the user account data without corresponding passwords in to the standard comma-separated value format.
      
      For more information, see [Exporting .csv Files](#).
   b. Select `.web` to export your user account data along with corresponding hashed passwords as a `.web` file. The `.web` format is an encrypted and password protected format.

4. Click `Export`.
11. Managing Users as the Tenant Admin

Exporting .csv Files

When exporting a .csv file, the first line of the 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.

<table>
<thead>
<tr>
<th>UserType</th>
<th>Username</th>
<th>Password</th>
<th>Fullname</th>
<th>Email</th>
<th>Extension</th>
<th>Group</th>
<th>Language</th>
<th>Description</th>
<th>Proxy</th>
<th>LocationTag</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>adm.1</td>
<td>pw</td>
<td>adm.1</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010101</td>
<td>Default</td>
<td>en</td>
<td>Tenant A</td>
<td>No Proxy</td>
<td>Default</td>
</tr>
<tr>
<td>admin</td>
<td>adm-2</td>
<td>pw</td>
<td>Lk@2</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010102</td>
<td>Default</td>
<td>it</td>
<td>Tenant B</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>normal</td>
<td>nor@1</td>
<td>pw</td>
<td>nor@1</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010104</td>
<td>Default</td>
<td>fr</td>
<td>Abnormal</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>normal</td>
<td>qa12</td>
<td>pw</td>
<td>qa12</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010105</td>
<td>Default</td>
<td>ja</td>
<td>So normal it’s scary</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>operator</td>
<td>opr1</td>
<td>pw</td>
<td>opr1</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010107</td>
<td>Default</td>
<td>sc</td>
<td>Smooth</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>operator</td>
<td>opr-2</td>
<td>pw</td>
<td>opr-2</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010108</td>
<td>Default</td>
<td>pt</td>
<td>Heavy equipment</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>vidyoroom</td>
<td>vrm.1</td>
<td>pw</td>
<td>vrm.1</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010110</td>
<td>Default</td>
<td>fi</td>
<td>Room full of video</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>vidyoroom</td>
<td>vrm-2</td>
<td>pw</td>
<td>vrm-2</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010111</td>
<td>Default</td>
<td>po</td>
<td>At the monkey house</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>executive</td>
<td>exe1</td>
<td>pw</td>
<td>exe1</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010113</td>
<td>Default</td>
<td>tc</td>
<td>Privilege</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>executive</td>
<td>exe_2</td>
<td>pw</td>
<td>exe_2</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010114</td>
<td>Default</td>
<td>en</td>
<td>Action</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>legacy</td>
<td>leg1</td>
<td>pw</td>
<td>leg1</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010116</td>
<td>Default</td>
<td>es</td>
<td>Subaru</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>legacy</td>
<td>leg2</td>
<td>pw</td>
<td>leg2</td>
<td><a href="mailto:test@vidyo.com">test@vidyo.com</a></td>
<td>101010117</td>
<td>default</td>
<td>fr</td>
<td>Yet another MCU</td>
<td>Default</td>
<td>Default</td>
</tr>
</tbody>
</table>

The columns in the .csv file are described below.

- The User Type column shows the various user types. You can import all types of users including admins, operators, VidyoRooms, executives and legacy devices; however, when imported, they are all created as the Normal user type.
- The Username, Password, Fullname, and Email columns provide details about the user.
- The Extension column shows the users unique extension. The extension values must be numeric values.
- The Group column shows the provisioned group to which the user belongs. You must define groups before assigning them.

For more information about managing groups, see 14. Managing Tenant Admin Groups as the Tenant Admin.
- The Language column shows the two-letter language code for the particular user. For more information about languages, see Setting the Tenant Language.
- The Description column shows the optional information that may have been entered when the user was added.

For more information, see Adding a New User.
- The Proxy column shows the optional proxy to which the user has been assigned.

For more information, see Adding a New User.
- The LocationTag column shows the location tag to which the user has been assigned.

For more information, see Adding a New User and Creating User Location Tags.
11. Managing Users as the Tenant Admin

Note  Except for Proxy and Description, all user account fields are required when importing users.

Importing Users

If you need to add multiple user accounts, you can do so by importing a .csv or .veb file that contains the user information. All imported users are created as the Normal user type.

Note  Imported users do not trigger new user account notifications; therefore, administrators should directly email the login credentials to all imported users.

To import users:

1. Log in to the Admin portal using your Admin account. For more information, see Logging In as a Tenant Admin. The Users page displays by default.

2. Click Import Users on the bottom of the page. The Import Users pop-up displays.

3. Click Browse....

4. Locate and open your .csv or .veb file.

5. Enter the same password that was used to create the .veb file bundle to import a .veb file.

6. Click Import Users.

A message displays confirming the number of imported users.
12. Managing Meeting Rooms as the Tenant Admin

Every user has a personal room that is automatically assigned. 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.
   The Users page displays by default.
2. Click the Meeting Rooms tab.
   The Meeting Rooms page displays.

Calls taking place in your VidyoPortal display on the table and include Room Name, Ext, Type, Enabled, State, and Control Meeting 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.
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 displays only if the room is locked. The third icon displays 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.
Personal rooms are deleted by deleting the user associated with the personal room.
For more information, see Deleting a User.

3. 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.

4. Use the following buttons at the bottom of the page to change your view of the table.
   - 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.

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.
   The Users page displays by default.

2. Click the Meeting Rooms tab.
   The Meeting Rooms page displays.

3. Click Add Meeting Room at the bottom of the page.
12. Managing Meeting Rooms as the Tenant Admin

The *Add Room: New Room* pop-up displays.

4. Enter a display name for your room in the *Room Display Name* field.
   The Room Display Name may contain special characters and spaces. The system alerts you when entering an existing name.

5. Enter a name for your room in the *Room Name* field.
   The Room Name is used for URI dialing and 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 when providing an existing name.

   **Note** The Room Name will be auto-generated when a user creates a public room.

6. Select the person to manage and control meetings in the public room from the *Room Owner* drop-down
   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.

7. Enter the number used for the user’s direct calls and speed dial in the *Extension* text field.
   The extension value provided must be numeric and unique.

8. Select the group you want to associate with your new meeting room in the *Group* drop-down.
12. Managing Meeting Rooms as the Tenant Admin

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 14. Managing Tenant Admin Groups as the Tenant Admin.

9. Enter any information that would be useful for the users, such as “This room is used for the weekly sales meeting” in the Description field.

10. Select the Enabled checkbox to enable your room.

Deselecting this checkbox 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.

11. Select the Locked checkbox to prevent additional users from accessing your room.

12. Select the Enter new PIN radio button 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.

13. Select the Leave PIN Alone radio button 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.

14. Select the Enter new PIN radio button 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.

15. Select the Leave PIN Alone radio button 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.

Note Room owners can lock the room and configure room and moderator PINs from the User portal.

16. 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.

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.
   The Users page displays by default.
2. Click the Meeting Rooms tab.
   The Meeting Rooms page displays.
3. Find the room that needs to be edited by using the search filters, sorting on the headers, or by pagination.
4. Click the name of the room that needs to be edited.
   The Edit Room pop-up displays.
5. Edit the room information as necessary.
   For more information, see Adding a Meeting Room.

6. Edit or delete the room URL, which is the link participants and guests use to join your room.

   - The system automatically generates a new URL.
   - Click 🔄 to the right of the Room URL field to delete the current room URL.

7. 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.

To delete a personal room associated with a user, you must first delete the user. Deleting the user automatically deletes his or her room.
12. Managing Meeting Rooms as the Tenant Admin

For more information, see Deleting a User.

Note The checkbox only displays 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.

   The Users page displays by default.

2. Click the Meeting Rooms tab.

   The Meeting Rooms page displays.
3. Find the public room that needs to be deleted by using the search filters, sorting on the headers, or by pagination.

4. Select one or more checkboxes for the room(s) that need to be deleted.

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 **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](#).

   The **Users** page displays by default.

2. Click the **Calls** tab.
   
   The **Calls** page displays. Calls taking place on your VidyoPortal display and include the following fields:
   - Conference Name
   - Name
   - Extension

3. Click the drop-down on the right of each column heading for the following features:
   - Select **Sort Ascending** to arrange the current calls displaying on the table in ascending order from top to bottom based on your selected column.
   - Select **Sort Descending** to arrange the current calls displaying 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 displaying in the table.
   - Select Group By This Field.
   - Select Show in Groups.
4. Use the following buttons at the bottom of the page to change your view of the table.

- 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
12. Managing Meeting Rooms as the Tenant Admin

Note  The screenshot shown previously shows personal rooms which have no corresponding checkbox and therefore cannot be deleted.

When you delete a user, their 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 Meetings

As an Administrator or Operator user type, you can control the meetings that are taking place on your VidyoPortal. The meeting functions that you can control include locking and unlocking meetings, disconnecting participants, muting participants, and adding and removing PINs.

You can access the Control Meeting page from your VidyoPortal, but it can also be accessed from VidyoDesktop or from a tablet.

Note  When accessed from a tablet, room links 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.
12. Managing Meeting Rooms as the Tenant Admin

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.  
   The Users page displays by default.
2. Click the Meeting Rooms tab.  
   The Manage Meeting Rooms page displays.
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 displays.

Tip: As you make configurations on the HTML-based Control Meeting screen, notifications display on the lower part of the screen.
4. Perform any of the following tasks:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add Participant" /></td>
<td>Add a participant to your room.</td>
</tr>
<tr>
<td><img src="image" alt="Email" /></td>
<td>Invite a participant to your room via email.</td>
</tr>
<tr>
<td><img src="image" alt="Lock" /></td>
<td>Toggle between locking and unlocking your room. Locking prevents additional users from accessing your room.</td>
</tr>
<tr>
<td><img src="image" alt="Record" /></td>
<td>Record or record and webcast a meeting using a selected VidyoReplay Record profile. This option only displays if your system includes VidyoReplay. At least one participant has to be in a conference in order for the recording to take place.</td>
</tr>
<tr>
<td><img src="image" alt="Pause" /></td>
<td>Pause a recording or webcast. This option only displays if your system includes VidyoReplay.</td>
</tr>
<tr>
<td><img src="image" alt="Stop" /></td>
<td>Stop a recording or webcast. This option only displays if your system includes VidyoReplay.</td>
</tr>
<tr>
<td><img src="image" alt="Set PIN" /></td>
<td>Set a moderator PIN, create or remove a room link, and set a room PIN. See Configuring Conference Settings.</td>
</tr>
<tr>
<td><img src="image" alt="Disable Video" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="image" alt="Disable Video All" /></td>
<td>Disable video on all participants’ cameras and allow them to re-enable.</td>
</tr>
<tr>
<td><img src="image" alt="Disable Video Single" /></td>
<td>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.</td>
</tr>
</tbody>
</table>
12. Managing Meeting Rooms as the Tenant Admin

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🗣️</td>
<td>Mute audio on all participants’ microphones and allow them to re-enable.</td>
</tr>
<tr>
<td>📞</td>
<td>Disconnect all participants from your meeting room. Or, disconnect a single participant from your meeting room.</td>
</tr>
<tr>
<td>📚</td>
<td>Alphabetically sort the list of your participants.</td>
</tr>
<tr>
<td>📅</td>
<td>Sort the list of your participants in attendance order.</td>
</tr>
<tr>
<td>⌛️</td>
<td>Toggle between viewing the current conference duration and viewing the current time of day. The conference timer is the default view.</td>
</tr>
</tbody>
</table>

Configuring Conference Settings

The *Control Meeting* page provides access to the *Settings* dialog box. This dialog box enables you to access the VidyoReplay Library (if applicable), configure or change a Moderator PIN, Room Link, Room PIN, Webcast Link, and Webcast PIN. You can also use this dialog box to enable and disable Presenter Mode.

**Note** VidyoReplay is an optional server appliance that enables users to stream live or pre-recorded video. For more information about VidyoReplay, contact your Vidyo sales representative.

**To configure your conference settings:**

1. Log in to the Admin portal using your Admin account.
   For more information, see [Logging In as a Tenant Admin](#).
   The *Users* page displays by default.

2. Click the *Meeting Rooms* tab.
   The *Manage Meeting Rooms* page displays.

3. Click the *Control Meeting* link in the Control Meeting column of the meeting that needs to be controlled.
   The HTML-based *Control Meeting* page displays.
4. Click 

The *Settings* dialog box displays.

5. Perform any of the following tasks:

- 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](http://support.vidyo.com).

- To set a Moderator PIN:
  - Enter four characters in the Moderator PIN text box.
12. Managing Meeting Rooms as the Tenant Admin

- Click **Save**.

To change or delete the room link URL, which is the link used by participants and guests to join the room.

- Click + to create a new room link URL.
  
  The system automatically generates a new link URL and displays it in the Room Link field.

- Click - to remove the room link URL that currently displays in the Room Link field.

- To set a Room PIN:
  
  - Enter four characters in the Room PIN textbox.
  
  - Click **Save**.

  Participants will be prompted to enter this PIN before they can join the room. Therefore, the meeting organizer should provide the participants with this PIN prior to holding meetings in the room.

- To change or delete the Webcast Link URL, which is the link used by participants and guests to access a webcast:
  
  - Click + to create a new Webcast Link URL.
  
  The system automatically generates a new webcast link URL and displays it in the Webcast Link field.

  - Click - to remove the webcast link URL that currently displays in the Webcast Link field.

When generating webcast links, the system resolves the VidyoReplay URL using DNS settings and establishes a connection on port 80 or 443 (depending on whether or not you have VidyoReplay security enabled). Therefore, port 80 or 443 must be opened on your network so your webcast links will work properly. For more information, see Appendix A, Firewall and Network Address Translations (NAT) Deployments, and refer to the VidyoReplay Administrator Guide.

- To set a Webcast PIN:
  
  - Enter four characters in the Webcast PIN textbox.
  
  - Click **Save**.

  Viewers will be prompted to enter this PIN before they can view the webcast. Therefore, the webcast owner should provide viewers with this PIN when notifying them about the webcast.

- Click the Presenter Mode switch to enable or disable Presenter mode. When entering or exiting Presenter mode, the following displays:
When Presenter Mode is enabled and a user joins a Vidyo meeting, instead of seeing all the meeting participants, the user sees presenter only, or if the presenter has not yet joined the meeting, the user sees a message telling them to please wait for the meeting to begin. In addition, the user’s microphone is muted.

