VidyoGateway™

Administrator Guide

Product Version 3.5.2

Document Version A

October, 2017

TABLE OF CONTENTS

Overview 1

Conventions Used in This Guide 1

1. VidyoGateway Server Models and Capacities.. 2

Identifying Your VidyoGateway Model 2

Capacity of the VidyoGateway Models 3

Maximum Number Concurrent Calls of the Same Type 3

Maximum Number Concurrent Calls of Different Types 4

Maximum Number Concurrent Calls of Different Types and Resolutions 4

Discontinued VidyoGateway Model Capacities 5

VidyoGateway Physical Setup Guidelines 5

2. Understanding the VidyoGateway Configuration Procedure 6

Making Configurations on Your VidyoGateway 6

Making Configurations on Your VidyoPortal for Your VidyoGateway 6

Making Additional VidyoGateway Configurations 7

3. Configuring Your Server via the System Console 8

Logging in to the System Console and Changing the Default Password 9

Viewing Application and System Information 10

Viewing Application Information 10

Viewing System Information 12

Setting the Hostname and the Domain 14

Configuring the Production Interface 17

Viewing the Production Interface Active Information 17

Configuring the IPv4 Production Interface 19

Configuring IPv4 Static Routes 29

Configuring the IPv6 Production Interface 35

Configuring the MTU and Auto Negotiation for the Production Interface 44

Configuring the Management Interface 49

Viewing the Management Interface Active Information 49

Configuring the IPv4 Management Interface 51

Configuring IPv4 Static Routes 57

Configuring the MTU and Auto Negotiation for the Management Interface 62

Configuring Time Servers (NTP) 68

Configuring Users 69

TABLE OF CONTENTS

Viewing Active User Information 69
Adding Users 71
Removing Users....75
Changing User Passwords....78
Configuring RADIUS Authentication....81
Accessing Tools....81
Performing Advanced Configuration....83
Configuring FIPS....83
Maintaining Pre-shared Keys 85
Running the Recovery Utility....97
Configuring SNMP 110
Configuring SSH 157
Managing Static Hosts 159
Configuring Remote Vidyo Support Access 168
Rebooting the System Console....173
Shutting Down the System Console....174
Logging in to the Admin Portal....175
Setting the Language for the VidyoGateway Admin Pages 177
4. Configuring RADIUS 178
Viewing the Current RADIUS Configuration 178
Configuring RADIUS 180
Adding Additional Servers 183
Creating a RADIUS-Enabled Account....186
Viewing a RADIUS-Enabled Account 189
Removing a RADIUS-Enabled Account 189
Disabling RADIUS Authentication 189
Enabling FIPS Mode 192
Disabling FIPS Mode 194
5. Configuring Your System 197
Configuring the General Settings 197
Configuring the VidyoPortal Settings....197
Configuring SIP Settings....199
Configuring H.323 Settings 202

TABLE OF CONTENTS

Configuring Audio Settings....205
Configuring Video Loopback Settings....206
Configuring Quality of Service (QoS) Settings....207
Configuring Prompts and Call Control via DTMF Tones....209
Configuring Advanced Settings....211
Configuring Access Control Settings....215
Understanding VidyoGateway Clusters....218
Clustering Benefits....219
Cluster Configuration with a Legacy Gatekeeper Interface....219
Deploying Multiple VidyoGateway Clusters....220
Configuring Clusters....221
Understanding the Clustering Procedure....222
Returning a Repaired Controller to Your System Setup....222
Replacing an Irreparable Controller to Your System Setup....222
Configuring Your Standalone VidyoGateway....223
Configuring Controller 1....224
Configuring Nodes for the Active Controller in Cluster Mode....226
Configuring Controller 2....231
Configuring Your Cluster Node....233
Managing Services....234
Adding a Service....234
Activating and Deactivating Services....240
Deleting a Service....242
Editing a Service....242
Understanding Call Types and Service Examples....244
H.323 Outgoing Call Examples....244
H.323 Incoming Call Examples....245
SIP Incoming Call Using a Prefix Example....245
SIP Incoming URI Dialing Example....246
Dialing from a Legacy H.323 Endpoint into a Vidyo PIN-Protected Room....247
TCS4 Delimiters....247
Configuring Integrated Voice Response (IVR) Settings....248
Enabling Your IVR Settings....248
Configuring General IVR Settings....249
Configuring Appearance IVR Settings....251

TABLE OF CONTENTS

Configuring VidyoGateway IVR Screen Instruction Settings 255
Configuring VidyoGateway IVR Screen Prompt Settings 259
Importing and Exporting VidyoGateway IVR Media and Prompt Settings 262
Enabling and Disabling VidyoGateway IVR Settings 263
Checking the Status of Your VidyoGateway 264
Viewing Call Statistics 265
Capturing Application Logs 267
Diagnostics 269
Downloading Application Logs 269
Running Diagnostic Logs 271
Viewing Diagnostic Logs 272
Downloading Diagnostic Logs 273
Configuring a Public IP Address and Viewing Your VidyoGateway Network Settings 274
Configuring a Public IP Address 274
Viewing Your VidyoGateway Network Settings 276
Understanding VidyoGateway Security 277
Securing Your VidyoGateway System with SSL and HTTPS 278
Importing, Exporting, and Regenerating an SSL Private Key 278
Generating and Viewing an SSL CSR 281
Certificates Received from Your Certificate Authority 284
Uploading or Editing Your Server Certificate 286
Configuring HTTPS Port Settings for Your Admin Pages 288
Importing Client Root CA Certificates from the Advanced Tab 289
Enabling HTTPS on Your Vidyo Server 294
Configuring Your Vidyo Server's Management Interface and Port 296
Configuring OCSP 298
Enabling OCSP from the VidyoGateway 298
Disabling OCSP from the VidyoGateway 299
Disabling OCSP from the System Console 300
Upgrading Your VidyoGateway 303
Shutting Down or Rebooting Your VidyoGateway 304
Extending Your VidyoGateway Session 305
Logging Out of Your VidyoGateway 305
6. Auditing 307

TABLE OF CONTENTS

Downloading Audit Logs from Your VidyoGateway....307
Understanding Audit Log Content....308
Content Captured in the Audit Log....308
Sample Audit Log Content....309
7. Integrating VoIP Phones and IP PBXs....310
Network Topology....311
Connecting to VidyoConferences from VoIP Phones....311
Connecting to VidyoConferences Via an IP PBX....312
8. Integrating Direct Phone Calls with IVR Functionality....313
Phone Setups Using the IVR Functionality....313
9. Using VidyoGateway Virtual Edition (VE)....314
Understanding VidyoGateway VE Requirements....314
Virtual Machine Provisioning Requirements....315
Example Configurations....316
Understanding VidyoGateway VE Support of VMware Features....317
Installing VidyoGateway VE....317
Appendix A. Definitions....326
Appendix B. Legacy TCS4 Delimiters....329
Appendix C. Deployment Examples....330
Appendix D. NAT/Firewall Traversal....333
Appendix E. Reliability....338
Limitations of Reliability Prediction Models....338
General Prediction Methodology....338
Electronic Equipment Procedure....338
Component Parameters and Assumptions....339
Supplier MTBF Data....339
Subsystem MTBF Data Release Policy....339
MTBF Reliability....339

Overview

The VidyoGateway is a 1U rack-mountable server that connects VidyoPortal™ users with users on systems using the SIP and H.323 videoconferencing protocols. The systems that use these protocols are referred to as Legacy systems.

This document describes how to use the VidyoGateway to connect with a VidyoConferencing™ system that includes Legacy systems. It is written for system administrators who must set up and maintain a VidyoConferencing system.

The VidyoGateway is also available as the VidyoGateway Virtual Edition, and can be run as a virtual appliance. For more information, see 9. Using VidyoGateway Virtual Edition (VE).

Note To perform the setup and configuration described in this manual, you must have Admin access to your VidyoGateway and Super Admin access to your VidyoPortal.

Terms used in this guide are defined in a separate section. For more information, see Appendix A. Definitions. For more standard VidyoConferencing definitions, refer to the *VidyoConferencing Administrator Guide*.

Conventions Used in This Guide

- 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*.

1. VidyoGateway Server Models and Capacities

Identifying Your VidyoGateway Model

VidyoGateway is available in Standard and XL platforms. The previously offered VidyoGateway MKII has been discontinued and replaced with the VidyoGateway XL model. The XL model is a higher capacity, more powerful system for more demanding applications.

For more information, refer to the *Vidyo Server Installation Guide*.

The current VidyoGateway looks like the following:

The discontinued VidyoGateway MKII looks like the following:

You can identify your VidyoGateway model by checking the hardware:

- Current VidyoGateway hardware version numbers contain 31230 or 5645 combinations
- Current VidyoGateway hardware labels contain an 02-0A combination
- Previous VidyoGateway hardware labels contain 00-0A, 01-0B or 01-0A combinations

Starting with software version 2.1.3.22, you can also identify your model by looking at the top of the *VidyoGateway Configuration Page*. The model information is shown as follows:

- Model: VidyoGateway, VidyoGateway XL, or VidyoGateway MKII
- Software version: x.x.x.xxx
- Hardware Version: xxxxxxx

Capacity of the VidyoGateway Models

The following tables show the maximum number of concurrent calls allowable for different scenarios including calls of the same type, different types, and different types and resolutions. All capacity data is based on software version 2.1.3.22 and later.

Maximum Number Concurrent Calls of the Same Type

Capacity	VidyoGateway	VidyoGateway	VidyoGateway MKII	VidyoGateway	VidyoGateway XL
Hardware Label	xxxx-00-0A xxxx-01-0A xxxx-01-0B	xxxx-00-0A xxxx-01-0A xxxx-01-0B	xxxx-MKII 00-0A xxxx-MKII-01-0A	xxxx-02-0A	xxxx-02-0A
Status	Previous model	Previous model	Previous model	Current model	Current model
H.235 Encryption	Off	On	On/Off	On/Off	On/Off
HD 1080P Calls, 30 fps	N/A	N/A	N/A	N/A	2
HD 720P Calls, 30 fps @ 1 Mbps	1	1	3	1	5
SD Calls @ 512 Kbps	4	3	12	4	15
CIF Calls @ 384 Kbps	12	9	24	12	25
Voice Calls	50	50	50	50	50

Maximum Number Concurrent Calls of Different Types

The following list shows the maximum number of concurrent calls of different types and resolutions that the VidyoGateway models can handle with software version 2.1.3.22 and later.

- SD & CIF
  - 1 SD + 9 CIF
  - 2 SD + 6 CIF
  - 3 SD + 3 CIF

Maximum Number Concurrent Calls of Different Types and Resolutions

The following table shows the maximum number of concurrent calls of different types and resolutions that the VidyoGateway XL can handle with software version 2.1.3.22 and later.

HD & SD	HD/SD/CIF	SD & CIF	HD & CIF
1 HD + 12 SD	1 HD + 6 SD + 6 CIF	3 SD + 18 CIF	3 HD + 6 CIF
2 HD + 9 SD	2 HD + 3 SD + 6 CIF	7 SD + 10 CIF	
3 HD + 6 SD	3 HD + 1 SD + 4 CIF		
4 HD + 3 SD			

Note When a Legacy device attempts to join a conference whose VidyoGateway is operating at full capacity, the call fails to connect.

Discontinued VidyoGateway Model Capacities

These tables show the maximum number of calls that the previous VidyoGateway models running 2.1.3.20 or later software version can handle simultaneously when all calls are of the same type and resolution with and without H.235 encryption.

VidyoGateway (previous model)
1 x HD 720p30fps @ 1 Mbps
4 x SD @ 512 Kbps
12 x CIF @ 384 Kbps
50 x voice-only calls

VidyoGateway (previous model) using H.235 Encryption
1 x HD 720p30fps @ 1 Mbps
3 x SD @ 512 Kbps
9 x CIF @ 384 Kbps
50 x voice-only calls

VidyoGateway MK II with or without H.235 Encryption
1 x HD 720p30fps @ 1 Mbps
12 x SD @ 512 Kbps
24 x CIF @ 384 Kbps
50 x voice-only calls

VidyoGateway Physical Setup Guidelines

When physically setting up your VidyoGateway, Vidyo recommends the following guidelines:

- Locate the VidyoGateway as close as possible to your Legacy system(s), preferably on the same LAN.
- If the Legacy systems are in dispersed locations, install the VidyoGateway on the same LAN as your VidyoRouter™.
- If the VidyoGateway is on a QoS network, give high priority to the traffic between the VidyoGateway and the Legacy system(s). Specify lower QoS for traffic between the VidyoGateway and your VidyoRouter.

2. Understanding the VidyoGateway Configuration Procedure

The overall procedure for configuring your VidyoGateway requires cumulative steps performed on both the VidyoPortal and the VidyoGateway as described in the following procedures. Complete all of the following steps on your VidyoGateway and VidyoPortal in the order that they appear.

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

Making Configurations on Your VidyoGateway

To make configurations on your VidyoGateway:

1. Configure your network interface settings in the VidyoReplay 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 Viewing Application and System Information.

2. Secure your VidyoGateway server (if applicable).

   For more information, see Securing Your VidyoGateway System with SSL and HTTPS.

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

   For more information, see Configuring the VidyoPortal Settings.

Making Configurations on Your VidyoPortal for Your VidyoGateway

To make configurations on your VidyoPortal for your VidyoGateway:

1. Add the VidyoGateway as a component to the VidyoConferencing system.

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

For more information, refer to the “Adding a VidyoGateway to Your VidyoPortal” section in the *VidyoConferencing Administrator Guide*.

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

   For more information, refer to “Making the VidyoGateway Components Available” in the *VidyoConferencing Administrator Guide*.

Making Additional VidyoGateway Configurations

Now you can configure additional VidyoGateway features as needed, such as:

- If desired, set up unique service prefixes, or use any of the predefined services.

  For more information, see Managing Services and Understanding Call Types and Service Examples.

- Perform the following configurations as needed:
  - To connect to an NTP server, see Viewing Application and System Information.
  - To upload image files for video loopback, see Configuring Video Loopback Settings.
  - To view the network settings, see Viewing Your VidyoGateway Network Settings.
  - To check the status of your VidyoGateway, see Checking the Status of Your VidyoGateway.
  - To upload a new security certificate, see Uploading or Editing Your Server Certificate.
  - To upgrade your VidyoGateway, see Upgrading Your VidyoGateway.
  - To restart the VidyoGateway, see Shutting Down or Rebooting Your VidyoGateway.

- Create VidyoGateway clusters if desired.

  For information, see Configuring Clusters.

- Integrate VoIP phones and IP PBXs as needed.

  For more information, see 7. Integrating VoIP Phones and IP PBXs, and refer to the Integrating VoIP Phones and IP PBXs with VidyoGateway Vidyo Technical Note.

- For convenient access to Legacy systems (if you have them), add your video device in your directory using *Users > Add Legacy Device* in your VidyoPortal Super Admin portal.

  For more information, refer to the *VidyoConferencing Administrator Guide*.

3. Configuring Your Server via the System Console

Immediately after you have physically installed your Vidyo server as described in the Vidyo Server Installation Guide, you must configure your VidyoGateway 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/.

As you begin the configuration, keep the following deployment guidelines in mind:

- 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. You can restrict Vidyo Customer Support SSH access by configuring your firewall or contact Vidyo Customer Support for other options.
- Restrict access to your VidyoGateway Admin portal by performing one of the following:
  - Block HTTP/HTTPS access from untrusted networks including the Internet.
  - Move the VidyoGateway Admin portal to the Management Interface (if you have not yet configured your Management Interface, it must be configured at this time).

    For more information, see Configuring Your Vidyo Server's Management Interface and Port.
- Change your VidyoGateway System Administrator Console default password. This must be changed after the first log in. For more information, see the following procedure.
- Configure the network settings at the System Console. You can view the settings (read-only) in the VidyoGateway Admin Pages.

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.

Logging in to the System Console and Changing the Default Password

The very first time you log into your VidyoGateway server, you are required to change the default System Console password to one that is more secure. This System Console account is also the same one used when accessing the VidyoGateway Admin Portal.

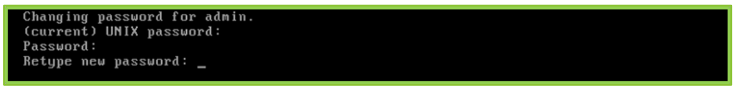
To log in to the System Console (also referred to as the Admin Console) and change the default password:

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

   User Name: **`admin`**

   Password: **`password`** (case sensitive)
3. Enter **`admin`** at the “login” 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.

   ```
   Changing password for admin.
   (current) UNIX password:
   Password:
   Retype new password: _
   ```
5. Type a new password at the “Password” prompt.

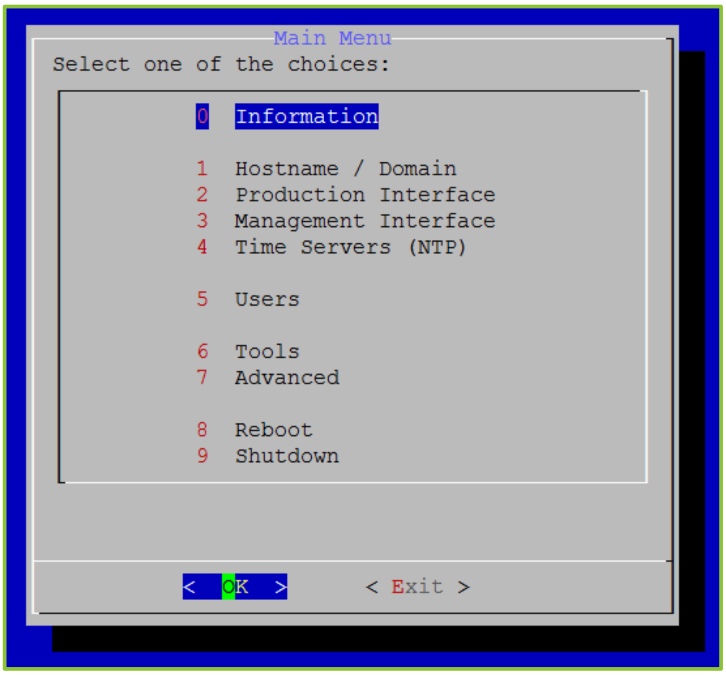
   When selecting a new password, follow these guidelines:

   - The password should not be too similar to the old password.

     The default setting is at least three characters and should be different from the old password.
   - The password should not be too simple or too short.

     The algorithm here is a point system to satisfy the min password length (the default is length 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 only of the old password or should not be the reverse of the old password.
6. Type 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 Main Menu opens immediately.



```
Main Menu
Select one of the choices:

               0  Information

               1  Hostname / Domain
               2  Production Interface
               3  Management Interface
               4  Time Servers (NTP)

               5  Users

               6  Tools
               7  Advanced

               8  Reboot
               9  Shutdown

         <  OK  >      < Exit >
```

Note If you need to reset the password, see Changing User Passwords.

Viewing Application and System Information

You can use the System Console to view which Vidyo applications and versions you have as well as to view the system time and disk space.

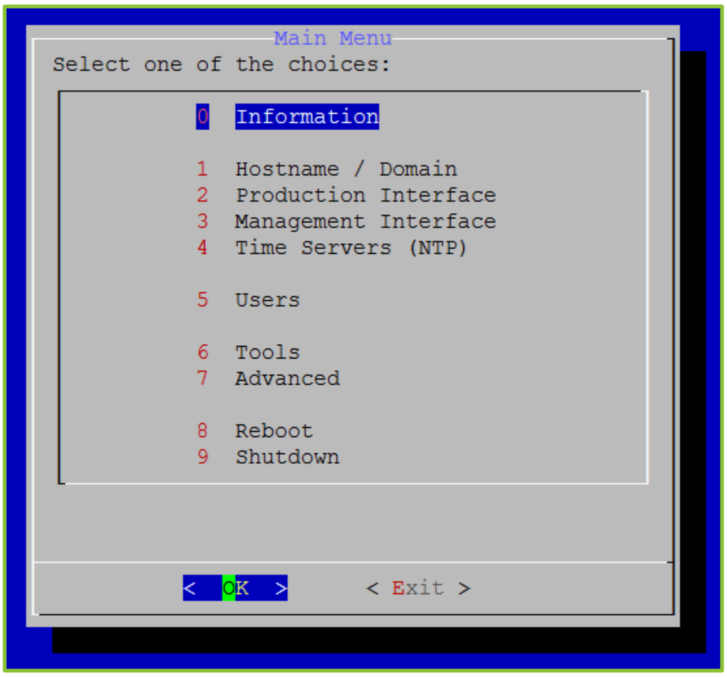
Viewing Application Information

To view application information:

1. Log in to the System Console.

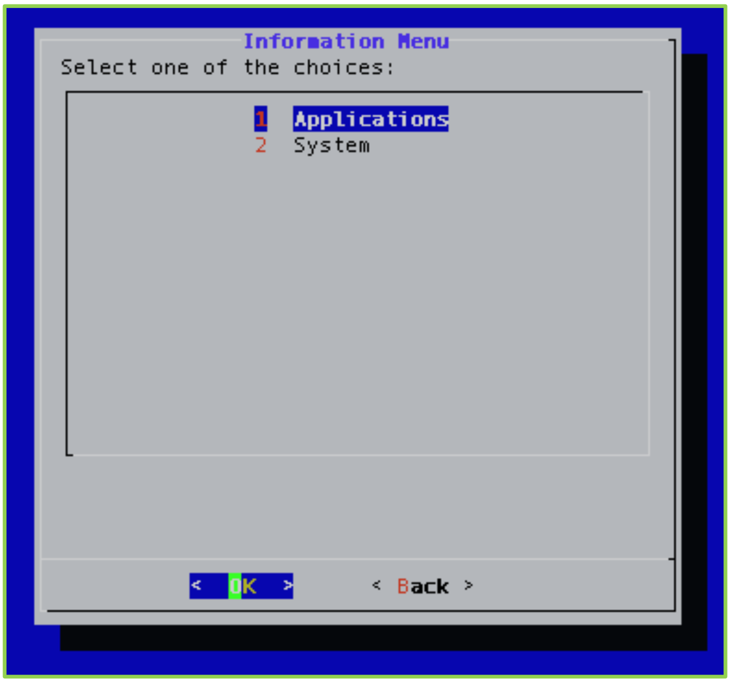
   For more information, see Logging in to the System Console and Changing the Default Password.

The Main Menu displays.



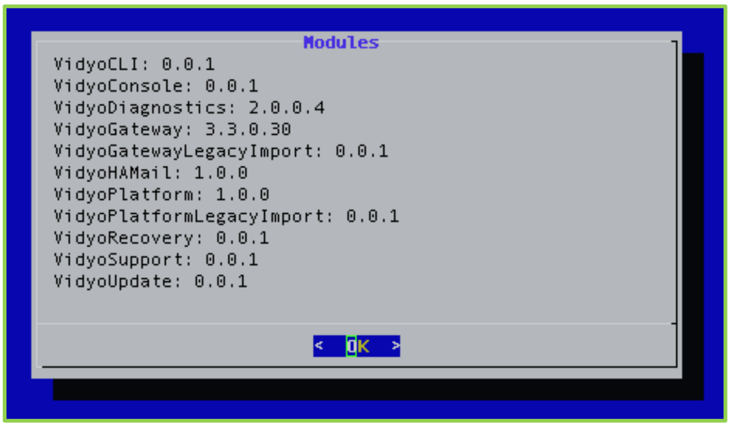
2. Enter **0** to select the Information option.
3. Press the **Enter** key to select **OK**.

The Information Menu displays.



4. Enter **1** to select the Applications option.
5. Press the Enter key to select OK.

   The *Modules* window displays.



```
Modules
VidyoCLI: 0.0.1
VidyoConsole: 0.0.1
VidyoDiagnostics: 2.0.0.4
VidyoGateway: 3.3.0.30
VidyoGatewayLegacyImport: 0.0.1
VidyoHAMail: 1.0.0
VidyoPlatform: 1.0.0
VidyoPlatformLegacyImport: 0.0.1
VidyoRecovery: 0.0.1
VidyoSupport: 0.0.1
VidyoUpdate: 0.0.1
```

This window displays the list of the platform applications and the version number of each one. This information is mostly internal and useful for troubleshooting by the Vidyo Customer Support team.

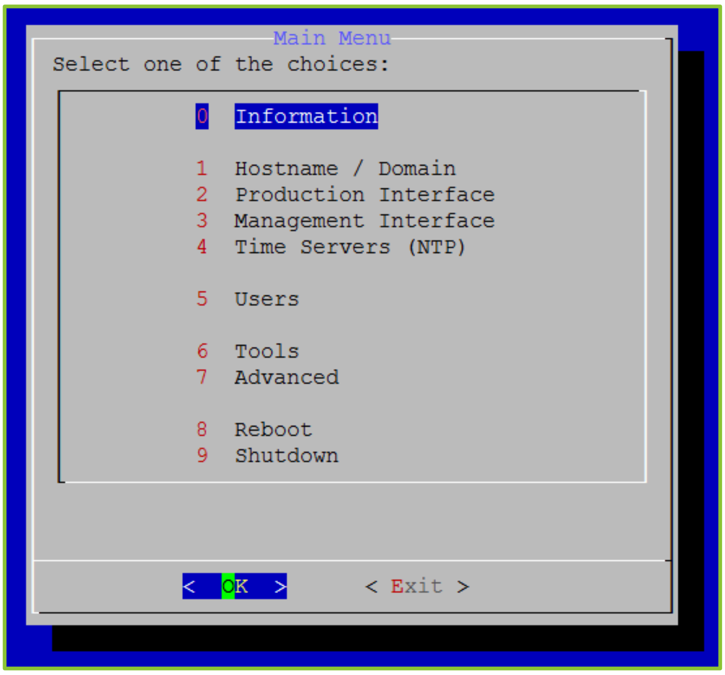
Viewing System Information

To view system information:

1. Log in to the System Console.

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

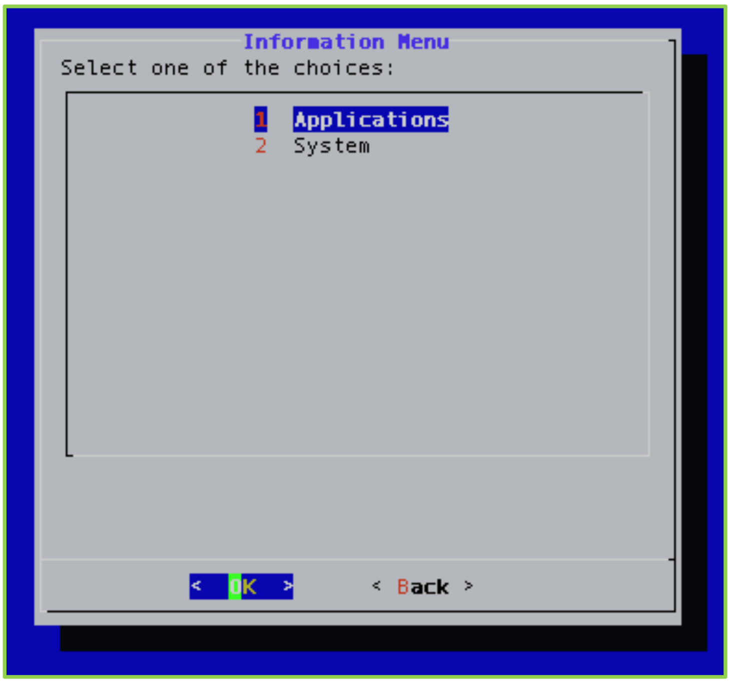
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

     <  OK  >        < Exit >
```

2. Enter **0** to select the Information option.
3. Press the **Enter** key to select **OK**.

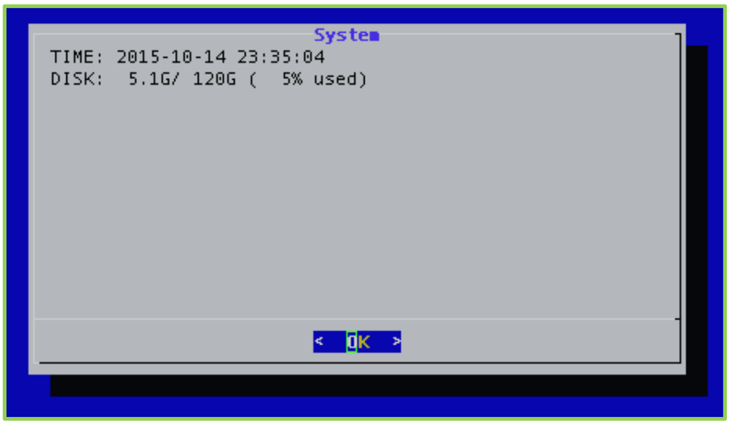
The Information Menu displays.



```
Information Menu
Select one of the choices:

        1  Applications
        2  System

     <  OK  >        < Back >
```

4. Enter **2** to select the System option.
5. Press the **Enter** key to select **OK**.

   The *System* window displays.

   ```
   System
   TIME: 2015-10-14 23:35:04
   DISK:  5.1G/ 120G (  5% used)
   ```

   This window displays the system time, the used disk space, the available disk space, and the percentage used.

Setting the Hostname and the Domain

Your Vidyo server default IP is **192.168.1.110** and should be changed to align with your local area network.

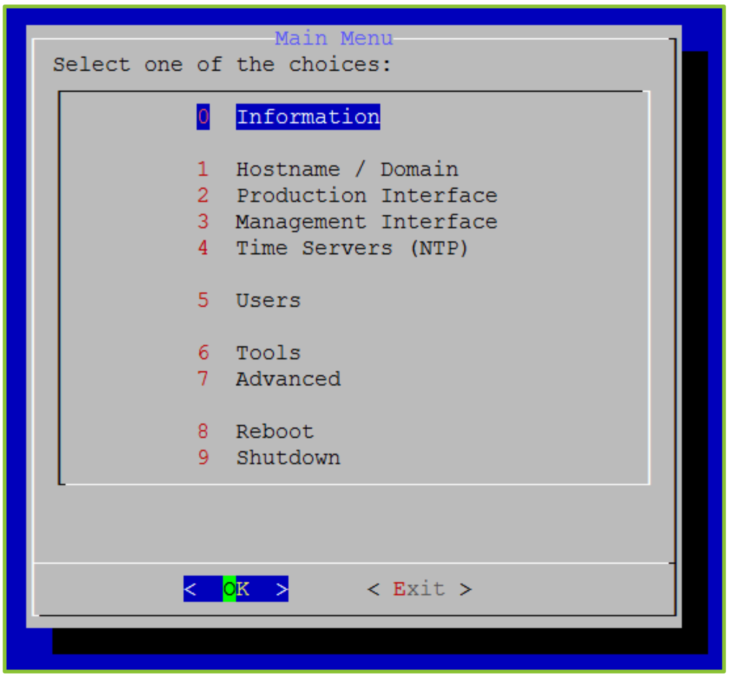
Note A network setup must be performed for each of your Vidyo servers.

To set the hostname and the domain:

1. Log in to the System Console.

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

The Main Menu displays.

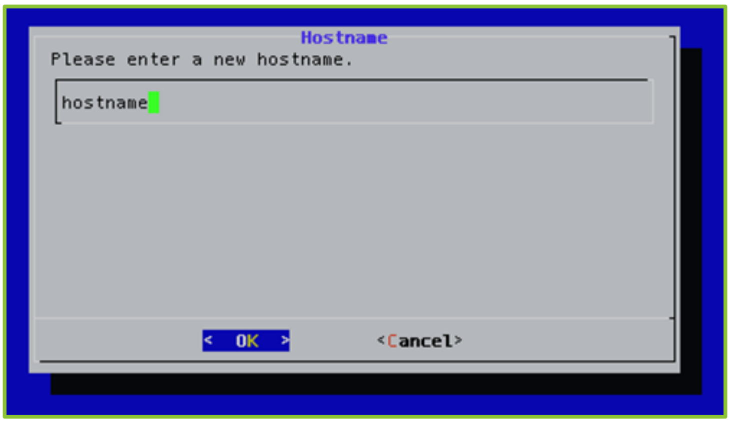


Main Menu

Select one of the choices:

2. Enter **1** to select the Hostname/Domain option.
3. Press the Enter key to select OK.

   The *Hostname* window displays.



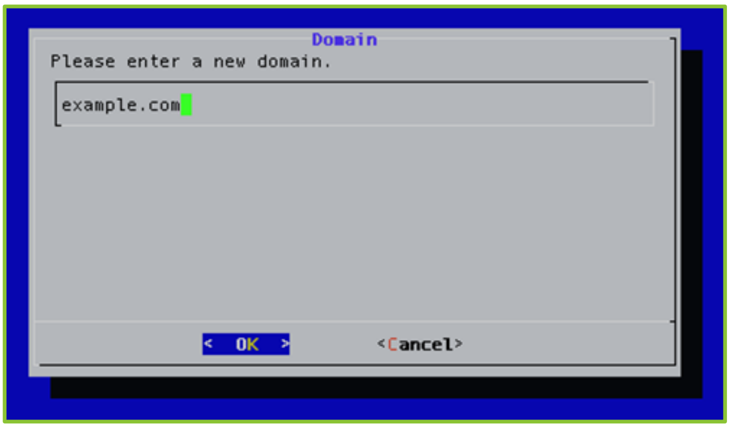
Hostname

Please enter a new hostname.

hostname

4. Enter the hostname.
5. Press the Enter key to select OK.

The *Domain* window displays.

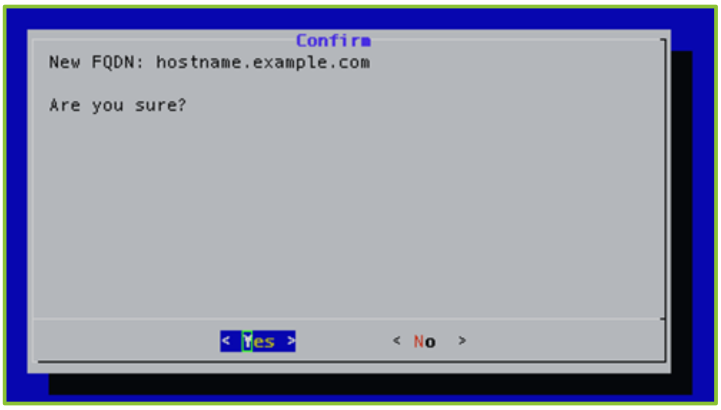

Domain

Please enter a new domain.

example.com

6. Enter the domain.
7. Press the **Enter** key to select **OK**.

   The *Confirm* window displays.

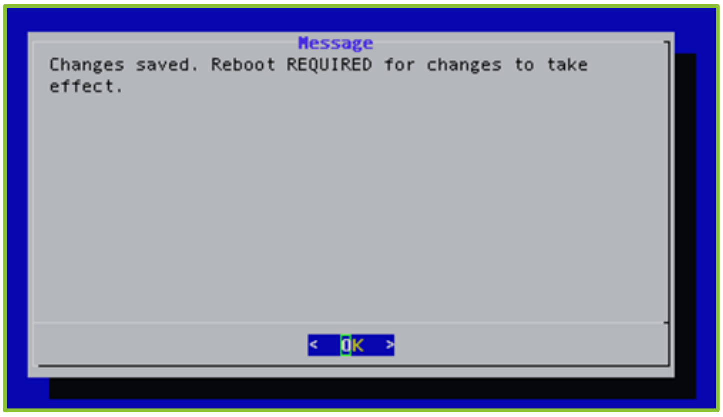

Confirm

New FQDN: hostname.example.com

Are you sure?

8. Press the **Enter** key to select **Yes**.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”


Message

Changes saved. Reboot REQUIRED for changes to take effect.

9. Press the **Enter** key to select **OK**.

Configuring the Production Interface

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 that 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.

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.

Viewing the Production Interface Active Information

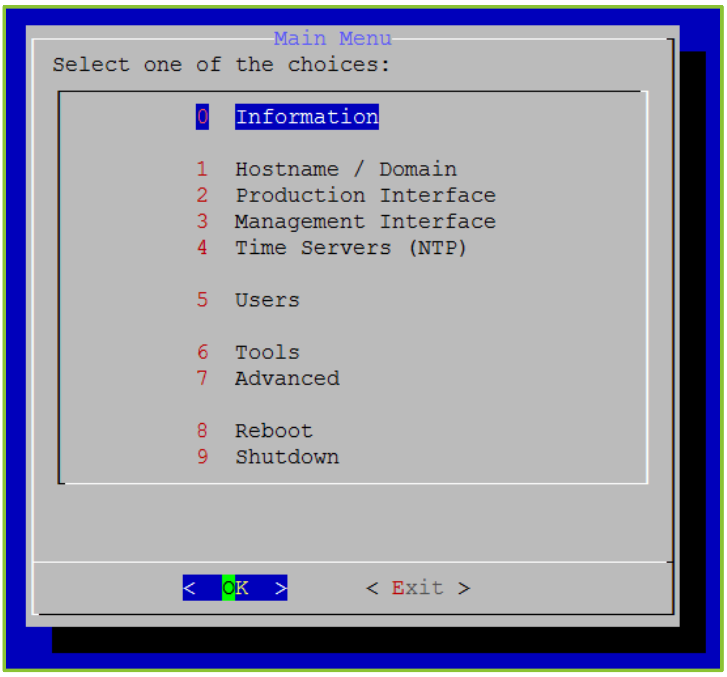
The Production Interface Active Information window provides important information about the Production Interface, such as the currently configured IP address, link status, and duplex settings.

To view the Production Interface active information:

1. Log in to the System Console.

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

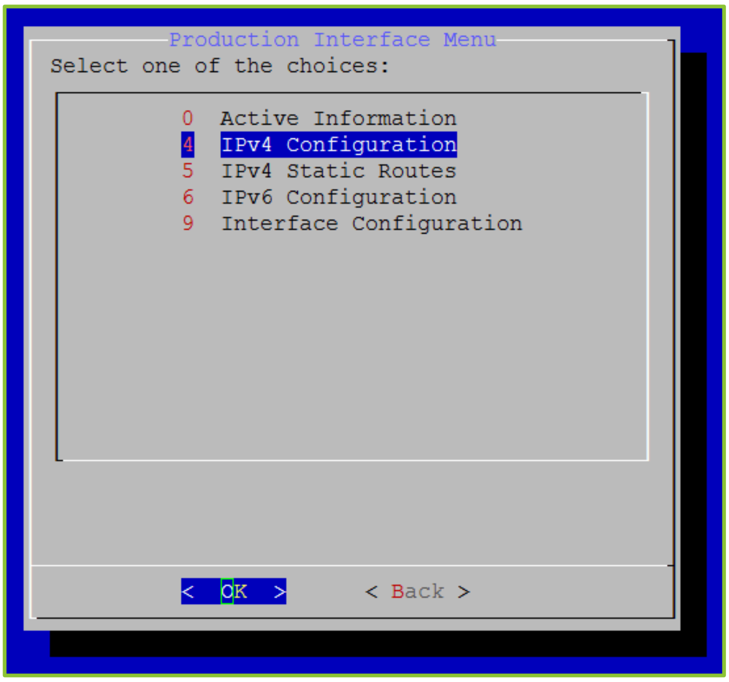
The Main Menu displays.



```
Main Menu
Select one of the choices:

         0  Information

         1  Hostname / Domain
         2  Production Interface
         3  Management Interface
         4  Time Servers (NTP)

         5  Users

         6  Tools
         7  Advanced

         8  Reboot
         9  Shutdown

       <  OK  >       < Exit >
```

2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**.

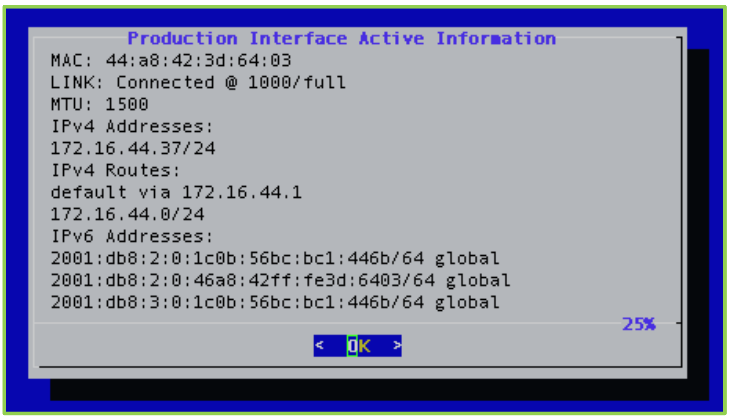
The Production Interface Menu displays.



```
Production Interface Menu
Select one of the choices:

         0  Active Information
         4  IPv4 Configuration
         5  IPv4 Static Routes
         6  IPv6 Configuration
         9  Interface Configuration

       <  OK  >       < Back >
```

4. Enter **0** to select the Active Information option.
5. Press the **Enter** key to select **OK**.

   The *Product Interface Active Information* window displays.



```
Production Interface Active Information
MAC: 44:a8:42:3d:64:03
LINK: Connected @ 1000/full
MTU: 1500
IPv4 Addresses:
172.16.44.37/24
IPv4 Routes:
default via 172.16.44.1
172.16.44.0/24
IPv6 Addresses:
2001:db8:2:0:1c0b:56bc:bc1:446b/64 global
2001:db8:2:0:46a8:42ff:fe3d:6403/64 global
2001:db8:3:0:1c0b:56bc:bc1:446b/64 global
```

Configuring the IPv4 Production Interface

This section describes how to manually enable and disable the IPv4 Production Interface, how to configure IPv4 static and dynamic routes, and how to add and remove static routes.

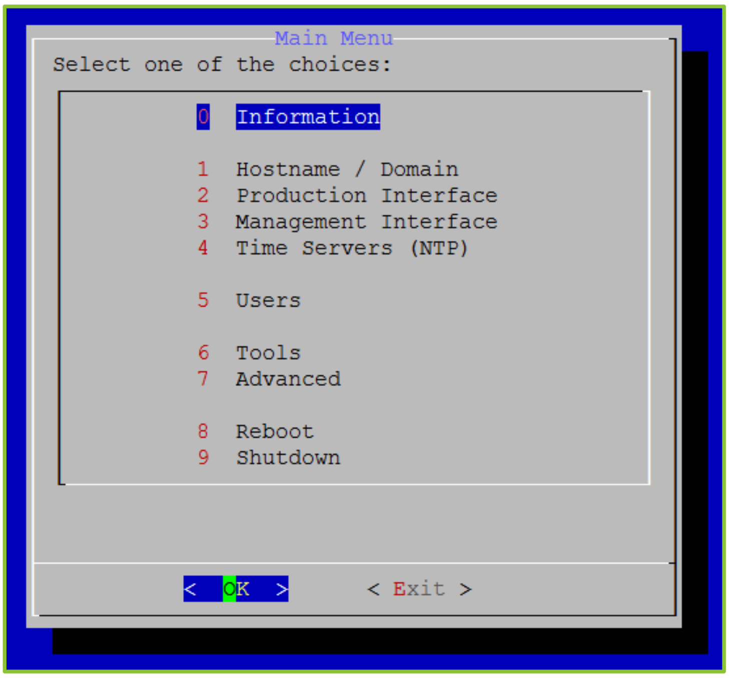
Manually Disabling and Enabling the IPv4 Production Interface

To manually disable or enable the IPv4 Production Interface:

1. Log in to the System Console.

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

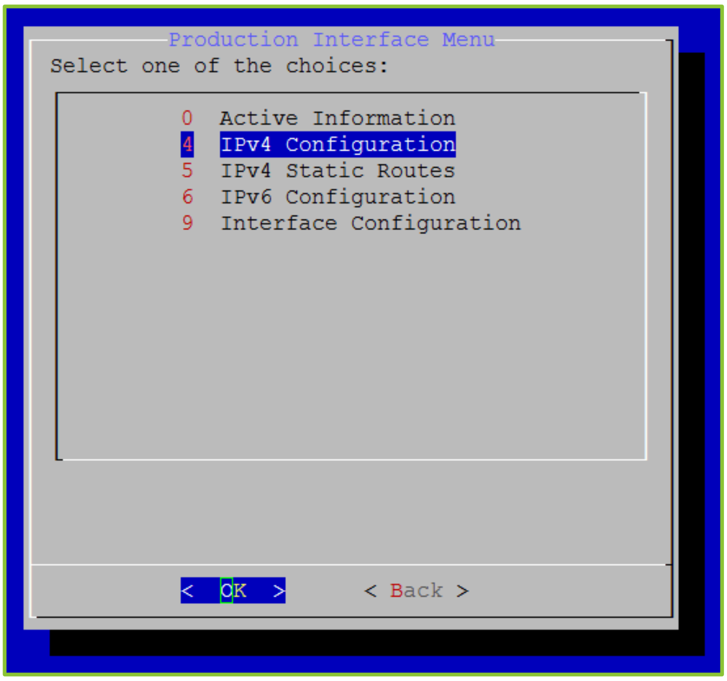
The Main Menu displays.



```
                 Main Menu
Select one of the choices:

           0  Information

           1  Hostname / Domain
           2  Production Interface
           3  Management Interface
           4  Time Servers (NTP)

           5  Users

           6  Tools
           7  Advanced

           8  Reboot
           9  Shutdown


          <  OK  >      < Exit >
```

2. Enter **2** to select the Production Interface option.
3. Press the Enter key to select OK.

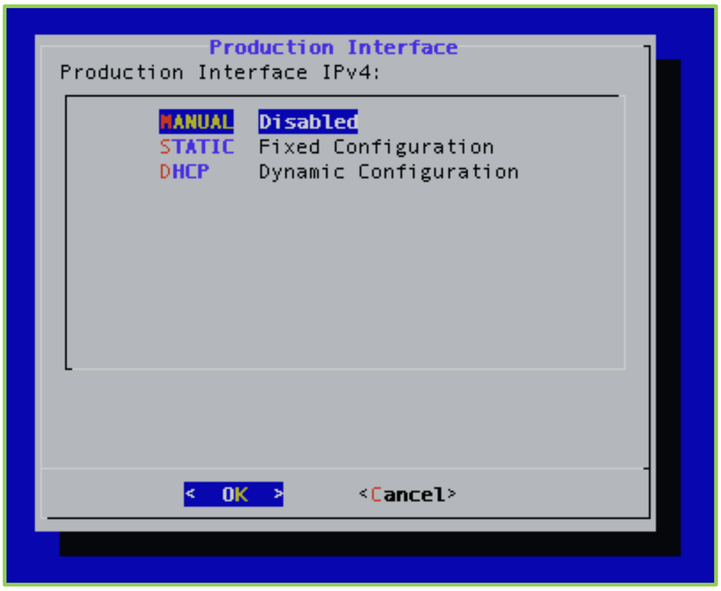
The Production Interface Menu displays.



```
Production Interface Menu
Select one of the choices:

        0  Active Information
        4  IPv4 Configuration
        5  IPv4 Static Routes
        6  IPv6 Configuration
        9  Interface Configuration

        <  OK  >        < Back >
```

4. Enter **4** to select the IPv4 Configuration option.

5. Press the Enter key to select OK.

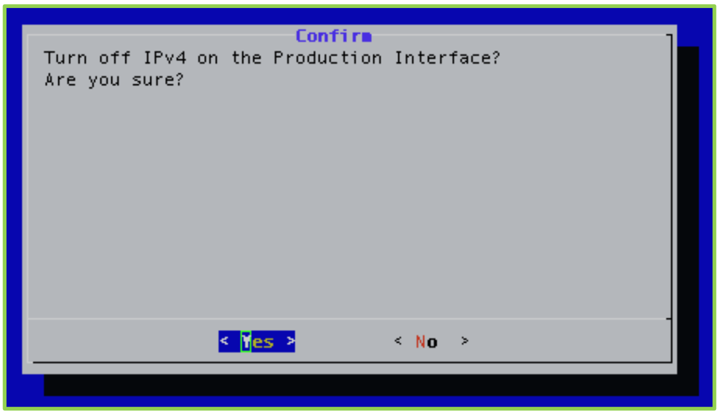


```
Production Interface
Production Interface IPv4:

        MANUAL   Disabled
        STATIC   Fixed Configuration
        DHCP     Dynamic Configuration

        <  OK  >       <Cancel>
```

6. Enter **M** to select the MANUAL option.

7. Press the Enter key to select OK.

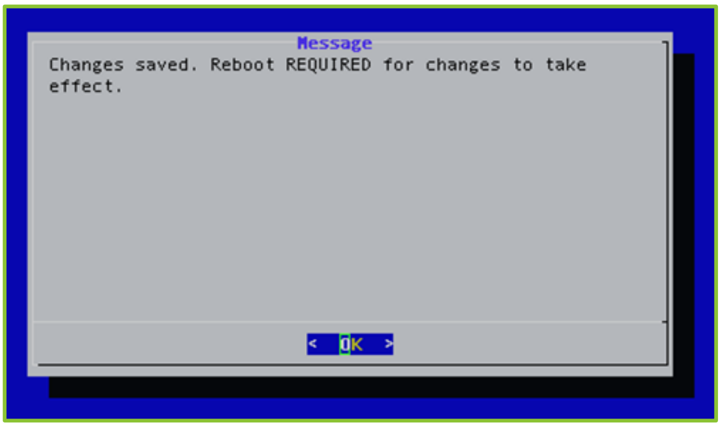
If the current state of the Production Interface is enabled, you are asked to confirm if you want to disable it. If the current state of the Production Interface is disabled, you are asked to confirm if you want to enable it.



```
Turn off IPv4 on the Production Interface?
Are you sure?
```

8. Press the Enter key to select Yes.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”



```
Changes saved. Reboot REQUIRED for changes to take
effect.
```

9. Press the Enter key to select OK.

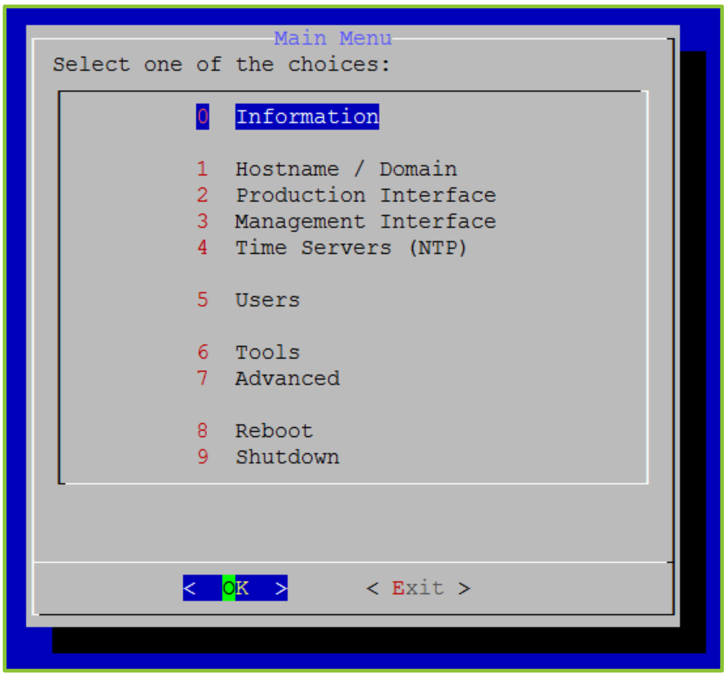
Configuring an IPv4 Static Production Interface

To configure an IPv4 Production Interface:

1. Log in to the System Console.

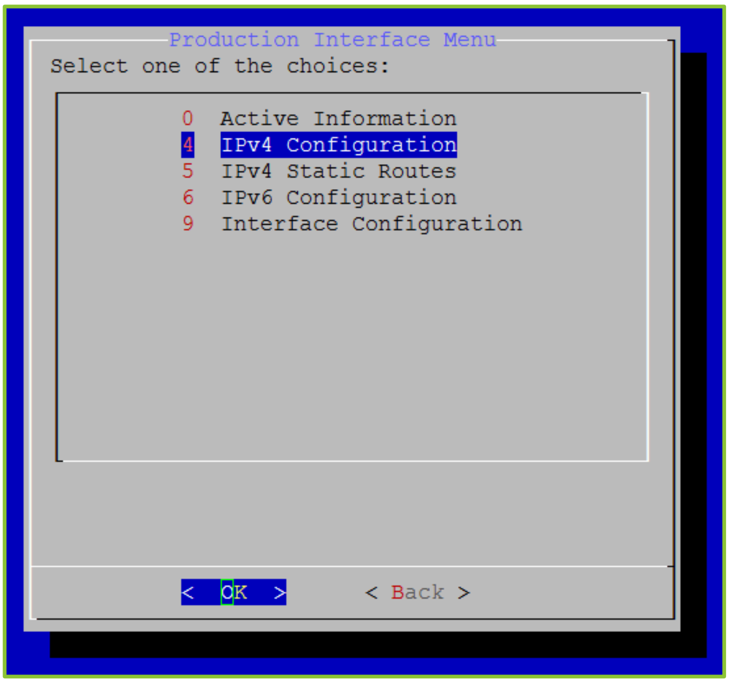
   For more information, see Logging in to the System Console and Changing the Default Password.

The Main Menu displays.

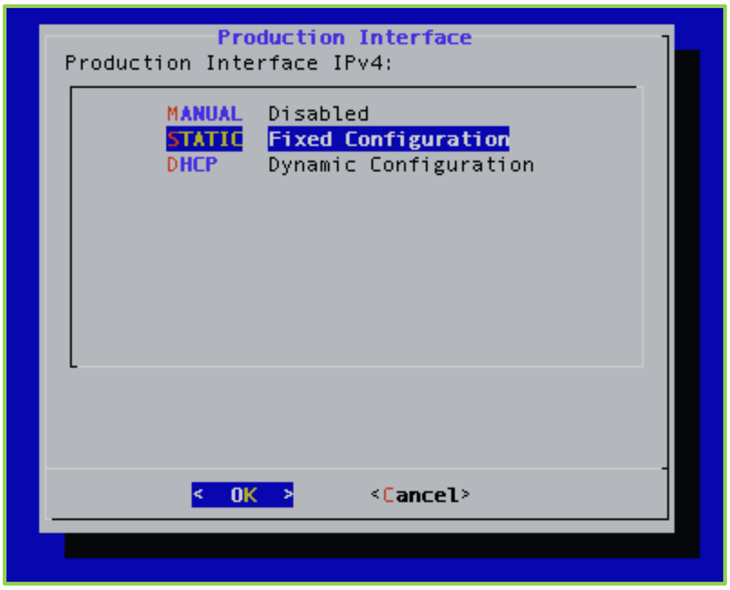


2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**.

The Production Interface Menu displays.

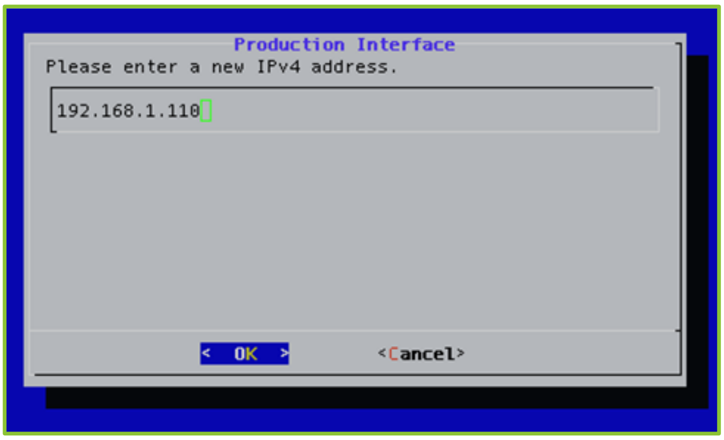


4. Enter **4** to select the IPv4 Configuration option.
5. Press the Enter key to select OK.



```
Production Interface
Production Interface IPv4:

    MANUAL   Disabled
    STATIC   Fixed Configuration
    DHCP     Dynamic Configuration

        <  OK  >        <Cancel>
```

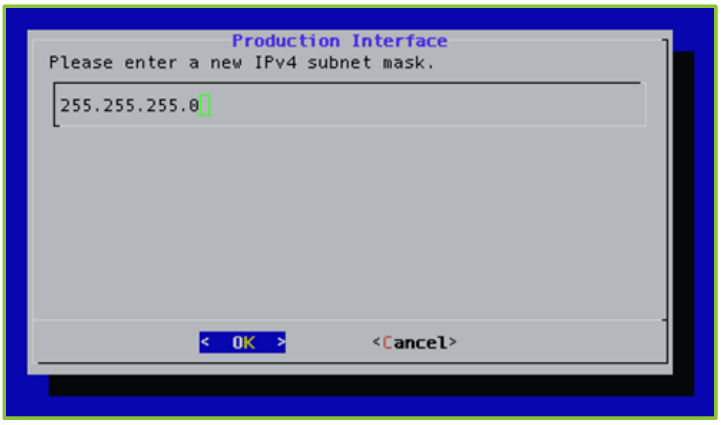
6. Enter **S** to select the STATIC option.
7. Press the Enter key to select OK.
8. Delete the existing IPv4 address and enter a new one.



```
Production Interface
Please enter a new IPv4 address.
192.168.1.110

        <  OK  >        <Cancel>
```

9. Press the Enter key to select OK.

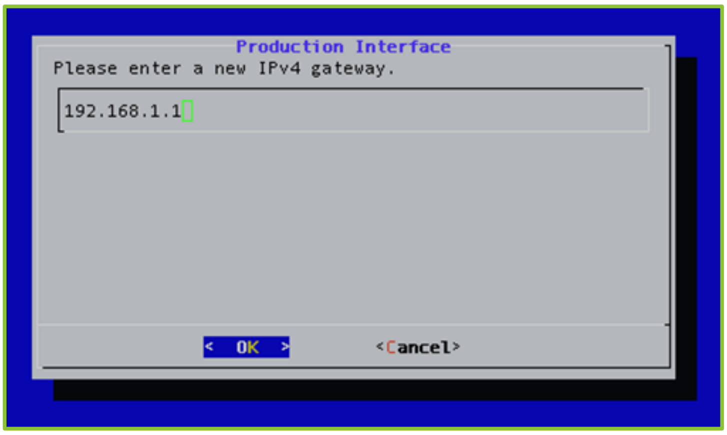
10. Delete the existing IPv4 subnet mask and enter a new one.



```
Production Interface
Please enter a new IPv4 subnet mask.
255.255.255.0
```

11. Press the **Enter** key to select **OK**.

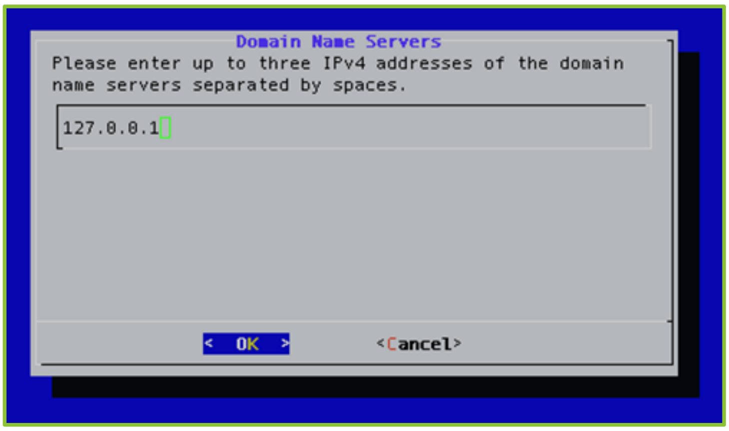
12. Delete the existing IPv4 gateway and enter a new one.



```
Production Interface
Please enter a new IPv4 gateway.
192.168.1.1
```

13. Press the **Enter** key to select **OK**.

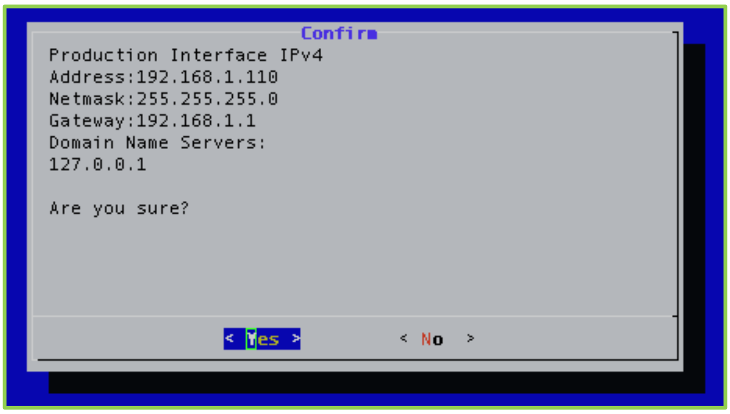
14. Delete the existing Domain Name Server and enter up to three.



```
Domain Name Servers
Please enter up to three IPv4 addresses of the domain
name servers separated by spaces.
127.0.0.1
```

15. Press the **Enter** key to select **OK**.

The *Confirm* window displays.



```
Confirm
Production Interface IPv4
Address:192.168.1.110
Netmask:255.255.255.0
Gateway:192.168.1.1
Domain Name Servers:
127.0.0.1

Are you sure?
```

16. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

17. Press the **Enter** key to select **OK**.

    For more information about configuring the Production and Management interfaces, see Configuring Your Vidyo Server’s Management Interface and Port.

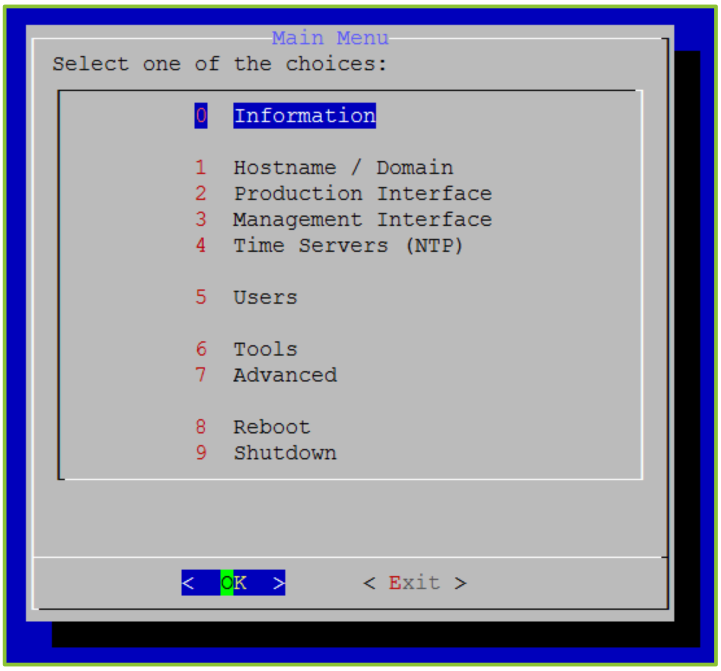
Configuring an IPv4 DHCP Production Interface

To configure an IPv4 DHCP Production Interface:

1. Log in to the System Console.

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

The Main Menu displays.

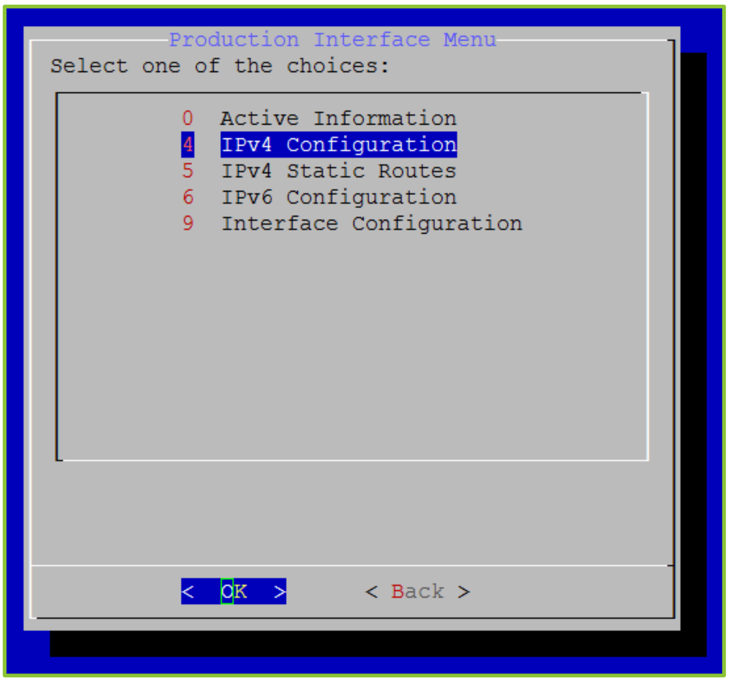


```
                     Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown


           <  OK  >       < Exit >
```

2. Enter **2** to select the Production Interface option.

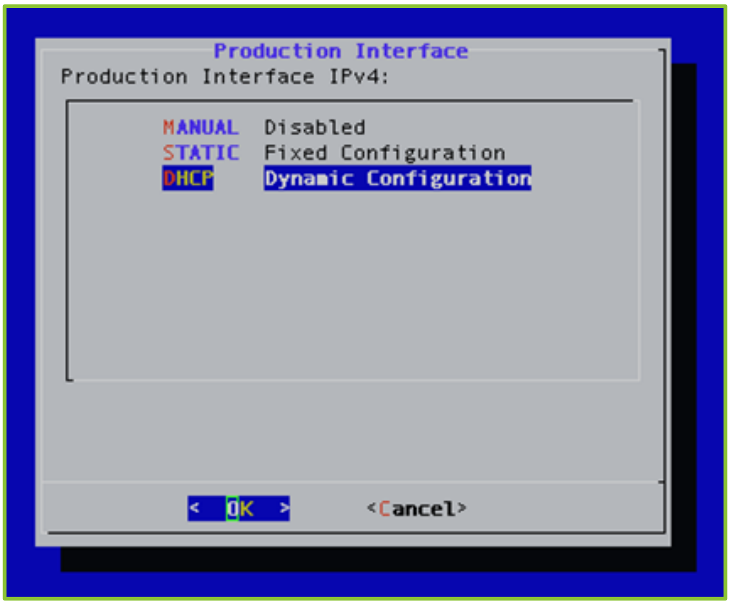
3. Press the Enter key to select OK.

The Production Interface Menu displays.



```
              Production Interface Menu
 Select one of the choices:

             0  Active Information
             4  IPv4 Configuration
             5  IPv4 Static Routes
             6  IPv6 Configuration
             9  Interface Configuration


           <  OK  >       < Back >
```

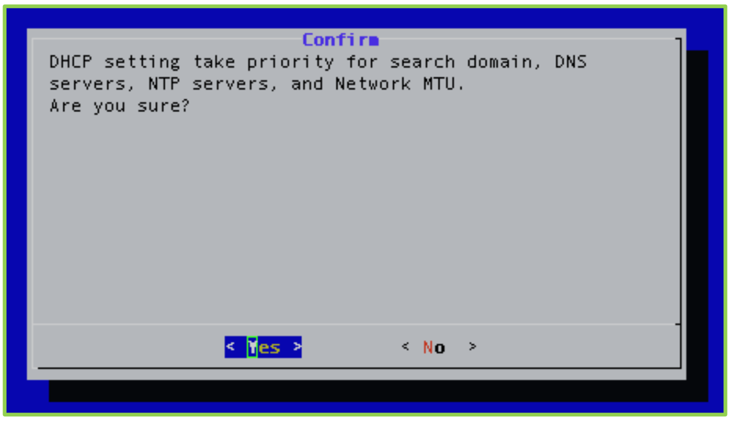
4. Enter **4** to select the IPv4 Configuration option.
5. Press the Enter key to select OK.



```
Production Interface
Production Interface IPv4:

    MANUAL   Disabled
    STATIC   Fixed Configuration
    DHCP     Dynamic Configuration
```

6. Enter **D** to select the DHCP option.
7. Press the Enter key to select OK.

   The *Confirm* window displays.



```
Confirm
DHCP setting take priority for search domain, DNS
servers, NTP servers, and Network MTU.
Are you sure?
```

8. Press the Enter key to select Yes.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
9. Press the Enter key to select OK.

Configuring IPv4 Static Routes

This section describes how to add and remove IPv4 static routes.

The VidyoGateway system supports IPv4 only or IPv6 only mode. Dual stack mode is not supported.

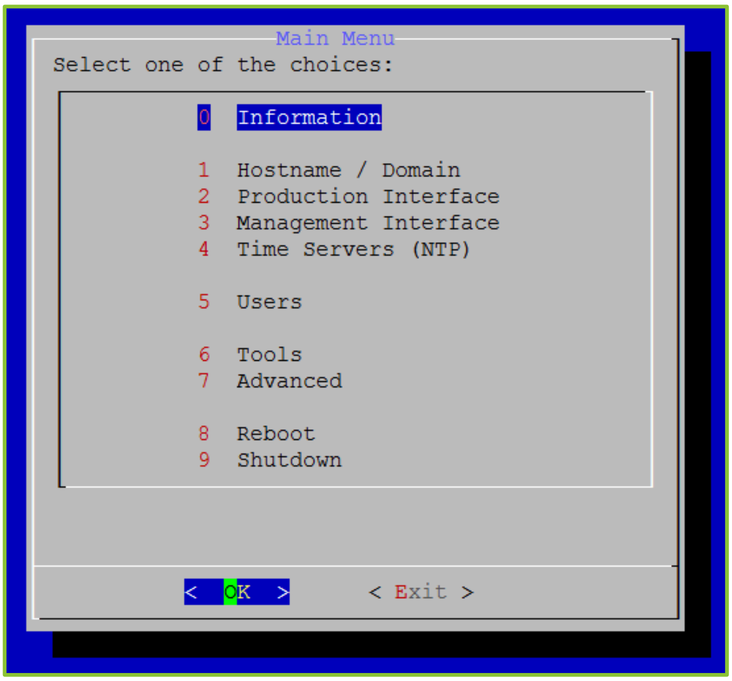
Adding IPv4 Static Routes

To add IPv4 Static routes:

1. Log in to the System Console.

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

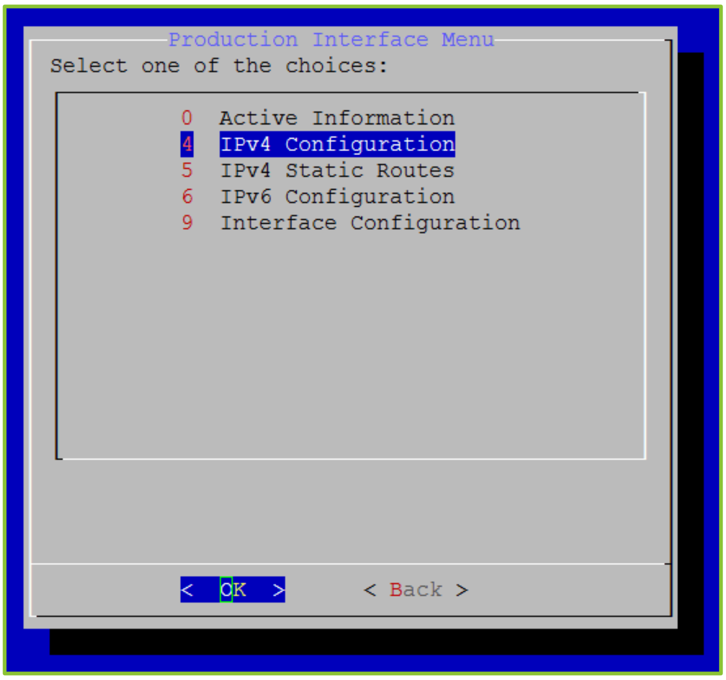
   The Main Menu displays.



```
                     Main Menu
 Select one of the choices:

                0  Information

                1  Hostname / Domain
                2  Production Interface
                3  Management Interface
                4  Time Servers (NTP)

                5  Users

                6  Tools
                7  Advanced

                8  Reboot
                9  Shutdown


              <  OK  >        < Exit >
```

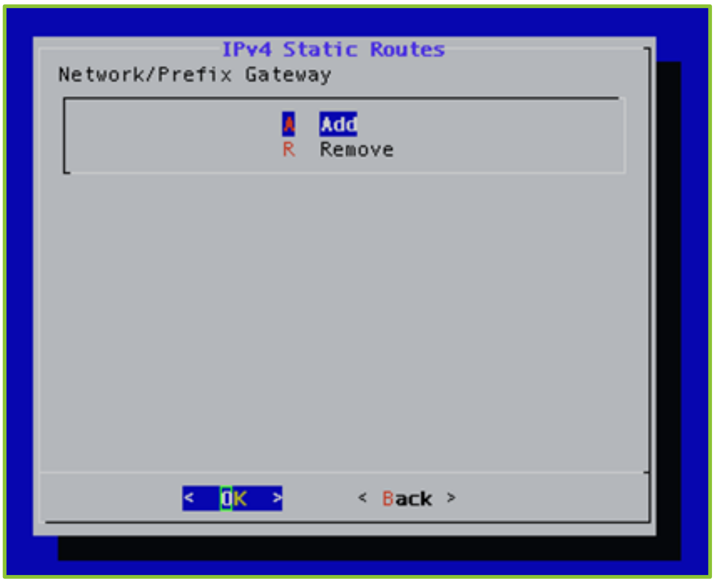
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**.

The Production Interface Menu displays.



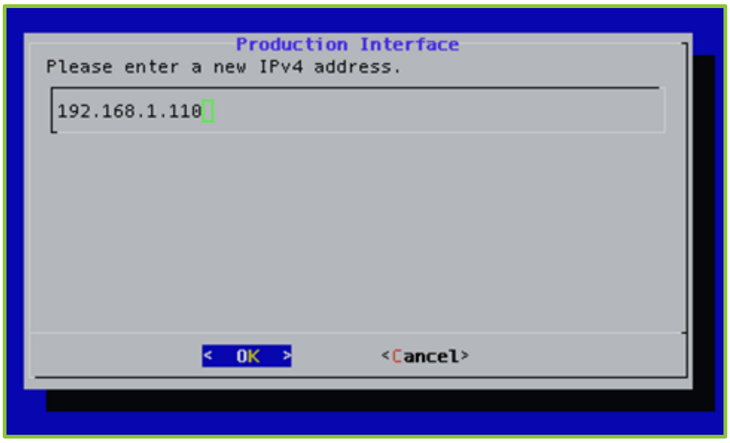
4. Enter **5** to select the IPv4 Static Routes option.
5. Press the Enter key to select OK.

   The *IPv4 Static Routes* window displays.



6. Enter **A** to select the Add option.
7. Press the Enter key to select OK.

8. Delete the existing IPv4 address and enter a new one.



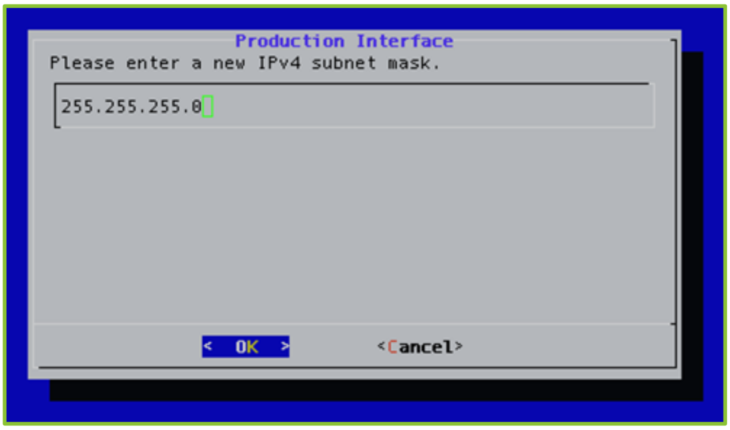
Production Interface

Please enter a new IPv4 address.

```
192.168.1.110
```

9. Press the **Enter** key to select **OK**.

10. Delete the existing IPv4 subnet mask and enter a new one.



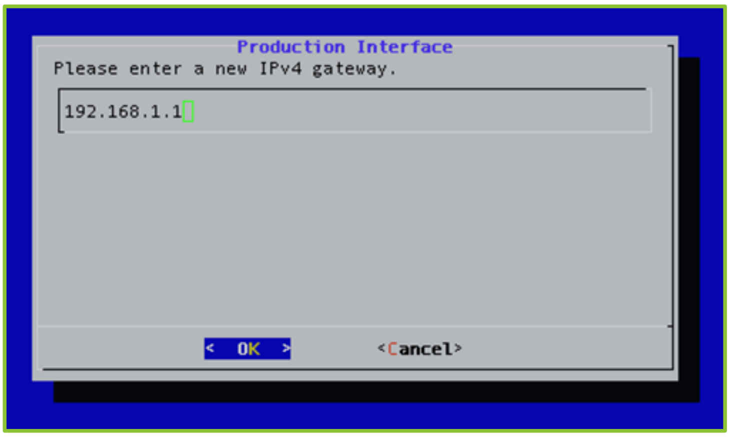
Production Interface

Please enter a new IPv4 subnet mask.

```
255.255.255.0
```

11. Press the **Enter** key to select **OK**.

12. Delete the existing IPv4 gateway and enter a new one.

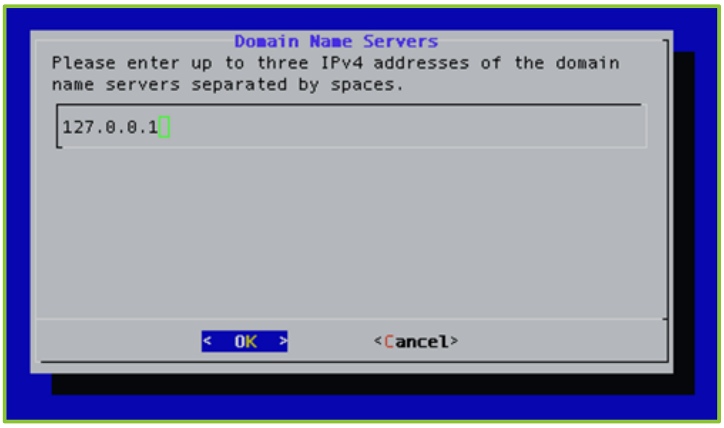


Production Interface

Please enter a new IPv4 gateway.

```
192.168.1.1
```

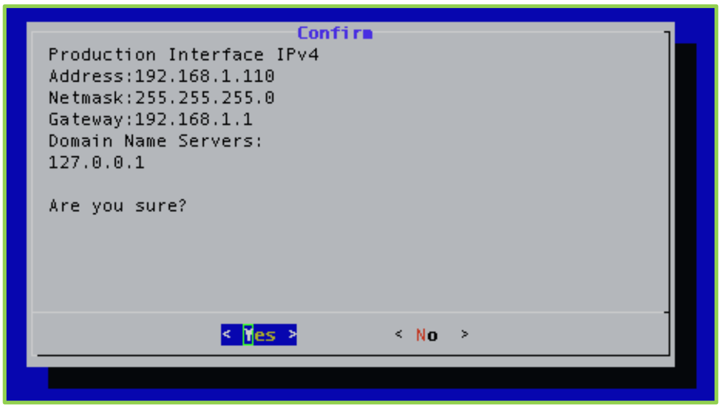
13. Press the **Enter** key to select **OK**.
14. Delete the existing Domain Name Server and enter up to three.



```
Domain Name Servers
Please enter up to three IPv4 addresses of the domain
name servers separated by spaces.

127.0.0.1
```

15. Press the **Enter** key to select **OK**.

    The *Confirm* window displays.



```
Confirm
Production Interface IPv4
Address:192.168.1.110
Netmask:255.255.255.0
Gateway:192.168.1.1
Domain Name Servers:
127.0.0.1

Are you sure?
```

16. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

17. Press the **Enter** key to select **OK**.

    For more information about configuring the Production and Management interfaces, see Configuring Your Vidyo Server’s Management Interface and Port.

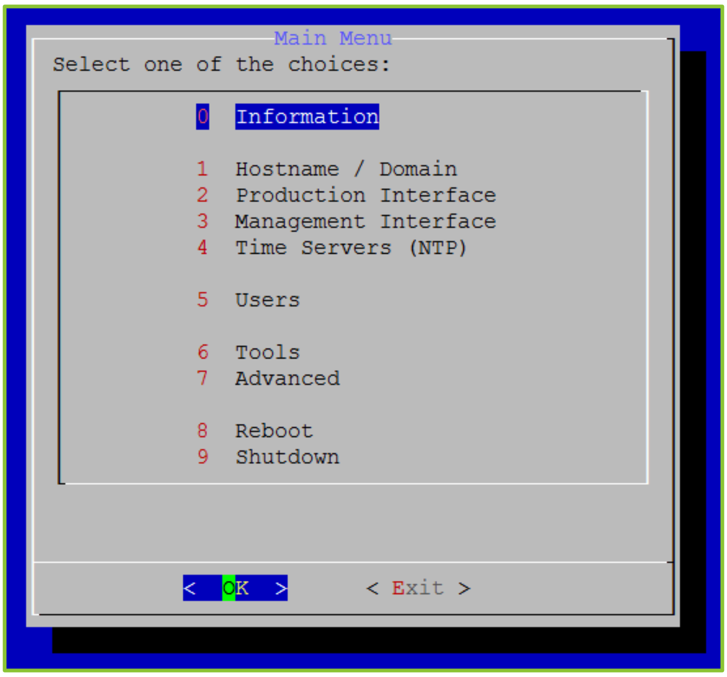
Removing IPv4 Static Routes

To remove IPv4 static routes:

1. Log in to the System Console.

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

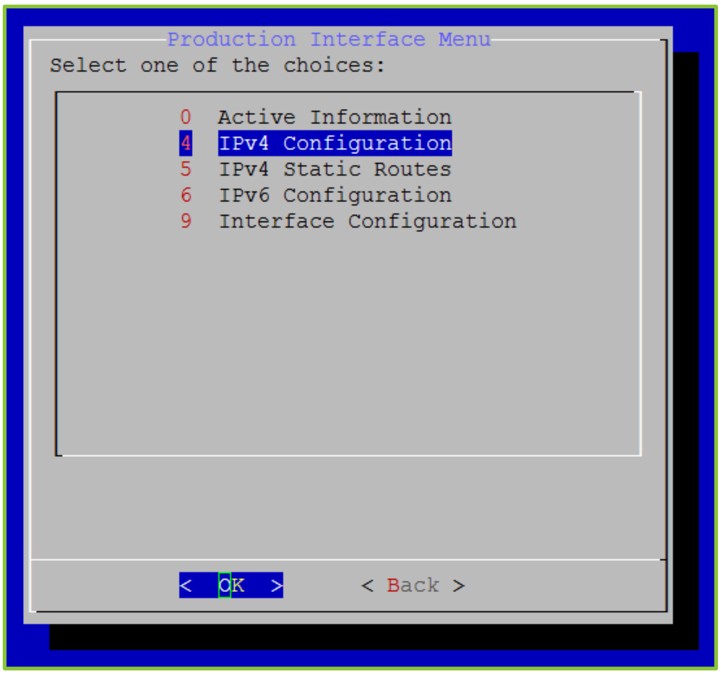
The Main Menu displays.



```
                        Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown

             <  OK  >       < Exit >
```

2. Enter **2** to select the Production Interface option.
3. Press the Enter key to select OK.

The Production Interface Menu displays.

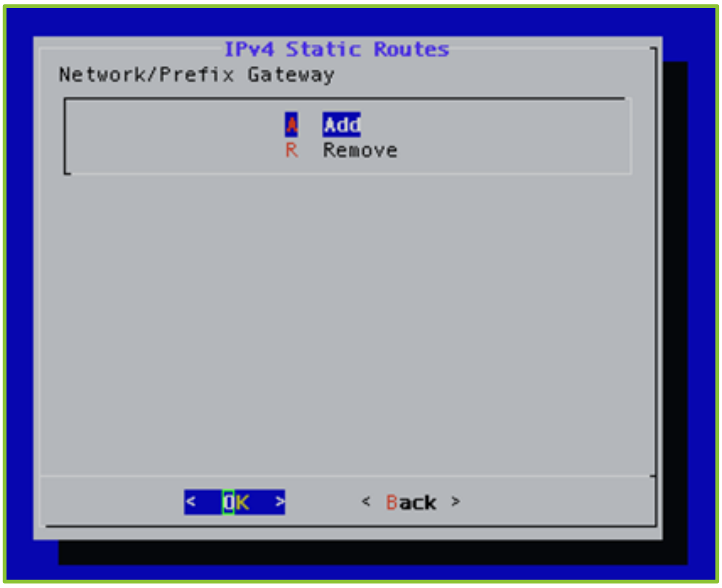


```
              Production Interface Menu
 Select one of the choices:

             0  Active Information
             4  IPv4 Configuration
             5  IPv4 Static Routes
             6  IPv6 Configuration
             9  Interface Configuration

             <  OK  >       < Back >
```

4. Enter **5** to select the IPv4 Static Routes option.

5. Press the **Enter** key to select **OK**.

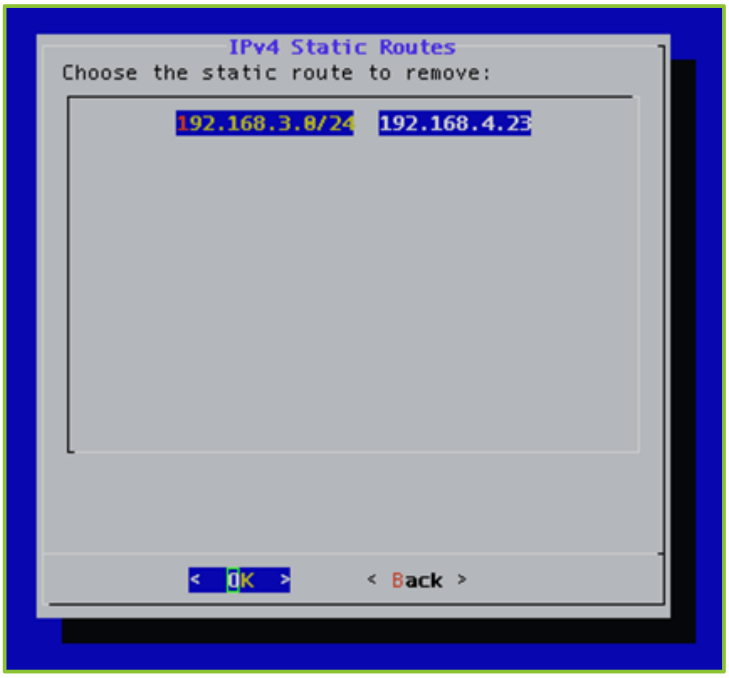
   The *IPv4 Static Routes* window displays.



```
IPv4 Static Routes
Network/Prefix Gateway

        A  Add
        R  Remove
```

6. Enter **R** to select the Remove option.
7. Press the **Enter** key to select **OK**.

   The *IPv4 Static Routes* window displays.