- When enabling Presenter mode, a system notification displays at the top of the HTML-based Control Meeting screen asking you to “Please assign a presenter or click ‘Group’ to exit this mode” and you must select a participant as the presenter.

- When disabling Presenter Mode, a notification displays asking “Are you sure you want to exit Presenter mode?” and you must click OK.

A system notification then displays asking you to “Please wait for Presenter mode to begin.”

A system notification then displays asking you to “Please wait for Presenter mode to end.”

**Note** Alternatively, you can access Presenter Mode by clicking the **Presenter** button on the Control Meeting page, and you can exit Presenter Mode by clicking the **Group** button.

Waiting Room mode and some Presenter mode configurations are controlled by the Tenant Admin. For more information, see Configuring Room Attributes on Your Tenant and refer to the VidyoDesktop Quick User Guide.
6. Click **Close** to close the *Settings* dialog box.
   If you clicked the **Presenter Mode** switch, the *Settings* dialog box closes automatically.

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 lower-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.

The Participants list displays on the left side of the screen.
3. Click the Launch Control Meeting Panel.

4. Enter the Room Moderator PIN (provided to you by the room owner) in the prompt.

5. Click OK.

The HTML-based Control Meeting screen displays. 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 Meetings.

Controlling a Meeting from VidyoDesktop

Users who do not have administrator rights can access the Control Meeting page from VidyoDesktop only if they are the room owner or if they have been provided with the Moderator PIN. For more information, refer to the VidyoDesktop Quick User Guide.
Controlling a Meeting from a Tablet

If a user receives an invitation to a Vidyo meeting, and they click the guest link from their tablet, they are provided with an option to moderate the meeting. The user can moderate a meeting in their own room or in another person’s room by entering the Moderator PIN.

**To control a meeting from 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 page displays.
4. Tap **Manage Conference**.
The *Control Meeting Login* dialog box displays.

5. Enter your **Username** and **Password**.

6. Tap **OK**.
   - If the conference is being held in your own room, the *Control Meeting* screen displays.
   - If the conference is being held in another user’s room, you must first provide the Moderator PIN.
     - Enter the Moderator PIN provided by the room owner in the *Moderator PIN* dialog box.
     - Tap **OK**.
For more information about the tasks that you can perform from the Control Meeting screen, see Controlling Meetings.

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.
   The Users page displays by default.

2. Click the Meeting Rooms tab.
   The Meeting Rooms page displays.

3. Click Control Meeting for the meeting room containing participants you want to manage.
   The HTML-based Control Meeting screen displays.
   For more information, see Controlling Meetings.
13. Managing Tenant Admin Room Systems

The *Room Systems* tab displays the Display Name, IP Address, and Status for each room system that has been configured for the Tenant Admin. Upon clicking the blue **IP Address** link for the corresponding room system, the Admin UI for that room system displays.

For more information about how to configure and manage room systems, refer to the *VidyoRoom and VidyoPanorama600 Administrator Guide*.

<table>
<thead>
<tr>
<th>Display Name</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amr HD230</td>
<td></td>
<td>UP</td>
</tr>
<tr>
<td>Ben Pinkerton HD460</td>
<td></td>
<td>UP</td>
</tr>
<tr>
<td>dnu4</td>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>jpl3</td>
<td></td>
<td>DOWN</td>
</tr>
</tbody>
</table>
14. Managing Tenant Admin Groups as the Tenant Admin

Groups are special designations of users who have the common attributes such as the 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 Groups.

You may choose to create groups based on specific employee needs or departmental divisions. Changing the group settings for the 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.

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.
   The Users page displays by default.

2. Click the Groups tab.
   The Groups page displays.

   Groups on VidyoPortal display on the table and include Group Name, Max Participants, Max Bandwidth Out, and Max Bandwidth In as columns.

   **Tip**: You can drag and drop the column headings to arrange them in the order you prefer.

3. Search by group name using the Group Name search box above the table.
14. Managing Tenant Admin Groups as the Tenant Admin

4. Use the following functions at the bottom of the table:
   - 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](#). The **Users** page displays by default.

2. Click the **Groups** tab. The **Groups** page displays.

3. Click **Add Group** at the bottom of the **Groups** screen. The **Add Group: New Group** pop-up displays.

![Add Group: New Group](image)

4. Enter values in the following required fields:
   - Enter the name of the group in the **Group Name** field. The system checks to ensure it is unique.
   - Add an optional description for the group in the **Description** field.

**Note** The Max Number of Participants, Max Receive Bandwidth Per User (Kbps), and Max Transmit Bandwidth Per User (Kbps) fields are populated by default.
Enter values in the Max Number of Participants, Max Receive Bandwidth Per User (Kbps), and Max Transmit Bandwidth Per User (Kbps) fields if necessary.

Select the Allow VidyoReplay checkbox if you want to enable members of this group to start recording meetings.

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.

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.
   The Users page displays by default.

2. Click the Groups tab.
   The Groups page displays.

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.

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.
   The Users page displays by default.

2. Click the Groups tab.
   The Groups page displays.
3. Find the group you wish to delete by using the search filters, sorting on the headers, and pagination.

Once the group has been found, select the checkbox in the Delete column for the group.

4. Click **Delete** at the bottom of the page.

5. Click **Yes** in the *Confirmation* dialog box that opens.

6. Repeat for all groups that you wish to delete.
15. 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.
   The Users page displays by default.
2. Click the Settings tab.
   The License page displays by default.
3. Review your license terms shown on the License screen.

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.

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.
15. Configuring Settings as the Tenant Admin

**Note** Since Super Admin endpoint software uploads overwrite Tenant Admin uploads, Tenant Admins should always upload files on their tenants after Super Admin uploads are completed.

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](#).  
   The *Users* page displays by default.

2. Click the *Settings* tab.  
   The *License* page displays by default.

3. Click *Upload Endpoint Software* on the left menu.  
   The *Upload Endpoint Software* page displays.

4. Click *Browse*.

5. Click *Upload* to import the installation file after selecting 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 displays in the Uploaded Endpoint Software list under its corresponding heading. Scroll through this list to view all available installation files.

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](#).
   
   The *Users* page displays by default.

2. Click the *Settings* tab.
   
   The *License* page displays by default.

3. Click *Upload Endpoint Software* on the left menu.
   
   The *Upload Endpoint Software* page displays.

4. Select the checkboxes for the files you wish to activate.

5. Click *Activate* at the top or bottom of the list.
15. Configuring Settings as the Tenant Admin

The file name displays 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.
   The Users page displays by default.

2. Click the Settings tab.
   The License page displays by default.

3. Click Upload Endpoint Software on the left menu.
   The Upload Endpoint Software page displays.

4. Select the checkboxes for the files you wish to delete.
15. Configuring Settings as the Tenant Admin

5. Click **Delete**.

6. Click **Yes** in the **Confirmation** pop-up that opens.

   If you delete a file by mistake, you must 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 15 languages:

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

To set the system language of your tenants to one of the 15 available languages:

1. Log in to the Admin portal using your Admin account.
15. Configuring Settings as the Tenant Admin

For more information, see [Logging In as a Tenant Admin](#).

The *Users* page displays by default.

2. Click the *Settings* tab.

   The *License* page displays by default.

3. Click *System Language* on the left menu.

   The *System Language* page displays.

4. Select the System Language from the *Default System Language* drop-down.

   ![System Language](image)

   **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*.  

---

272
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](#).
   The Users page displays by default.

2. Click the Settings tab.
   The License page displays by default.

3. Click Guest’s Settings on the left menu.
   The Guest’s Settings page displays.

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 displays when users click *About Us* at the bottom of the VidyoPortal home page and the VidyoPortal Admin and Super Admin Portal.

<table>
<thead>
<tr>
<th>Note</th>
<th>Configurations made in the Tenant Admin portal override settings made in the Super Admin portal.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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](#).  
   The *Users* page displays by default.
2. Click the *Settings* tab.  
   The *License* page displays by default.
3. Click to the left of *Customization* on the left menu.
4. Click the *About Info* from the submenu.
15. Configuring Settings as the Tenant Admin

The About Info page displays.

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](#).

   The Users page displays by default.

2. Click the Settings tab.
   
   The License page displays by default.
3. Click ‌+‌ to the left of *Customization* on the left menu.

4. Click *About Info* from the submenu.
   The *About Info* page displays.

5. Click *Default* to remove any previously saved customized text and revert to the default system text provided by Vidyo.
   A *Confirmation* pop-up displays.

   ![Confirmation Pop-up](image)

   6. Click *Yes*.

**Customizing Support Information**

The *Support Info* page enables you to create and format a contact page that displays 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 use to contact you. 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*.
   The *Users* page displays by default.

2. Click the *Settings* tab.
   The *License* page displays by default.

3. Click ‌+‌ to the left of *Customization* on the left menu.

4. Click *Support Info* from the submenu.
15. Configuring Settings as the Tenant Admin

The Support Info page displays.

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

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

6. Apply any formatting desired.

7. 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:

1. Log in to the Admin portal using your Admin account.
   For more information, see Logging In as a Tenant Admin.
15. Configuring Settings as the Tenant Admin

The Users page displays by default.

2. Click the Settings tab.

The License page displays by default.

3. Click + to the left of Customization on the left menu.

4. Click Support Info from the submenu.

The Support Info page displays.

5. Click Default to remove any previously saved customized text and revert to the default system text provided by Vidyo.

A Confirmation pop-up displays.

6. 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 If a From email address is not provided, SMTP servers may block emails or change 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.

   The Users page displays by default.

2. Click the Settings tab.
15. Configuring Settings as the Tenant Admin

The *License* page displays by default.

3. Click ☰ to the left of *Customization* on the left menu.

4. Click *Notification* from the submenu.

The *Notification* page displays.

5. Enter the **Email (From)** and **Email (To)** email addresses.

6. Select the **New Account Notification** checkbox to have the system send a welcome email to each new account created.

7. Click **Save**.

Customizing the Invite Text

The *Invite Text* page enables you to customize the boilerplate 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.
15. Configuring Settings as the Tenant Admin

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](#).

**To customize Invite Text:**

1. Log in to the Admin portal using your Admin account.
   For more information, see [Logging In as a Tenant Admin](#).
   The *Users* page displays by default.

2. Click the *Settings* tab.
   The *License* page displays by default.

3. Click the + to the left of *Customization* on the left menu.

4. Click *Invite Text* from the submenu.
5. Change the text from the Email Content, Voice Only, Webcast, and Email Subject sections as desired.

The following system variables (uppercase text inside of brackets) display and can be inserted in sections of your invite text using the following buttons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📞</td>
<td>Available in the Email Content and Voice Only sections, the [DIALIN_NUMBER] variable inserts the dial-in number of your room into your invite text.</td>
</tr>
<tr>
<td>🌐</td>
<td>Available in the Email Content and Voice Only sections, the [PIN_ONLY] variable inserts the PIN (if one is configured) of your room into your invite text.</td>
</tr>
<tr>
<td>📞</td>
<td>Available in the Email Content and Voice Only sections, the [EXTENSION_ONLY] variable inserts the room extension (if one is configured) into your invite text.</td>
</tr>
</tbody>
</table>
| 🌐 | Required in the Email Content section, the [ROOMLINK] variable inserts a hyperlink to your room into your invite text.  
When accessed from a tablet, room links may be used to join a conference, annotate, or manage a meeting. |
15. Configuring Settings as the Tenant Admin

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="arrow_up" /></td>
<td>Available in the Email Content section, the <code>[LEGACY_URI]</code> variable inserts the URI participants will use to access your room from Legacy endpoints.</td>
</tr>
<tr>
<td><img src="image" alt="phone" /></td>
<td>Available in the Email Content section, the <code>[DIALSTRING]</code> variable inserts the phone number participants will use to access your room voice-only telephones.</td>
</tr>
<tr>
<td><img src="image" alt="ellipsis" /></td>
<td>Required in the Webcast section, the <code>[WEBCASTURL]</code> variable inserts the URL participants can use to access your webcast.</td>
</tr>
</tbody>
</table>

Some additional variables (ones that do not have buttons or icons) and display in sections of your invite text include:

- The `[DISPLAYNAME]` variable inserts the specific user’s display name as it was entered in to the system in the Email Content section.
- The `[EXTENSION]` variable inserts the room extension (if one is configured) along with the room PIN (if one is configured) into your invite text.
- The `[PIN]` variable inserts the room PIN (if one is configured) in the Email Content section.
- The `[ROOMNAME]` variable inserts name of the room for which the invite was issued.
- The `[TENANTURL]` variable inserts the name of the tenant in the Email Content section.

**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.

6. Click **Save** to save the invitations.

**Making Common Invite Text Changes**

You can make the following common changes to invite text:

- If your organization uses mobile devices that support a tap-to-connect functionality, you can add the following template to your invite: Voice only users can tap-to-connect: “[DIALIN_NUMBER], [EXTENSION]#”.

- 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, room links 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**  Some browsers may not support email invitation generation due to a limitation on the number of characters in the invite text. Vidyo recommends that you generate the email invitation prior to making that text the default, and reduce the number of characters if needed.

### 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](#).
   The *Users* page displays by default.

2. Click the *Settings* tab.
   The *License* page displays by default.

3. Click the ![plus](plus.png) to the left of *Customization* on the left menu.

4. Click *Invite Text* from the submenu.
   The *Invite Text* page displays.

5. Click *Default* to remove any previously saved customized text and revert to the default system text provided by Vidyo.
15. Configuring Settings as the Tenant Admin

A Confirmation pop-up displays.

6. Click Yes.

Uploading Custom Logos on Your Tenant

You can customize the logo that appears on the VidyoDesktop Download page, which is the page shown to users when a software update is performed, and on the Control Meeting page, which is the page shown to meeting moderators.

**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.

The customized logos per tenant display on the HTML-based Control Meeting screen.

For more information, see Controlling Meetings.

**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.
   
   The Users page displays by default.
   
2. Click the Settings tab.
   
   The License page displays by default.
   
3. Click + to the left of Customization on the left menu.
   
4. Click Customize Logos from the submenu.
5. Click Browse… to locate the logo that needs to be uploaded.

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 Meetings.

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 displays in a new browser tab.

8. Click Remove to delete the logo file currently in use.
   If you remove a customized logo file, it 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, Web Services, or SAML authentication.

For more information, see Configuring Authentication Using Web Services or Configuring Authentication Using SAML.
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 first be set up.