```
IPv4 Static Routes
Choose the static route to remove:

    192.168.3.0/24  192.168.4.23
```

8. Select the static route to remove.

9. Press the **Enter** key to select **OK**.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

10. Press the **Enter** key to select **OK**.

Configuring the IPv6 Production Interface

This section describes how to manually enable and disable the IPv6 Production Interface, how to configure IPv6 static and dynamic routes, and how to add and remove static routes.

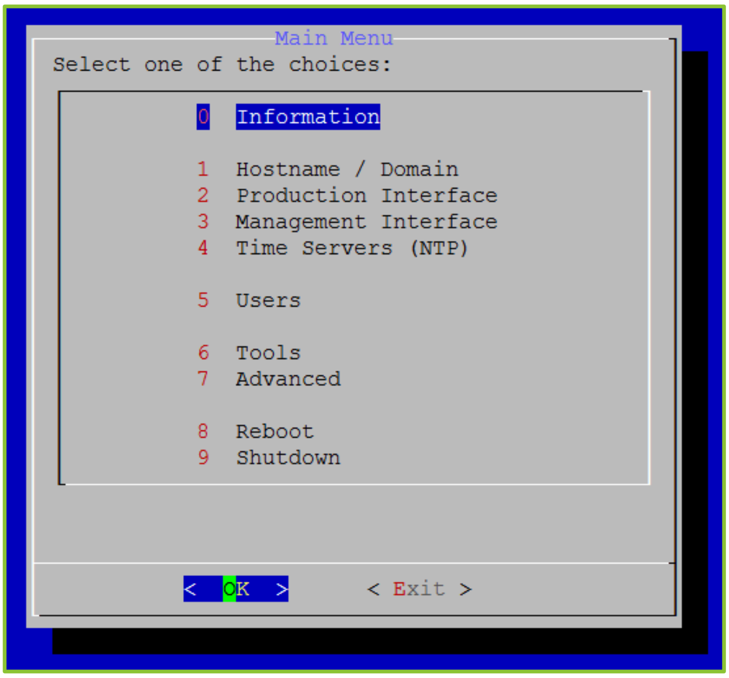
Manually Disabling and Enabling the IPv6 Production Interface

To manually disable or enable the IPv6 Production Interface:

1. Log in to the System Console.

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

   The Main Menu displays.

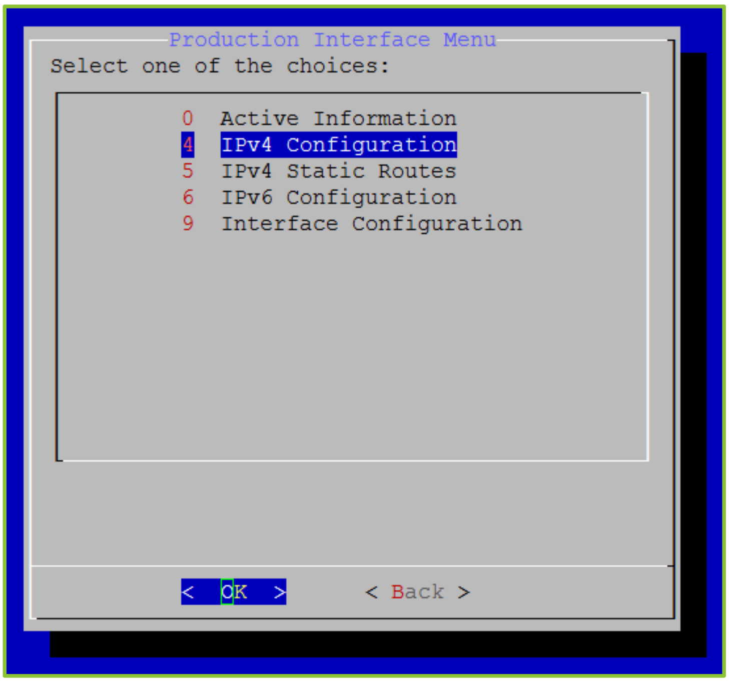


```
                 Main Menu
Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown

          <  OK  >      < Exit >
```

2. Enter **2** to select the Production Interface option.

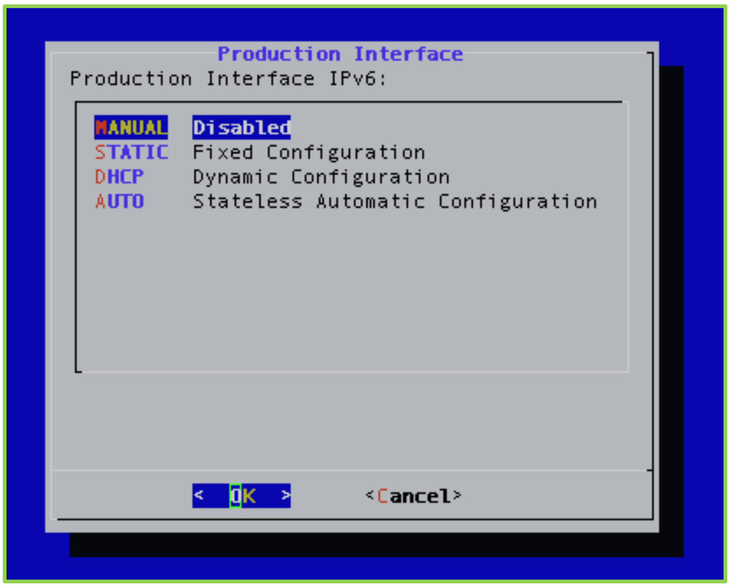
3. Press the **Enter** key to select **OK**.

The Production Interface Menu displays.



```
Production Interface Menu
Select one of the choices:

          0  Active Information
          4  IPv4 Configuration
          5  IPv4 Static Routes
          6  IPv6 Configuration
          9  Interface Configuration

        <  OK  >          < Back >
```

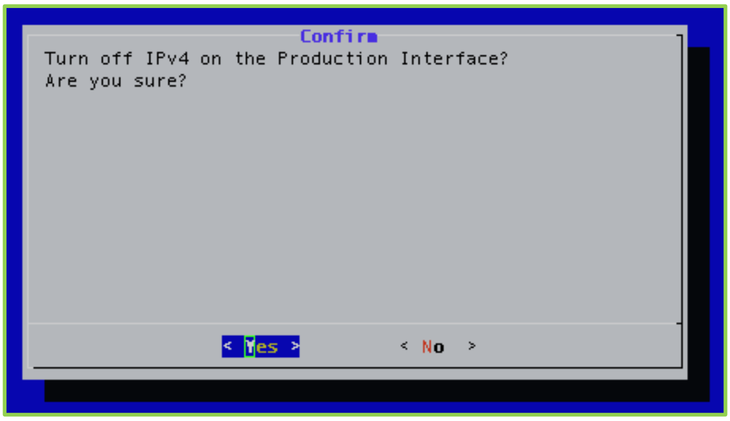
4. Enter **6** to select the IPv6 Configuration option.
5. Press the Enter key to select OK.



```
Production Interface
Production Interface IPv6:

  MANUAL   Disabled
  STATIC   Fixed Configuration
  DHCP     Dynamic Configuration
  AUTO     Stateless Automatic Configuration

        <  OK  >       <Cancel>
```

6. Enter **M** to select the MANUAL option.
7. Press the Enter key to select OK.

If the current state of the Production Interface is enabled, you are asked to confirm if you want to disable it. If the current state of the Production Interface is disabled, you are asked to confirm if you want to enable it.



```
Confirm
Turn off IPv4 on the Production Interface?
Are you sure?
```

8. Press the **Enter** key to select **Yes**.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

9. Press the **Enter** key to select **OK**.

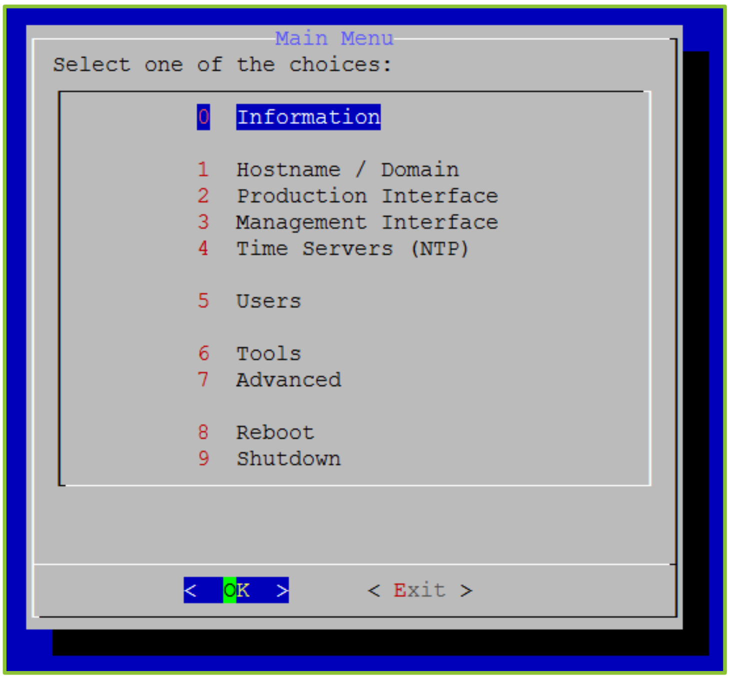
Configuring an IPv6 Static Production Interface

To configure an IPv6 static Production Interface:

1. Log in to the System Console.

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

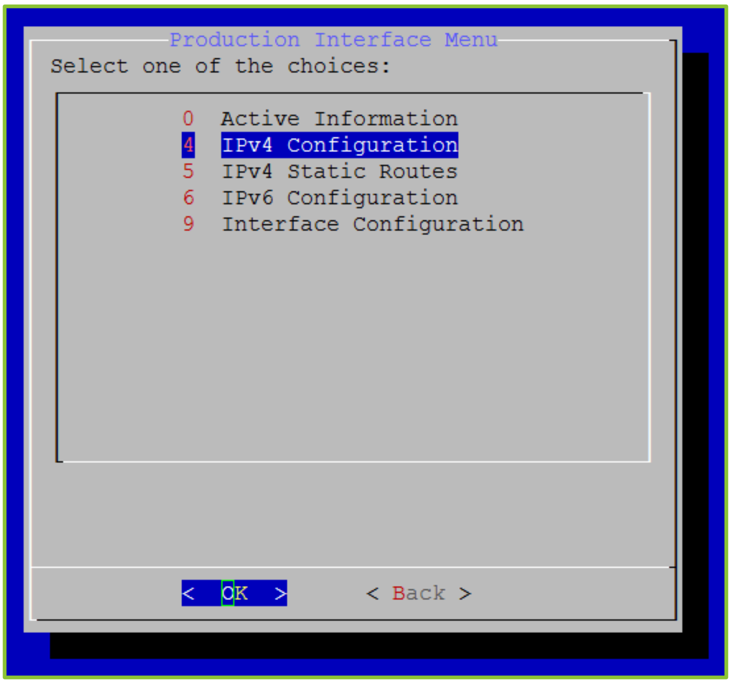
The Main Menu displays.



```
Main Menu
Select one of the choices:

     0  Information

     1  Hostname / Domain
     2  Production Interface
     3  Management Interface
     4  Time Servers (NTP)

     5  Users

     6  Tools
     7  Advanced

     8  Reboot
     9  Shutdown

        <  OK  >        < Exit >
```

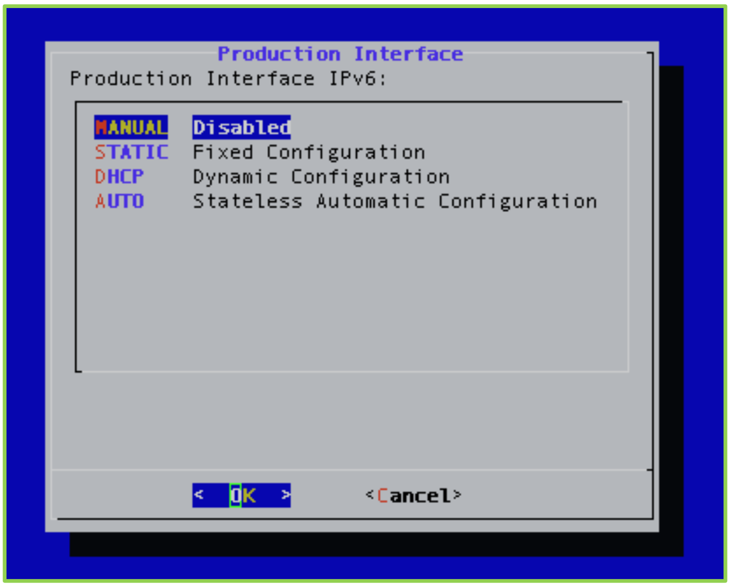
2. Enter **2** to select the Production Interface option.
3. Press the Enter key to select OK.

The Production Interface Menu displays.



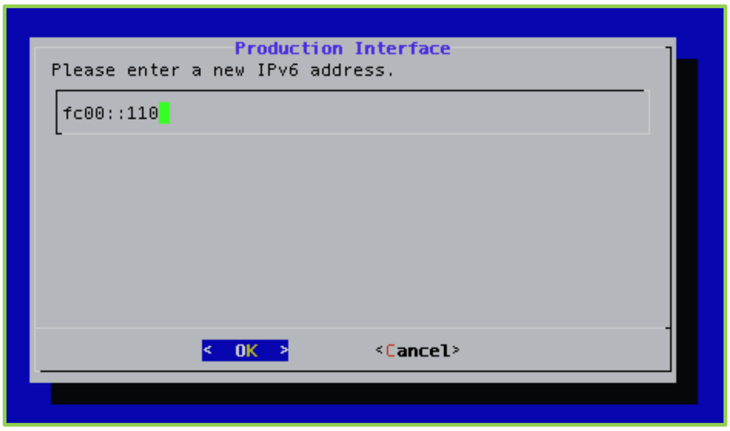
```
Production Interface Menu
Select one of the choices:

     0  Active Information
     4  IPv4 Configuration
     5  IPv4 Static Routes
     6  IPv6 Configuration
     9  Interface Configuration

        <  OK  >        < Back >
```

4. Enter **6** to select the IPv6 Configuration option.
5. Press the Enter key to select OK.



```
Production Interface
Production Interface IPv6:

MANUAL   Disabled
STATIC   Fixed Configuration
DHCP     Dynamic Configuration
AUTO     Stateless Automatic Configuration

         <  OK  >        <Cancel>
```

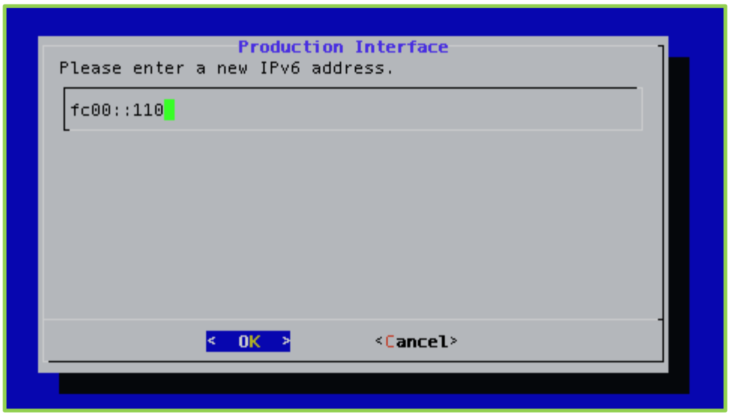
6. Enter **S** to select the STATIC option.
7. Press the Enter key to select OK.
8. Delete the existing IPv6 address and enter a new one.



```
Production Interface
Please enter a new IPv6 address.

fc00::110

         <  OK  >        <Cancel>
```

9. Press the Enter key to select OK.

10. Delete the existing IPv6 address and enter a new one.



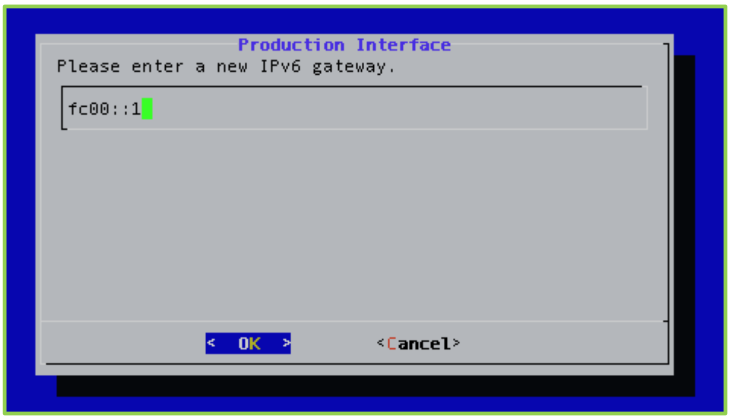
Production Interface

Please enter a new IPv6 address.

```
fc00::110
```

11. Press the **Enter** key to select **OK**.

12. Delete the existing IPv6 gateway and enter a new one.



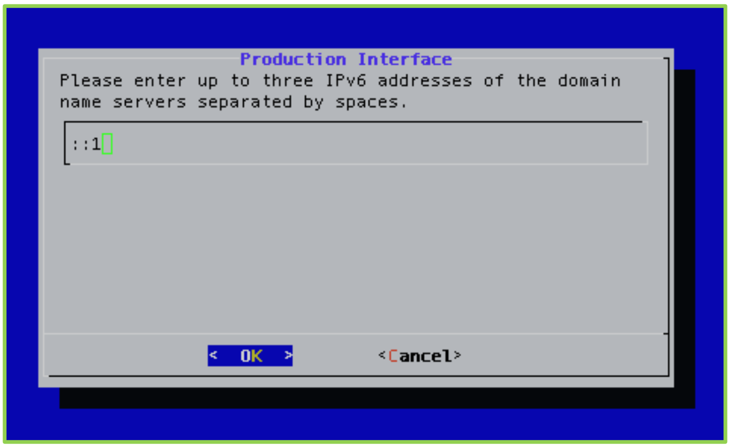
Production Interface

Please enter a new IPv6 gateway.

```
fc00::1
```

13. Press the **Enter** key to select **OK**.

14. Delete the existing Domain Name Server and enter up to three.



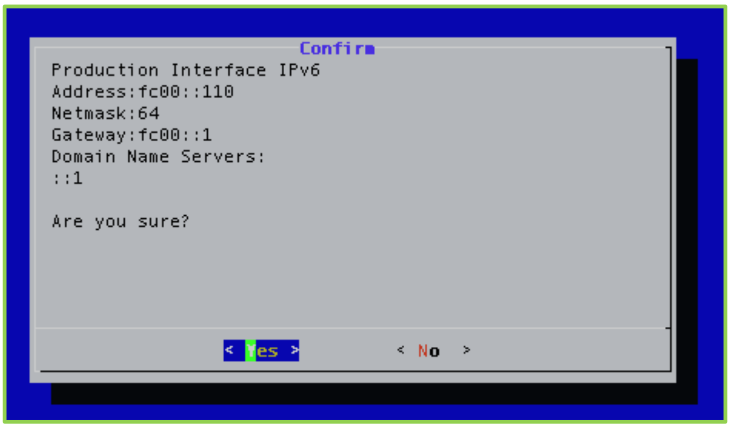
Production Interface

Please enter up to three IPv6 addresses of the domain name servers separated by spaces.

```
::1
```

15. Press the **Enter** key to select **OK**.

The *Confirm* window displays.



```
Confirm
Production Interface IPv6
Address:fc00::110
Netmask:64
Gateway:fc00::1
Domain Name Servers:
::1

Are you sure?
```

16. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

17. Press the **Enter** key to select **OK**.

    For more information about configuring the Production and Management interfaces, see Configuring Your Vidyo Server’s Management Interface and Port.

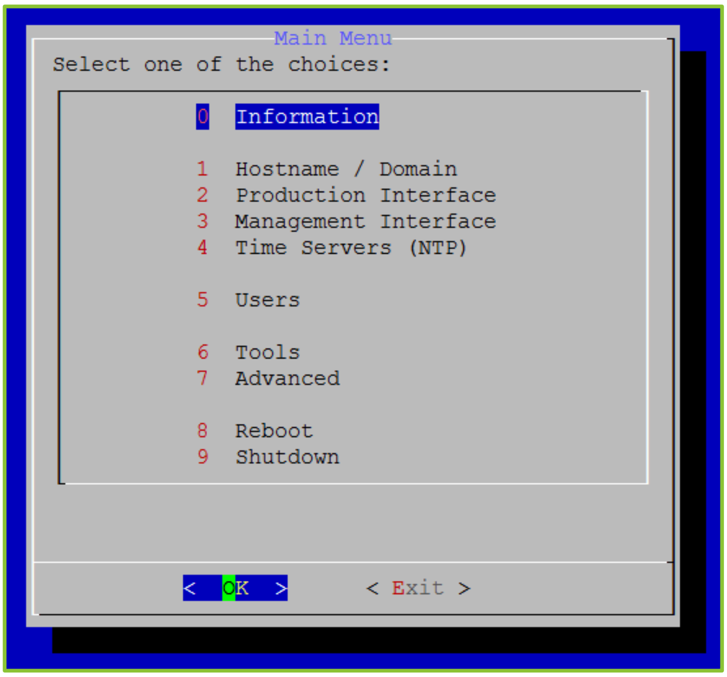
Configuring Stateless Automatic Configuration

To configure stateless automatic configuration:

1. Log in to the System Console.

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

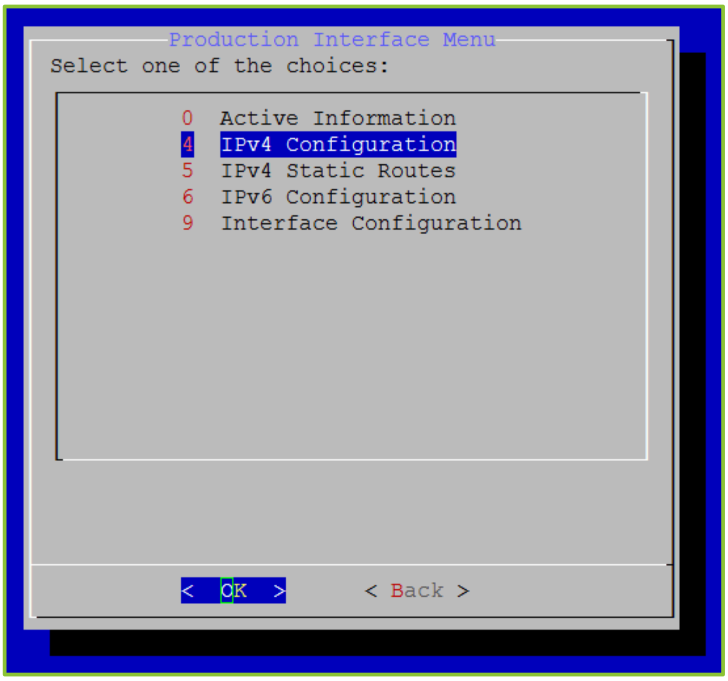
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

     <  OK  >        < Exit >
```

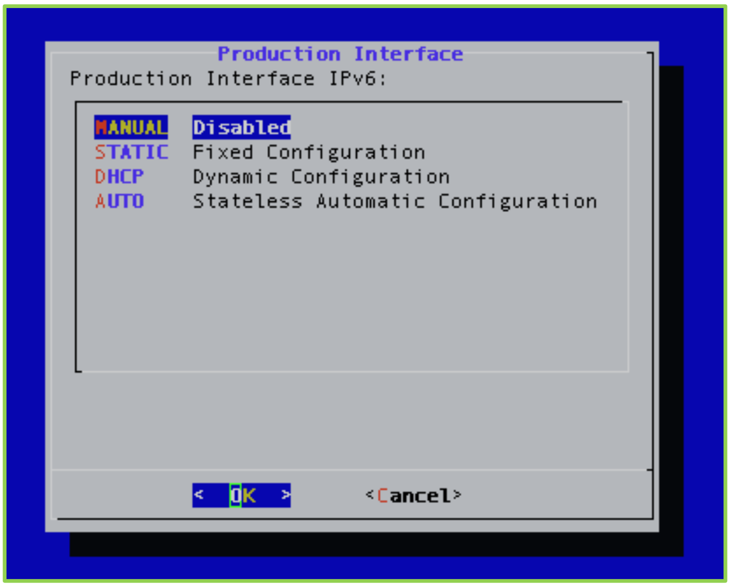
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**.

The Production Interface Menu displays.



```
Production Interface Menu
Select one of the choices:

       0  Active Information
       4  IPv4 Configuration
       5  IPv4 Static Routes
       6  IPv6 Configuration
       9  Interface Configuration

     <  OK  >        < Back >
```

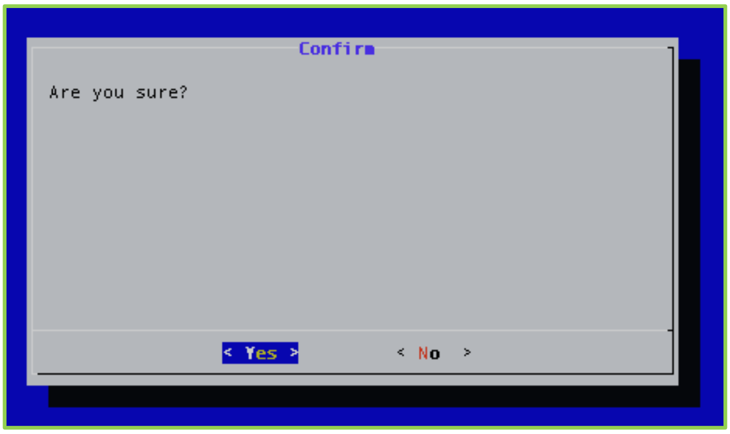
4. Enter **6** to select the IPv6 Configuration option.
5. Press the Enter key to select OK.



```
Production Interface
Production Interface IPv6:

  MANUAL   Disabled
  STATIC   Fixed Configuration
  DHCP     Dynamic Configuration
  AUTO     Stateless Automatic Configuration
```

6. Enter **A** to select the AUTO option.
7. Press the Enter key to select OK.

   The *Confirm* window displays.



```
Confirm
Are you sure?
```

8. Press the Enter key to select Yes.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
9. Press the Enter key to select OK.

Configuring the MTU and Auto Negotiation for the Production Interface

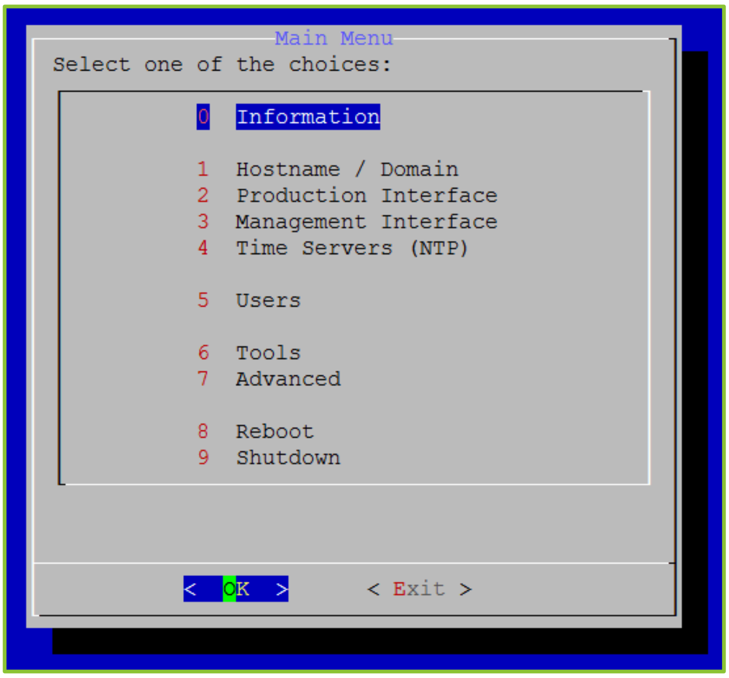
Configuring the Maximum Transmission Unit (MTU)

To configure the Maximum Transmittion Unit (MTU):

1. Log in to the System Console.

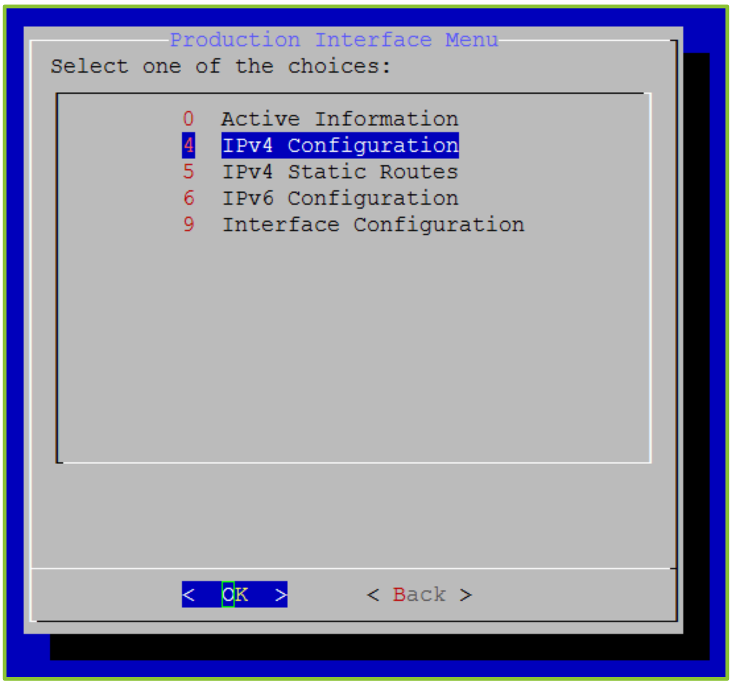
   For more information, see Logging in to the System Console and Changing the Default Password.

   The Main Menu displays.



2. Enter **2** to select the Production Interface option.
3. Press the Enter key to select OK.

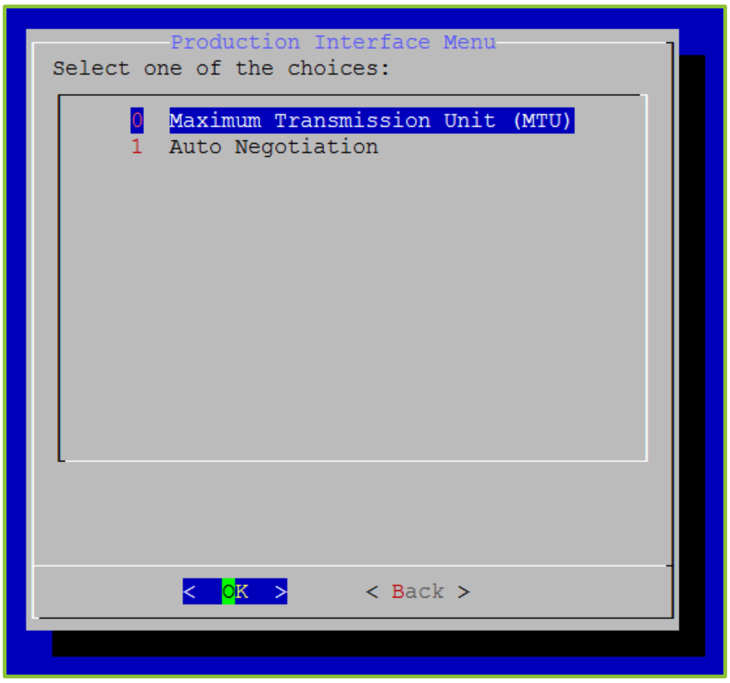
The Production Interface Menu displays.



```
Production Interface Menu
Select one of the choices:

            0  Active Information
            4  IPv4 Configuration
            5  IPv4 Static Routes
            6  IPv6 Configuration
            9  Interface Configuration

          <  OK  >        < Back >
```

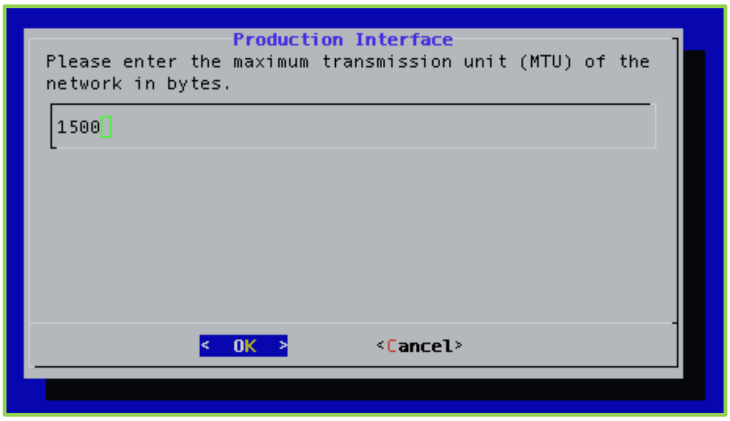
4. Enter **9** to select the Interface Configuration option.
5. Press the Enter key to select OK.

The Production Interface Menu displays.



```
Production Interface Menu
Select one of the choices:

        0  Maximum Transmission Unit (MTU)
        1  Auto Negotiation

          <  OK  >        < Back >
```

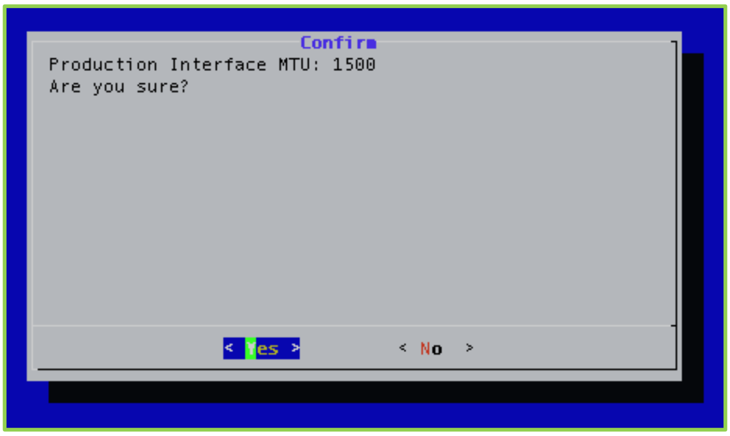
6. Enter **0** to select the Maximum Transmission Unit (MTU) option.
7. Enter the MTU of the networks in bytes.



```
Please enter the maximum transmission unit (MTU) of the
network in bytes.

1500
```

8. Press the **Enter** key to select **OK**.

   A *Confirm* window displays.



```
Production Interface MTU: 1500
Are you sure?
```

9. Press the **Enter** key to select **Yes**.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

10. Press the **Enter** key to select **OK**.

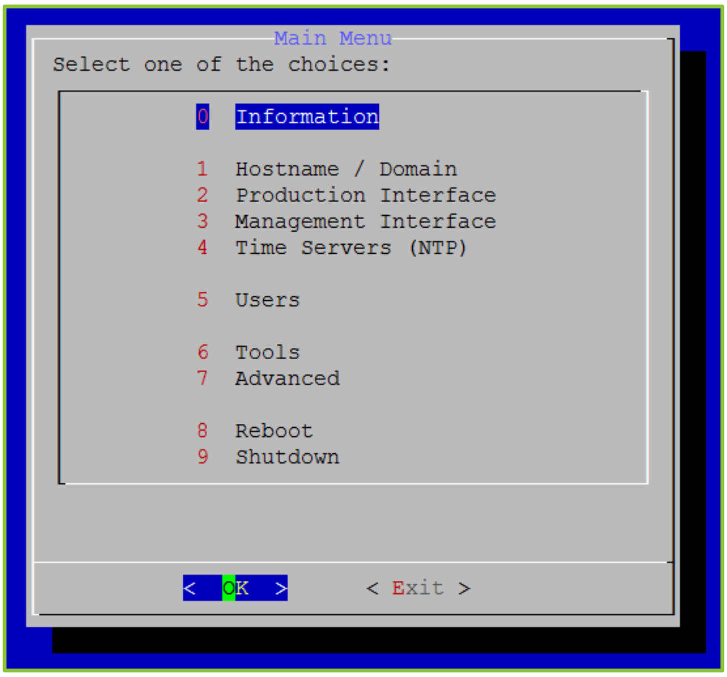
Configuring Auto Negotiation

To configure auto negotiation:

1. Log in to the System Console.

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

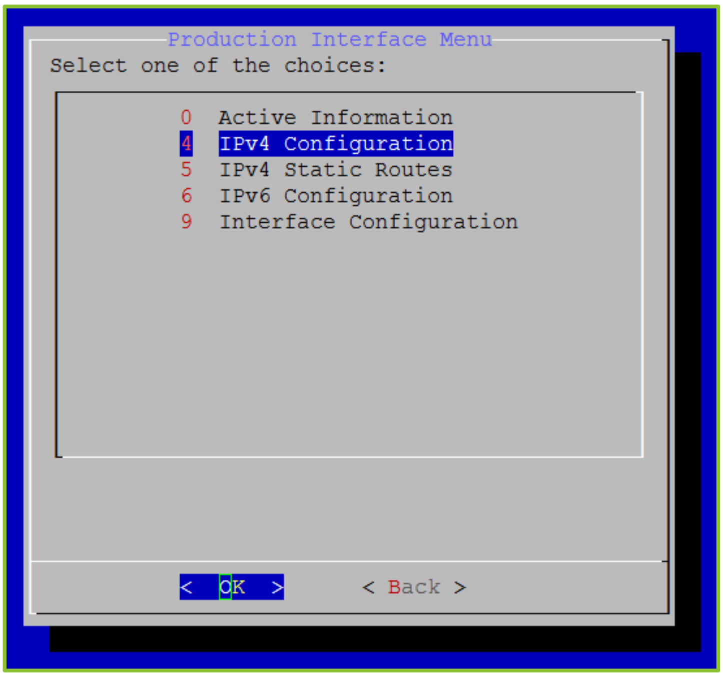
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

     <  OK  >        < Exit >
```

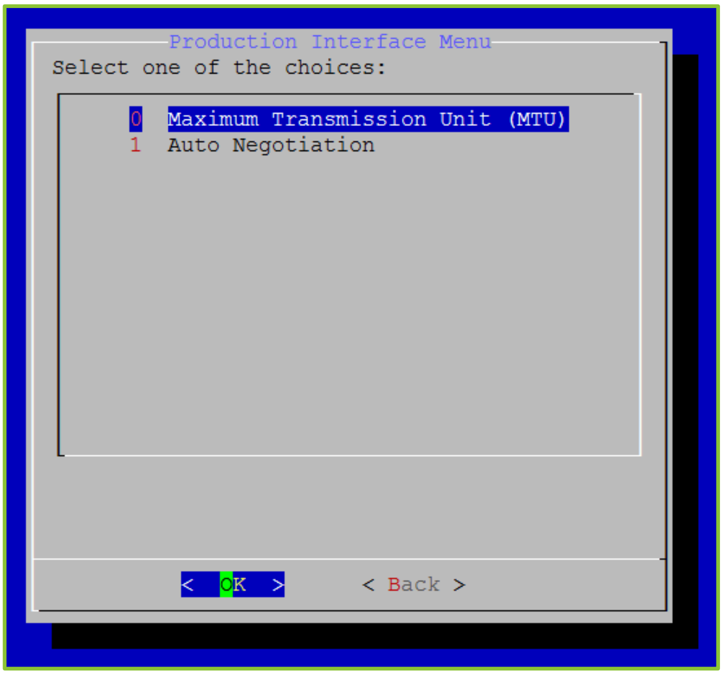
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**.

The Production Interface Menu displays.



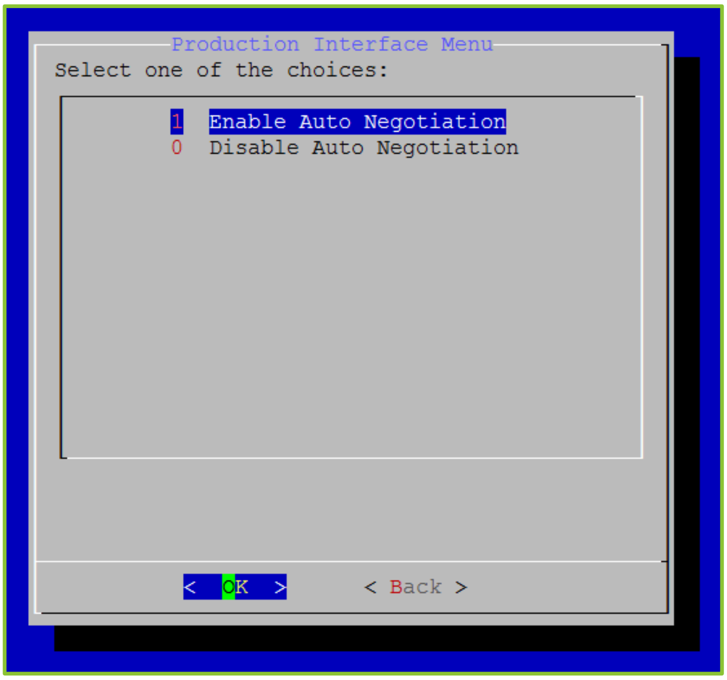
```
Production Interface Menu
Select one of the choices:

      0  Active Information
      4  IPv4 Configuration
      5  IPv4 Static Routes
      6  IPv6 Configuration
      9  Interface Configuration

     <  OK  >        < Back >
```

4. Enter **9** to select the Interface Configuration option.
5. Press the Enter key to select OK.



```
Production Interface Menu
Select one of the choices:

      0   Maximum Transmission Unit (MTU)
      1   Auto Negotiation
```

6. Enter **1** to select the Auto Negotiation option.
7. Press the Enter key to select OK.



```
Production Interface Menu
Select one of the choices:

      1   Enable Auto Negotiation
      0   Disable Auto Negotiation
```

8. Enter **1** to enable Auto Negotiation or enter **0** to disable Auto Negotiation.
9. Press the **Enter** key to select **OK**.

   A *Confirm* window displays.
10. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
11. Press the **Enter** key to select **OK**.

Configuring the Management Interface

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 that 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.

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.

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

Viewing the Management Interface Active Information

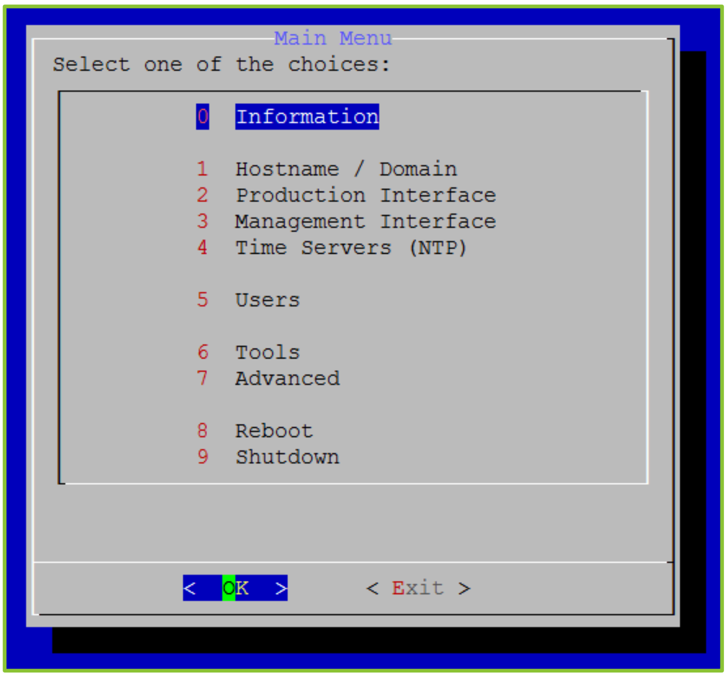
The *Management Interface Active Information* window provides important information about the Management Interface, such as the currently configured IP address and the link status.

To view the Management Interface active information:

1. Log in to the System Console.

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

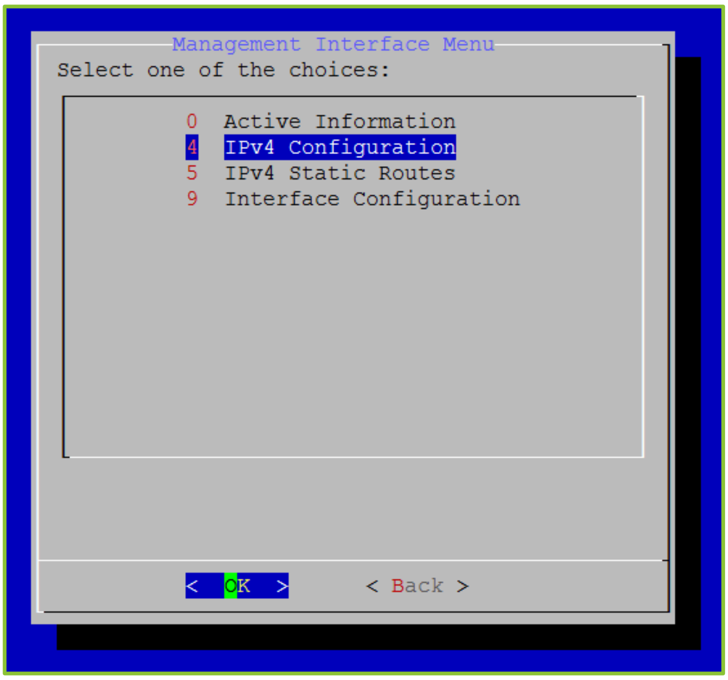
The Main Menu displays.



```
Main Menu
Select one of the choices:

            0  Information

            1  Hostname / Domain
            2  Production Interface
            3  Management Interface
            4  Time Servers (NTP)

            5  Users

            6  Tools
            7  Advanced

            8  Reboot
            9  Shutdown

       <  OK  >          < Exit >
```

2. Enter **3** to select the Management Interface option.
3. Press the **Enter** key to select **OK**.

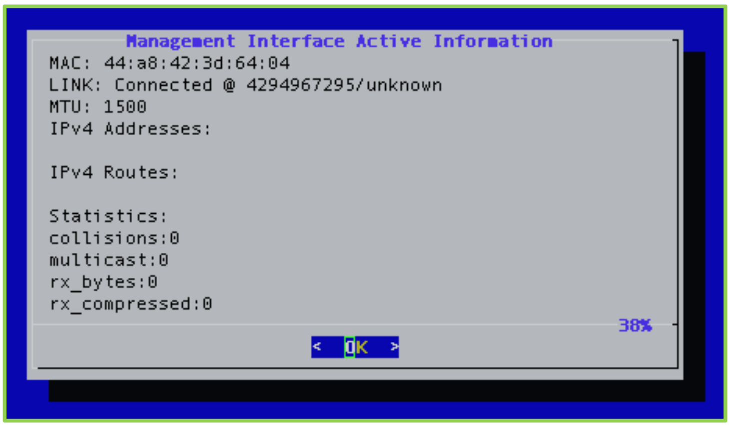
The Management Interface Menu displays.



```
Management Interface Menu
Select one of the choices:

           0  Active Information
           4  IPv4 Configuration
           5  IPv4 Static Routes
           9  Interface Configuration

       <  OK  >          < Back >
```

4. Enter **0** to select the Active Information option.
5. Press the **Enter** key to select **OK**.

   The Management Interface Active Information window displays.



```
Management Interface Active Information
MAC: 44:a8:42:3d:64:04
LINK: Connected @ 4294967295/unknown
MTU: 1500
IPv4 Addresses:

IPv4 Routes:

Statistics:
collisions:0
multicast:0
rx_bytes:0
rx_compressed:0
                                                      38%
```

Configuring the IPv4 Management Interface

This section describes how to manually enable and disable the IPv4 Production Interface, how to configure IPv4 static and dynamic routes, and how to add and remove static routes.

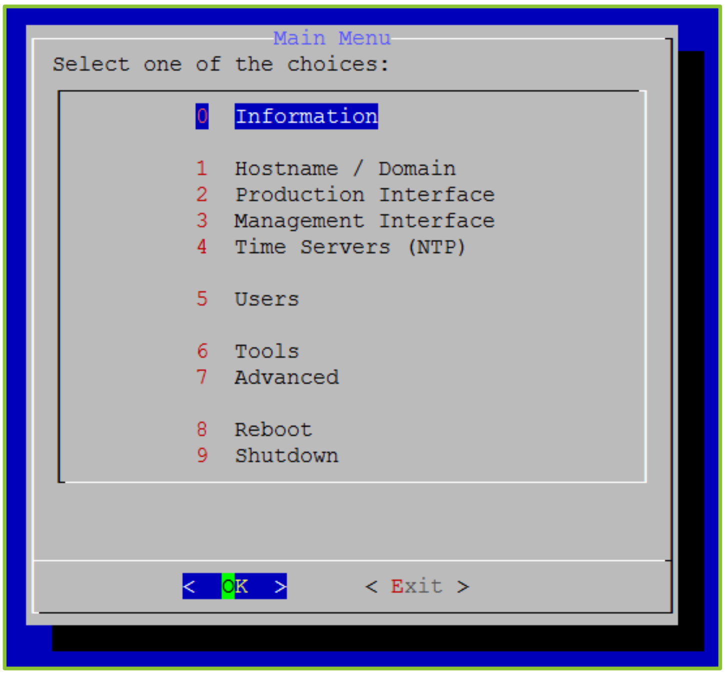
Manually Disabling and Enabling the IPv4 Management Interface

To manually disable or enable the IPv4 Management Interface:

1. Log in to the System Console.

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

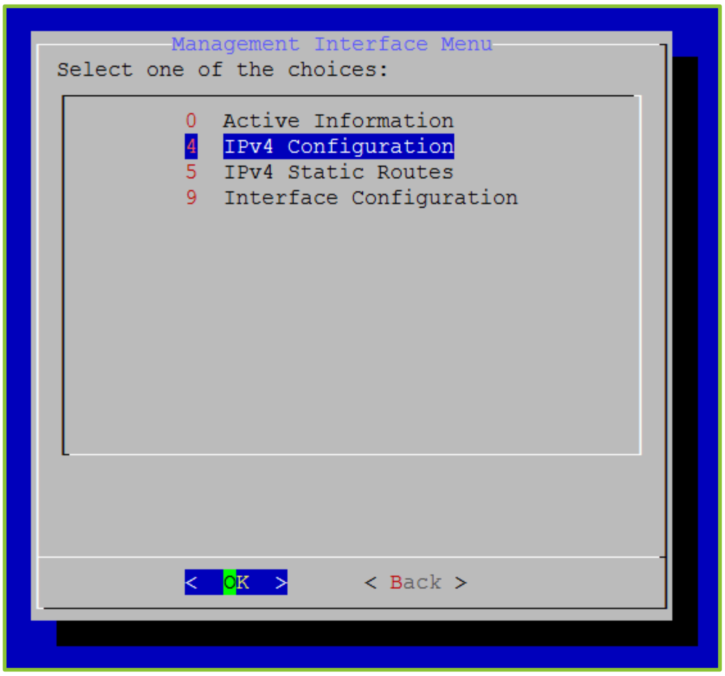
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

       <  OK  >         < Exit >
```

2. Enter **3** to select the Management Interface option.
3. Press the **Enter** key to select **OK**.

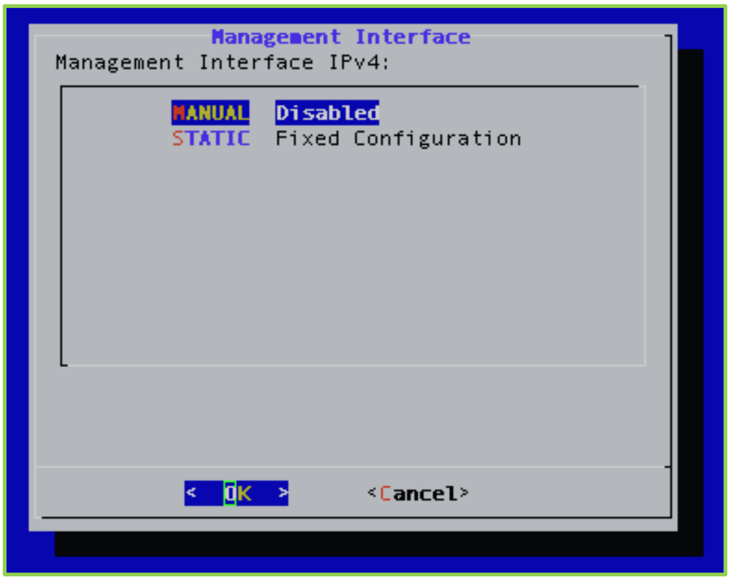
The Management Interface Menu displays.



```
Management Interface Menu
Select one of the choices:
       0  Active Information
       4  IPv4 Configuration
       5  IPv4 Static Routes
       9  Interface Configuration

       <  OK  >         < Back >
```

4. Enter **4** to select the IPv4 Configuration option.

5. Press the **Enter** key to select **OK**.

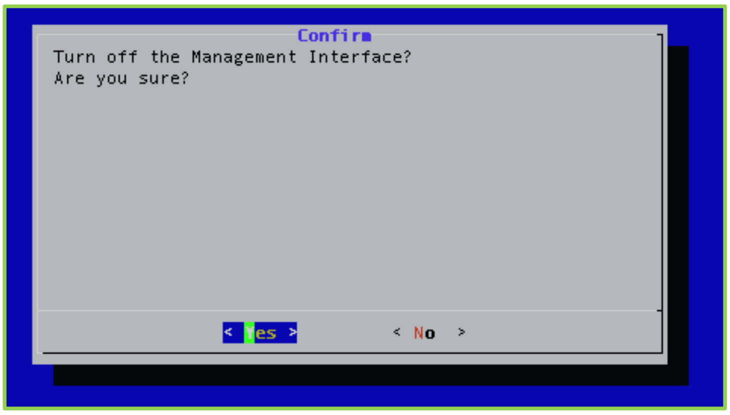


```
Management Interface
Management Interface IPv4:

          MANUAL  Disabled
          STATIC  Fixed Configuration
```

6. Enter **M** to select the MANUAL option.

7. Press the **Enter** key to select **OK**.

   If the current state of the Management Interface is enabled, you are asked to confirm if you want to disable it; if the current state of the Management Interface is disabled, you are asked to confirm if you want to enable it.



```
Confirm
Turn off the Management Interface?
Are you sure?
```

8. Press the **Enter** key to select **Yes**.

   A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

9. Press the **Enter** key to select **OK**.

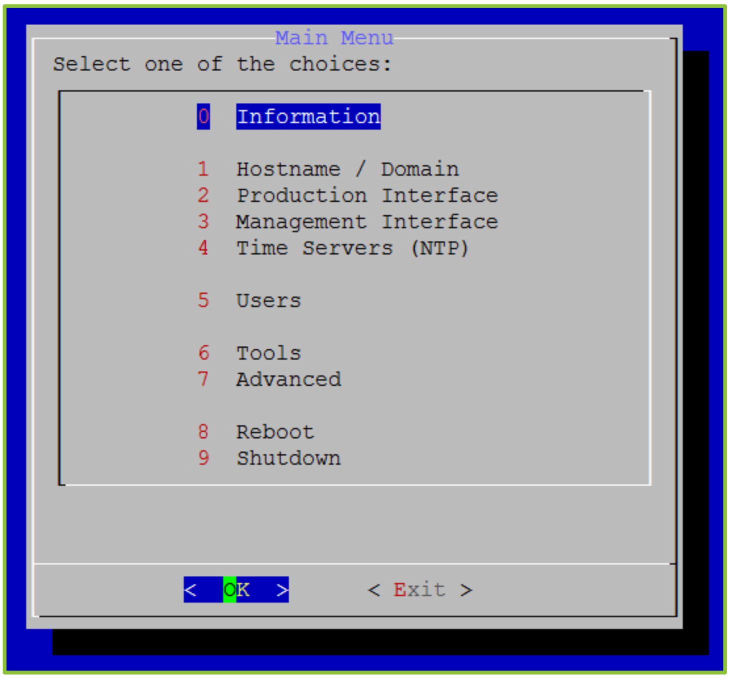
Configuring an IPv4 Static Management Interface

To configure an IPv4 static Management Interface:

1. Log in to the System Console.

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

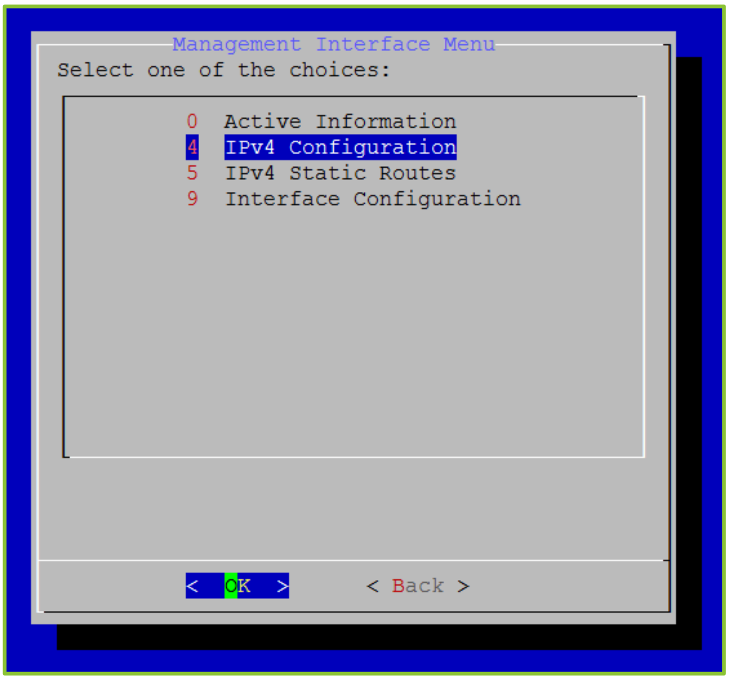
   The Main Menu displays.



```
                    Main Menu
Select one of the choices:

                0   Information

                1   Hostname / Domain
                2   Production Interface
                3   Management Interface
                4   Time Servers (NTP)

                5   Users

                6   Tools
                7   Advanced

                8   Reboot
                9   Shutdown

              <  OK  >        < Exit >
```

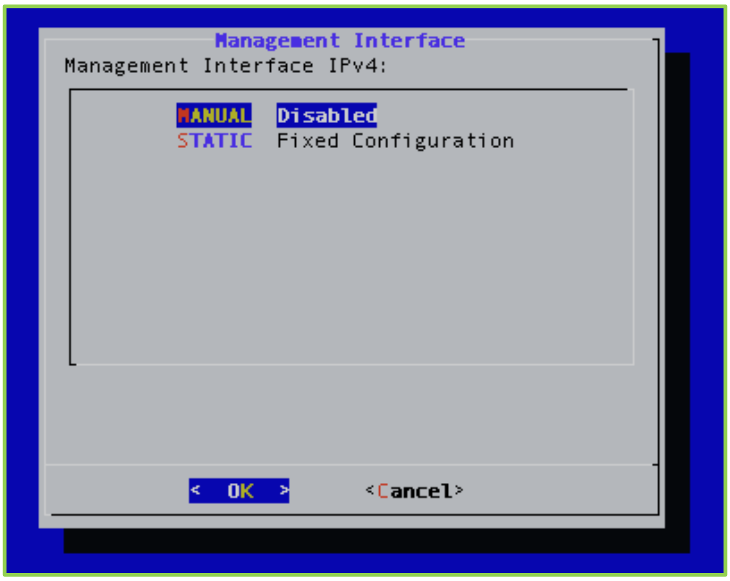
2. Enter **3** to select the Management Interface option.
3. Press the **Enter** key to select **OK**.

The Management Interface Menu displays.



```
Management Interface Menu
Select one of the choices:

          0   Active Information
          4   IPv4 Configuration
          5   IPv4 Static Routes
          9   Interface Configuration
```

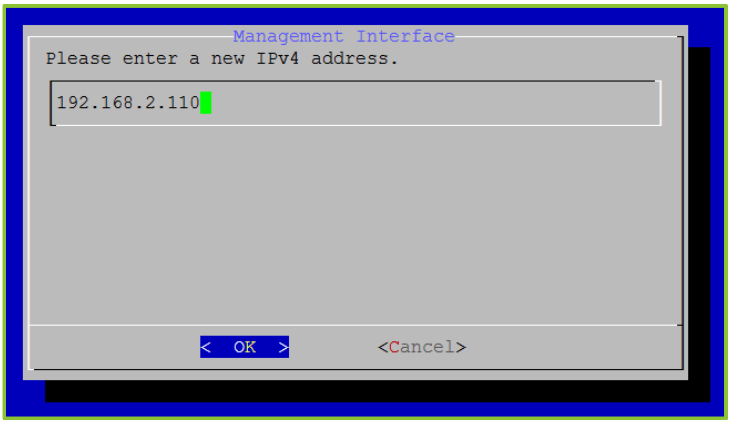
4. Enter **4** to select the IPv4 Configuration option.
5. Press the Enter key to select OK.
6. Enter **S** to select the STATIC option.



```
Management Interface
Management Interface IPv4:

        MANUAL   Disabled
        STATIC   Fixed Configuration
```

7. Press the Enter key to select OK.

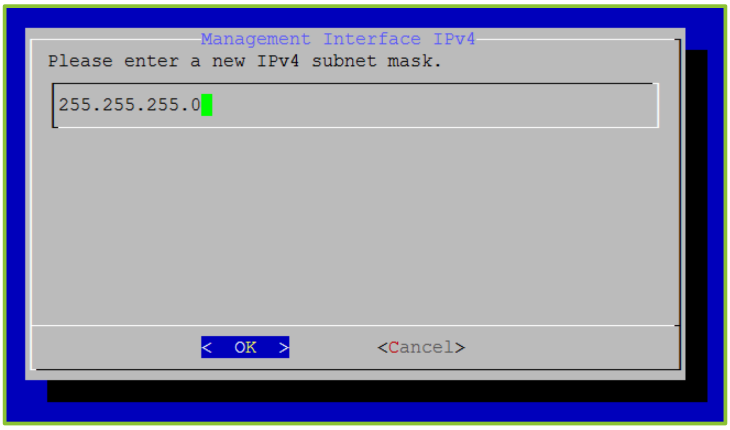
8. Delete the existing IPv4 address and enter a new one.



```
Management Interface
Please enter a new IPv4 address.
192.168.2.110
```

9. Press the **Enter** key to select **OK**.

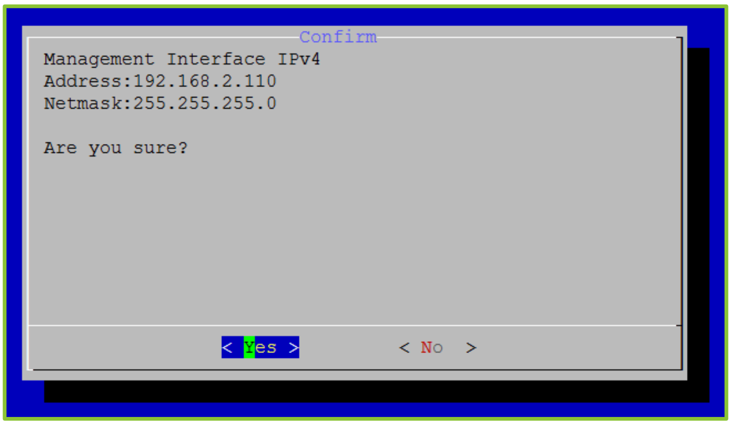
10. Delete the existing IPv4 subnet mask and enter a new one.



```
Management Interface IPv4
Please enter a new IPv4 subnet mask.
255.255.255.0
```

11. Press the **Enter** key to select **OK**.

The *Confirm* window displays.



```
Confirm
Management Interface IPv4
Address:192.168.2.110
Netmask:255.255.255.0

Are you sure?
```

12. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

13. Press the **Enter** key to select **OK**.

    For more information about configuring the Production and Management interfaces, see Configuring Your Vidyo Server’s Management Interface and Port.

Configuring IPv4 Static Routes

This section describes how to add and remove IPv4 static routes.

The VidyoGateway system supports IPv4 only or IPv6 only mode. Dual stack mode is not supported.

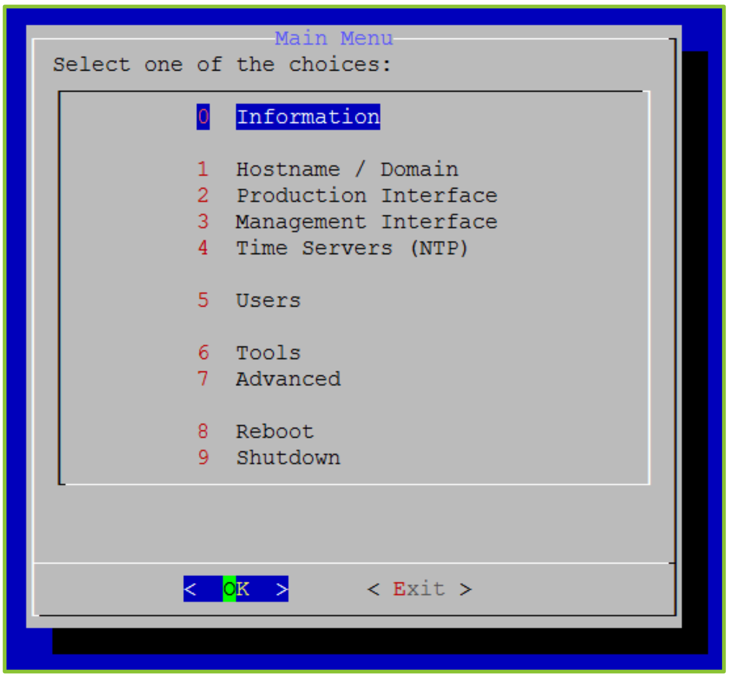
Adding IPv4 Static Routes

To add IPv4 Static Routes:

1. Log in to the System Console.

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

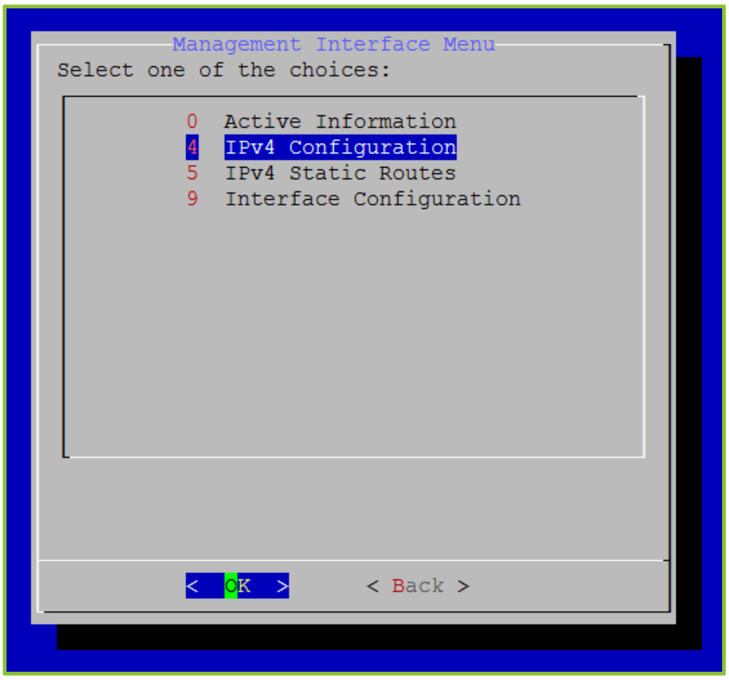
   The Main Menu displays.



```
                    Main Menu
 Select one of the choices:

             0  Information

             1  Hostname / Domain
             2  Production Interface
             3  Management Interface
             4  Time Servers (NTP)

             5  Users

             6  Tools
             7  Advanced

             8  Reboot
             9  Shutdown

            <  OK  >       < Exit >
```

2. Enter **3** to select the Management Interface option.
3. Press the **Enter** key to select **OK**.

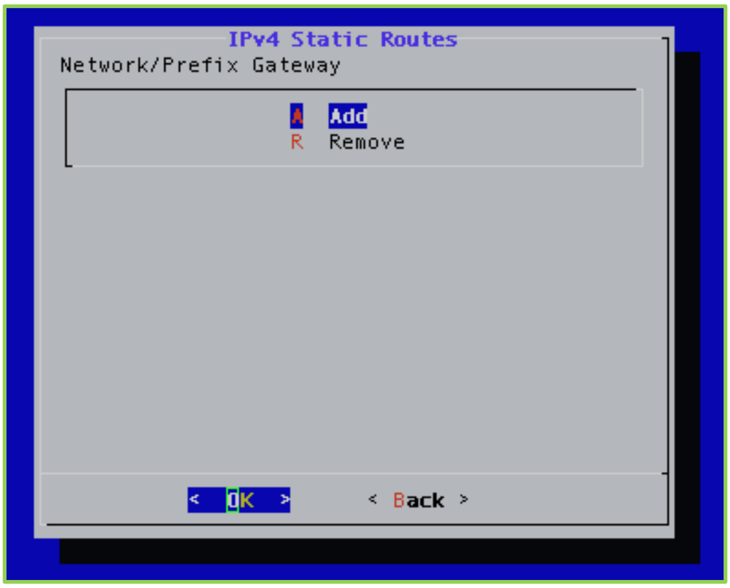
The Management Interface Menu displays.



```
Management Interface Menu
Select one of the choices:

          0  Active Information
          4  IPv4 Configuration
          5  IPv4 Static Routes
          9  Interface Configuration

        <  OK  >        < Back >
```

4. Enter **5** to select the IPv4 Static Routes option.
5. Press the Enter key to select OK.

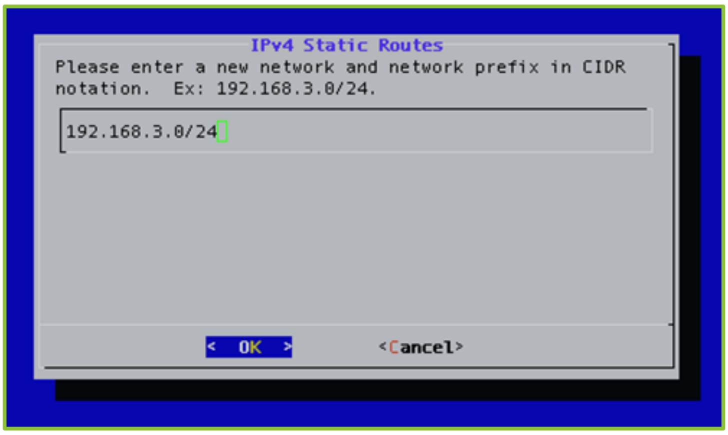
   The *IPv4 Static Routes* window displays.



```
IPv4 Static Routes
Network/Prefix Gateway

            A  Add
            R  Remove

        <  OK  >        < Back >
```

6. Enter **A** to select the Add option.
7. Press the Enter key to select OK.

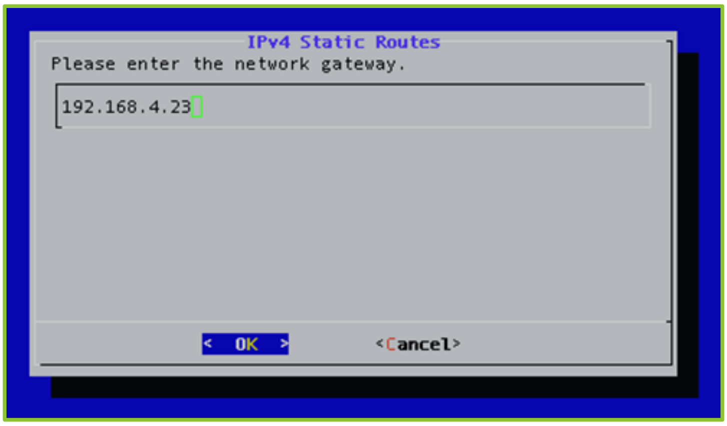
The *IPv4 Static Routes* window displays.



IPv4 Static Routes

```
Please enter a new network and network prefix in CIDR
notation.  Ex: 192.168.3.0/24.

192.168.3.0/24
```

8. Enter a new network with the prefix in CIDR notation (e.g., 192.168.3.0/24).
9. Press the Enter key to select OK.
10. Enter a new network gateway.

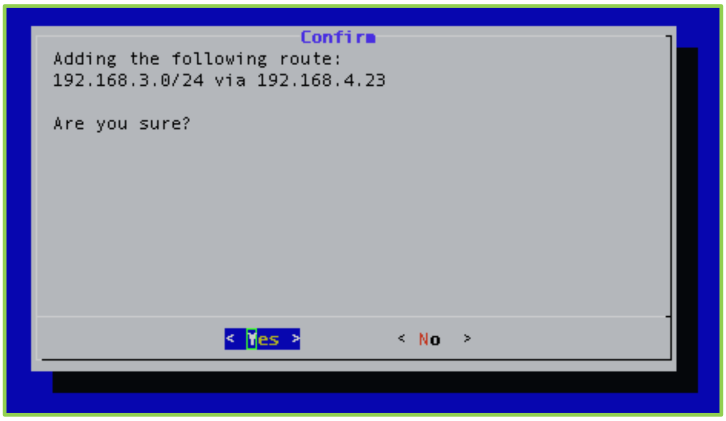


IPv4 Static Routes

```
Please enter the network gateway.

192.168.4.23
```

11. Press the Enter key to select OK.

The *Confirm* window displays.



Confirm

```
Adding the following route:
192.168.3.0/24 via 192.168.4.23

Are you sure?
```

12. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

13. Press the **Enter** key to select **OK**.

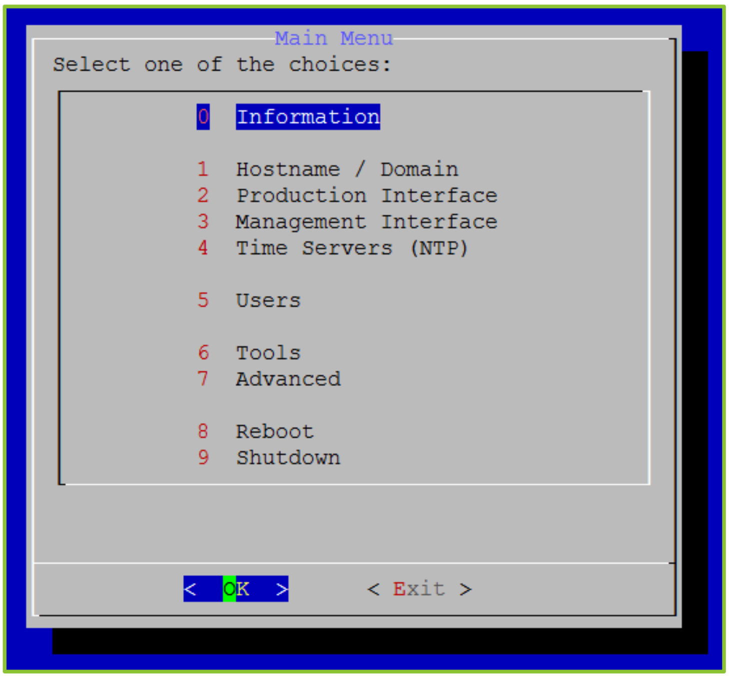
Removing IPv4 Static Routes

To remove IPv4 static routes:

1. Log in to the System Console.

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

   The Main Menu displays.

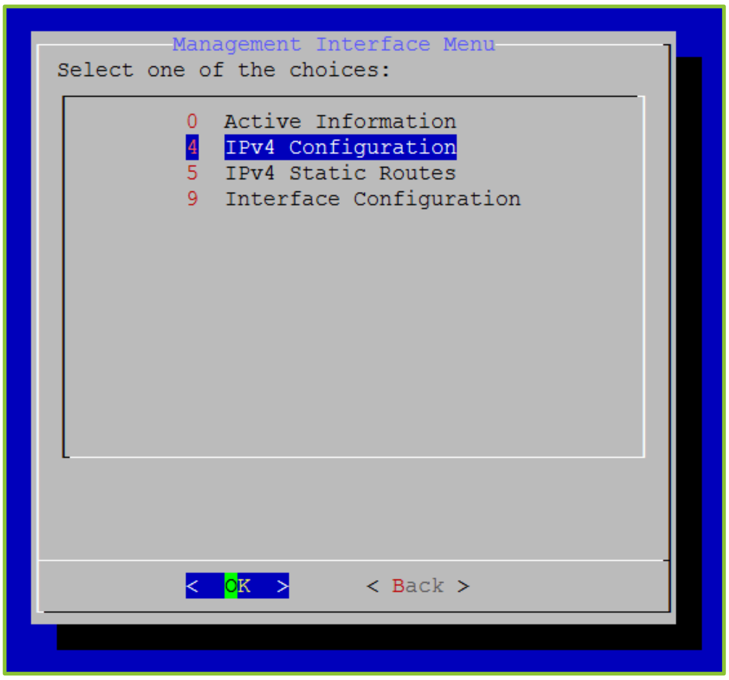


```
                    Main Menu
 Select one of the choices:

            0  Information

            1  Hostname / Domain
            2  Production Interface
            3  Management Interface
            4  Time Servers (NTP)

            5  Users

            6  Tools
            7  Advanced

            8  Reboot
            9  Shutdown


          <  OK  >        < Exit >
```

2. Enter **3** to select the Management Interface option.

3. Press the **Enter** key to select **OK**.

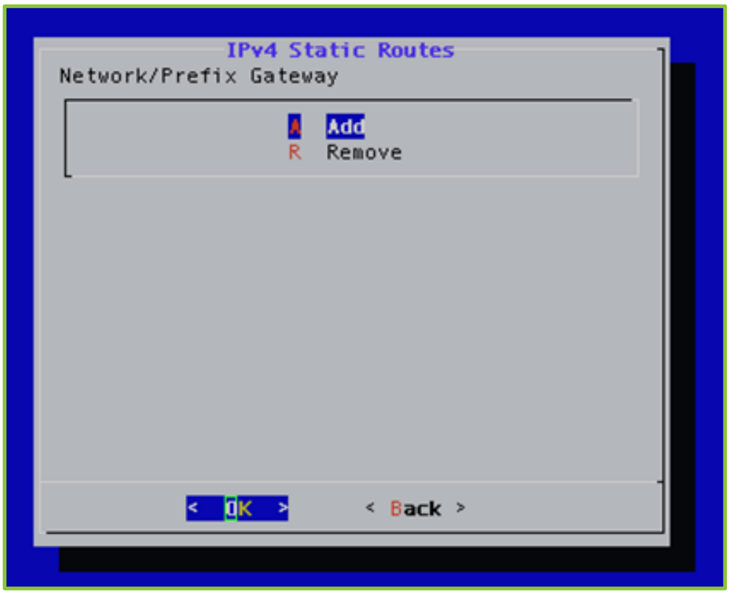
The Management Interface Menu displays.



```
Management Interface Menu
Select one of the choices:

        0  Active Information
        4  IPv4 Configuration
        5  IPv4 Static Routes
        9  Interface Configuration

     <  OK  >        < Back >
```

4. Enter **5** to the IPv4 Static Routes option.
5. Press the Enter key to select OK.

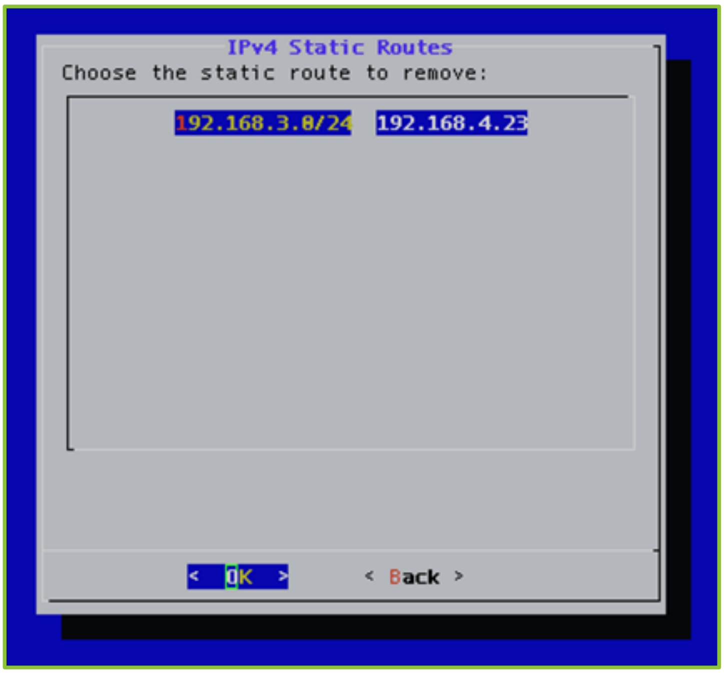
   The *IPv4 Static Routes* window displays.



```
IPv4 Static Routes
Network/Prefix Gateway

           A  Add
           R  Remove

     <  OK  >        < Back >
```

6. Enter **R** to select the Remove option.
7. Press the Enter key to select OK.

The *IPv4 Static Routes* window displays.



```
IPv4 Static Routes
Choose the static route to remove:
192.168.3.0/24  192.168.4.23
```

8. Select the static route to remove.
9. Press the **Enter** key to select **OK**.

   The *Confirm* window displays.
10. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
11. Press the **Enter** key to select **OK**.

Configuring the MTU and Auto Negotiation for the Management Interface

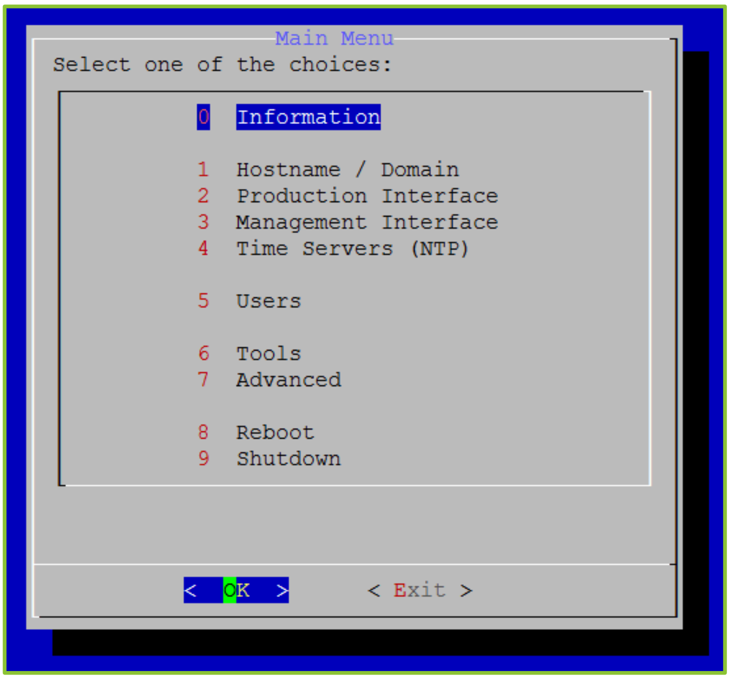
Configuring the Maximum Transmission Unit (MTU)

To configure the Maximum Transmittion Unit (MTU):

1. Log in to the System Console.

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

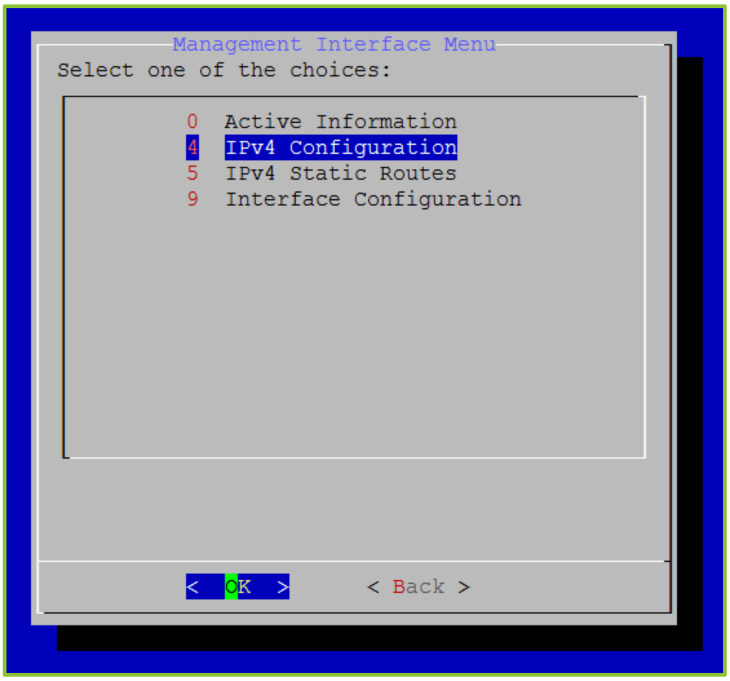
The Main Menu displays.



```
Main Menu
Select one of the choices:

          0   Information

          1   Hostname / Domain
          2   Production Interface
          3   Management Interface
          4   Time Servers (NTP)

          5   Users

          6   Tools
          7   Advanced

          8   Reboot
          9   Shutdown

       <  OK  >       < Exit >
```

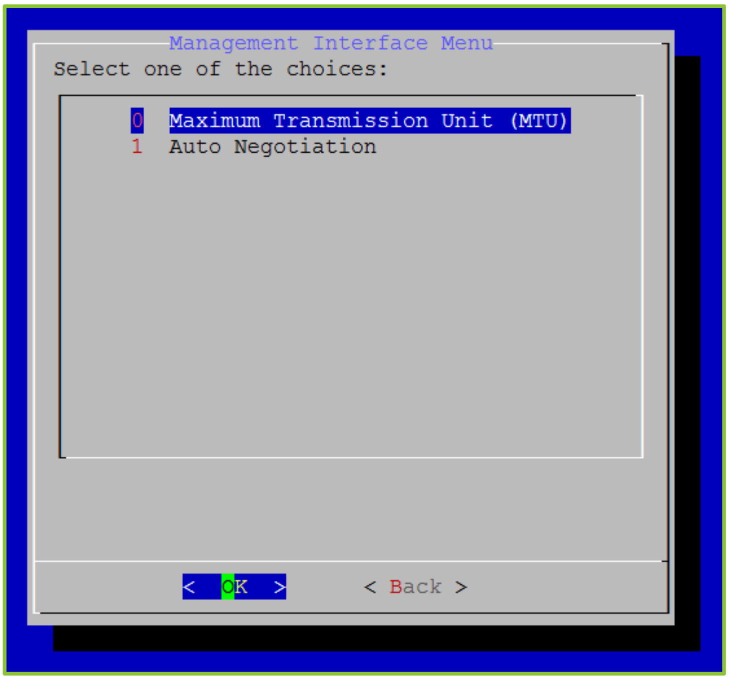
2. Enter **3** to select the Management Interface option.
3. Press the Enter key to select OK.

The Management Interface Menu displays.