### Configuring Your VidyoPortal Tenant 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](#).

---

**Note**

To use secured LDAP, upload your LDAP certificate chain (intermediates and root) from your certification authority using the *Security* page before enabling LDAP. For more information, see [Securing Your VidyoConferencing System with SSL and HTTPS](#).

When LDAP authentication is enabled, the User and Admin Portals do not show Change or Forgot 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](#).
   
   The *Users* page displays by default.

2. Click the *Settings* tab.
   
   The *License* page displays by default.

3. Click *Authentication* on the left menu.
   
   The *Authentication* page displays.
4. Select **LDAP** from the **Authentication Type** drop-down.

The **Authentication** page expands and shows additional fields as follows:

![Authentication page screenshot](image)

*Note*  
Field entries on the screenshot show a typical LDAP configuration.

5. Enter the following information:

- Enter the LDAP server URL in the **URL** field.
  
The format is **ldap:// [IP or FQDN address]/:389**.

*Note*  
To use secure LDAP (LDAPS), use an “ldaps” prefix:

**ldaps:// [IP or FQDN address]/:636**

- Overwrite the auto-populated credentials in the **Bind DN** or **username** field to log in to the LDAP server if necessary.
15. Configuring Settings as the Tenant Admin

For example: \texttt{uid=user, ou=employees, dc=vidyo, dc=com}.

**Note**  
The user must be able to search the LDAP tree.

- Overwrite the auto-populated password in the *Bind password* field needed to bind with the LDAP server if necessary.

- Enter the base object (baseObject) used for searching in the optional *Search base* field.

  For example: \texttt{ou=employees, dc=vidyo, dc=com}.

- Enter the configuration string to return the LDAP Distinguished Name (DN) in the *Filter template* field.

  For example: \texttt{uid=<>} where \texttt{<>} is replaced by the VidyoPortal user name during authentication.

- Select the base object (baseObject) from the Scope options 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* pop-up displays.

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](#) or [Understanding LDAP Authentication with Auto-Provisioning](#).

9. Apply authentication to specific user types.

   For more information, see [Applying Authentication (LDAP or Web Service) to Specific User Types](#).

288
15. Configuring Settings as the Tenant Admin

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**.
   
   The *Users* page displays by default.
2. Click the *Settings* tab.
   
   The *License* page displays by default.
3. Click *Authentication* on the left menu.
   
   The *Authentication* page displays.
4. Configure your VidyoPortal to use your LDAP server.
   
   For more information, see **Configuring Your VidyoPortal Tenant to Use Your LDAP Server**.
5. Create user accounts manually on your tenant. User accounts can be added at any time.
   
   For more information, see **Adding a New User** or **Importing Users**.

**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 Forgot Password options.

6. Apply authentication to specific user types.
   
   For more information, see **Applying Authentication (LDAP or Web Service) to Specific User Types**.
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:
15. Configuring Settings as the Tenant Admin

1. The user name and password is validated against the LDAP server. For more information, see Configuring Your VidyoPortal Tenant to Use Your LDAP Server.

2. If authentication succeeds, the LDAP server returns the user’s attributes as you have specified using the LDAP Attributes Mapping pop-up.

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** pop-up looks like the following:
15. Configuring Settings as the Tenant Admin

Each row on the LDAP Attributes Mapping pop-up 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 pop-up 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** field, 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 Tenant to Use Your LDAP Server.

  - 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** field, 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.

  - 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 pop-up 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 pop-up.
15. Configuring Settings as the Tenant Admin

The following screenshot provides an example of a Value mapping configuration where the `memberOf` LDAP Attribute Name is used.

![LDAP Attributes Mapping](image)

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 field, 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 field, 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 field, 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** field, 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. The number of digits in the auto generated extension values is not fixed and may vary.

- **No Value** mapping configurations are made for the **Extension**.

**Group** is the name of this specific LDAP attribute in the VidyoPortal.

- **In the **LDAP Attribute Name** field, 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 group configured as Default, VidyoUS_East, VidyoUS_West, etc. values from which you can select. Map these groups using the Attribute Value Mapping pop-up.

- 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 pop-up 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 pop-up.
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 **Default** group and logs in to the User or Admin portal, the account is created with the **Default** Group.

- **Description** is the name of this specific LDAP attribute in the VidyoPortal.
  - In the **LDAP Attribute Name** field, 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 Description when the **LDAP Attribute Name** does not exist or returns an invalid attribute value or no Value mapping criteria is met.
15. Configuring Settings as the Tenant Admin

- 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** field, enter a value to map to the Proxy 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 `nj2-al-vvr1`, `il2-al-vvr1`, `nj1-al-vr1`, etc. from which you can select. Map these groups using the **Attribute Value Mapping pop-up**.

![LDAP Attributes Mapping](image-url)
15. Configuring Settings as the Tenant Admin

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 Proxy.

Different users return different LDAP Attribute Values. The Attribute Values Mapping pop-up allows you to map specific associations for all possible values returned.

Click the **Duplicate** and **Remove** buttons to create or delete rows in the Attribute Values Mapping pop-up if desired.

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 `nj2-al-vvr1` VidyoProxy and logs in to the User or Admin portal, the account is created with the `nj2-al-vvr1` VidyoProxy.

- **Location Tag** is the name of this specific LDAP attribute in the VidyoPortal.

- In the **LDAP Attribute Name** field, 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, east_us_region_tag, west_us_region_tag, etc. 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 location tag.

Different users return different LDAP Attribute Values. The Attribute Values Mapping pop-up allows you to map specific associations for all possible values returned.

Click the Duplicate and Remove buttons to create or delete rows in the Attribute Values Mapping pop-up if desired.
The following screenshot provides an example of a Value mapping configuration where the **physicalDeliveryOfficeName** LDAP Attribute Name is used.

![LDAP Attributes Mapping](image)

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 **EAST** Location Tag.

- The following attributes are optional biographical information about the user. Therefore, default values are not set for these attributes:
  - Phone Number 1
  - Phone Number 2
  - Phone Number 3
  - Department
  - Title
  - IM
  - Location

- Thumbnail Photo is the name of this specific LDAP attribute in the VidyoPortal.
  - The Thumbnail Photo must be a `.png`, `.jpg`, or `.jpeg` and smaller than the maximum size that the Super Admin configures in **Settings > Feature Settings > User Attributes** within the Super Admin Portal.
  - For more information, see [Configuring User Attributes](#).
  - No **Default Value** is entered for Thumbnail Photo.
  - No Value mapping configurations are made for Thumbnail Photo.

### 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 process.
15. Configuring Settings as the Tenant Admin

Mapping step in the following procedure. For more information, see Understanding LDAP Authentication with Auto-Provisioning and Understanding the VidyoPortal User Account Attributes.

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.
   The Users page displays by default.

2. Click the Settings tab.
   The License page displays by default.

3. Click Authentication on the left menu.
   The Authentication page displays.

4. Configure your VidyoPortal to use your LDAP server.
   For more information, see Configuring Your VidyoPortal Tenant to Use Your LDAP Server.

5. Select the LDAP Attributes Mapping checkbox.
   The Edit Attributes Mapping and Test Attributes Mapping buttons display.

6. Click Edit Attributes Mapping.
   The LDAP Attributes Mapping pop-up displays.
   An example of the LDAP Attributes Mapping pop-up with data looks like the following:
15. Configuring Settings as the Tenant Admin

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 actually making the configurations in the LDAP Attributes Mapping pop-up. For more information, see Understanding LDAP Authentication with Auto-Provisioning and Understanding the VidyoPortal User Account Attributes.

Each row on the LDAP Attributes Mapping pop-up 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. Click Test Attributes Mapping and provide the user account credentials for the account you wish to test as follows only after configuring your LDAP Attributes Mapping:

a. Type the User Name for the account you wish to test.
15. Configuring Settings as the Tenant Admin

b. Type the **Password** for the account you wish to test.

c. Click **Submit**.

If successful, the *LDAP Attributes Mapping results* pop-up displays 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](#).

### Configuring Authentication Using Web Services

Using Web Service Authentication requires an enabled Vidyo API license.

**To configure Web Service Authentication:**

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](#).
   
   The *Users* page displays by default.

2. Click the **Settings** tab.
   
   The *License* page displays by default.

3. Click **Authentication** on the left menu.
   
   The *Authentication* page displays.

4. Configure your VidyoPortal to use your LDAP server.
   
   For more information, see [Configuring Your VidyoPortal Tenant to Use Your LDAP Server](#).
5. Select **Web Service** from the **Authentication Type** drop-down.

6. Enter the URL of your authentication server in the **URL** field.

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.
   The Users page displays by default.

2. Click the Settings tab.
   The License page displays by default.

3. Click Authentication on the left menu.
   The Authentication page displays.

4. Configure your VidyoPortal to use your LDAP server.
   For more information, see Configuring Your VidyoPortal Tenant to Use Your LDAP Server.

   For more information, see Configuring LDAP Authentication with Manual User Creation. The following attributes are optional biographical information about the user. Therefore, default values are not set for these attributes:

   - Phone Number 1
   - Phone Number 2
   - Phone Number 3
   - Department
   - Title
   - IM
   - Location

   Thumbnail Photo is the name of this specific LDAP attribute in the VidyoPortal.

   - The Thumbnail Photo must be a .png, .jpg, or jpeg and smaller than the maxium size that the Super Admin configures in Settings > Feature Settings > User Attributes within the Super Admin Portal.

     For more information, see Configuring User Attributes.

   - No Default Value is entered for Thumbnail Photo.

   - No Value mapping configurations are made for Thumbnail Photo.
Configuring LDAP Authentication with Auto-Provisioning, or Configuring Authentication Using Web Services.

6. Select one or more user types to validate by LDAP from the Available types list.

7. Click the Right Arrow button to transfer your selection or selections to the Selected types list.

8. Click Save.

9. Verify that the selected user types are configured with the authentication you selected (LDAP or Web Service) by logging in to your User portal.

Configuring Authentication Using SAML

You can configure authentication using SAML to provide Single Sign-On (SSO) and Auto-Provisioning capabilities for Normal and Executive user types on your system. Other account types such as VidyoRoom, VidyoPanorama, Admin, and Operator must be manually provisioned.

For more information, see Understanding the Different System Accounts.

Once configured, SAML authentication will let your users log in and create Vidyo accounts on-the-fly based on authorized credentials from a SAML Identity Provider (IdP).

Note SAML 2.0 functionality operates in browser-based application environments and is not currently supported on VidyoMobile or VidyoRoom.

You cannot use more than one IdP for a given tenant. However, multiple tenants can use the same IdP.

Where Are You From (WAYF) services are not supported at this time.

Configuring Your VidyoPortal Tenant to Use Your SAML Server

When you configure your VidyoPortal tenant for SAML authentication, your VidyoPortal uses the SAML 2.0 protocol to externally authenticate your Vidyo users against your SAML server.

Normal or Executive user types can be authenticated by SAML. For more information, see Understanding the Different System Accounts.

Note When SAML authentication is enabled, the User and Admin Portals do not show Change or Forgot Password options.

You must first choose and configure your user provisioning model before deploying your tenants SP metadata to your IdP. The following topics explain how you can configure your VidyoPortal tenant to manually or automatically provision your users.
15. Configuring Settings as the Tenant Admin

Configuring SAML Authentication with Manual User Creation

This SAML Authentication method requires you to manually create user accounts on your tenant. The user attributes are manually maintained directly on the VidyoPortal by the Tenant Admin. Only the username and password are externally verified from your SAML server before your VidyoDesktop user is logged in to the system.

To configure SAML 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.
   The Users page displays by default.

2. Click the Settings tab.
   The License page displays by default.

3. Click Authentication on the left menu.
   The Authentication page displays.

4. Select SAML from the Authentication Type drop-down.

5. Enter the following information:
   - Enter your IdP Metadata XML in the Identity Provider (IdP) Metadata XML field.
     Your SAML administrator should be able to provide you with the IdP Metadata.
The **Entity ID** field includes your tenants FQDN address by default. However, you may overwrite this default value if necessary.

**Note** If your system includes multiple tenants configured to use SAML authentication, this field must contain a unique entity ID for each tenant.

- Select **MetaIOP** or **PKIX** validation from the Security Profile options. PKIX is the most common profile used.
- Select **MetaIOP** or **PKIX** validation from the SSL/TLS Profile options.
- Select **PKIX** if you’re not certain of which profile to choose.
- Select **Yes** or **No** from the Sign Metadata options.
- Select **Local** from the **SAML provisioning type** drop-down.
- Enter your IdP attribute in the **IdP Attribute For User Name** field, which will be used when mapping your user names.

**Note** This should be provided to you from your IdP administrator. The value of this attribute must exactly match the user name ID used by your VidyoPortal.

- Click **View Service Provider (SP) Metadata XML** to view your service provider metadata XML for your SAML-enabled tenant.

**Note** You must provide this metadata XML to your IdP administrator to complete the SAML configuration on your tenant.

6. Create user accounts manually on your tenant.
   
   User accounts can be added at any time.

   For more information, see [Adding a New User](#) or [Importing Users](#).

**Note** When you create a new user with SAML authentication enabled, the user name must match the IdP attribute value for user name on your SAML server.

When creating new users, passwords are mandatory; however, when you enable SAML, the password in the local database is not used to authenticate the user.

When SAML authentication is enabled, the User Portal does not provide Change or Forgot Password options.

Only Normal or Executive user types are authenticated by SAML. For more information, see [Understanding the Different System Accounts](#).
15. Configuring Settings as the Tenant Admin

7. Click Save.

Understanding SAML Authentication with Auto-Provisioning

This SAML Authentication method automatically creates user accounts on your tenant based on mapping configurations. When your users log in to the User portal, the following takes place:

1. The VidyoPortal redirects the user to your IdP authentication page.
2. Your user name and password is validated against the SAML IdP server.
3. If authentication succeeds, the SAML server returns the user’s attributes as you have specified using the *SAML Attributes Mapping* pop-up.
   
   For more information, see [Understanding the VidyoPortal User Account Attributes](#).
4. The VidyoPortal then uses the set of attributes returned from the SAML server to create a new user account in the system.

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 SAML IdP Attributes in order to create accounts automatically.

**Note** When you provision users with SAML, user data is read-only in the system from the *Admin Portal > Users > Manage Users > Edit User* pop-up.
The following list explains VidiyoPortal attributes (Portal Attribute Names) that can be mapped to SAML 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 SAML attribute in the VidiyoPortal.
  - In the **SAML IdP Attribute Name** field, enter a name you have decided as being the attribute you want to associate the **User Name** within your existing SAML schema.
  - 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 SAML attribute in the VidiyoPortal.
15. Configuring Settings as the Tenant Admin

- Enter a value to map to the User Type in the **IdP Attribute Name** field.
- The **Default Value** you enter here is used as the default User Type when the **IdP Attribute Name** does not exist or returns an invalid attribute value or no Value mapping criteria is met.

You can select from Normal or Executive options. For more information, see [Users](#).

- The Value mapping is used to make specific associations between exact Portal Attribute Values and IdP Attribute Values based on the IdP Attribute Name selected for your User Type.

  Different users return different IdP Attribute Values. The **Attribute Values Mapping** pop-up 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** pop-up.

  The following screenshot shows the **Attribute Value Mapping** pop-up.

  ![Screen Shot of Attribute Mapping](image.png)

  **Note** In order to create these Portal User Type mapping associations, Vidyo recommends your IdP administrator creates specific security groups on your SAML server in advance.

<table>
<thead>
<tr>
<th>Portal Attribute Name</th>
<th>SAML IdP Attribute Name</th>
<th>Default Value</th>
<th>Value Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>User Type</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>User Type</td>
<td></td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>yourcompany.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extension</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>idp Provisioned User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy</td>
<td>No Proxy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location Tag</td>
<td>Default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  - **Display Name** is the name of this specific SAML attribute in the VidyoPortal.
  - In the **SAML IdP Attribute Name** field, enter a name you have decided as being the attribute you want to associate the User Name within your existing SAML schema.
  - In the **Default Value** field, enter a value for the Display Name 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 SAML attribute in the VidyoPortal.
  - In the SAML IdP Attribute Name field, enter a name you have decided as being the attribute you want to associate the E-Mail Address within your existing SAML schema. When a user logs in to the User portal, the system validates whether or not the SAML IdP Attribute Name value is actually an email address. If it’s not an email address, 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 SAML IdP 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 SAML attribute in the VidyoPortal.
  - In the SAML IdP Attribute Name field, enter a value you have decided as being the attribute you want to associate the Extension within your existing SAML schema.
  - No Default Value is entered for User Name. When a user logs in to the User or Admin portal and an empty or invalid SAML IdP Attribute Name is retrieved from your SAML 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 SAML IdP 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.

  - Group is the name of this specific attribute in the VidyoPortal.
  - In the SAML IdP Attribute Name field, enter a name you have decided as being the attribute you want to associate the Group within your existing SAML schema.
If the **SAML IdP Attribute Name** does not exist or returns an invalid attribute value or no Value mapping criteria is met, the value you specify here is used as the default User Type. The VidyoPortal tenant used in this example has Groups configured as **Default**, **PanoRoom – 2M**, etc. values, from which you can select. Map these groups using the **Attribute Value Mapping** pop-up.

The **Value Mapping** is used to make specific associations between exact Portal Attribute Values and SAML IdP Attribute Values based on the **SAML IdP Attribute Name** selected for your User Type.

Different users return different SAML IdP Attribute Values. The **Attribute Values Mapping** pop-up allows you to map specific associations for all possible values returned.
Click the **Duplicate** and **Remove** buttons to create or delete rows in the *Attribute Values Mapping* pop-up if desired.

For example, using the screenshot shown here, you can see that when a user is a member of the **Default** group and logs in to the User or Admin portal, the account is created with the **Default** Group.

- **Proxy** is the name of this specific IdP attribute in the VidyoPortal.
- In the **IdP Attribute Name** field, enter a value to map to the **Proxy** in your IdP schema.

Many users choose to enter **memberOf** as the **IdP 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 IdP 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 nj2-al-vvr1, il2-al-vvr1, etc. from which you can select. Map these groups using the Attribute Value Mapping pop-up.

The Value mapping is used to make specific associations between exact Portal Attribute Values and IdP Attribute Values based on the IdP Attribute Name selected for your proxy. Different users return different IdP Attribute Values. The Attribute Values Mapping pop-up allows you to map specific associations for all possible values returned.

Click the Duplicate and Remove buttons to create or delete rows in the Attribute Values Mapping pop-up if desired.
15. Configuring Settings as the Tenant Admin

The following screenshot shows the *Attribute Values Mapping* pop-up.

- **Location Tag** is the name of this specific IdP attribute in the VidyoPortal.
- In the **IdP Attribute Name** field, enter a value to map to the Location Tag in your IdP schema.
- **Default Value** you enter here is used as the default Location Tag when the **IdP Attribute Name** does not exist or returns an invalid attribute value or no Value mapping criteria is met.
15. Configuring Settings as the Tenant Admin

The VidyoPortal tenant used in this example has Location Tags configured as Default from which you can select.

- The Value mapping is used to make specific associations between exact Portal Attribute Values and IdP Attribute Values based on the IdP Attribute Name selected for your location tag.

  Different users return different IdP Attribute Values. The Attribute Values Mapping pop-up allows you to map specific associations for all possible values returned.

  Click the Duplicate and Remove buttons to create or delete rows in the Attribute Values Mapping pop-up if desired.
The following screenshot shows the *Attribute Values Mapping* pop-up.

- Description is the name of this specific IdP attribute in the VidyoPortal.
  - In the **IdP Attribute Name** field, enter a value to map the Description in your IdP schema.
  - The **Default Value** you enter here is used as the default Description when the **IdP 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.

**Configuring SAML Authentication with Auto-Provisioning**

Before configuring SAML Authentication with auto-provisioning, it is highly recommended that you first decide which SAML attributes you want to map to your VidyoPortal user account attributes. These mapping decisions become your SAML auto-provisioning scheme during the Edit Attributes Mapping step in the following procedure. For more information, see [Understanding SAML Authentication with Auto-Provisioning](#) and [Understanding the VidyoPortal User Account Attributes](#).
Note  You can still manually create users even if you configure SAML authentication with auto-provisioning. However, these manual users do not automatically update attributes from your IdP server.

To configure SAML 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.
   The *Users* page displays by default.

2. Click the *Settings* tab.
   The *License* page displays by default.

3. Click ✪ to the left of *Customization* on the left menu.

4. Click *Authentication* on the left menu.
   The *Authentication* page displays.

5. Select *SAML* from the *Authentication Type* drop-down.

6. Enter the following information:

   - Enter your IdP Metadata XML in the *Identity Provider (IdP) Metadata XML* field. Your SAML administrator should be able to provide you with the IdP Metadata.
   - Select *MetalOP* or *PKIX* validation from the Security Profile options. PKIX is the most common profile used.
   - Select *MetalOP* or *PKIX* validation from the SSL/TLS Profile options. Select *PKIX* if you’re not certain of which profile to choose.
   - Select *Yes* or *No* from the Sign Metadata options.
   - Select *SAML* from the *SAML provisioning type* drop-down.
Click **Edit IdP Attributes Mapping** and configure your IdP attribute to be used for mapping your user accounts.

Each row on the **SAML IdP Attributes Mapping** pop-up represents an attribute. For each attribute, there is an associated Portal Attribute Name, SAML IdP Attribute Name, Default Value, and Value mapping (where applicable). These configurations become the rules telling the system what values to populate in specific user account fields when the new account is created.

**Note** Changes made to Attribute Mapping information also affect the View Service Provider (SP) Metadata XML information.

You should spend some time analyzing your VidyoPortal user account attributes in order to decide which SAML IdP attributes you want to associate with them before actually making the configurations on the **SAML IdP Attributes Mapping** pop-up. For more information, see **Understanding the VidyoPortal User Account Attributes**.
15. Configuring Settings as the Tenant Admin

- Click **View Service Provider (SP) Metadata XML** to view your service provider metadata XML for your SAML-enabled tenant.

**Note** You must provide this metadata XML to your IdP administrator to complete the SAML configuration on your tenant.

7. Click **Save**.

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 their account is created. Location tags are a feature of the Router Pools architecture. For more information, see [Configuring Router Pools](#).

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](#).
   The **Users** page displays by default.

2. Click the **Settings** tab.
   The **License** page displays by default.

3. Click **Manage Location Tags** on the left menu.
15. Configuring Settings as the Tenant Admin

The *Location Tags* page displays.

4. Select the location tag from the **Default Location Tag** drop-down 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](#).

5. Click **Advanced**.
The Assign Location Tags to Groups table opens, which allows you to assign a location tag to existing users of selected groups.

<table>
<thead>
<tr>
<th>Location Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Location Tag on the left, Group(s) on the right, then click Assign</td>
</tr>
<tr>
<td>Available Location Tags</td>
</tr>
<tr>
<td>Default</td>
</tr>
<tr>
<td>pool1_tag</td>
</tr>
<tr>
<td>pool2_tag</td>
</tr>
<tr>
<td>pool3_tag</td>
</tr>
<tr>
<td>pool4_tag</td>
</tr>
<tr>
<td>pool5_tag</td>
</tr>
<tr>
<td>pool6_tag</td>
</tr>
</tbody>
</table>

6. 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 checkbox).

7. Click Assign.
   
   All existing users within the selected Group or Groups will now have this location tag assigned to them.

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.
   
   The Users page displays by default.

2. Click the Settings tab.
   
   The License page displays by default.

3. Click CDR Access on the left menu.
The CDR Access page displays.

4. Specify a date range.
5. Click Export.

**Note**  The export record limit is 65,000 records. If the export contains more than 65,000 records, a message displays 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.
Configuring Endpoint Network Settings 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 are assigned corresponding values that 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.

You may tag packets as a non-Administrative user, if desired, using Windows Group Policy settings. Sites may be able to establish domain policy rules implementing these settings.


**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.

You can also configure the media port range and enable use of the VidyProxy on the *Endpoint Network Settings* page.

**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](#).

   The *Users* page displays by default.

2. Click the *Settings* tab.

   The *License* page displays by default.
3. Click *Endpoint Network Settings* on the left menu.

The *Endpoint Network Settings* page displays.

![Endpoint Network Settings page](image)

4. Enter DSCP values for Video, Audio, Content, and Signaling.

Values provided must be decimals from 0 to 63. The values default to 0.

5. Enter the appropriate values in the fields in the Media Port Range section.

6. Click **Save**.

A *Confirmation* pop-up displays.

![Confirmation pop-up](image)

7. Click **Yes**.
A message displays stating that 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 Feature Settings on Your Tenant

You can configure Room Attribute feature settings on your tenants for your users. However, your Super Admin is able to decide whether or not the VidyoWeb, Chat, and User Attributes features may be configured on tenants.

For more information, see Setting Global Features.

Configuring VidyoWeb on Your Tenant

The VidyoWeb function does not display in Feature Settings if your Super Admin has decided to make it unavailable. For more information, see Enabling VidyoWeb Access. 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 extension 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.
   The Users page displays by default.

2. Click the Settings tab.
   The License page displays by default.

3. Click + to the left of Feature Settings on the left menu.
4. Click *VidyoWeb* from the submenu. The *VidyoWeb* page displays.

5. Deselect the **Enable VidyoWeb for guests** checkbox if you want to restrict VidyoWeb use on your tenant.

6. Select the **Enabled WebRTC for guests** checkbox if you want to allow WebRTC use on your tenant.

   The *Vidyo Server for WebRTC cluster address* field becomes active upon selecting the **Enabled WebRTC for guests** checkbox.

7. Enter the appropriate URL in the *Vidyo Server for WebRTC cluster address* field if you are using Vidyo Server for WebRTC.

   For more information about Vidyo Server for WebRTC, refer to the *Vidyo Server for WebRTC Administrator Guide*.

8. Click **Save**.
Configuring Public and Private Chat on Your Tenant

You can configure public or private chat on your tenant.

To configure public and private chat on your tenant:

1. Log in to the Admin portal using your Admin account.
   For more information, see Logging In as a Tenant Admin.
   The Users page displays by default.

2. Click the Settings tab.
   The License page displays by default.

3. Click ☁️ to the left of Feature Settings on the left menu.

4. Click Chat from the submenu.
15. Configuring Settings as the Tenant Admin

The *Chat* page displays.

5. Deselect the **Enable public chat** checkbox if you want to deny public chat for your tenant.
6. Deselect the **Enable private chat** checkbox if you want to deny private chat for your tenant.
7. Click **Save**.

Configuring Room Attributes on Your Tenant

On the *Room Attributes* page, you can configure room attributes on your tenant and control Waiting Room, Group Mode, and Presenter Mode feature settings. For more information about using Waiting Room, Group Mode, and Presenter Mode, refer to the *VidyoDesktop Quick User Guide*.

You can also make scheduled rooms available to your tenants. 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.

Allowing your tenants to create public rooms is configured here as well.
15. Configuring Settings as the Tenant Admin

To configure room attributes on your tenant:

1. Log in to the Admin portal using your Admin account.
   For more information, see Logging In as a Tenant Admin.
   The *Users* page displays by default.

2. Click the *Settings* tab.
   The *License* page displays by default.

3. Click ☐ to the left of *Feature Settings* on the left menu.

4. Click the *Room Attributes* from the submenu.
   The *Room Attributes* page displays.

5. Deselect the **Enable Waiting Room and Presenter mode** checkbox if you want to disable the waiting room and presenter mode features for your users.
15. Configuring Settings as the Tenant Admin

**Note** If you deselect the Enable Waiting Room and Presenter mode checkbox, the Select the Automatically start all meetings in Waiting Room mode and Prevent endpoints that do not support Presenter and Waiting Room modes from joining meetings when these modes are on checkboxes become inactive.

- Select the **Automatically start all meetings in Waiting Room mode** checkbox if you want all meetings to start in Waiting Room mode for your tenants.

  The **Automatically switch to Group mode when the owner joins** and **Stay in Waiting Room mode until a presenter is selected (Presenter mode)** radio buttons become active upon selecting the **Automatically start all meetings in Waiting Room mode** checkbox.

- Select either the **Automatically switch to Group mode when the owner joins** radio button to have conference participants interact with one another until the room owner joins the conference or the **Stay in Waiting Room mode until a presenter is selected (Presenter mode)** radio button if you don’t want the participants interacting with one another until a presenter is selected by a conference moderator.

6. Select the **Prevent endpoints that do not support Presenter and Waiting Room modes from joining meetings when these modes are on** checkbox to prevent users from entering meetings that use Presenter or Waiting Room modes if they are accessing the conference from endpoints that do not support those features.

7. Deselect the **Make Scheduled Rooms available on your tenant** checkbox if you want to restrict scheduled rooms from being available for your tenant.