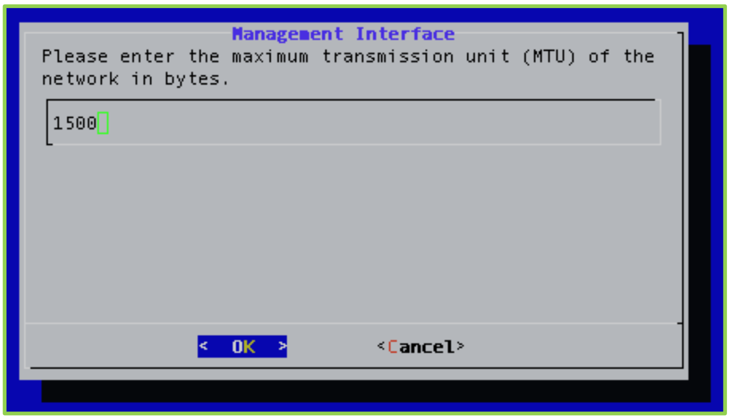
```
Management Interface Menu
Select one of the choices:

          0   Active Information
          4   IPv4 Configuration
          5   IPv4 Static Routes
          9   Interface Configuration

       <  OK  >       < Back >
```

4. Enter **9** to select the Interface Configuration option.
5. Press the Enter key to select OK.



```
Management Interface Menu
Select one of the choices:

      0   Maximum Transmission Unit (MTU)
      1   Auto Negotiation
```

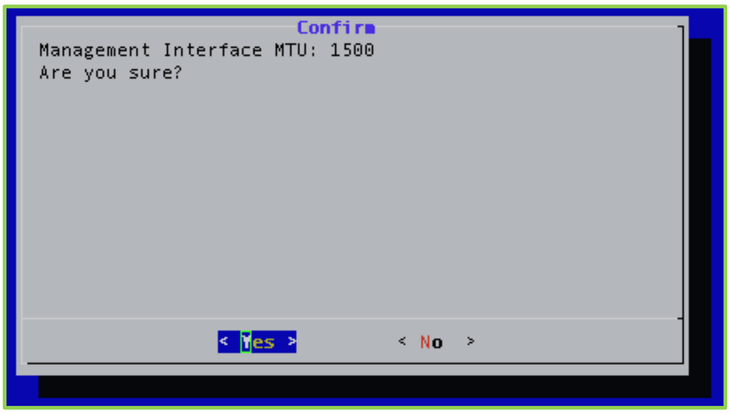
6. Enter 0 to select the Maximum Transmission Unit (MTU) option.
7. Press the Enter key to select OK.
8. Enter the MTU of the networks in bytes.



```
Management Interface
Please enter the maximum transmission unit (MTU) of the
network in bytes.

1500
```

9. Press the Enter key to select OK.

A *Confirm* window displays.



```
Confirm
Management Interface MTU: 1500
Are you sure?
```

10. Press the **Enter** key to select **Yes**.

    A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”

11. Press the **Enter** key to select **OK**.

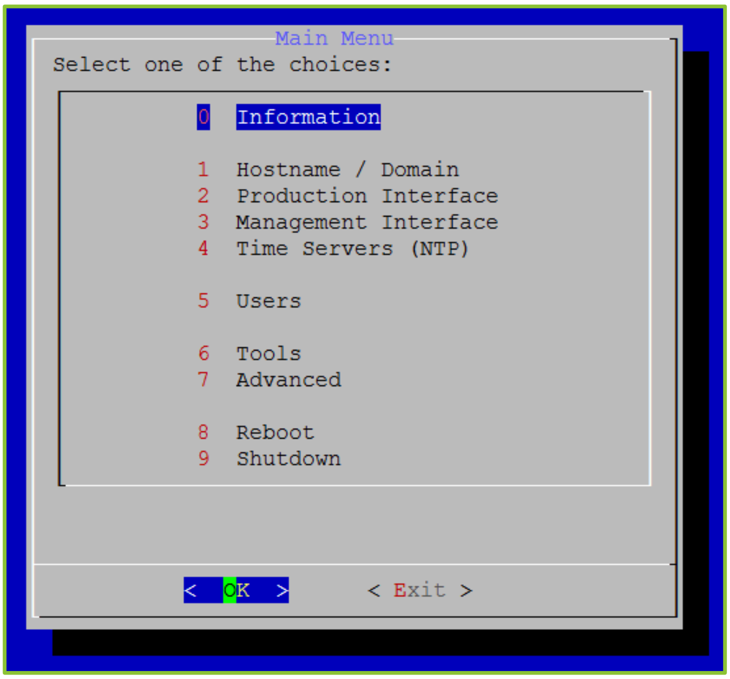
Configuring Auto Negotiation

To configure auto negotiation:

1. Log in to the System Console.

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

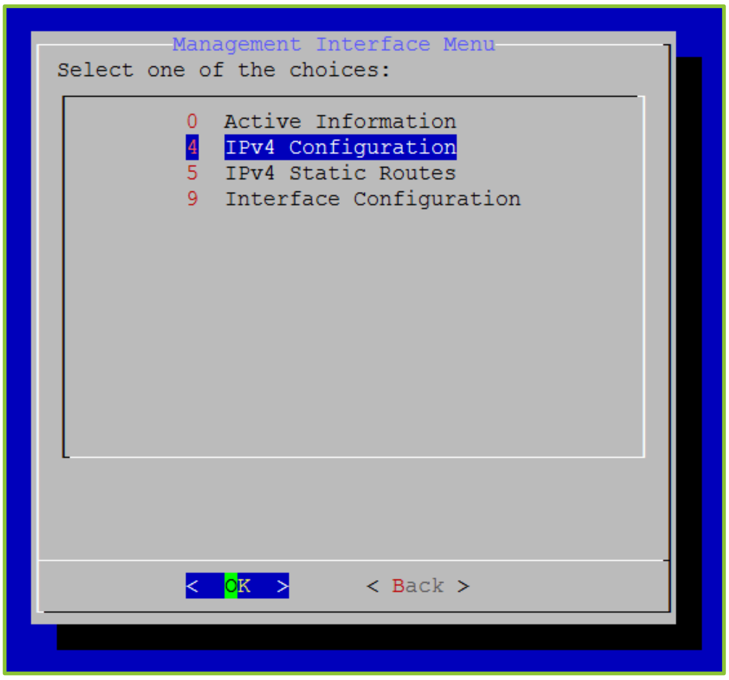
The Main Menu displays.



```
Main Menu
Select one of the choices:

            0   Information

            1   Hostname / Domain
            2   Production Interface
            3   Management Interface
            4   Time Servers (NTP)

            5   Users

            6   Tools
            7   Advanced

            8   Reboot
            9   Shutdown

          <  OK  >        < Exit >
```

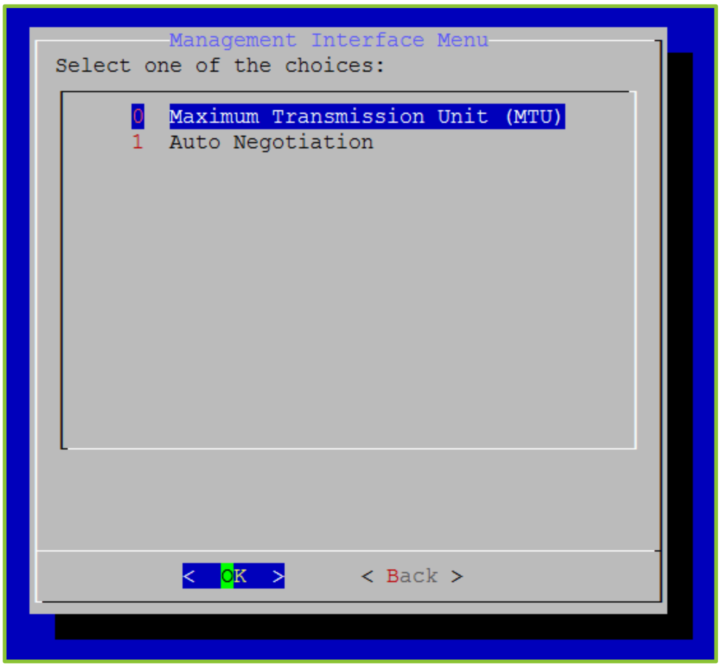
2. Enter **3** to select the Management Interface option.
3. Press the Enter key to select OK.

The Management Interface Menu displays.



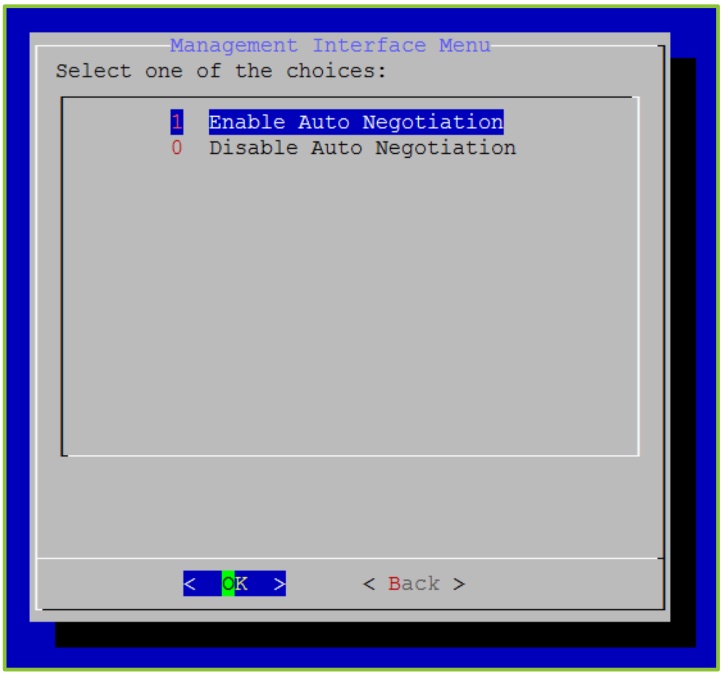
```
Management Interface Menu
Select one of the choices:

           0   Active Information
           4   IPv4 Configuration
           5   IPv4 Static Routes
           9   Interface Configuration

         <  OK  >        < Back >
```

4. Enter **9** to select the Interface Configuration option.
5. Press the Enter key to select OK.



```
Management Interface Menu
Select one of the choices:

      0  Maximum Transmission Unit (MTU)
      1  Auto Negotiation
```

6. Enter **1** to select the Auto Negotiation option.
7. Press the Enter key to select OK.



```
Management Interface Menu
Select one of the choices:

         1  Enable Auto Negotiation
         0  Disable Auto Negotiation
```

8. Enter **1** to enable Auto Negotiation or enter **0** to disable Auto Negotiation.

A *Confirm* window displays.

9. Press the **Enter** key to select **Yes**.

   A message displays stating "Changes saved. Reboot REQUIRED for changes to take effect."

10. Press the **Enter** key to select **OK**.

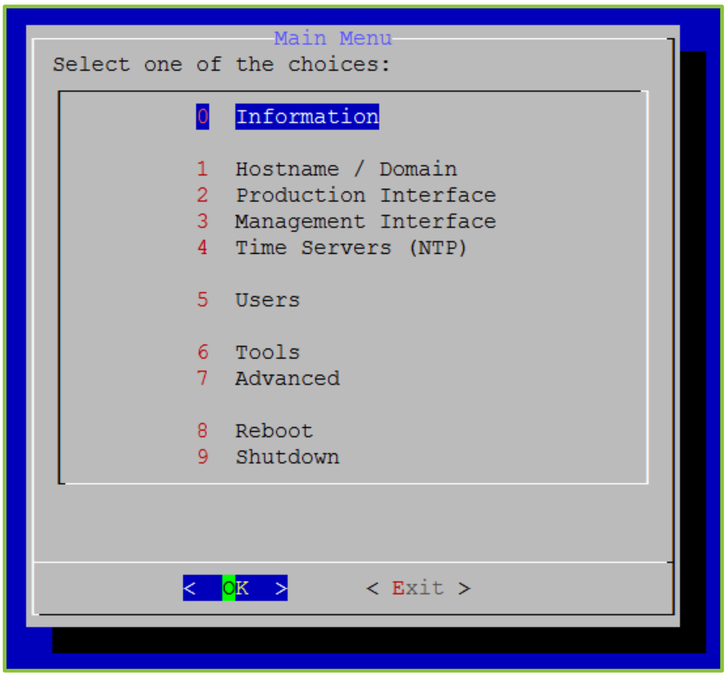
Configuring Time Servers (NTP)

To configure time servers (NTP):

1. Log in to the System Console.

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

   The Main Menu displays.



```
Main Menu
Select one of the choices:

            0   Information

            1   Hostname / Domain
            2   Production Interface
            3   Management Interface
            4   Time Servers (NTP)

            5   Users

            6   Tools
            7   Advanced

            8   Reboot
            9   Shutdown

        <  OK  >        < Exit >
```

2. Enter **4** to select the Time Servers (NTP) option.

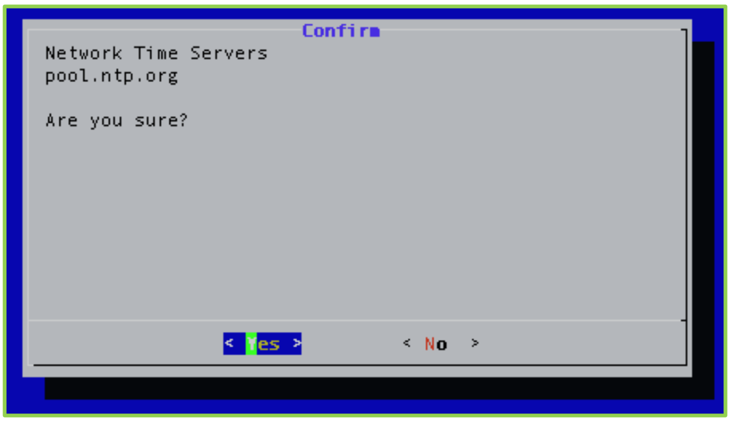
3. Press the **Enter** key to select **OK**.

   If you have DHCP configured, a message displays stating "The nameservers configured by DHCP take priority over the values configured here" and you must press the **Enter** key to select **OK**.

4. Enter up to three network time servers separated by a space (e.g., pool.ntp.org).

5. Press the **Enter** key to select **OK**.

A *Confirm* window displays.



```
Network Time Servers
pool.ntp.org

Are you sure?
```

6. Press the **Enter** key to select **Yes**.

   A message displays stating “Sync time with timeservers now? Timeservers must be reachable. Are you sure?”

7. Press the **Enter** key to select **OK**.

   A message displays stating “System time updated.”

Configuring Users

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

The System Console allows for the creation of up to ten System Console user accounts.

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 meet password complexity requirements.

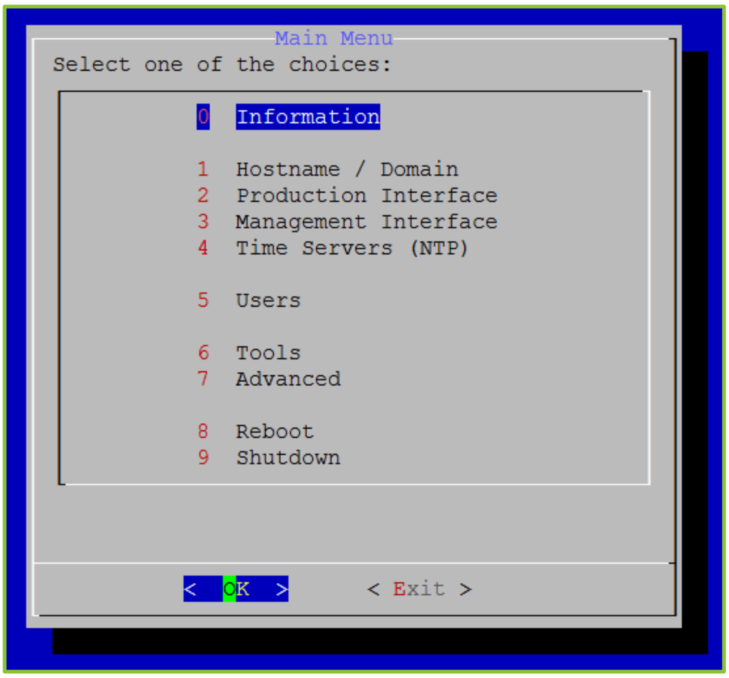
Viewing Active User Information

To view active user information:

1. Log in to the System Console.

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

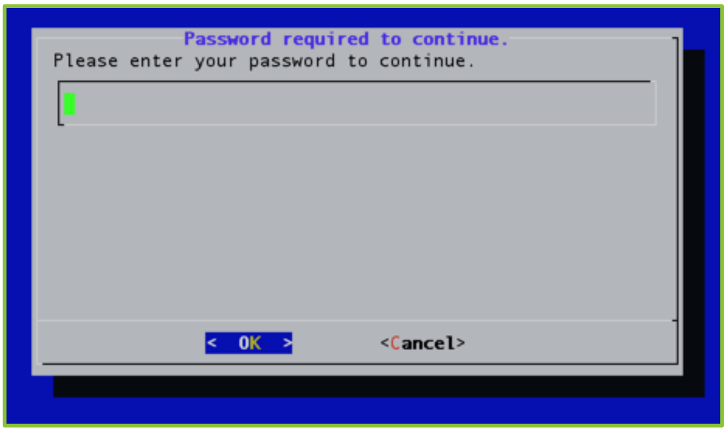
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

          <  OK  >        < Exit >
```

2. Enter **5** to select the Users option.
3. Press the Enter key to select OK.

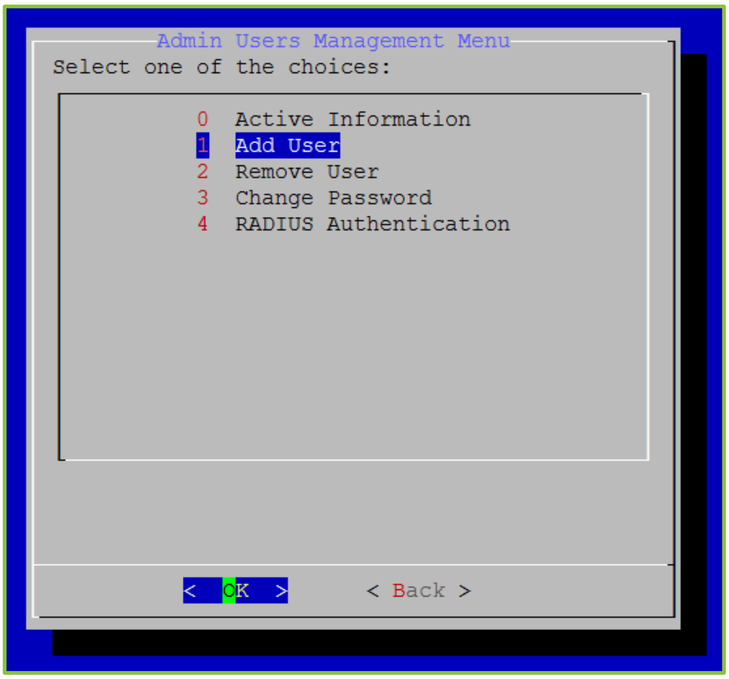
   The *Password required to continu*e window displays.



```
Password required to continue.
Please enter your password to continue.

          <  OK  >        <Cancel>
```

4. Enter your password.
5. Press the Enter key to select OK.

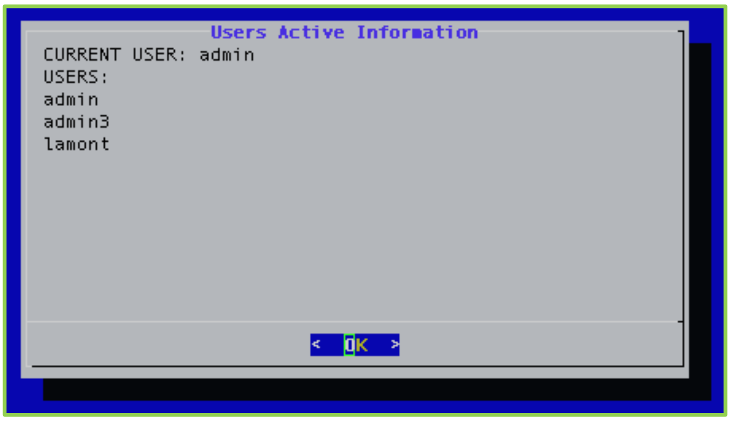
The Admin Users Management Menu displays.



```
Admin Users Management Menu
Select one of the choices:

    0  Active Information
    1  Add User
    2  Remove User
    3  Change Password
    4  RADIUS Authentication

      <  OK  >        < Back >
```

6. Enter **0** to select the Active Information option.
7. Press the **Enter** key to select **OK**.

   The *Users Active Information* window displays.



```
Users Active Information
CURRENT USER: admin
USERS:
admin
admin3
lamont

              <  OK  >
```

8. Press the **Enter** key to select **OK**.

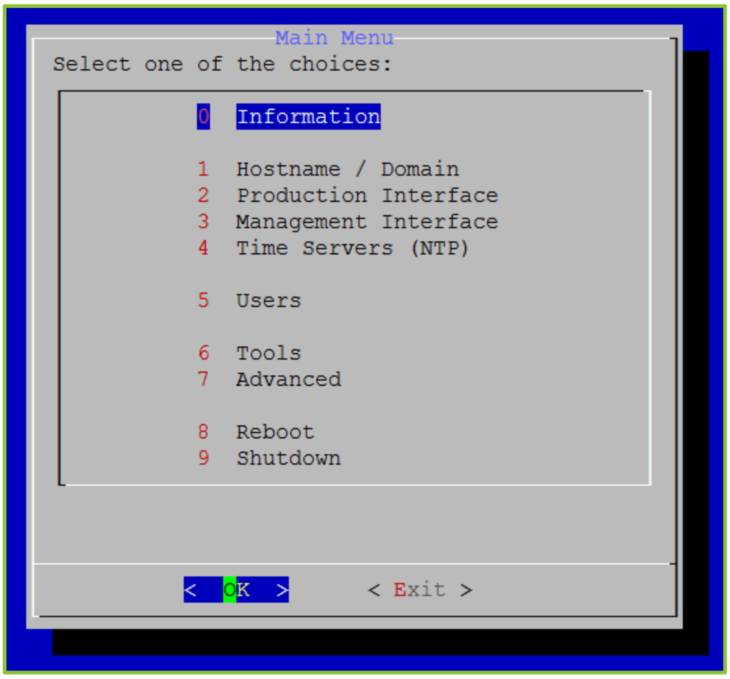
Adding Users

To add users:

1. Log in to the System Console.

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

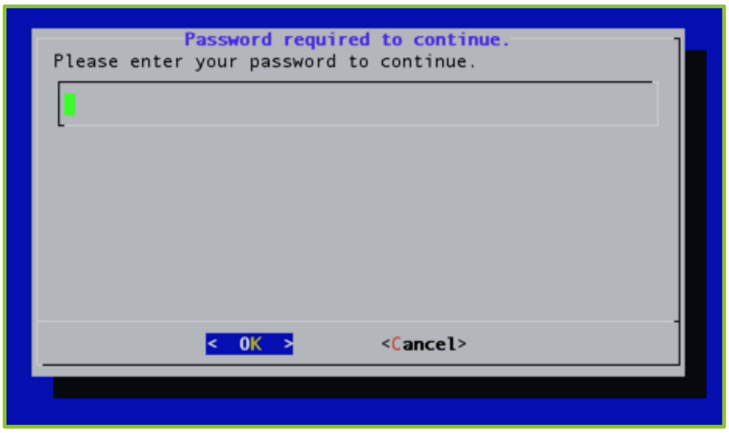
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

     <  OK  >        < Exit >
```

2. Enter **5** to select the Users option.
3. Press the Enter key to select OK.

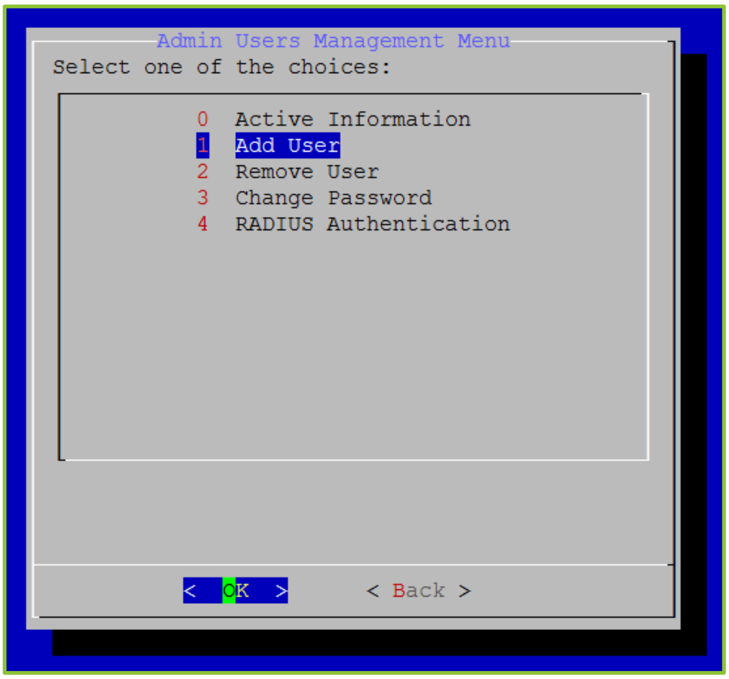
   The *Password required to continue* window displays.



```
Password required to continue.
Please enter your password to continue.

     <  OK  >        <Cancel>
```

4. Enter your password.
5. Press the Enter key to select OK.

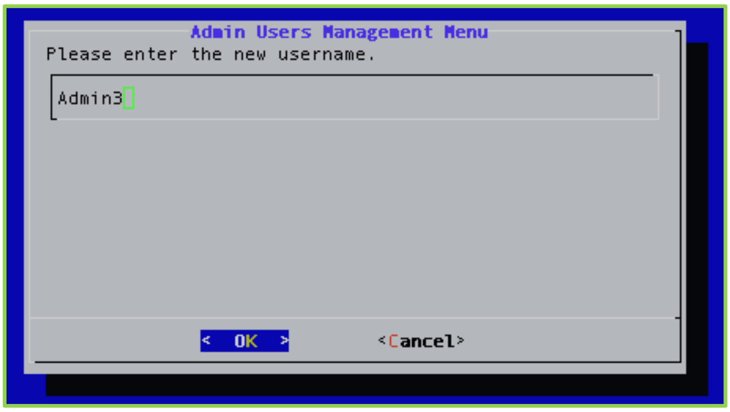
The Admin Users Management Menu displays.



```
Admin Users Management Menu
Select one of the choices:

          0  Active Information
          1  Add User
          2  Remove User
          3  Change Password
          4  RADIUS Authentication

     <  OK  >        < Back >
```

6. Enter **1** to select the Add Users option.

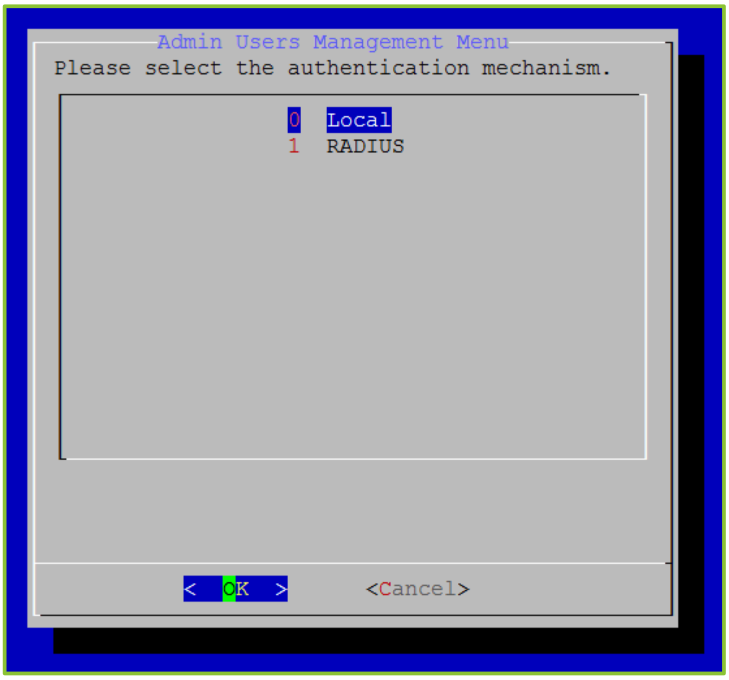
7. Press the Enter key to select OK.



```
Admin Users Management Menu
Please enter the new username.
Admin3

     <  OK  >        <Cancel>
```

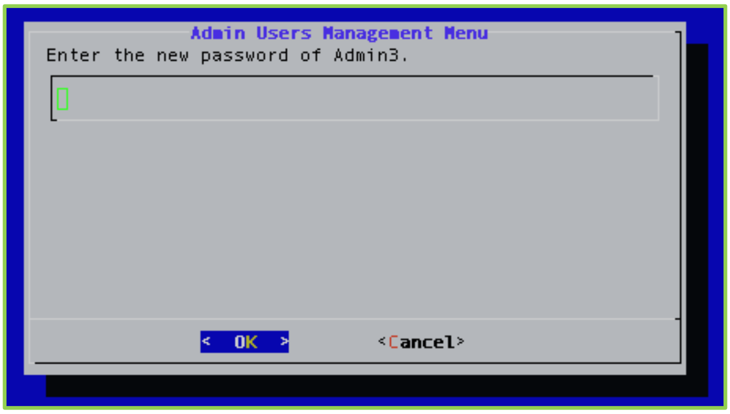
8. Enter the user name of the user you are adding.

9. Press the **Enter** key to select **OK**.
10. Enter **0** to select the Local option.



```
Admin Users Management Menu
Please select the authentication mechanism.

          0  Local
          1  RADIUS

        <  OK  >        <Cancel>
```

11. Press the **Enter** key to select **OK**.
12. Enter the password of the user you are adding.



```
Admin Users Management Menu
Enter the new password of Admin3.

        <  OK  >        <Cancel>
```

Enter a unique password that follows these password complexity requirements:

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.

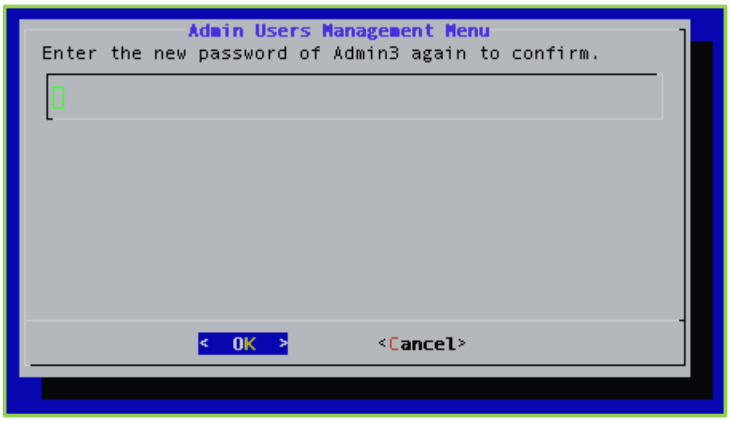
  The default setting is at least three characters should be different from the old password.

- 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 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.

13. Press the **Enter** key to select **OK**.



```
Admin Users Management Menu
Enter the new password of Admin3 again to confirm.
```

14. Enter the password again to confirm it.

    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 option `3. Change Password`. This functionality is only available for local admin accounts.

For more information, see Changing User Passwords.

15. Press the **Enter** key to select **OK**.

    A message displays stating "[User] has been added."

16. Press the **Enter** key to select **OK**.

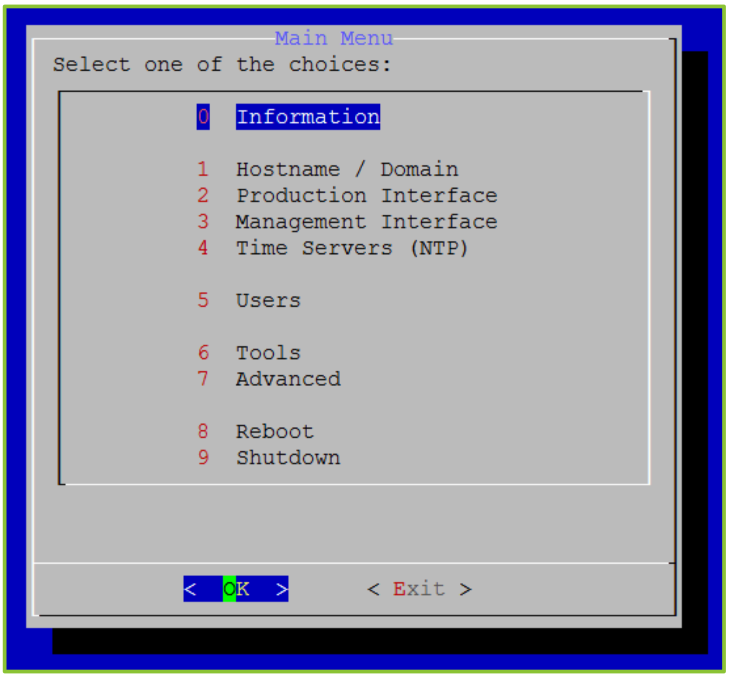
Removing Users

To remove users:

1. Log in to the System Console.

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

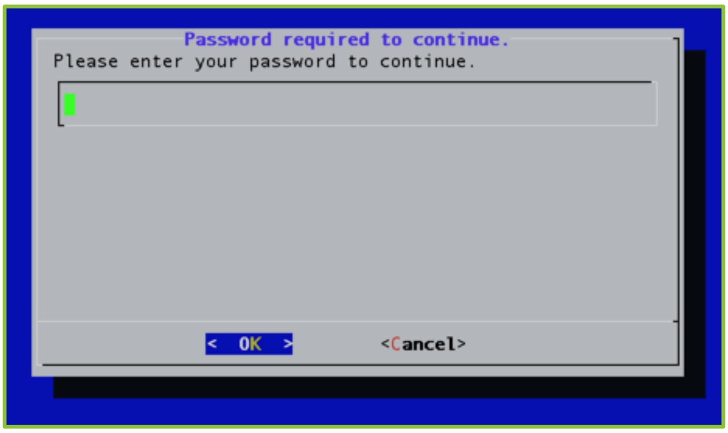
The Main Menu displays.



```
Main Menu
Select one of the choices:

          0  Information

          1  Hostname / Domain
          2  Production Interface
          3  Management Interface
          4  Time Servers (NTP)

          5  Users

          6  Tools
          7  Advanced

          8  Reboot
          9  Shutdown

        <  OK  >        < Exit >
```

2. Enter **5** to select the Users option.
3. Press the Enter key to select OK.

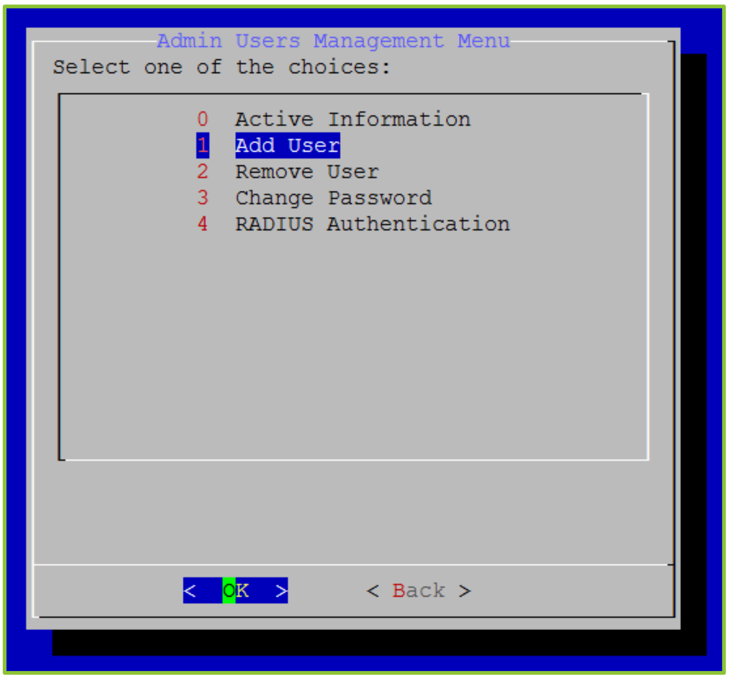
   The *Password required to continue* window displays.



```
Password required to continue.
Please enter your password to continue.

          <  OK  >          <Cancel>
```

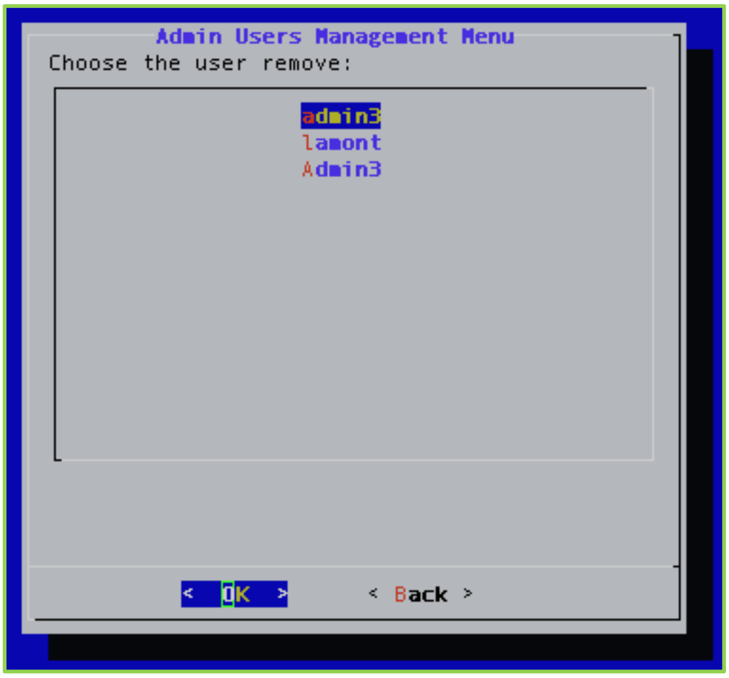
4. Enter your password.
5. Press the Enter key to select OK.

The Admin Users Management Menu displays.



```
Admin Users Management Menu
Select one of the choices:

        0  Active Information
        1  Add User
        2  Remove User
        3  Change Password
        4  RADIUS Authentication

      <  OK  >        < Back >
```

6. Enter **2** to select the Remove Users option.



```
Admin Users Management Menu
Choose the user remove:

             admin3
             lamont
             Admin3

      <  OK  >        < Back >
```

7. Select the user you want to remove.
8. Press the Enter key to select OK.

The *Confirm* window displays.

9. Press the **Enter** key to select **Yes**.

   A message displays stating "[User] has been removed."

10. Press the **Enter** key to select **OK**.

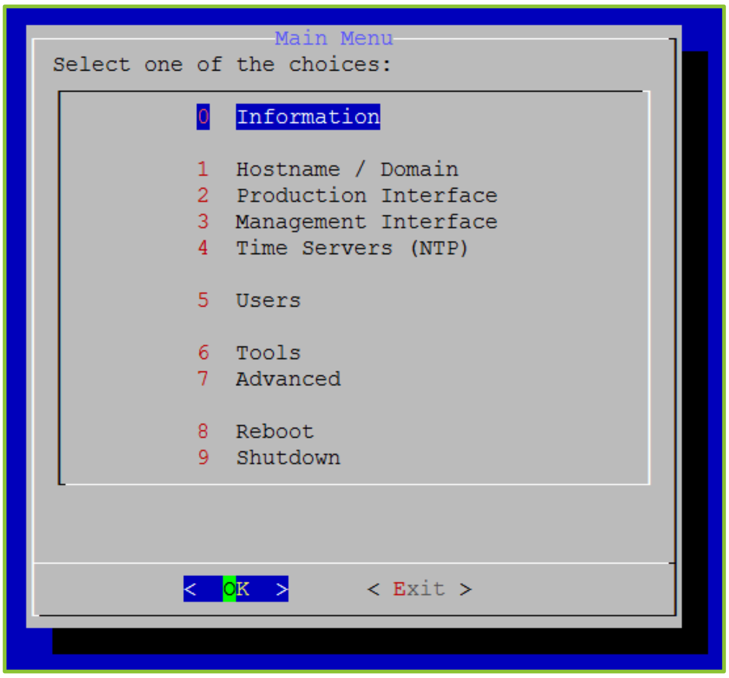
Changing User Passwords

To change user passwords:

1. Log in to the System Console.

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

   The Main Menu displays.

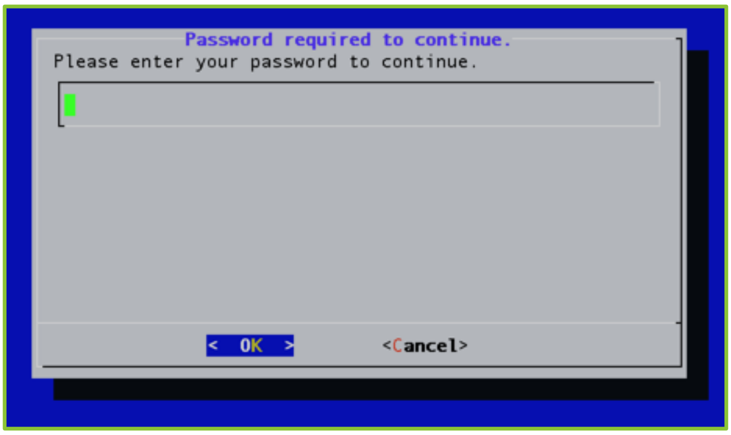


```
Main Menu
Select one of the choices:

         0  Information

         1  Hostname / Domain
         2  Production Interface
         3  Management Interface
         4  Time Servers (NTP)

         5  Users

         6  Tools
         7  Advanced

         8  Reboot
         9  Shutdown

      <  OK  >          < Exit >
```

2. Enter **5** to select the Users option.

3. Press the **Enter** key to select **OK**.

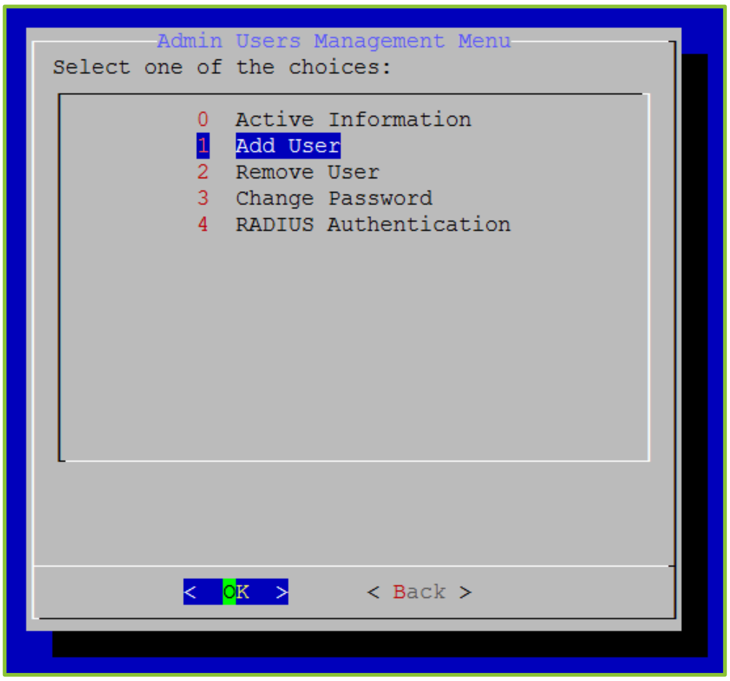
The *Password required to continue* window displays.



```
Password required to continue.
Please enter your password to continue.
```

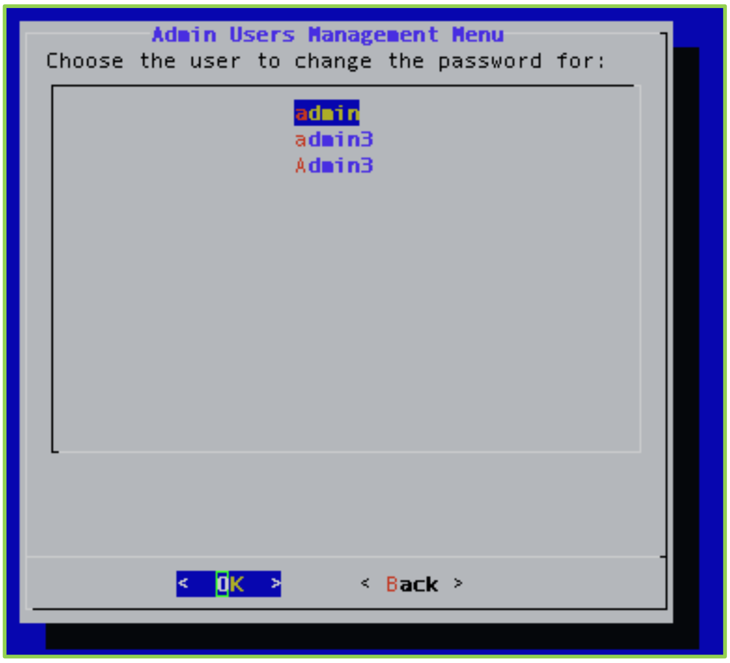
4. Enter your password.
5. Press the **Enter** key to select **OK**.

The Admin Users Management Menu displays.



```
Admin Users Management Menu
Select one of the choices:

0  Active Information
1  Add User
2  Remove User
3  Change Password
4  RADIUS Authentication
```

6. Enter **3** to select the Change Password option.
7. Press the Enter key to select OK.

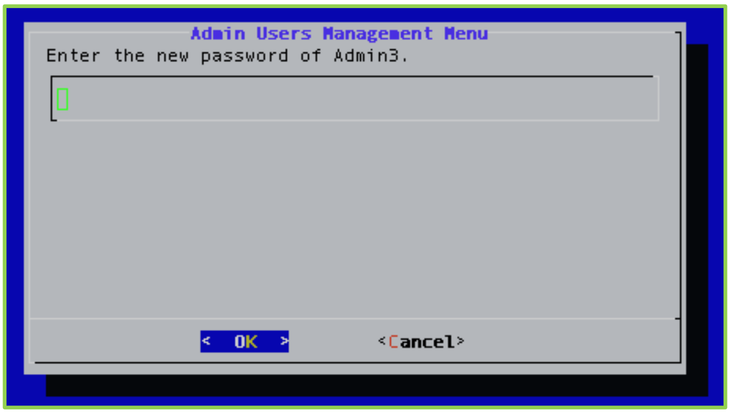


Admin Users Management Menu
Choose the user to change the password for:

admin
admin3
Admin3

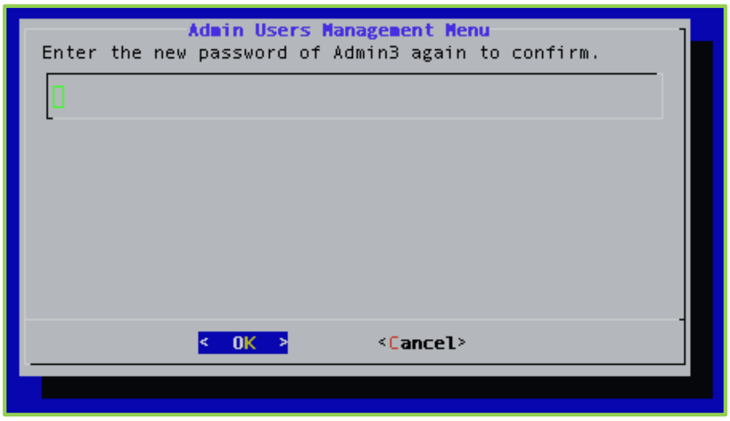
8. Select the user whose password you want to change.
9. Press the Enter key to select OK.

   The *Confirm* window displays.
10. Press the Enter key to select Yes.
11. Enter the new password for the user.



Admin Users Management Menu
Enter the new password of Admin3.

12. Press the **Enter** key to select **OK**.



Admin Users Management Menu

Enter the new password of Admin3 again to confirm.

13. Enter the password again to confirm it.
14. Press the **Enter** key to select **OK**.

    A message displays stating "Password changed for [user]."
15. Press the **Enter** key to select **OK**.

Configuring RADIUS Authentication

For additional information, see 4. Configuring RADIUS.

Accessing Tools

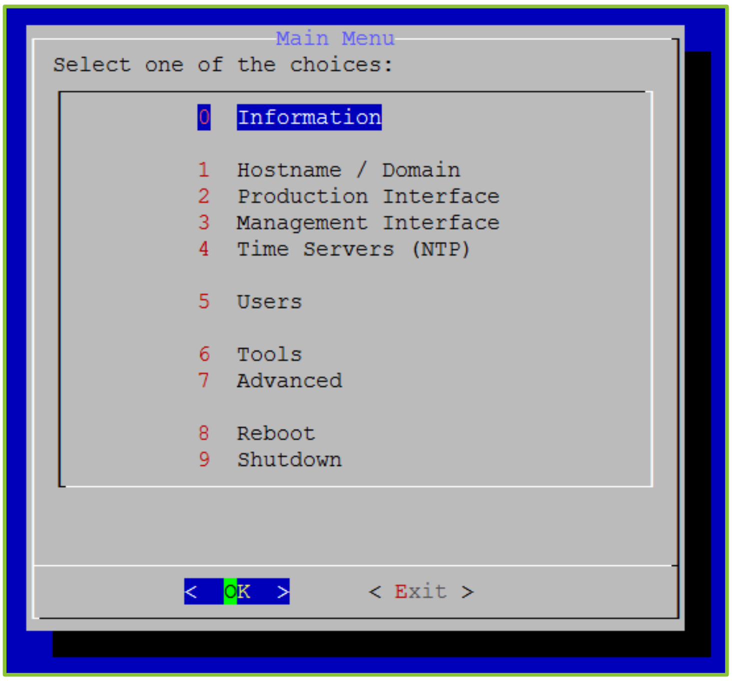
The Tools menu enables you to access the Ping, DNS Lookup, and Traceroute tools.

To access tools:

1. Log in to the System Console.

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

The Main Menu displays.

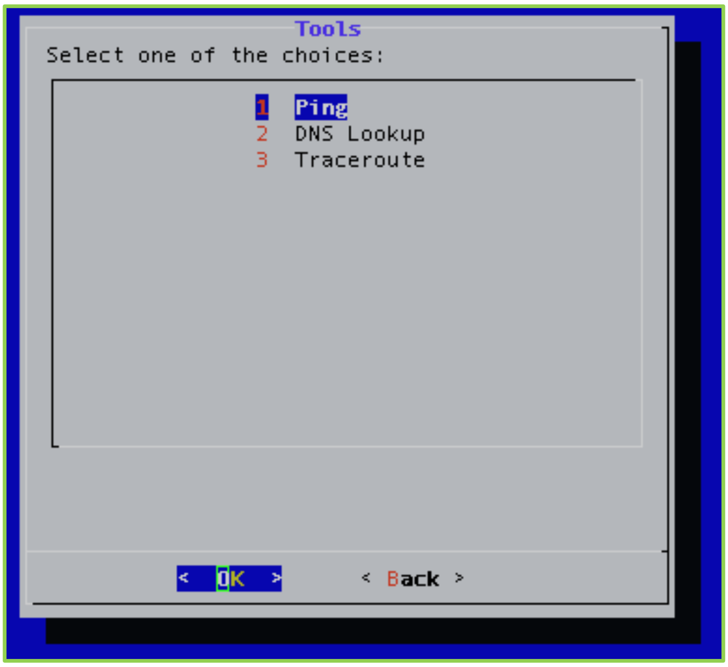


```
                    Main Menu
Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown

         <  OK  >        < Exit >
```

2. Enter **6** to select the Tools option.

3. Press the Enter key to select OK.

The Tools menu displays.



```
                     Tools
Select one of the choices:

                  1  Ping
                  2  DNS Lookup
                  3  Traceroute

         <  OK  >        < Back >
```

4. Do any of the following:
    - Enter **1** to test connectivity to an IP address.
    - Enter **2** to perform a DNS lookup.
    - Enter **3** to perform a traceroute.
5. Press the **Enter** key to select **OK**.

Performing Advanced Configuration

The *Advanced* screen allows adminstrators to perform more advanced configuration functions, such as setting SNMP, taking backups of the system, and reconfiguring SSH ports among others.

Configuring FIPS

FIPS is the Federal Information Processing Standard 140-2. By default, FIPS mode is disabled on your Vidyo server.

FIPS Certified Modules include the following:

- Vidyo's SDK has been FIPS 140-2 validated:

  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm
- Third party applications – Apache, Net-SNMP, OpenSSH, and OpenSSL – have been built using the FIPS-validated OpenSSL module.

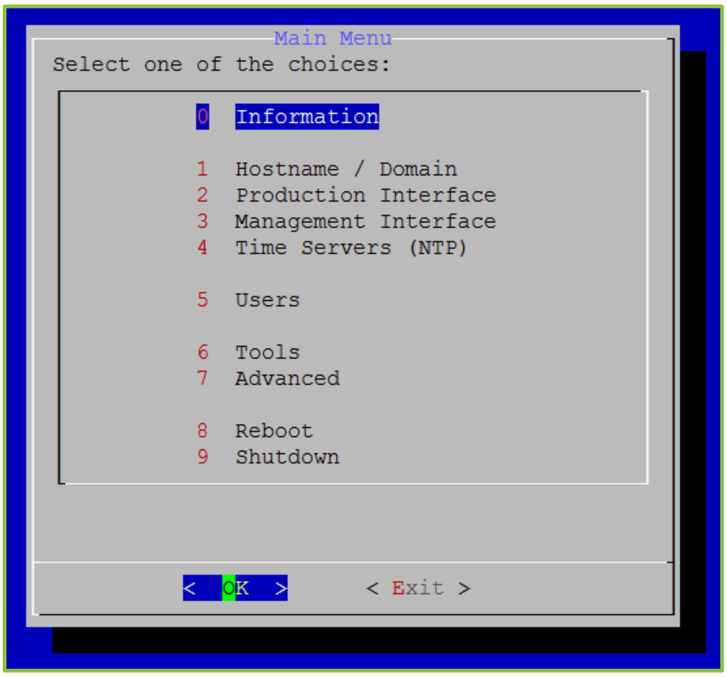
The following steps show you how to enable or disable FIPS mode from the System Console.

To configure FIPS:

1. Log in to the System Console.

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

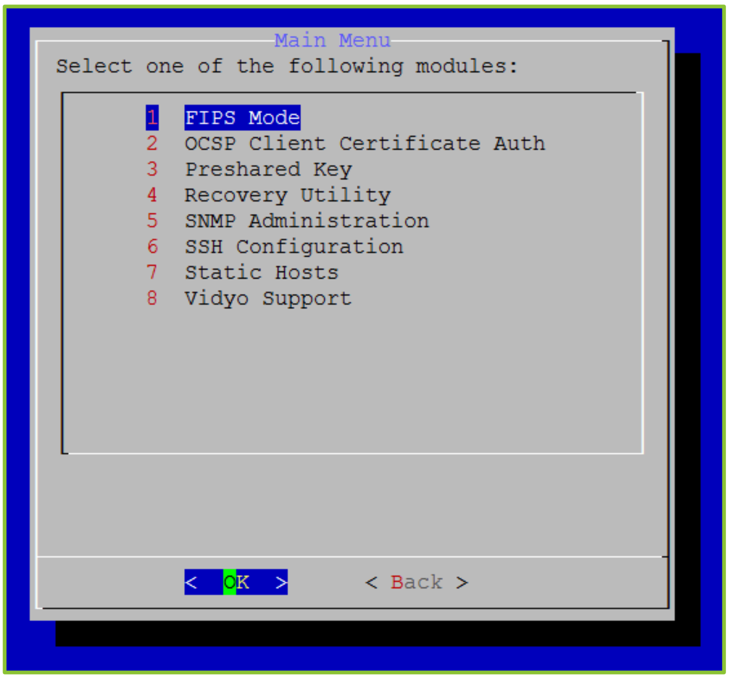
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

     <  OK  >          < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**.

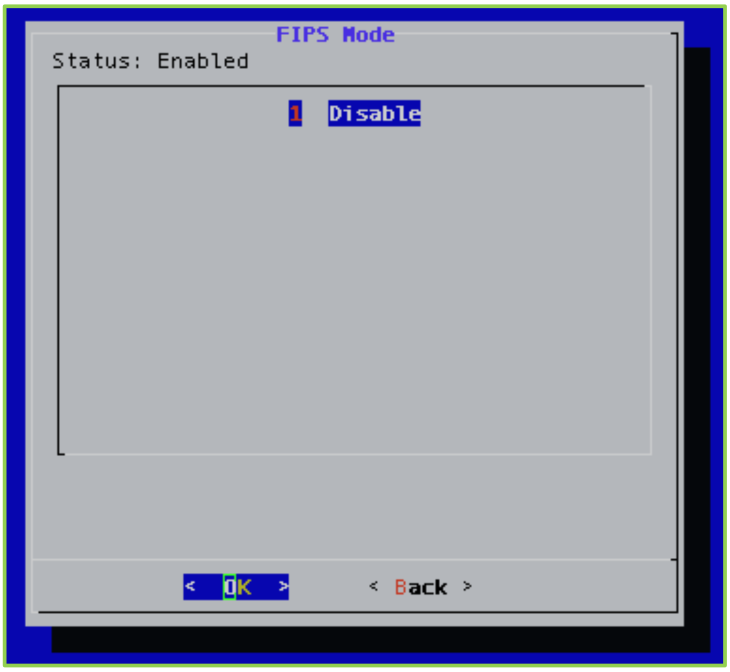
   The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

     1  FIPS Mode
     2  OCSP Client Certificate Auth
     3  Preshared Key
     4  Recovery Utility
     5  SNMP Administration
     6  SSH Configuration
     7  Static Hosts
     8  Vidyo Support

     <  OK  >          < Back >
```

4. Enter **1** to select the FIPS Mode option.
5. Press the Enter key to select OK.

   The *FIPS Mode* window displays. The administrator can view the current status of FIPS mode in the system and toggle the state. If FIPS is enabled, the window includes the **Disable** option only; if FIPS is disabled, the window includes the **Enable** option only.



FIPS Mode

Status: Enabled

1 Disable

6. Enter **1** to select **Disable** or enter **2** to select **Enable**.
7. Press the Enter key to select OK.

   When your system comes back online, FIPS is then disabled (or enabled) on your Vidyo server.

Note When FIPS is enabled, the *SIP* tab in the VidyoGateway Admin Portal contains Address and Port fields. However, when FIPS is disabled, the *SIP* tab contains Address, Port, Username, Password, and Confirm Password fields. For more information, see Configuring SIP Settings.

Maintaining Pre-shared Keys

An encrypted communication channel is established between the active cluster controller and each node on port 49999. The channel is authenticated using a pre-shared key. Your system comes with a default pre-shared key, but allows you to generate a unique pre-shared key for your cluster if desired.

Use the following steps to configure the pre-shared key in a VidyoGateways cluster configuration:

1. Generate the pre-shared key from the Active Controller.

   For more information, see Generating a Pre-shared Key.

2. Export the pre-shared key from the Active Controller.

   For more information, see Exporting a Pre-shared Key.

3. Import the pre-shared key to the Standby Controller and Cluster Nodes.

   For more information, see Importing a Pre-shared Key.

   After generating and exporting the pre-shared key from the Active Controller in your VidyoGateway cluster configuration, you then import the key to your Standby Controller and Cluster Nodes.

Generating a Pre-shared Key

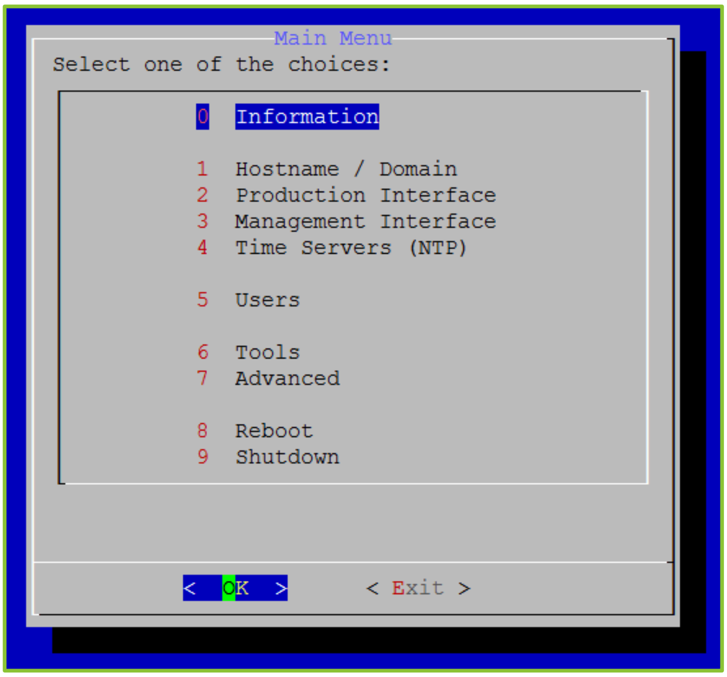
When initially setting up a VidyoGateway cluster, it is recommended to generate a unique pre-shared key from your Active Controller.

To generate a pre-shared key:

1. Log in to the System Console.

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

   The Main Menu displays.

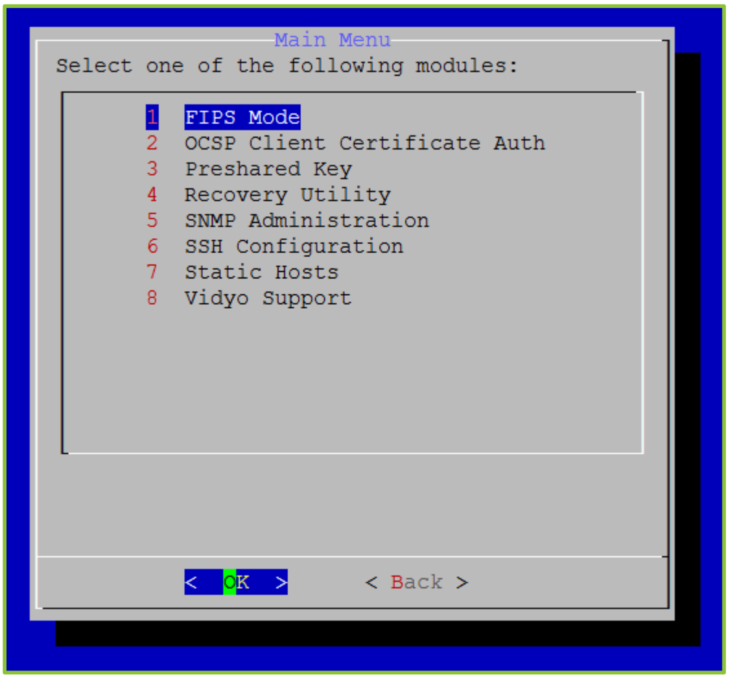


```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

      <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.

3. Press the **Enter** key to select **OK**.

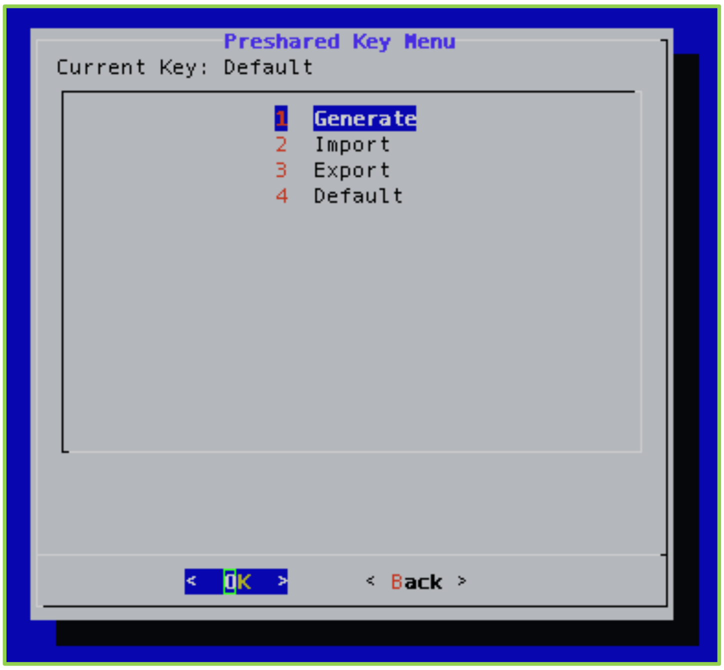
   The Main Menu for the Advanced configuration displays.



```
                    Main Menu
Select one of the following modules:

      1   FIPS Mode
      2   OCSP Client Certificate Auth
      3   Preshared Key
      4   Recovery Utility
      5   SNMP Administration
      6   SSH Configuration
      7   Static Hosts
      8   Vidyo Support

         <  OK  >          < Back >
```

4. Enter **3** to select the Preshared Key option.
5. Press the **Enter** key to select **OK**.

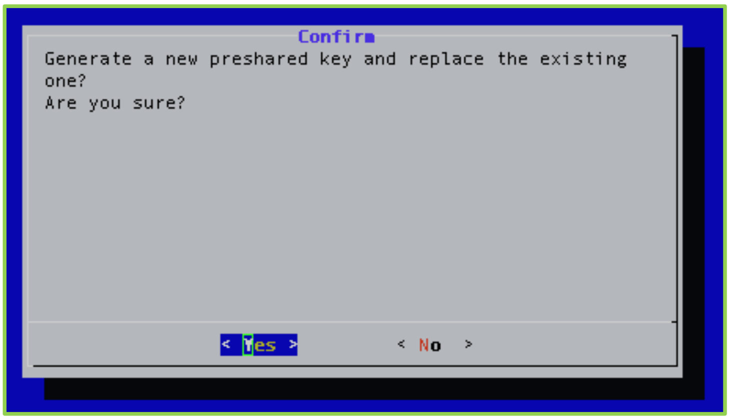
   The Preshared Key Menu displays.



```
                 Preshared Key Menu
Current Key: Default

                  1   Generate
                  2   Import
                  3   Export
                  4   Default

         <  OK  >          < Back >
```

6. Enter **1** to select the Generate option.
7. Press the **Enter** key to select **OK**.

   The *Confirm* window displays.



Confirm

```
Generate a new preshared key and replace the existing
one?
Are you sure?
```

8. Press the **Enter** key to select **Yes**.

   A message displays stating "New preshared key generated. Hash: [key]."
9. Press the **Enter** key to select **OK**.

   You can now export the pre-shared key.

Exporting a Pre-shared Key

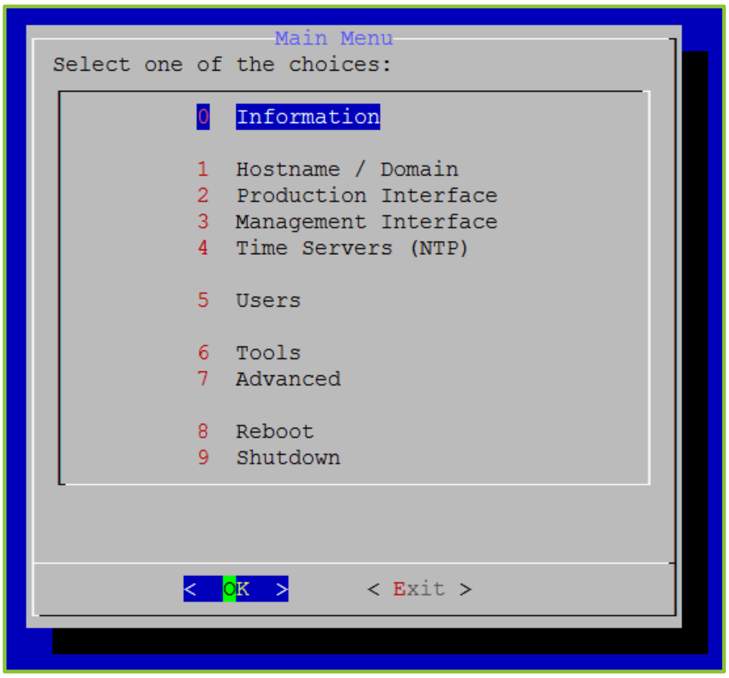
After generating the pre-shared key on the Active Controller in your VidyoGateway cluster configuration, you then export the key from the same server. For more information about clusters, see Configuring Access Control Settings.

To export a pre-shared key:

1. Log in to the System Console.

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

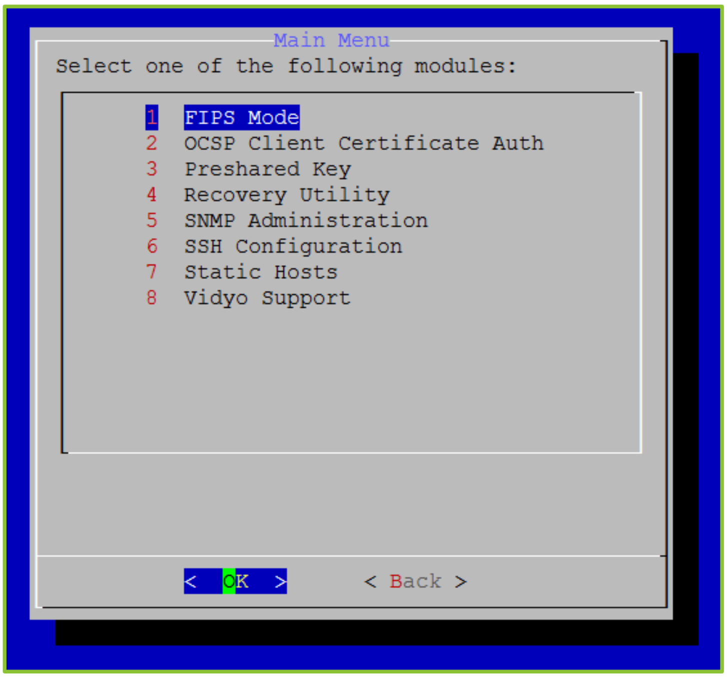
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

      <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

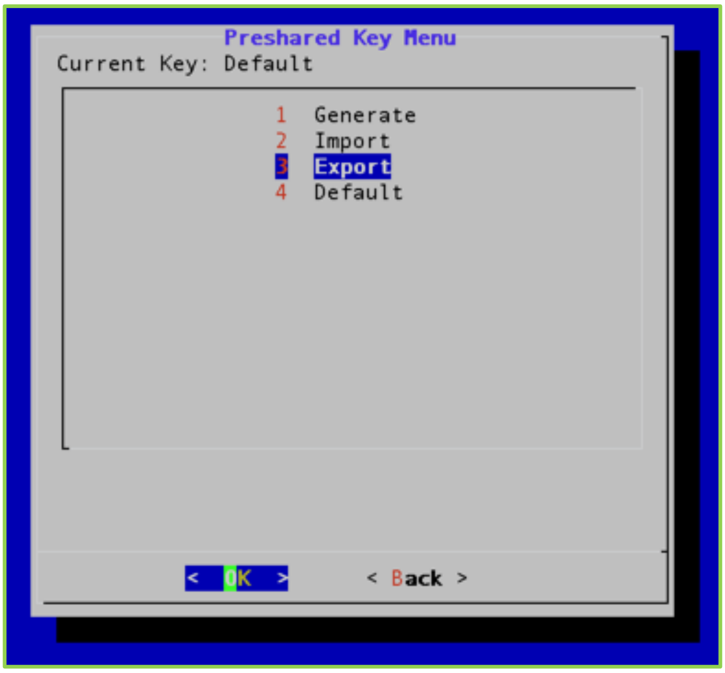
   The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

     1  FIPS Mode
     2  OCSP Client Certificate Auth
     3  Preshared Key
     4  Recovery Utility
     5  SNMP Administration
     6  SSH Configuration
     7  Static Hosts
     8  Vidyo Support

      <  OK  >        < Back >
```

4. Enter **3** to select the Preshared Key option.
5. Press the **Enter** key to select **OK**.

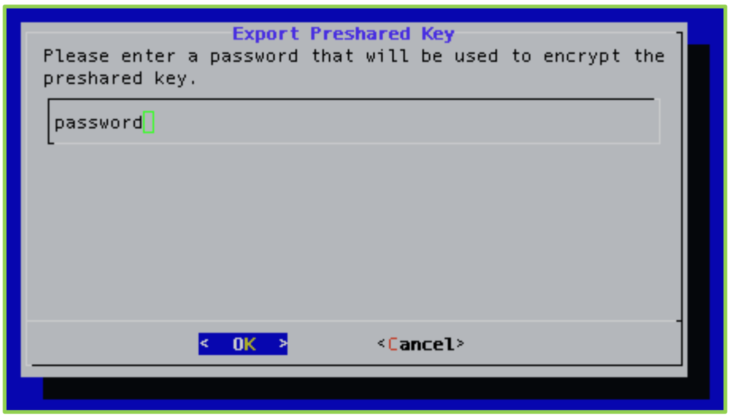
   The Preshared Key Menu displays.



Current Key: Default

6. Enter **3** to select the Export option.
7. Press the **Enter** key to select **OK**.

   The *Export Preshared Key* window displays.

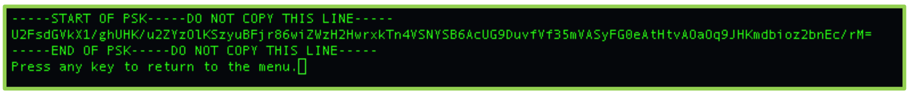


Please enter a password that will be used to encrypt the preshared key.

password

8. Enter a password to encrypt the preshared key.

Your encrypted pre-shared key displays on the screen.



```
-----START OF PSK-----DO NOT COPY THIS LINE-----
U2FsdGVkX1/ghUHK/u2ZYzOlKSzyuBFjr86wiZWzH2HwrxkTn4VSNYSB6AcUG9DuvfVf35mVASyFG0eAtHtvA0a0q9JHKmdbioz2bnEc/rM=
-----END OF PSK-----DO NOT COPY THIS LINE-----
Press any key to return to the menu.
```

Importing a Pre-shared Key

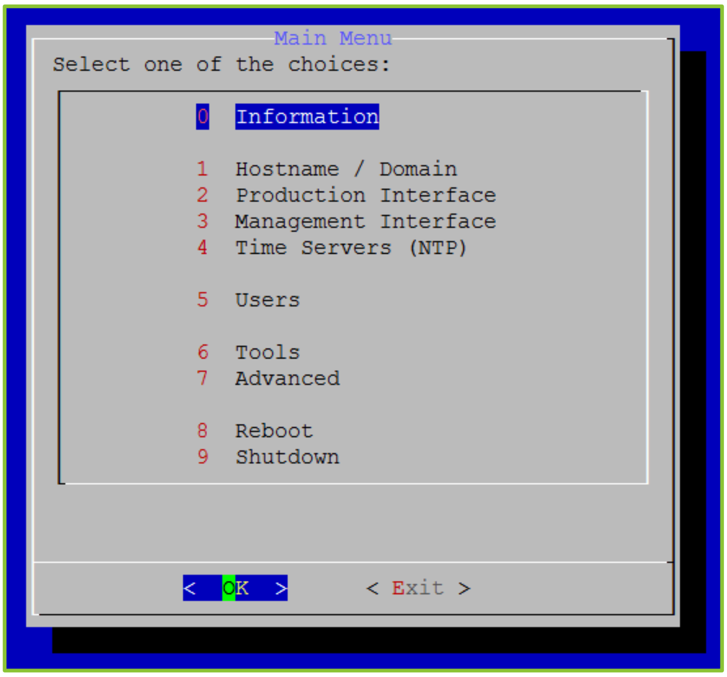
After generating and exporting the pre-shared key from the Active Controller in your VidyoGateway cluster configuration, you then import the key to your Standby Controller and Cluster Nodes. For more information about clusters, see Configuring Access Control Settings.

To import a pre-shared key:

1. Log in to the System Console.

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

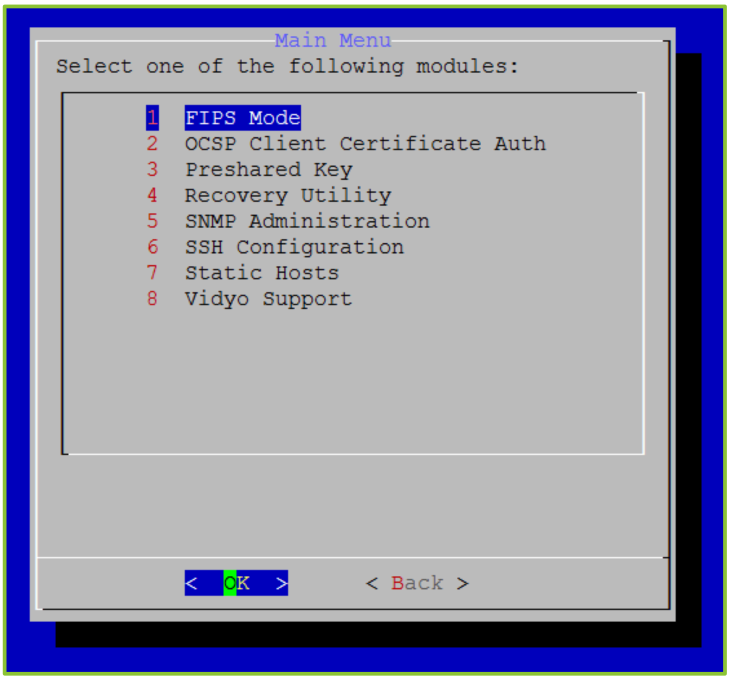
   The Main Menu displays.

2. Enter **7** to select the Advanced option.

3. Press the **Enter** key to select **OK**.

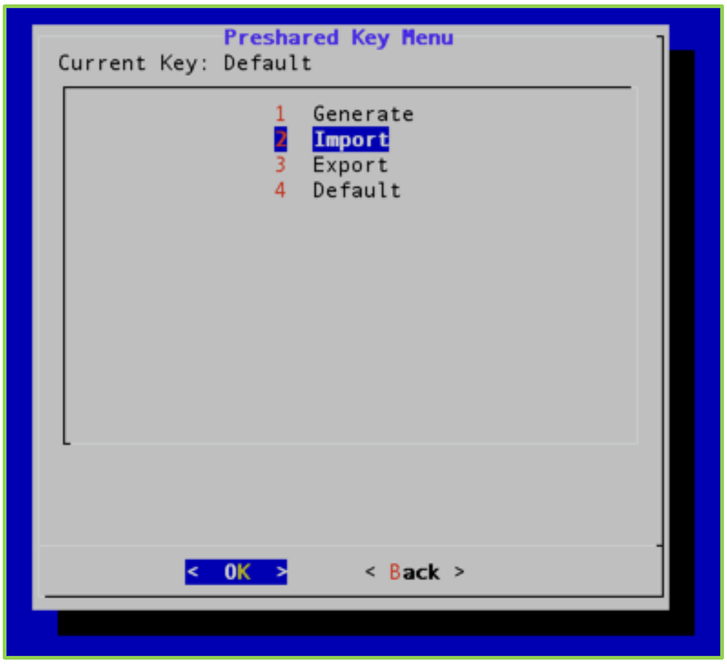
The Main Menu for the Advanced configuration displays.



```
                     Main Menu
Select one of the following modules:

      1  FIPS Mode
      2  OCSP Client Certificate Auth
      3  Preshared Key
      4  Recovery Utility
      5  SNMP Administration
      6  SSH Configuration
      7  Static Hosts
      8  Vidyo Support

          <  OK  >      < Back >
```

4. Enter **3** to select the Preshared Key option.
5. Press the Enter key to select OK.

The Preshared Key Menu displays.

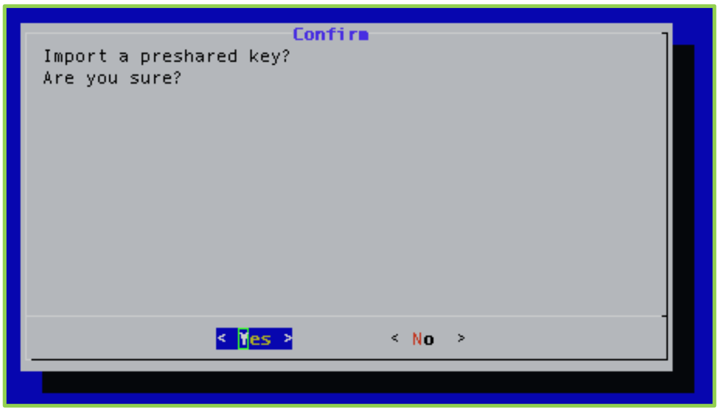


```
            Preshared Key Menu
Current Key: Default

          1  Generate
          2  Import
          3  Export
          4  Default

     <  OK  >      < Back >
```

6. Enter **2** to select the Import option.

7. Press the **Enter** key to select **OK**.

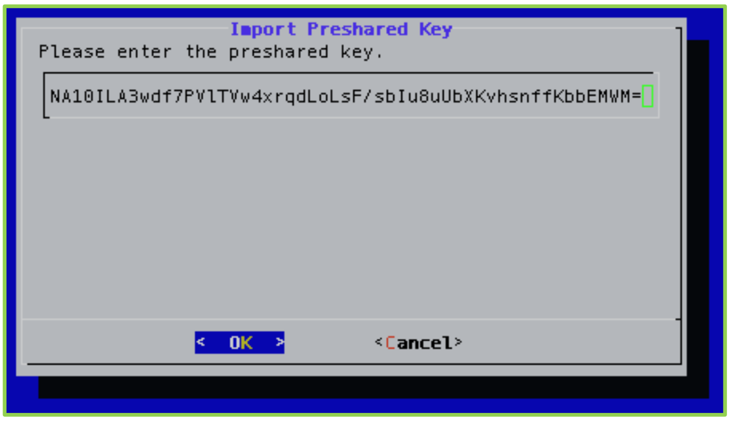
   The *Confirm* window displays.



```
Confirm
Import a preshared key?
Are you sure?
```

8. Press the **Enter** key to select **Yes**.
9. Enter the preshared key that you previously generated.

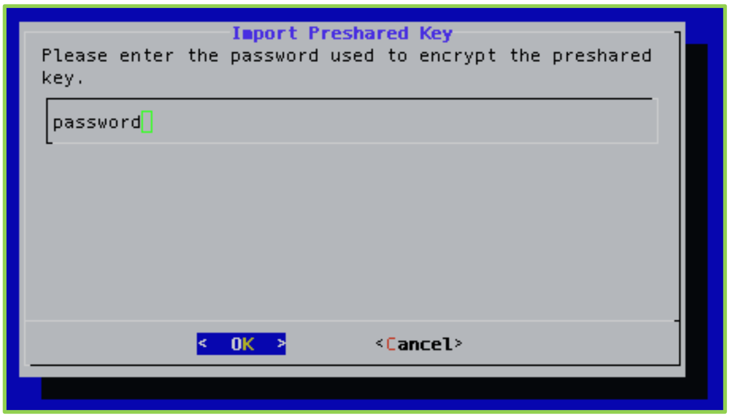
   For information about how to generate a pre-shared key, see Generating a Pre-shared Key.



```
Import Preshared Key
Please enter the preshared key.
NA10ILA3wdf7PVlTVw4xrqdLoLsF/sbIu8uUbXKvhsnffKbbEMWM=
```

10. Press the **Enter** key to select **OK**.

11. Enter the same password previously used to encrypt the pre-shared key.



```
Import Preshared Key
Please enter the password used to encrypt the preshared
key.

password
```

12. Press the **Enter** key to select **OK**.

    A message displays stating "Preshared key successfully imported. Hash: [key]."

13. Press the **Enter** key to select **OK**.

    Your system is now using the pre-shared key you just imported.

Note Until a pre-shared key is exported from your Active Controller and imported to your Standby Controller and Cluster Nodes, calls on your Standby Controller or Cluster Nodes will not be visible from the *Status* tab in your Active Controller. For more information, see Checking the Status of Your VidyoGateway.

Selecting the Default Pre-shared Key

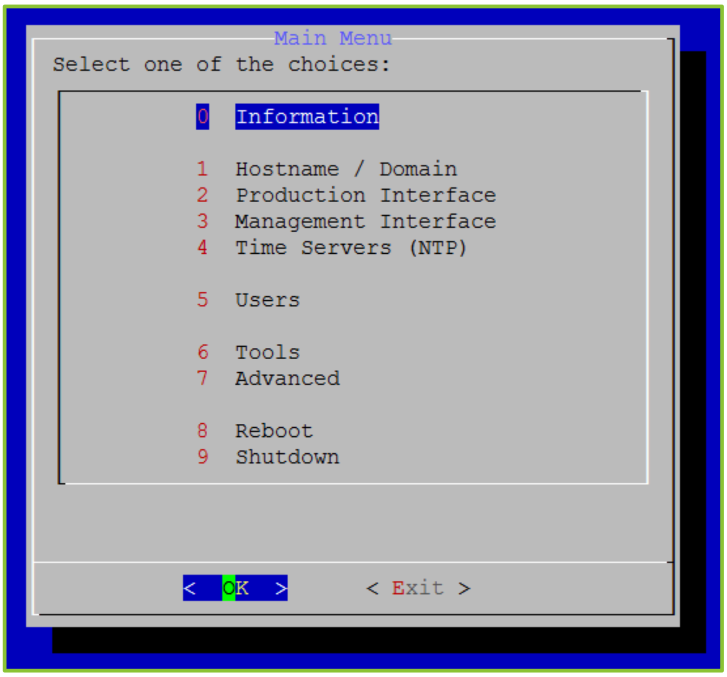
The default key is automatically used on your system when configuring your VidyoGateways as a cluster. Therefore, you only need to select the default pre-shared key if you have previously generated or imported one and now want to revert to the default.

To select the default pre-shared key:

1. Log in to the System Console.

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

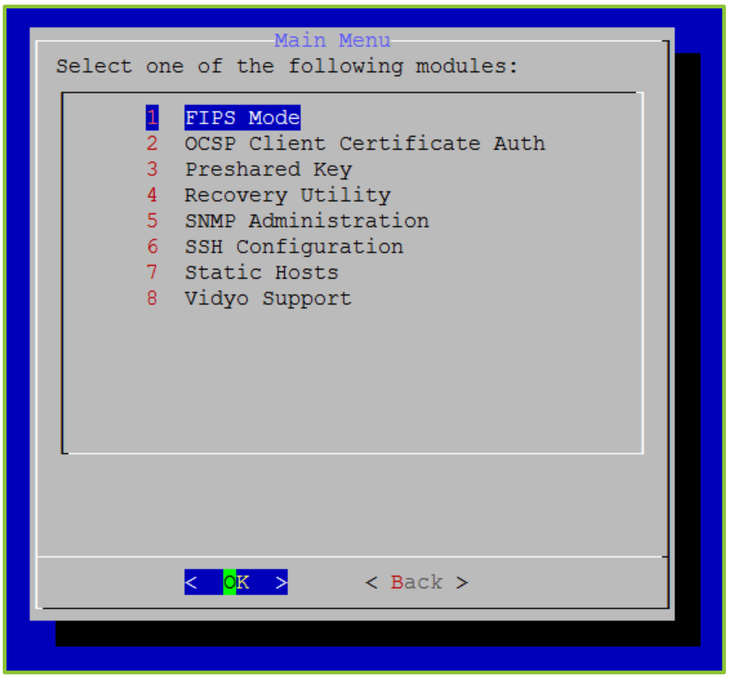
The Main Menu displays.