8. Select the **Allow Public Room creation by users** checkbox if you want to allow your users to create public rooms.

   Upon selecting the **Allow Public Room creation by users** checkbox, the **Maximum number of rooms per User** field becomes active.
15. Configuring Settings as the Tenant Admin

9. Enter the maximum number of public rooms that the user can create in the **Maximum number of rooms per User** field.

10. Click **Save**.

**Configuring User Attributes**

You can allow or restrict users from uploading their own thumbnail photos.

**Note** In order to use this feature, the Vidyo endpoint must also support it.

If the user uploads a thumbnail photo, it will override LDAP and SAML provided images. When the user authenticates, the LDAP or SAML thumbnail photo is retrieved only if they have not uploaded a photo.

**To configure user attributes:**

1. Log in to the Admin portal using your Admin account.
   For more information, see [Logging In as a Tenant Admin](#).
   The **Users** page displays by default.

2. Click the **Settings** tab.
   The **License** page displays by default.

3. Click the **Feature Settings** on the left menu.

4. Click the **User Attributes** from the submenu.
The User Attributes page displays.

5. Select the Enable Thumbnail Photos checkbox to allow tenants to upload thumbnail photos.

The Allow users to upload their own image checkbox displays.

6. Select the Allow users to upload their own image checkbox to allow users to upload their own images on the Users page.

For more information, see Editing a User.

7. Click Save.
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 Syslog.

### 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.

For more information, see Audit Logs.

### Downloading Audit Logs from Your VidyoRouter

To download the Audit logs from your VidyoRouter:

1. Log in to your VidyoRouter Configuration Pages using your System Console account.

**Note** The URL of your VidyoRouter is typically a domain name: http://[IP or FQDN address]/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 Server and Changing the Default Password.

Although the default username for this page is admin, only the Super Admin accesses these pages.

The Settings tab and Maintenance left menu item displays by default.
2. Click the *Download Logs* subtab.

![Screenshot of Vidyo Gateway Settings page](image)

3. Select corresponding checkboxes for the logs you want to download.

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.

### Downloading Audit Logs From Your VidyoGateway

To download audit logs from your VidyoGateway:

1. Log in to your VidyoGateway using your System Console account.

**Note** The URL of your VidyoGateway is typically a domain name: `http://[vidyogateway.example.com]/`. 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 Server and Changing the Default Password](#).
2. Navigate to *Maintenance > Diagnostics*.

3. Click the **Download Audit Logs** button to download the file.
   The browser downloads the `.tar.gz` 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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Login</td>
<td>Login Successful</td>
</tr>
<tr>
<td></td>
<td>Logoff</td>
</tr>
<tr>
<td></td>
<td>Login Unsuccessful</td>
</tr>
<tr>
<td>Components</td>
<td>Component Updated</td>
</tr>
<tr>
<td></td>
<td>Router Pools Activated</td>
</tr>
<tr>
<td></td>
<td>Component Enabled</td>
</tr>
<tr>
<td></td>
<td>Gateway Added</td>
</tr>
<tr>
<td></td>
<td>Component Deleted</td>
</tr>
<tr>
<td></td>
<td>Gateway Modified</td>
</tr>
<tr>
<td></td>
<td>Component Disabled</td>
</tr>
<tr>
<td></td>
<td>Gateway Deleted</td>
</tr>
<tr>
<td>Tenants</td>
<td>Add Tenant</td>
</tr>
<tr>
<td></td>
<td>Delete Tenant</td>
</tr>
<tr>
<td></td>
<td>Modify Tenant</td>
</tr>
<tr>
<td>Router Pools</td>
<td>Add / Delete Pool</td>
</tr>
<tr>
<td></td>
<td>Discard Modified Config</td>
</tr>
<tr>
<td></td>
<td>Add / Delete Priority List</td>
</tr>
<tr>
<td></td>
<td>Create Location</td>
</tr>
<tr>
<td></td>
<td>Add / Delete Rule</td>
</tr>
<tr>
<td></td>
<td>Delete Location</td>
</tr>
<tr>
<td></td>
<td>Activate Cloud Config</td>
</tr>
<tr>
<td></td>
<td>Add / Delete Pool Connection</td>
</tr>
<tr>
<td></td>
<td>Create Modified Config</td>
</tr>
<tr>
<td>Settings</td>
<td>System License Updated</td>
</tr>
<tr>
<td></td>
<td>System Restart</td>
</tr>
</tbody>
</table>
### 16. Auditing

- Software Updated
- Database Backup
- Database Upload
- Database Download
- System Upgrade
- Ports Apply
- Generate CSR
- Upload CSR
- Clear CSR
- Certs Uploaded

<table>
<thead>
<tr>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
</tr>
<tr>
<td>- Login Successful</td>
</tr>
<tr>
<td>- Login Unsuccessful</td>
</tr>
<tr>
<td>Users</td>
</tr>
<tr>
<td>- Add User</td>
</tr>
<tr>
<td>- Delete User</td>
</tr>
<tr>
<td>Meeting Rooms</td>
</tr>
<tr>
<td>- Add Meeting Room</td>
</tr>
<tr>
<td>- Modify Meeting Room</td>
</tr>
<tr>
<td>Groups</td>
</tr>
<tr>
<td>- Add Groups</td>
</tr>
<tr>
<td>- Modify Groups</td>
</tr>
<tr>
<td>Settings</td>
</tr>
<tr>
<td>- Upload Software</td>
</tr>
<tr>
<td>- LDAP Save</td>
</tr>
<tr>
<td>- Authentication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VidyoManager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
</tr>
<tr>
<td>- Login Successful</td>
</tr>
<tr>
<td>- Logoff</td>
</tr>
</tbody>
</table>
16. Auditing

<table>
<thead>
<tr>
<th>Login Unsuccessful</th>
</tr>
</thead>
</table>

**Basic**

<table>
<thead>
<tr>
<th>Apply Config Server</th>
</tr>
</thead>
</table>

**Restart**

<table>
<thead>
<tr>
<th>Restart</th>
<th>Shutdown</th>
</tr>
</thead>
</table>

**VidyoRouter**

**Login**

<table>
<thead>
<tr>
<th>Login Successful</th>
<th>Logoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Unsuccessful</td>
<td></td>
</tr>
</tbody>
</table>

**Basic**

<table>
<thead>
<tr>
<th>Apply Config Server</th>
</tr>
</thead>
</table>

**Security**

<table>
<thead>
<tr>
<th>Ports Apply</th>
<th>Upload CSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate CSR</td>
<td>Clear CSR</td>
</tr>
</tbody>
</table>

**Upload**

<table>
<thead>
<tr>
<th>Upload and Upgrade</th>
<th>Shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart</td>
<td></td>
</tr>
</tbody>
</table>

**VidyoGateway**

**Login**

<table>
<thead>
<tr>
<th>Login Successful</th>
<th>Logoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Unsuccessful</td>
<td></td>
</tr>
</tbody>
</table>

**Config**

<table>
<thead>
<tr>
<th>Save</th>
<th>Save and Apply</th>
</tr>
</thead>
</table>

**Services**
16. Auditing

- Add Service
- Modify Service
- Delete 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 includes Timestamp, User ID, IP Address, and Description.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>User</th>
<th>IP Address</th>
<th>Action</th>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-09-13 10:46:43</td>
<td>admin</td>
<td>172.16.5.209</td>
<td>New Session</td>
<td></td>
<td>Session is reset</td>
</tr>
<tr>
<td>2011-09-13 10:46:48</td>
<td>admin</td>
<td>172.16.5.209</td>
<td>Login with correct userid/password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011-09-13 10:47:07</td>
<td>admin</td>
<td>172.16.5.209</td>
<td>Downloaded audit history files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011-09-13 10:48:06</td>
<td>admin</td>
<td>172.16.5.209</td>
<td>Downloaded audit history files</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 includes: Action ID, User ID, Tenant Name, Action, Action Result, Timestamp, IP Address, and Action Description.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>144</td>
<td>admin</td>
<td>main</td>
<td>Login</td>
<td>FAILURE</td>
<td>18:10.0</td>
<td>192.168.1.100</td>
</tr>
<tr>
<td>2</td>
<td>145</td>
<td>super</td>
<td>main</td>
<td>Login</td>
<td>SUCCESS</td>
<td>18:31.0</td>
<td>192.168.1.101</td>
</tr>
<tr>
<td>3</td>
<td>146</td>
<td>admin2</td>
<td>tenant2</td>
<td>Login</td>
<td>SUCCESS</td>
<td>18:54.0</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>4</td>
<td>147</td>
<td>super2</td>
<td>main</td>
<td>Login</td>
<td>SUCCESS</td>
<td>19:02.0</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>5</td>
<td>148</td>
<td>admin3</td>
<td>tenant2</td>
<td>Login</td>
<td>FAILURE</td>
<td>20:01.0</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>

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" action="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" action="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.
17. Configuring OCSP

The VidyoPortal, VidyoRouter, and VidyoGateway support Online Certificate Status Protocol (OCSP) verification. OCSP verification can be enabled on the following pages:

- VidyoPortal and VidyoRouter vr2conf
- 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 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. OCSP must then 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.
   The **License** page displays by default.
3. Click ☐ to the left of **Security** on the left menu
4. Click Advanced from the submenu.

The Advanced page displays.

5. Select the Enable OCSP checkbox.

6. Select the Override CA OCSP Responder checkbox and enter the IP or FQDN address of the new responder in the Responder URL field if you want to override the OCSP responders specified in the Client, Intermediate, and Root certificate.

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](#).

   The Components page displays by default.

2. Click the Settings tab.
The *License* page displays by default.

3. Click ☑ to the left of *Security* on the left menu.

4. Click *Applications* from the submenu.

   The *Applications* page displays.

5. Look in the Applications column for the application for which you want to enable OCSP, and then select the checkbox 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.

4. Select **disabled** from the *Status* drop-down.

5. Select **enabled** from the *Override Responder* drop-down and enter the IP or FQDN address of the new responder in Default Responder if you want to override the OCSP responders specified in the Client, Intermediate, and Root certificate.

6. Click **Save**.

   For VidyoRouter and VidyoGateway, this will immediately require OCSP certificate verification for the vr2conf 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.
17. Configuring OCSP

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:

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 Server and Changing the Default Password.

**Note**  Press the Enter key after each prompt.

2. Enter **m** for more options.

3. Enter **A** for Advanced Options.

4. Enter **3** to select the Disable OCSP option.

5. Enter **y** to save the configuration.
Note  OCSP can be disabled using the System Console option 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. 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.
Appendix A. Firewall and Network Address Translations (NAT) Deployments

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:

<table>
<thead>
<tr>
<th>VidyoDesktop and VidyoRoom Connectivity to VidyoPortal and VidyoRouter</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TCP Port 80</strong></td>
<td>HTTP – Outbound to VidyoPortal</td>
</tr>
<tr>
<td><strong>TCP Port 443</strong></td>
<td>TCP – Outbound to VidyoProxy (running on a VidyoRouter - optional)</td>
</tr>
<tr>
<td><strong>TCP Port 8443</strong></td>
<td>HTTPS – Outbound to VidyoRouter (optional)</td>
</tr>
<tr>
<td><strong>TCP Port 443</strong></td>
<td>HTTPS – Outbound to VidyoPortal (optional)</td>
</tr>
<tr>
<td><strong>TCP Port 17992</strong></td>
<td>EMCP – Outbound to VidyoPortal</td>
</tr>
<tr>
<td><strong>TCP Port 17990</strong></td>
<td>SCIP – Outbound to VidyoPortal/VidyoRouter</td>
</tr>
</tbody>
</table>

**Note** If you are using a VidyoRouter, the VidyoPortal does not apply.

| 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 |
Appendix A. Firewall and Network Address Translations (NAT) Deployments

**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 Appendix B. VidyoProxy.

When using VidyoReplay and generating webcast links, the system resolves the VidyoReplay URL using DNS settings and establishes a connection on port 80 or 443 (depending on whether or not you have VidyoReplay security enabled). Therefore, port 80 or 443 must be opened on your network so your webcast links will work properly. For more information, see Configuring Conference Settings, and refer to the VidyoReplay Administrator Guide.

### 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, VidyoGateway, and VidyoReplay

<table>
<thead>
<tr>
<th>Port</th>
<th>Service Description</th>
<th>Access Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port 80</td>
<td>HTTP – Inbound to Server</td>
<td>Web Access to VidyoPortal and VidyoRouter</td>
</tr>
<tr>
<td>TCP Port 443</td>
<td>HTTPS – Inbound to Server (optional)</td>
<td>Secure Web Access to VidyoPortal and VidyoRouter</td>
</tr>
<tr>
<td>TCP Port 22/2222</td>
<td>SSH – Inbound to Server</td>
<td>SSH access to the VidyoPortal and VidyoRouter</td>
</tr>
</tbody>
</table>

The following services outline the ports required for Router Pools cascading.

#### Router Pools Connectivity to VidyoPortal and VidyoRouter to VidyoRouter

<table>
<thead>
<tr>
<th>Port</th>
<th>Service Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port 80</td>
<td>HTTP – Router to VidyoPortal</td>
<td>Client to VidyoPortal authentication and GUI</td>
</tr>
<tr>
<td>TCP Port 443</td>
<td>HTTPS – Router to VidyoPortal (optional)</td>
<td>Optional for SSL connection to VidyoPortal</td>
</tr>
<tr>
<td>TCP Port 17991</td>
<td>RMCP – Router to VidyoPortal</td>
<td>Router connection to VidyoManager</td>
</tr>
<tr>
<td>TCP Port 17990</td>
<td>SCIP – Bi-Directional to and from VidyoRouters</td>
<td>Signaling connections between VidyoRouters</td>
</tr>
</tbody>
</table>
Router Pools  Connectivity to VidyoPortal and VidyoRouter to VidyoRouter

| UDP Ports 50,000 – 65,535 | RTP, sRTP, RTCP – Bi-Directional to and from VidyoRouters | Audio and Video Media from participants (6 ports per participant) |
| TCP Port 389 | LDAP – Outbound from Server | Optional authentication to LDAP and Active Directory. |

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.
Appendix A. Firewall and Network Address Translations (NAT) Deployments

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 vidyoportal.example.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](#).
Appendix A. Firewall and Network Address Translations (NAT) Deployments

**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**

**To configure 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](#).

   The *Components* page displays by default.

2. Click the *Tenants* tab.

   The *Tenants* page displays.

3. 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](#).

   The *Components* page displays by default.