```
                     Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown

            <  OK  >       < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

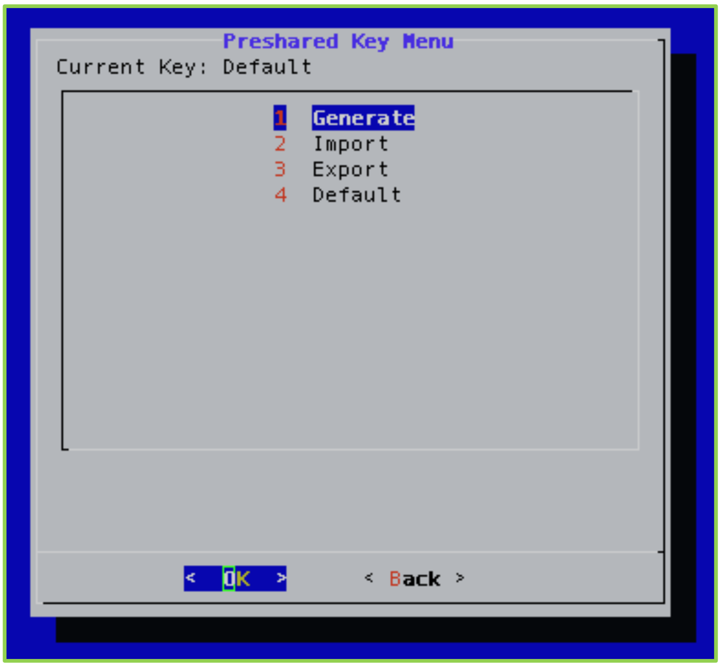
The Main Menu for the Advanced configuration displays.



```
                     Main Menu
 Select one of the following modules:

          1  FIPS Mode
          2  OCSP Client Certificate Auth
          3  Preshared Key
          4  Recovery Utility
          5  SNMP Administration
          6  SSH Configuration
          7  Static Hosts
          8  Vidyo Support

            <  OK  >       < Back >
```

4. Enter **3** to select the Preshared Key option.
5. Press the Enter key to select OK.

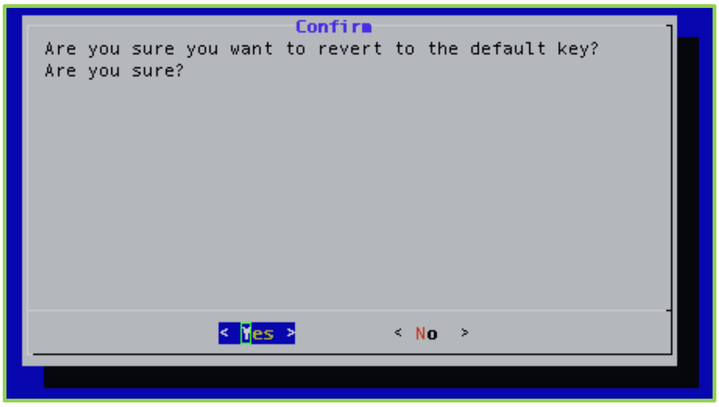
   The Preshared Key Menu displays.



```
Preshared Key Menu
Current Key: Default

        1  Generate
        2  Import
        3  Export
        4  Default
```

6. Enter **4** to select the Default option.
7. Press the Enter key to select OK.

   The *Confirm* window displays.



```
Confirm
Are you sure you want to revert to the default key?
Are you sure?
```

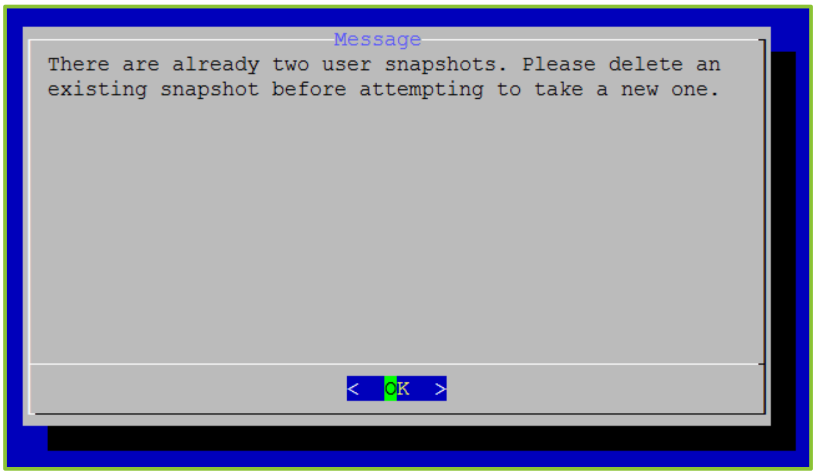
8. Press the Enter key to select Yes.

Running the Recovery Utility

The recovery utility enables you to take snapshots of your system, restore the snapshots, delete the snapshots, and restore the factory default.

Taking Snapshots

A maximum of two user snapshots are allowed. This limitation does not include snapshots that are automatically generated upon upgrading your VidyoGateway (e.g., VidyoUpdate). When two user snapshots already exist and the user attempts to take a new one, the following message will display:



Message

There are already two user snapshots. Please delete an existing snapshot before attempting to take a new one.

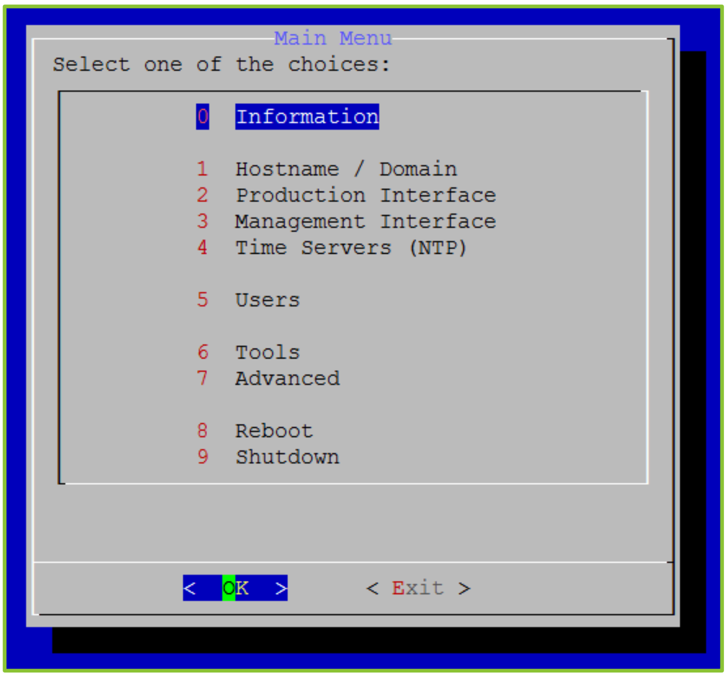
For more information about deleting snapshots, see Deleting Snapshots.

To take snaphots:

1. Log in to the System Console.

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

The Main Menu displays.

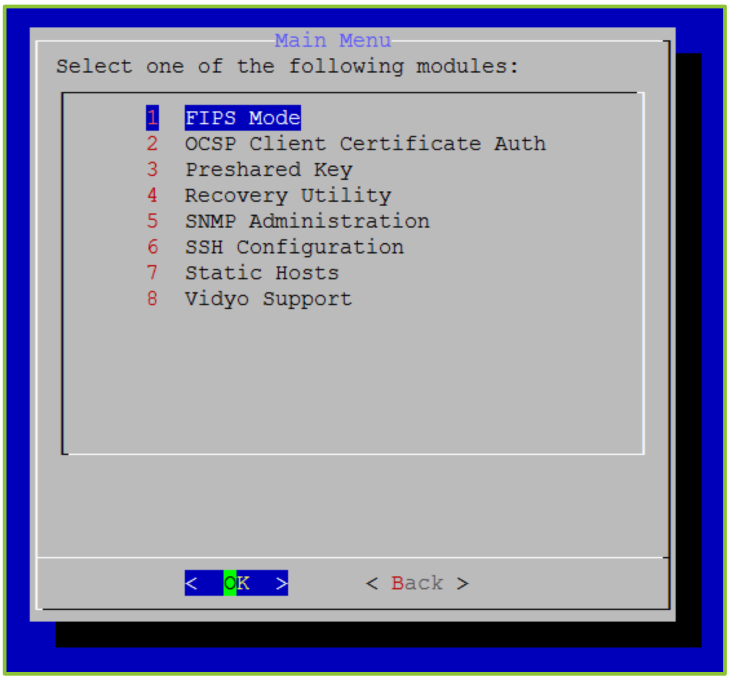


```
Main Menu
Select one of the choices:

          0  Information

          1  Hostname / Domain
          2  Production Interface
          3  Management Interface
          4  Time Servers (NTP)

          5  Users

          6  Tools
          7  Advanced

          8  Reboot
          9  Shutdown

        <  OK  >      < Exit >
```

2. Enter **7** to select the Advanced option.

3. Press the Enter key to select OK.

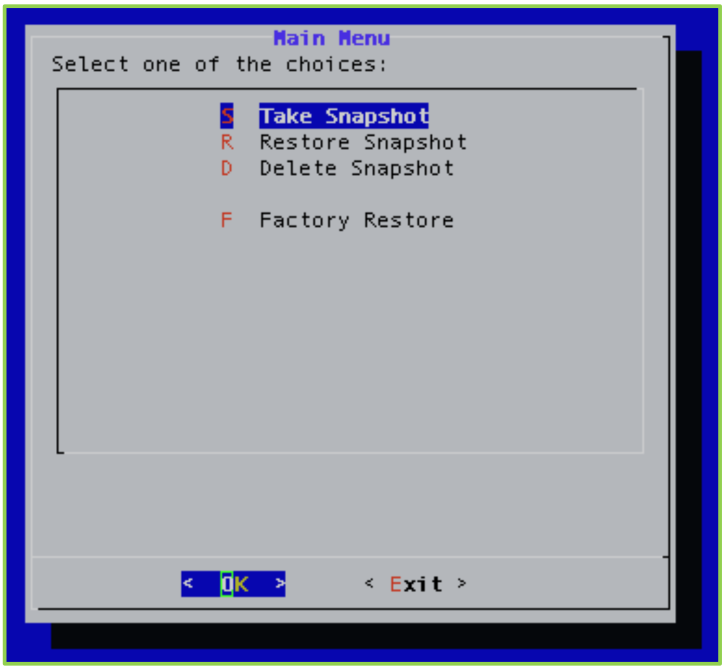
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

      1  FIPS Mode
      2  OCSP Client Certificate Auth
      3  Preshared Key
      4  Recovery Utility
      5  SNMP Administration
      6  SSH Configuration
      7  Static Hosts
      8  Vidyo Support

        <  OK  >      < Back >
```

4. Enter **4** to select the Recovery Utility option.
5. Press the Enter key to select OK.

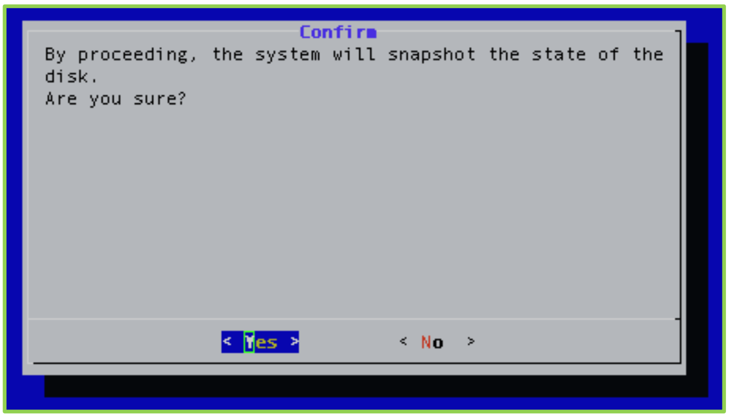
   The Recover Utility Main Menu displays.



```
Main Menu
Select one of the choices:

          S  Take Snapshot
          R  Restore Snapshot
          D  Delete Snapshot

          F  Factory Restore

      <  OK  >          <  Exit  >
```

6. Enter **S** to select the Take Snapshot option.
7. Press the Enter key to select OK.

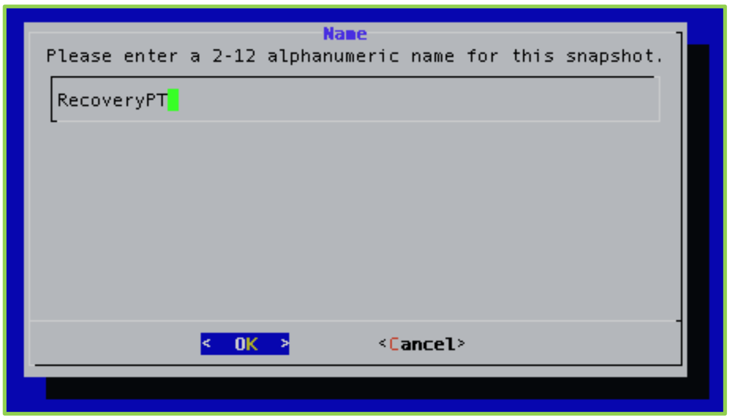
   The *Confirm* window displays.



```
Confirm
By proceeding, the system will snapshot the state of the
disk.
Are you sure?

      < Yes >          <  No  >
```

8. Press the Enter key to select Yes.

The *Name* window displays.



Name

Please enter a 2-12 alphanumeric name for this snapshot.

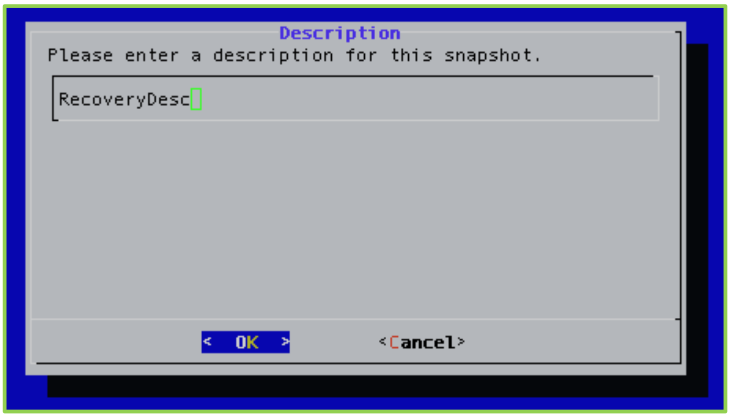
```
RecoveryPT
```

9. Enter a name for the snapshot.

   The name must be from two to twelve alphanumeric characters in length.

10. Press the **Enter** key to select **OK**.

    The *Description* window displays.



Description

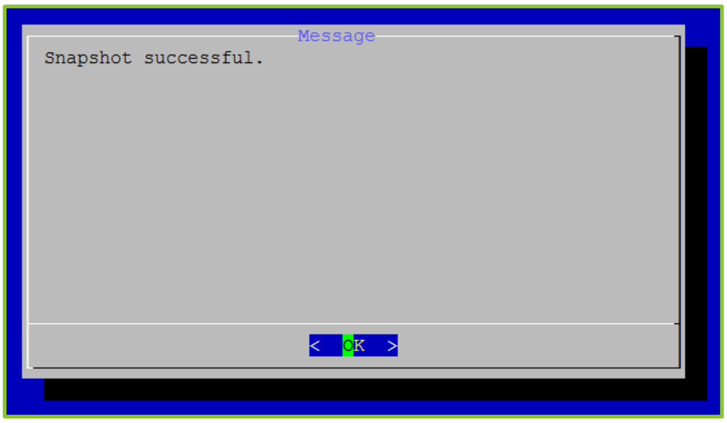
Please enter a description for this snapshot.

```
RecoveryDesc
```

11. Enter a description for the snapshot.

12. Press the **Enter** key to select **OK**.

A message displays stating “Snapshot successful.”



Snapshot successful.

13. Press the **Enter** key to select **OK**.

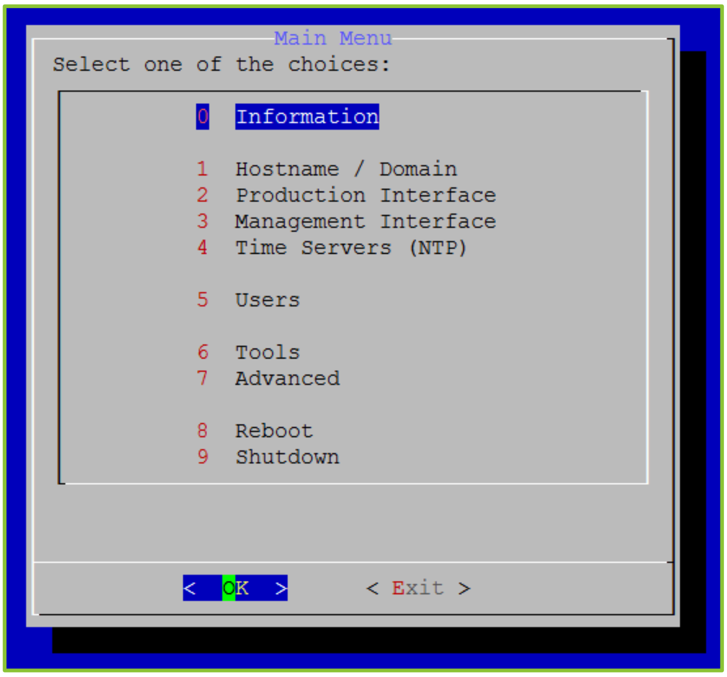
Restoring Snapshots

To restore snaphots:

1. Log in to the System Console.

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

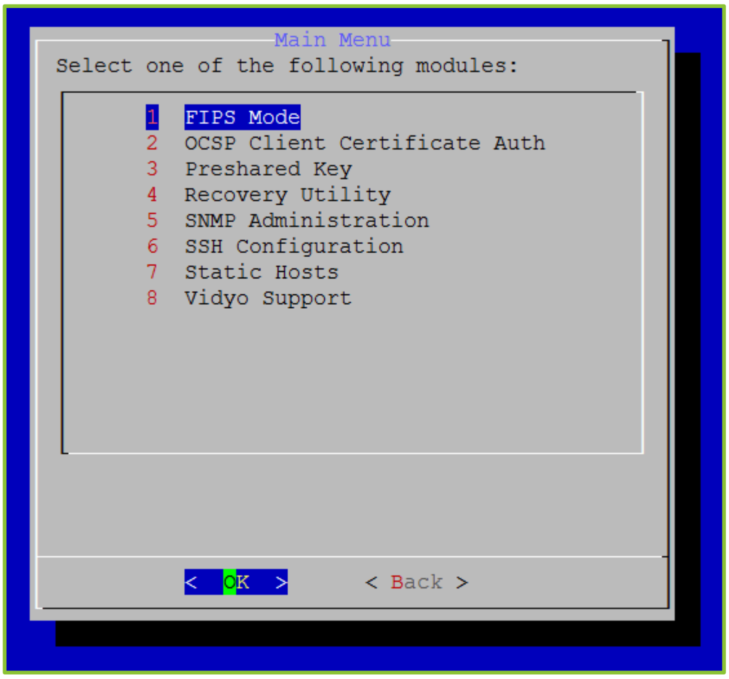
   The Main Menu displays.



2. Enter **7** to select the Advanced option.

3. Press the **Enter** key to select **OK**.

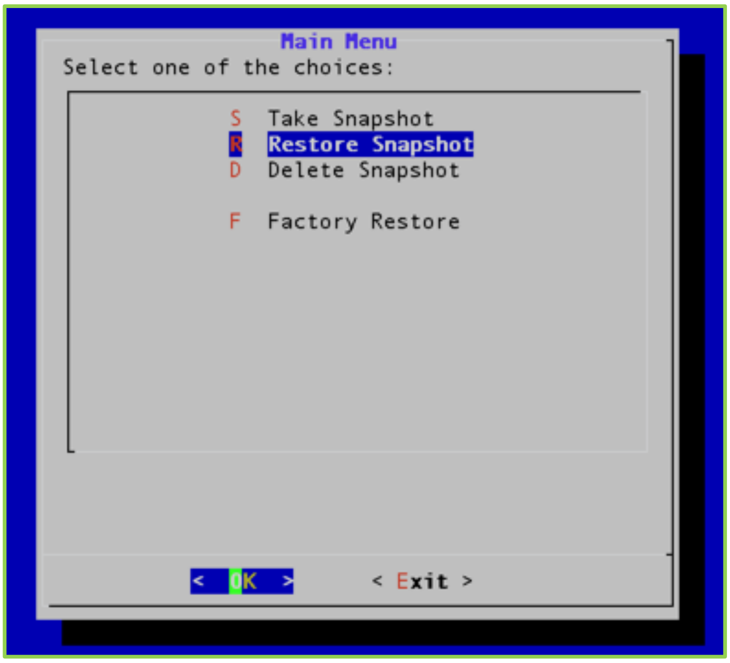
   The Main Menu for the Advanced configuration displays.



```
                    Main Menu
Select one of the following modules:

       1  FIPS Mode
       2  OCSP Client Certificate Auth
       3  Preshared Key
       4  Recovery Utility
       5  SNMP Administration
       6  SSH Configuration
       7  Static Hosts
       8  Vidyo Support

          <  OK  >        < Back >
```

4. Enter **4** to select the Recovery Utility option.
5. Press the **Enter** key to select **OK**.

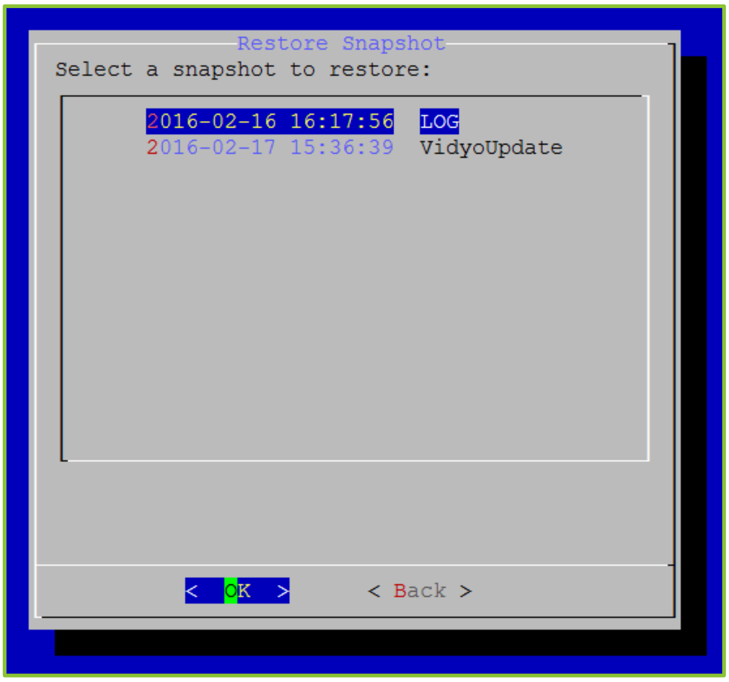
   The Recover Utility Main Menu displays.



```
                    Main Menu
Select one of the choices:

            S  Take Snapshot
            R  Restore Snapshot
            D  Delete Snapshot

            F  Factory Restore

          <  OK  >        < Exit >
```

6. Enter **R** to select the Restore Snapshot option.
7. Press the Enter key to select OK.

   The *Restore Snapshot* window displays.



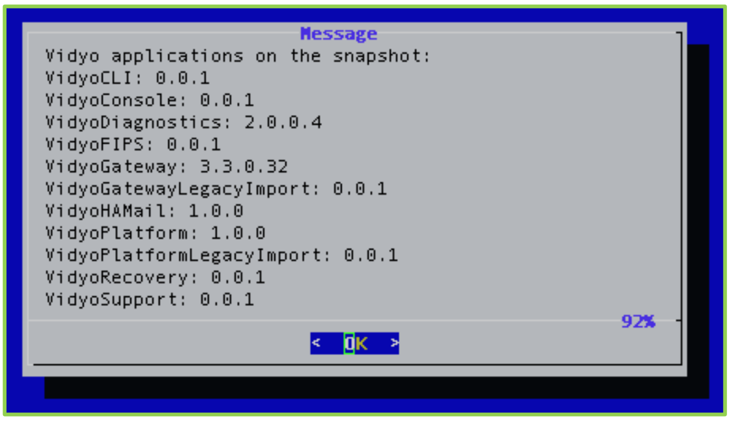
```
Restore Snapshot
Select a snapshot to restore:

        2016-02-16 16:17:56  LOG
        2016-02-17 15:36:39  VidyoUpdate
```

8. Select the snapshot you want to restore.
9. Press the Enter key to select OK.

   To ensure that you have selected the correct snapshot, a message displays stating "Description of the snapshot: [snapshot description]."

10. Press the Enter key to select OK.

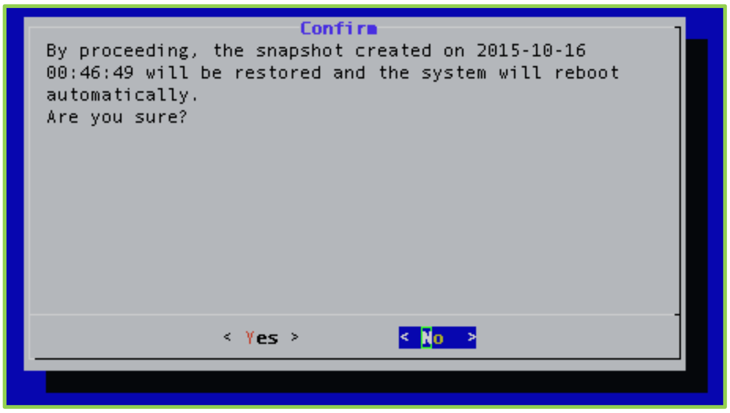
    A *Message* window displays listing the Vidyo applications on the snapshot as well as the version number of each application.



```
Message
Vidyo applications on the snapshot:
VidyoCLI: 0.0.1
VidyoConsole: 0.0.1
VidyoDiagnostics: 2.0.0.4
VidyoFIPS: 0.0.1
VidyoGateway: 3.3.0.32
VidyoGatewayLegacyImport: 0.0.1
VidyoHAMail: 1.0.0
VidyoPlatform: 1.0.0
VidyoPlatformLegacyImport: 0.0.1
VidyoRecovery: 0.0.1
VidyoSupport: 0.0.1
                                    92%
```

11. Press the **Enter** key to select **OK**.

    The *Confirm* window displays.

    ```
    By proceeding, the snapshot created on 2015-10-16
    00:46:49 will be restored and the system will reboot
    automatically.
    Are you sure?
    ```

12. Press the **Enter** key to select **Yes**.

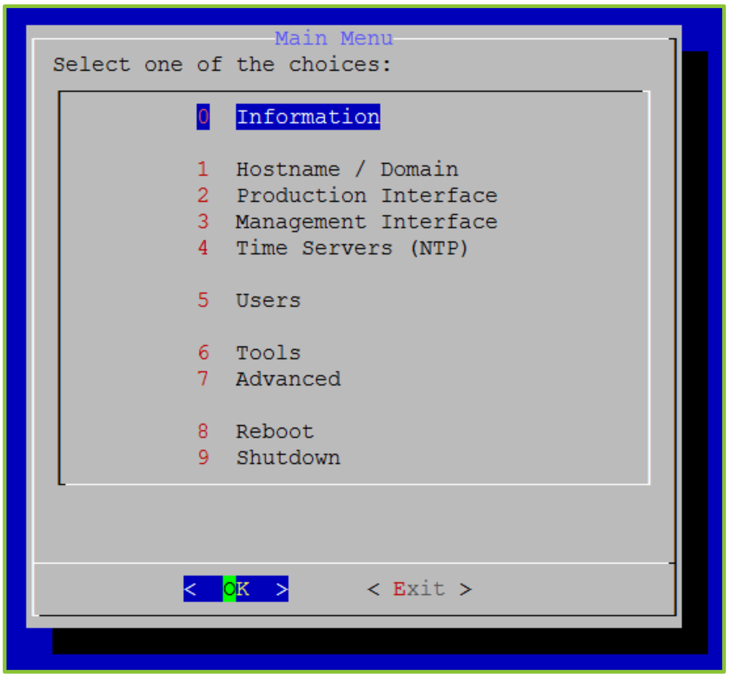
Deleting Snapshots

To delete snaphots:

1. Log in to the System Console.

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

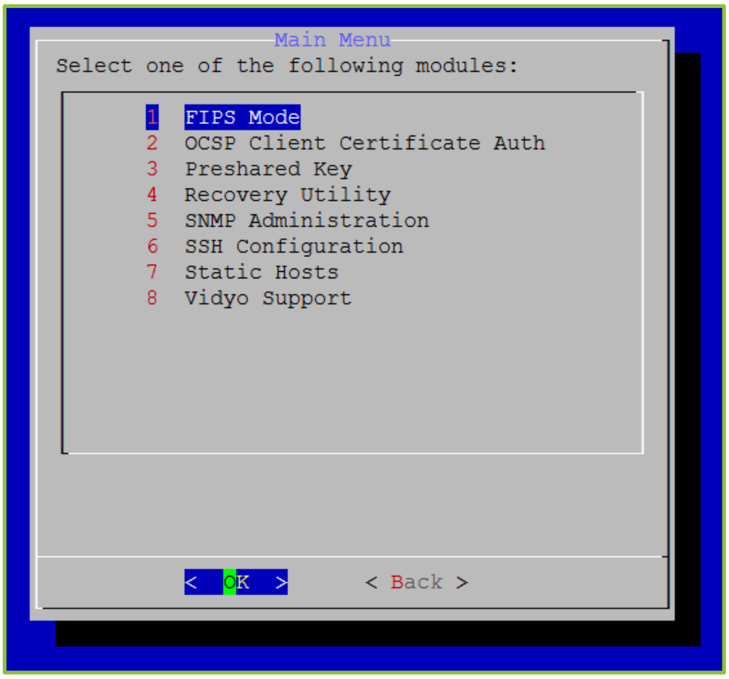
   The Main Menu displays.

2. Enter **7** to select the Advanced option.

3. Press the **Enter** key to select **OK**.

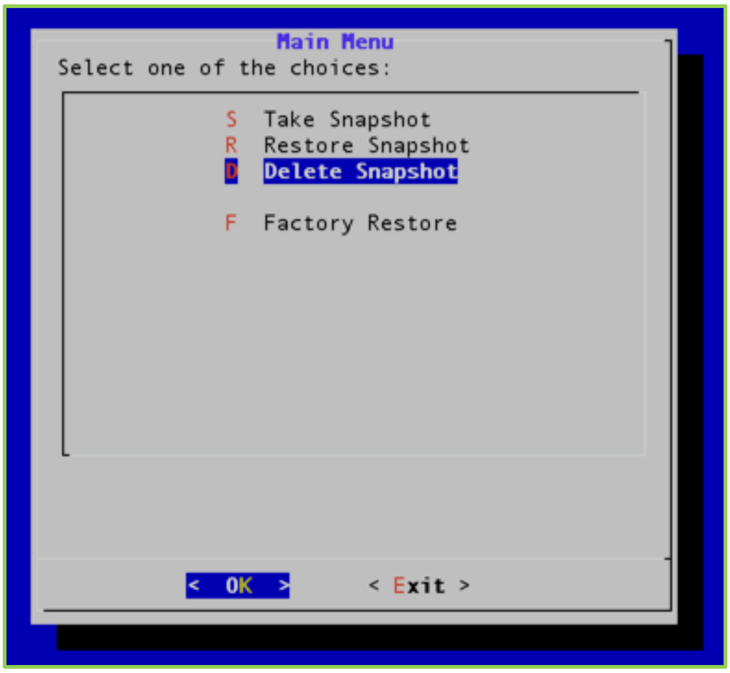
   The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

      1   FIPS Mode
      2   OCSP Client Certificate Auth
      3   Preshared Key
      4   Recovery Utility
      5   SNMP Administration
      6   SSH Configuration
      7   Static Hosts
      8   Vidyo Support

          <  OK  >      < Back >
```

4. Enter **4** to select the Recovery Utility option.
5. Press the **Enter** key to select **OK**.

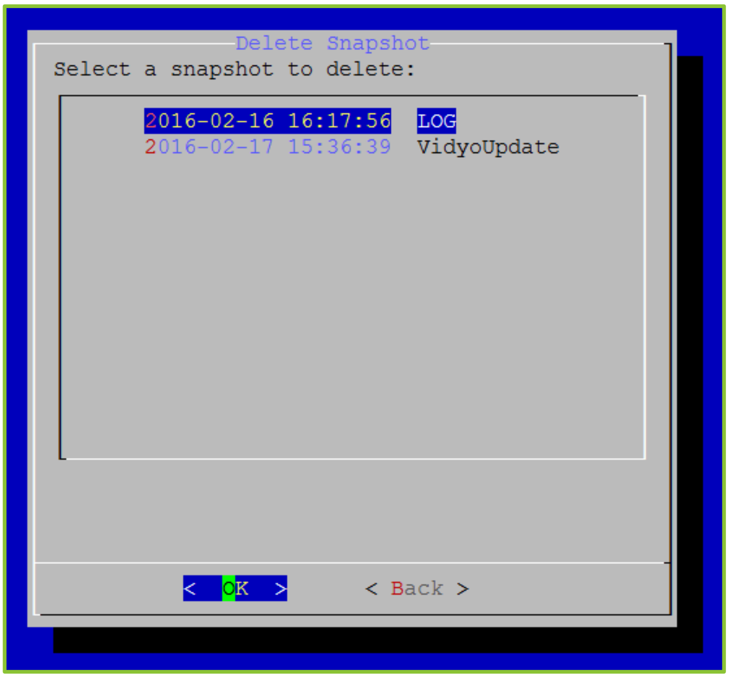
   The Recover Utility Main Menu displays.



```
Main Menu
Select one of the choices:

            S   Take Snapshot
            R   Restore Snapshot
            D   Delete Snapshot

            F   Factory Restore

          <  OK  >      < Exit >
```

6. Enter **D** to select the Delete Snapshot option.
7. Press the Enter key to select OK.

   The *Delete Snapshot* window displays.

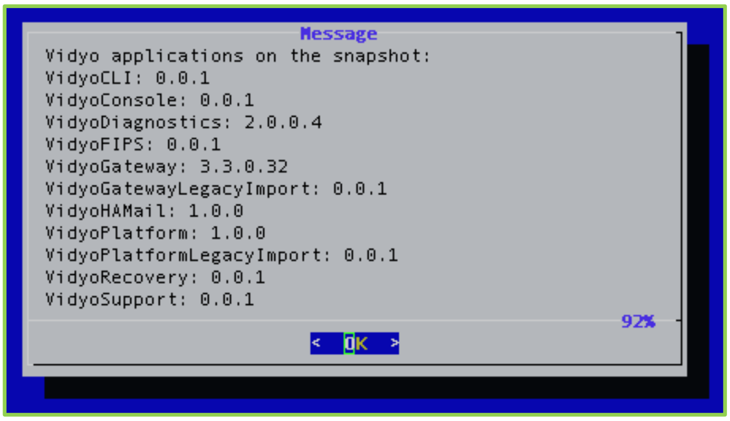


```
Select a snapshot to delete:

    2016-02-16 16:17:56   LOG
    2016-02-17 15:36:39   VidyoUpdate
```

8. Select the snapshot you want to delete.
9. Press the Enter key to select OK.

   To ensure that you have selected the correct snapshot, a message displays stating "Description of the snapshot: [snapshot description]."
10. Press the Enter key to select OK.

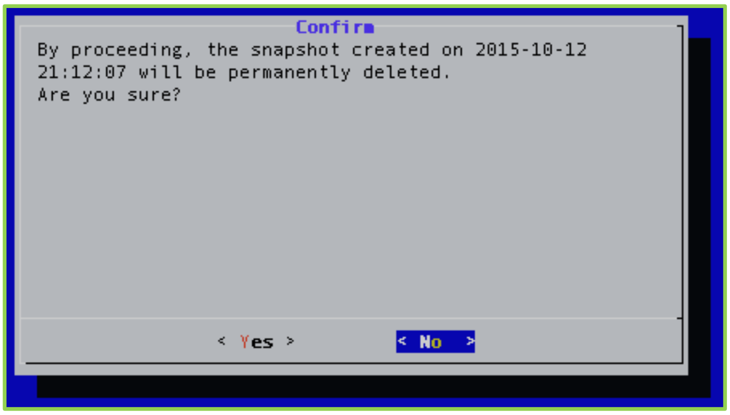
    A *Message* window displays listing the Vidyo applications on the snapshot as well as the version number of each application.



```
Vidyo applications on the snapshot:
VidyoCLI: 0.0.1
VidyoConsole: 0.0.1
VidyoDiagnostics: 2.0.0.4
VidyoFIPS: 0.0.1
VidyoGateway: 3.3.0.32
VidyoGatewayLegacyImport: 0.0.1
VidyoHAMail: 1.0.0
VidyoPlatform: 1.0.0
VidyoPlatformLegacyImport: 0.0.1
VidyoRecovery: 0.0.1
VidyoSupport: 0.0.1
```

11. Press the **Enter** key to select **OK**.

    The *Confirm* window displays.



```
By proceeding, the snapshot created on 2015-10-12
21:12:07 will be permanently deleted.
Are you sure?
```

12. Press the **Enter** key to select **Yes**.

    A message displays stating “Snapshot successfully deleted.”

13. Press the **Enter** key to select **OK**.

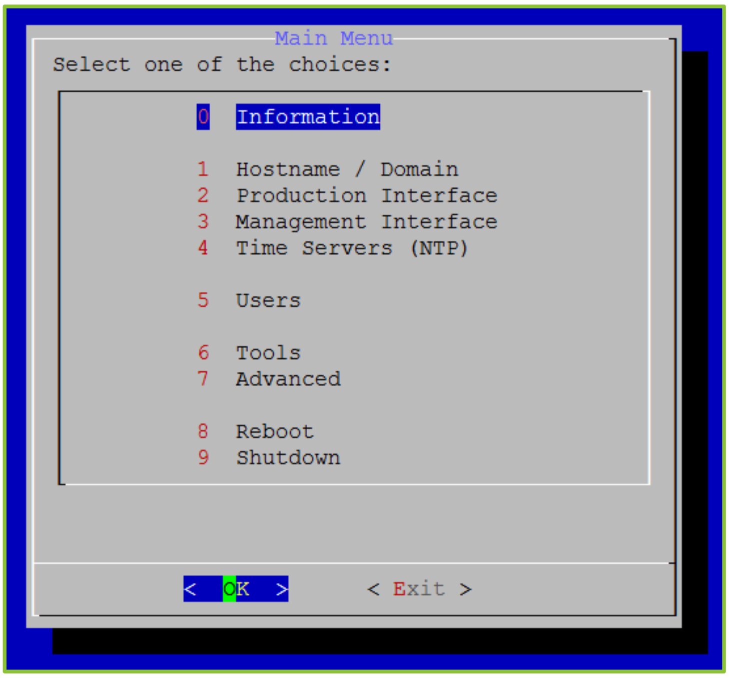
Performing a Factory Restore

To perform a factory restore:

1. Log in to the System Console.

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

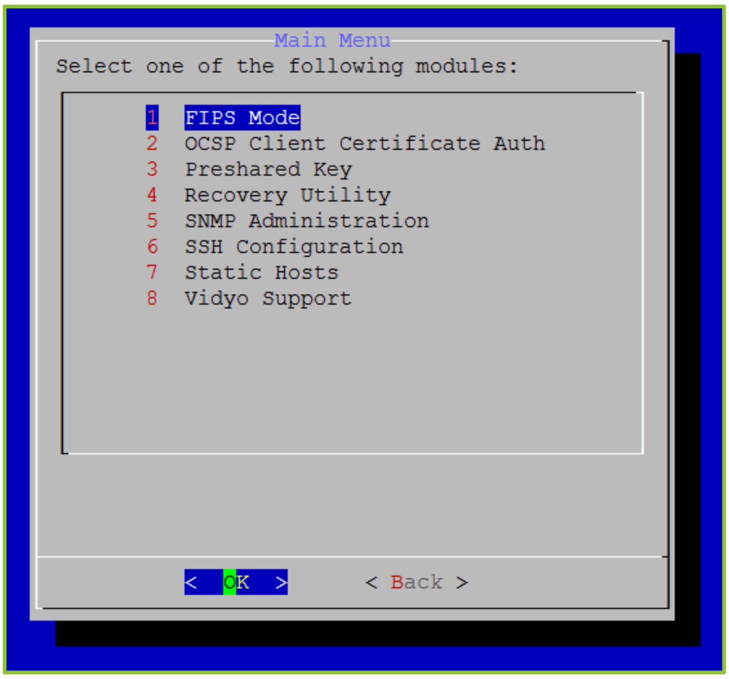
The Main Menu displays.



```
Main Menu
Select one of the choices:

            0   Information

            1   Hostname / Domain
            2   Production Interface
            3   Management Interface
            4   Time Servers (NTP)

            5   Users

            6   Tools
            7   Advanced

            8   Reboot
            9   Shutdown

        <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**.

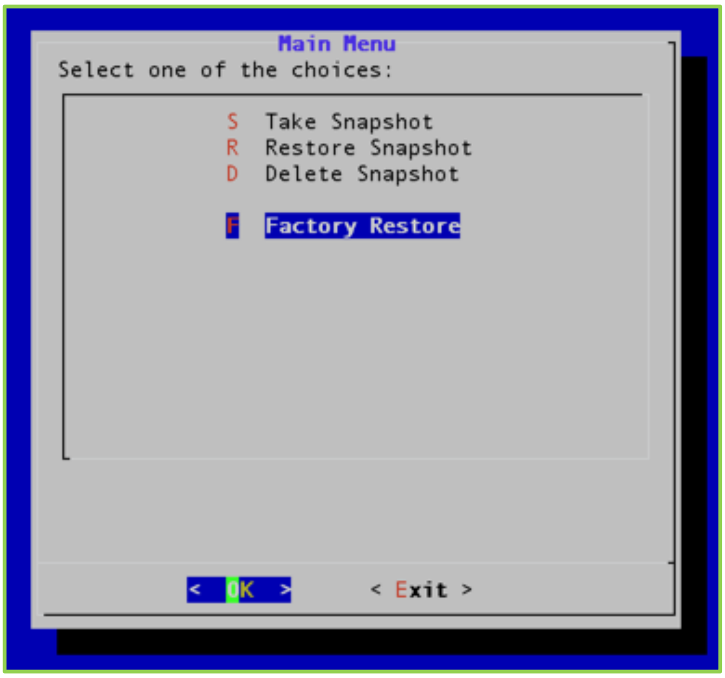
   The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

        <  OK  >        < Back >
```

4. Enter **4** to select the Recovery Utility option.

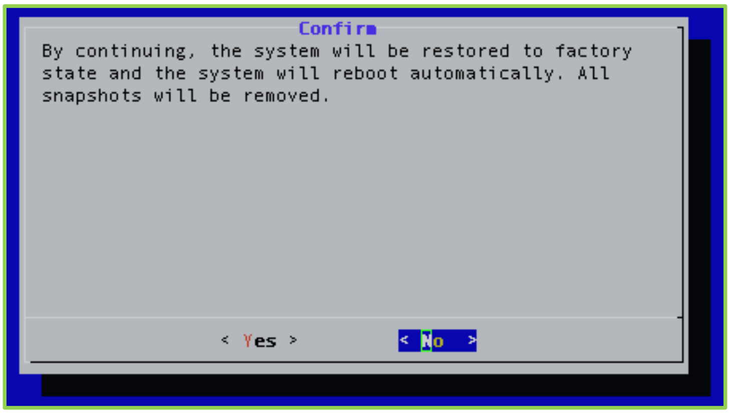
   The Recover Utility Main Menu displays.



```
Main Menu
Select one of the choices:

S  Take Snapshot
R  Restore Snapshot
D  Delete Snapshot

F  Factory Restore

<  OK  >        < Exit >
```

5. Enter **F** to select the Factory Restore option.
6. Press the Enter key to select OK.

   The *Confirm* window displays.



```
Confirm
By continuing, the system will be restored to factory
state and the system will reboot automatically. All
snapshots will be removed.

< Yes >        < No >
```

7. Press the Enter key to select Yes.

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 VidyoGateway traps include the following object identifiers (OIDs):

1. vidyoGatewayNodeLegacyMediaQualityThresholdAlert
   - This trap provides an indication that the MediaQuality threshold for a Legacy call has been reached on the legacy side.
   - This trap can be turned on and off by setting the notification from the System Console and a specific threshold can be set from the SNMP manager. The jitter is measured in milliseconds and the default time setting is 0.
   - This trap repeats every 10 seconds as long as the condition persists.
2. vidyoGatewayNodeLegacyPacketLossThresholdAlert
   - This trap provides an indication that the PacketLoss threshold for a Legacy call has been reached on the legacy side.
   - This trap can be turned on and off by setting the notification from the System Console and specific threshold can be set from the SNMP manager. The packet loss is measured in percentage and the default time setting is 0.
   - This trap repeats every 10 seconds as long as the condition persists.
3. vidyoGatewayControllerJoinedClusterAlert
   - This trap provides an indication that a new VidyoGateway has joined the cluster.
   - When a VidyoGateway node is added to the cluster, this trap can be turned on and off by setting the notification from the System Console.
   - There is no notification frequency setting for this trap.
4. vidyoGatewayControllerLeftClusterAlert
   - This trap provides an indication that an existing VidyoGateway has been removed from the cluster.
   - When a VidyoGateway node is removed from the cluster, this trap can be turned on and off by setting the notification from the System Console.
   - There is no notification frequency setting for this trap.
5. vidyoGatewayControllerVmConnEstablishedAlert
   - This trap provides an indication that VidyoGateway has established a connection with the VidyoManager.
   - There are no configuration settings for this trap.

- There is no notification frequency setting for this trap.

6. vidyoGatewayControllerVmConnLostAlert
   - This trap provides an indication that VidyoGateway has lost its connection with the VidyoManager.
   - There are no configuration settings for this trap.
   - There is no notification frequency setting for this trap.
7. vidyoGatewayControllerIPAddedToBlackListAlert
   - This trap is triggered when a new IP Address is automatically blacklisted when Access Control is operated in the "**Automatically block IP addresses with whitelist and blacklist overrides"** mode.
8. vidyoGatewayControllerClusterRoleAlert
   - This trap is triggered when failover occurs.
   - An instance of this occurrence is when the Active Controller goes offline or the Standby Controller becomes active.
9. vidyoGatewayControllerCallRejectedAlert
   - This trap is triggered when the VidyoGateway rejects a call because the cluster or standalone VidyoGateway capacity is fully utilized.

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.

For more information about Vidyo enterprise Notifications, as well as Get, and Set Polling OIDs, refer to the Vidyo MIB file at http://www.vidyo.com/services-support/technical-support/product-documentation/administrator-guides.

If your VidyoGateway 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 VidyoGateways using a management interface so your SNMP notifications can be sourced from unique management interface IP addresses. In this case, your network management system (NMS) should be accessible over your management network. For more information, see Enabling the Management Interface in the System Console.

Enabling, Disabling, and Restarting SNMP

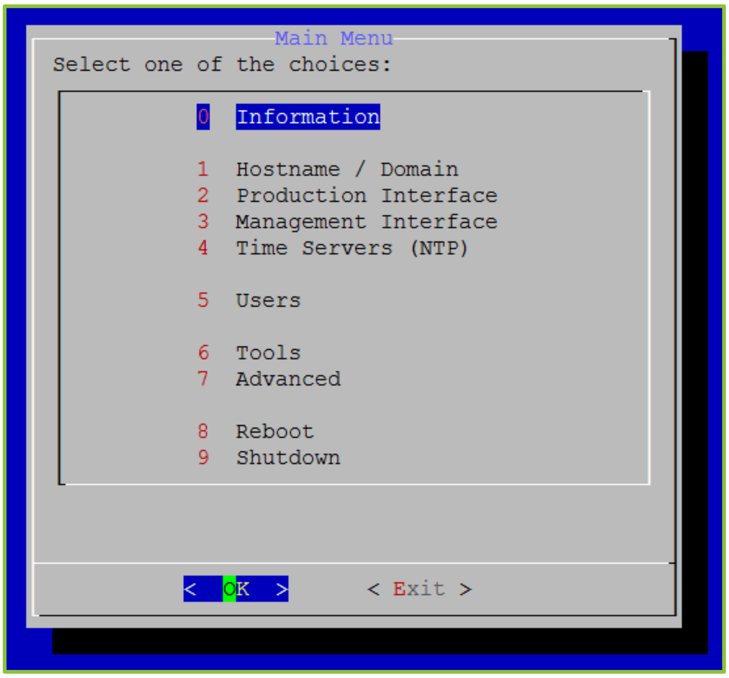
Enable SNMP only after configuring SNMP2 community strings or SNMPv3 users and creating notifications or traps.

To enable, disable, or restart SNMP:

1. Log in to the System Console.

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

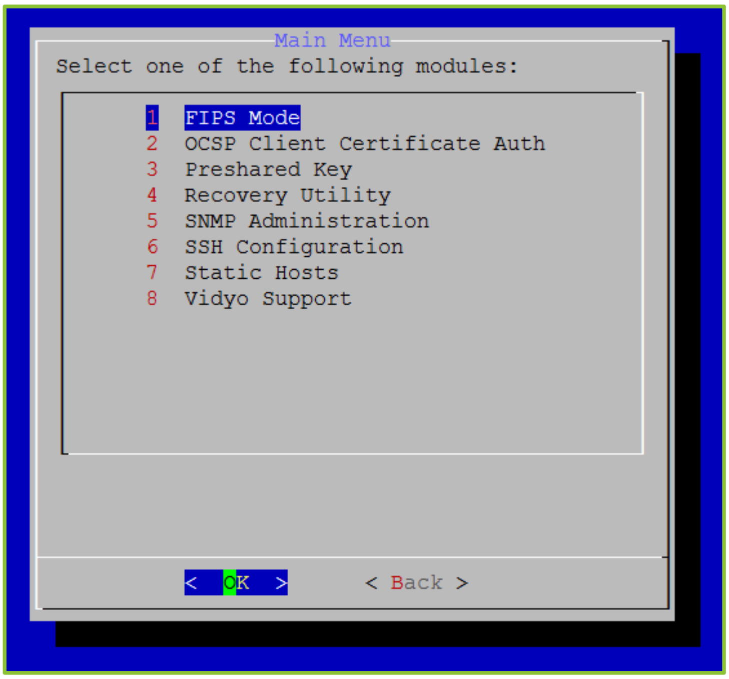
   The Main Menu displays.



```
                    Main Menu
Select one of the choices:

             0  Information

             1  Hostname / Domain
             2  Production Interface
             3  Management Interface
             4  Time Servers (NTP)

             5  Users

             6  Tools
             7  Advanced

             8  Reboot
             9  Shutdown

            <  OK  >       < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

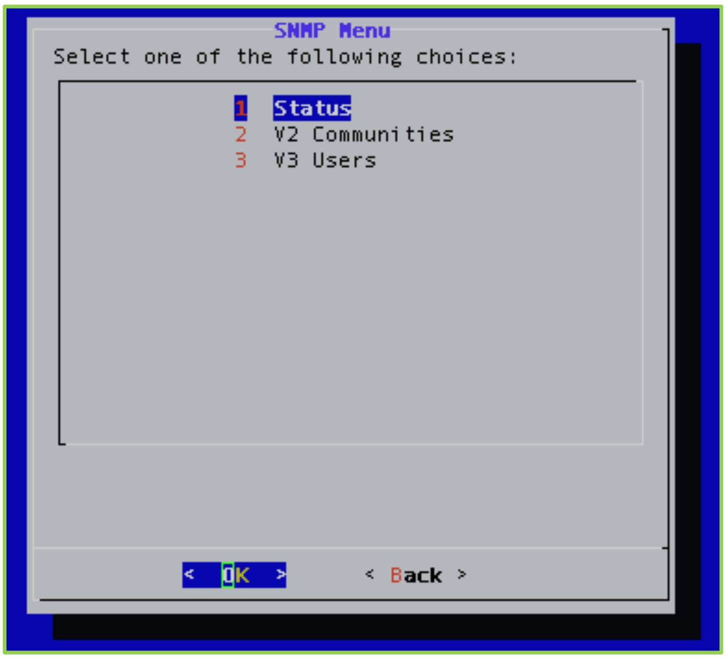
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1  FIPS Mode
        2  OCSP Client Certificate Auth
        3  Preshared Key
        4  Recovery Utility
        5  SNMP Administration
        6  SSH Configuration
        7  Static Hosts
        8  Vidyo Support

          <  OK  >      < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**.

   The SNMP Menu displays.

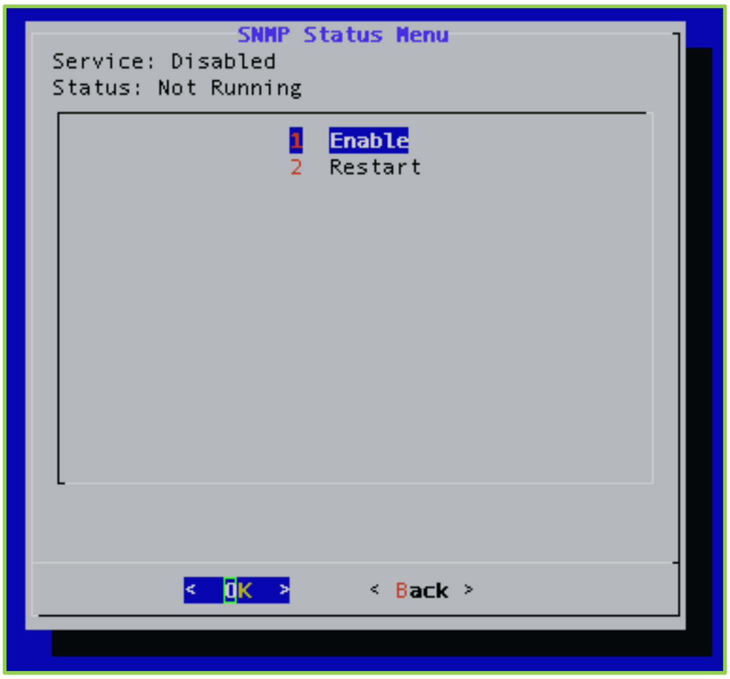


```
SNMP Menu
Select one of the following choices:

               1  Status
               2  V2 Communities
               3  V3 Users

          <  OK  >      < Back >
```

6. Enter **1** to select the Status option.

7. Press the **Enter** key to select **OK**.

   The SNMP Status Menu displays including the current status. If SNMP is enabled, the window includes the Disable option only; if SNMP is disabled, the window includes the Enable option only.



SNMP Status Menu

Service: Disabled
Status: Not Running

8. Enter **1** to select Enable or Disable, or enter **2** to select the Restart option.
9. Press the **Enter** key to select **OK**.

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

Configuring SNMP v2 Communities

You can create two SNMP v2 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.

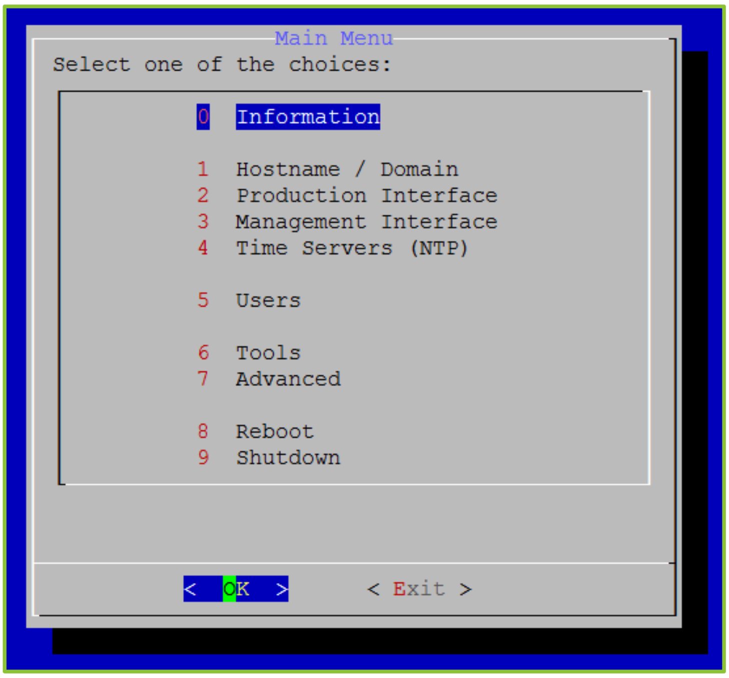
Listing the SNMP v2 Communities

To list the SNMP v2 communities:

1. Log in to the System Console.

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

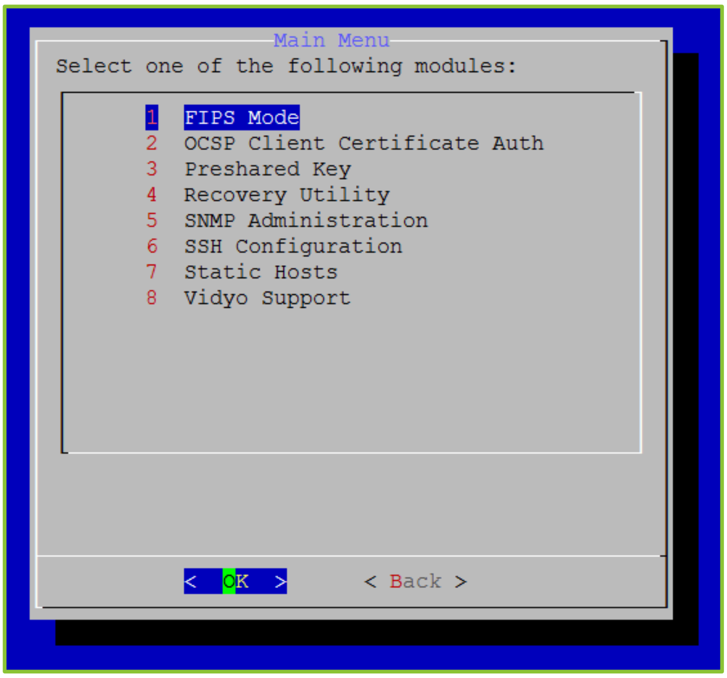
The Main Menu displays.



```
                    Main Menu
Select one of the choices:

           0   Information

           1   Hostname / Domain
           2   Production Interface
           3   Management Interface
           4   Time Servers (NTP)

           5   Users

           6   Tools
           7   Advanced

           8   Reboot
           9   Shutdown

          <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**.

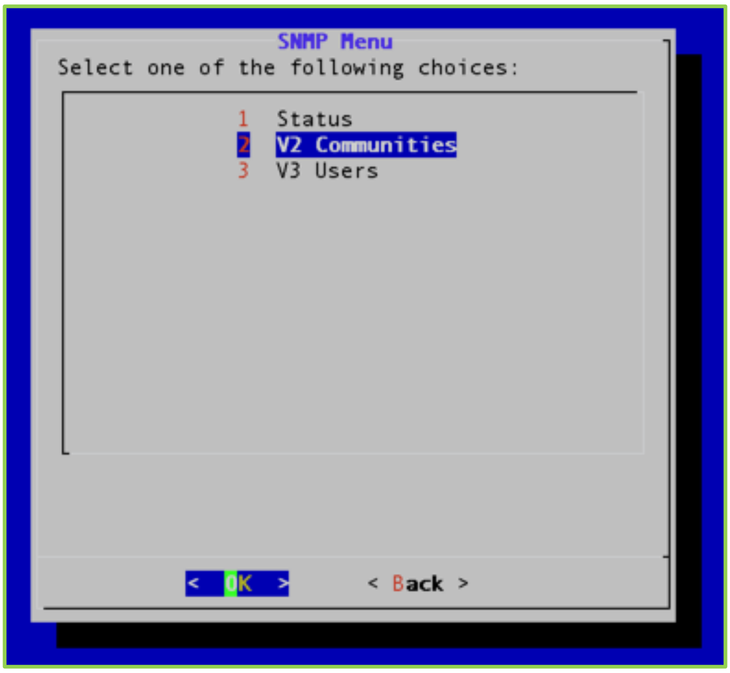
   The Main Menu for the Advanced configuration displays.



```
                    Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

          <  OK  >        < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

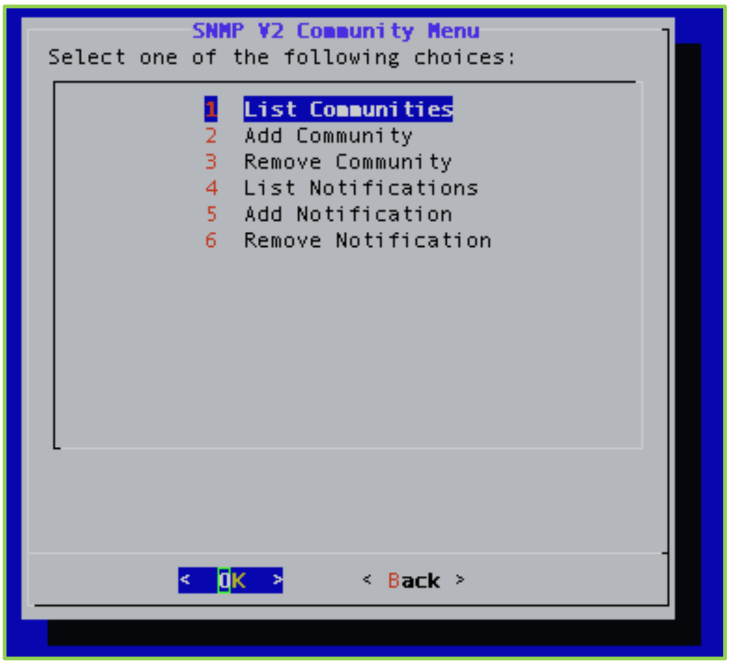
   The SNMP Menu displays.



```
                    SNMP Menu
Select one of the following choices:

              1  Status
              2  V2 Communities
              3  V3 Users

        <  OK  >        < Back >
```

6. Enter **2** to select the V2 Communities option.
7. Press the Enter key to select OK.

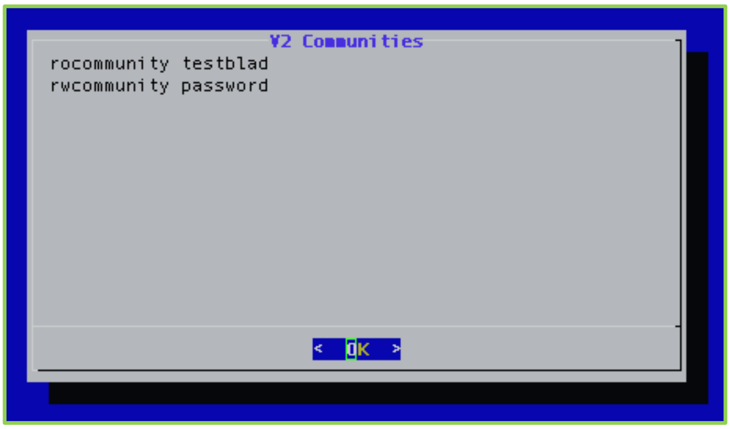
The SNMP V2 Community Menu displays.



8. Enter **1** to select the List Communities option.

9. Press the Enter key to select OK.

   The *V2 Communities* window, which lists the current v2 communities, displays.



```
rocommunity testblad
rwcommunity password
```

10. Press the Enter key to select OK.

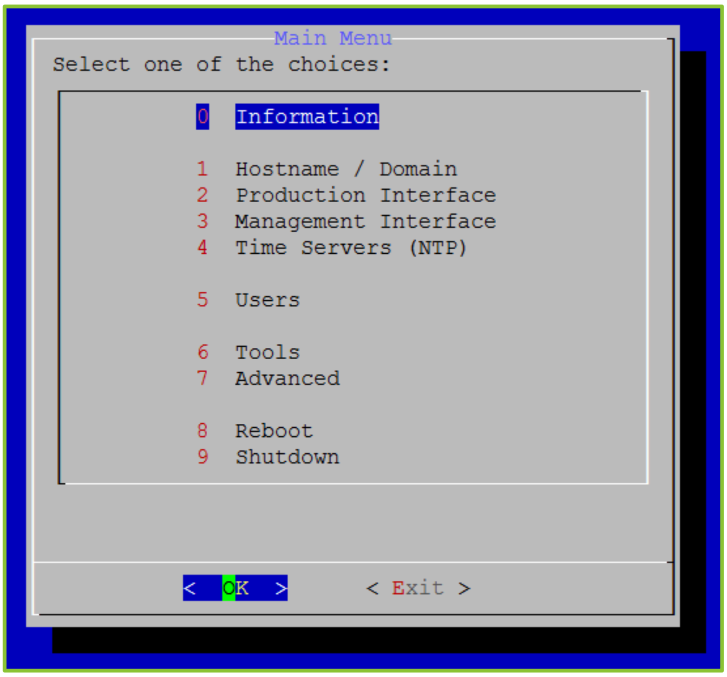
Adding SNMP v2 Communities

To add SNMP v2 communities:

1. Log in to the System Console.

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

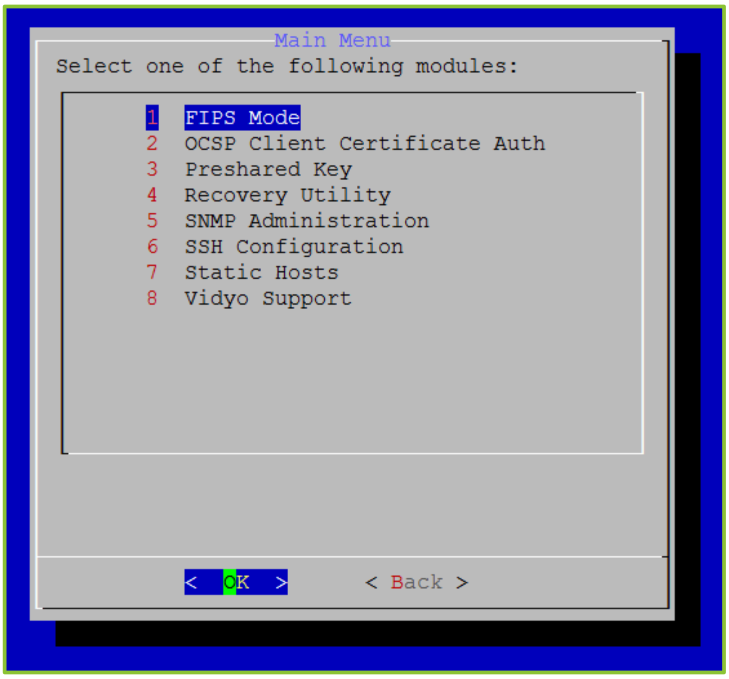
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0   Information

        1   Hostname / Domain
        2   Production Interface
        3   Management Interface
        4   Time Servers (NTP)

        5   Users

        6   Tools
        7   Advanced

        8   Reboot
        9   Shutdown

      <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

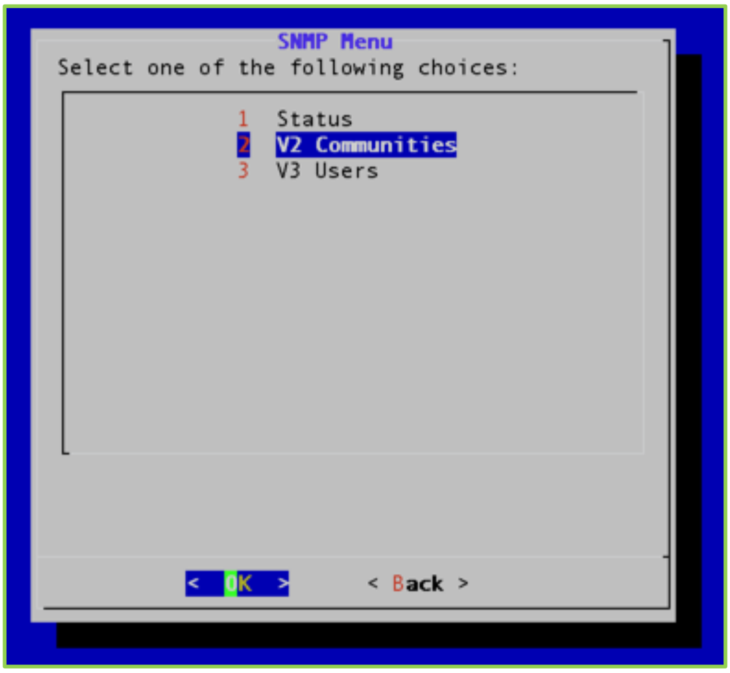
   The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

      1   FIPS Mode
      2   OCSP Client Certificate Auth
      3   Preshared Key
      4   Recovery Utility
      5   SNMP Administration
      6   SSH Configuration
      7   Static Hosts
      8   Vidyo Support

      <  OK  >        < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.

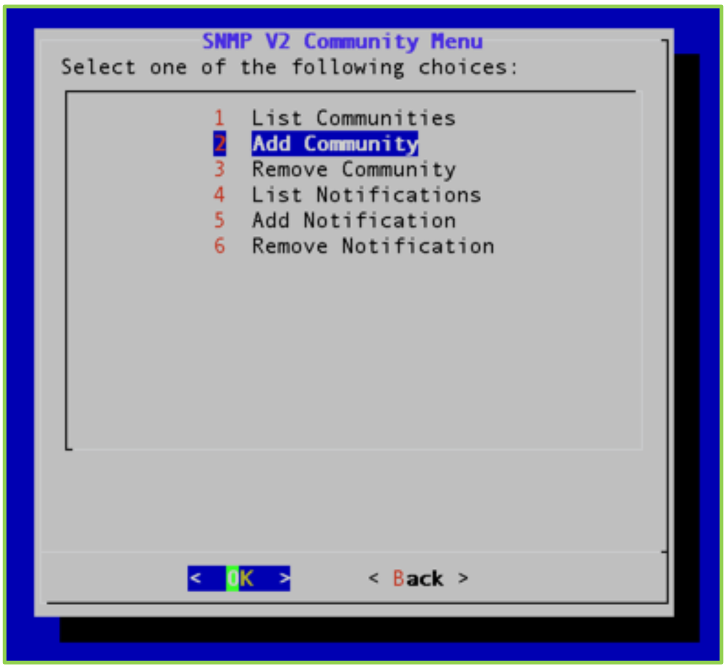


SNMP Menu

Select one of the following choices:

6. Enter **2** to select the V2 Communities option.
7. Press the Enter key to select OK.

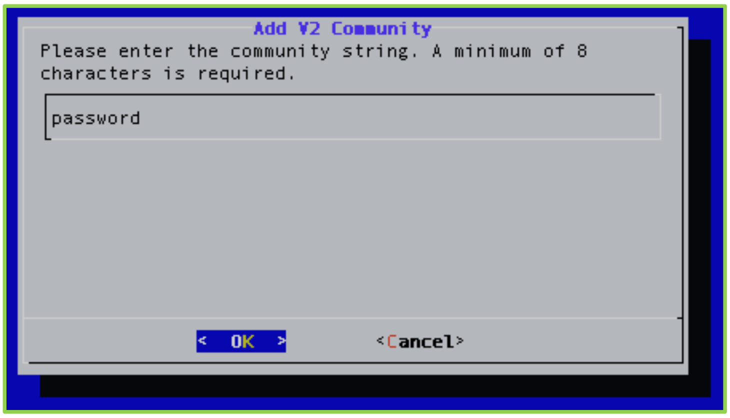
The SNMP V2 Community Menu displays.



Select one of the following choices:

8. Enter **2** to select the Add Community option.
9. Press the Enter key to select OK.

The *Add V2 Community* window displays.

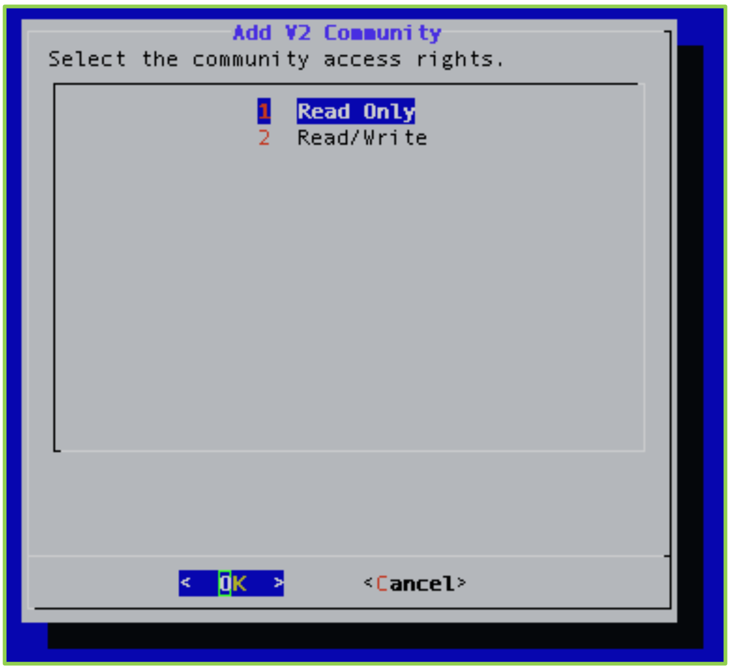


Please enter the community string. A minimum of 8 characters is required.

password

10. Enter the community string using no less than eight characters.
11. Press the Enter key to select OK.

The next *Add V2 Community* window displays.

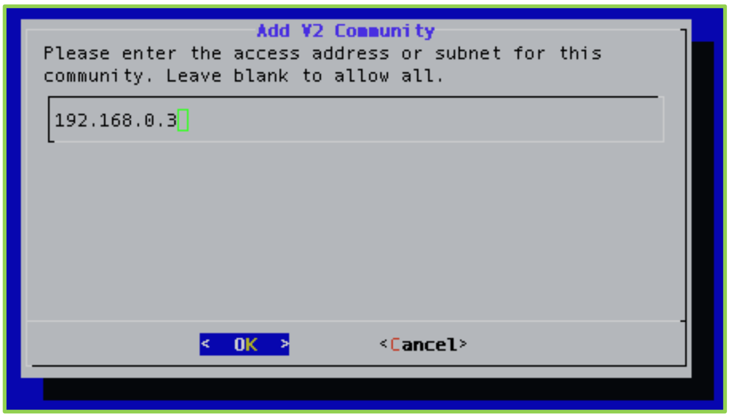


```
Add V2 Community
Select the community access rights.

            1  Read Only
            2  Read/Write

        <  OK  >        <Cancel>
```

12. Enter **1** if you want the community access rights to be read only or enter **2** if you want the community access rights to be read and write.

13. Press the Enter key to select OK.

    The next *Add V2 Community* window displays.



```
Add V2 Community
Please enter the access address or subnet for this
community. Leave blank to allow all.

192.168.0.3

        <  OK  >        <Cancel>
```

14. Enter the IP address or subnet to access this community, or leave the text box blank if you want to allow access to all.

15. Press the Enter key to select OK.

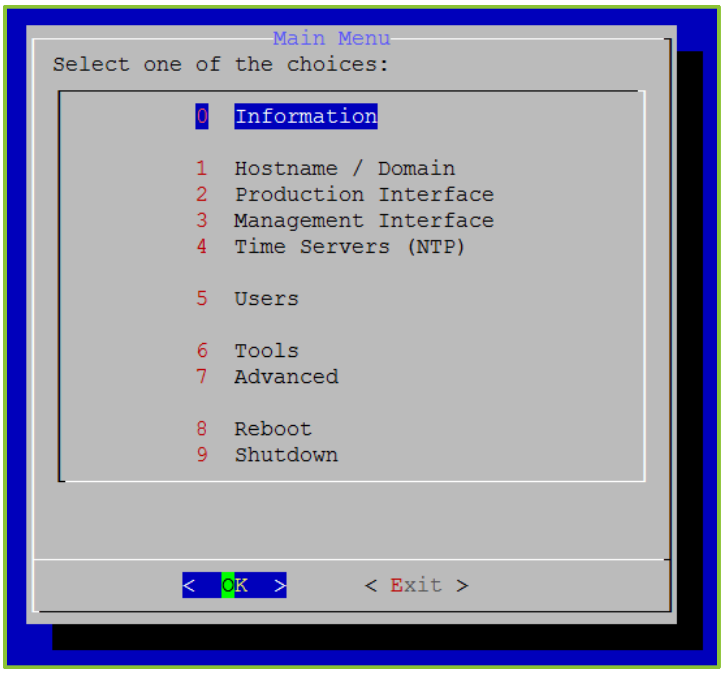
Removing an SNMP Community String

To remove an SNMP v2 community:

1. Log in to the System Console.

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

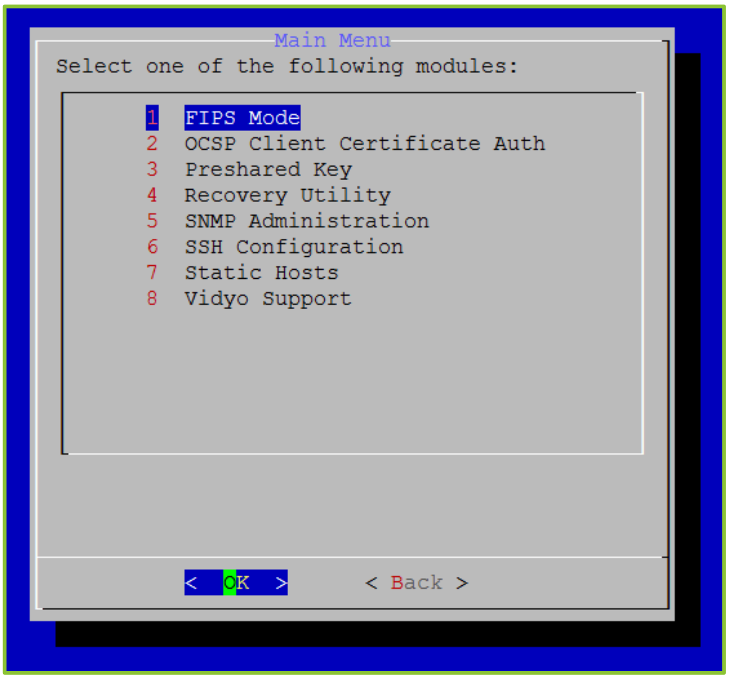
   The Main Menu displays.



```
                    Main Menu
Select one of the choices:

           0   Information

           1   Hostname / Domain
           2   Production Interface
           3   Management Interface
           4   Time Servers (NTP)

           5   Users

           6   Tools
           7   Advanced

           8   Reboot
           9   Shutdown

          <  OK  >       < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

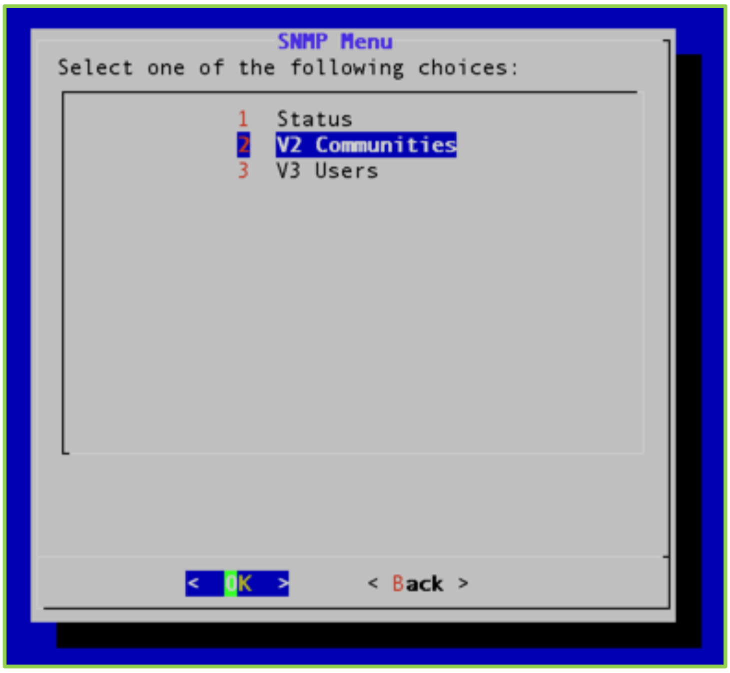
The Main Menu for the Advanced configuration displays.



```
                      Main Menu
 Select one of the following modules:

         1  FIPS Mode
         2  OCSP Client Certificate Auth
         3  Preshared Key
         4  Recovery Utility
         5  SNMP Administration
         6  SSH Configuration
         7  Static Hosts
         8  Vidyo Support

           <  OK  >         < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.

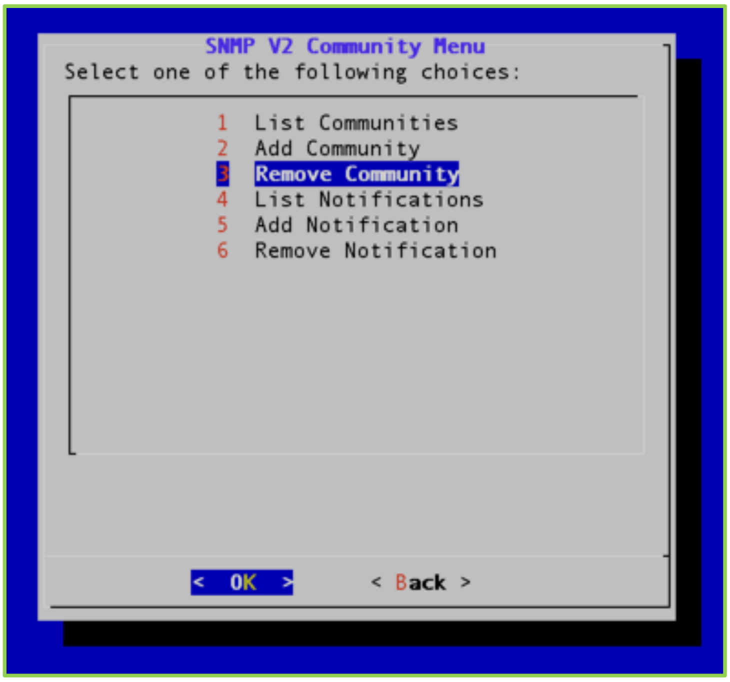


```
                      SNMP Menu
 Select one of the following choices:

                1  Status
                2  V2 Communities
                3  V3 Users

           <  OK  >         < Back >
```

6. Enter **2** to select the V2 Communities option.

7. Press the **Enter** key to select **OK**.

   The SNMP V2 Community Menu displays.

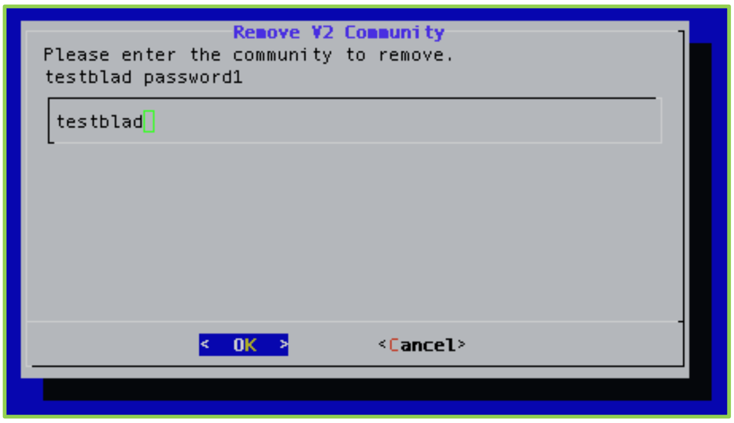


```
SNMP V2 Community Menu
Select one of the following choices:
```

8. Enter **3** to select the Remove Community option.

9. Press the **Enter** key to select **OK**.

   The *Remove V2 Community* window displays.



```
Remove V2 Community
Please enter the community to remove.
testblad password1

testblad
```

10. Enter the community string of the community you want to remove.

11. Press the **Enter** key to select **OK**.

    A message displays stating “Successfully removed community.”

12. Press the **Enter** key to select **OK**.

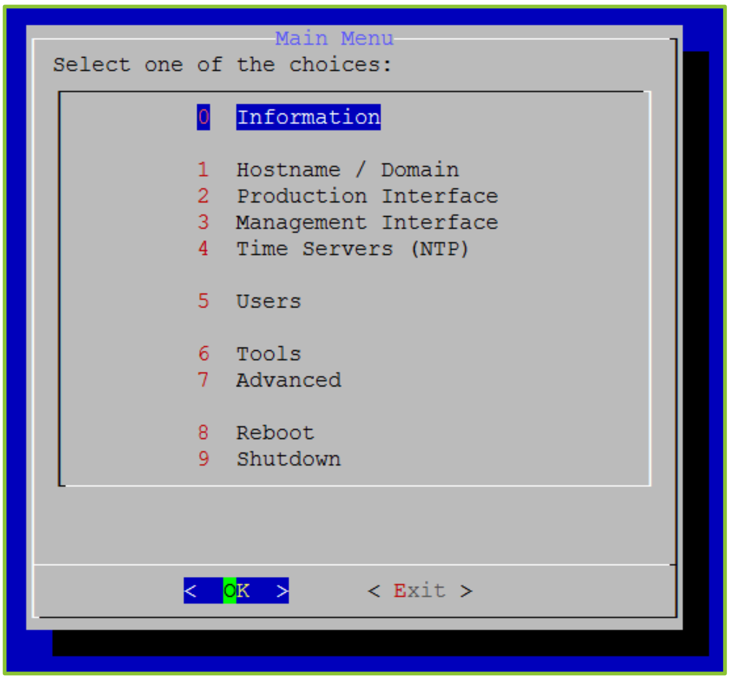
Listing SNMP v2 Notifications

To list an SNMP v2 notification:

1. Log in to the System Console.

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

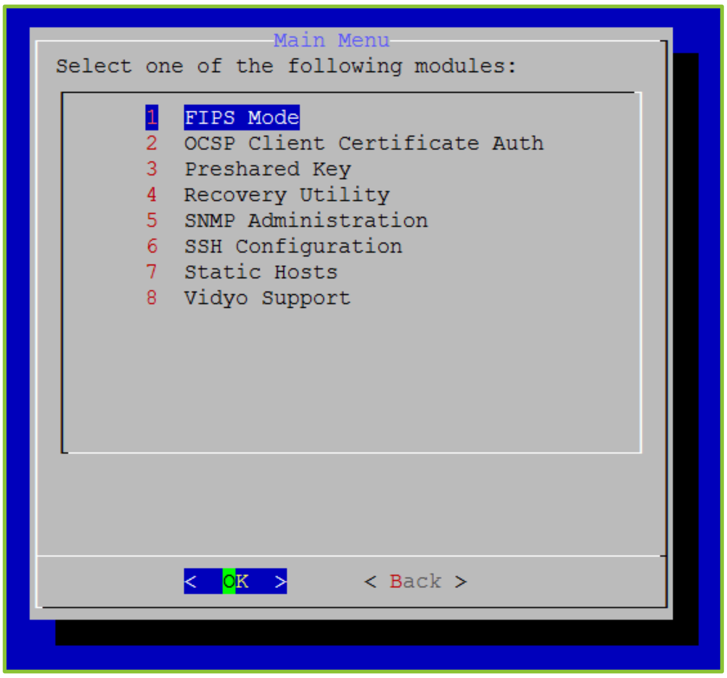
   The Main Menu displays.

   ```
                   Main Menu
   Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown

           <  OK  >        < Exit >
   ```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

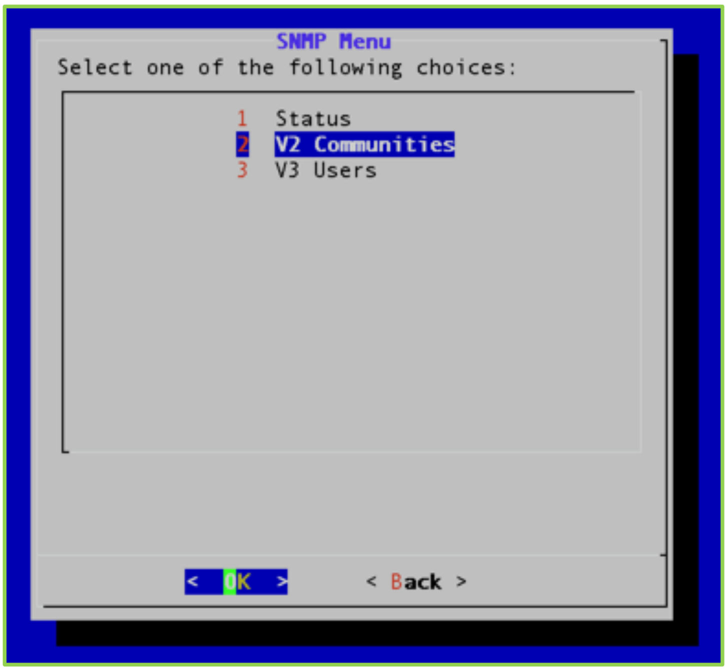
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1  FIPS Mode
        2  OCSP Client Certificate Auth
        3  Preshared Key
        4  Recovery Utility
        5  SNMP Administration
        6  SSH Configuration
        7  Static Hosts
        8  Vidyo Support

        <  OK  >       < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.

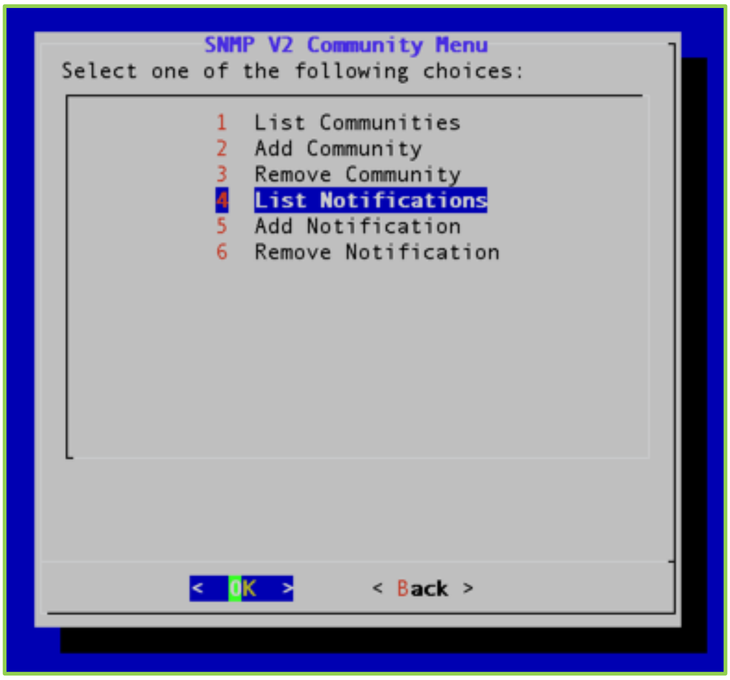


```
SNMP Menu
Select one of the following choices:

               1  Status
               2  V2 Communities
               3  V3 Users

        <  OK  >       < Back >
```

6. Enter **2** to select the V2 Communities option.

7. Press the **Enter** key to select **OK**.

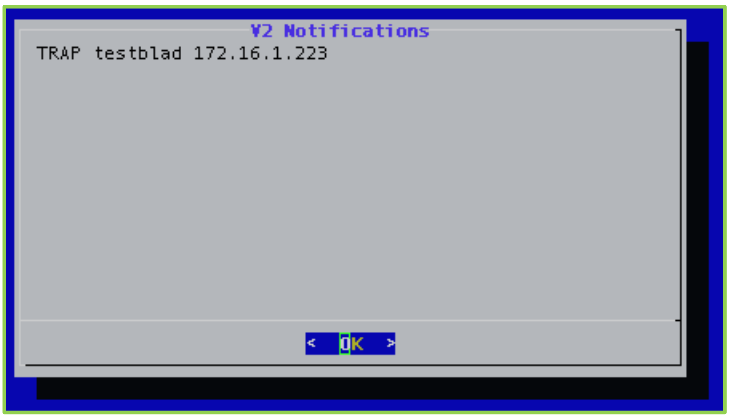
   The SNMP V2 Community Menu displays.



```
Select one of the following choices:
```

8. Enter **4** to select the List Notifications option.
9. Press the **Enter** key to select **OK**.

   The *V2 Notifications* window displays.



```
TRAP testblad 172.16.1.223
```

10. Press the **Enter** key to select **OK**.

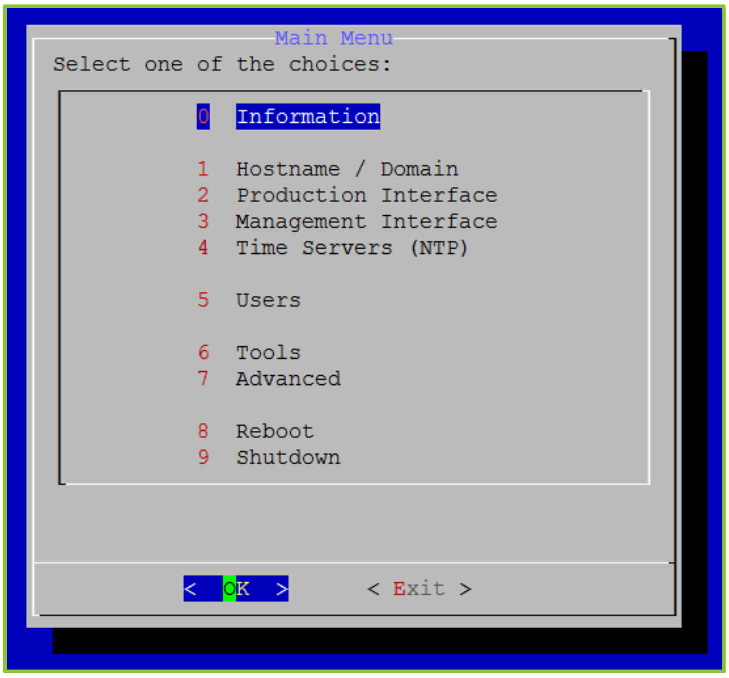
Adding SNMP v2 Notifications

To add an SNMP v2 notification:

1. Log in to the System Console.

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

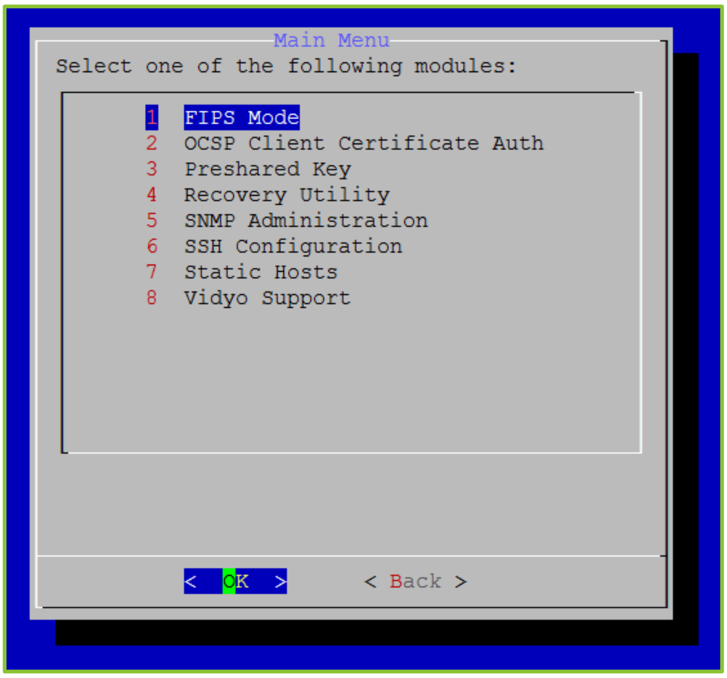
The Main Menu displays.



```
                    Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown


              <  OK  >      < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

The Main Menu for the Advanced configuration displays.

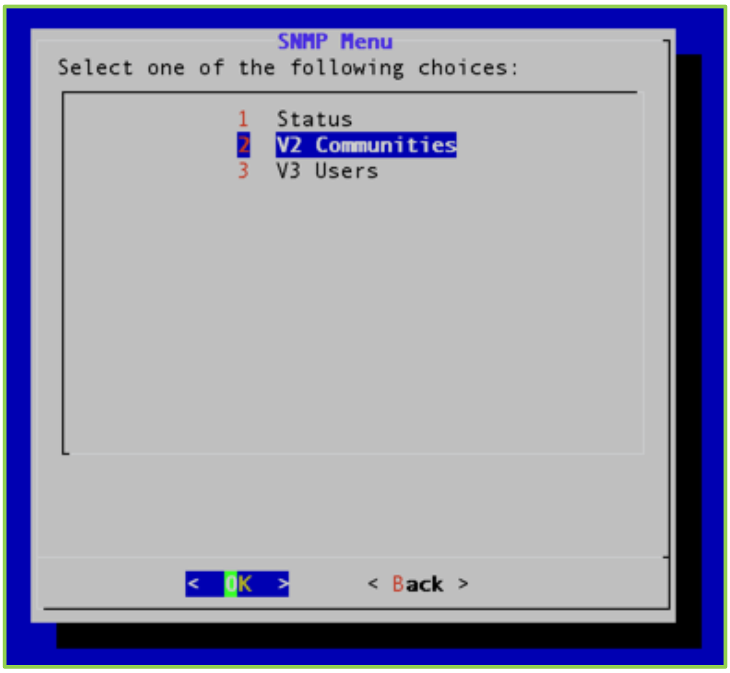


```
Main Menu
Select one of the following modules:

      1  FIPS Mode
      2  OCSP Client Certificate Auth
      3  Preshared Key
      4  Recovery Utility
      5  SNMP Administration
      6  SSH Configuration
      7  Static Hosts
      8  Vidyo Support

          <  OK  >      < Back >
```

4. Enter **5** to select the SNMP Administration option.

5. Press the **Enter** key to select **OK**.

   The SNMP Menu displays.

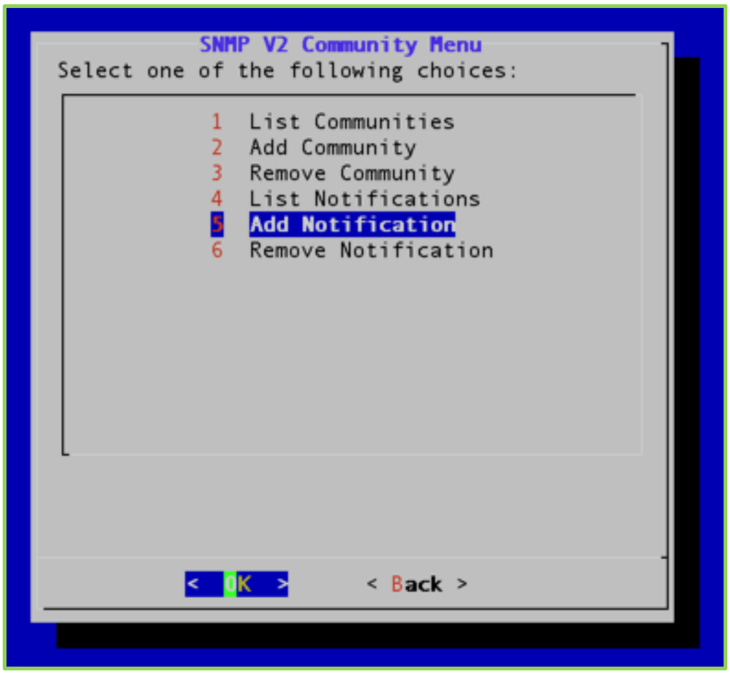


```
SNMP Menu
Select one of the following choices:

             1  Status
             2  V2 Communities
             3  V3 Users

          <  OK  >      < Back >
```

6. Enter **2** to select the V2 Communities option.

7. Press the **Enter** key to select **OK**.

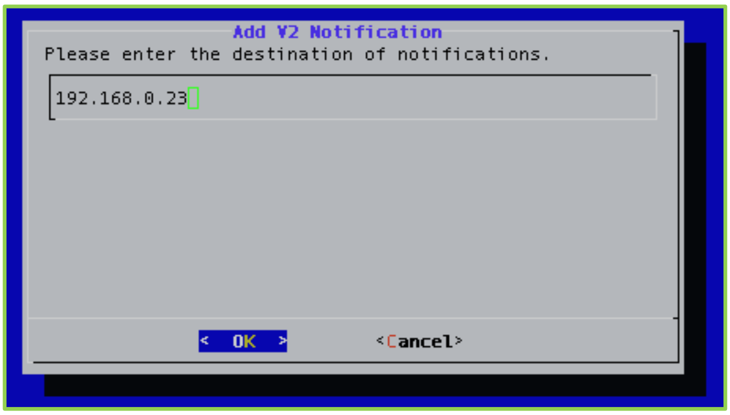
   The SNMP V2 Community Menu displays.



Select one of the following choices:

8. Enter **5** to select the Add Notifications option.
9. Press the **Enter** key to select **OK**.

   The *Add V2 Notification* window displays.

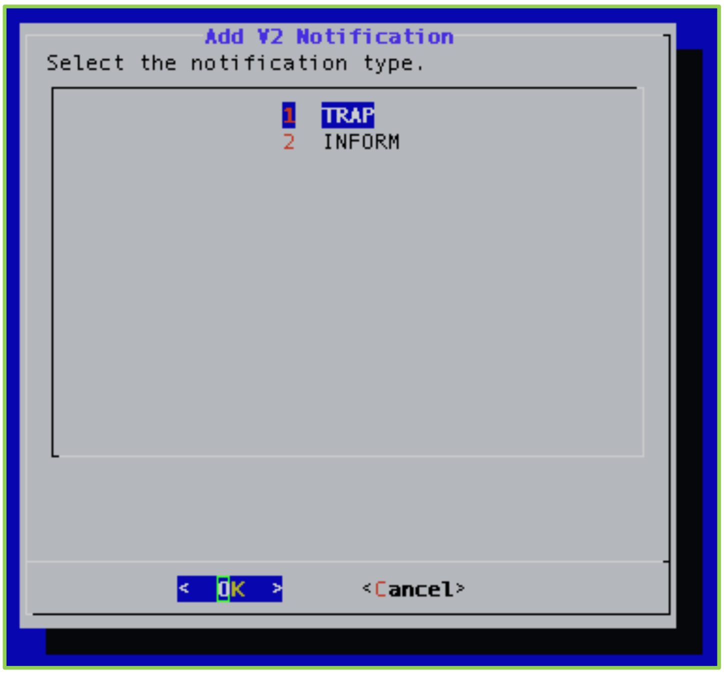


Please enter the destination of notifications.

192.168.0.23

10. Enter the IP address of the SNMP notification’s destination.
11. Press the **Enter** key to select **OK**.

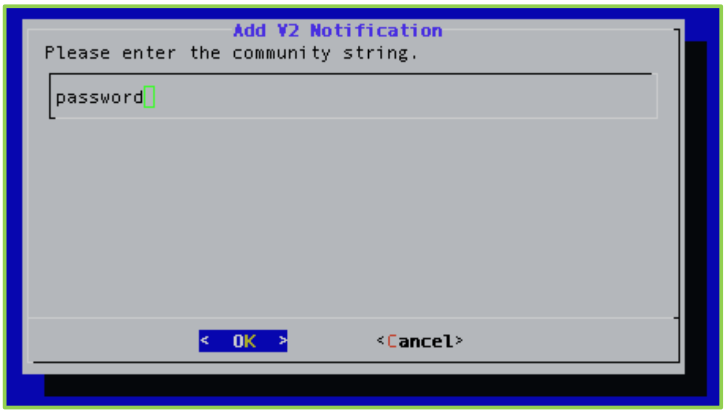
The next *Add V2 Notification* window displays.



Add V2 Notification

Select the notification type.

12. Enter **1** if the notification type is a **TRAP** or enter **2** if the notification type is an **INFORM**.
13. Press the Enter key to select OK.



Add V2 Notification

Please enter the community string.

password

14. Enter the password for the community string.
15. Press the Enter key to select OK.

    A message displays stating “Successfully added notification.”
16. Press the Enter key to select OK.

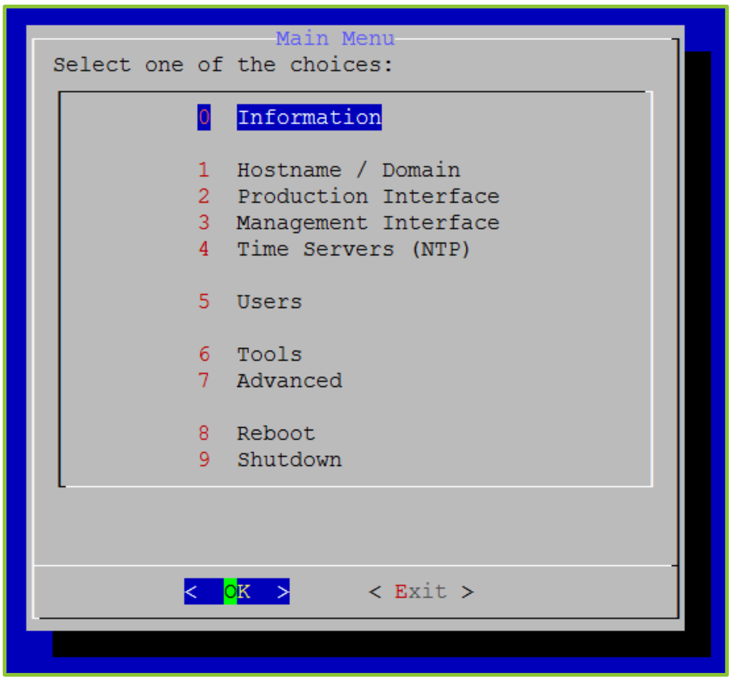
Removing SNMP v2 Notifications

To remove an SNMP v2 notification:

1. Log in to the System Console.

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

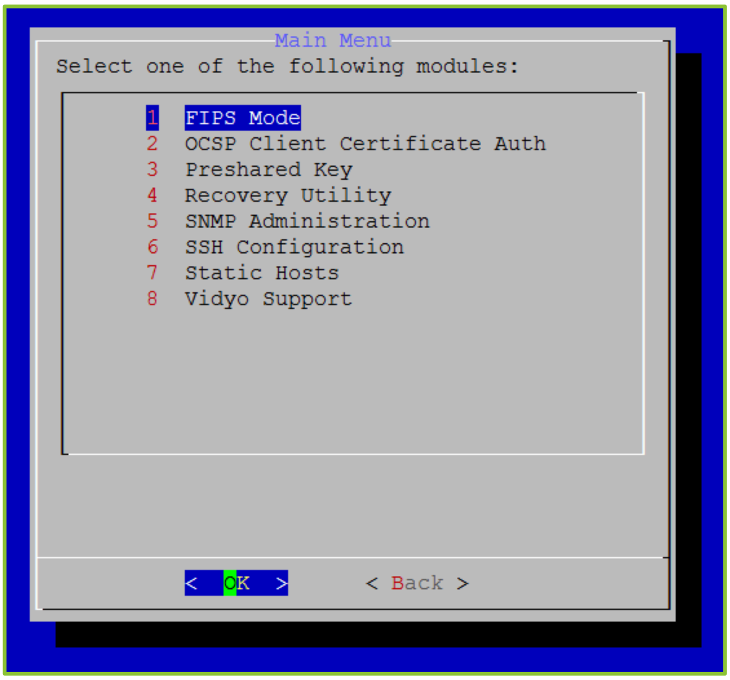
   The Main Menu displays.



```
                    Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown

            <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

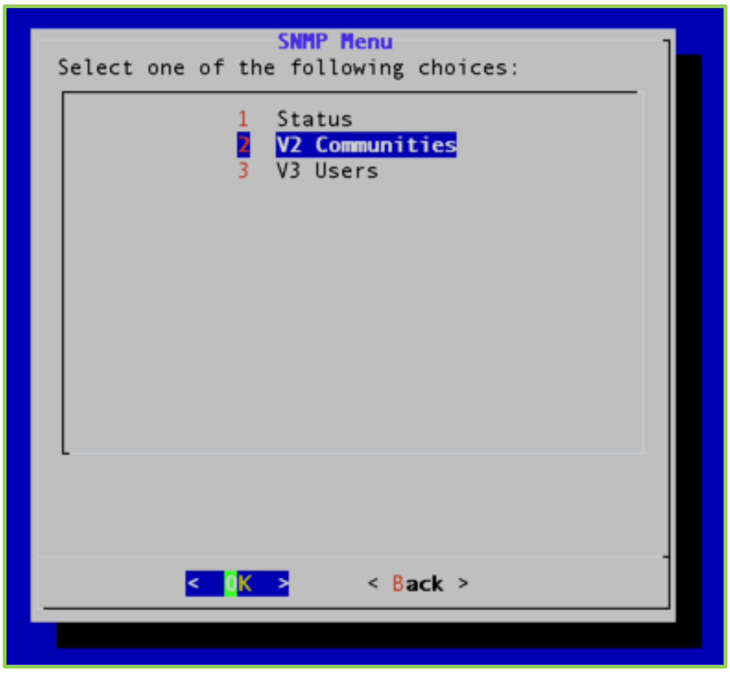
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

          <  OK  >        < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

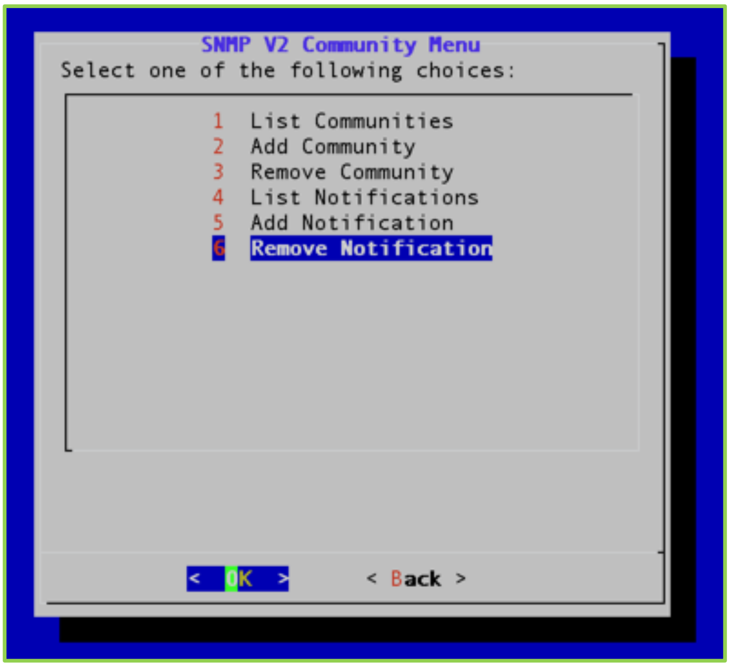
   The SNMP Menu displays.



```
SNMP Menu
Select one of the following choices:

               1   Status
               2   V2 Communities
               3   V3 Users

          <  OK  >        < Back >
```

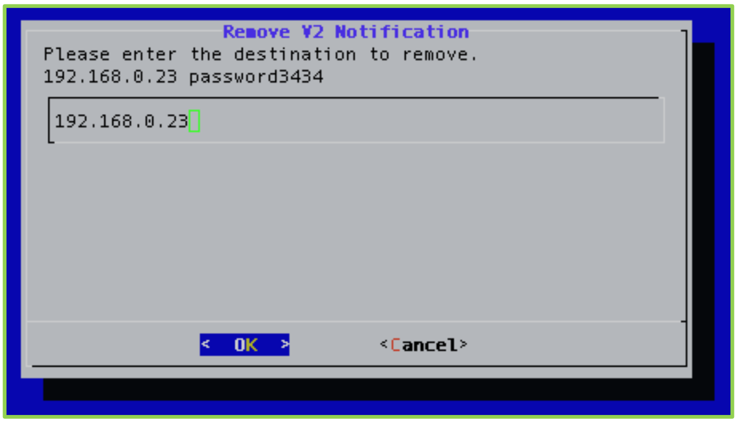
6. Enter **2** to select the V2 Communities option.
7. Press the Enter key to select OK.

   The SNMP V2 Community Menu displays.



8. Enter **6** to select the Remove Notification option.
9. Press the Enter key to select OK.

   The *Remove V2 Notification* window displays.



Please enter the destination to remove.
192.168.0.23 password3434

192.168.0.23

10. Enter the IP address of the notification you want to remove.

    The list of notifications available for removal is displayed above the text box.
11. Press the Enter key to select OK.

    A message displays stating “Successfully removed notification.”

12. Press the **Enter** key to select **OK**.

Configuring SNMP v3 Users

This section describes how to list the SNMP v3 users, add and remove them, and list, add, and remove notifications.

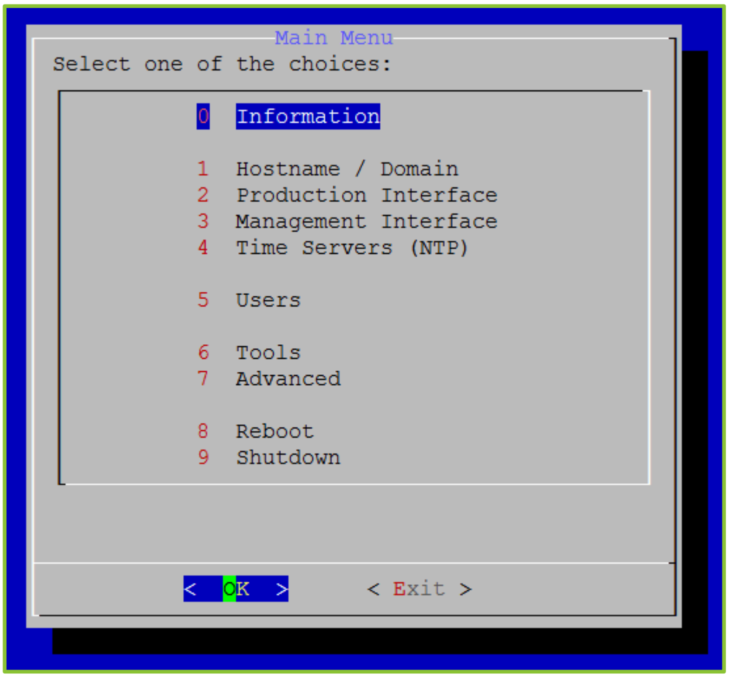
Listing SNMP v3 Users

To list SNMP v3 Users:

1. Log in to the System Console.

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

   The Main Menu displays.

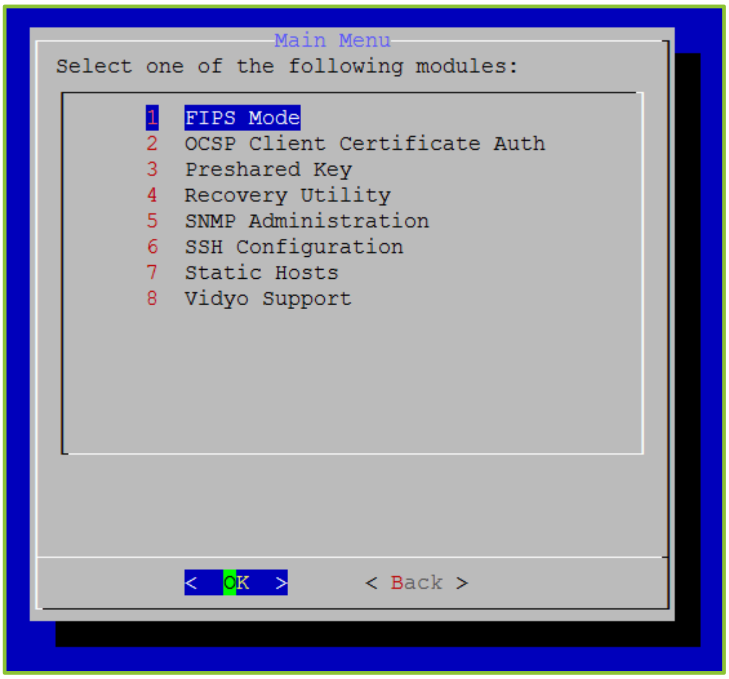


```
                     Main Menu
 Select one of the choices:

          0   Information

          1   Hostname / Domain
          2   Production Interface
          3   Management Interface
          4   Time Servers (NTP)

          5   Users

          6   Tools
          7   Advanced

          8   Reboot
          9   Shutdown


        <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.

3. Press the **Enter** key to select **OK**.

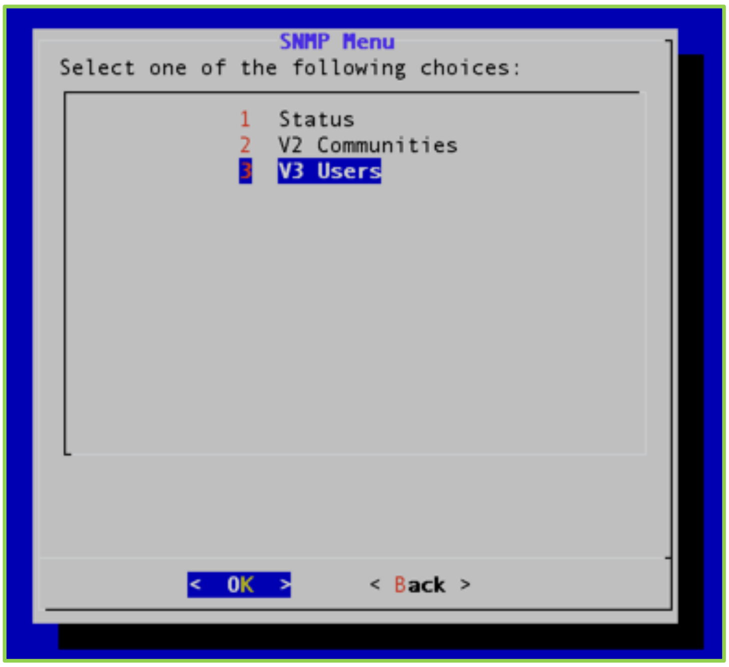
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

    1  FIPS Mode
    2  OCSP Client Certificate Auth
    3  Preshared Key
    4  Recovery Utility
    5  SNMP Administration
    6  SSH Configuration
    7  Static Hosts
    8  Vidyo Support

    <  OK  >       < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.

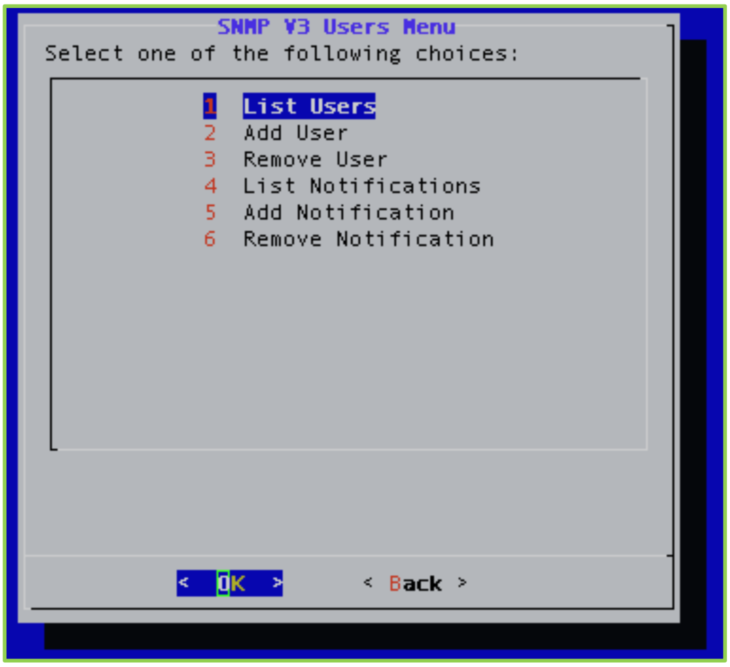


```
SNMP Menu
Select one of the following choices:

    1  Status
    2  V2 Communities
    3  V3 Users

    <  OK  >       < Back >
```

6. Enter **3** to select the V3 Users option.

7. Press the **Enter** key to select **OK**.

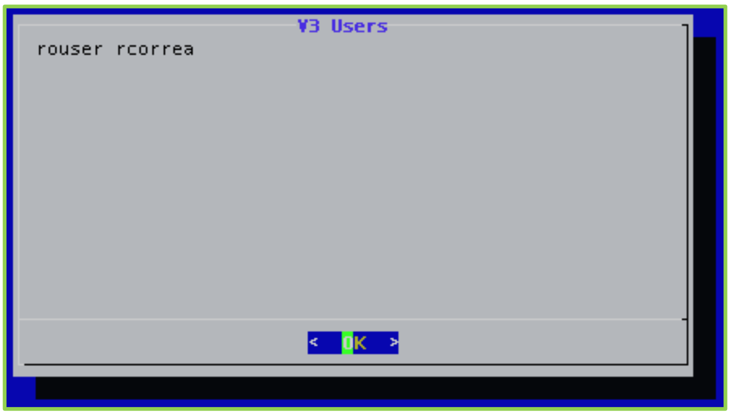
   The SNMP V3 Community Menu displays.



```
SNMP V3 Users Menu
Select one of the following choices:

            1  List Users
            2  Add User
            3  Remove User
            4  List Notifications
            5  Add Notification
            6  Remove Notification

        <  OK  >          <  Back  >
```

8. Enter **1** to select the List Users option.
9. Press the **Enter** key to select **OK**.

   The *V3 Users* window, which lists all the V3 users, displays.



```
V3 Users
rouser rcorrea

                 <  OK  >
```

10. Press the **Enter** key to select **OK**.

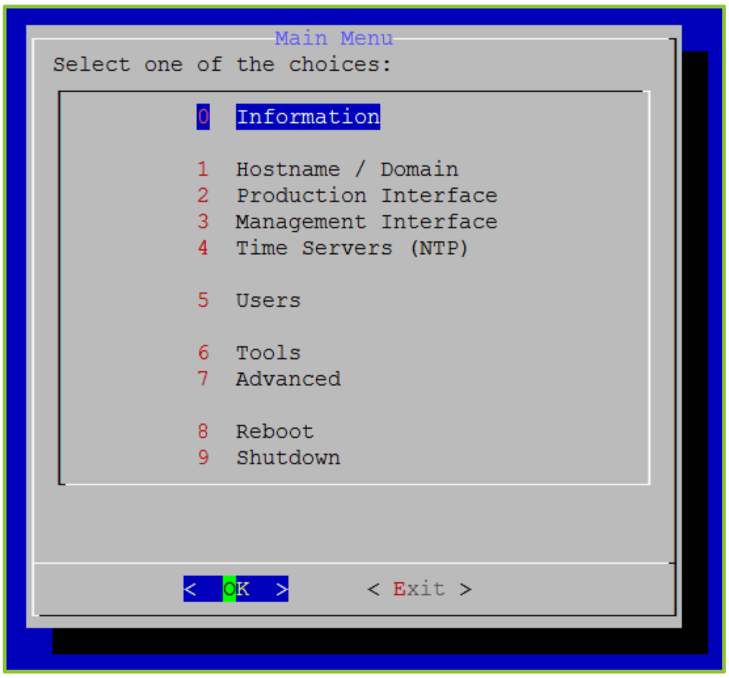
Adding SNMP v3 Users

To add SNMP v3 Users:

1. Log in to the System Console.

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

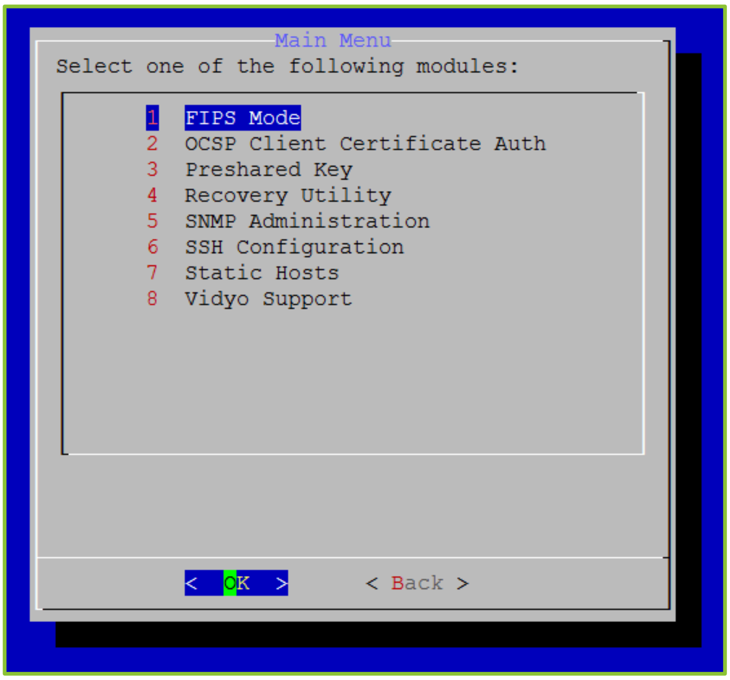
The Main Menu displays.



```
                    Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown


             <  OK  >       < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

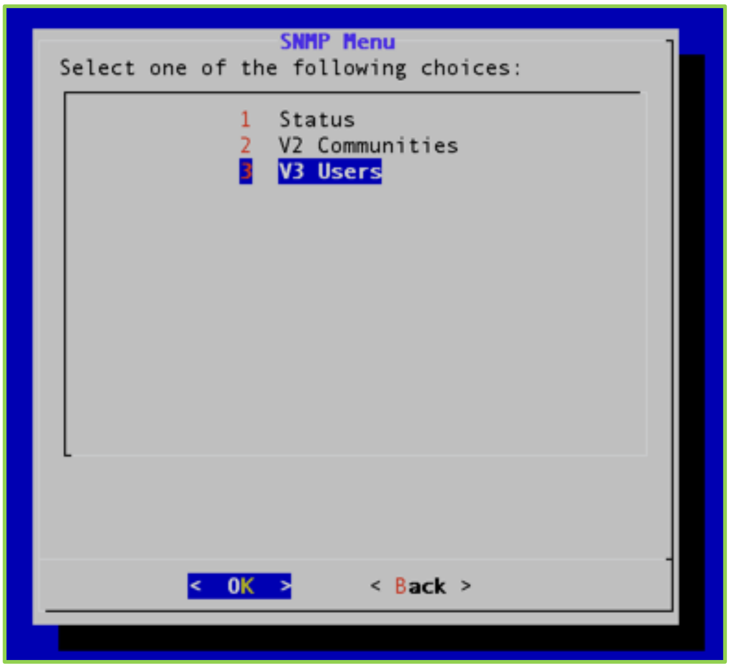
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

        <  OK  >          < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.

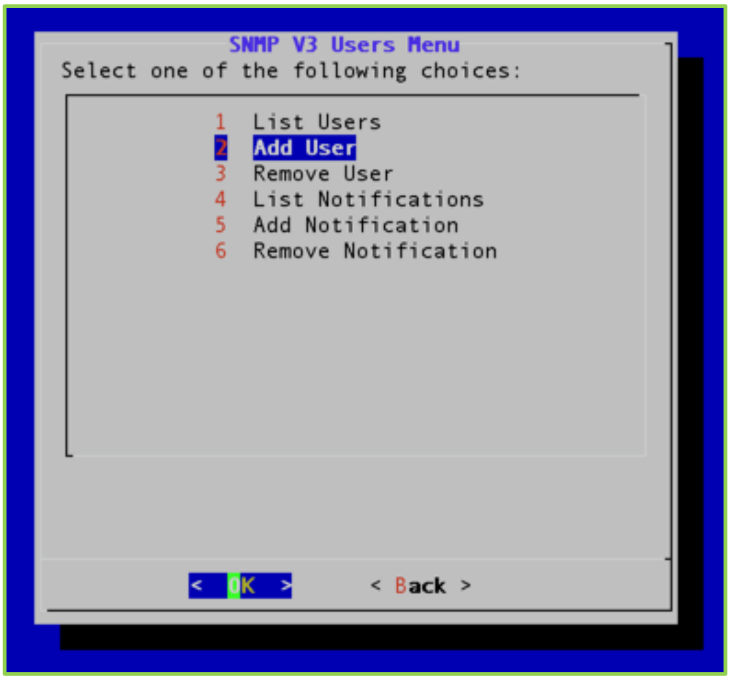


```
SNMP Menu
Select one of the following choices:

               1  Status
               2  V2 Communities
               3  V3 Users

        <  OK  >          < Back >
```

6. Enter **3** to select the V3 Users option.

7. Press the **Enter** key to select **OK**.

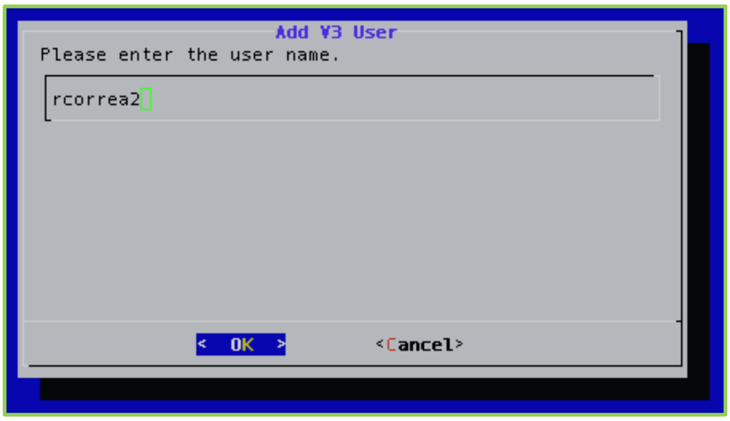
   The SNMP V3 Community Menu displays.



Select one of the following choices:

8. Enter **2** to select the Add User option.
9. Press the **Enter** key to select **OK**.

   The *Add V3 User* window displays.

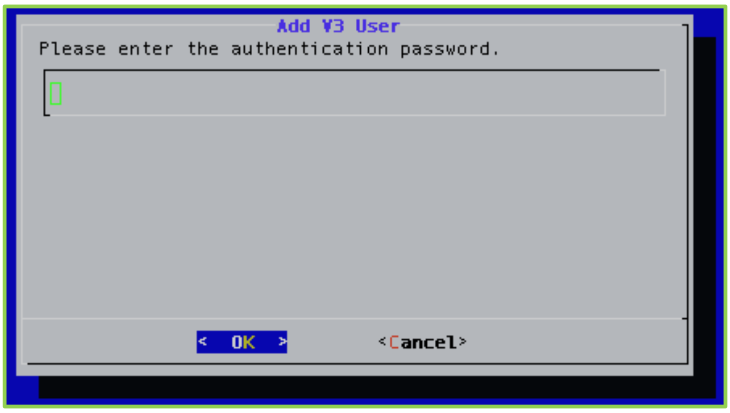


Please enter the user name.

rcorrea2

10. Enter the user name of the v3 user you want to add.
11. Press the **Enter** key to select **OK**.

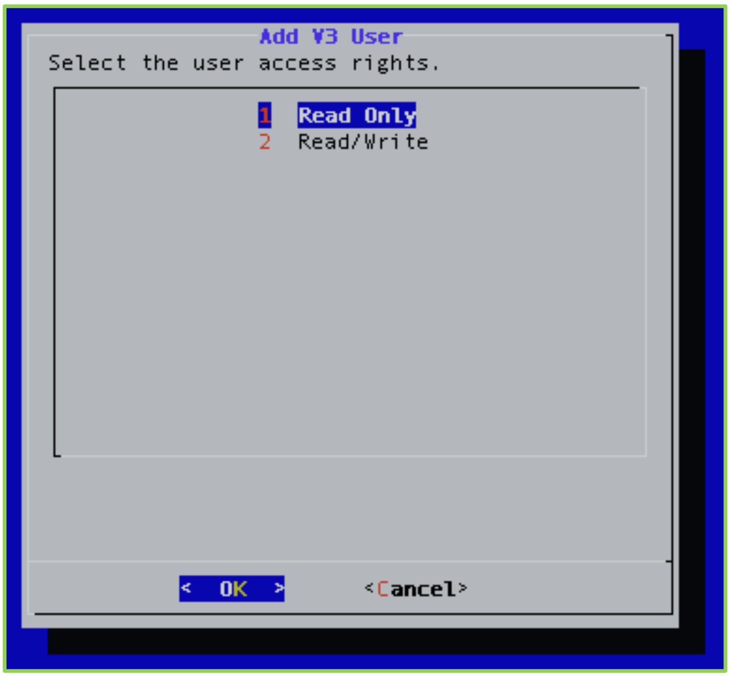
The next *Add V3 User* window displays.



```
Add V3 User
Please enter the authentication password.
```

12. Enter the password for the new V3 user.
13. Press the **Enter** key to select **OK**.

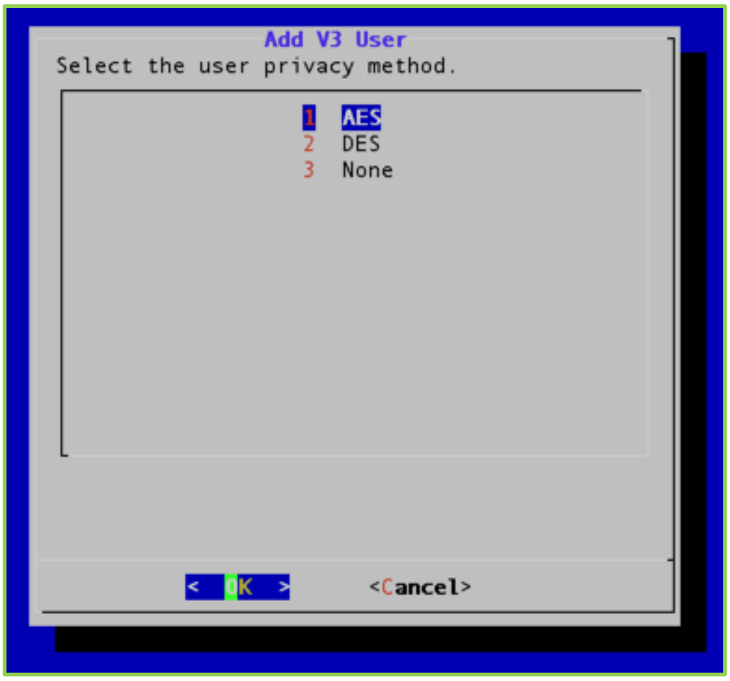
The next *Add V3 User* window displays.



```
Add V3 User
Select the user access rights.
    1  Read Only
    2  Read/Write
```

14. Enter **1** if you want the new v3 user's access rights to be read only or enter **2** if you want the new v3 user's access rights to be read and write.

15. Press the Enter key to select OK.



```
Add V3 User
Select the user privacy method.

1  AES
2  DES
3  None

<  OK  >     <Cancel>
```

16. Select the user privacy method: **AES**, **DES**, or **None**.

17. Press the Enter key to select OK.

18. Enter the privacy password.

19. Press the Enter key to select OK.

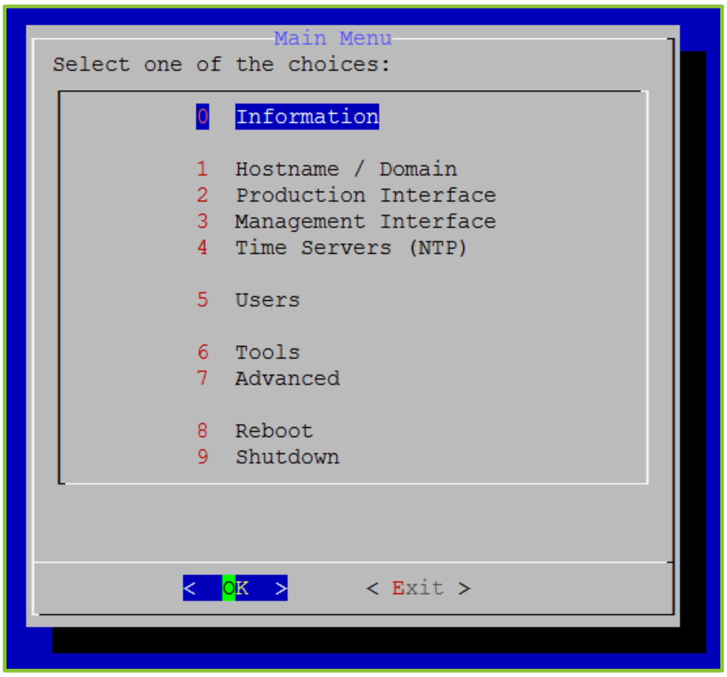
Removing an SNMP v3 User

To remove an SNMP v3 user:

1. Log in to the System Console.

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

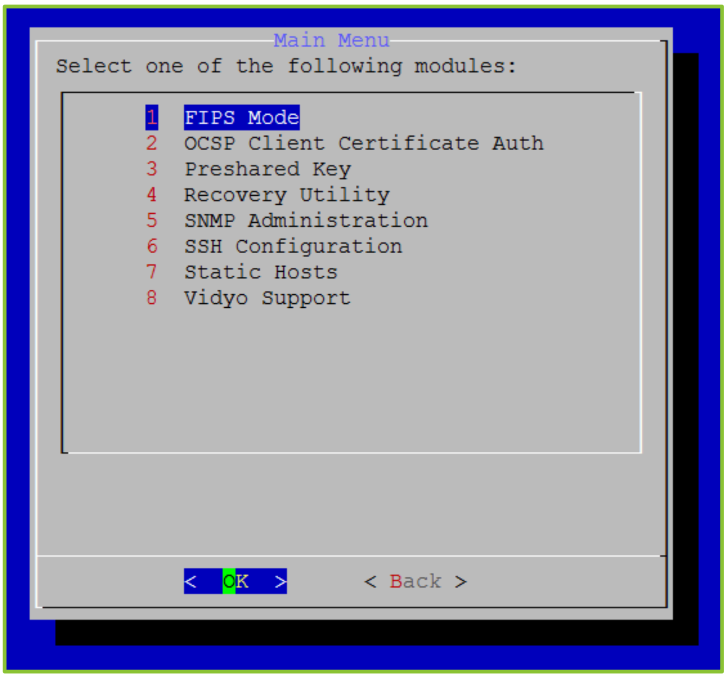
The Main Menu displays.



```
                    Main Menu
Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown


          <  OK  >         < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

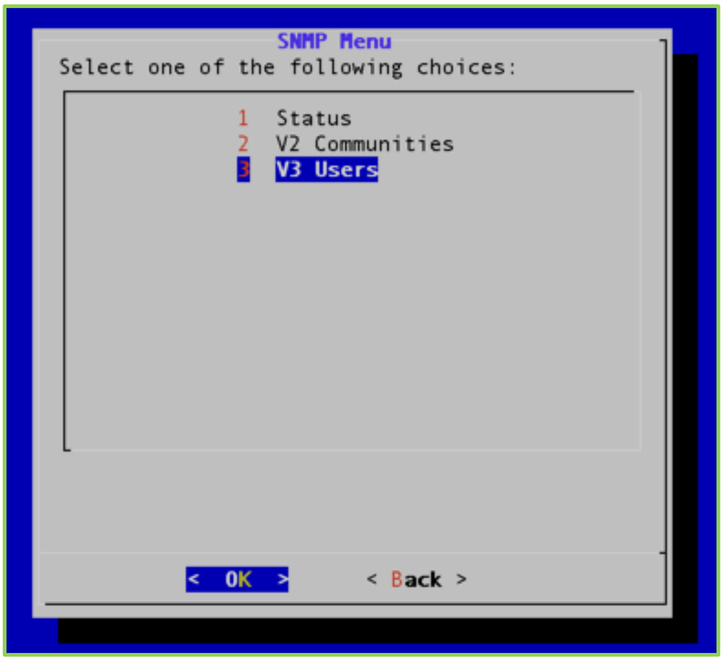
The Main Menu for the Advanced configuration displays.



```
                    Main Menu
Select one of the following modules:

          1  FIPS Mode
          2  OCSP Client Certificate Auth
          3  Preshared Key
          4  Recovery Utility
          5  SNMP Administration
          6  SSH Configuration
          7  Static Hosts
          8  Vidyo Support


          <  OK  >         < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**.

   The SNMP Menu displays.

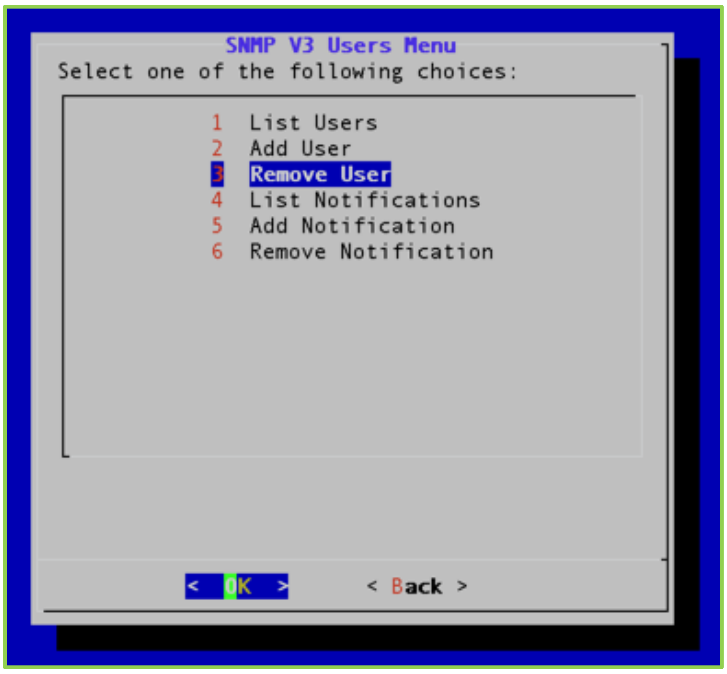


SNMP Menu

Select one of the following choices:

6. Enter **3** to select the V3 Users option.
7. Press the **Enter** key to select **OK**.

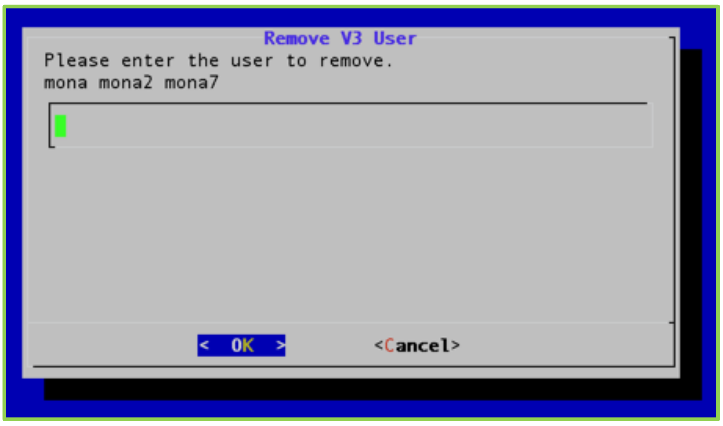
The SNMP V3 Users Menu displays.



```
SNMP V3 Users Menu
Select one of the following choices:
```

8. Enter **3** to select the Remove User option.
9. Press the Enter key to select OK.

   The *Remove V3 User* window displays.



```
Remove V3 User
Please enter the user to remove.
mona mona2 mona7
```

10. Press the Enter key to select OK.

    A message displays stating “Successfully removed user.”

11. Press the Enter key to select OK.

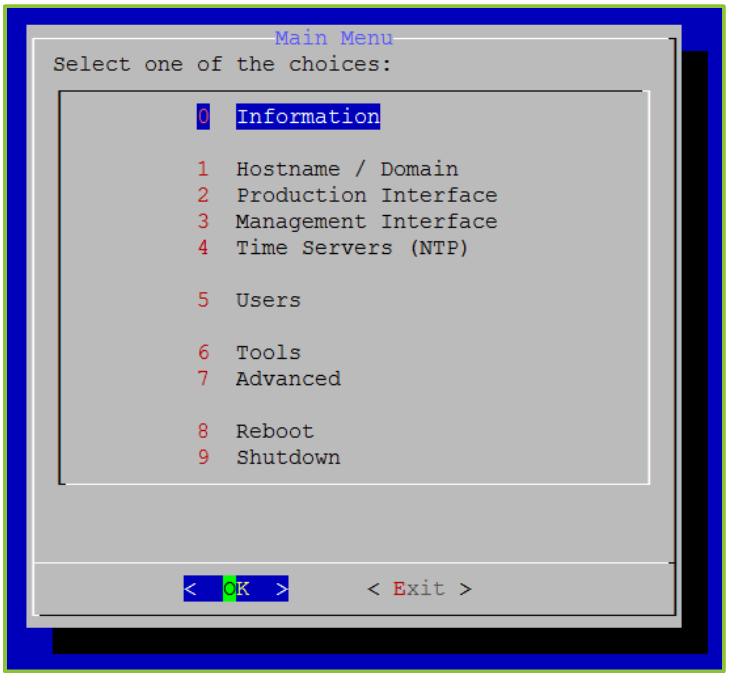
Listing SNMP v3 Notifications

To list an SNMP v3 notification:

1. Log in to the System Console.

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

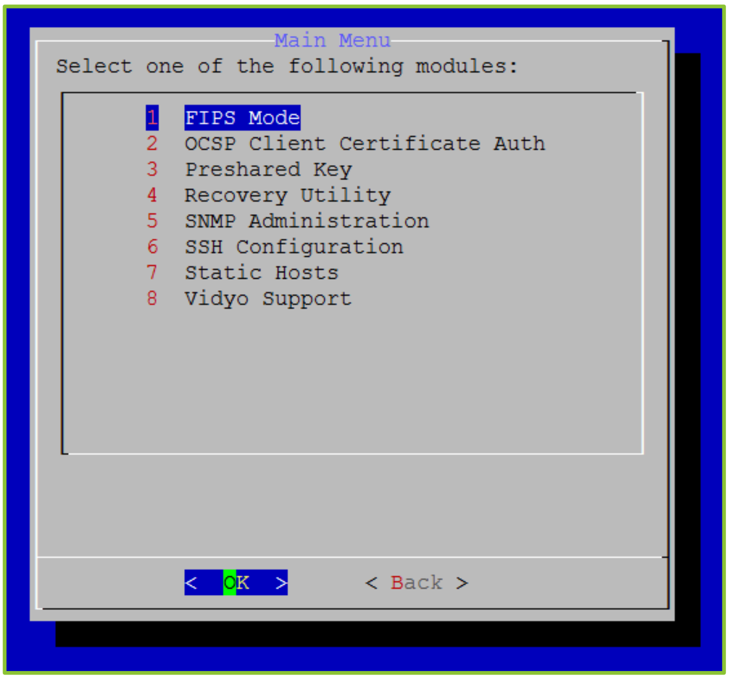
   The Main Menu displays.

   ```
   Main Menu
   Select one of the choices:

       0  Information

       1  Hostname / Domain
       2  Production Interface
       3  Management Interface
       4  Time Servers (NTP)

       5  Users

       6  Tools
       7  Advanced

       8  Reboot
       9  Shutdown

   <  OK  >        < Exit >
   ```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

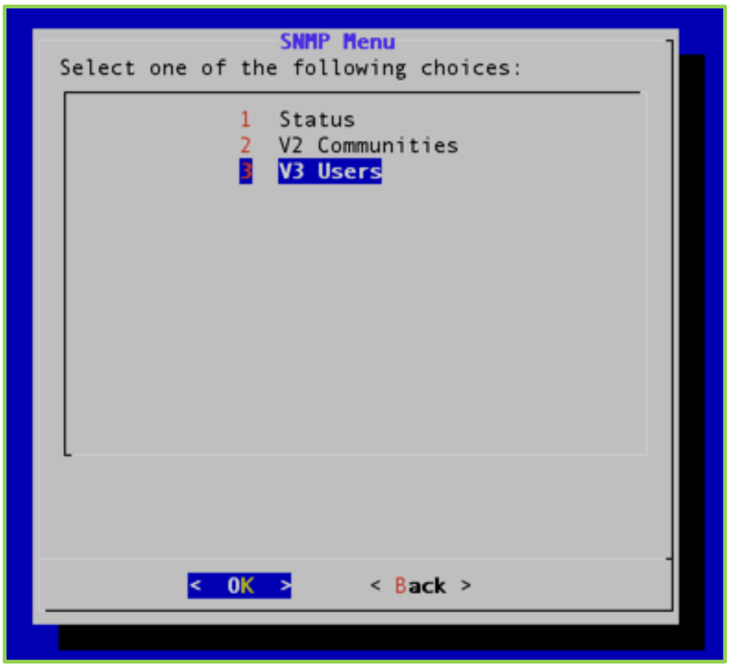
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

          <  OK  >      < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.

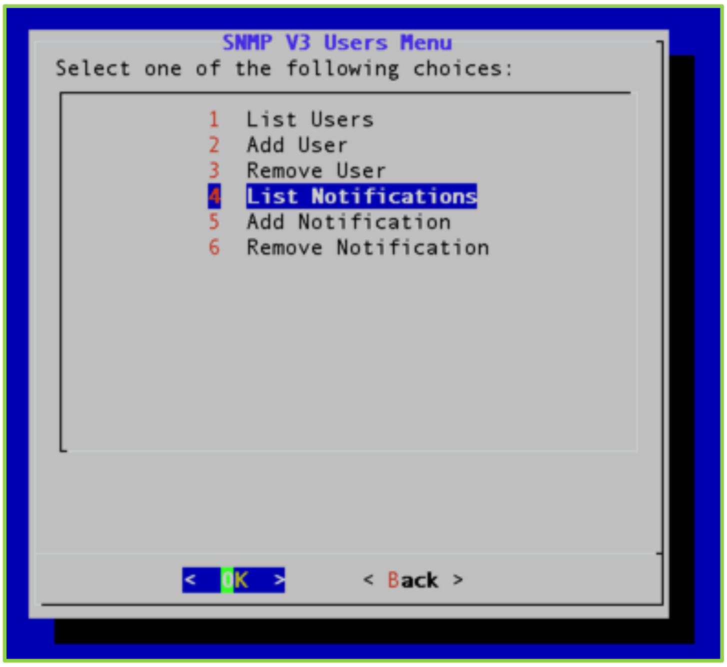


```
SNMP Menu
Select one of the following choices:

            1   Status
            2   V2 Communities
            3   V3 Users

          <  OK  >      < Back >
```

6. Enter **3** to select the V3 Users option.

7. Press the **Enter** key to select **OK**.

   The SNMP V3 Users Menu displays.

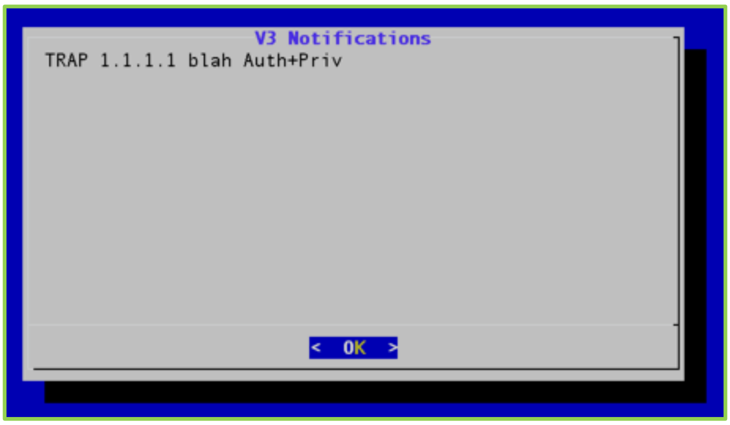


```
Select one of the following choices:
```

8. Enter **4** to select the List Notifications option.

9. Press the **Enter** key to select **OK**.

   The *V3 Notifications* window displays.



```
TRAP 1.1.1.1 blah Auth+Priv
```

10. Press the **Enter** key to select **OK**.

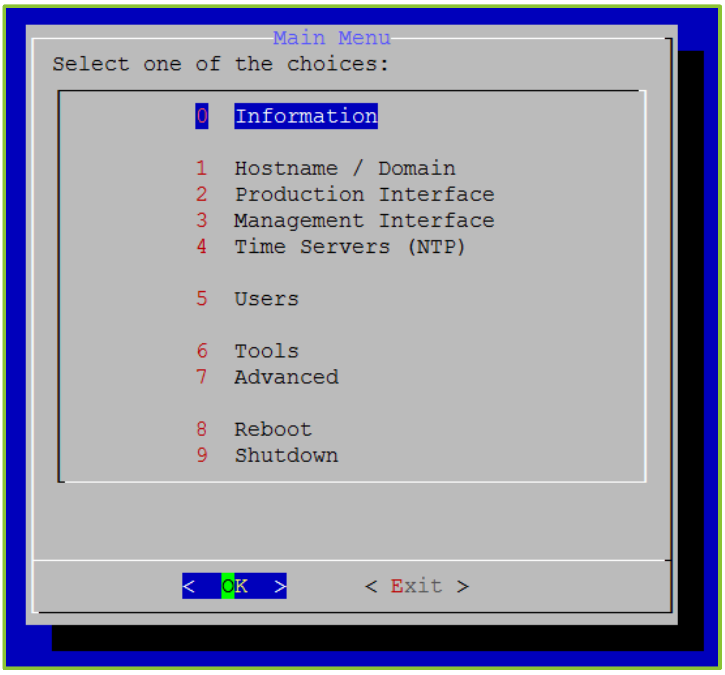
Adding SNMP v3 Notifications

To add an SNMP v3 notification:

1. Log in to the System Console.

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

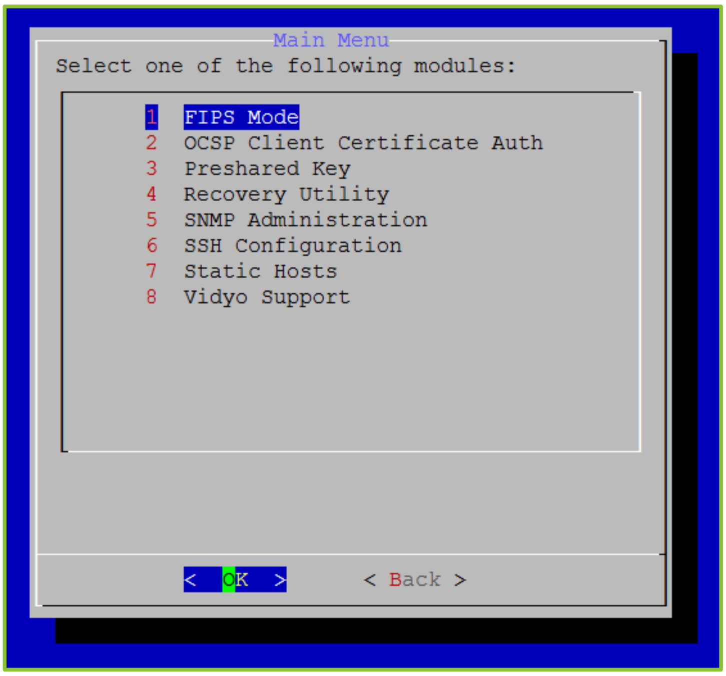
The Main Menu displays.



```
                      Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown


            <  OK  >      < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

The Main Menu for the Advanced configuration displays.



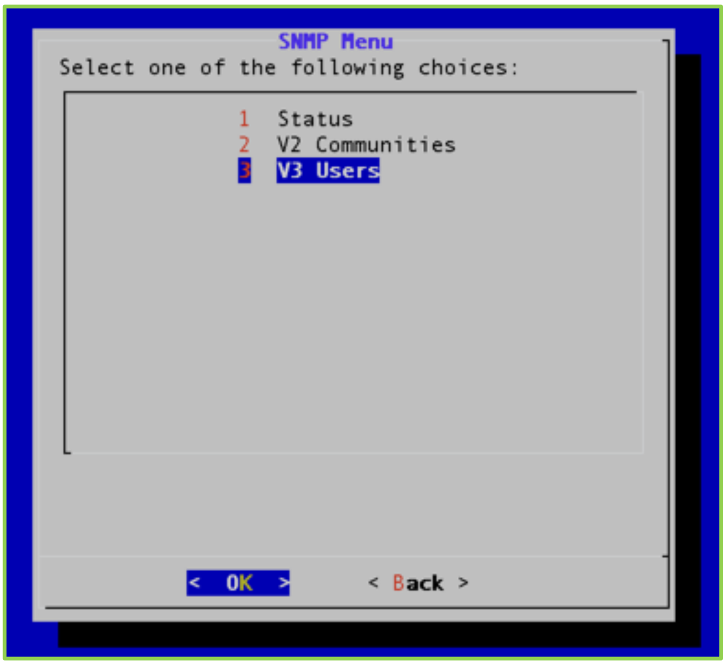
Main Menu

Select one of the following modules:

```
1   FIPS Mode
2   OCSP Client Certificate Auth
3   Preshared Key
4   Recovery Utility
5   SNMP Administration
6   SSH Configuration
7   Static Hosts
8   Vidyo Support
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.



SNMP Menu

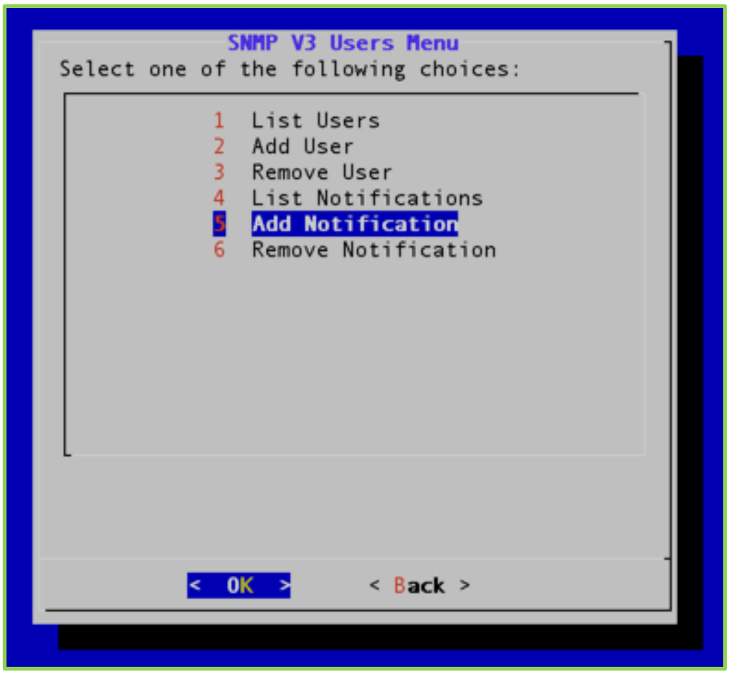
Select one of the following choices:

```
1   Status
2   V2 Communities
3   V3 Users
```

6. Enter **3** to select the V3 Users option.

7. Press the Enter key to select OK.

   The SNMP V3 Users Menu displays.



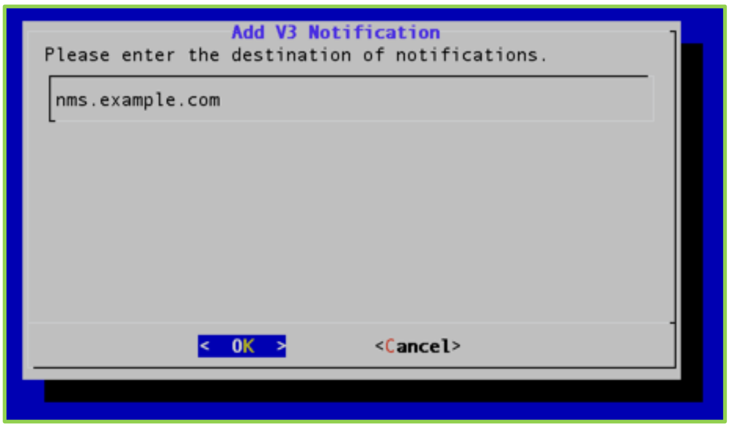
SNMP V3 Users Menu

Select one of the following choices:

8. Enter **5** to select the Add Notification option.

9. Press the Enter key to select OK.

   The *Add V3 Notification* window displays.



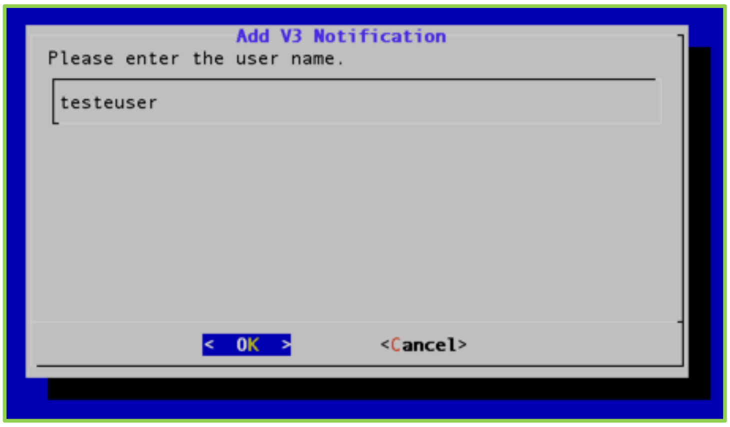
Add V3 Notification

Please enter the destination of notifications.

nms.example.com

10. Enter the IP address or FQDN of the notification's destination.

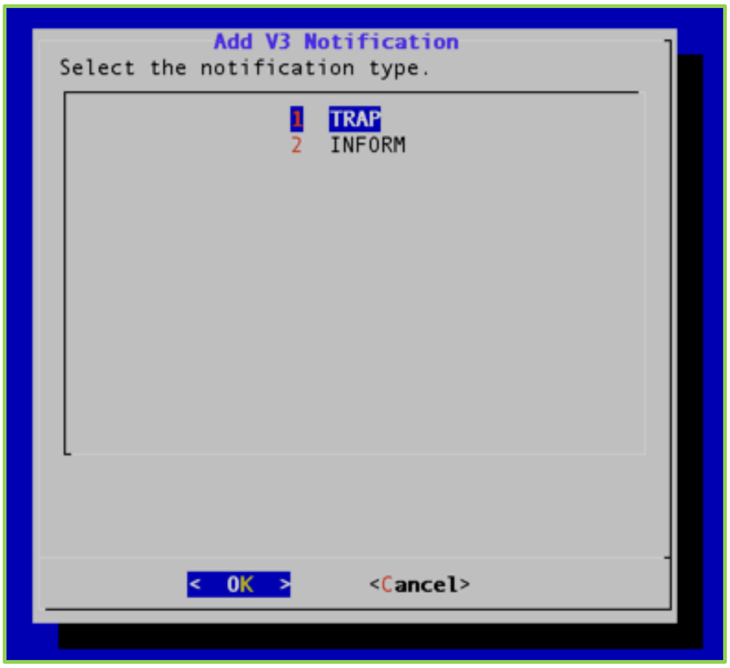
11. Press the **Enter** key to select **OK**.



```
Add V3 Notification
Please enter the user name.

testeuser
```

12. Enter the user name.

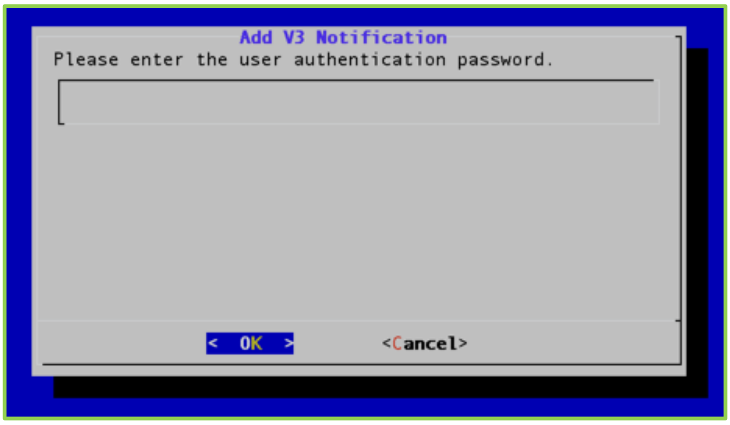
13. Press the **Enter** key to select **OK**.



```
Add V3 Notification
Select the notification type.

1  TRAP
2  INFORM
```

14. Enter **`1`** if the notification type is a **`TRAP`** or enter **`2`** if the notification type is an **`INFORM`**.

15. Press the Enter key to select OK.

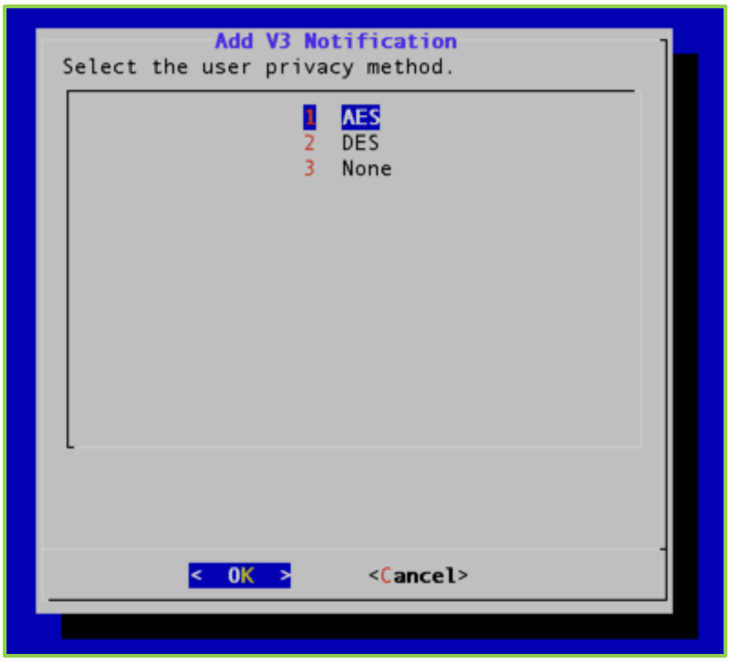


Add V3 Notification

Please enter the user authentication password.

16. Enter the user authentication password.

17. Press the Enter key to select OK.



Add V3 Notification

Select the user privacy method.

18. Select the user privacy method: **AES**, **DES**, or **None**.

19. Press the Enter key to select OK.

20. Enter the privacy password.

21. Press the Enter key to select OK.

    A message displays stating “Successfully added notification.”

22. Press the Enter key to select OK.

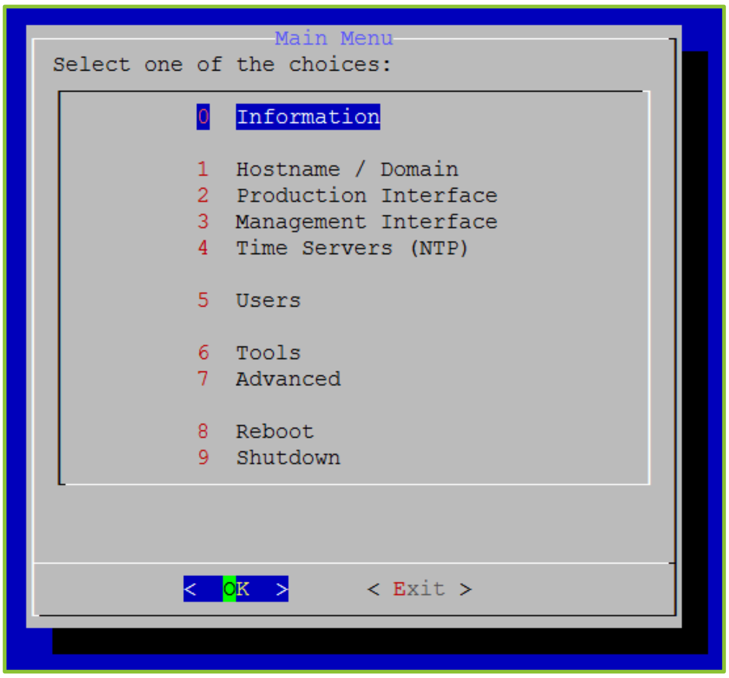
Removing SNMP v3 Notifications

To remove an SNMP v3 notification:

1. Log in to the System Console.

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

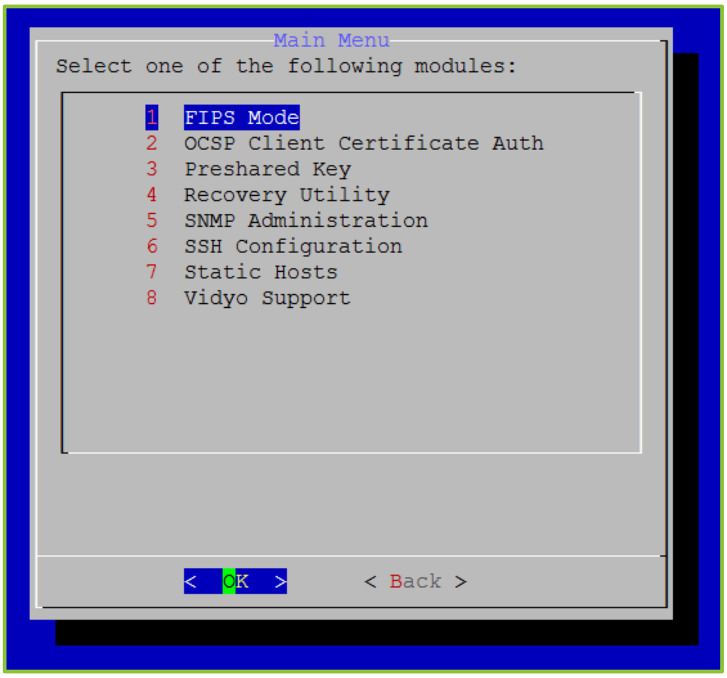
   The Main Menu displays.

```
                     Main Menu
Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown


              <  OK  >      < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

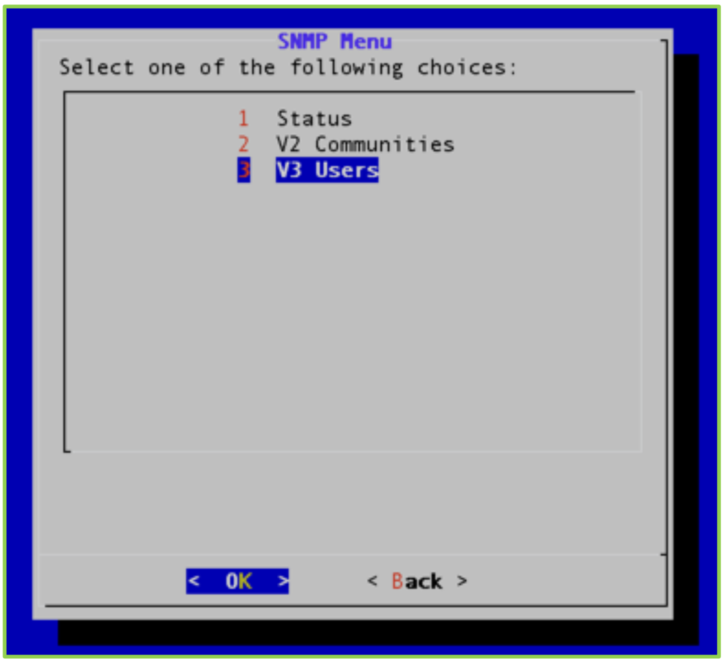
The Main Menu for the Advanced configuration displays.



```
                     Main Menu
Select one of the following modules:

      1  FIPS Mode
      2  OCSP Client Certificate Auth
      3  Preshared Key
      4  Recovery Utility
      5  SNMP Administration
      6  SSH Configuration
      7  Static Hosts
      8  Vidyo Support

          <  OK  >       < Back >
```

4. Enter **5** to select the SNMP Administration option.
5. Press the Enter key to select OK.

   The SNMP Menu displays.

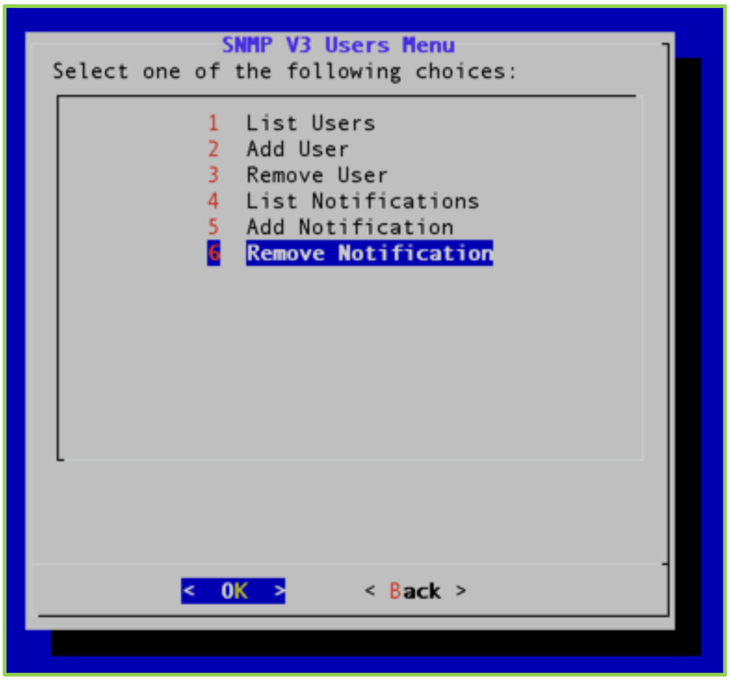


```
                     SNMP Menu
Select one of the following choices:

              1  Status
              2  V2 Communities
              3  V3 Users

          <  OK  >       < Back >
```

6. Enter **3** to select the V3 Users option.

7. Press the **Enter** key to select **OK**.

   The SNMP V3 Users Menu displays.



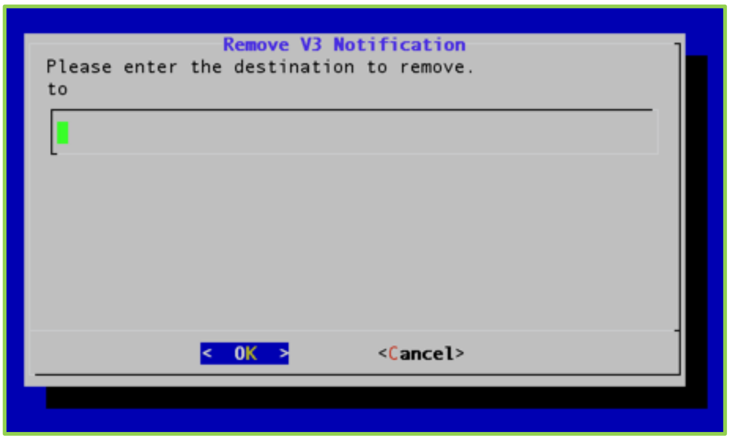
SNMP V3 Users Menu

Select one of the following choices:

8. Enter **6** to select the Remove Notification option.

9. Press the **Enter** key to select **OK**.

   The Remove V3Notification window displays.



Remove V3 Notification

Please enter the destination to remove.
to

10. Enter the IP address or FQDN of the notification you want to remove.

11. Press the **Enter** key to select **OK**.

    A message displays stating "Successfully removed notification."