2. Double-Click the blue *Name* link for the VidyoManager entry. The *VidyoManager* pop-up displays.

3. Enter the server **FQDN** (e.g., vidyoserver.example.com).

4. Edit the **EMCP Port** according to your needs and firewall rules.

   The default value for V2.0 is 17992; the default in V1 was 10000.
5. 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](#). The **Components** page displays by default.

2. Double-Click the blue **Name** link for the VidyoManager entry.
3. Edit the FQDN address (e.g., vidyorouter.example.com) in the SCIP section.

4. Edit the Port field according to your needs and firewall rules.

   The SCIP Port field is where you can set the SCIP (VidyoRouter) TCP Port. The default value for v2.0 is 17990; the default in v1 was 50000.

   Each VidyoRouter server requires a unique and separate FQDN to your VidyoPortal server. Use each server’s unique FQDN for the SCP address on each VidyoRouter configuration.

   For example: vr1.example.com, vr2.example.com, etc.

5. Click Save.

   For additional information about configuring your VidyoRouter, see Configuring Your VidyoRouter Component.
Appendix A. Firewall and Network Address Translations (NAT) Deployments

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, person icons display in green. If all person icons remain 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.

![VidyoDesktop™ - Logon](image)

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 you have successfully joined 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. Test from both the Inside LAN and from the Public Network by using the same URL – e.g., [http://portal.example.com](http://portal.example.com).

3. Test from each remote network segment if using multiple Media Address Maps.
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 Firewalled 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).
Appendix B. VidyoProxy

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 VidyoRoom 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.
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 your Vidyo server, 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 your Vidyo server.
  
  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).
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**
2. **Configuring Your Components to Work with HTTPS**
3. **Configuring Each VidyoPortal Component to Use Your FQDN**
4. **Applying VidyoPortal SSL Certificates to VidyoRooms**
5. **Implementing Encryption Using the Secured VidyoConferencing Option**

---

**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 page** – This page is used for generating or importing an SSL Private Key.
2. **SSL CSR page** – This page is used for generating an SSL Certificate Signing Request (CSR).
3. **Server Certificate page** – This page is for deploying your server certificate.
4. **Server CA Certificates page** – This page is for deploying your server Certification Authority (CA) certificates.
5. **Applications page** – Regarding Security, this page is used to correctly configure HTTPS Port settings to 443.

**Note** This page is also used for Management Interface configurations. For more information, see 5. **Configuring RADIUS**.

6. **Advanced page** – This page is for deploying your Client Root CA certificates.
Appendix C. Security

Note  The Advanced page is also used to upload, import and reset security settings. For more information, see Recovering from an HTTPS Failure and Resetting Your Security Configuration to Factory Defaults.

7. Passwords page – This page is used for setting password complexity rules and parameters.

The following ordered sections explain these steps in detail.

Note  When configuring a VidyoRouter for security, access your VidyoRouter at http://[IP or FQDN address]/vr2conf and use the exact same procedures for VidyoPortal SSL and HTTPS configuration described in Configuring Your Components to Work with HTTPS and Configuring Each VidyoPortal Component to Use Your FQDN.

- The URL of your VidyoRouter is typically a domain name: http://[IP or FQDN address]/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 Server and Changing the Default Password.

- Although the default username for this page is admin, only the Super Admin accesses these pages.

Importing, Exporting, and Regenerating an SSL Private Key

The following procedures show you how to import, export, and regenerate an SSL Private Key.

An initial key with a 2048 key size is automatically generated when you first set up your system. When regenerating, examine your own security requirements and applicable policies carefully before deciding on a suitable key size.

Importing an SSL Private Key

Private keys can be imported into your server. Vidyo recommends carefully backing up your existing SSL Private Key in its entirety before starting SSL Private Key procedures.
Note In order to import an SSL Private Key, you must first clear the HTTPS Only checkbox.

You can only import encrypted and password protected private keys that were exported from servers that also encrypted and password protected the private keys.

Changes made to an SSL Private Key require a new CSR and SSL Server Certificate. This includes importing existing keys, exporting existing keys, and regenerating new 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.

To import 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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click to the left of Security on the left menu.

4. Click SSL Private Key from the submenu.
   The SSL Private Key page displays.
5. Click **Import Private Key**.
   
The *Select Private Key* pop-up displays.

6. Click the **Select File** icon.

7. Locate and select your private key file.

8. Click **Open**.

9. Enter a password in the **Password (if any)** field if necessary.

10. Click **Upload**.
    
    If the upload is successful, the *File Upload Success* pop-up displays.
    
    A hash of the private key you imported displays in the **SHA256** field.

Regenerating 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** In order to regenerate an SSL Private Key, you must first clear the **HTTPS Only** checkbox.

Changes made to an SSL Private Key require a new CSR and SSL Server Certificate. This includes importing existing keys and regenerating new keys.

---

To regenerate 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](#).

   The *Components* page displays by default.

2. Click the **Settings** tab.

   The *Upload System License* page displays by default.

3. Click **Security** to the left of **Security** on the left menu.

4. Click **SSL Private Key** from the submenu.
The **SSL Private Key** page displays.

5. Specify a **1024**, **2048**, or **4096** key size from the **Key Size (bits)** drop-down.

**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.

6. Click **Regenerate**.

   The key is then shown on the Private Key area of the screen.

### Regenerating and Viewing 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.

### Regenerating an SSL CSR

**To regenerate 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](#).

The *Components* page displays by default.

2. Click the *Settings* tab.

   The *Upload System License* page displays by default.

3. Click + to the left of *Security* on the left menu.

4. Click *SSL CSR* from the submenu.

   The *SSL CSR* page displays.

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
Appendix C. Security

- 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](#).

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 **Regenerate**.

   **Note** Click **Reset** to reload any previously saved field information.

   Your SSL CSR is generated based on the SSL Private Key you entered during [Importing an SSL Private Key](#) or [Regenerating an SSL Private Key](#).

**Viewing an SSL CSR**

**To view 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](#).

   The *Components* page displays by default.

2. Click the **Settings** tab.

   The *Upload System License* page displays by default.

3. Click ☀ to the left of **Security** on the left menu.

4. Click **SSL CSR** from the submenu.

   The **SSL CSR** page displays.
5. View the lower portion of the screen labeled CSR as desired.

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: *.example.com or *.portal.example.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 some 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, your Vidyo server 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. Your Vidyo server 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 pages. For more information, see Deploying Your Server Certificate, Deploying Your Server CA Certificates (Intermediates), and Importing Security Settings from the Advanced Tab.
Bundles (.p7b, .pfx, and .vidyo) are imported and exported (only .vidyo files can be exported) from the Advanced Tab. For more information, see Importing Security Settings from the Advanced Tab.

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 the Network Settings at the System Console.

If you 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.
   The Components page displays by default.
2. Click the Settings tab.
   The Upload System License page displays by default.
3. Click to the left of Security on the left menu.
4. Click Server Certificate from the submenu.
The *Server Certificate* page displays.

5. Click **Upload**.
The Select Server Certificate pop-up displays.

6. Click the Select File icon.

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 pop-up displays.

   The page 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.

- 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.

   The Components page displays by default.

2. Click the Settings tab.

   The Upload System License page displays by default.

3. Click ☐ to the left of Security on the left menu.
4. Click **Server CA Certificates** from the submenu. The **Server CA Certificates** page displays.

5. Click **Upload**. The **Select Server CA Certificate** pop-up displays.

6. Click the **Select File** icon.

7. 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**.
Appendix C. Security

**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* pop-up displays.

The page then loads the Certificate Information, Issuer, Subject, and the Certificates in the screen.

### Configuring HTTPS Port Settings on Your Applications

**Note** The *Applications* page is also used for Management Interface settings. For more information, see 5. Configuring RADIUS.

### 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](#).

   The *Components* page displays by default.

2. Click the *Settings* tab.
   
   The *Upload System License* page displays by default.

3. Click ![left menu](#) to the left of *Security* on the left menu.

4. Click *Applications* from the submenu.
The *Applications* page displays.

![Security Settings Table](image)

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 Security Settings from the Advanced Tab

The *Advanced* page is used to upload trusted Client Root CA Certificates. This includes all Intermediate and Root Certificates.

You can import from `.p7b` and `.pfx` standard formats. In addition, the `.vidyo` bundle format is available for importing certificates from other Vidyo servers.

**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 page.

To upload security settings 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](#).
The Components page displays by default.

2. Click the Settings tab.

The Upload System License page displays by default.

3. Click + to the left of Security on the left menu.

4. Click Advanced from the submenu.

The Advanced page displays.

5. Click Import Security Bundle (.pfx, .p7b).

The Select bundle (PKCS 7, PKCS 12) pop-up displays.

6. Click the Select File ( ) icon to locate the bundle file.
7. Enter the password if using the .pfx format.

8. Click **Upload** to upload the bundle file.
   If the upload is successful, the *File Upload Success* pop-up displays.

---

**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 into your Vidyo Server.

---

**Enabling SSL and HTTPS Only**

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](#).

Do not use the **Enable SSL** button and **HTTPS Only** checkbox 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 with SSL and HTTPS](#).

**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](#).
   The *Components* page displays by default.

2. Click the **Settings** tab.
   The *Upload System License* page displays by default.

3. Click **to the left of Security** on the left menu.

4. Click **Advanced** from the submenu.
   The *Advanced* page displays.

5. Click **Enable SSL** at the top of the page.
   A *Confirmation* pop-up displays.

6. Click **Yes** to confirm that you want to enable SSL.
   A *Success* pop-up displays.

7. Click **OK**.
   You can now browse your VidyoConferencing system over HTTPS.
Appendix C. Security

8. Browse to any of your Admin portals 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., \texttt{https://[FQDN]}). Verify that HTTPS displays on the left side of the address bar and that a lock icon displays (typically in the lower right corner). Some browsers emphasize an HTTPS session with a color like green or blue.

\textbf{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 additional information.

If your browser generates a root certificate error, first check that your operating system has the latest root certificates update applied.

9. Continue with the next procedure if you are successful browsing to your Admin pages using HTTPS and you do not receive any browser errors.

\textbf{Note} If you are unable to connect to your Admin pages over HTTPS, see \textit{Enabling HTTPS Only}.

\section*{Enabling HTTPS Only}

Before you Enable HTTPS Only, you must configure your components to work with HTTPS. For more information, see \textit{Configuring Your Components to Work with HTTPS}.

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.

\textbf{To enable HTTPS Only:}

\begin{enumerate}
\item Log in to the Super Admin portal using your Super Admin account.
    For more information, see \textit{Logging in to the Super Admin Portal}.
    The \textit{Components} page displays by default.
\item Click the \textit{Settings} tab.
    The \textit{Upload System License} page displays by default.
\item Click $\mathds{1}$ to the left of \textit{Security} on the left menu.
\item Click \textit{Advanced} from the submenu.
    The \textit{Advanced} page displays.
\item Select the \textbf{HTTPS Only} checkbox at the top of the page.
    A \textit{Confirmation} pop-up displays.
\item Click \textbf{Yes} to confirm that you want to enable HTTPS only.
\end{enumerate}
Appendix C. Security

A Success pop-up displays.

7. Click OK.

A Confirmation pop-up displays indicating that your “SSL settings have been reset. Do you want to reboot the server now?”

8. 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 checkbox is selected, which confirms that your SSL and HTTPS implementation is successful.

- When the Disable http to https redirect checkbox is checked, redirecting from http to https is disabled.

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.

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

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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click ☀ to the left of Security on the left menu.

4. Click Advanced from the submenu.
   The Advanced page displays.

5. Click Import Trusted CA Certificates.
   The Select file pop-up displays.

6. 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 the Select File icon 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.

![Select File dialog box]

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 pop-up displays indicating that your “Upload successful. Do you want to reboot the server now?”

9. Click Yes.

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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click to the left of Security on the left menu.

4. Click Advanced from the submenu.
   The Advanced page displays.

5. Click Export Security Bundle.
Appendix C. Security

The Export Bundle pop-up displays.

6. Enter a password in the Password field to encrypt the security bundle.
7. Re-enter the password in the Confirm Password field to confirm.
8. Click Export.
   
   Your browser then downloads the 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.
   
   The Components page displays by default.
2. Click the Settings tab.
   
   The Upload System License page displays by default.
3. Click ☃ to the left of Security on the left menu.
4. Click Advanced from the submenu.
   
   The Advanced page displays.
5. Click Reset Security.
   
   A confirmation pop-up displays.
6. Click Yes.
   
   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 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.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click to the left of Security on the left menu.

4. Click Advanced from the submenu.
   The Advanced page displays.

5. Click Enable Default Trusted CA Bundle.
   The Enable Default Trusted CA Bundle pop-up displays.

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 Server and Changing the Default Password.

Configuring Your Components to Work with HTTPS

After implementing SSL and enabling HTTPS on your Vidyo server, 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
2. Setting the FQDN on Your VidyoRouter Configuration Pages
3. Setting the FQDN on Your Tenants

## 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.

## Setting the FQDN on Your VidyoRouter Configuration Pages

The FQDN on your VidyoRouter is set up using the following procedure.

**To set the FQDN on your VidyoRouter Configuration pages:**

1. Log in to your VidyoRouter using your System Console account.

---

**Note** The URL of your VidyoRouter is typically a domain name: `http://[IP or FQDN address]/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 Server and Changing the Default Password.

Although the default username for this page is admin, only the Super Admin accesses these pages.

The VidyoRouter Configuration Pages display.

2. Set the Configuration Server to a valid FQDN of the VidyoPortal on the Basic tab as defined by the applied certificate.
Note  The best practice is to provide a full URL for your Config Server value beginning with \texttt{https://}, using your IP or FQDN address, and even a port reference if desired.

3. Click \textit{Apply}.
4. Click \textit{OK} to restart the VidyoRouter.
5. Proceed and set the FQDN on your tenants.

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 \texttt{Logging in to the Super Admin Portal}.
   
   The \textit{Components} page displays by default.

2. Click the \textit{Tenants} tab.
   
   The \textit{Tenants} page displays.

3. Ensure that each Tenant (including the Default Tenant) is using a valid FQDN for the Tenant URL as defined by the certificate applied.
   
   For more information, see \texttt{Adding a Default Tenant or Adding a New Tenant}.

Configuring Each VidyoPortal Component to Use Your FQDN

You must now 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 VidyoRouter Component Configuration

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](#).

The *Components* page displays by default.

2. Double-click the **Name** link on the VidyoRouter row.
   The *VidyoRouter* pop-up displays.

3. Do the following in the *SCIP* section:
   a. Edit the **FDQN** field (VidyoRouter signaling address) by clicking the text.
b. Edit the Port field by clicking the text.

4. Click Save.
5. 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.
   The Components tab is selected by default.
2. Verify that all components are Online (Status UP) and have no alarms.

   ![Component screenshot]

3. Login to a User portal and place test calls to verify that the VidyoPortal and components are functional.

   **Note** If your system includes VidyoRouters, see [Accessing Your VidyoRouter Configuration Page](#).

   For enabling HTTPS on your VidyoGateway and VidyoReplay, refer to respective security sections in the *VidyoGateway* and *VidyoReplay Administrator Guides* available from the Vidyo Support Center at [http://support.vidyo.com](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 contains 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 your VidyoRoom systems. 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](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://[IP or FQDN address]

2. Go to the Tools menu in Firefox once the page loads 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. Select X.509 Certificate with chain (PEM) from the Save as Type drop-down.

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.

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 and Configuring Each VidyoPortal Component to Use Your FQDN 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.
   The Components page displays by default.

2. Click the Settings tab. The Upload System License page displays by default.

3. Scroll down to the Encryption line in the System License information section.

If Encryption is enabled in the VidyoPortal License, the setting reads 128 Bits, otherwise it shows Disable.
Enabling Encryption on the VidyoConferencing System

Before enabling the encryption 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 enabling Encryption by clicking the Enable Encryption button.

- For more information, see Implementing Encryption Using the Secured VidyoConferencing Option.

- Enabling encryption enables it for full signaling and media security on the VidyoRouter, VidyoManager, and VidyoPortal. For using encryption (referred to as the Secured VidyoConferencing Option) with VidyoGateway and VidyoReplay, refer to respective security sections in the 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. Click the Configuration icon in the VidyoDesktop client, and select the Status tab.

If you have a secure connection, refer to "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 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 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** page enables you to grant permission via the access password and host IP or hostname for the cdraccess user.

![CDR Access Page](image)

**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](#).

**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 displays 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](#) and [Exporting CDR Files from the Admin Portal](#).
## CDR Version2.1 Tables

### ClientInstallations2

This table is used to record software installation.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Login Name of the user installing client software</td>
</tr>
<tr>
<td>DisplayName</td>
<td>Display name</td>
</tr>
<tr>
<td>TenantName</td>
<td>The Endpoint ID of a user’s host machine</td>
</tr>
<tr>
<td>EID</td>
<td>Endpoint identifier of a user’s host machine</td>
</tr>
<tr>
<td>ipAddress</td>
<td>IP address of machine where client software is installed</td>
</tr>
<tr>
<td>HostName</td>
<td>Host name of machine where client software is installed</td>
</tr>
<tr>
<td>RoomName</td>
<td>This field is populated for guest users and indicates which room they were trying to join that started the client software installation</td>
</tr>
<tr>
<td>RoomOwner</td>
<td>Room owner</td>
</tr>
<tr>
<td>TimeInstalled</td>
<td>Time of installation</td>
</tr>
</tbody>
</table>

### ConferenceCall2

**Note**  Refer to this table when working with exported CDR file data.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallID</td>
<td>Auto increment</td>
</tr>
<tr>
<td>UniqueCallID</td>
<td>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.</td>
</tr>
<tr>
<td>ConferenceName</td>
<td>Name of the conference</td>
</tr>
<tr>
<td>TenantName</td>
<td>Name of the Tenant</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConferenceType</td>
<td>D – Direct Call (two party)</td>
</tr>
<tr>
<td></td>
<td>C – Conference Call</td>
</tr>
<tr>
<td></td>
<td>ID – Inter-portal Direct Call</td>
</tr>
<tr>
<td></td>
<td>IC – Inter-portal Conference Call</td>
</tr>
<tr>
<td>EndpointType</td>
<td>R – VidyoRoom</td>
</tr>
<tr>
<td></td>
<td>D – VidyoDesktop</td>
</tr>
<tr>
<td></td>
<td>G – Guest</td>
</tr>
<tr>
<td></td>
<td>L – Call to Legacy via VidyoGateway</td>
</tr>
<tr>
<td></td>
<td>C – Call Recorded via VidyoReplay and Recorder (if applicable)</td>
</tr>
<tr>
<td>CallerID</td>
<td>Caller identifier [Login name of the caller]</td>
</tr>
<tr>
<td></td>
<td>For Legacy Calls, this is the extension number used.</td>
</tr>
<tr>
<td>CallerName</td>
<td>Display Name of the Caller or name of the legacy device</td>
</tr>
<tr>
<td>JoinTime</td>
<td>Join time</td>
</tr>
<tr>
<td>LeaveTime</td>
<td>Leave time</td>
</tr>
<tr>
<td>Call State</td>
<td>Current state of the call:</td>
</tr>
<tr>
<td></td>
<td><strong>RINGING</strong> – The status of the side initiating the call (P2P or conference).</td>
</tr>
<tr>
<td></td>
<td><strong>RING ACCEPTED</strong> – This status indicates to the initiating side that the</td>
</tr>
<tr>
<td></td>
<td>callee has accepted the call. It will switch to “in progress” once the</td>
</tr>
<tr>
<td></td>
<td>conference begins.</td>
</tr>
<tr>
<td></td>
<td><strong>RING REJECTED</strong> – This status indicates to the initiating side that the</td>
</tr>
<tr>
<td></td>
<td>alert was not accepted.</td>
</tr>
<tr>
<td></td>
<td><strong>RING NO ANSWER</strong> – This status indicates to the initiating side that the</td>
</tr>
<tr>
<td></td>
<td>call timed out.</td>
</tr>
<tr>
<td></td>
<td><strong>RING CANCELLED</strong> – This status indicates to the initiating side that the</td>
</tr>
<tr>
<td></td>
<td>call was aborted from the initiating side.</td>
</tr>
<tr>
<td></td>
<td><strong>ALERTING</strong> – The status indicates to the callee side that there is an</td>
</tr>
<tr>
<td></td>
<td>incoming call (P2P or conference).</td>
</tr>
<tr>
<td></td>
<td><strong>ALERT CANCELLED</strong> – This status indicates to the callee side that the</td>
</tr>
<tr>
<td></td>
<td>initiating side cancelled the call.</td>
</tr>
<tr>
<td></td>
<td><strong>IN PROGRESS</strong> – This status indicates to both sides that the call is in</td>
</tr>
<tr>
<td></td>
<td>progress.</td>
</tr>
<tr>
<td></td>
<td><strong>COMPLETED</strong> – This status indicates to both sides that the call was</td>
</tr>
<tr>
<td></td>
<td>completed.</td>
</tr>
<tr>
<td>Direction</td>
<td>I – Inbound Call</td>
</tr>
<tr>
<td></td>
<td>O – Outbound Call</td>
</tr>
</tbody>
</table>

396
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RouterID</td>
<td>VidyoRouter used for this call.</td>
</tr>
<tr>
<td>GwPrefix</td>
<td>Service prefix used. This applies only to calls that involve a VidyoGateway or VidyoRecorder. For other calls, it is set to NULL.</td>
</tr>
<tr>
<td>GwID</td>
<td>Gateway ID used for this call. Set to NULL otherwise.</td>
</tr>
<tr>
<td>ReferenceNumber</td>
<td>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.</td>
</tr>
</tbody>
</table>
| ApplicationName    | This field identifies VidyoConference usage from different endpoint types. The information is reported by endpoints when connecting to the VidyoPortal. Usage is reported from the following endpoint types:  
  - 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         | **U** – Registered User  
  **G** – Guest  
  **L** – Call to Legacy via VidyoGateway  
  **R** – Call Recorded via VidyoReplay and Recorder (if applicable) |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RoomType</td>
<td>M – Private room belonging to a registered member on the VidyoPortal</td>
</tr>
<tr>
<td></td>
<td>P – Public room</td>
</tr>
<tr>
<td></td>
<td>S – Scheduled room</td>
</tr>
<tr>
<td>RoomOwner</td>
<td>The logged in username of the room owner.</td>
</tr>
<tr>
<td>ApplicationOS*</td>
<td>This field identifies the operating system on which a Vidyo client is</td>
</tr>
<tr>
<td></td>
<td>running. All VidyoClients (and Client lib based apps) are required to</td>
</tr>
<tr>
<td></td>
<td>provide this information if requested. The following operating systems are</td>
</tr>
<tr>
<td></td>
<td>supported:</td>
</tr>
<tr>
<td></td>
<td>- Windows XP</td>
</tr>
<tr>
<td></td>
<td>- Windows7</td>
</tr>
<tr>
<td></td>
<td>- Windows8</td>
</tr>
<tr>
<td></td>
<td>- Mac OS</td>
</tr>
<tr>
<td></td>
<td>- Linux</td>
</tr>
<tr>
<td></td>
<td>- iOS</td>
</tr>
<tr>
<td></td>
<td>- Android</td>
</tr>
<tr>
<td>CallCompletionCode</td>
<td>This field provides one of the following call completion codes:</td>
</tr>
<tr>
<td></td>
<td>0 – The call completion reason is not available.</td>
</tr>
<tr>
<td></td>
<td>1 – The user disconnected the call.</td>
</tr>
<tr>
<td></td>
<td>2 – The call was disconnected by the admin, operator, or room owner.</td>
</tr>
<tr>
<td></td>
<td>3 – The call was disconnected due to a network failure on the VidyoManager.</td>
</tr>
<tr>
<td>EndpointGUID</td>
<td>This field captures the endpoint's GUID in the conference.</td>
</tr>
</tbody>
</table>

**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.

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 setup 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 9. Using the VidyoPortal and VidyoRouter Virtual Editions (VE).

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.
Appendix E. Hot Standby

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 prior to 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 Appendix D. CDR.
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.

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 at the System Console.

**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 that 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 and write down specific IP address and FQDN values that you designated 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 Your Vidyo Licenses and Applying the System License Keys to Your System.

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.
Appendix E. Hot Standby

To verify correct installation of VidyoPortal licenses with the Hot Standby option:

1. Open a new System Console for VP1 using the Native IP or FQDN address.

   ![System Console Menu]

   - 1. Configure IP Address
   - 2. Configure DNS Nameserver
   - 3. Configure NTP Time Servers
   - 4. Configure Time Zone
   - 5. Configure Network 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
     a. .. (more options)
     x. Exit System Administrator Console

   ![System Administrator Console]

   17. Configure Adobe Connect plugin
   18. Display System ID
   H. Hot Standby
   b. ... (back to previous menu)

   **Selection:**

2. Enter `m` for more options.

3. Press the **Enter** key.

   ![System Administrator Console]

   **Selection:**

---

**Note** System Console menu options are not case sensitive.

4. Verify that the **H. Hot Standby** option displays in the menu.
   
   If it does, the license for your Hot Standby option is applied correctly on VP1.
   
   If desired, you may leave the VP1 System Console open.
Appendix E. Hot Standby

**Note** If you do not see the **H. Hot Standby** option, review the steps for applying system license keys. For more information, see [Requesting Your Vidyo Licenses](#) and [Applying the System License Keys to Your System](#).

---

**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 or FQDN address you designated for VP.
  2. Enter `m` for more options.
  3. Press the **Enter** key.

  The software version is shown in red at the top of the System Console.

  ![System Administrator Console](image)

  4. Confirm that both of your machines are running the same software version.

     If desired, you may leave the VP1 System Console open.

     - Back up and download the database on the machine you’re using as VP1. For more information, see [Performing System Maintenance](#).

**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 that 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 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 that 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 Addresses section of the Configuring the Network Settings at the System Console.

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. 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 and VP2.

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 or FQDN address.
   
   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.
Note  Press the Enter key after each prompt.

2. Enter m for more options.

Note  System Console menu options are not case sensitive.
3. Enter **H** to select the Hot Standby option.

4. Enter **A** to select the Show Configuration option.

   The *Hot Standby Status* screen displays.

5. Enter **y** to confirm changes to current settings.
The *New Configuration* screen displays.

![New Configuration Screen](image)

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](#), 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.

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 at the System Console.

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.

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 or FQDN address you designated for VP.

2. Enter 14 to reboot the 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 or FQDN address.
   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

   **Note** You must use the Cluster IP or FQDN address 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.

2. Verify that the appropriate Vidyo components and licenses display.
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
2. Rebooting to Apply the New Hot Standby Configuration Values on VP1
   After rebooting VP2, the machine will be in Standby mode.
3. Do the following:
   a. Generate and import the security keys on VP1 and VP2.
      For more information, see Generating and Importing the Security Keys.
   b. Perform a database synchronization on VP1.
      For more information, see Triggering the First Database Synchronization from VP1.
   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 or Forcing a Hot Standby from the System Console on Your Active VidyoPortal.
Note If you put your Standby VidyoPortal in to Maintenance mode, the Settings > Hot Standby screens do not display when accessed via the Internet Explorer Web browser.

4. Verify your VP1 functionality.
   See Verifying VP1 Functionality.

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 from the Super Admin Portal or from the System Console using Forcing a Hot Standby from the System Console on Your Active VidyoPortal.

   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

   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.

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 or FQDN address you designated for VP1.

   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

Note Press the Enter key after each prompt.

Note You must use the Cluster IP or FQDN address to access the Active Vidyo Portal. Its Active status disables the native IP address.

   Refer to the specific IP address and FQDN values that you designated for your VP1, VP2, and Cluster in the Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.
2. Enter m for more options.

3. Enter H to select the Hot Standby option.

**Note** Even though the H. Hot Standby option may not display on the main menu, you can still select it.

4. Enter F to select the Node Synchronization option.

The Node Synchronization Menu displays.

5. Enter A to select the Generate/Show Security Key option.

6. Enter y to confirm the key generation.
Appendix E. Hot Standby

The system generates a security key for VP2.

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 the Enter key to stop viewing the key.

9. Enter x to exit the VP1 System Console.

10. Open a new (or return to an already open) System Console for VP2 using the native IP or FQDN address you designated for VP2.

For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.
11. Enter m for more options.

12. Enter H to select the Hot Standby option.

**Note** Even though the H. Hot Standby option may not display on the main menu, you can still select it.

13. Enter F to select the Node Synchronization option.

14. Enter B to import security key from peer.
15. Paste the key (generated from VP1) here on VP2.

16. Enter **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. Enter **A** to select the Generate/Show Security Key option.

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 or FQDN address you designated for VP1.