12. Press the **Enter** key to select **OK**.

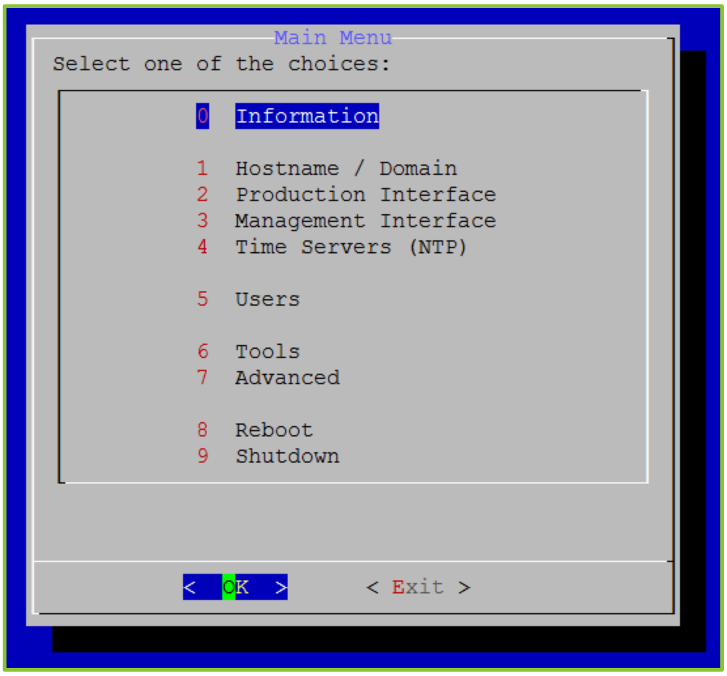
Configuring SSH

To configure SSH:

1. Log in to the System Console.

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

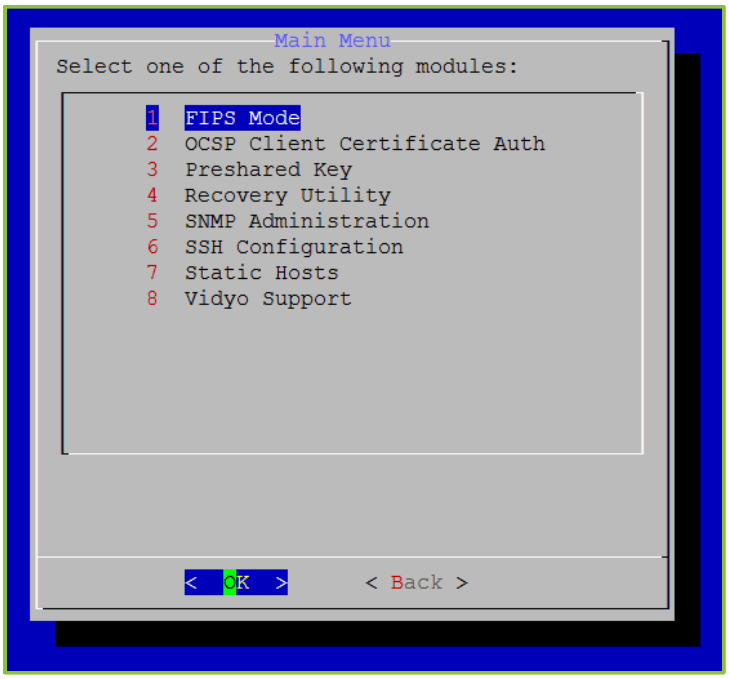
   The Main Menu displays.



```
                     Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown


            <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**.

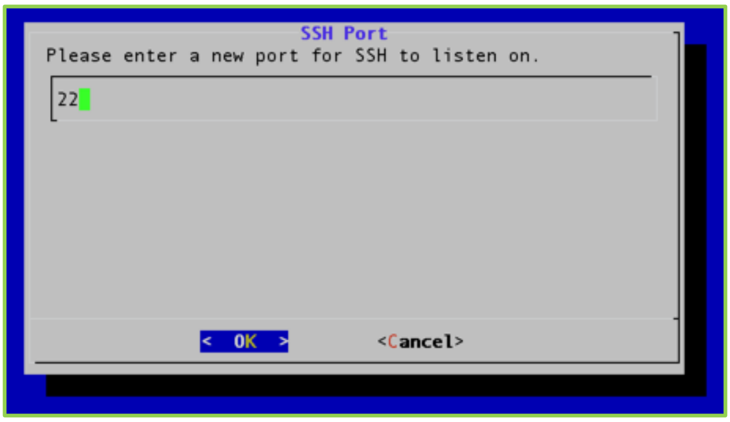
The Main Menu for the Advanced configuration displays.



Select one of the following modules:

4. Enter **6** to select the SSH Configuration option.
5. Press the Enter key to select OK.

   The *SSH Port* window displays.

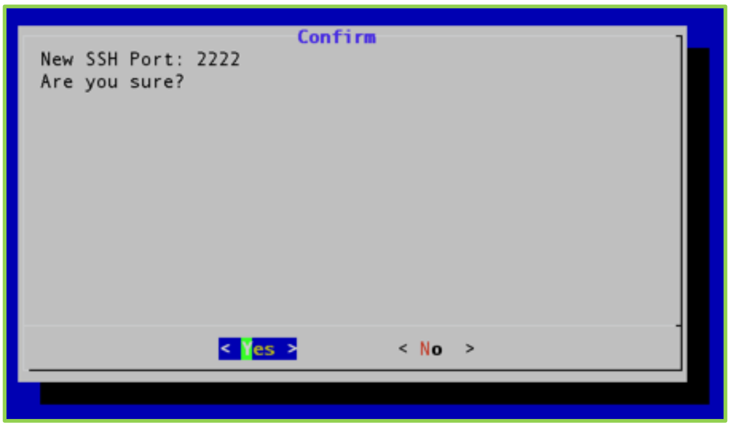


Please enter a new port for SSH to listen on.

22

6. Enter the port number on which SSH can listen.
7. Press the Enter key to select OK.

The *Confirm* window displays.



```
Confirm
New SSH Port: 2222
Are you sure?
```

8. Press the **Enter** key to select **Yes**.

   Another *Confirm* window displays asking if you want to apply the new SSH port setting.

9. Press the **Enter** key to select **Yes**.

Managing Static Hosts

Static Host entries can be added to a single hostfile on your VidyoPortal. These entries are used to map an IP address to a specific Static Host 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.

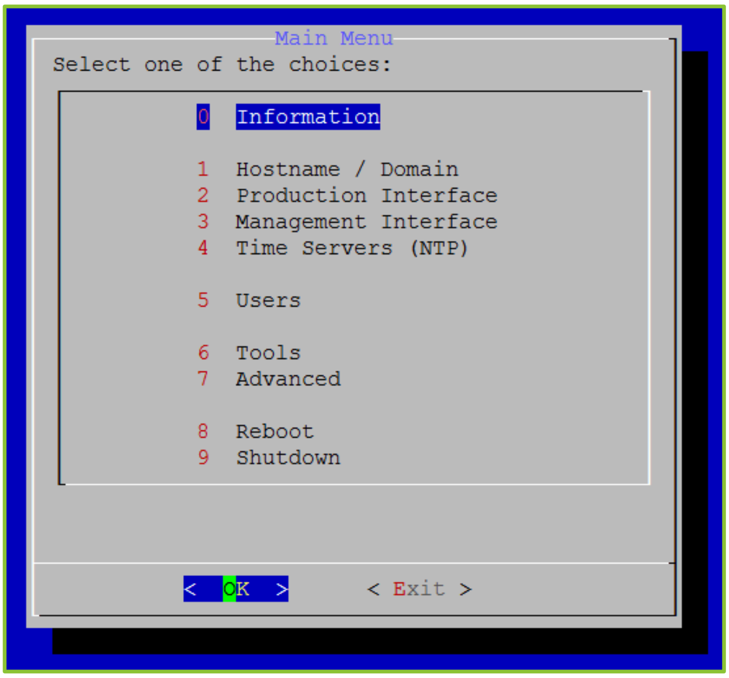
Viewing Active Information

To view active information:

1. Log in to the System Console.

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

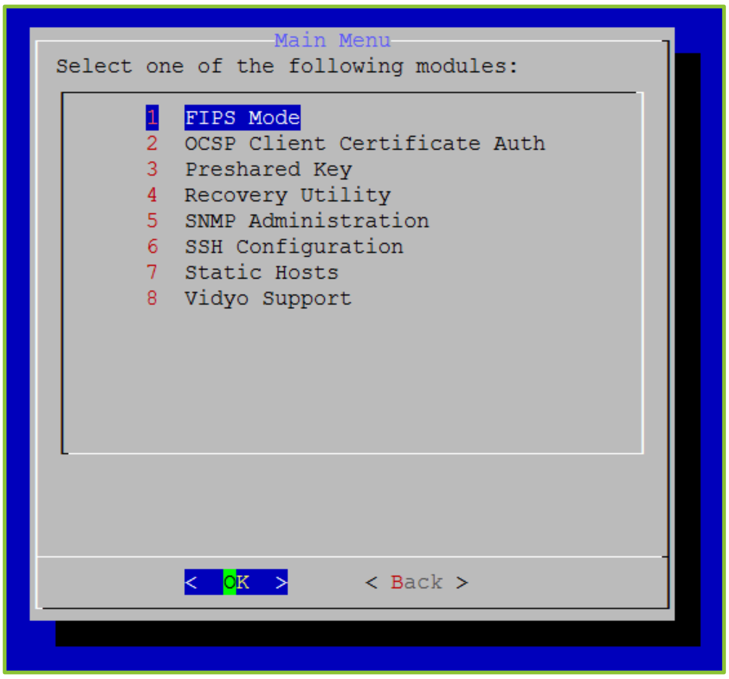
The Main Menu displays.



2. Enter **7** to select the Advanced option.

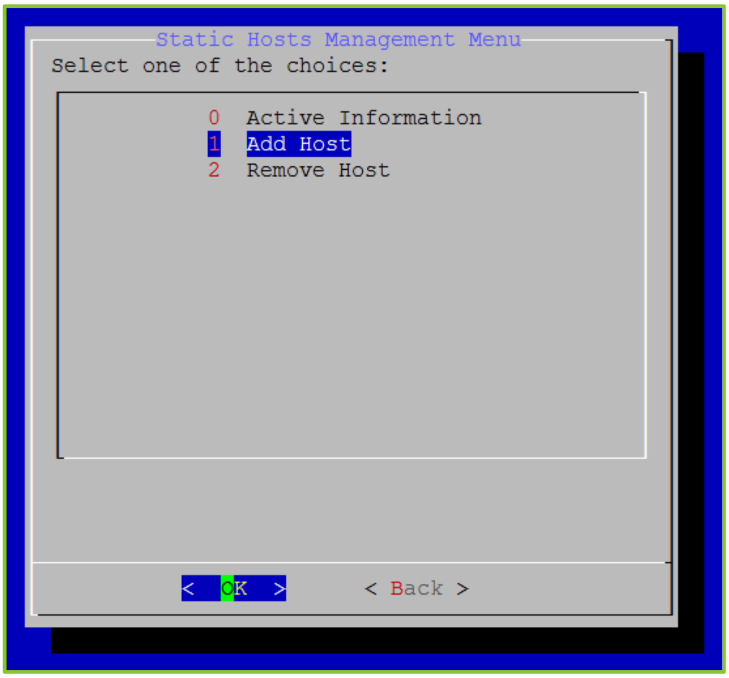
3. Press the Enter key to select OK.

   The Main Menu for the Advanced configuration displays.



4. Enter **7** to select the Static Hosts option.
5. Press the Enter key to select OK.

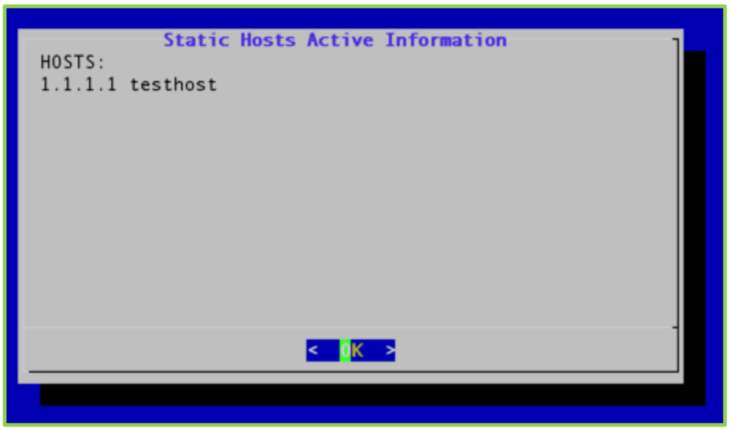
   The Static Hosts Management Menu displays.



```
Static Hosts Management Menu
Select one of the choices:

          0  Active Information
          1  Add Host
          2  Remove Host
```

6. Enter 0 to select the Active Information option.
7. Press the Enter key to select OK.

   The *Static Hosts Active Information* window displays.



```
Static Hosts Active Information
HOSTS:
1.1.1.1 testhost
```

8. Press the Enter key to select OK.

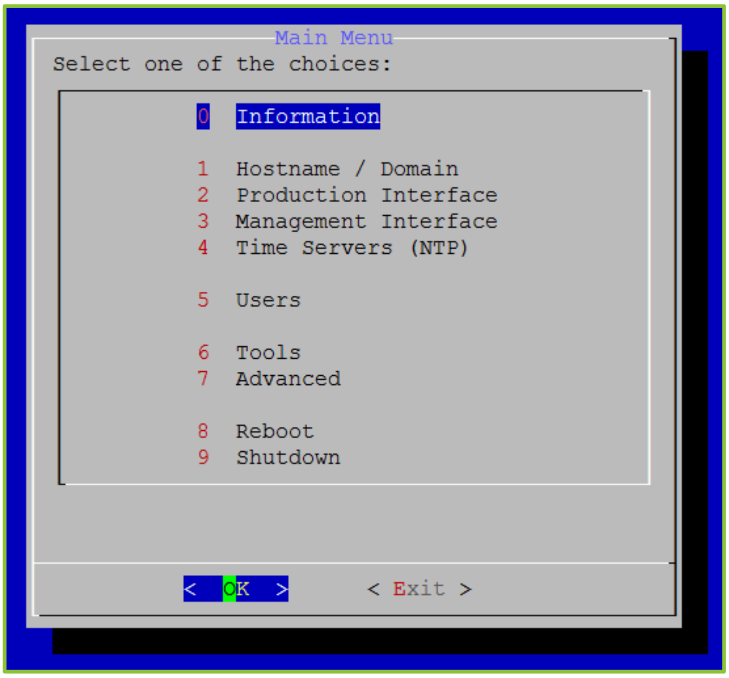
Adding Static Hosts

To view add static hosts:

1. Log in to the System Console.

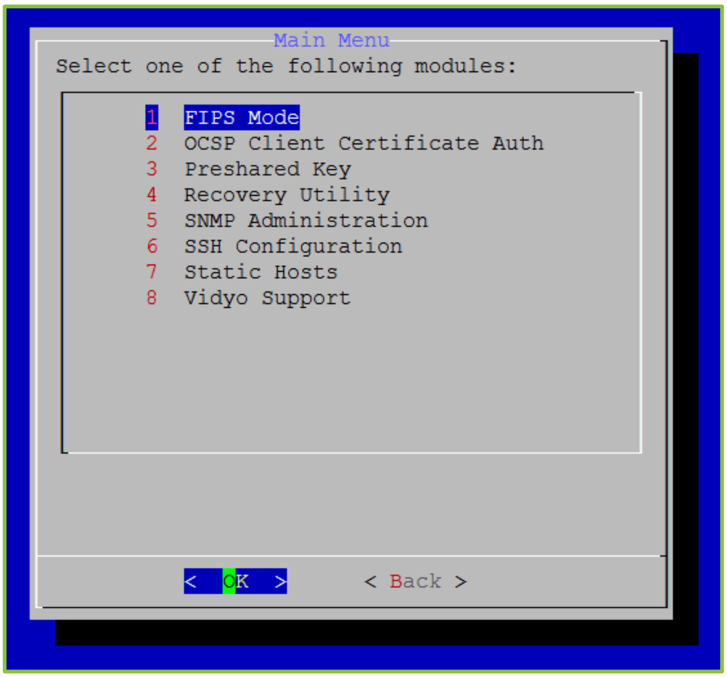
   For more information, see Logging in to the System Console and Changing the Default Password.

   The Main Menu displays.



2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

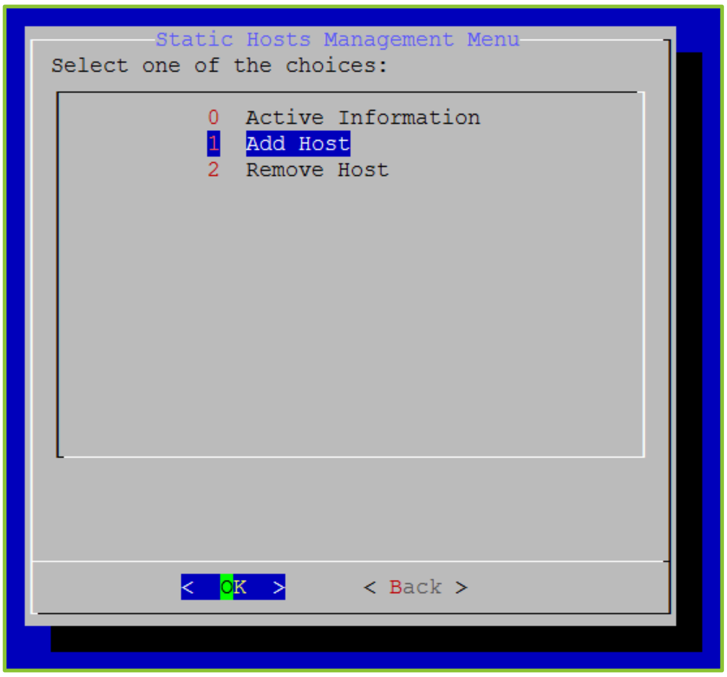
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

          <  OK  >      < Back >
```

4. Enter **7** to select the Static Hosts option.
5. Press the Enter key to select OK.

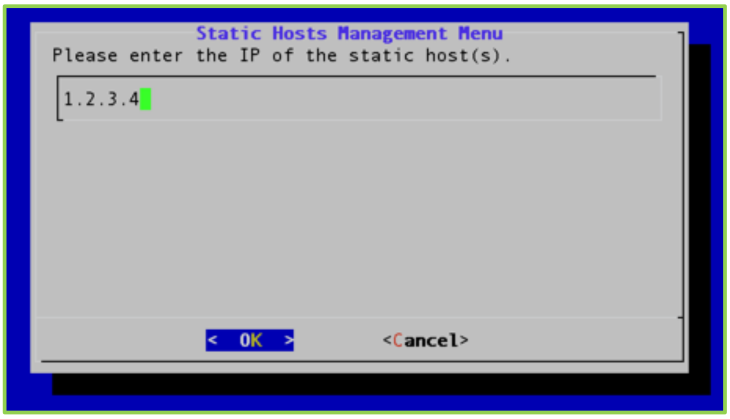
The Static Hosts Management Menu displays.



```
Static Hosts Management Menu
Select one of the choices:

             0   Active Information
             1   Add Host
             2   Remove Host

          <  OK  >      < Back >
```

6. Enter **1** to select the Add Host option.
7. Press the Enter key to select OK.

   The *Static Hosts Management Menu* window displays.



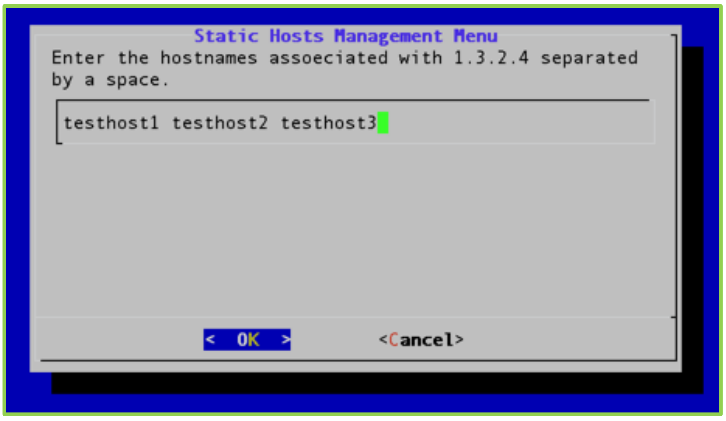
Static Hosts Management Menu

Please enter the IP of the static host(s).

```
1.2.3.4
```

8. Enter the IP address of the static host you want to add.
9. Press the Enter key to select OK.

   The next *Static Hosts Management Menu* window displays.



Static Hosts Management Menu

Enter the hostnames assoeciated with 1.3.2.4 separated by a space.

```
testhost1 testhost2 testhost3
```

10. Enter the hostname(s) you want to associate with the IP address you just entered.
11. Press the Enter key to select Yes.

    The *Message* window displays indicating that the IP address has been added.
12. Press the Enter key to select OK.

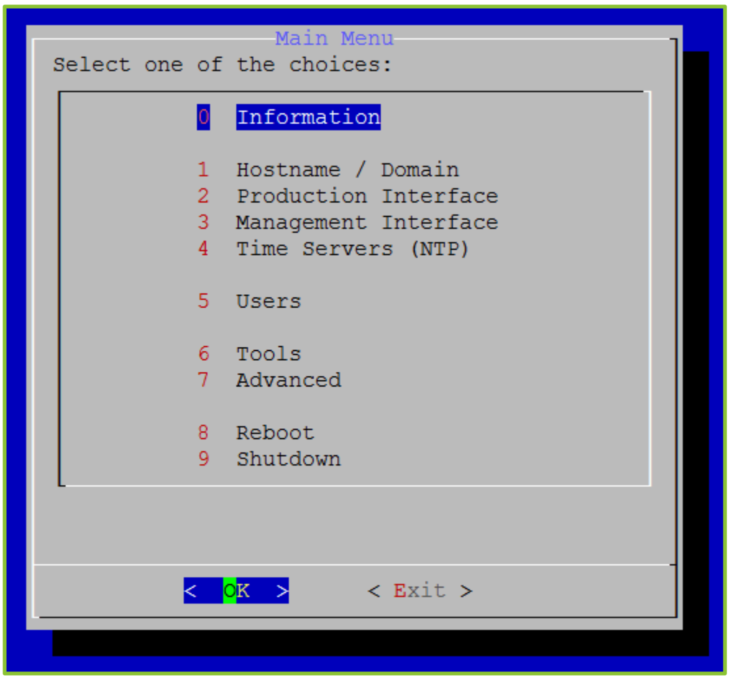
Removing Static Hosts

To view remove static hosts:

1. Log in to the System Console.

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

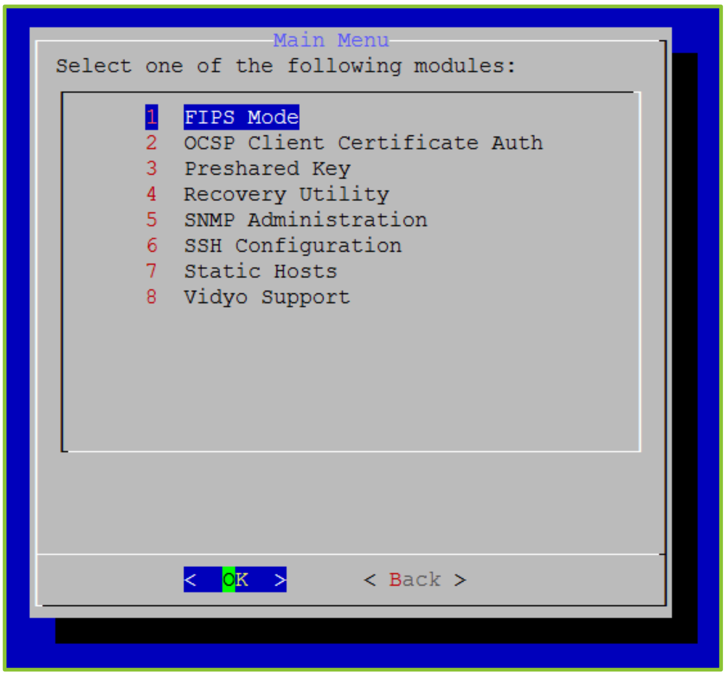
The Main Menu displays.



```
                     Main Menu
Select one of the choices:

          0  Information

          1  Hostname / Domain
          2  Production Interface
          3  Management Interface
          4  Time Servers (NTP)

          5  Users

          6  Tools
          7  Advanced

          8  Reboot
          9  Shutdown

          <  OK  >        < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

The Main Menu for the Advanced configuration displays.

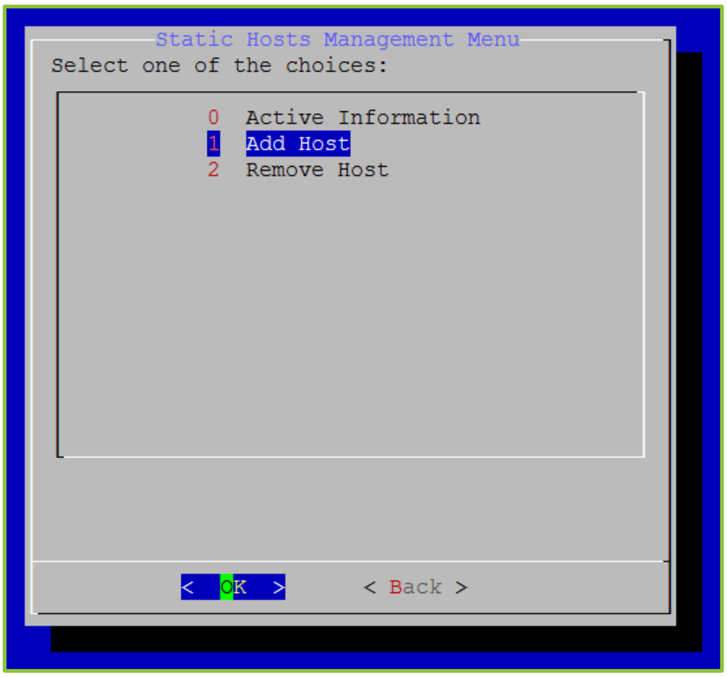


```
Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

          <  OK  >          < Back >
```

4. Enter **7** to select the Static Hosts option.

5. Press the **Enter** key to select **OK**.

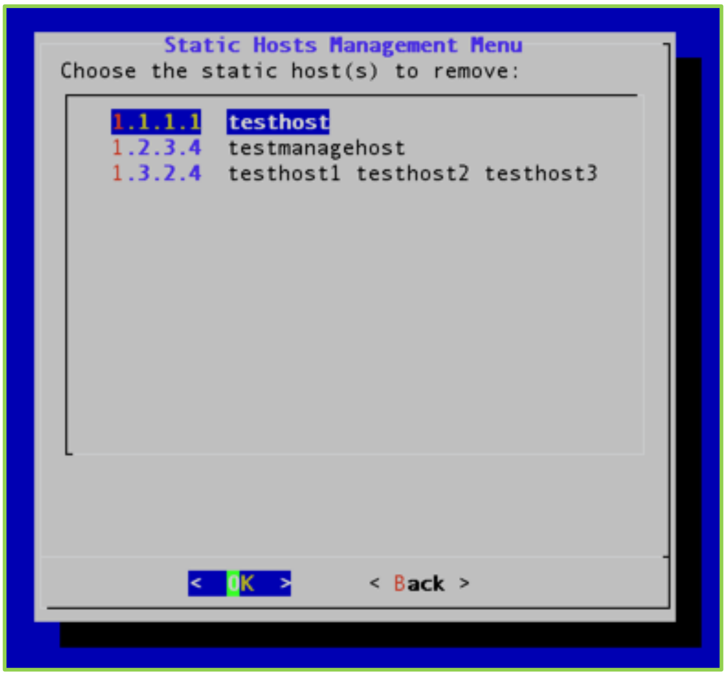
   The Static Hosts Management Menu displays.



```
Static Hosts Management Menu
Select one of the choices:

             0   Active Information
             1   Add Host
             2   Remove Host

          <  OK  >          < Back >
```

6. Enter **2** to select the Remove Host option.
7. Press the Enter key to select OK.

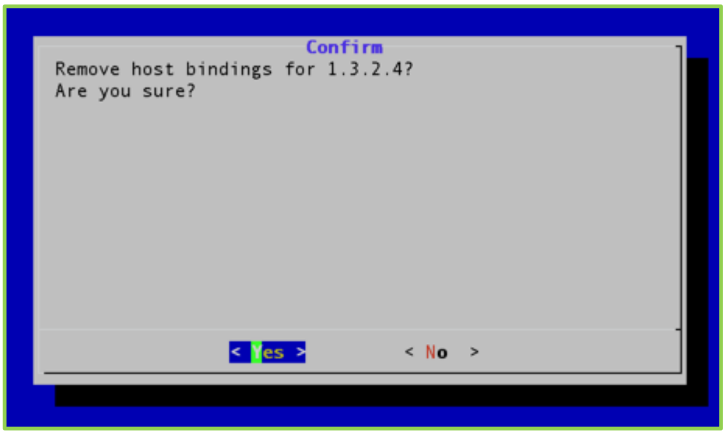
   The *Static Hosts Management Menu* window displays.



```
Static Hosts Management Menu
Choose the static host(s) to remove:

  1.1.1.1  testhost
  1.2.3.4  testmanagehost
  1.3.2.4  testhost1 testhost2 testhost3
```

8. Select the IP address of the static host you want to remove.
9. Press the Enter key to select OK.

   The *Confirm* window displays.



```
Confirm
Remove host bindings for 1.3.2.4?
Are you sure?
```

10. Press the Enter key to select Yes.

    The *Message* window displays indicating that the IP address has been removed.
11. Press the Enter key to select OK.

Configuring Remote Vidyo Support Access

This section describes how to generate a one-time encrypted password that enables the Vidyo Customer Support team to remotely access your VidyoGateway system in a secure manner. The encrypted password that is generated expires at midnight UTC the day after it is generated.

You can also disable remote Vidyo Support access as described in this section.

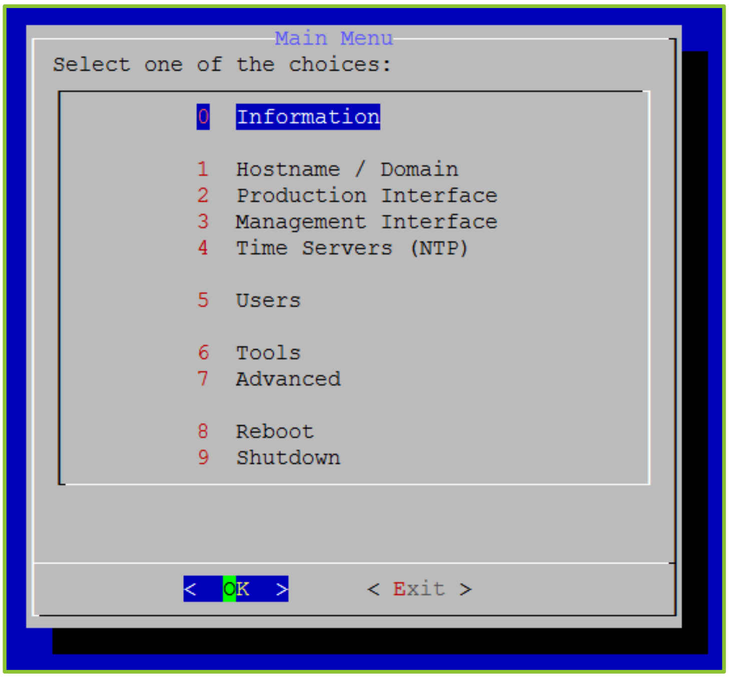
Enabling Remote Vidyo Support Access

To enable remote Vidyo Support access:

1. Log in to the System Console.

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

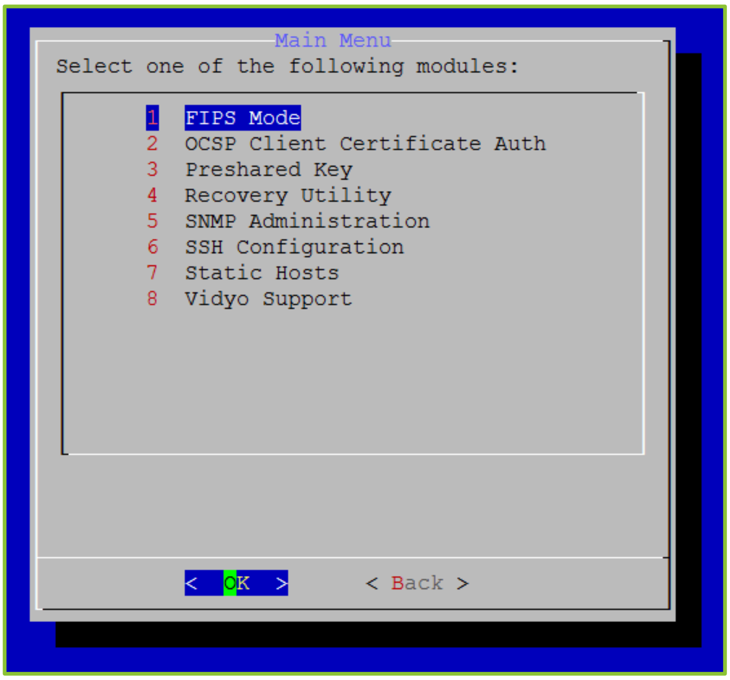
   The Main Menu displays.



```
Main Menu
Select one of the choices:

          0  Information

          1  Hostname / Domain
          2  Production Interface
          3  Management Interface
          4  Time Servers (NTP)

          5  Users

          6  Tools
          7  Advanced

          8  Reboot
          9  Shutdown

        <  OK  >        < Exit >
```

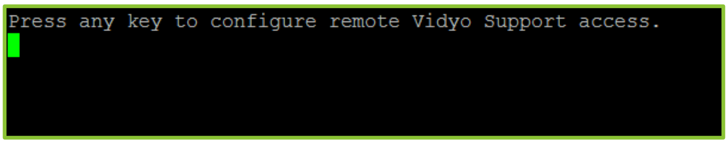
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**.

The Main Menu for the Advanced configuration displays.



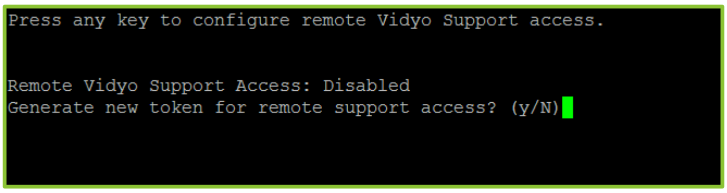
4. Enter **8** to select the Vidyo Support option.
5. Press the Enter key to select OK.

   The following message displays:



```
Press any key to configure remote Vidyo Support access.
```

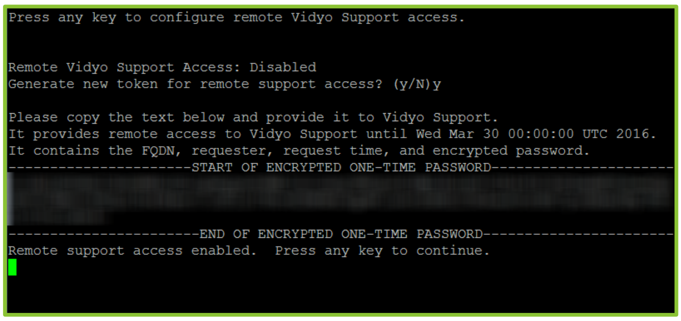
6. Press any key on your keyboard.
7. Enter **y** to generate a new token for remote support access.



```
Press any key to configure remote Vidyo Support access.


Remote Vidyo Support Access: Disabled
Generate new token for remote support access? (y/N)
```

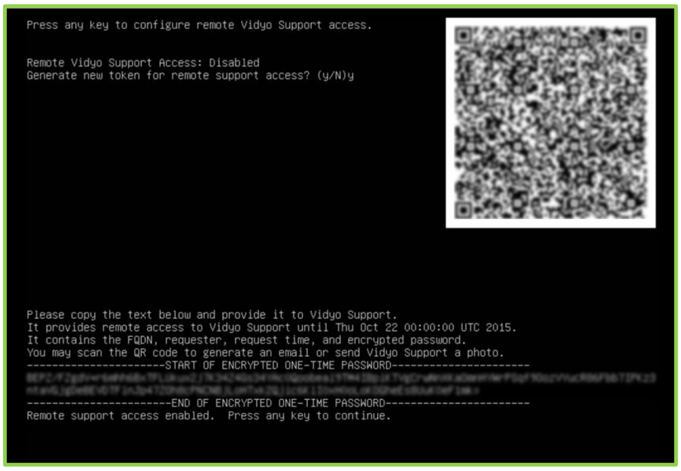
8. Press the Enter key.

- If you are accessing the System Console via SSH, a one-time encrypted password is generated as shown:



```
Press any key to configure remote Vidyo Support access.


Remote Vidyo Support Access: Disabled
Generate new token for remote support access? (y/N)y

Please copy the text below and provide it to Vidyo Support.
It provides remote access to Vidyo Support until Wed Mar 30 00:00:00 UTC 2016.
It contains the FQDN, requester, request time, and encrypted password.
----------------------START OF ENCRYPTED ONE-TIME PASSWORD----------------------
[redacted]
-----------------------END OF ENCRYPTED ONE-TIME PASSWORD-----------------------
Remote support access enabled.  Press any key to continue.
```

- If you are directly accessing the System Console, a one-time encrypted password is generated as shown:



```
Press any key to configure remote Vidyo Support access.


Remote Vidyo Support Access: Disabled
Generate new token for remote support access? (y/N)y









Please copy the text below and provide it to Vidyo Support.
It provides remote access to Vidyo Support until Thu Oct 22 00:00:00 UTC 2015.
It contains the FQDN, requester, request time, and encrypted password.
You may scan the QR code to generate an email or send Vidyo Support a photo.
----------------------START OF ENCRYPTED ONE-TIME PASSWORD----------------------
[redacted]
-----------------------END OF ENCRYPTED ONE-TIME PASSWORD-----------------------
Remote support access enabled.  Press any key to continue.
```

9. Do one of the following:
   - If you are accessing the System Console via SSH, copy the one-time encrypted password shown on the screen and provide it to Vidyo Support.
   - If you are directly accessing the System Console, scan the QR code and send it to Vidyo Support.

Note The password that is generated expires at midnight UTC the day after it is generated.

10. Press any key to return to the Advanced Main Menu.

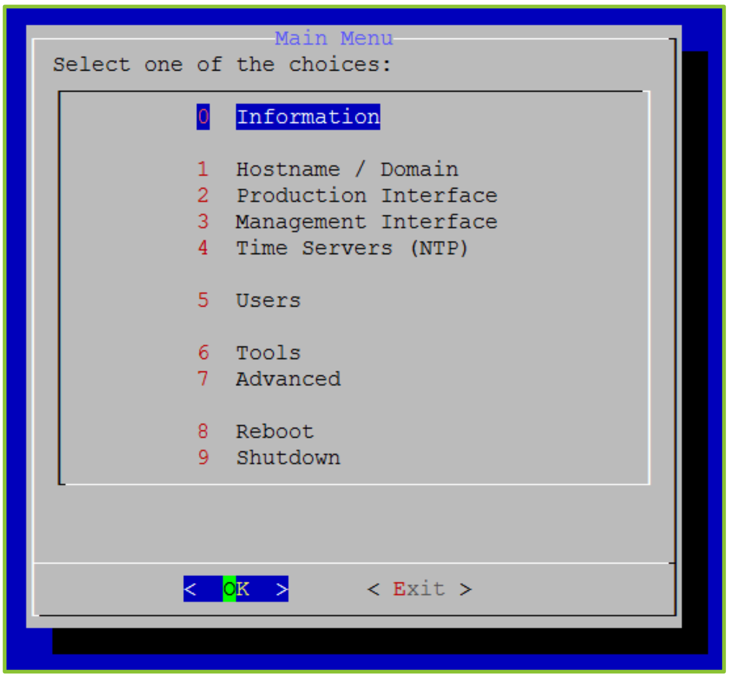
Disabling Remote Vidyo Support Access

To disable remote Vidyo Support access:

1. Log in to the System Console.

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

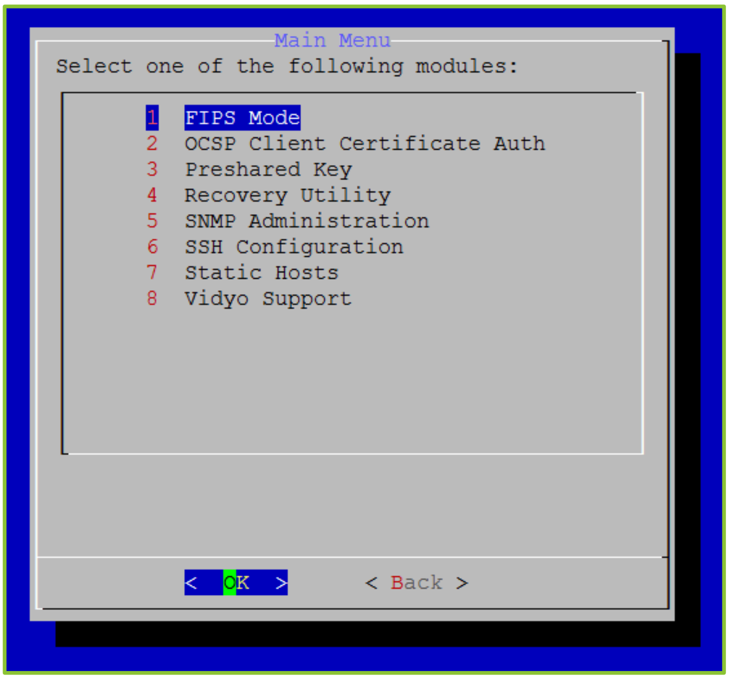
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

      <  OK  >        < Exit >
```

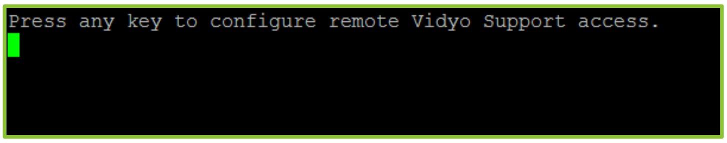
2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

The Main Menu for the Advanced configuration displays.



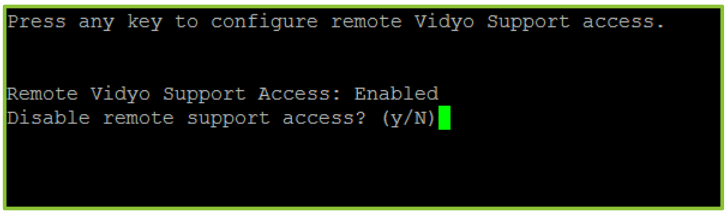
4. Enter **8** to select the Vidyo Support option.
5. Press the Enter key to select OK.

   The following message displays:



```
Press any key to configure remote Vidyo Support access.
```

6. Press any key on your keyboard.
7. Enter **y** to disable remote support access.



```
Press any key to configure remote Vidyo Support access.


Remote Vidyo Support Access: Enabled
Disable remote support access? (y/N)
```

8. Press the Enter key.

   A message indicates that remote access is disabled.
9. Press any key to return to the Advanced Main Menu.

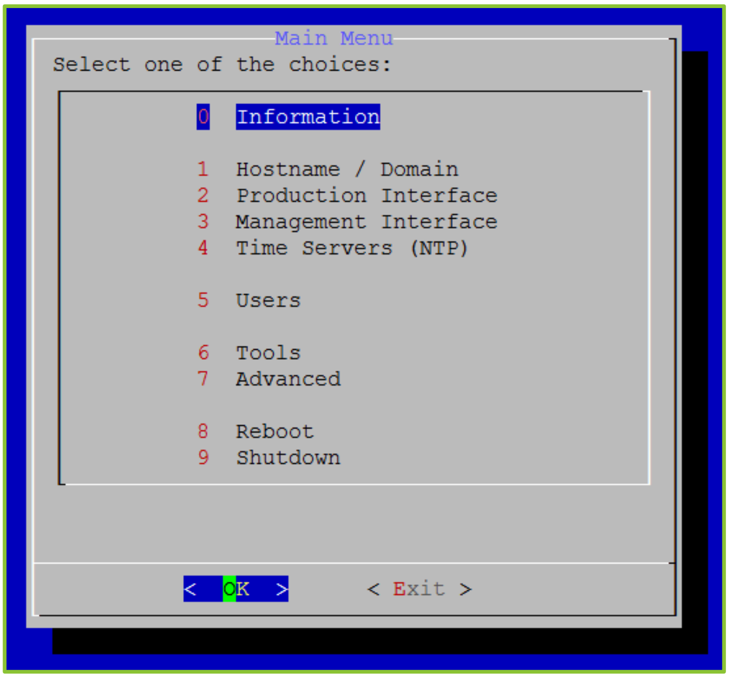
Rebooting the System Console

To shut down the System Console:

1. Log in to the System Console.

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

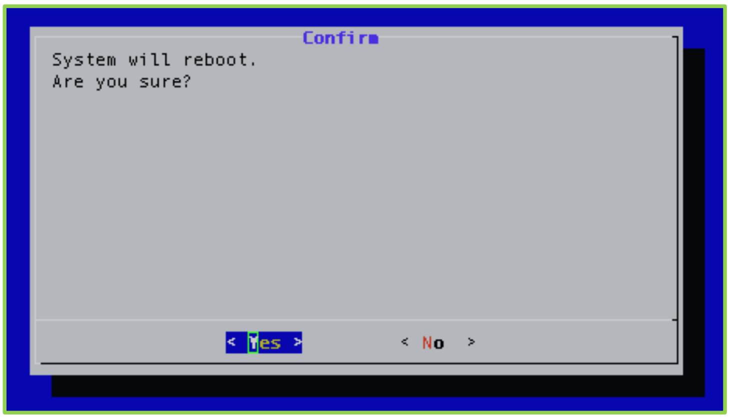
   The Main Menu displays.



Select one of the choices:

2. Enter **8** to select the Reboot option.
3. Press the Enter key to select OK.

   The *Confirm* window displays.



```
System will reboot.
Are you sure?
```

4. Press the **Enter** key to select **Yes**.

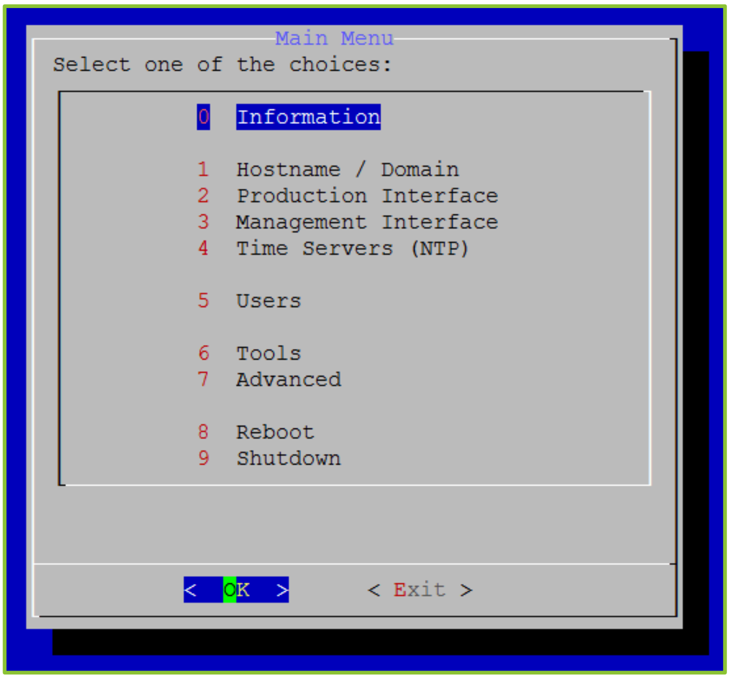
Shutting Down the System Console

To shut down the System Console:

1. Log in to the System Console.

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

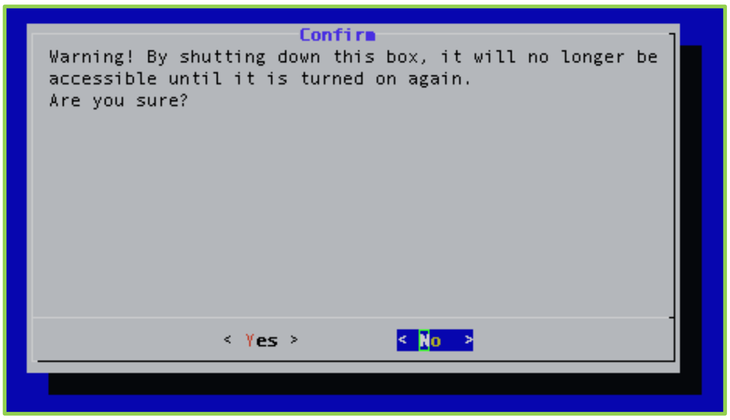
   The Main Menu displays.



```
                  Main Menu
 Select one of the choices:

          0   Information

          1   Hostname / Domain
          2   Production Interface
          3   Management Interface
          4   Time Servers (NTP)

          5   Users

          6   Tools
          7   Advanced

          8   Reboot
          9   Shutdown

         <  OK  >        < Exit >
```

2. Enter **9** to select the Shutdown option.
3. Press the **Enter** key to select **OK**.

The *Confirm* window displays.



```
Confirm
Warning! By shutting down this box, it will no longer be
accessible until it is turned on again.
Are you sure?

              < Yes >          < No  >
```

4. Press the **Enter** key to select **Yes**.

Logging in to the Admin Portal

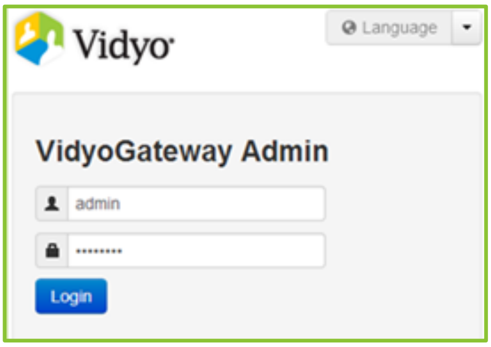
Now that you have connected your VidyoGateway server to the network, you must log in to its Admin portal using the System Console account and configure your VidyoGateway so it can function within your VidyoConferencing system.

To log in to the Admin Portal:

1. Enter the URL or IP address for the VidyoGateway in the address bar of a web browser:

   The URL of your VidyoGateway is typically a domain name: `[examplegateway.com]`

2. Log in to the Admin portal using your System Console account.



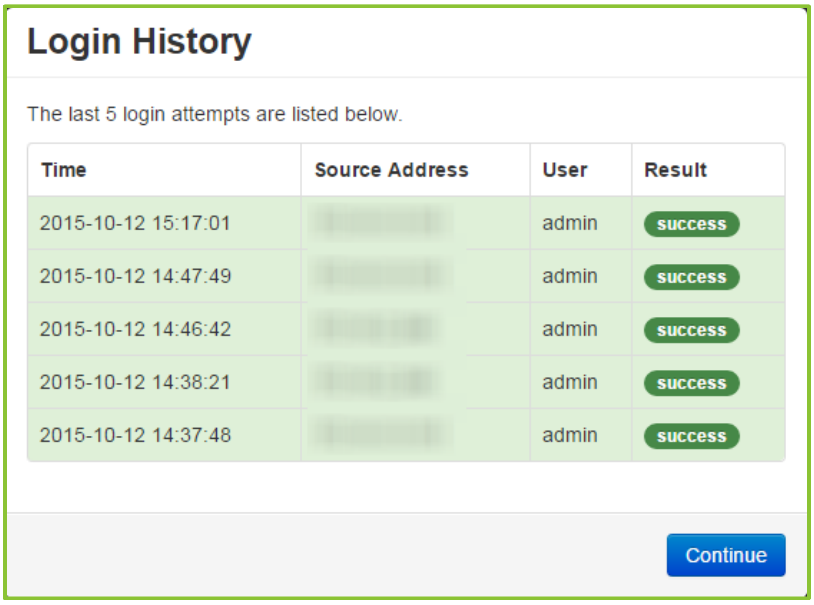
VidyoGateway Admin

admin

••••••••

Note If you do not enter information on this page, you will be logged out from inactivity.

Prior to logging in, the *Login History* pop-up shows the last five login attempts made to the Admin portal.

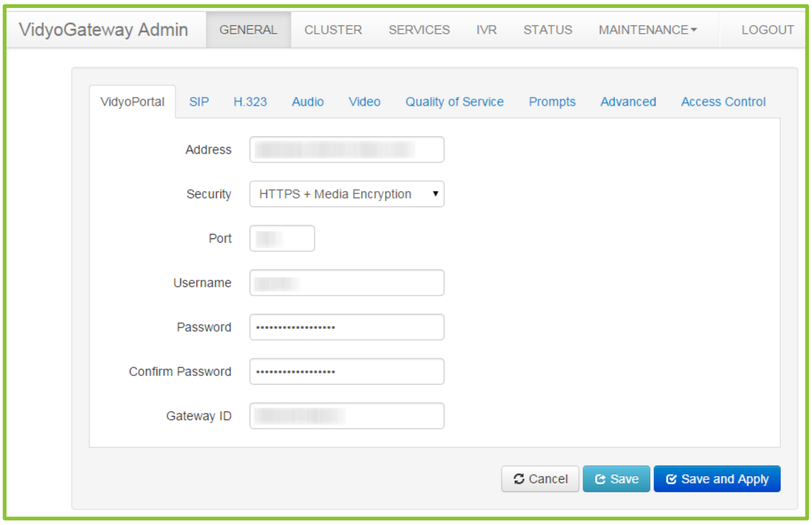


Login History

The last 5 login attempts are listed below.

Time	Source Address	User	Result
2015-10-12 15:17:01	[redacted]	admin	success
2015-10-12 14:47:49	[redacted]	admin	success
2015-10-12 14:46:42	[redacted]	admin	success
2015-10-12 14:38:21	[redacted]	admin	success
2015-10-12 14:37:48	[redacted]	admin	success

3. Click **Continue**.



Address: [redacted]

Security: HTTPS + Media Encryption

Port: [redacted]

Username: [redacted]

Password: ••••••••••••••••••

Confirm Password: ••••••••••••••••••

Gateway ID: [redacted]

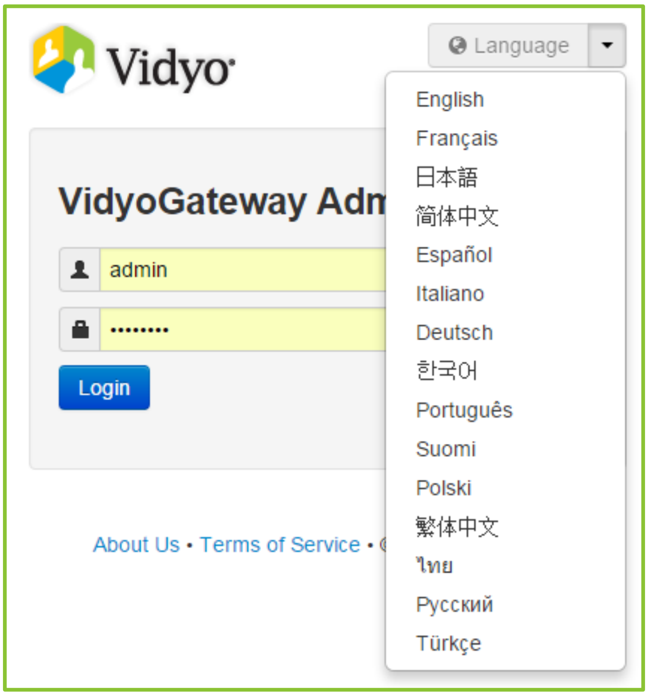
Setting the Language for the VidyoGateway Admin Pages

The VidyoGateway's Admin Pages are available in these 15 languages:

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

To set your preferred language:

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



4. 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.

Viewing the Current RADIUS Configuration

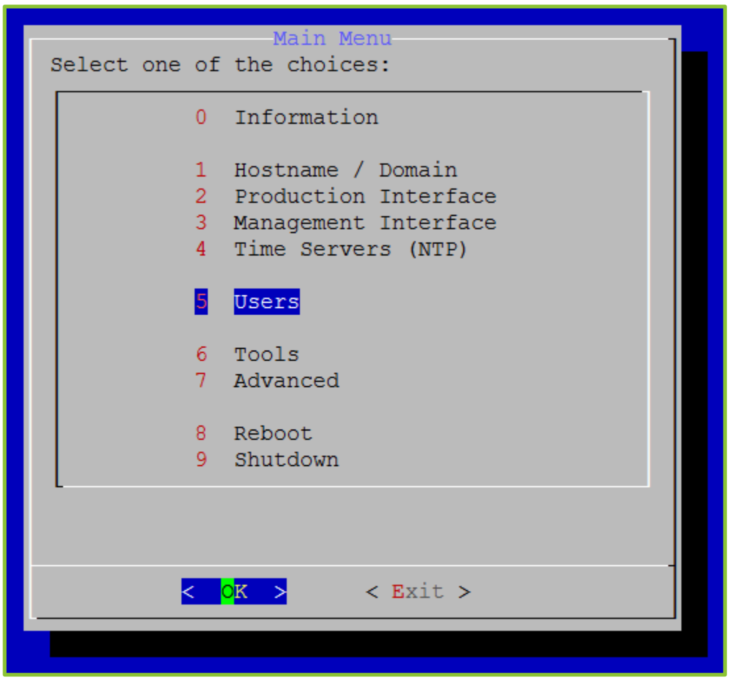
You should always review your RADIUS server configurations for accuracy.

To view the current RADIUS configuration:

1. Log in to the System Console.

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

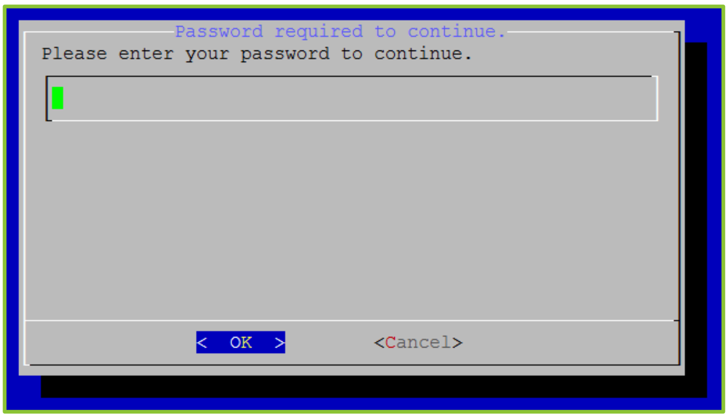
   The Main Menu displays.



```
                    Main Menu
 Select one of the choices:

           0  Information

           1  Hostname / Domain
           2  Production Interface
           3  Management Interface
           4  Time Servers (NTP)

           5  Users

           6  Tools
           7  Advanced

           8  Reboot
           9  Shutdown

        <  OK  >        < Exit >
```

2. Enter **5** to select the Users option.
3. Press the **Enter** key to select OK.

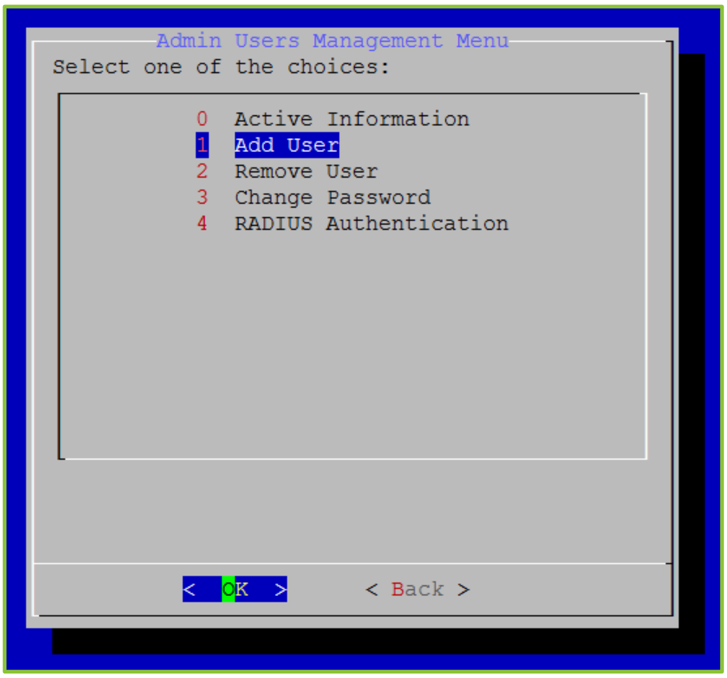
The *Password required to continue* window displays.



```
Password required to continue.
Please enter your password to continue.
```

4. Enter your password.
5. Press the **Enter** key to select **OK**.

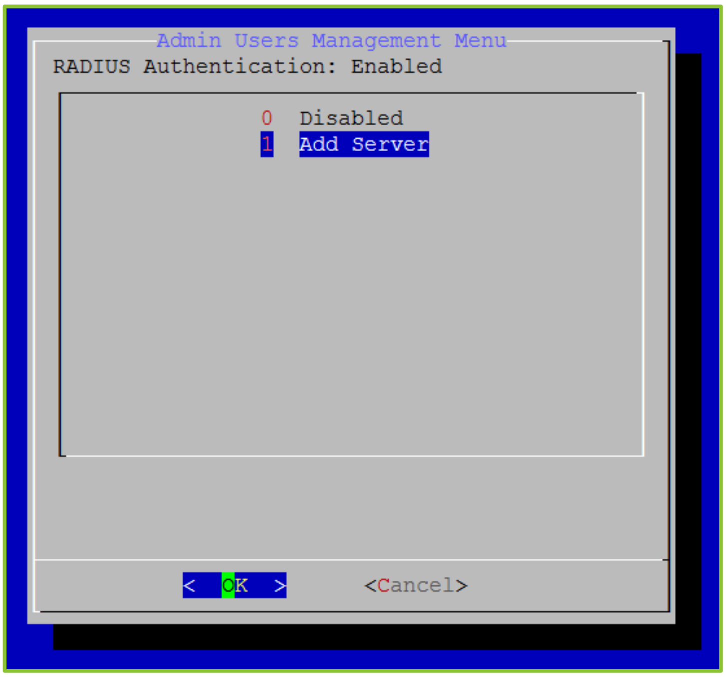
The Admin Users Management Menu displays.



```
Admin Users Management Menu
Select one of the choices:
```

6. Enter **4** to select the RADIUS Authentication option.

The current RADIUS authentication status displays.



```
Admin Users Management Menu
RADIUS Authentication: Enabled

        0  Disabled
        1  Add Server

   < OK >        <Cancel>
```

Enter **1** to select the Add Server option and proceed to step 6 in the Configuring RADIU section.

Configuring RADIUS

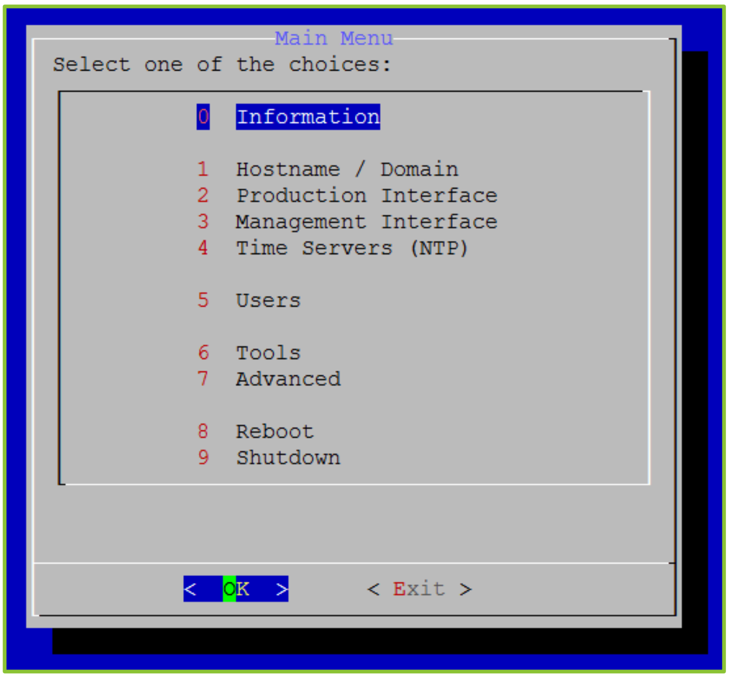
FIPS mode is disabled by default.

To configure RADIUS:

1. Log in to the System Console.

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

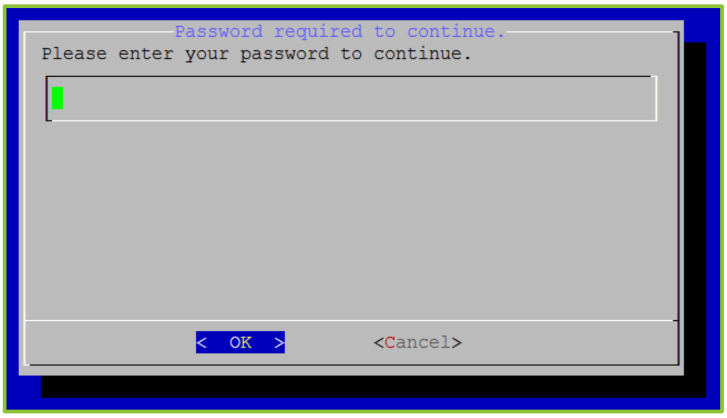
The Main Menu displays.



```
Main Menu
Select one of the choices:

            0  Information

            1  Hostname / Domain
            2  Production Interface
            3  Management Interface
            4  Time Servers (NTP)

            5  Users

            6  Tools
            7  Advanced

            8  Reboot
            9  Shutdown

        <  OK  >        < Exit >
```

2. Enter **5** to select the Users option.

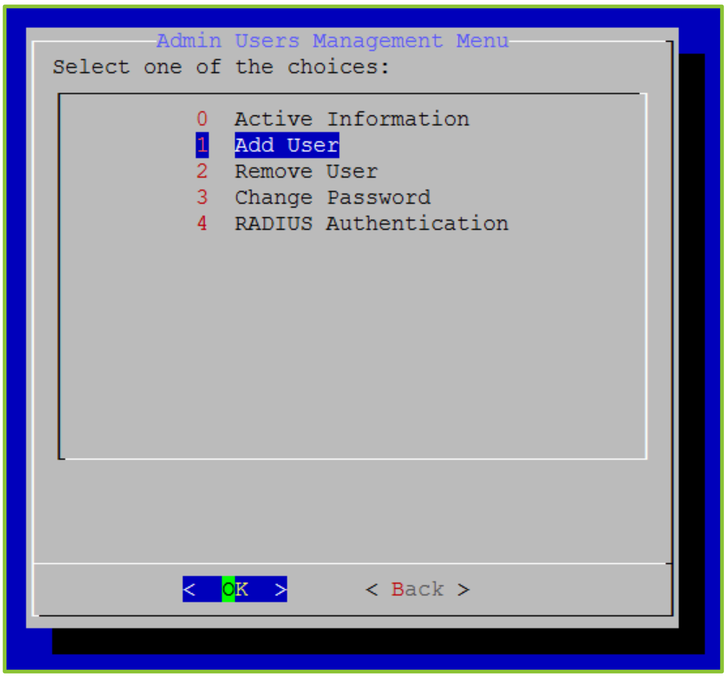
   The *Password required to continue* window displays.



```
Password required to continue.
Please enter your password to continue.

        <  OK  >        <Cancel>
```

3. Enter your password.
4. Press the Enter key to select OK.

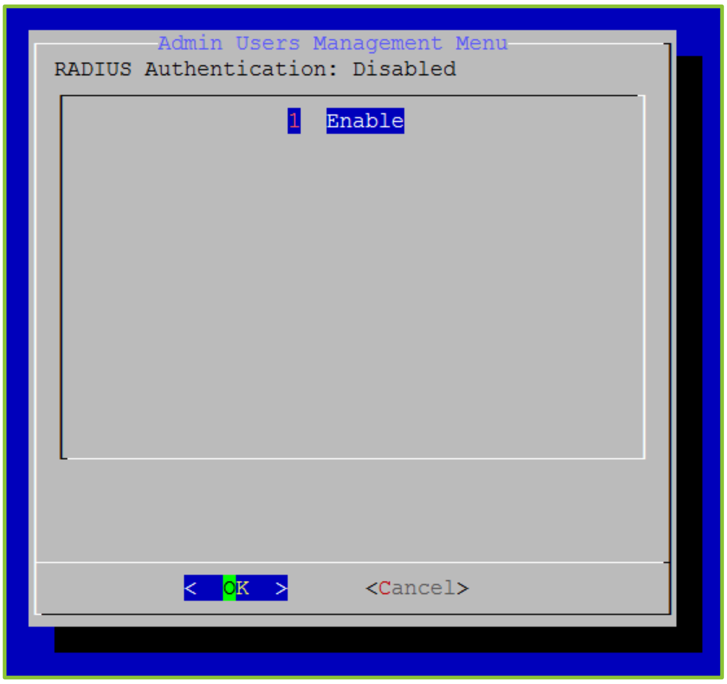
The Admin Users Management Menu displays.



```
Admin Users Management Menu
Select one of the choices:

        0  Active Information
        1  Add User
        2  Remove User
        3  Change Password
        4  RADIUS Authentication

      <  OK  >        < Back >
```

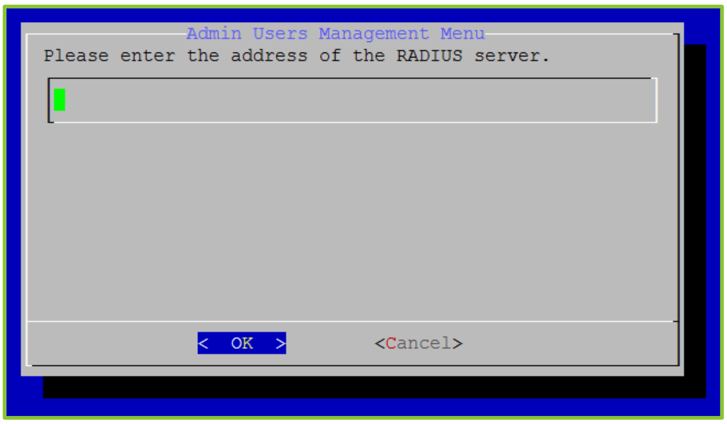
5. Enter **4** to select the RADIUS Authentication option.
6. Press the **Enter** key to select **OK**.

The Admin Users Management Menu displays.



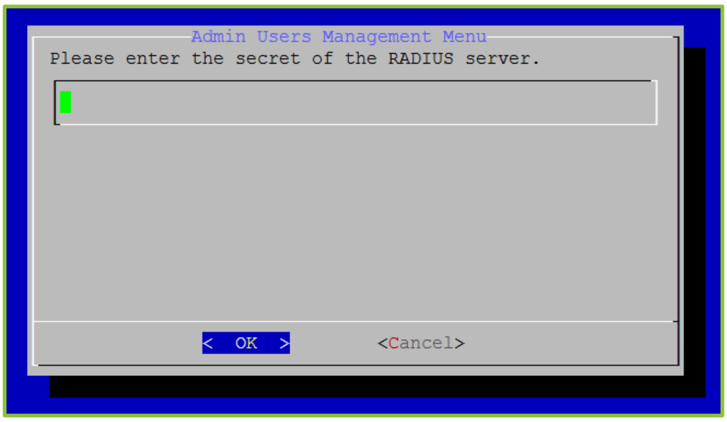
```
Admin Users Management Menu
RADIUS Authentication: Disabled

              1  Enable

      <  OK  >        <Cancel>
```

7. Enter **1** to select the Enable option.
8. Press the **Enter** key to select **OK**.
9. Enter the IP or FQDN of the RADIUS server or leave blank to cancel.



Please enter the address of the RADIUS server.

10. Press the **Enter** key to select **OK**.
11. Enter the secret for the VidyoGateway that is being configured for RADIUS.



Please enter the secret of the RADIUS server.

A message displays stating “RADIUS successfully enabled.”

12. Press the **Enter** key to select **OK**.

The Admin Users Management Menu displays.

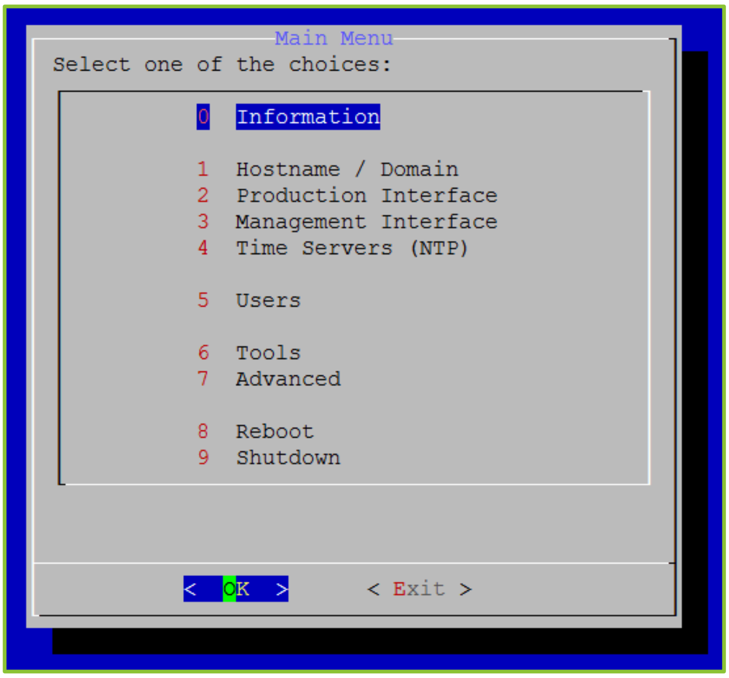
Adding Additional Servers

To additional servers:

1. Log in to the System Console.

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

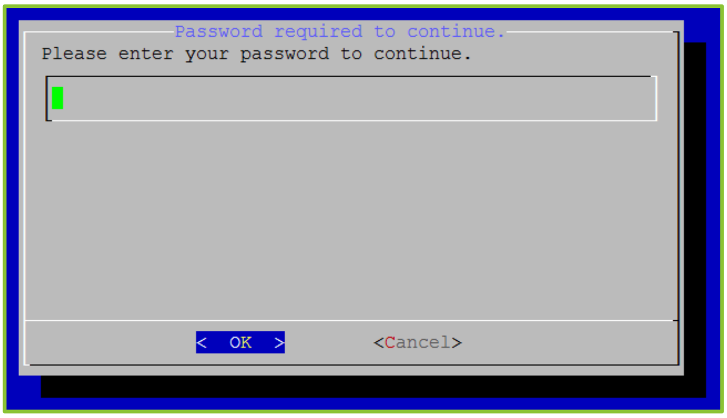
The Main Menu displays.



```
Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

     <  OK  >          < Exit >
```

2. Enter **5** to select the Users option.

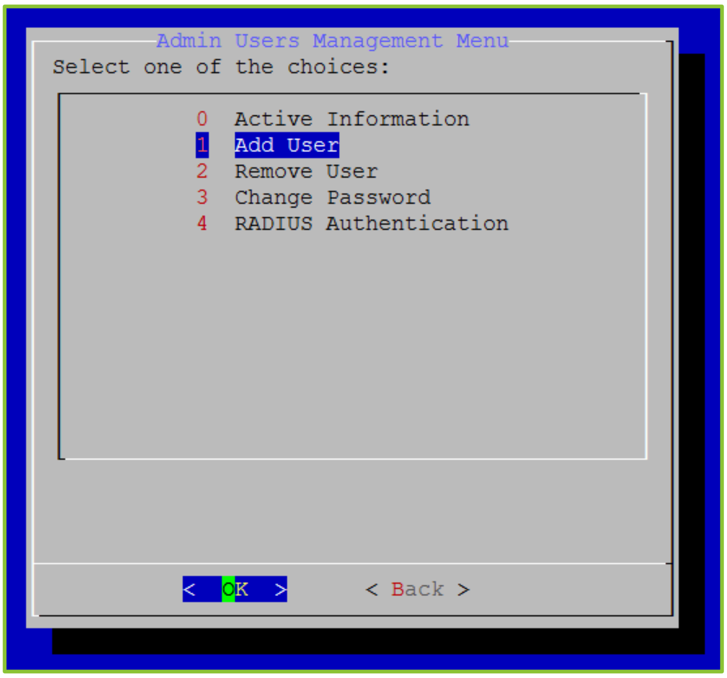
   The *Password required to continue* window displays.



```
Password required to continue.
Please enter your password to continue.



        <  OK  >          <Cancel>
```

3. Enter your password.
4. Press the Enter key to select OK.

The Admin Users Management Menu displays.

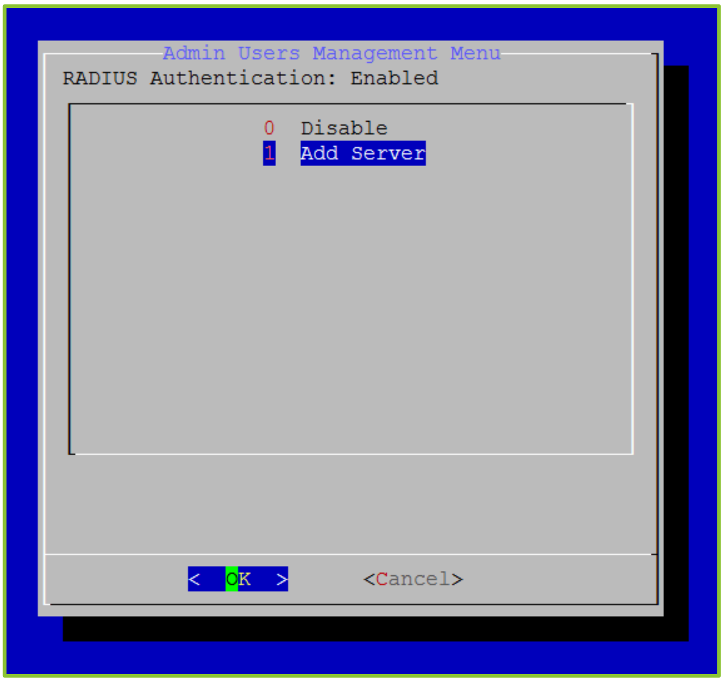


```
Admin Users Management Menu
Select one of the choices:

            0   Active Information
            1   Add User
            2   Remove User
            3   Change Password
            4   RADIUS Authentication

        <  OK  >          < Back >
```

5. Enter **4** to select the RADIUS Authentication option.

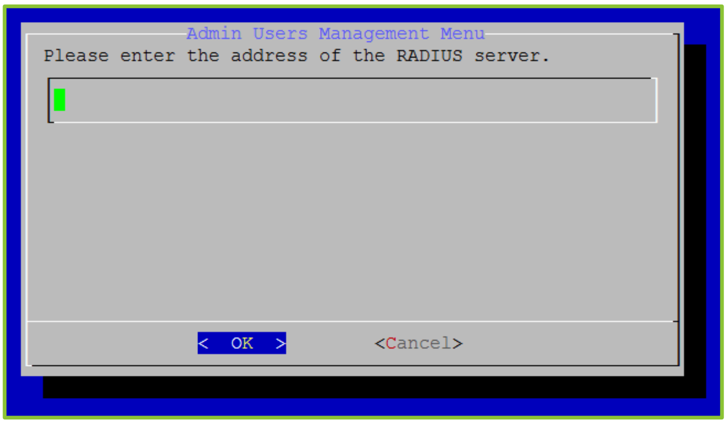
6. Press the **`Enter`** key to select OK.

The Admin Users Management Menu displays.



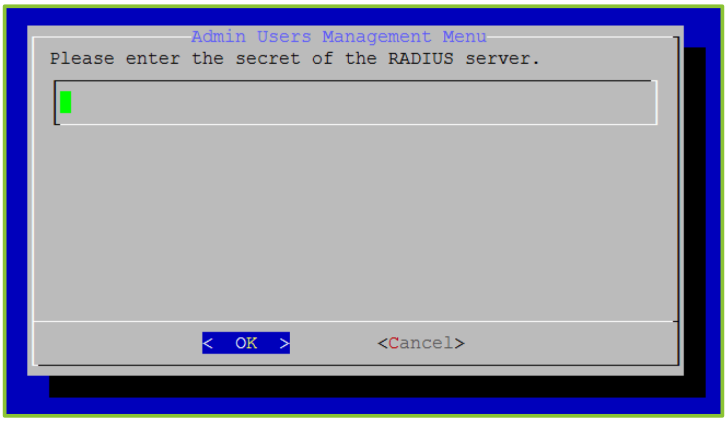
```
Admin Users Management Menu
RADIUS Authentication: Enabled

            0   Disable
            1   Add Server

        <  OK  >          <Cancel>
```

7. Enter **1** to select the Add Server option.
8. Press the **Enter** key to select OK.
9. Enter the IP or FQDN of the RADIUS server or leave blank to cancel.



```
Please enter the address of the RADIUS server.
```

10. Press the **Enter** key to select OK.
11. Enter the secret for the VidyoGateway that is being configured for RADIUS.



```
Please enter the secret of the RADIUS server.
```

A message displays stating “RADIUS successfully enabled.”

12. Press the Enter key to select OK.

The Admin Users Management Menu displays.

Creating a RADIUS-Enabled Account

To create a RADIUS-enabled account:

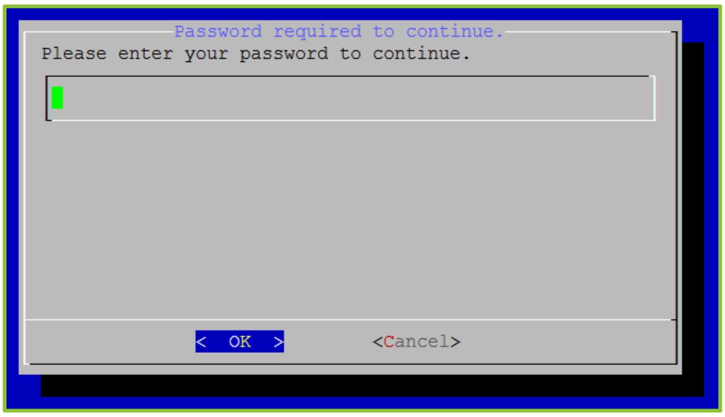
1. Log in to the System Console.

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

The Main Menu displays.

2. Enter **5** to select the Users option.
3. Press the **Enter** key to select OK.

The *Password required to continue* window displays.

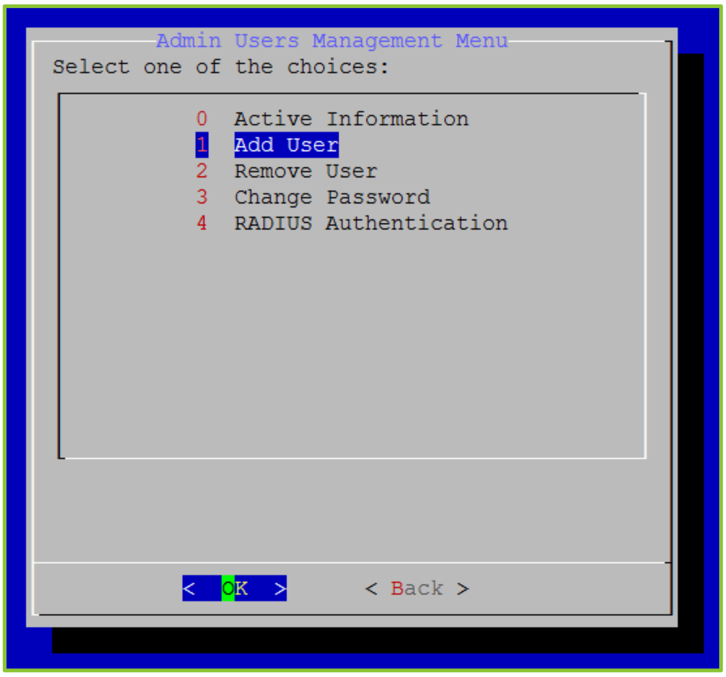


Password required to continue.

Please enter your password to continue.

4. Enter your password.
5. Press the Enter key to select OK.

The Admin Users Management Menu displays.

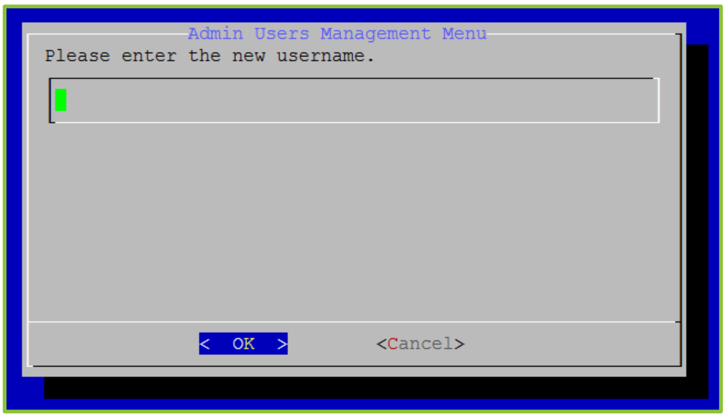


Admin Users Management Menu

Select one of the choices:

6. Enter **1** to select the Add User option.
7. Press the Enter key to select OK.

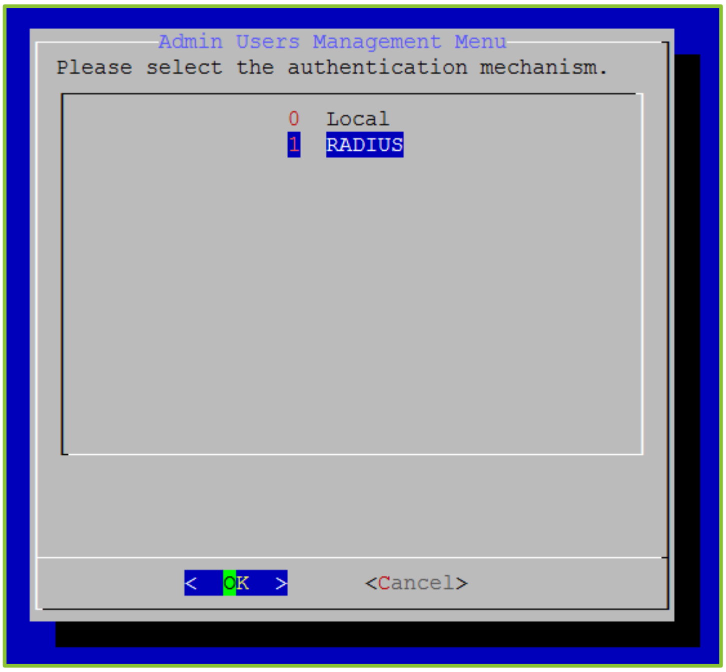
8. Enter a username for the user that is being added.



```
Admin Users Management Menu
Please enter the new username.
```

9. Press the **Enter** key to select **OK**.

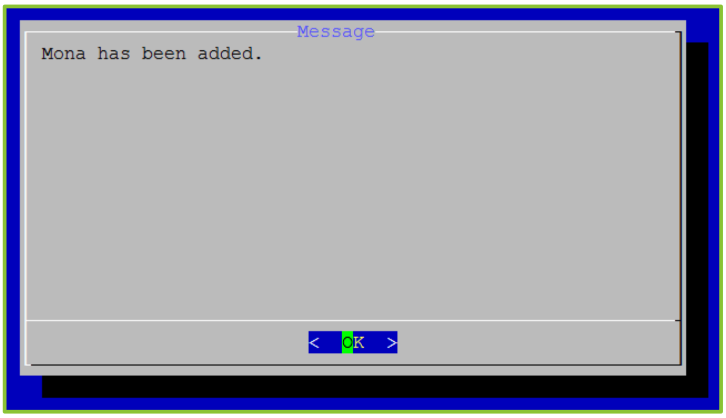
10. Enter **1** to select the RADIUS option.



```
Admin Users Management Menu
Please select the authentication mechanism.

0  Local
1  RADIUS
```

11. Press the **Enter** key to select **OK.**

A message displays stating that the user has been added.



Mona has been added.

12. Press the **Enter** key to select **OK**.

    The Admin Users Management Menu displays.

Viewing a RADIUS-Enabled Account

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

To view a RADIUS-enabled account, see Viewing Active User Information.

Removing a RADIUS-Enabled Account

To remove a RADIUS-enabled account, see Removing Users.

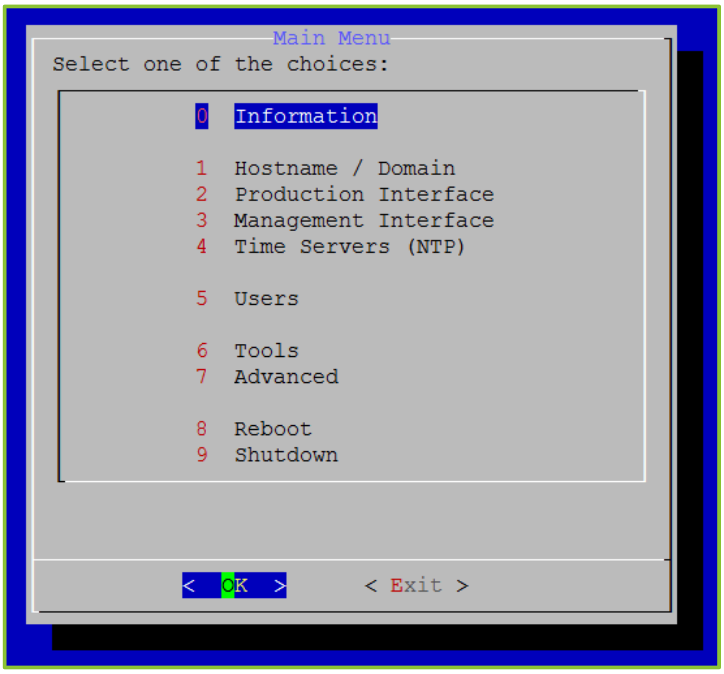
Disabling RADIUS Authentication

To disable RADIUS authentication:

1. Log in to the System Console.

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

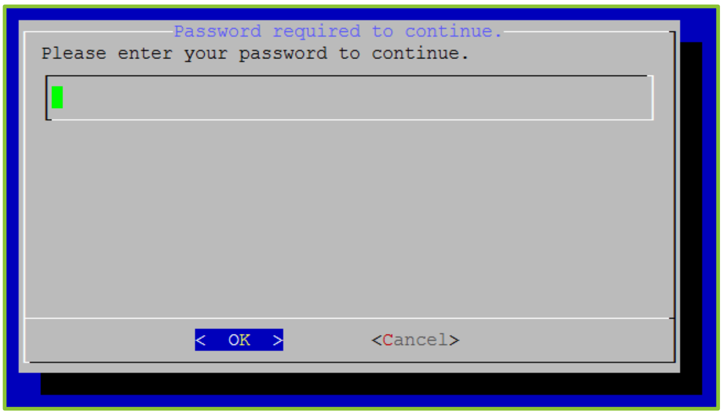
The Main Menu displays.



Select one of the choices:

2. Enter **5** to select the Users option.
3. Press the **Enter** key to select OK.

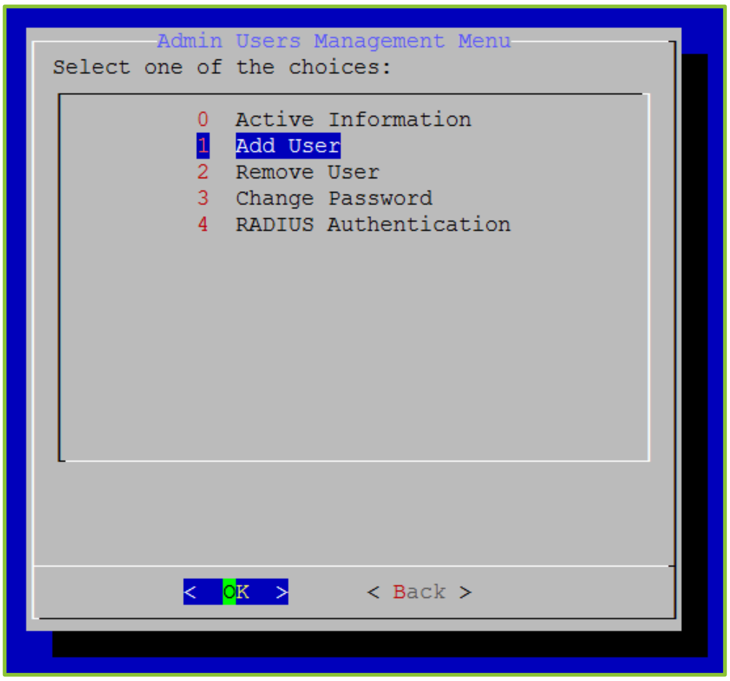
The *Password required to continue* window displays.



Please enter your password to continue.

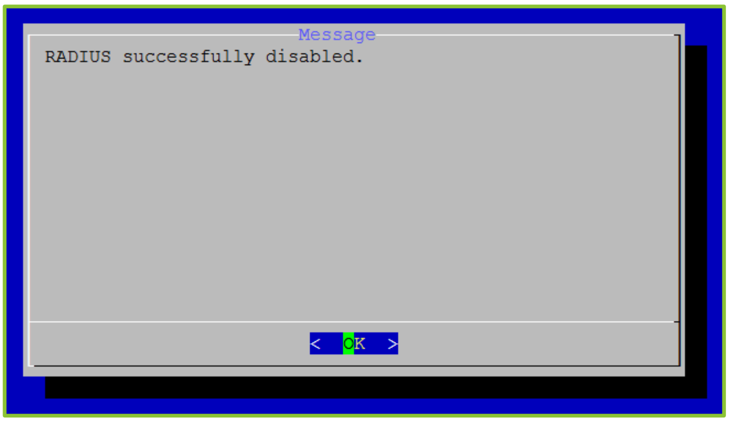
4. Enter your password.
5. Press the Enter key to select OK.

The Admin Users Management Menu displays.



6. Enter **4** to select the RADIUS Authentication option.
7. Enter **0** to select the Disabled option.
8. Press the **Enter** key to select **OK**.

   A message displays stating "RADIUS successfully disabled."



```
RADIUS successfully disabled.
```

9. Press the **Enter** key to select **OK**.

   The Admin Users Management Menu displays.

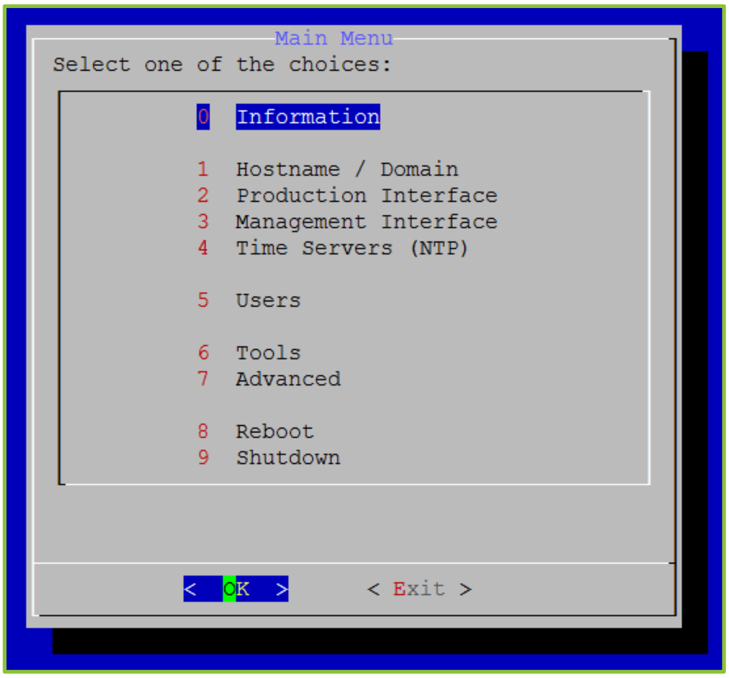
Enabling FIPS Mode

To enable FIPS mode:

1. Log in to the System Console.

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

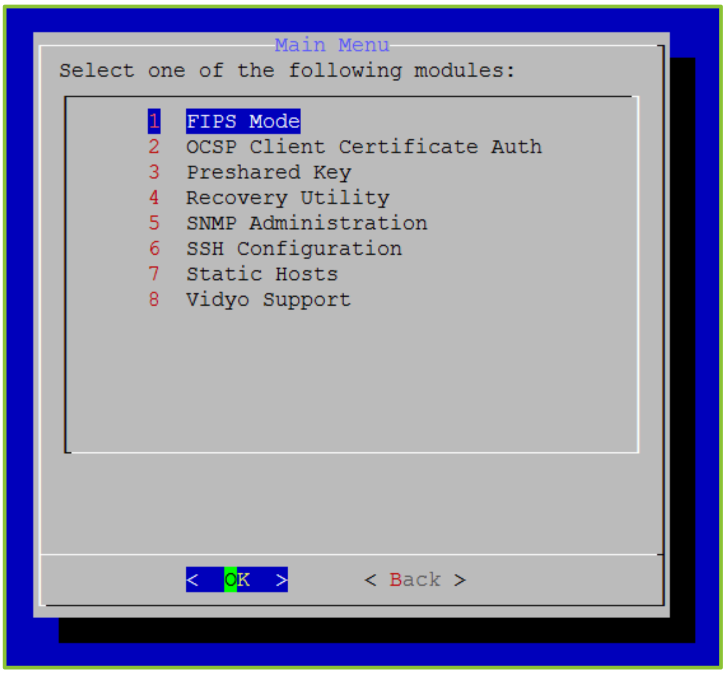
   The Main Menu displays.

```
                    Main Menu
 Select one of the choices:

              0  Information

              1  Hostname / Domain
              2  Production Interface
              3  Management Interface
              4  Time Servers (NTP)

              5  Users

              6  Tools
              7  Advanced

              8  Reboot
              9  Shutdown

            <  OK  >       < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.

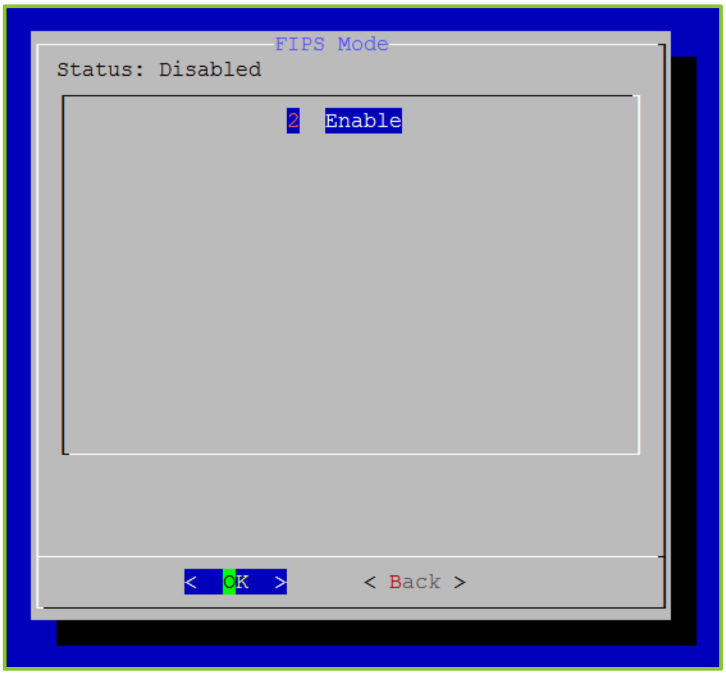
4. Enter **1** to select the FIPS Mode option.



```
                 Main Menu
Select one of the following modules:

      1  FIPS Mode
      2  OCSP Client Certificate Auth
      3  Preshared Key
      4  Recovery Utility
      5  SNMP Administration
      6  SSH Configuration
      7  Static Hosts
      8  Vidyo Support

         <  OK  >       < Back >
```

5. Press the Enter key to select OK.

   The Enable option is selected.

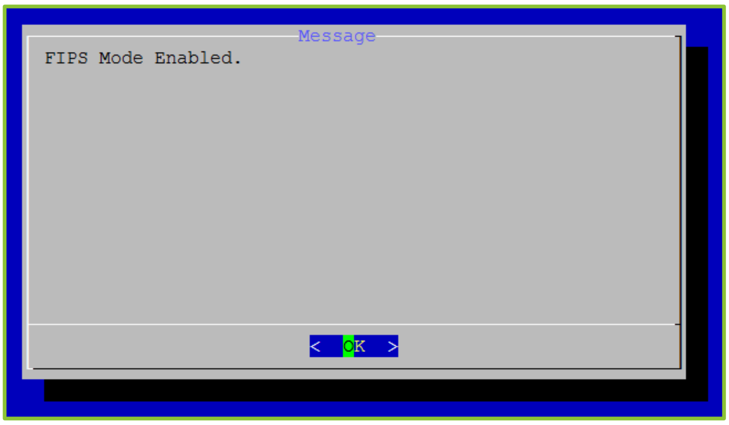


```
                 FIPS Mode
Status: Disabled

                 2  Enable

         <  OK  >       < Back >
```

Note This setting toggles between disable and enable states.

6. Press the **Enter** key to select **OK**.

   A message displays stating “FIPS Mode Enabled.”



```
FIPS Mode Enabled.
```

7. Press the **Enter** key to select **OK**.

Disabling FIPS Mode

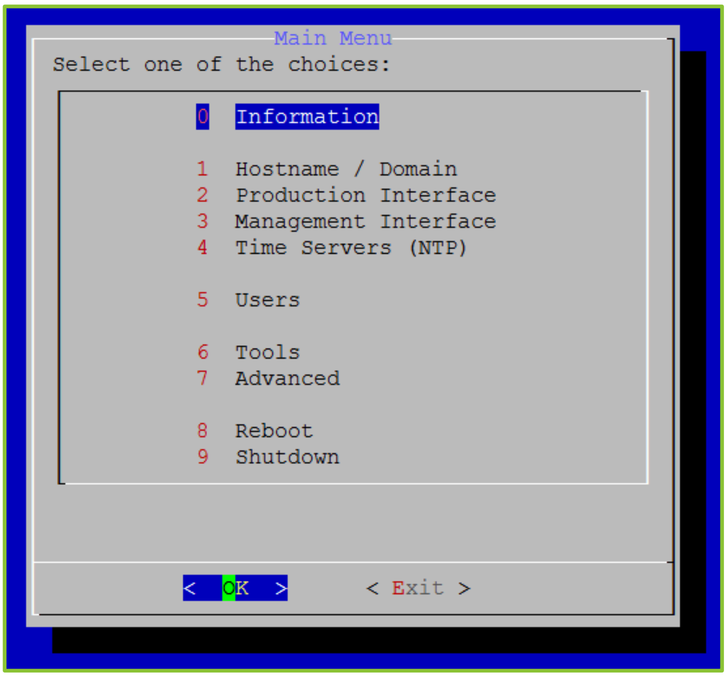
RADIUS configuration is allowed only when the Vidyo server has FIPS disabled. If FIPS is enabled, follow the procedures in this section to disable it. If FIPS is already disabled, then proceed to the Enabling section.

To disable FIPS mode:

1. Log in to the System Console.

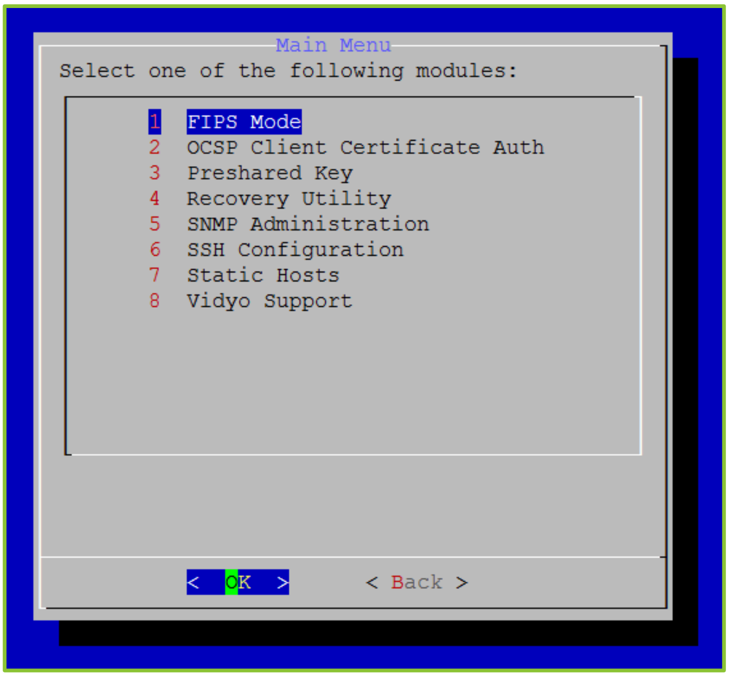
   For more information, see Logging in to the System Console and Changing the Default Password.

The Main Menu displays.



```
                Main Menu
Select one of the choices:

        0  Information

        1  Hostname / Domain
        2  Production Interface
        3  Management Interface
        4  Time Servers (NTP)

        5  Users

        6  Tools
        7  Advanced

        8  Reboot
        9  Shutdown

       <  OK  >        < Exit >
```

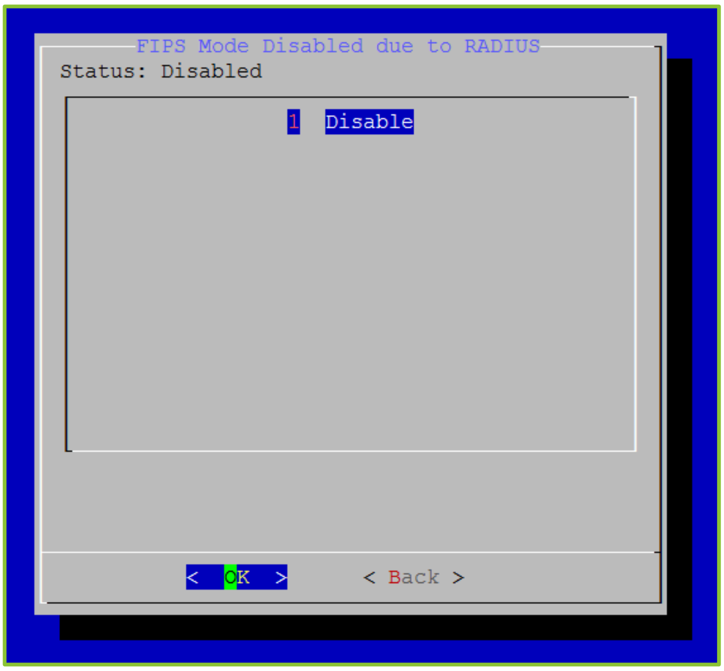
2. Enter **7** to select the Advanced option.
3. Press the Enter key to select OK.
4. Enter **1** to select the FIPS Mode option.



```
                Main Menu
Select one of the following modules:

      1  FIPS Mode
      2  OCSP Client Certificate Auth
      3  Preshared Key
      4  Recovery Utility
      5  SNMP Administration
      6  SSH Configuration
      7  Static Hosts
      8  Vidyo Support

       <  OK  >        < Back >
```

5. Press the Enter key to select OK.

The Disable option is selected.

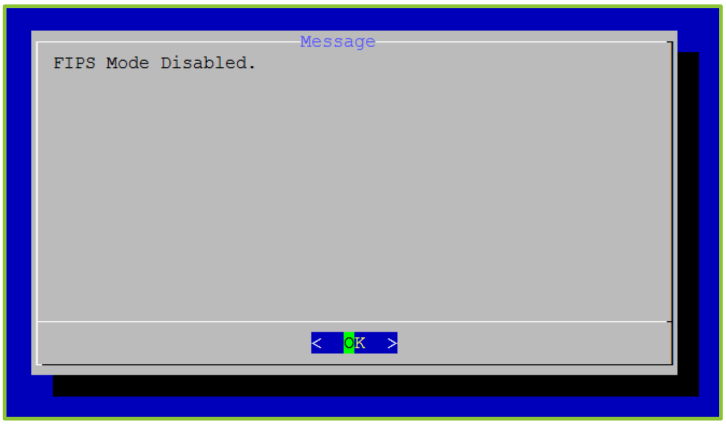


```
FIPS Mode Disabled due to RADIUS
Status: Disabled

                    1  Disable
```

Note This setting toggles between disable and enable states.

6. Press the **Enter** key to select **OK**.

   A message displays stating “FIPS Mode disabled.”

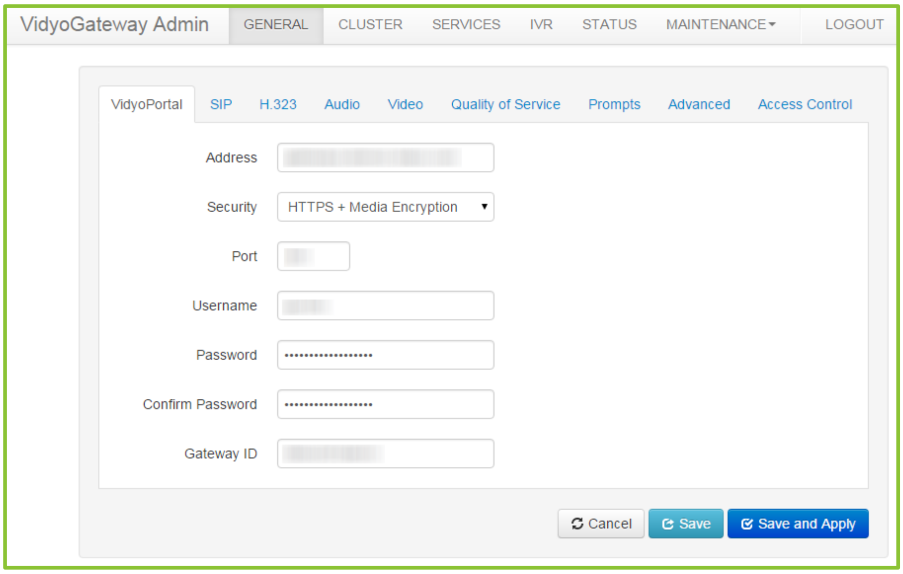