For more information, see [Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster](#).
20. Enter menu choices **m > H > F** to access VP1’s Node Synchronization Menu.

21. Enter **B** to 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. Enter **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 or FQDN address.

   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

   Note Press the Enter key after each prompt.

2. Enter D from the System Console Node Synchronization menu on VP1 to validate the security key.

   The message Validating security...[Success] displays 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 or FQDN address.

   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

5. Enter m > H > F from the main menu to access VP2’s Node Synchronization Menu.

6. Enter D to validate the security key.
The message Validating security...[Success] displays 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 or FQDN address.
   
   For more information, see [Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster](#).

   **Note** Press the **Enter** key after each prompt.

2. Enter `m > H > F` from the main menu to access VP1’s Node Synchronization Menu.

3. Enter `C` from the Node Synchronization Menu to 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 or FQDN address.
   
   For more information, see [Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster](#).

   **Note** Press the **Enter** key after each prompt.

2. Enter `m > H` from the main menu to access VP1’s Hot Standby Menu.

3. Enter `D` to 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. Enter x to exit the VP1 System Console.

5. Open a new (or return to an already open) System Console for VP2 using the Native IP or FQDN address.
   
   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

6. Enter m > H from the main menu to access VP2's Hot Standby Menu.

7. Enter D to 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. Enter x to exit the VP2 System Console.

**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 Triggering the First Database Synchronization from VP1.

**To check the status of the Hot Standby configuration:**

1. Access the Super Admin portal of the Active VidyoPortal using the Cluster IP or FQDN address.
   
   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.
The *Components* page displays by default.

2. Click the *Settings* tab.
   
The *Upload System License* page displays by default.

3. Click ☐ to the left of *Hot Standby* on the left menu.
4. Click *Status* from the submenu.
   
The *Status* page displays.

**Note**  The following screenshot does not actually show the database synchronization taking place.

![Vidyo Portal Status Page](image)

The Status table displays. This is a read-only table that contains the following Hot Standby information:

- **Current Role** – UNKNOWN displays if the VidyoPortal is in Maintenance mode; otherwise, ACTIVE displays.
- **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 displays if the VidyoPortal is reachable; UNKNOWN displays 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.)
- **Peer Status** – The status (either ONLINE or OFFLINE) of the partner VidyoPortal.
- **Peer Server IP** – The configured IP address of the peer VidyoPortal.
Database Synchronization – The state of the database synchronization. If the standby server database is not in-sync, the number of minutes behind will be displayed. If the database is unable to be synchronized, the Super Admin will be prompted to click a button to replicate the database. If there is a connectivity issue, a descriptive message displays.

Note If the Super Admin initiates a database replication, the database may be offline for a few seconds.

Statues generally correspond to the ones shown when using the System Console during Verifying the Node Status on VP1 and VP2.

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

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.

If you put your Standby VidyoPortal in to Maintenance mode, the Settings > Hot Standby screens do not display when accessed via the Internet Explorer Web browser.

To force the Active VidyoPortal into Standby mode from the Super Admin portal:

1. Access the Super Admin portal of your Active VidyoPortal using the Cluster IP or FQDN address.
   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.
   The Components page displays by default.

2. Click the Settings tab.
   The Upload System License page displays by default.

3. Click to the left of Hot Standby on the left menu.
4. Click *Status* from the submenu.

5. Click *Force Standby*.

   A *Confirmation* pop-up displays.

6. 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**” displays, and you are unable to force the currently Active VidyoPortal into Standby mode.
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.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Email or Emails Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active VidyoPortal switches over to Standby VidyoPortal</td>
<td>Two emails:</td>
</tr>
<tr>
<td></td>
<td>□ [VidyoPortal] is now the ACTIVE node.</td>
</tr>
<tr>
<td></td>
<td>□ Standby Node is ONLINE.</td>
</tr>
<tr>
<td>Active VidyoPortal switches over to Maintenance mode and Standby</td>
<td>Two emails:</td>
</tr>
<tr>
<td>VidyoPortal takes over</td>
<td>□ [VidyoPortal] is now the ACTIVE node.</td>
</tr>
<tr>
<td></td>
<td>□ Standby Node is OFFLINE.</td>
</tr>
<tr>
<td>VidyoPortal switches from Maintenance mode to Standby</td>
<td>Standby Node is ONLINE.</td>
</tr>
<tr>
<td>VidyoPortal switches from Maintenance mode to Active without Standby</td>
<td>Two emails:</td>
</tr>
<tr>
<td></td>
<td>□ [VidyoPortal] is now the ACTIVE node.</td>
</tr>
<tr>
<td></td>
<td>□ Standby Node is OFFLINE.</td>
</tr>
<tr>
<td>Standby VidyoPortal reboots</td>
<td>Two emails:</td>
</tr>
<tr>
<td></td>
<td>□ Standby Node OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>□ Standby Node ONLINE. (This email is</td>
</tr>
<tr>
<td></td>
<td>sent when it comes back online.)</td>
</tr>
<tr>
<td>Standby VidyoPortal IP connectivity was lost and restored</td>
<td>Two emails:</td>
</tr>
<tr>
<td></td>
<td>□ Standby Node OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>□ Standby Node ONLINE. (This email is</td>
</tr>
<tr>
<td></td>
<td>sent when it comes back online.)</td>
</tr>
</tbody>
</table>

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
Appendix E. Hot Standby

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 that you designated for your VP1, VP2, and Cluster in the Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

Switching to Maintenance Mode and Upgrading Your Standby VidyoPortal

If you put your Standby VidyoPortal into Maintenance mode, the Settings > Hot Standby screens do not display 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 or FQDN address.

   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

   **Note** Press the Enter key after each prompt.

2. Put the Standby VidyoPortal into Maintenance mode using the following steps:
   a. Enter m > H from the main menu to access the Standby VidyoPortal’s Hot Standby Menu.
   b. Enter C to select the Maintenance Mode option.
   c. Enter y to confirm putting your Standby VidyoPortal into Maintenance mode.
Alternatively, you can put the Standby VidyoPortal into Maintenance mode via the Super Admin Portal by navigating to Settings > Hot Standby > Status, clicking Switch to Maintenance, and then clicking Yes in the confirmation pop-up that displays.

3. Upgrade the Standby VidyoPortal as described in the Upgrading Your VidyoPortal System Software.

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 or FQDN address.

For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

**Note**  
Press the Enter key after each prompt.

5. Take the Standby VidyoPortal out of Maintenance mode using the following steps:
   
a. Enter m > H from the main menu to access the Standby VidyoPortal’s Hot Standby Menu.

b. Enter C to select the Maintenance Mode option.

c. Enter 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 or FQDN address.

   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

**Note**  
Press the Enter key after each prompt.

2. Force a Hot Standby using the following steps:

   a. Select m > H from the main menu to access the Standby VidyoPortal’s Hot Standby Menu.

   b. Enter E to select the Force Standby option.
c. Enter **y** to confirm forcing your Active VidyoPortal into Standby mode.

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 from the Super Admin Portal](#).

---

3. 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](#) 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 or FQDN address to put your Standby VidyoPortal into Maintenance mode.

   For more information, see [Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster](#).

---

**Note**  Press the **Enter** key after each prompt.
Appendix E. Hot Standby

a. Select $m > H$ from the main menu to access the Standby VidyoPortal’s Hot Standby Menu.

b. Enter $C$ to select the Maintenance Mode option.

c. Enter $y$ to confirm putting your Standby VidyoPortal into Maintenance mode.

2. Open a new System Console and access the Active VidyoPortal using the Native IP or FQDN address to put your Active VidyoPortal into Maintenance mode.

   For more information, see Preparing Specific IP and FQDN Values for Your VP1, VP2, and Cluster.

   a. From the main menu, select $m > H$ to access the Active VidyoPortal’s Hot Standby Menu.

   b. Enter $C$ to select the Maintenance Mode option.

   c. Enter $y$ to confirm putting your Standby VidyoPortal into Maintenance mode.

   Both of your VidyoPortals should now be offline and in Maintenance Mode.

3. Upgrade both VidyoPortals as described in the Performing System Maintenance.
After the upgrades are complete and the servers are restarted, return the VidyoPortal that was originally your Active VidyoPortal using the Native IP or FQDN address.

4. 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. Select `m > H` from the main menu to access the Standby VidyoPortal’s Hot Standby Menu.
   b. Enter `C` to select the Maintenance Mode option.
   c. Enter `y` to confirm putting your VidyoPortal back into Active mode.

      Return the VidyoPortal that was originally your Standby VidyoPortal using the Native IP or FQDN address.

5. Put this machine in to Standby mode using the following steps:

   **Note**  The second VidyoPortal server that you take out of Maintenance Mode becomes the Standby VidyoPortal just by removing it from Maintenance Mode.

   a. Enter `m > H` from the main menu to access the Standby VidyoPortal’s Hot Standby Menu.
   b. Enter `C` to select the Maintenance Mode option.
   6. Enter `y` to confirm putting your VidyoPortal back into Standby mode.
Appendix F. Vidyo Support

The Vidyo Customer Support team has a two-stage authentication process that enables them to remotely SSH into the VidyoGateway for troubleshooting purposes. The authentication flow requires the system administrator and Vidyo Customer Support to collaborate in order to create a one-time temporary password for SSH.

Enabling Vidyo Support

To enable Vidyo Support:

1. Log in to the System Console.
   For more information, see [Logging in to the System Console of Your Server and Changing the Default Password](#).

Note Press the Enter key after each prompt.

2. Enter m for more options.
3. Enter S to select the Vidyo Support option.
4. Enter y to generate a new token for remote support access.
Appendix F. Vidyo Support

5. Copy and paste the encrypted one-time password and send it to Vidyo’s Support team.

Disabling Vidyo Support

To disable Vidyo Support:

1. Log in to the System Console.
   For more information, see Logging in to the System Console of Your Server and Changing the Default Password.

   **Note** Press the Enter key after each prompt.

2. Enter m for more options.

3. Enter S to select the Vidyo Support option.

4. Enter n to generate a new token for remote support access.
   A message indicates that remote access is disabled.

5. Press any key to return to the menu.
Appendix G. 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 25°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 40°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.

<table>
<thead>
<tr>
<th>Product</th>
<th>Part Number</th>
<th>MTBF</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD-3</td>
<td>PKG-RM-HD3-NTPM-GROUP, PKG-RM-HD3-GROUP, DEV-RM-HD3-SA, DEV-RM-HD3-NTPM-SA</td>
<td>179,500 hours</td>
</tr>
<tr>
<td>HD-40B</td>
<td>DEV-RM-HD40-B-SA-0A</td>
<td>66,640 hours</td>
</tr>
<tr>
<td>HD-40C</td>
<td>DEV-RM-HD40-C-SA-0A</td>
<td>61,825 hours</td>
</tr>
<tr>
<td>Product</td>
<td>Part Number</td>
<td>MTBF</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>HD-100D</td>
<td>DEV-RM-HD100-D9020-SA-0A &amp; DEV-RM-HD100-D-NTPM-SA-0A</td>
<td>75,400 hours</td>
</tr>
<tr>
<td>HD-230</td>
<td>DEV-RM-HD230-NTPM-SA-0A &amp; DEV-RM-HD230-SA-0A</td>
<td>80,520 hours</td>
</tr>
<tr>
<td>VidyoGateway</td>
<td>DEV-SRV-GW-N2-0B</td>
<td>29,900 hours</td>
</tr>
<tr>
<td>VidyoGateway XL</td>
<td>DEV-SRV-GW-XL-N3-0A</td>
<td>121,400 hours</td>
</tr>
<tr>
<td>VidyoH20 for Google+ Hangouts</td>
<td>DEV-SRV-H20-XL-N3-0A</td>
<td>121,400 hours</td>
</tr>
<tr>
<td>VidyoOne</td>
<td>DEV-SRV-ONE-N2-0B</td>
<td>29,900 hours</td>
</tr>
<tr>
<td>VidyoPanorama 600</td>
<td>DEV-SRV-PAN600-N2-0A</td>
<td>109,186 hours</td>
</tr>
<tr>
<td>VidyoPortal</td>
<td>DEV-SRV-PT-N2-0B</td>
<td>29,900 hours</td>
</tr>
<tr>
<td>VidyoPortal XL</td>
<td>DEV-SRV-PT-XL-N3-0A</td>
<td>116,700 hours</td>
</tr>
<tr>
<td>VidyoReplay</td>
<td>DEV-SRV-REP-N3-0A</td>
<td>116,700 hours</td>
</tr>
<tr>
<td>VidyoRouter</td>
<td>DEV-SRV-RTR-N2-0B</td>
<td>29,900 hours</td>
</tr>
<tr>
<td>VidyoRouter XL</td>
<td>DEV-SRV-RTR-XL-N3-0A</td>
<td>103,600 hours</td>
</tr>
</tbody>
</table>
Appendix H. 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:
   
a. You must give any other recipients of the Work or Derivative Works a copy of this License; and
   
b. You must cause any modified files to carry prominent notices stating that You changed the files; and
   
c. 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
   
d. 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 display. 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.

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 display 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” display 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 Ssleay License

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, Lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT 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:

- it must be made available under this Agreement; and
- a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. Commercial Distribution

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively “Losses”) arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor’s responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. No Warranty

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. Disclaimer Of Liability

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. 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 “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.
A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

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.


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:
Appendix H. Licensing

i) 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.

ii) Accompany the Combined Work with a copy of the GNU GPL and this license document.

iii) 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.

iv) Do one of the following:
   
   (1) 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.

   (2) 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.

   (3) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)


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.
Appendix H. Licensing

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU General Public License

Version 3, 29 June 2007Copyright © 2007 Free Software Foundation, Inc. (http://fsf.org/)

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too,
receive or can get the source code. And you must show them these terms so they know their rights.

 Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

 For the developers’ and authors’ protection, the GPL clearly explains that there is no warranty for this free software. For both users’ and authors’ sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

 Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users’ freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

 Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

 The precise terms and conditions for copying, distribution and modification follow.

 TERMS AND CONDITIONS

 a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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”.
Appendix H. Licensing

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.

g. 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.

h. 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.
Appendix H. Licensing

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.

i. 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.

j. 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.

k. 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
Appendix H. Licensing

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.

I. 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.

m. 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.

n. 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.

o. 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.

p. 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.

q. 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.

r. 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:
Appendix H. Licensing

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.
Appendix H. Licensing

- 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.

467
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
Appendix H. Licensing

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.