```
Message
FIPS Mode Disabled.
```

7. Press the **Enter** key to select **OK**.

5. Configuring Your System

Tabs shown along the top of your VidyoGateway Admin Pages for *GENERAL*, *CLUSTER*, *SERVICES*, *IVR*, *MAINTENANCE*, and *LOGOUT* are used to configure different areas of your system. The following sections cover these tabs in more detail.



Address [redacted]

Security HTTPS + Media Encryption ▾

Port [redacted]

Username [redacted]

Password ••••••••••••••••••

Confirm Password ••••••••••••••••••

Gateway ID [redacted]

Configuring the General Settings

The *General* tab contains subtabs covering VidyoPortal, SIP, H.323, Video, Quality of Service, Prompts, and Advanced settings for your VidyoGateway. The following sections cover these subtabs in more detail.

Configuring the VidyoPortal Settings

The *VidyoPortal* subtab is used to connect your VidyoGateway to your VidyoPortal.

- You must add your VidyoGateway server as a component on your VidyoPortal.

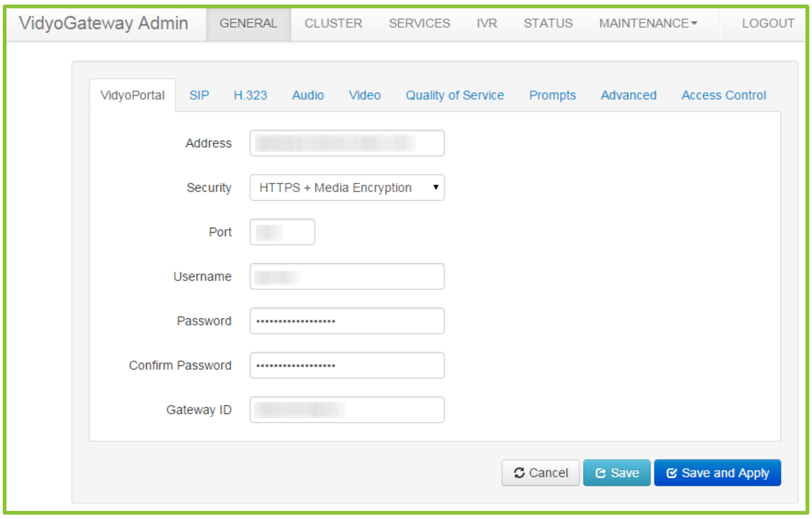
  For more information, see 2. Understanding the VidyoGateway Configuration Procedure.

- The values you provide in the fields on the *VidyoPortal* subtab are automatically propagated to your Cluster Nodes. Therefore, the *VidyoPortal* subtab does not appear when accessed from your Cluster Node servers. To make configurations on the tab, you must access it from your Active Controller.

To configure the VidyoPortal settings:

1. Log in to the Admin portal using your System Console account.

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



Address [redacted]

Security HTTPS + Media Encryption

Port [redacted]

Username [redacted]

Password ••••••••••••••••••

Confirm Password ••••••••••••••••••

Gateway ID [redacted]

The *GENERAL > VidyoPortal* page displays by default.

2. Enter the IP or FQDN address of the VidyoPortal tenant to which your VidyoGateway will be connected.
3. Select **None**, **HTTPS**, or **HTTPS + Media Encryption** from the **Security** drop-down.

   HTTPS or **HTTPS + Media Encryption** must be selected for TLS protocol fields to display on the *General > SIP* tab.

   For more information, see Configuring SIP Settings.
4. Enter the port number on which your VidyoGateway listens.

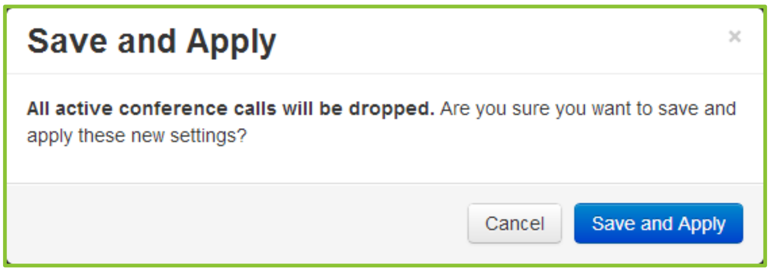
   Default port numbers for HTTP and HTTPS are **80** and **443**, respectively. You can change these values as necessary. The port number in your VidyoGateway must match the value set in your VidyoPortal. You can also configure these ports to match the firewall port range required by Legacy systems as necessary.
5. Enter your user name in the **Username** field.

   This is the username you created when adding your VidyoGateway component on your VidyoPortal. For more information, see Making Configurations on Your VidyoPortal for Your VidyoGateway.
6. Enter and confirm your password.

   This is the password you created when adding your VidyoGateway component on your VidyoPortal.
7. Enter the Gateway ID for your VidyoGateway.

   A default value is provided.
8. Click **Save** or **Save and Apply** as desired.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

- Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring SIP Settings

Use the *SIP* subtab to configure your VidyoGateway session initiation protocol (SIP) settings.

Note Values you provide in the fields on the *SIP* tab are automatically propagated to your Cluster Nodes. Therefore, the *SIP* tab does not display when accessed from your Cluster Node servers. To make configurations on the tabs, you must access them from your Active Controller.

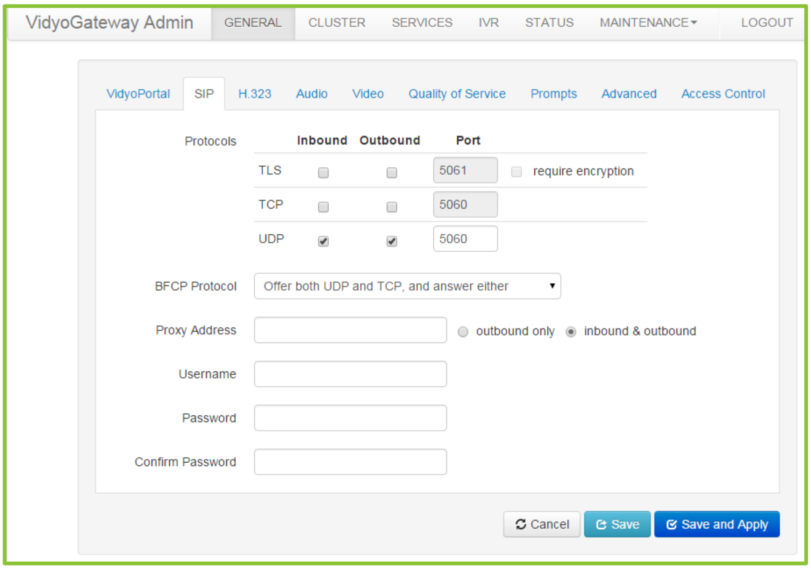
To configure the SIP settings:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *SIP* subtab.



Protocols	Inbound	Outbound	Port	
TLS	□	□	5061	□ require encryption
TCP	□	□	5060	
UDP	☑	☑	5060	

BFCP Protocol: Offer both UDP and TCP, and answer either

Proxy Address: ○ outbound only ● inbound & outbound

Username

Password

Confirm Password

3. When using the TLS protocol, provide the following information:
   a. Select the **TLS** checkboxes to encrypt the SIP signaling between the VidyoGateway and a proxy server for inbound and outbound calls.
   b. Enter a port value for **TLS**.
   c. Select the **require encryption** checkbox to only allow calls in which the media is encrypted via the secure real-time transport protocol (SRTP).

      When this checkbox is not selected, calls without SRTP media encryption are permitted on the VidyoGateway.
4. When using the TCP protocol, provide the following information:
   a. Select the **TCP** checkboxes to enable SIP over TCP support for inbound and outbound calls.
5. When using the UDP protocol, provide the following information:
   a. Select the **UDP** checkboxes to enable SIP over UDP for inbound and outbound calls.

      If both TLS and TCP are not enabled, then all outbound SIP calls will use UDP, which is not encrypted.
   b. Enter a port value for UDP.

Note If you select more than one protocol (i.e. TLS, TCP, and/or UDP), inbound traffic will be received on any of the selected protocols. Outbound calls will be routed using the following logic on selected protocols only:

Perform an outbound call using the protocol that has a resolved domain record going by the order TLS to TCP to UDP (if selected).

If all selected protocols do not have resolved domain records (i.e. DNS lookup failed on all selected protocls), the VidyoGateway will attempt an outbound call by the order UDP to TCP to TLS (if selected).

For example, if you select all three (TLS, TCP, UDP), the VidyoGateway will be listening to inbound traffic on three protocols. For outbound traffic, the VidyoGateway will attempt TLS first and if the DNS for TLS doesn't resolve, it will attempt to resolve the DNS for TCP. If that succeeds, the VidyoGateway will make an outbound SIP call using TCP.

6. Use the **BFCP Protocol** drop-down to select one of the following:
   - Select **Offer both UDP and TCP**, and answer either to offer and answer both protocols.
   - Select **Offer only UDP / prefer UDP** on answer to only offer the UDP protocol and prefer it when answering calls.
   - Select **Offer only TCP / prefer TCP** on answer to only offer the TCP protocol and prefer it when answering calls.

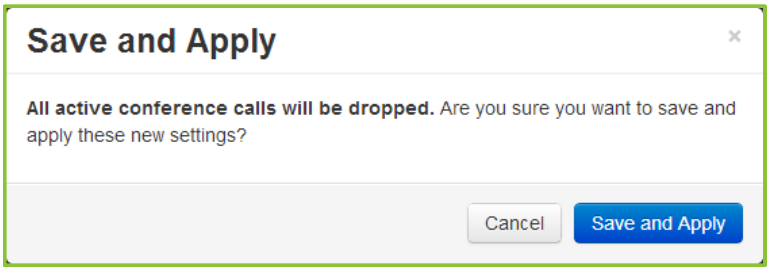
Note VidyoGateway can only act as a BFCP server.

7. When using a Proxy Address, provide the following information:
   a. Enter a Proxy Address.
   b. Select one of the following:
      - □ Select **outbound only** if you want to only route outbound calls through your proxy.

        With **outbound only** selected, all calls are sent to the proxy; however, inbound calls are accepted from any device.
      - □ Select **inbound & outbound** to route both inbound and outbound calls through your proxy.

        With **inbound & outbound** selected, calls received from any device other than the proxy are rejected.
8. Enter the username for your proxy server.
9. Enter the password for your proxy server.
10. Click **Save** or **Save and Apply** as desired.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

- Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.
- For information about the Local SIP Port, see Configuring Advanced Settings.

Configuring H.323 Settings

The *H.323* subtab is used to configure your VidyoGateway H.323 protocol settings. However, before you configure your H.323 settings, you must select whether you are using a Standalone VidyoGateway (a single component acting as both Controller and VidyoGateway) or Clustered VidyoGateways because the fields on the *H.323* subtab change depending on which configuration you set.

For more information about Standalone and Clustered VidyoGateways and about how to set either configuration, see Understanding VidyoGateway Clusters and Configuring Clusters.

Note Values you provide in the fields on the *H.323* subtab are automatically propagated to your Cluster Nodes. Therefore, the *H.323* subtab does not display when accessed from your Cluster Node servers. To make configurations on the tabs, you must access them from your Active Controller.

Configuring H.323 Settings When Using a Standalone VidyoGateway

When your VidyoGateway is configured as a Standalone VidyoGateway, the following settings are available in the *H.323* subtab.

For more information, see Configuring Clusters.

To configure the H.323 settings when using a Standalone VidyoGateway:

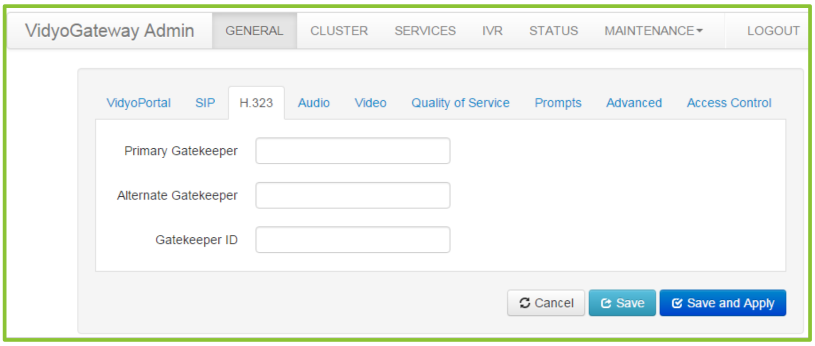
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *H.323* subtab.

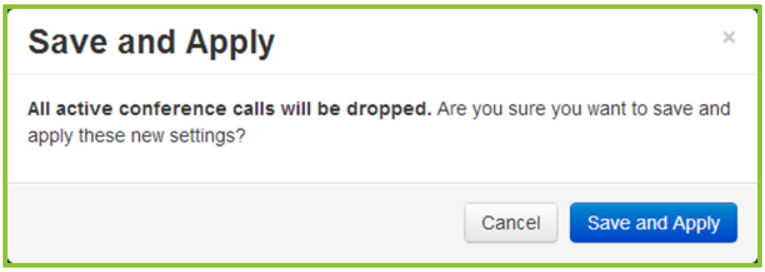
The following screenshot shows the fields that display when the VidyoGateway has been configured as a Standalone VidyoGateway using the *Cluster* tab described in Configuring Clusters.



3. Enter the hostname or IP address of your primary gatekeeper in the **Primary Gatekeeper** field.
4. Enter the name of your alternate gatekeeper in the **Alternate Gatekeeper** field.

Note An alternate gatekeeper is automatically registered when the active gatekeeper fails and remains connected until the active gatekeeper and the VidyoGateway are restarted.

5. Enter your Gatekeeper ID in the **Gatekeeper ID** field.
6. Click **Save** or **Save and Apply** as desired.
   - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.


Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

   - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring H.323 Settings When Clustering Your VidyoGateways

When you configure your VidyoGateway as a cluster, the following settings are available in the *H.323* subtab.

For more information, see Configuring Clusters.

To configure the H.323 settings when clustering your VidyoGateways:

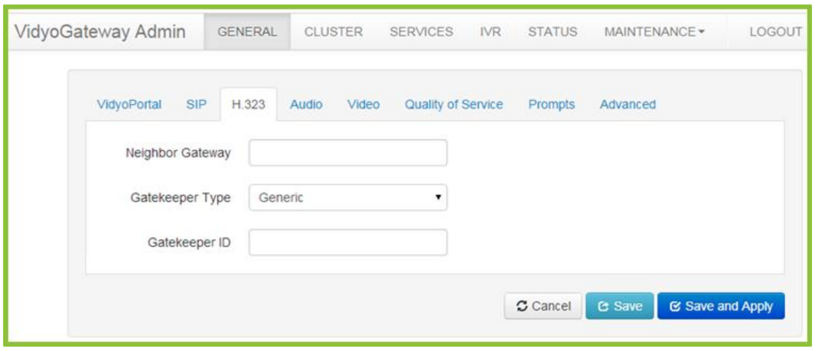
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *H.323* subtab.

   The following screenshot shows the fields that appear when the VidyoGateway has been configured as a cluster VidyoGateway using the *Cluster* tab described in Configuring Clusters.



Neighbor Gateway

Gatekeeper Type: Generic

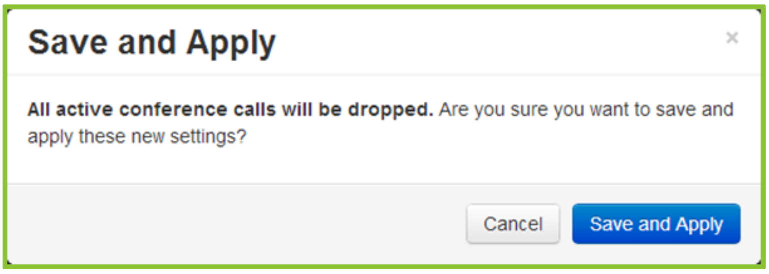
Gatekeeper ID

3. Enter the hostname or IP address of your gatekeeper in the **Neighbor Gateway** field.
4. Select your gatekeeper type in the **Gatekeeper Type** drop-down.
5. Enter your Gatekeeper ID in the **Gatekeeper ID** field.

Note Neighboring mode requires reconfiguration of your external H.323 gatekeeper to support neighboring. For more information, refer to your external gatekeeper documentation.

6. Click **Save** or **Save** and **Apply** as desired.

   - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

   - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring Audio Settings

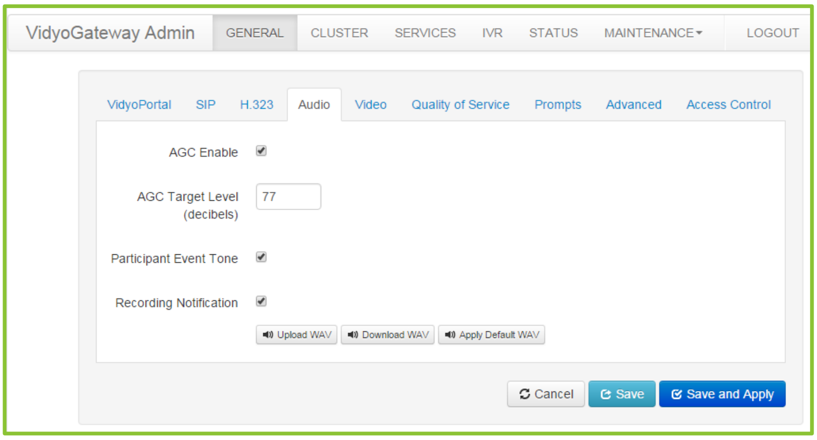
To configure the audio settings:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *Audio* subtab.



AGC Enable ☑

AGC Target Level (decibels) 77

Participant Event Tone ☑

Recording Notification ☑

3. Select the **AGC Enable** checkbox to control the audio stream coming from your Legacy devices and going out of your VidyoGateway to Vidyo endpoints.

   This checkbox is enabled by default.

4. Enter a desired decibel level for your gain control setting in the **AGC Target Level (decibels)** field.

   You can only enter a decibel level in the **AGC Target Level (decibels)** field when the **AGC Enable** checkbox is selected. The supported range is 58-89 dB; however, Vidyo recommends that you do not change the AGC default level.

5. Select the **Participant Event Tone** checkbox to sound a tone whenever conference participants join or leave conferences.

6. Select the **Recording Notification** checkbox to play a message or tone whenever the conference is being recorded.

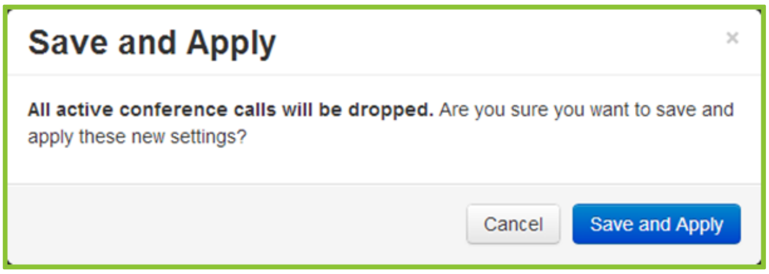
7. Select the .wav files as follows:

   - Click **Upload WAV** to select a custom sound file to alert users whenever a recording is happening.
   - Click **Download WAV** to save the sound file being currently used to alert users whenever a recording is happening.

- Click **Apply Default WAV** to use the original system sound file to alert users whenever a recording is happening.

8. Click **Save** or **Save and Apply** as desired.

   - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

   - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring Video Loopback Settings

Video loopback is not available if IVR is enabled. For more information, see Configuring Integrated Voice Response (IVR) Settings.

The video loopback image is the on-screen image that the Legacy user sees when connected to a VidyoRoom™ and no other participants have entered the VidyoConference. For example, if you call a VidyoRoom and no one else has joined the conference yet, instead of seeing an image of yourself in the other tile, you would see the loopback image. The image must be a **.bmp** file.

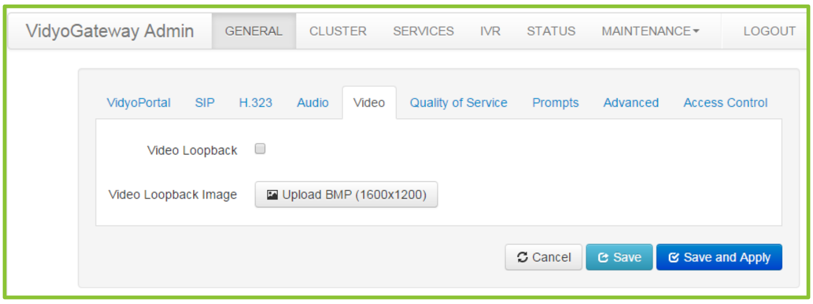
To configure the video loopback settings:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *Video* subtab.



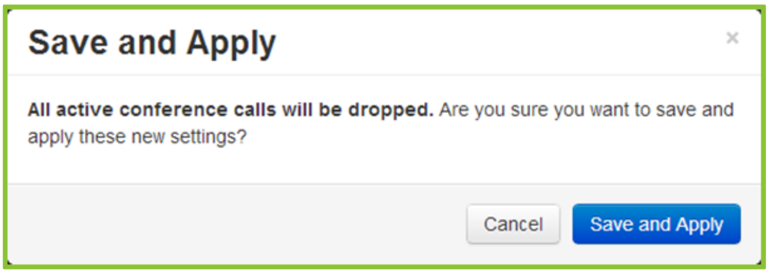
Video Loopback ☐

Video Loopback Image

3. Select the **Vidyo Loopback** checkbox.

4. Click **Upload BMP (1600X1200)** to locate the **.bmp** image file.

5. Click **Save** or **Save and Apply** as desired.
   - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

   - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring Quality of Service (QoS) Settings

The *Quality of Service* subtab is where you select the service used for prioritizing incoming and outgoing media packets.

You can choose between IP Precedence or Differentiated Services Code Point (DSCP) service types. Depending on the service type selected, you can assign specific values to packets coming from your VidyoGateway to your VidyoRouter and your Legacy device for video, audio, content data, and signaling services set on this screen.

With these specified values assigned to media types coming from your VidyoGateway, you can then configure your network router or switch to prioritize the packets as desired.

Tip: Look online for the most current IP Precedence or DSCP service value conversion table data.

Quality of Service Settings with IP Precedence Selected as the Type of Service

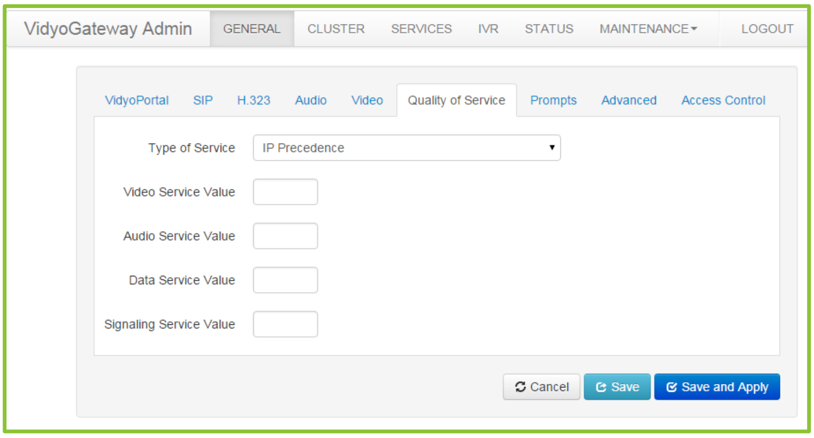
To configure quality of service settings with IP precedence selected as the type of service:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.
2. Click the *Quality of Service* subtab.

3. Select **IP Precedence** from the **Type of Service** drop-down.



Type of Service: IP Precedence

Video Service Value

Audio Service Value

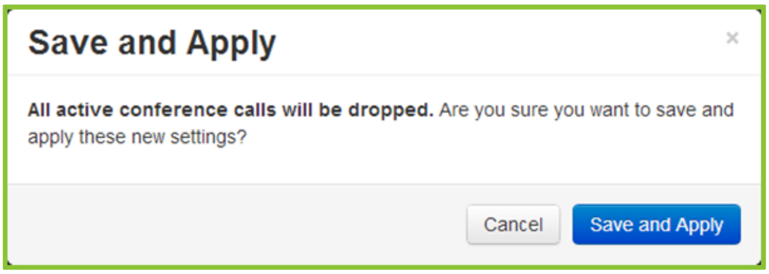
Data Service Value

Signaling Service Value

4. Enter the appropriate values for your service assignments in the **Video Service Value**, **Audio Service Value**, **Data Service Value**, and **Signaling Service Value** fields.

5. Click **Save** or **Save and Apply** as desired.

   - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

   - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Quality of Service Settings with DSCP Selected as the Type of Service

To configure quality of service settings with DSCP selected as the type of service:

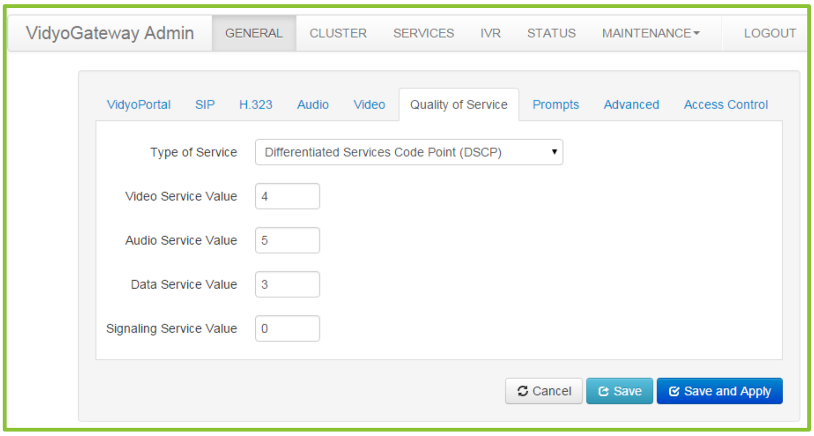
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *Quality of Service* subtab.

3. Click the **Type of Service** drop-down and select **Differentiated Service Code Point (DSCP)**.



Type of Service: Differentiated Services Code Point (DSCP)

Video Service Value: 4

Audio Service Value: 5

Data Service Value: 3

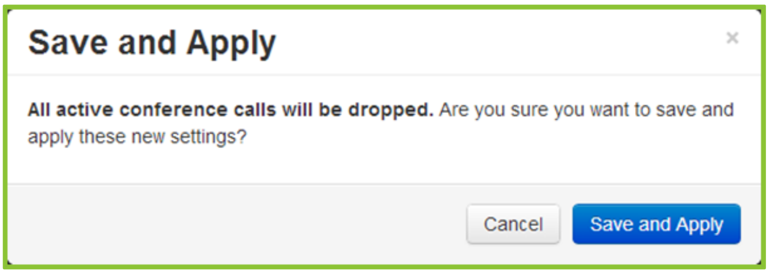
Signaling Service Value: 0

4. Enter the appropriate values for your service assignments in the **Video Service Value**, **Audio Service Value**, **Data Service Value**, and **Signaling Service Value** fields.

   Leave the default values provided for each of these fields if you are uncertain of the configuration that is needed.

5. Click **Save** or **Save and Apply** as desired.

   - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

   - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring Prompts and Call Control via DTMF Tones

You can use the *Prompts* subtab to configure BMP and WAV files for the waiting room IVR, which will be presented to participants while they are in Waiting Room mode. Additionally, audio prompts can be configured for call control options via DTMF tones by uploading new WAV files. All WAV files must be PCM encoded at 16 KHz sampling.

The default call control options are as follows:

- *0: To list all call control options
- *3: To enable/disable the hearing of entry and exit tones

- *6: To mute and unmute the line

Administrators can enable or disable the use of DTMF control options for their end users by selecting or deselecting the **Enable DTMF Control Keys** checkbox as explained below.

For more information about Waiting Room mode, refer to "Configuring Conference Settings" in the *VidyoConferencing Administrator Guide*.

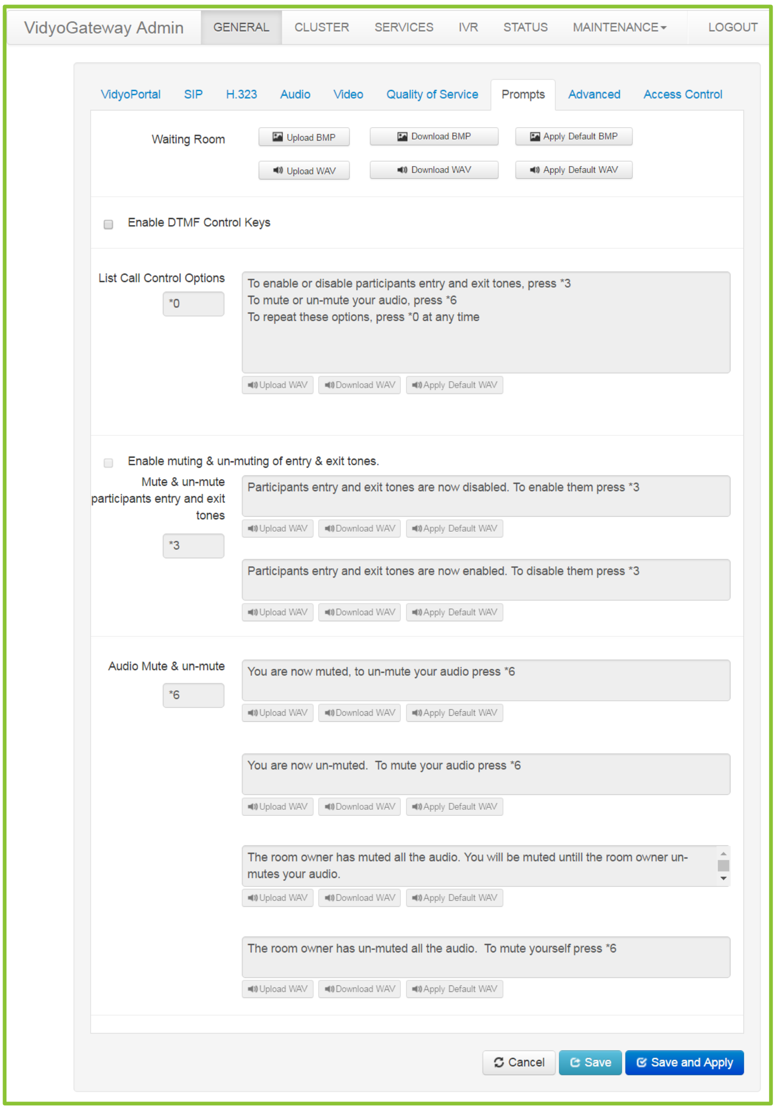
To configure prompts and call control via DTMF tones:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *Prompts* subtab.



Waiting Room

□ Enable DTMF Control Keys

List Call Control Options: *0

To enable or disable participants entry and exit tones, press *3
To mute or un-mute your audio, press *6
To repeat these options, press *0 at any time

□ Enable muting & un-muting of entry & exit tones.

Mute & un-mute participants entry and exit tones: *3

Participants entry and exit tones are now disabled. To enable them press *3

Participants entry and exit tones are now enabled. To disable them press *3

Audio Mute & un-mute: *6

You are now muted, to un-mute your audio press *6

You are now un-muted. To mute your audio press *6

The room owner has muted all the audio. You will be muted untill the room owner un-mutes your audio.

The room owner has un-muted all the audio. To mute yourself press *6

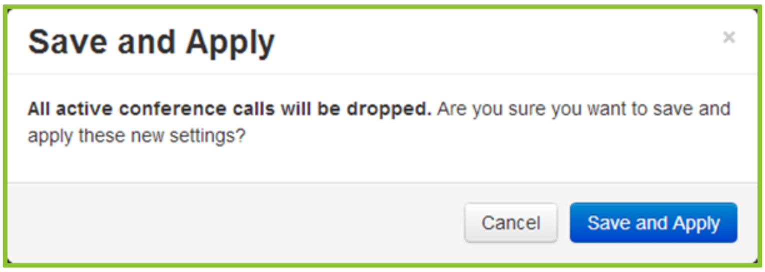
3. Use any of the following options that apply to the prompt type that needs to be configured:
   - Click **Upload BMP** to upload a custom screen image file.
   - Click **Upload WAV** to upload a custom sound file.
   - Click **Download BMP** to view the screen image file currently in use.
   - Click **Download WAV** to play the sound file currently in use.

Note The **`.wav`** file for the waiting room prompt is played in a loop every 10 seconds after the announcement finishes as long as the conference is in Waiting Room mode.

   - Click **Apply Default BMP** to use the original system screen image.

     A system notification displays indicating that the system has applied the default waiting room BMP.
   - Click **Apply Default WAV** to use the original system sound file.

     A system notification displays indicating that the system has applied the default waiting room WAV.
4. Select the **Enable DTMF Control Keys** checkbox if you want to allow users to use the default call control options when on a call.
5. Select the **Enable muting & un-muting of entry & exit tones** checkbox if you want to allow users to use the mute and un-mute of entry and exit tone prompts when on a call.
6. Click **Save** or **Save and Apply** as desired.
   - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

   - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring Advanced Settings

The *Advanced* subtab is used to configure specific port settings and specify a PIN delimiter.

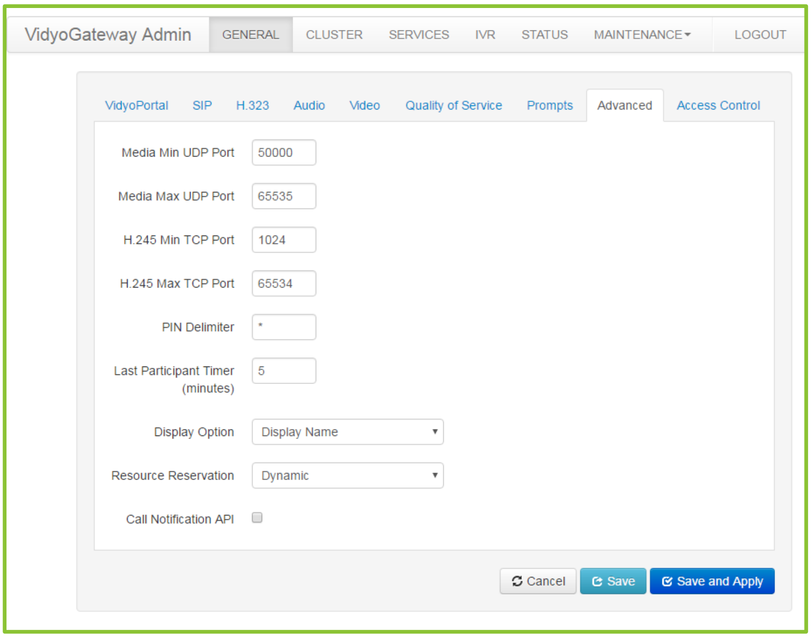
To configure advanced settings:

1. Log in to the Admin portal using your System Console account.

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

The *GENERAL > VidyoPortal* page displays by default.

2. Click the *Advanced* subtab.



Media Min UDP Port: 50000
Media Max UDP Port: 65535
H.245 Min TCP Port: 1024
H.245 Max TCP Port: 65534
PIN Delimiter: *
Last Participant Timer (minutes): 5
Display Option: Display Name
Resource Reservation: Dynamic
Call Notification API: □

3. Enter the UDP ports in the **Media Min UDP Port** and **Media Max UDP Port** fields used for media transport between the VidyoGateway and the Legacy device and between the VidyoGateway and the VidyoRouter.

   You must specify a minimum range of 1000.

   - Enter the lower limit of the port range in the **Media Min UDP Port** field. The default (and recommended) value is **1024**.
   - Enter the upper limit of the port range in the **Media Max UDP Port** field. The default (recommended and maximum) value is **65535**.

4. Enter the number of TCP ports in the **H.245 Min TCP Port** and **H.245 Max TCP Port** fields used for media transport between the VidyoGateway and the Legacy device and between the VidyoGateway and the VidyoRouter.

   You must specify a minimum range of 1000.

   - Enter the minimum port number in the **H.245 Min TCP Port** field to use for H.243 traffic. The value must be an inclusive number between 1 and 65535.
   - Enter the maximum port number in the **H.245 Max TCP Port** field to use for H.243 traffic. The value must be an inclusive number between 1 and 65535.

5. Enter the character you want used as the separator between the username and the personal identification number on PIN-protected endpoint call requests in the **PIN Delimiter** field.

6. Enter a value in the **Last Participant Timer (minutes)** field to indicate when a participant, who joined the conference from a Legacy endpoint and remains the only participant on the call, is automatically disconnected from the conference.

   This feature has a default setting of **0** (zero) which disables the timeout. Enter an amount of time (in minutes) to avoid lone VidyoConference participants from Legacy endpoints accidentally tying up lines to VidyoConferences.

7. Select **Display Name**, **E.164**, or **E.164 & Display Name** from the **Display Option** drop-down to determine the items you want included for identification purposes on your calls and added to the CDR data on your VidyoPortal.

8. Select **Dynamic** or **Static** from the **Resource Reservatio**n drop-down to specify how resources are allocated.

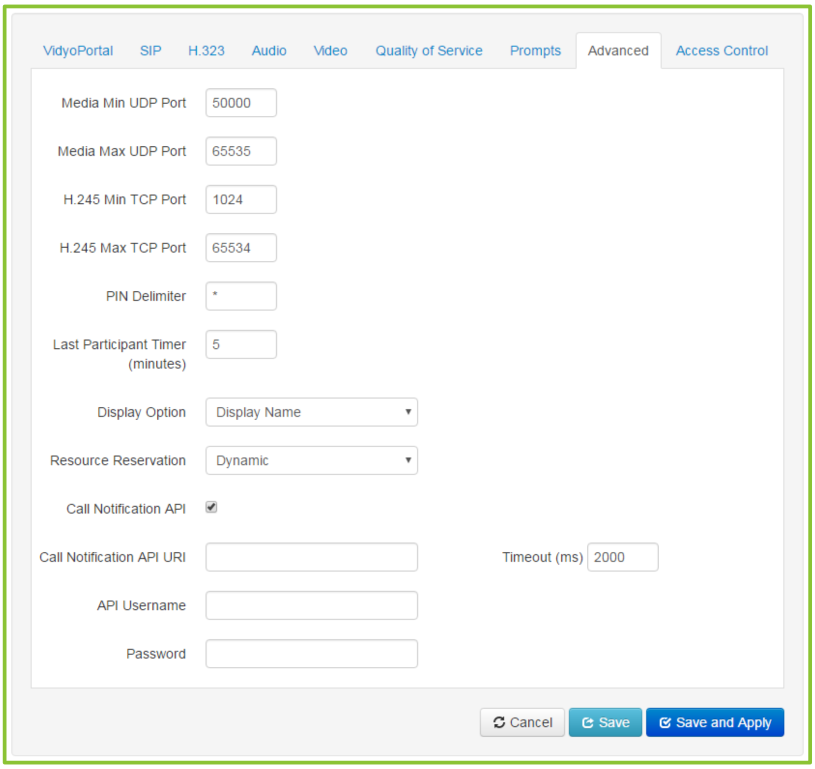
   - For example, when **Dyamic** is selected, a SD call made on an HD prefix consumes SD resources.
   - When **Static** is selected, resources are consumed based on the prefix solely.

   With static allocation and high frame rate share, the resource allocated to a call is based on the sum of the video resolution and the share resolution. For example, if the video resolution is set to SD and share resolution is set to HD, then the call consumes as much resources as one HD call and one SD call. The frame rate of the video or app share streams is not relevant.

Note When selecting **Static** from the **Resource Reservation** drop-down, it is recommended that the administrator provides a sufficient amount of bandwidth for HD content sharing.

9. Select the **Call Notification API** checkbox if you want to enable VidyoGateway to convey to the external application the details of an incoming call (including the extension dialed, source IP address, protocol, and device information) and to receive a response with either a new dial string that will be used for connecting the call to the VidyoPortal or an indication to reject the incoming call.

When you select this checkbox, additional fields appear and you must do the following:



Media Min UDP Port: 50000

Media Max UDP Port: 65535

H.245 Min TCP Port: 1024

H.245 Max TCP Port: 65534

PIN Delimiter: *

Last Participant Timer (minutes): 5

Display Option: Display Name

Resource Reservation: Dynamic

Call Notification API: ☑

Call Notification API URI:

Timeout (ms): 2000

API Username:

Password:

a. Enter the URI address in the **Call Notification API URI** field for which the API call should be made.

b. Enter the time in milliseconds in the **Timeout (in ms)** field, to wait to get a response back from the external application.

   The default is 2000 ms.

c. Enter the credentials in the optional **API Username** and **Password** fields to be used for authentication against the external application.

Note The faults received from the external application (as detailed in the *Vidyo Web Services API User Guide*) are mapped to the following IVR prompts:

- 425 is mapped to “Retry Locked Room”

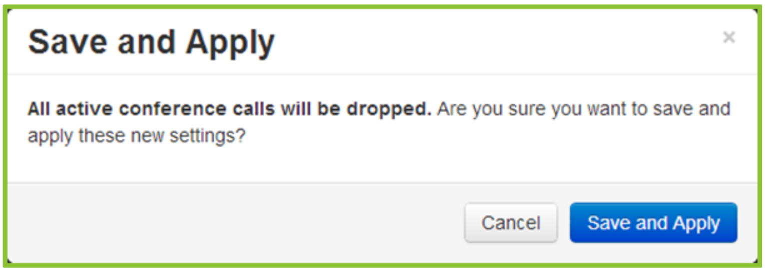
- 404 is mapped to “Retry Conference Extension”

- Other faults are mapped to “Retry Room Generic Error”

For more information about the Call Notification API, refer to the “VidyoGateway API” chapter of the *Vidyo Web Services API User Guide*.

Caution	Once you have enabled the Call Notification API, Vidyo strongly recommends that you check the connectivity to the external application. Since all incoming calls will then be routed via the external application, you must ensure that you have not inadvertently configured the external application to prevent calls from being sent to the VidyoPortal.

10. Click **Save** or **Save and Apply** as desired.
    - When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

    - Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring Access Control Settings

The *Access Control* subtab is used for protecting the VidyoGateway from intrusion or DoS attacks. The administrator can configure the VidyoGateway for one of four modes.

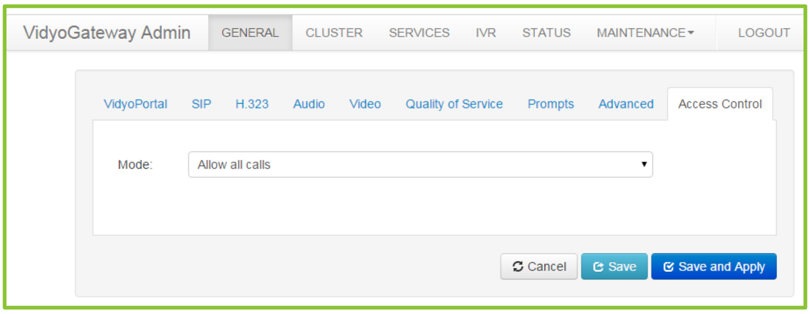
To configure access control settings:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

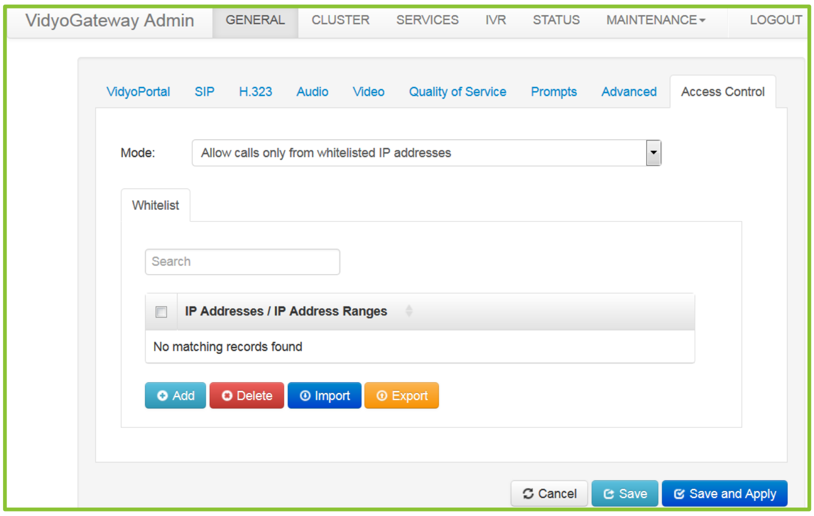
2. Click the *Access Control* subtab.



Mode: Allow all calls

3. Select the appropriate option from the **Mode** drop-down.

- **Allow all calls** will not block any calls reaching the VidyoGateway.

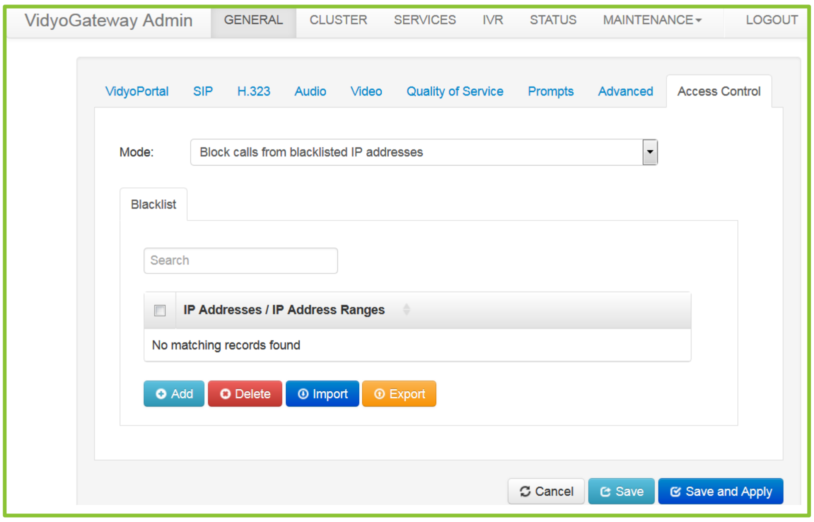


Mode: Allow calls only from whitelisted IP addresses

No matching records found

- **Allow calls only from whitelisted IP addresses** will only allow incoming calls from pre-configured IP addresses.
  - □ Enter IPs that have been configured to interact with the VidyoGateway in the **Search** field.

    The search results display below.
  - □ Click **Add** to add additional IPs and IP Ranges.
  - □ Select the checkbox to the left of the IP Address or IP Address Range that needs to be deleted, and click **Delete**.
  - □ Click **Import** to import a `.csv` file that contains a list of IPs and IP Ranges.
  - □ Click **Export** to export the IPs and IP Ranges.

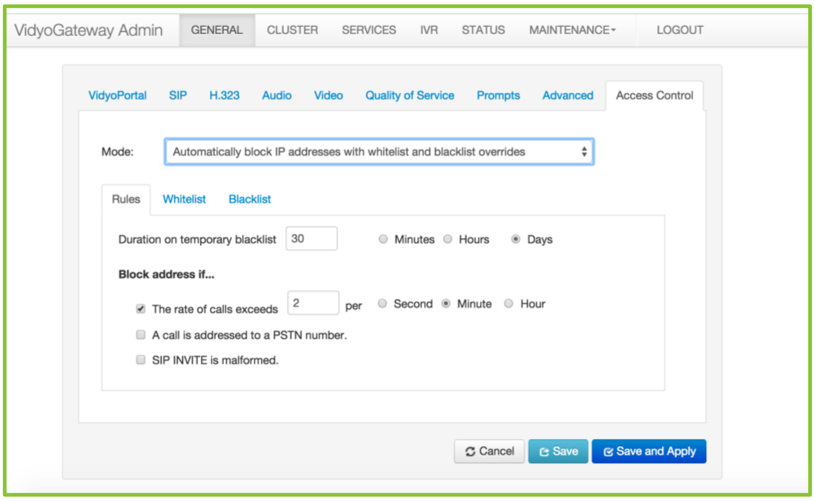


Mode: Block calls from blacklisted IP addresses

No matching records found

- **Block calls from blacklisted IP addresses** will allow incoming calls that are not configured in the blacklist table.
  - Enter IPs that have been configured to be blocked from reaching the VidyoGateway in the **Search** field.

    The search results display below.
  - Click **Add** to add additional IPs and IP Ranges.
  - Select the checkbox to the left of the IP Address or IP Address Range that needs to be deleted, and click **Delete**.
  - Click **Import** to import a **`.csv`** file that contains a list of IPs and IP Ranges.
  - Click **Export** to export the IPs and IP Ranges.



Mode: Automatically block IP addresses with whitelist and blacklist overrides

Duration on temporary blacklist 30 ○ Minutes ○ Hours ● Days

Block address if...

☑ The rate of calls exceeds 2 per ○ Second ● Minute ○ Hour

☐ A call is addressed to a PSTN number.

☐ SIP INVITE is malformed.

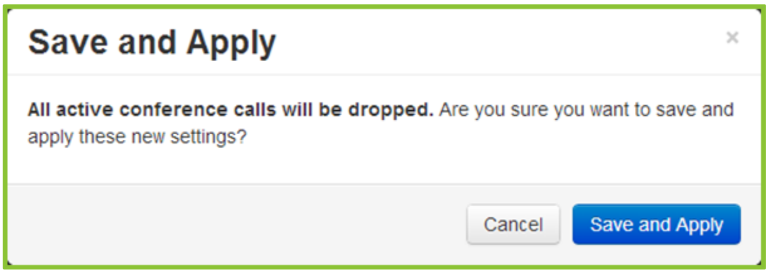
- **Automatically block IP addresses with whitelist and blacklist overrides** will dynamically add blacklisted IP addresses that comply with the rules configured with overrides of whitelisting and blacklisting tables in the adjacent subtabs.
  - From the *Rules* subtab:
    - Enter a value for the **Duration on temporary blacklist** and select the corresponding radio button that best represents the type of duration in time (e.g., Minutes, Hours, or Days).
    - Set the following parameters if the address should be blocked for any of the following reasons:
      - Select the **The rate of calls exceeds** checkbox, enter a value in the text box, and select the corresponding radio button that best represents the type of duration in time (e.g., Second, Minute, or Hour).
      - Select the **A call is addressed to a PSTN number** checkbox.
      - Select the **SIP INVITE is malformed** checkbox.

- □ Click the *Whitelist* and *Blacklist* subtabs and do the following as needed:
    - o Enter IPs that have been configured to interact or be blocked from reaching the VidyoGateway in the **Search** field.

      The search results display below.
    - o Click **Add** to add additional IPs and IP Ranges.
    - o Select the checkbox to the left of the IP Address or IP Address Range that needs to be deleted, and click **Delete**.
    - o Click **Import** to import a `.csv` file that contains a list of IPs and IP Ranges.
    - o Click **Export** to export the IPs and IP Ranges.

4. Click **Save** or **Save and Apply** as desired.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

- Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Understanding VidyoGateway Clusters

A VidyoGateway can be configured as a single Standalone VidyoGateway (a single component acting as both Controller and VidyoGateway) or as a cluster setup with an Active Controller, Standby Controller, and Cluster Node VidyoGateway.

This section explains various VidyoGateway cluster configurations used to support as many H.323 and SIP calls required prior to going through the *CLUSTER* tab in the VidyoGateway Admin Pages. Think of a VidyoGateway cluster as a large, single VidyoGateway system.

Note With Clustering enabled on your VidyoGateway, some security scanners may indicate the presence of Telnet as running on your server. This detection is a false positive and Telnet is not actually running on your VidyoGateway.

When configuring your VidyoGateways as a cluster, you must export the pre-shared key from your Active Controller and import it into your Standby Controller and Cluster Nodes. Otherwise, calls on your Standby Controller or Cluster Nodes will not be visible from the *STATUS* tab in your Active Controller.

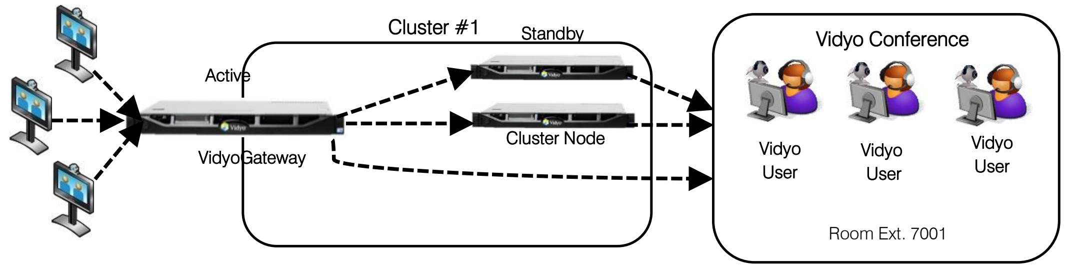
Clustering Benefits

VidyoGateway clustering enables you to scale your VidyoGateway capacity to hundreds of simultaneous calls by deploying multiple VidyoGateways per VidyoPortal and per tenant. By clustering, you are enabling the multiple VidyoGateways to balance both the H.323 and SIP load, thereby increasing your call scalability.

When creating clusters, you need to assign Controller 1 to one of your VidyoGateways and designate the other VidyoGateways as Controller 2 and/or Cluster Node. Any VidyoGateway can be a Controller 1, Controller 2, or Cluster Node in your VidyoGateway cluster. The Active and Standby Controller roles will be automatically assigned by the system to the two controllers (Controller 1 and Controller 2).

The Active Controller automatically sends calls to the first available VidyoGateway in your cluster.

To assign the VidyoGateway Standalone, Controller 1, Controller 2, or Cluster Node, use the *CLUSTER* tab. For more information, see Configuring Clusters.



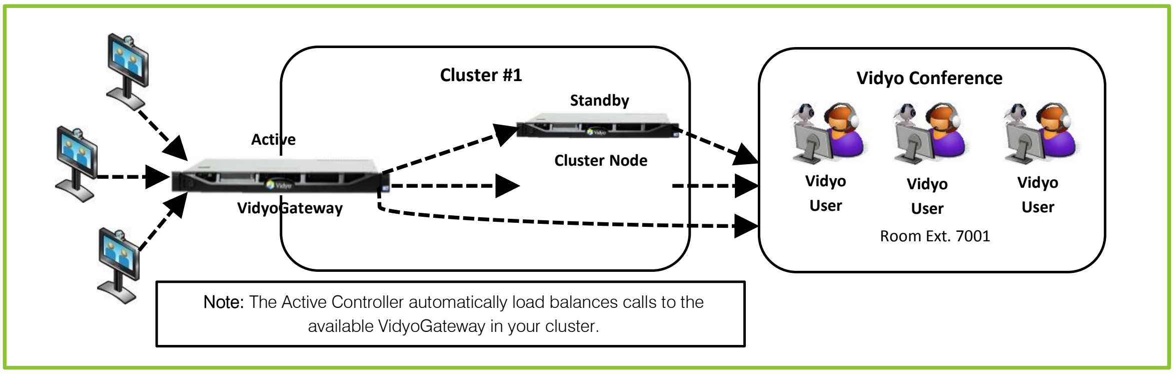
Note: The Active Controller automatically load balances calls to the available VidyoGateway in your cluster.

Note The Active Controller automatically sends calls to the first available VidyoGateway in your cluster.

Cluster Configuration with a Legacy Gatekeeper Interface

After configuring your VidyoGateway cluster, see Configuring Clusters, you can then configure your system to interface with a Legacy gatekeeper as shown in the following illustration.

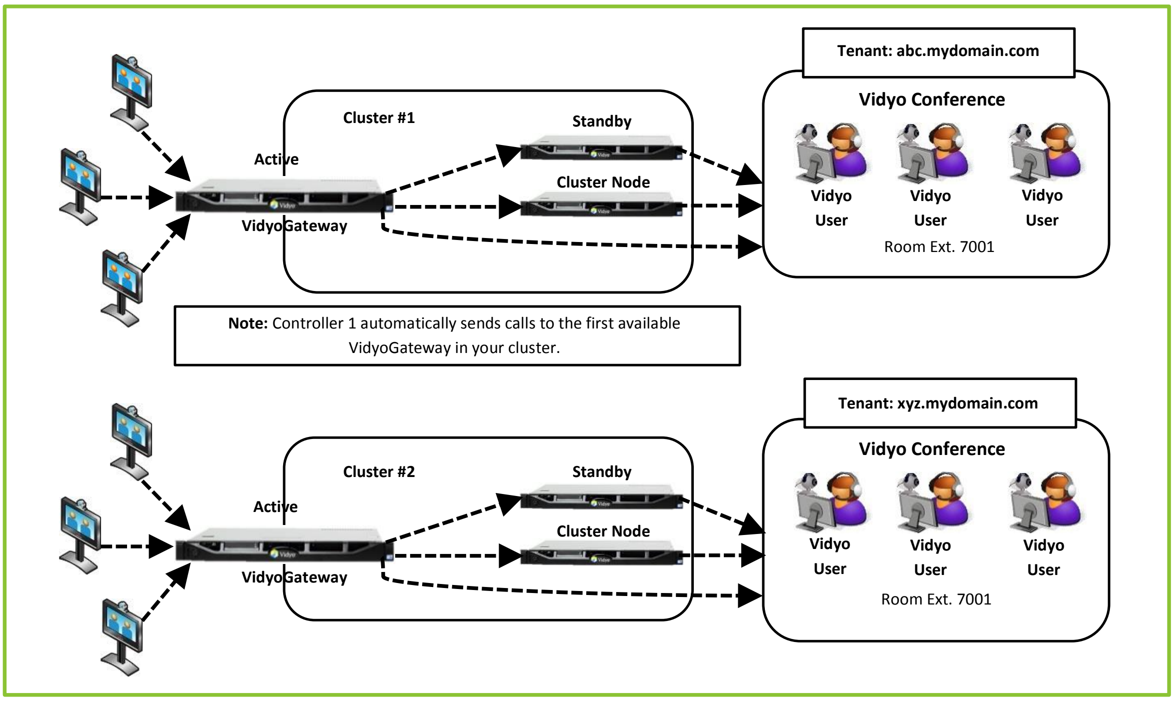
For more information about configuring gatekeepers, see Configuring H.323 Settings.


Cluster #1
Standby
Cluster Node
Active
VidyoGateway
Vidyo Conference
Vidyo User
Vidyo User
Vidyo User
Room Ext. 7001
Note: The Active Controller automatically load balances calls to the available VidyoGateway in your cluster.

Deploying Multiple VidyoGateway Clusters

If you deploy large-scale, geographically diverse networks serving multiple tenants, you can provision multiple VidyoGateway clusters in a single VidyoPortal. In such cases, you may want to dedicate scalable VidyoGateway clusters to certain locations or tenants as shown in the following illustration.

The VidyoGateway setting for pointing to a specific VidyoPortal is done from the *GENERAL > VidyoPortal* tab. For more information, see Configuring the VidyoPortal Settings.



The Standby Controller and Cluster Nodes must be associated with their corresponding Active Controller. This is done by entering the specific Controller 1 Peer IP Address in to the Shared

Controller IP Address field for the Controller 2 and Cluster Node VidyoGateways on the *CLUSTER* tab. For more information, see Configuring Clusters.

Configuring Clusters

The *CLUSTER* tab provides options to configure your VidyoGateway server as a Standalone, Controller 1, Controller 2, or Cluster Node. The following sections cover these configurations in more detail.

Each VidyoGateway server in your cluster must align to the following requirements:

- A public IP addresses must be used. This means none of the VidyoGateway servers in your cluster can be NATed.
- If they are behind a firewall, it must permit Legacy ports for each VidyoGateway server in your Cluster. This is usually configured as a set range of IP addresses in your firewall.
- Each VidyoGateway server in your cluster must have IVR Enabled and identical IVR configurations. For more information, see Configuring Integrated Voice Response (IVR) Settings.
- Each VidyoGateway server in your cluster must all be physically located in the same data center. The clustering functionality does not support VidyoGateways located in separate data centers.
- Each VidyoGateway server in your cluster must have a properly configured hostname, IP address, and shared IP address. The information for each of these fields is required for the Cluster to work. The shared IP address is the one that will be dialed by incoming calls. For more information, see Configuring Controller 1, Configuring Controller 2, and Configuring Your Cluster Node.
- VidyoGateway high availability relies on the address resolution protocol (ARP) request to determine whether the floating IP address is up. If it is not up, the VidyoGateway (active or standby) takes possession of the shared IP address.

The *Cluster Configuration* screen allows you to specifically designate your machine as a Standalone, Controller 1, Controller 2, or Cluster Node VidyoGateway. You can also provide additional data for each component depending on the machine's VidyoGateway cluster role. A specific email address can be set on the Controller nodes to send an automatic failover notification for protective measures.

When the Active Controller is configured properly, the following takes place in the event of a failure:

1. Existing calls fail as the Standby Controller takes the IP address of the Active Controller that went down.
2. The new Active Controller sends out the email notification alerting users of the system failure.

Note The original Active Controller must be repaired with its original hardware and software intact in order to be returned to your system setup.

Understanding the Clustering Procedure

Perform the steps from the following sections to create your VidyoGateway Cluster.

To create a VidyoGateway cluster:

1. Make sure you've assigned a hostname to Controller 1, and then reboot your machine.

   For more information, see Viewing Application and System Information.

2. Access Controller 2 and assign a different hostname to it, and then reboot your machine.

   For more information, see Viewing Application and System Information.

3. Configure the cluster settings on Controller 1, reboot, and then reboot your machine.

   For more information, see Configuring Controller 1.

4. Configure the nodes for the active controller.

   For more information, see Configuring Nodes for the Active Controller in Cluster Mode.

5. Configure the cluster settings on Controller 2, reboot, and then reboot your machine.

   For more information, see Configuring Controller 2.

6. Configure the cluster settings on your Cluster Node, and then reboot your machine.

   For more information, see Configuring Your Cluster Node.

Returning a Repaired Controller to Your System Setup

The original Active Controller should be returned to your system setup and configured as a Standby Controller.

Replacing an Irreparable Controller to Your System Setup

Vidyo recommends you replace the original Controller 1 with a Cluster Node (if you have one in your system setup). The Cluster Node VidyoGateway is then recognized as a Standby Controller, but is mislabeled as the Cluster Node.

Note If desired, you can reconfigure your Controllers to bear the correct Controller 1 and Controller 2 labeling. However, this is not required and the system is fully functional in this state.

Some people setup VidyoGateway systems with a single Standalone VidyoGateway (a single component acting as both Controller and VidyoGateway). Other clients designate Controller 1, Controller 2, and Cluster Node VidyoGateways. You can think of the latter as a large, single VidyoGateway system.

A variety of VidyoGateway cluster configurations are used to support H.323 and SIP call volume requirements. For more information, see Understanding VidyoGateway Clusters.

The following sections show you how to configure each VidyoGateway component type using the *CLUSTER* tab.

Configuring Your Standalone VidyoGateway

Your server is set as a Standalone VidyoGateway by default. Unless it's changed, you don't need to modify the configuration.

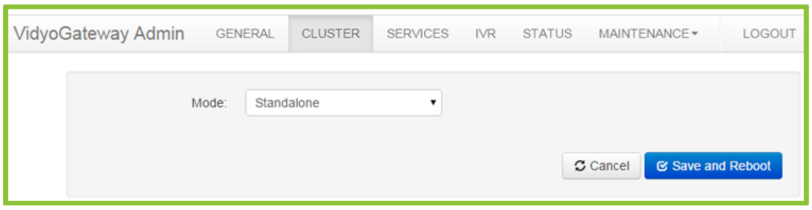
Note The *SERVICES* tab and the *Clusters > Nodes* subtab will not display once the Standalone VidyoGateway is configured.

To configure your Standalone VidyoGateway:

1. Log in to the Admin portal using your System Console account.

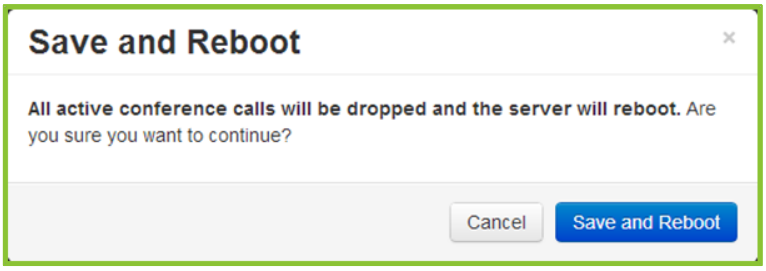
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.
2. Click the *CLUSTER* tab.
3. Select **Standalone** from the **Mode** drop-down.

   Mode: Standalone
4. Click **Save and Reboot**.
   - Any modifications you make to your Clusters accrue until you click **Save and Reboot**, and then all of your Cluster changes are applied to your VidyoGateway server.

- When you click **Save and Reboot**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Reboot

All active conference calls will be dropped and the server will reboot. Are you sure you want to continue?

Configuring Controller 1

Before configuring clusters, be sure to review Understanding the Clustering Procedure.

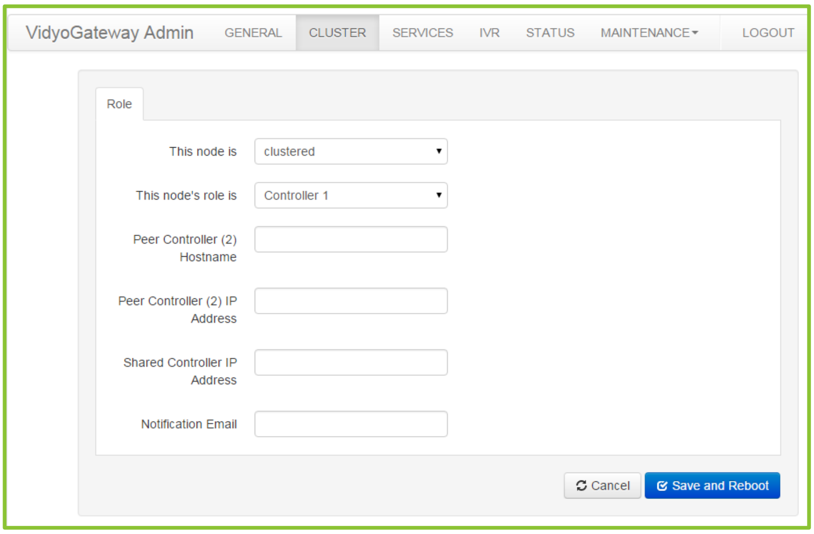
To configure Controller 1:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *CLUSTER* tab.
3. Select **clustered** from the **Mode** drop-down.
4. Select **Controller 1** from the **Role** drop-down.



This node is: clustered

This node's role is: Controller 1

Peer Controller (2) Hostname:

Peer Controller (2) IP Address:

Shared Controller IP Address:

Notification Email:

5. Configure Controller 1 as follows:

   - Enter a Controller 2 Hostname.

     Provide the Hostname exactly as it's shown in the System Console and do not provide an FQDN as the Peer Host Name.

For more information, see Viewing Application and System Information.

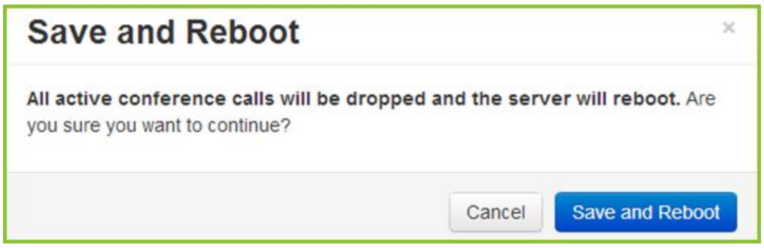
- Enter a Controller 2 IP Address.
- Enter a Shared Controller IP Address.

  This is the address that will be dialed by incoming calls (including Legacy callers).
- Enter a notification email address.

  Enter the email address you want to receive notifications in the event of a system failure.

6. Click **Save and Reboot**.

- Any modifications you make to your Clusters accrue until you click **Save and Reboot**, and then all of your Cluster changes are applied to your VidyoGateway server.
- When you click **Save and Reboot**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Reboot

All active conference calls will be dropped and the server will reboot. Are you sure you want to continue?

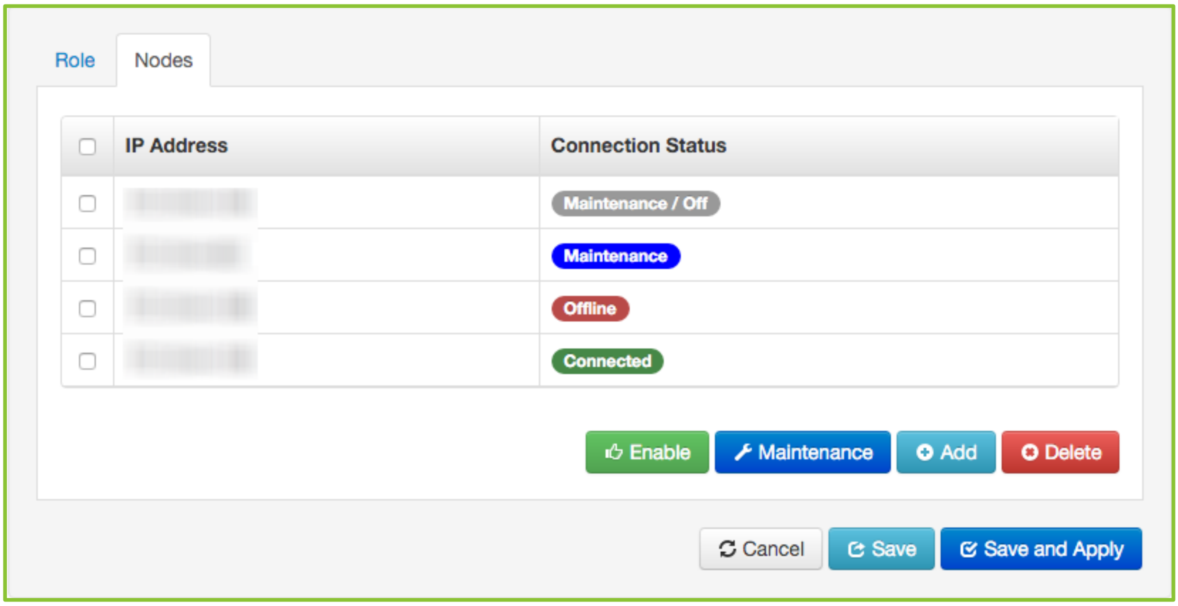
Configuring Nodes for the Active Controller in Cluster Mode

You have to manually add any nodes other than the Active Controller since it will automatically be added to the *Nodes* page after reboot.

Note The *Nodes* subtab is only visible when accessing the VidyoGateway Admin Pages for the Active Contoller.

The node may display as follows depending on its current connection status:

Connection Status	Color	Description
Maintenance / Off	Gray	Node is in maintenance mode and not registered with the controller
Maintenance	Blue	Node is in maintenance mode and still registered to the controller
Offline	Red	Node is not registered with the controller and not in maintenance mode
Connected	Green	Node is accepting calls



□	IP Address	Connection Status
□		Maintenance / Off
□		Maintenance
□		Offline
□		Connected

To configure nodes for the active controller in cluster mode:

1. Log in to the Admin portal using your System Console account.

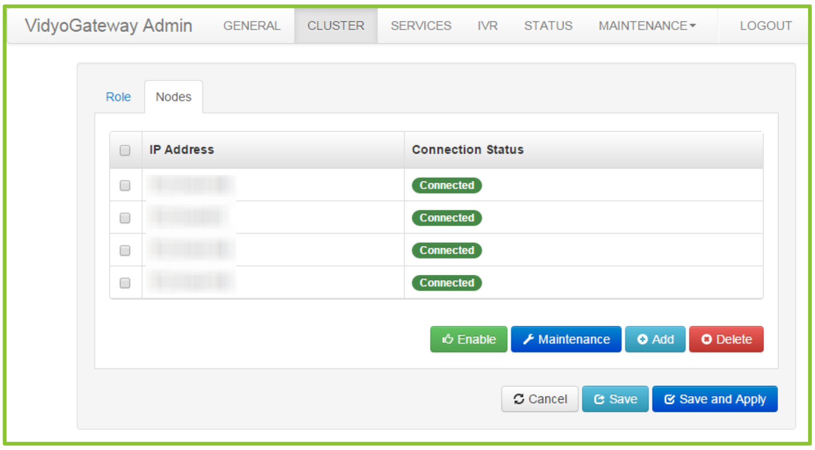
   For more information, see Logging in to the Admin Portal.

The *GENERAL > VidyoPortal* page displays by default.

2. Click the *CLUSTER* tab.

   The *CLUSTER > Role* page displays by default.

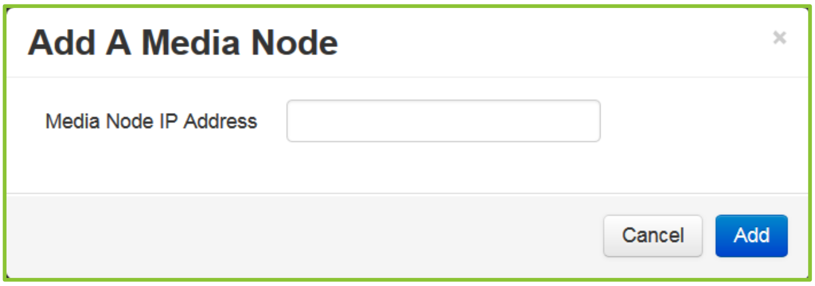
3. Click the *Nodes* subtab.



□	IP Address	Connection Status
□	[redacted]	Connected
□	[redacted]	Connected
□	[redacted]	Connected
□	[redacted]	Connected

4. Click **Add**.

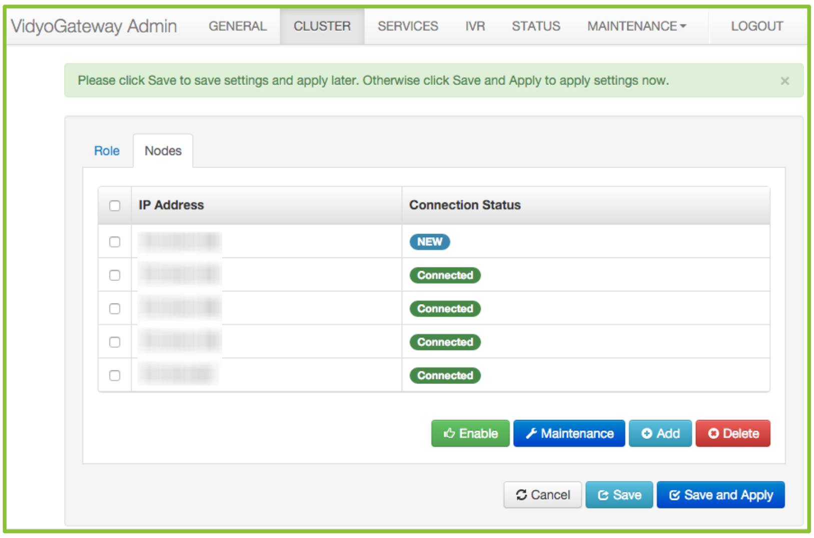
   The *Add A Media Node* pop-up displays.



5. Enter the **Media Node IP Address**.

6. Click **Add**.

The new Media Node IP Address is added to the *Nodes* page with a connection status of “NEW.”



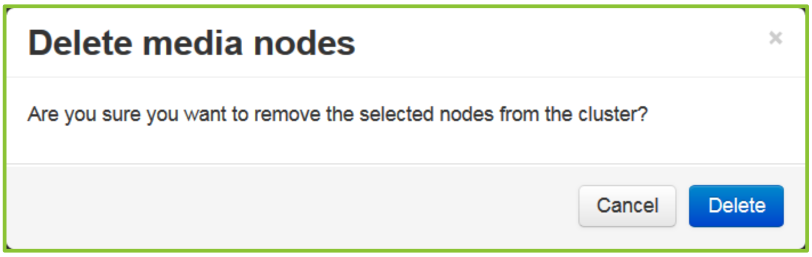
Please click Save to save settings and apply later. Otherwise click Save and Apply to apply settings now.

□	IP Address	Connection Status
□	[redacted]	NEW
□	[redacted]	Connected
□	[redacted]	Connected
□	[redacted]	Connected
□	[redacted]	Connected

Note To delete the media node IP Address, select the checkbox to the left of the IP Address column and click **Delete**.

A *Confirmation* pop-up displays.

Click **Delete**.



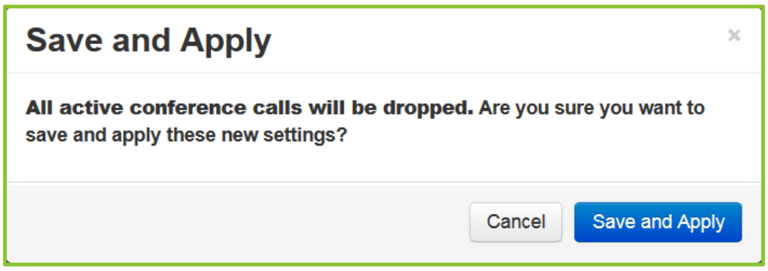
Delete media nodes

Are you sure you want to remove the selected nodes from the cluster?

7. Click **Save and Apply**.

- Any modifications you make to this page accrue until you click **Save and Apply**, and then all of your changes are applied to your VidyoGateway server.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new settings?

The node's connection status changes to "Connected" if the media node is currently running. Otherwise, it will change to "offline" if the media node is currently down.

Placing VidyoGatway Cluster Nodes in Maintenance Mode

When VidyoGateway cluster nodes are placed in maintenance mode, existing calls remain connected but new calls are not received. Only VidyoGateway cluster nodes that are online can be placed in maintenance mode.

Note When a node that has a status connection of offline, maintenance, or maintenance/off is selected and the **Maintenance** button is clicked, an error message displays stating "Only Online nodes may be put into Maintenance node".

To place VidyoGateway cluster nodes in maintenance mode:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

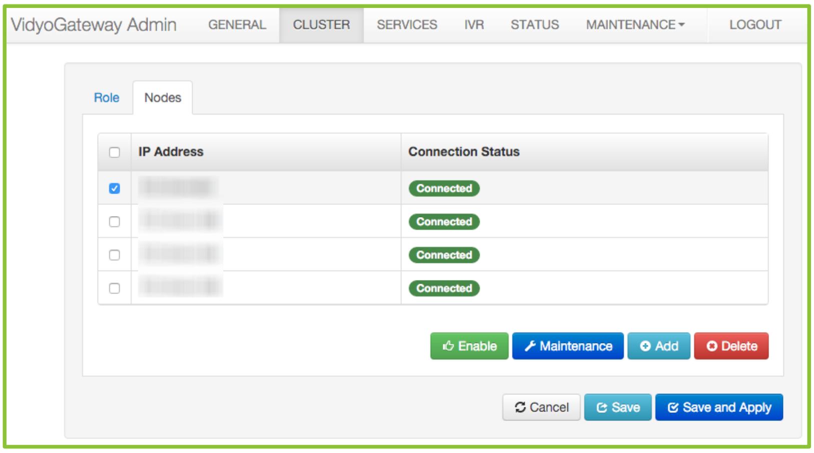
2. Click the *CLUSTER* tab.

   The *CLUSTER > Role* page displays by default.

3. Click the *Nodes* subtab.

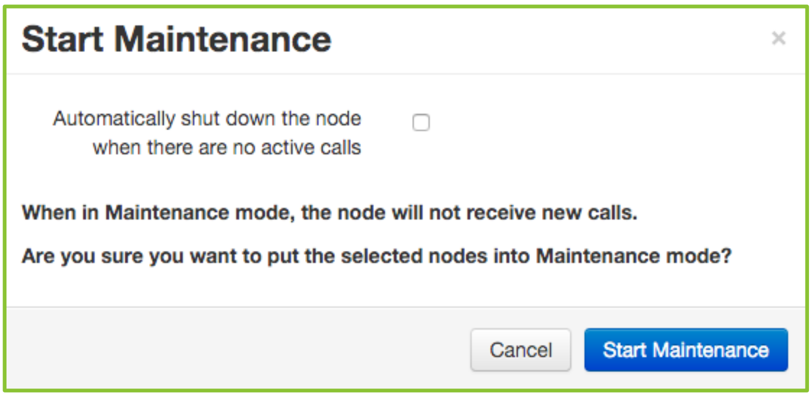
4. Select the checkbox for the appropriate node.

5. Click **Maintenance**.



☐	IP Address	Connection Status
☑	[redacted]	Connected
☐	[redacted]	Connected
☐	[redacted]	Connected
☐	[redacted]	Connected

The *Start Maintenance* pop-up displays.



Start Maintenance

Automatically shut down the node when there are no active calls ☐

When in Maintenance mode, the node will not receive new calls.

Are you sure you want to put the selected nodes into Maintenance mode?

6. Select the **Automatically shutdown the node when there are no active calls** checkbox if necessary.

Note Only Virtual Edition appliances will be automatically shut down. Physical appliances will ignore this command.

7. Click **Start Maintenance**.

   The node’s connection status changes to “Maintenance.”

Enabling VidyoGateway Cluster Nodes

Only VidyoGateway clusters that are in matenance mode can be enabled.

Note When a node that has a connection status of offline, online, or maintenance/off is selected and the **Enable** button is clicked, an error message displays stating “Only nodes in Maintenance mode may be Enabled.”

To place VidyoGateway cluster nodes in maintenance mode:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *CLUSTER* tab.

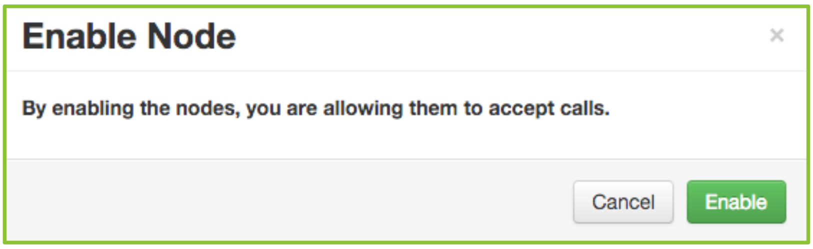
   The *CLUSTER > Role* page displays by default.

3. Click the *Nodes* subtab.

4. Select the checkbox for the appropriate node.

5. Click **Enable**.

   The *Enable Node* pop-up displays.



Enable Node

By enabling the nodes, you are allowing them to accept calls.

6. Click **Enable**.

   The node's connection status changes back to "Connected."

Configuring Controller 2

- Before configuring clusters, be sure to review Understanding the Clustering Procedure.
- When using VidyoGateway version 3.2 and later, your Services automatically propagate from your Active Controller to the Standby Controller and Cluster Nodes. Therefore, the *Services* tab does not display when accessed from your Standby Controller. To make configurations on the tabs, you must access them from your Active Controller. In addition, the fields on the *General > VidyoPortal, SIP, and H.323* subtabs are automatically populated from Controller 1. Please note that these fields will be greyed out since they are not configurable on the Standby Controller.
- If you choose to enable IVR on your Active Controller, you must also enable it on your Standby Controller and all of the Cluster Nodes.

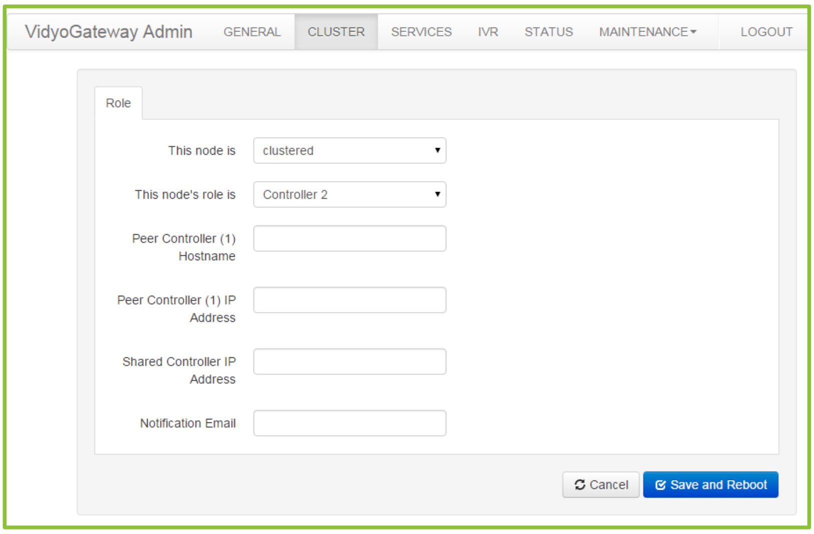
To configure Controller 2:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *CLUSTER* tab.
3. Select **clustered** from the **Mode** drop-down.
4. Select **Controller 2** from the **Role** drop-down.



This node is	clustered
This node's role is	Controller 2
Peer Controller (1) Hostname	
Peer Controller (1) IP Address	
Shared Controller IP Address	
Notification Email	

5. Configure Controller 2 as follows:
   - Enter a Controller 1 Hostname.

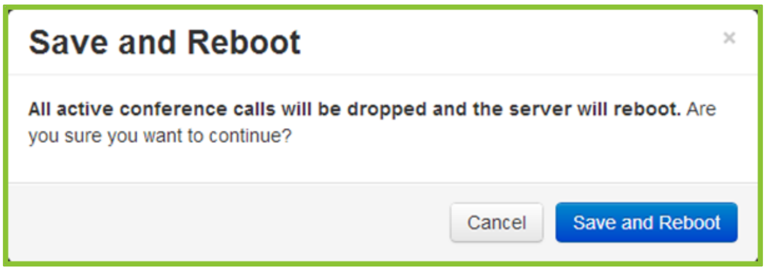
     Provide the Hostname exactly as it's shown in System Console Option 1. Do not provide an FQDN as the Peer Host Name.

     For information, see Viewing Application and System Information.
   - Enter a Controller 1 IP Address.
   - Enter a Shared Controller IP Address. This is the address Legacy callers will use.
   - Enter a notification email address.

     Enter the email address you want to receive notifications in the event of a system failure.

     Before clicking **Save and Reboot**, please ensure that Controller 1 is reachable from Controller 2.
6. Click **Save and Reboot**.
   - Any modifications you make to your Clusters accrue until you click **Save and Reboot**, and then all of your Cluster changes are applied to your VidyoGateway server.

- When you click **Save and Reboot**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Reboot

All active conference calls will be dropped and the server will reboot. Are you sure you want to continue?

Configuring Your Cluster Node

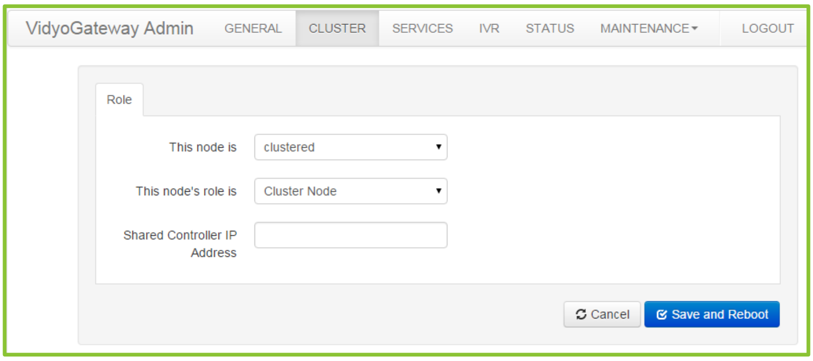
- Before configuring clusters, be sure to review Understanding the Clustering Procedure.
- When using VidyoGateway version 3.2 and later, your services and VidyoPortal, SIP, H.323 configurations automatically propagate from your Active Controller to the Cluster Nodes. Therefore, the *Services* tab as well as the *VidyoPortal*, *SIP*, *H.323* tabs (under General) do not display when accessed from your Cluster Node servers. To make configurations on the tabs, you must access them from your Active Controller.
- If you choose to enable IVR on your Active Controller, you must also enable it on your Standby Controller and all of the Cluster Nodes.

To configure your Cluster Node:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.
2. Click the *CLUSTER* tab.
3. Select **clustered** from the **Mode** drop-down.
4. Select **Cluster Node** from the **Role** drop-down.



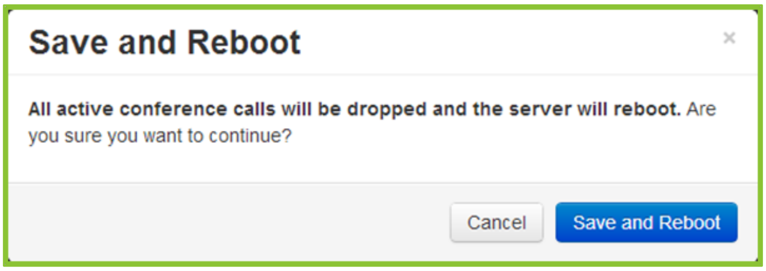
This node is: clustered

This node's role is: Cluster Node

Shared Controller IP Address:

5. Enter a **Shared Controller IP Address**.

6. Click **Save and Reboot**.
   - Any modifications you make to your Clusters accrue until you click **Save and Reboot**, and then all of your Cluster changes are applied to your VidyoGateway server.
   - When you click **Save and Reboot**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Reboot

All active conference calls will be dropped and the server will reboot. Are you sure you want to continue?

Managing Services

The *SERVICES* tab allows you to manage and configure prefixes for various call types both from and to Legacy devices.

Note At least one service with From Legacy as the Direction must be set as the default in order to use IVR. For more information about the Default service setting, see Adding a Service.

VidyoGateway services specify the type of call, the direction (to and from), and specific profile details. Prefixes are used when creating a dialing plan (if required) or when isolating a call through a specific VidyoGateway is necessary.

The VidyoGateway comes with preconfigured services for a variety of protocols. These defaults allow you to dial without specifying any prepending digits when sending or receiving calls from Legacy devices. You can modify these services or add new ones. For some service examples, see Example Configurations.

- When clustering your VidyoGateways, your Services are centralized; meaning, the ones configured on your Active controller are used on all servers in your cluster. For more information about Clustering, see Understanding VidyoGateway Clusters.
- For information about specific call types and services, see Understanding Call Types and Service Examples.

Adding a Service

When adding or editing a service for audio-only calls, the administrator can choose an audio codec to be used during calls. However, when adding or editing a service for video calls, the audio codec is negotiated as part of the call setup.

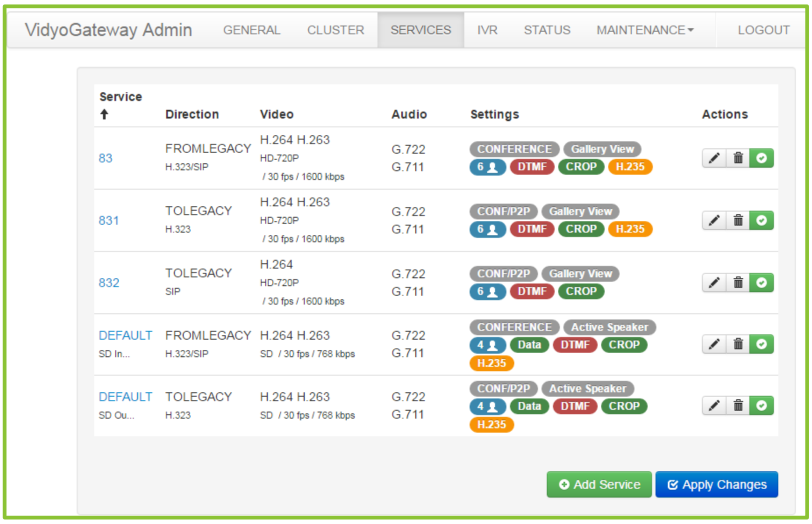
To add a service:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

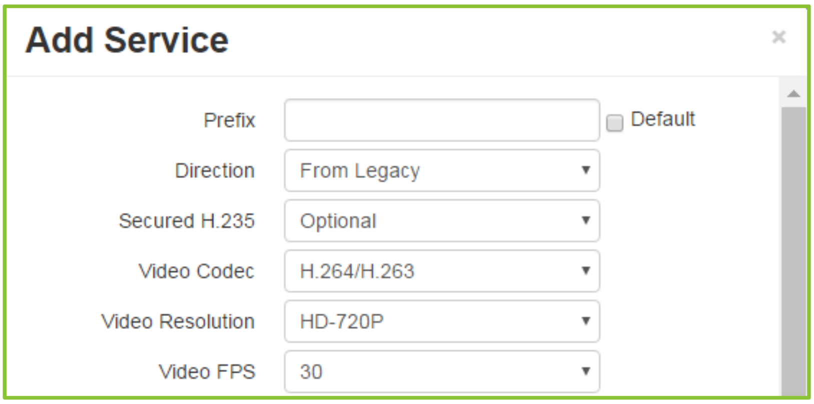
2. Click the *SERVICES* tab.



Service ↑	Direction	Video	Audio	Settings	Actions
83	FROMLEGACY H.323/SIP	H.264 H.263 HD-720P / 30 fps / 1600 kbps	G.722 G.711	CONFERENCE Gallery View 6 👤 DTMF CROP H.235	✎ 🗑 ✓
831	TOLEGACY H.323	H.264 H.263 HD-720P / 30 fps / 1600 kbps	G.722 G.711	CONF/P2P Gallery View 6 👤 DTMF CROP H.235	✎ 🗑 ✓
832	TOLEGACY SIP	H.264 HD-720P / 30 fps / 1600 kbps	G.722 G.711	CONF/P2P Gallery View 6 👤 DTMF CROP	✎ 🗑 ✓
DEFAULT SD In...	FROMLEGACY H.323/SIP	H.264 H.263 SD / 30 fps / 768 kbps	G.722 G.711	CONFERENCE Active Speaker 4 👤 Data DTMF CROP H.235	✎ 🗑 ✓
DEFAULT SD Ou...	TOLEGACY H.323	H.264 H.263 SD / 30 fps / 768 kbps	G.722 G.711	CONF/P2P Active Speaker 4 👤 Data DTMF CROP H.235	✎ 🗑 ✓

3. Click **Add Service**.

   The *Add Service* pop-up displays.



Add Service

Prefix		□ Default
Direction	From Legacy ▾	
Secured H.235	Optional ▾	
Video Codec	H.264/H.263 ▾	
Video Resolution	HD-720P ▾	
Video FPS	30 ▾	

4. Enter configuration settings for your new service. Available choices include the following:

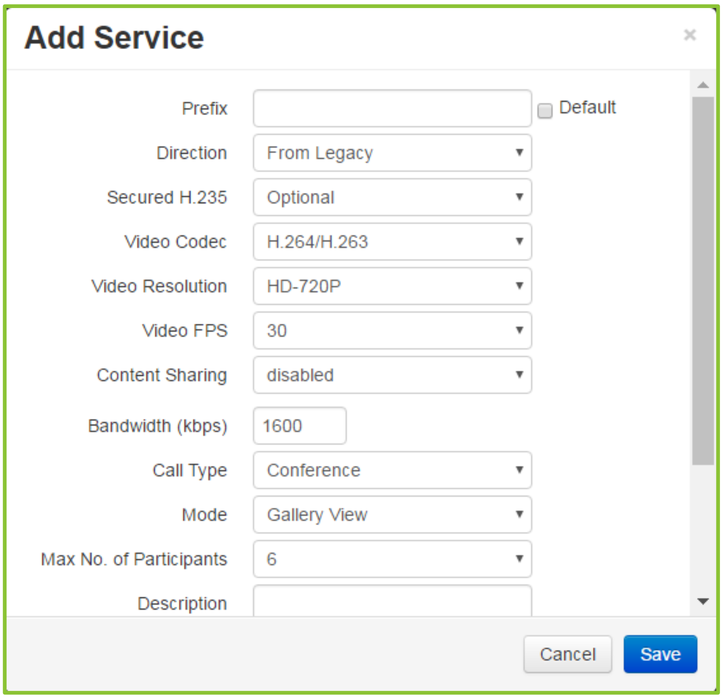
   a. Enter a numeric prefix for your configuration in the **Prefix** field.

   b. Select the **Default** checkbox to not require a dialing prefix when a user dials from a Legacy endpoint.

      At least one service with **From Legacy** as the direction must be set as the default in order to use IVR. For more information, see Enabling Your IVR Settings.

c. Select a call direction from the **Direction** drop-down for your prefix configuration as either **From** or **To Legacy**.

- If you select **To Legacy** from the **Direction** drop-down, the **Call Type** field becomes read-only with **Conference/P2P** selected.



Add Service

Prefix	□ Default
Direction	From Legacy
Secured H.235	Optional
Video Codec	H.264/H.263
Video Resolution	HD-720P
Video FPS	30
Content Sharing	disabled
Bandwidth (kbps)	1600
Call Type	Conference
Mode	Gallery View
Max No. of Participants	6
Description	

- If you select **From Legacy** from the **Direction** drop-down, you must select either **Conference** or **P2P** from the **Call Type** drop-down.

d. Select one of the following security options from the **Secured H.235** drop-down:

- Select **No** to not have your H.235 transmissions secured.
- Select **Optional** to have H.235 calls secured between your VidyoGateway and Legacy devices that support encryption for the protocol.
- Select **Required** to have H.235 calls secured between VidyoGateway and Legacy devices at all times (regardless of Legacy endpoint support for encryption for the protocol).

  If Legacy endpoint calls are set to **Required**, your VidyoPortal must be running the Vidyo encryption software option for a successful connection.

e. Select **Voice Only**, **H.264**, **H.263**, **H.264/H.263**, or **H263/H.264** as your video codec from the **Video Codec** drop-down.

When you select **Voice Only**, the **Bandwidth** field becomes read-only and the **Resolution** and **FPS** drop-downs disappear from the *Add Service* pop-up.

f. Select **CIF**, **SD**, **HD-720P**, or **FHD-1080P** as your resolution from the **Video Resolution** drop-down.

The setting determines the maximum resolution used for your service.

To determine the maximum number of concurrent calls of the same type and resolution for your VidyoGateway server, see Maximum Number Concurrent Calls of the Same Type. For example, you should select **HD1080 only** if you have a VidyoGateway XL and for not more than two concurrent calls. (Not applicable for audio-only calls.)

- When you select a Resolution value, the Bandwidth is changed accordingly in the following manner: CIF = 384 kbps, SD = 768 kbps, HD-720P = 1600 kbps, and FHD-1080P = 3072 kbps.
- If you select the **Voice Only** option as your Video Codec, the Resolution is fixed at 64 kbps.
- Although you must select a Resolution when you configure your service, the system dynamically negotiates both the bandwidth and resolution according to the Legacy device. VidyoGateway does not negotiate higher than the configured resolution.

g. Select **5, 10, 15, 20, 25**, or **30** from the **Video FPS** drop-down as your frames per second.

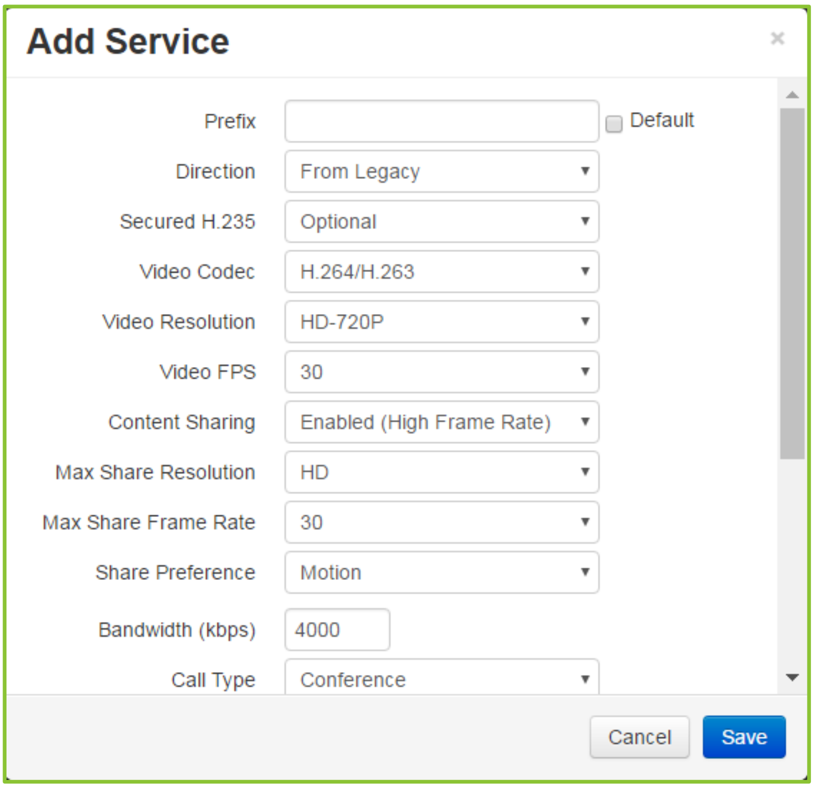
h. Select one of the following options from the **Content Sharing** drop-down:

- **Disabled** to disable support for the BFCP and H.239 protocols, as well as content sharing between H.323 and SIP devices.
- **Enabled** to enable support for the BFCP and H.239 protocols, as well as content sharing between H.323 and SIP devices.
- **Enabled (High Frame Rate)**

Note When **Enabled (High Frame Rate)** is selected, the default bandwidth is set to 4,000 kbps. The administrator can set the bandwidth higher than 4,000 kbps for HD content sharing if necessary.

The **Enabled (High Frame Rate)** option enables support for the BFCP and H.239 protocols. This allows content sharing between H.323 and SIP devices, along with the ability to configure bandwidth allocation between the main video and content share.

The following drop-downs display in the *Add Service* pop-up upon selecting the **Enabled (High Frame Rate)** option from the **Content Sharing** drop-down:



Add Service

Prefix	□ Default
Direction	From Legacy
Secured H.235	Optional
Video Codec	H.264/H.263
Video Resolution	HD-720P
Video FPS	30
Content Sharing	Enabled (High Frame Rate)
Max Share Resolution	HD
Max Share Frame Rate	30
Share Preference	Motion
Bandwidth (kbps)	4000
Call Type	Conference

- Select **1080HD**, **HD**, **SD**, or **CIF** from the **Max Share Resolution** drop-down as the max content share resolution.
- Select **30**, **25**, **20**, **15**, or **10** from the **Max Share Frame Rate** drop-down as the max content share frame rate.
- Select **Motion** or **Sharpness** from the **Share Preference** drop-down.

  When **Motion** is selected, the video resolution is reduced at a higher frame rate.

  When **Sharpness** is selected, the video resolution increases at a lower frame rate.

i. Enter a numeric value (in kbps) in the **Bandwidth (kbps)** field for the maximum bandwidth available for your service.

- The number that displays in this field is based on the Resolution selected in the following manner: 384 kbps = CIF, 768 kbps = SD, 1600 kbps = HD-720P, and 3072 kbps = FHD 1080P.
- If you select the **Voice Only** option as your Video Codec, the Resolution is fixed at 64 kbps.

j. Select **P2P** (Point to Point, from Legacy only) or **Conference** (to Legacy) from the **Call Type** drop-down as your audio codec.

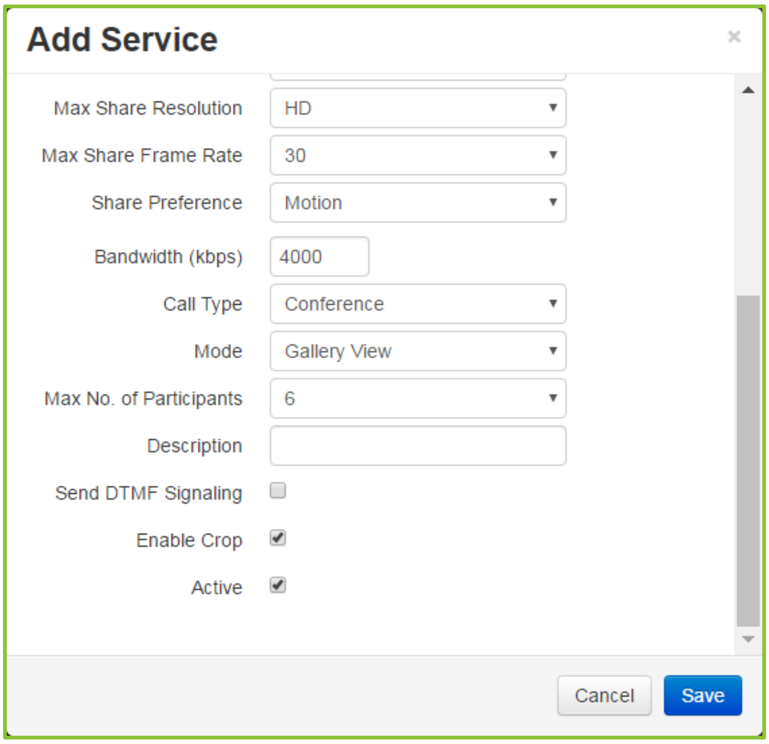
This field only displays when **From Legacy** is selected in the **Direction** field. If **To Legacy** is selected as the direction, the field is fixed as **Conference/P2P**.

k. Select from the following from the **Mode** drop-down:

- □ Select **Gallery View** to display participants in a filmstrip-type layout.
- □ Select **Active Speaker** to display the most recent speaker in a larger window than other users.
- □ Select **Continuous Presence** to display all participants in equal-sized windows.

l. Select **1**, **2**, **3**, **4**, **5**, **6**, **7**, or **8** from the **Max No. of Participants** drop-down as your specified maximum number of participants to be shown.

m. Enter a service name in the **Description** field for your configuration.



Add Service

Max Share Resolution	HD
Max Share Frame Rate	30
Share Preference	Motion
Bandwidth (kbps)	4000
Call Type	Conference
Mode	Gallery View
Max No. of Participants	6
Description	
Send DTMF Signaling	□
Enable Crop	☑
Active	☑

n. Select the **Send DTMF Signaling** checkbox to send DTMF tones per RFC 4733/2833 for SIP and via signaling for H.323.

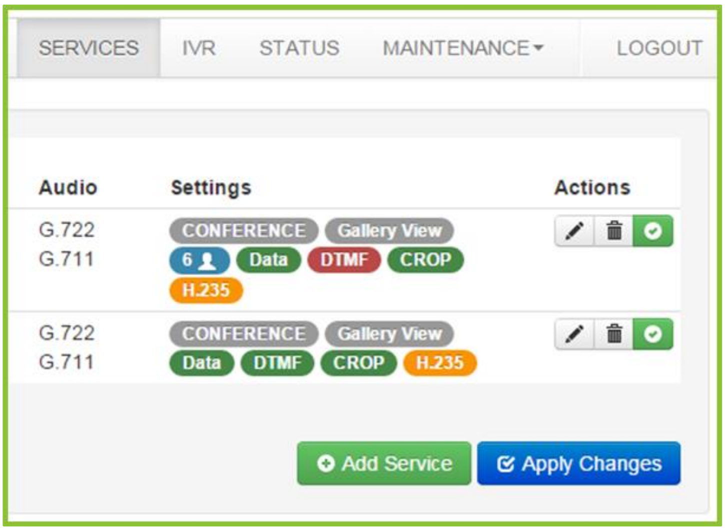
If you do not select the **Send DTMF Signaling** checkbox, DTMF tones will be sent via the media stream.

o. Select the **Enable Crop** checkbox to show 16:9 video formatted for a 4:3 display (full-screen).

Do not select the checkbox to show 16:9 video letterboxed on a 4:3 display.

p. Select the **Active** checkbox to make your service and all of its settings available for use on your system.

- Do not select the checkbox if you do not want to make your service and all of its settings available for use on your system.
- You can also click the corresponding checkbox to the right of the list of services to activate and deactivate services from the *Service* tab.



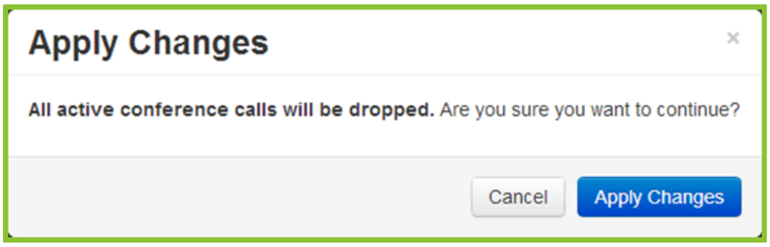
Audio	Settings	Actions
G.722 G.711	CONFERENCE Gallery View 6 Data DTMF CROP H.235	
G.722 G.711	CONFERENCE Gallery View Data DTMF CROP H.235	

5. Click **Save** in the *Add Service* pop-up.

   If desired, you can also select the **Edit**, **Delete**, **Activate**, or **Deactivate** buttons on the *Services* tab.

6. Click **Apply Changes** on the *Services* page if desired.

   - Any services you edit, delete, activate, and deactivate accrue until you click **Apply Changes**, and then all of your Service changes are applied to your VidyoGateway server.
   - When clicked, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



All active conference calls will be dropped. Are you sure you want to continue?

Activating and Deactivating Services

You can also activate or deactivate a service by selecting or clearing the **Active** checkbox from its corresponding *Add or Edit Service* pop-up. For more information, see Adding a Service.

To activate or deactivate a service:

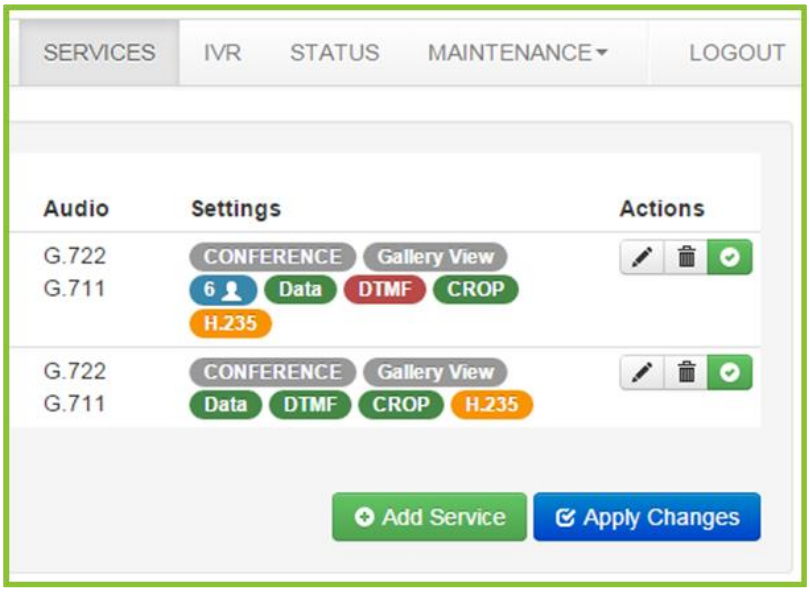
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *SERVICES* tab.

3. Click the corresponding **Check Mark** button to the right of the list of services to activate or deactivate a service.

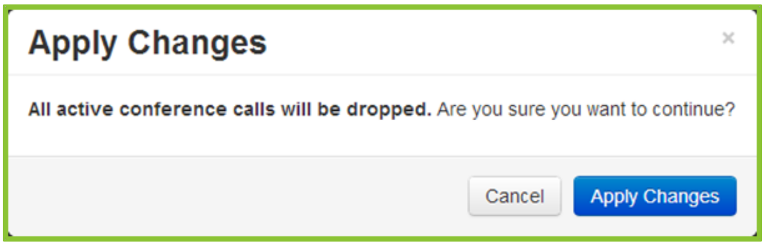


Audio	Settings	Actions
G.722 G.711	CONFERENCE Gallery View 6 Data DTMF CROP H.235	✎ 🗑 ✓
G.722 G.711	CONFERENCE Gallery View Data DTMF CROP H.235	✎ 🗑 ✓

   If desired, you can also select the **Edit** or **Delete** buttons.

4. Click **Apply Changes** on the *Services* tab if desired.

   - Any services you edit, delete, activate, and deactivate accrue until you click **Apply Changes**, and then all of your Service changes are applied to your VidyoGateway server.
   - When clicked, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



All active conference calls will be dropped. Are you sure you want to continue?

Deleting a Service

If you permanently delete a service from your system, it cannot be undone.

To delete a service:

1. Log in to the Admin portal using your System Console account.

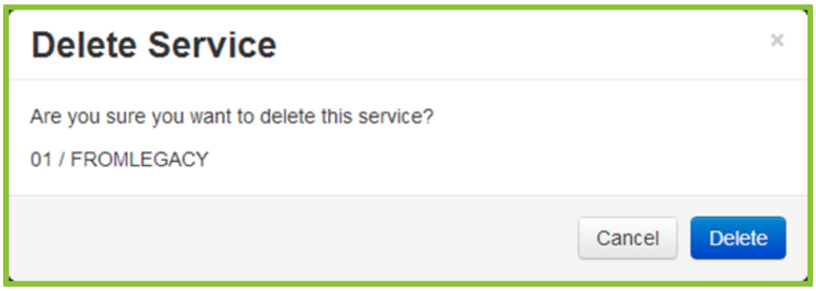
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *SERVICES* tab.

3. Click the corresponding **Delete** icon to the right of the list of services to delete a service.

   The *Delete Service* pop-up displays.



Delete Service

Are you sure you want to delete this service?

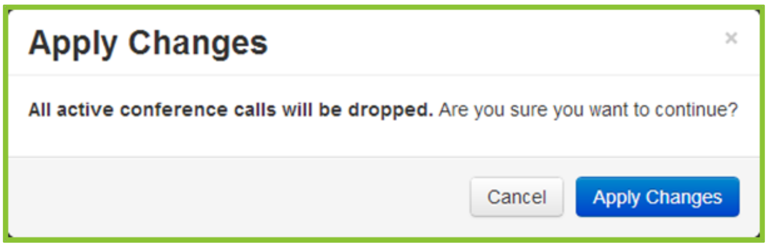
01 / FROMLEGACY

4. Click **Delete**.

   If desired, you can also select the **Edit**, **Activate**, and **Deactivate** buttons.

5. Click **Apply Changes** on the *Services* tab if desired.

   - Any services you edit, delete, activate, and deactivate accrue until you click **Apply Changes**, and then all of your service changes are applied to your VidyoGateway server.
   - When clicked, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Apply Changes

All active conference calls will be dropped. Are you sure you want to continue?

Editing a Service

To edit a service:

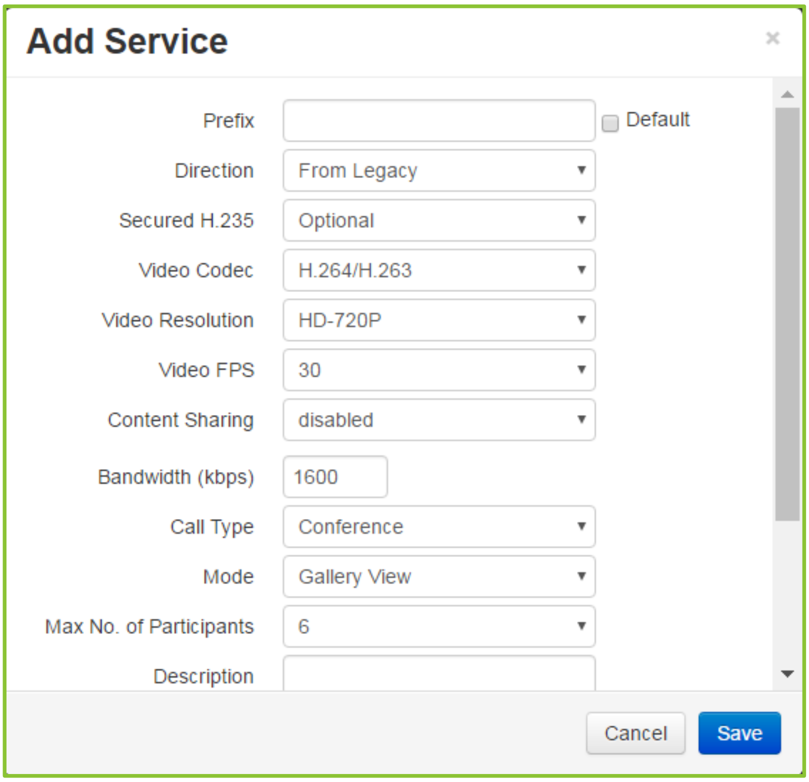
1. Log in to the Admin portal using your System Console account.

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

The *GENERAL > VidyoPortal* page displays by default.

2. Click the *SERVICES* tab.
3. Click the corresponding **Edit** icon to the right of the list of services to edit a service.

   The *Edit Service* pop-up displays.



Add Service

Prefix	☐ Default
Direction	From Legacy
Secured H.235	Optional
Video Codec	H.264/H.263
Video Resolution	HD-720P
Video FPS	30
Content Sharing	disabled
Bandwidth (kbps)	1600
Call Type	Conference
Mode	Gallery View
Max No. of Participants	6
Description	

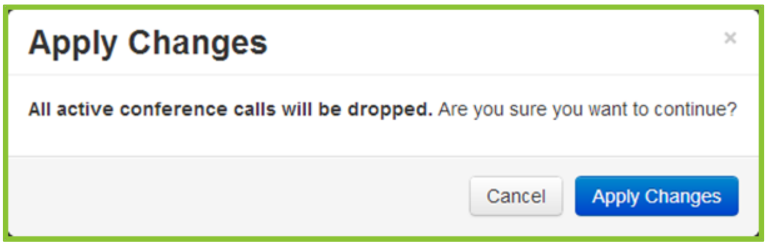
4. Modify your service as desired.

   For more information, see Adding a Service.
5. Click **Save** in the *Edit Service* pop-up.

   If desired, you can also select the **Delete**, **Activate**, and **Deactivate** buttons.
6. Click **Apply Changes** on the *Services* tab if desired.

   - Any services you edit, delete, activate, and deactivate accrue until you click **Apply Changes**, and then all of your Service changes are applied to your VidyoGateway server.

- When clicked, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Apply Changes

All active conference calls will be dropped. Are you sure you want to continue?

Understanding Call Types and Service Examples

The following call types and service examples are provided your reference. They include examples for H.323, SIP, Incoming URI Dialing, Legacy H.323, and TCS4 Delimiters.

Note The dialing examples mention service prefixes. Services enable the creation of default prefixes; meaning, when a given service is selected, the default prefix set for the service is used without having to include it when dialing through VidyoGateway. For more information, see Managing Services.

H.323 Outgoing Call Examples

Note All outgoing H.323 calls are P2P connections if dialed from a Vidyo user's homepage. For conferences or multipoint connections, you must be added via invitation from the Control Meeting or Admin Page functions.

- An outgoing VidyoGateway call (with a gatekeeper) to a Legacy H.323 endpoint:

  [VidyoGateway Outgoing service prefix] + [H.323 endpoint extension]

  Example: 039001

- An outgoing VidyoGateway call (with a gatekeeper) to an MCU/bridge conference endpoint:

  [VidyoGateway Outgoing service prefix] + [MCU conference ID]

  Example: 034001

- An outgoing VidyoGateway call (without a gatekeeper) to a Legacy H.323 endpoint:

  [VidyoGateway Outgoing service prefix] + [IP Address of H.323 system]

  Example: 03192.167.1.2

- An outgoing VidyoGateway call (without a gatekeeper) to an MCU/bridge conference endpoint:

  [VidyoGateway Outgoing service prefix] + [MCU conf ID]@[IP Address of MCU]

  Example: 032001@192.168.1.2

In this example, utilize H.323 URL dialing (Annex 0) to directly dial into an MCU conference.

H.323 Incoming Call Examples

Service prefixes can be used to set all of your incoming calls as either P2P or Conference, as desired. For more information, see Managing Services.

- **An incoming VidyoGateway call (with a gatekeeper) from a Legacy H.323 endpoint:**

  [VidyoGateway Incoming service prefix] + [Vidyo extension]

  Example: 035001

- **An incoming VidyoGateway call (without a gatekeeper) from a Codian MCU endpoint**:

  [VidyoGateway IP Address]![VidyoGateway incoming service prefix] + [Vidyo username or extension]

  Example: 192.168.1.110!035001

- **An incoming VidyoGateway call (without a gatekeeper) from a Legacy H.323 endpoint**:

  [VidyoGateway IP Address] + [TCS4 delimiter] + [VidyoGateway incoming service prefix] + [Vidyo extension]

  Example: 192.168.1.110##035001

Note This particular example is for Polycom and Lifesize endpoints using ## as the TCS4 delimiter. For additional delimiter examples, see TCS4 Delimiters.

- **An incoming VidyoGateway call (without a gatekeeper) from a Tandberg/Cisco H.323 endpoint**:

  [VidyoGateway service prefix] + [Vidyo extension]@[VidyoGateway IP Address]

  Example: 035001@192.168.1.110

Note Some Tandberg/Cisco endpoints (such as the C series) require h323: in front of the dial string. If the Tandberg/Cisco does not accept the call with the h323: starting the dial string, check your endpoint to ensure H.323 settings are enabled. Use the Tandberg/Cisco web UI to make settings as the handheld remote is rather cumbersome.

Example: h323: [VidyoGateway service prefix] + [Vidyo extension]@[VidyoGateway IP Address]

SIP Incoming Call Using a Prefix Example

Service prefixes can be used to set all of your incoming calls as either P2P or Conference, as desired. For more information, see Managing Services.

- **An incoming VidyoGateway call from a Legacy SIP endpoint**:

  [VidyoGateway Incoming service prefix] + [Vidyo username or extension]@[VidyoGateway IP Address]

  Example: 075001@192.168.1.11

SIP Incoming URI Dialing Example

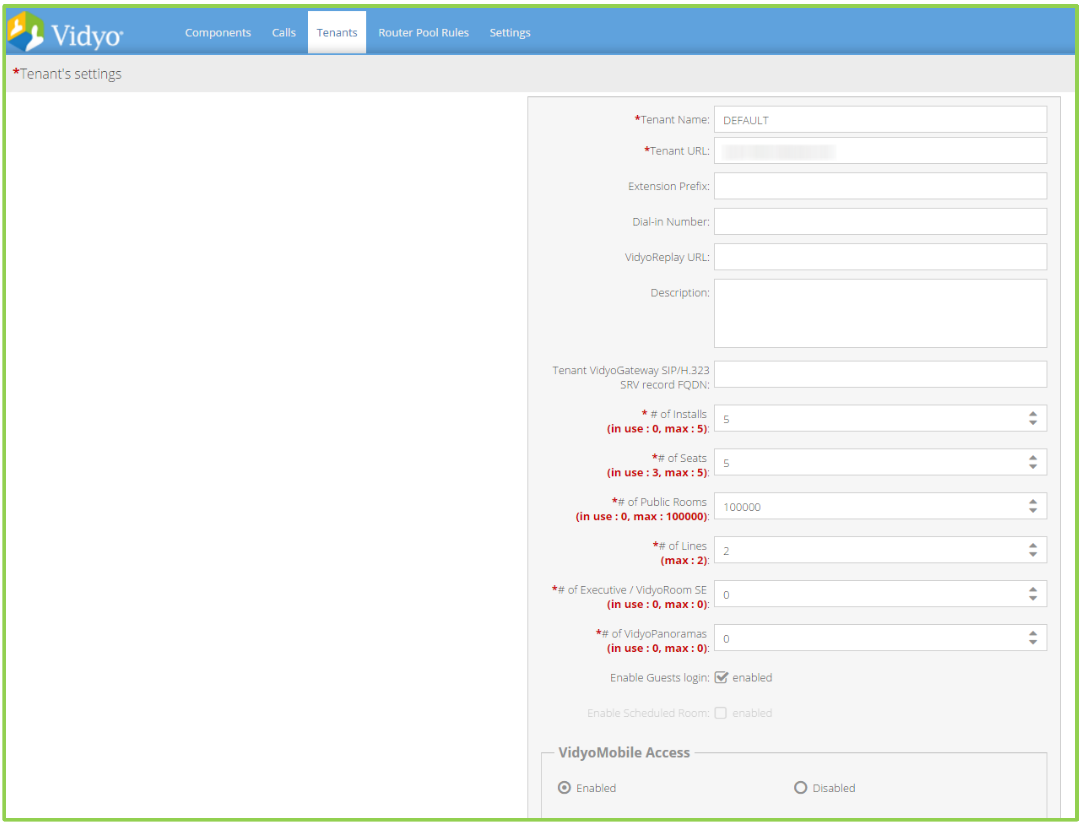
[`jsmith@examplecompany.com`]

Where jsmith is Member of the tenant named “tenant1.”

Note The SIP SRV record FQDN must be configured as **[`examplecompany.com`]** and it must be configured by your network administrator to point to the VidyoGateway IP address (Standalone or Cluster).

For more information, refer to your Legacy equipment documentation.

For multi-tenant systems, you must associate **[`examplecompany.com`]** to Tenant1. To do this, configure the **Tenant VidyoGateway SIP/H.323 SRV record FQDN** field to your **[`examplecompany.com`]** FQDN in the Super portal as part of the “tenant1” configuration.



*Tenant's settings

*Tenant Name: DEFAULT

*Tenant URL: [redacted]

Extension Prefix:

Dial-in Number:

VidyoReplay URL:

Description:

Tenant VidyoGateway SIP/H.323 SRV record FQDN:

* # of Installs (in use : 0, max : 5): 5

*# of Seats (in use : 3, max : 5): 5

*# of Public Rooms (in use : 0, max : 100000): 100000

*# of Lines (max : 2): 2

*# of Executive / VidyoRoom SE (in use : 0, max : 0): 0

*# of VidyoPanoramas (in use : 0, max : 0): 0

Enable Guests login: ☑ enabled

Enable Scheduled Room: □ enabled

VidyoMobile Access

● Enabled ○ Disabled

For more information, refer to the “Managing Tenants as the Super Admin” section in the *VidyoConferencing Administrator Guide*.

For more information about SIP URI configuration, see Configuring the VidyoPortal Settings.

Dialing from a Legacy H.323 Endpoint into a Vidyo PIN-Protected Room

[VidyoGateway IP Address] + [TCS4 delimiter] + [VidyoGateway service prefix] + [Vidyo extension] + [VidyoGateway PIN delimiter] + [Vidyo Users Room PIN]

Example: 192.168.1.110##035001*1234 (This is a Polycom Lifesize call string coming into a Vidyo PIN protected room.)

Note The VidyoGateway PIN delimiter can be set on the VidyoGateway *Configuration* page. The default is an asterisk *.

TCS4 Delimiters

The following are examples of TCS4 delimiters for various endpoints.

- **Polycom and Lifesize endpoints use ##**:

  Example: 192.168.1.110##035001

- **Polycom PVX v.8.0.4 uses @**:

  Example: 035001@192.168.1.110

- **Sony uses #**:

  Example: 192.168.1.110#035001

- **Tandberg/Cisco does not support TCS4 delimiters, but uses @ as an inverted format URL (Annex 0) style**:

  Examples: 035001@192.168.1.110, h323:35001@192.168.1.110

Note Tandberg C releases TC4.1.2 or later accepts the name@domain or name@IPAddress dialing formats without being registered to a gatekeeper.

- **Tandberg 2500 vB3.9 and Tandberg MCU 8+8 endpoints use ,**:

  Examples: 192.168.1.110,035001

- **Codian MCI uses !**:

  Example: 192.168.1.110!035001

Configuring Integrated Voice Response (IVR) Settings

IVR is not available if Video Loopback is enabled. For more information, see Configuring Video Loopback Settings.

When you dial into VidyoGateway from a Legacy device, a system of menus complete with text and voice prompts guide you through the IVR interfaces. You can configure these IVR interfaces using settings for Parameters, Prompts, and Import/Export IVR Media and Prompt Settings on the corresponding tabs.

The following DTMF Modes are supported by Vidyo's IVR functions:

- H.245 signal (tone) outband
- H.245 alphanumeric (string) outband
- RFC2833 (SIP Signaling with RTP payload)
- PCM waveform inband

IVR Prompts are initially disabled when your VidyoGateway comes from the factory.

Enabling Your IVR Settings

At least one service with From Legacy as the Direction must be set as the default in order to use IVR. For more information about the Default service setting, see Adding a Service.

If you are clustering your VidyoGateways, and choose to enable IVR, you must enable it on your Active Controller, Standby Controller, and all of your Cluster Nodes. Moreover, if you choose to customize the IVR settings, you must configure those on all of the VidyoGateway servers in the cluster (Active Controller, Standby Controller, Cluster Nodes). For more information about clusters, see Understanding VidyoGateway Clusters.

To enable your IVR settings:

1. Log in to the Admin portal using your System Console account.

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

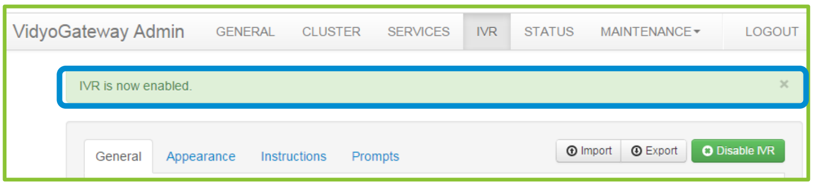
   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *IVR* tab.

   The *IVR > General* page displays by default.

3. Click **Enable IVR** after making all your desired settings on the *General*, *Appearance*, *Instructions*, and *Prompts* subtabs.

When clicked, a system notification indicates the IVR is now enabled (or disabled).



IVR is now enabled.

Note The feature toggles between enable and disable states.

The **Enable IVR** button is shown along with **Import** and **Export** buttons on the upper-right of the *IVR* tab. For more information, see Importing and Exporting VidyoGateway IVR Media and Prompt Settings.

Configuring General IVR Settings

To configure your General IVR settings:

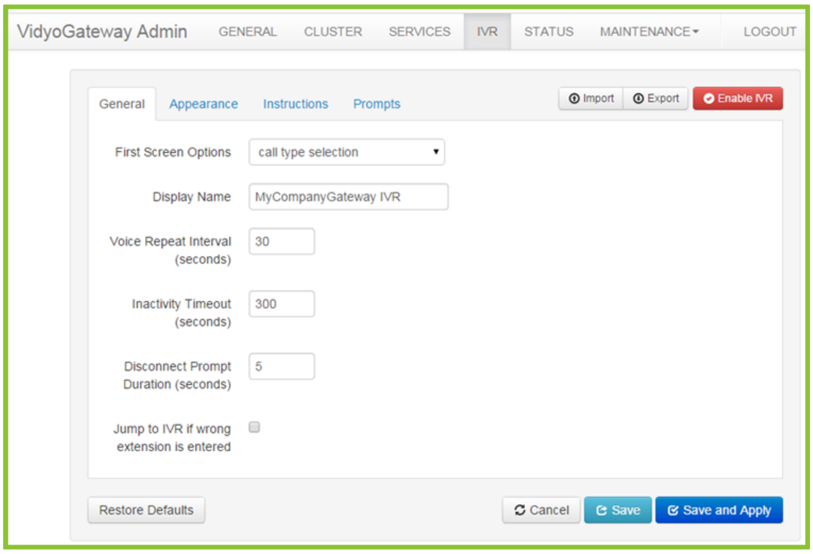
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *IVR* tab.

   The *IVR > General* page displays by default.



First Screen Options: call type selection

Display Name: MyCompanyGateway IVR

Voice Repeat Interval (seconds): 30

Inactivity Timeout (seconds): 300

Disconnect Prompt Duration (seconds): 5

Jump to IVR if wrong extension is entered: □

3. Enter General settings for your IVR. Available choices include the following:

   a. Select one of the following notification types from the **First Screen Options** drop-down to be first shown from your VidyoGateway server IVR Interface:

- □ Select **call type selection** to make both conference and direct calls available from the first screen. The Select Call Type notification displays. For more information about the Select Call Type notification, see VidyoGateway IVR Screen Prompt Types.
- □ Select **conference call only** to make only conference calls available from the first screen. The Enter Conference Extension notification displays. For more information about the Enter Conference Extension notification, see VidyoGateway IVR Screen Prompt Types.
- □ Select **direct call only** to make only direct calls available from the first screen. The Enter Direct Call Extension notification displays. For more information about the Enter Direct Call Extension notification, see VidyoGateway IVR Screen Prompt Types.

Note When placing a direct call and the remote participant has not answered, use the * key to cancel the call. For additional information, see VidyoGateway IVR Screen Instruction Type.

b. Enter the name of your VidyoGateway in the **Display Name** field to be shown when calling in from Legacy devices.

c. Enter a numeric time value (in seconds) in the **Voice Repeat Interval (seconds)** field to elapse between repeated voice responses.

d. Enter a numeric time value (in seconds) in the **Inactivity Timeout (seconds)** field to elapse before a Legacy endpoint is disconnected from your VidyoGateway due to inactivity.

e. Enter a numeric time value (in seconds) in the **Disconnect Prompt Duration (seconds)** field to elapse from when a Legacy endpoint is disconnected from your VidyoGateway due to inactivity until being returned to the VidyoGateway *IVR* screen.

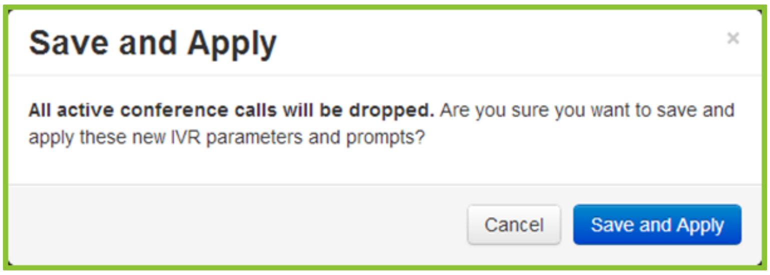
f. Select or deselect the **Jump to IVR if wrong extension is entered** checkbox:

- □ Select the checkbox to show the IVR when an incorrect extension or PIN is entered when dialing from the VidyoGateway IVR.
- □ Deselect the checkbox to keep the IVR from being shown when an incorrect extension or PIN is entered when dialing from the VidyoGateway IVR.

Note The IVR is still shown (or not shown) based on this selection even if you bypass the IVR and call directly in to VidyoConferences from Legacy endpoints using an IP address, Prefix (if any), and Extension.

4. Click **Save** or **Save and Apply** as desired.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new IVR parameters and prompts?

- Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring Appearance IVR Settings

To configure your Appearance IVR settings:

1. Log in to the Admin portal using your System Console account.

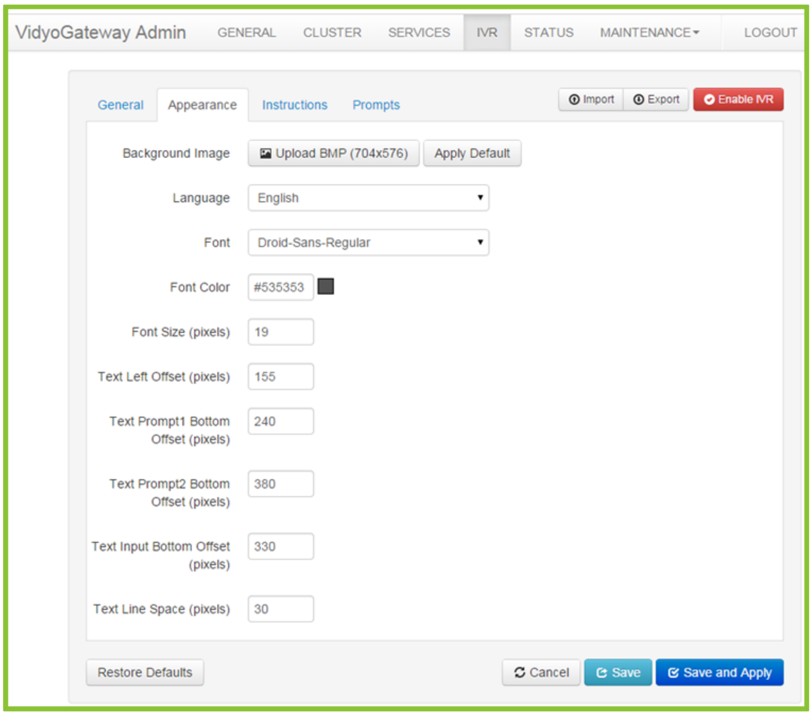
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *IVR* tab.

   The *IVR > General* page displays by default.

3. Click the *Appearance* subtab.



Background Image	
Language	English
Font	Droid-Sans-Regular
Font Color	#535353
Font Size (pixels)	19
Text Left Offset (pixels)	155
Text Prompt1 Bottom Offset (pixels)	240
Text Prompt2 Bottom Offset (pixels)	380
Text Input Bottom Offset (pixels)	330
Text Line Space (pixels)	30

4. Use the following two buttons to select a custom image or use the default for your VidyoGateway IVR background image:

   - Click **Upload BMP** to select a custom image for use on your VidyoGateway IVR.

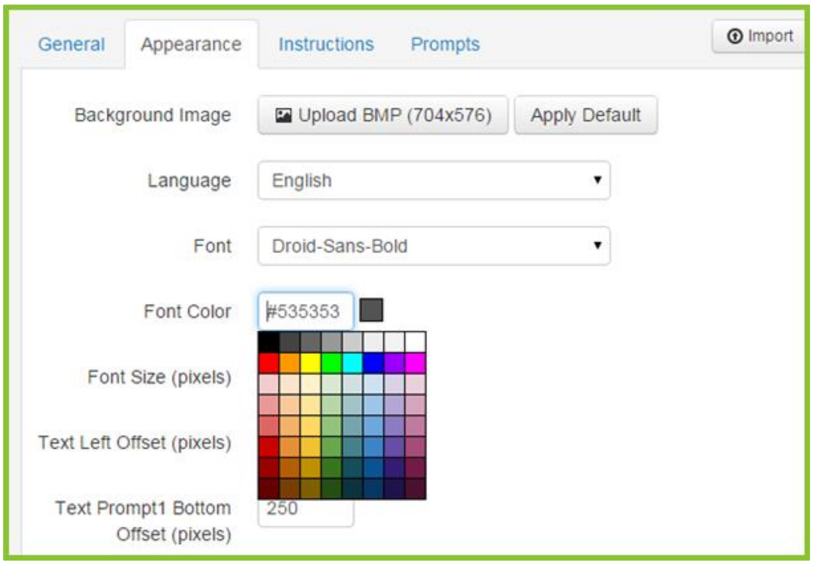
     Your **.bmp** file must be 704 x 576 and not exceed 10MB.

   - Click **Apply Default** to apply the default background image to your VidyoGateway IVR.

5. Click the **Language** drop-down and select the interface language for your IVR.

6. Click the **Font** drop-down and select the font you want to use for the text shown on your IVR interface.

7. Click the **Font Color** field and select from the palate of swatch colors that displays.



Background Image: Upload BMP (704x576) | Apply Default

Language: English

Font: Droid-Sans-Bold

Font Color: #535353

Font Size (pixels)

Text Left Offset (pixels)

Text Prompt1 Bottom Offset (pixels): 250

Note You can enter a standard color name or hexadecimal value directly in the field.

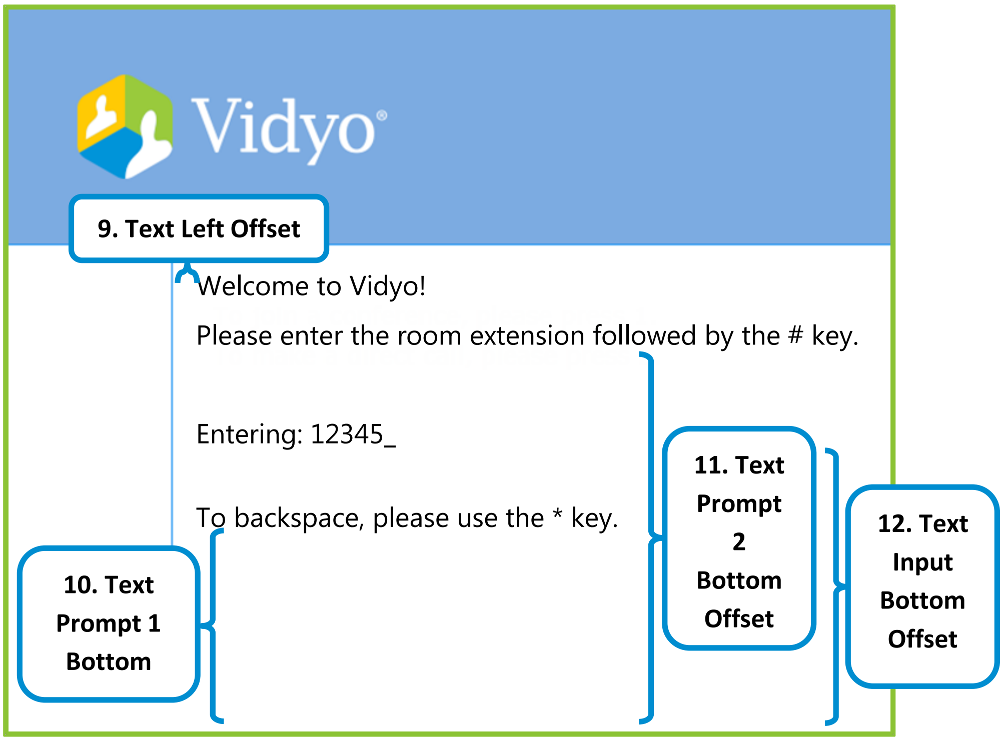
Hexadecimal color values are shown as you mouse-over swatches on the palate.

A swatch of the selected color is shown to the right of the field.

8. Enter a number value (in pixels) for the **Font Size** you want used for your VidyoGateway IVR screens.

9. Enter a number value (in pixels) for the **Text Left Offset** (the margin between the left of the screen and the start of your text) you want used for your VidyoGateway IVR.

The following screenshot shows the text left offset (and other offset values) on the VidyoGateway IVR screens:



Welcome to Vidyo!

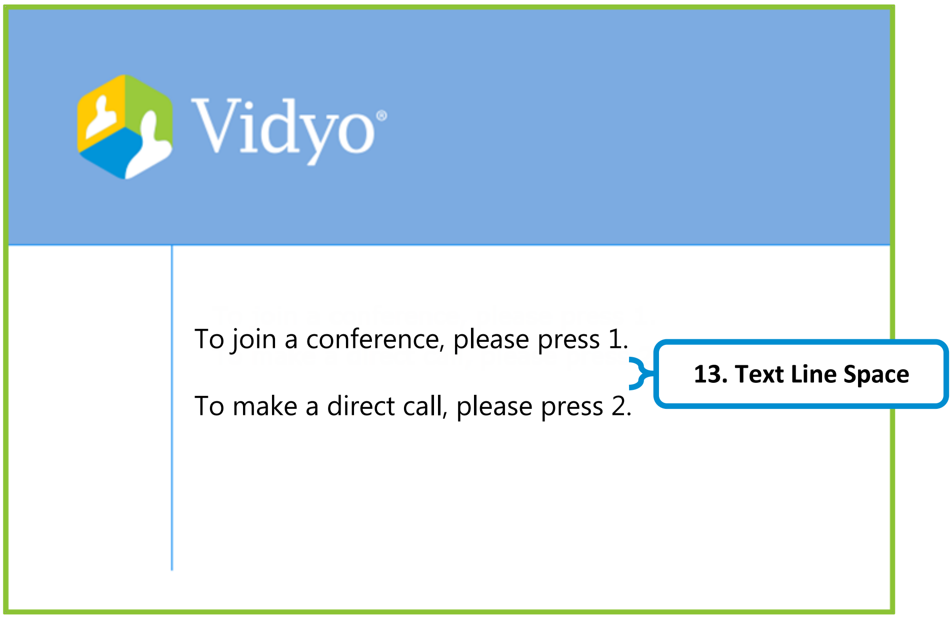
Please enter the room extension followed by the # key.

Entering: 12345_

To backspace, please use the * key.

10. Enter a number value (in pixels) for the **Text Prompt 1 Bottom Offset** (the space between the bottom and the start of your text in the first dialog box shown) you want used for your VidyoGateway IVR screens.
11. Enter a number value (in pixels) for the **Text Prompt 2 Bottom Offset** (the space between the bottom and the start of your text in the second dialog box shown) you want used for your VidyoGateway IVR screens.
12. Enter a number value (in pixels) for the **Text Input Bottom Offset** (the space between the bottom and the start of your text in the first input dialog box shown) you want used for your VidyoGateway IVR screens.
13. Enter a number value (in pixels) for the **Text Line Space** (the space between lines of text) you want used for your VidyoGateway IVR screens.

The following screenshot shows the line space on the VidyoGateway *IVR* screen:

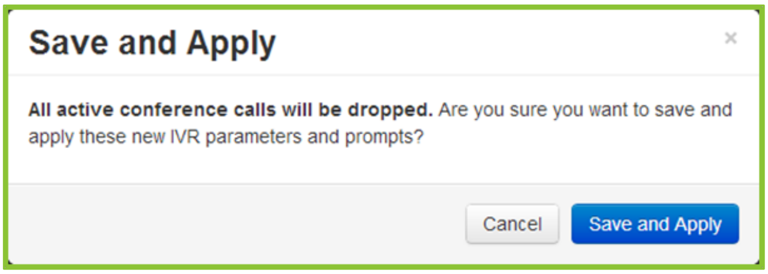


To join a conference, please press 1.

To make a direct call, please press 2.

14. Click **Save** or **Save and Apply** as desired.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new IVR parameters and prompts?

- Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

Configuring VidyoGateway IVR Screen Instruction Settings

To configure your VidyoGateway IVR screen instruction settings:

1. Log in to the Admin portal using your System Console account.

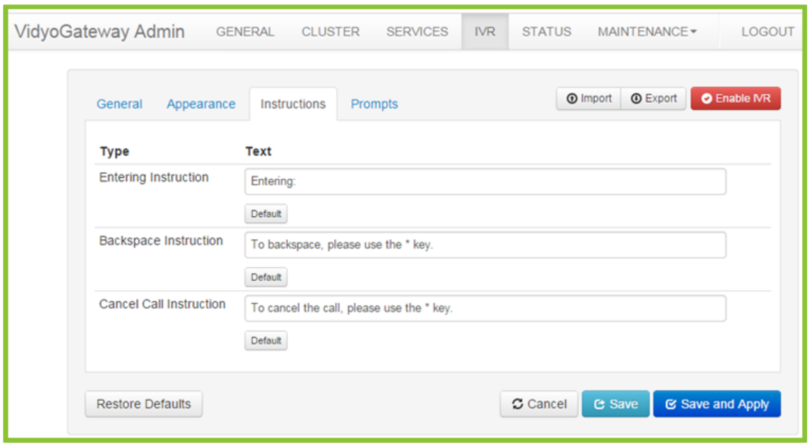
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *IVR* tab.

   The *IVR > General* page displays by default.

3. Click the *Instructions* subtab.



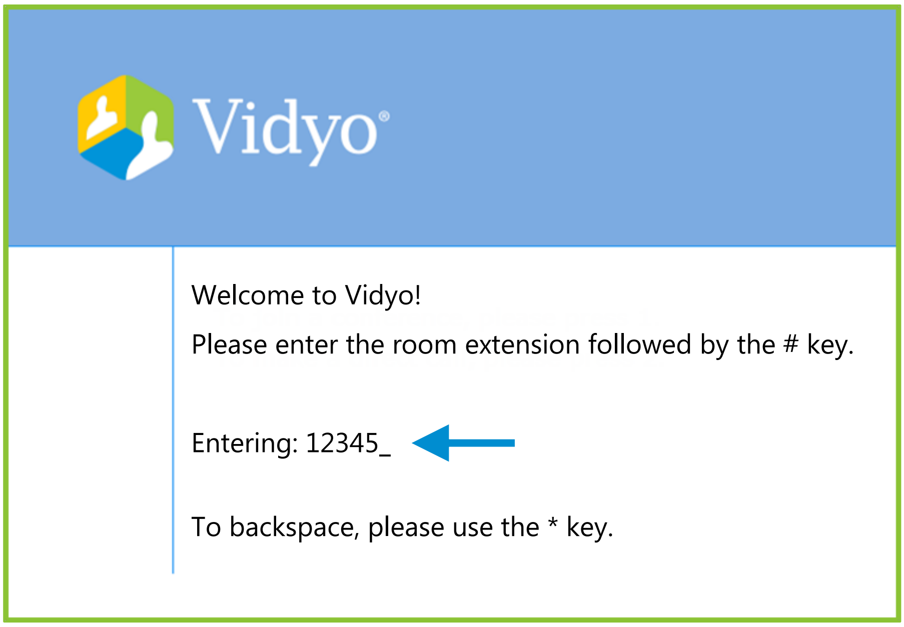
Type	Text
Entering Instruction	Entering:
Backspace Instruction	To backspace, please use the * key.
Cancel Call Instruction	To cancel the call, please use the * key.

4. Enter custom text for the Entering Instruction you want used for your VidyoGateway IVR screens.

   Entering Instruction is the announcement used when participants dialing from a Legacy device to join VidyoConferences.

Note Click **Default** at any time to restore the original system text for the corresponding instruction.

The following screenshot shows the entering instruction for the VidyoGateway IVR screen:



Welcome to Vidyo!

Please enter the room extension followed by the # key.

Entering: 12345_

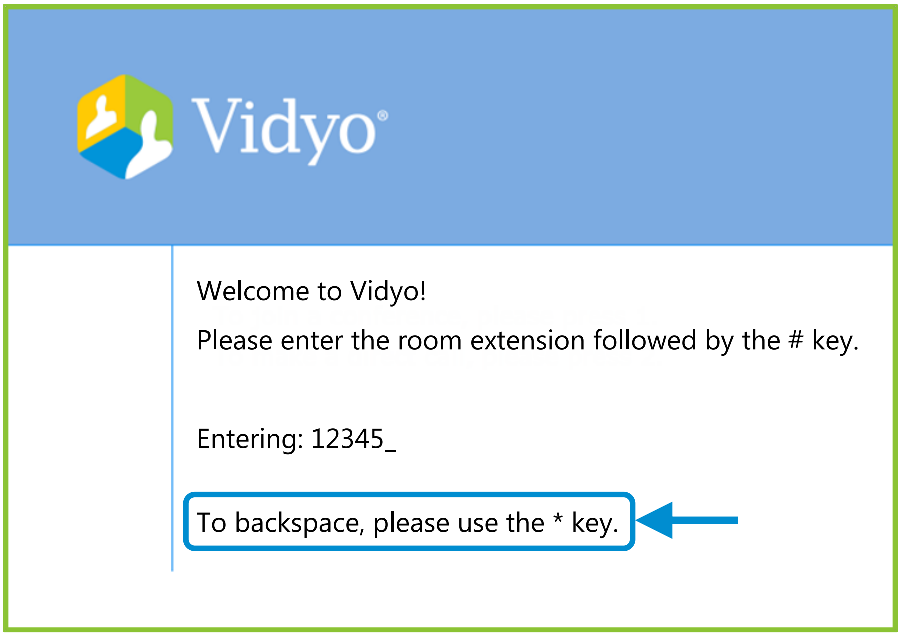
To backspace, please use the * key.

5. Enter custom text for the **Backspace Instruction** you want used for your VidyoGateway IVR screens.

The Backspace Instruction is what participants dialing from Legacy devices are told in order to move backward through menu selections.

Note Click **Default** at any time to restore the original system text for the corresponding instruction.

The following screenshot shows the backspace instruction for the VidyoGateway IVR screen:



Welcome to Vidyo!

Please enter the room extension followed by the # key.

Entering: 12345_

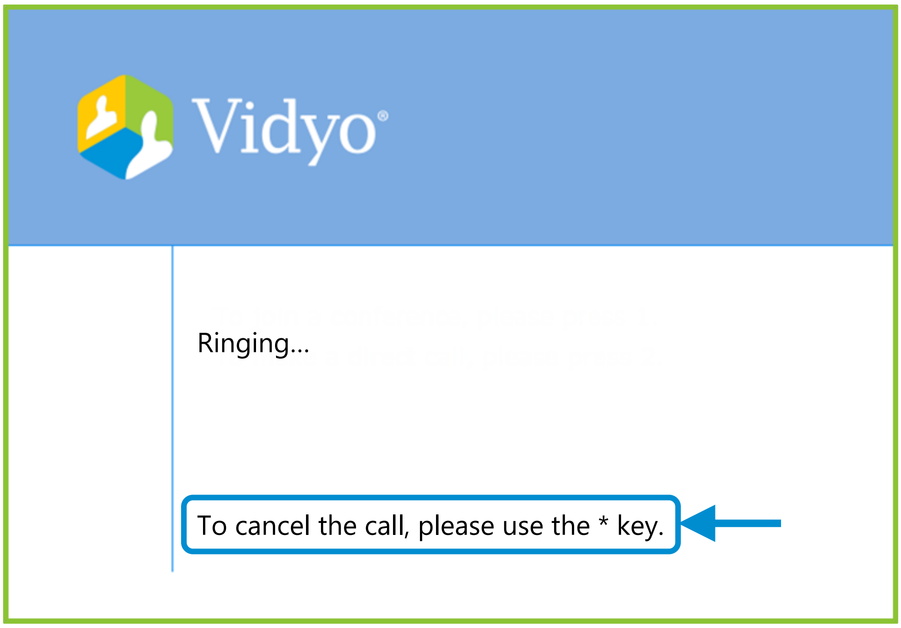
To backspace, please use the * key.

6. Enter custom text for the **Cancel Call Instruction** you want used for your VidyoGateway *IVR* screen.

   The Cancel Call Instruction is what participants dialing from Legacy devices are told in order to immediately end their call.

Note Click **Default** at any time to restore the original system text for the corresponding instruction.

The following screenshot shows the cancel call instruction for the VidyoGateway IVR screen:

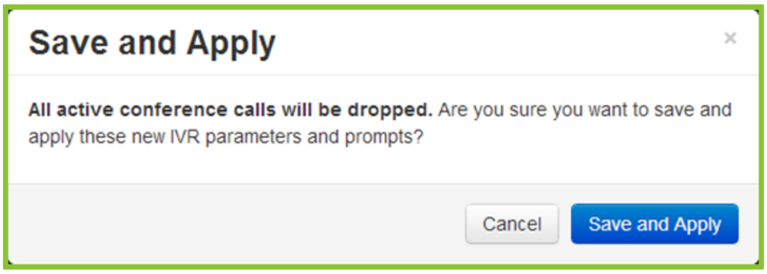


Ringing...

To cancel the call, please use the * key.

7. Click **Save** or **Save and Apply** as desired.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new IVR parameters and prompts?

- Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

VidyoGateway IVR Screen Instruction Type

VidyoGateway *IVR* screen instruction types include the following:

- The Entering Instruction pompt type. This prompt is shown when you start entering the number to complete the extension entry.
- The Backspace Instruction prompt type. This prompt is shown when you start entering room or direct extensions or pins. It displays text instructing you to use the * key as a backspace.

- The Cancel Call Instruction prompt type. This prompt is when you are in the process of connecting to a conference room. It displays text instructing you to use the * key to cancel the call.

Configuring VidyoGateway IVR Screen Prompt Settings

To configure your VidyoGateway IVR screen prompt settings:

1. Log in to the Admin portal using your System Console account.

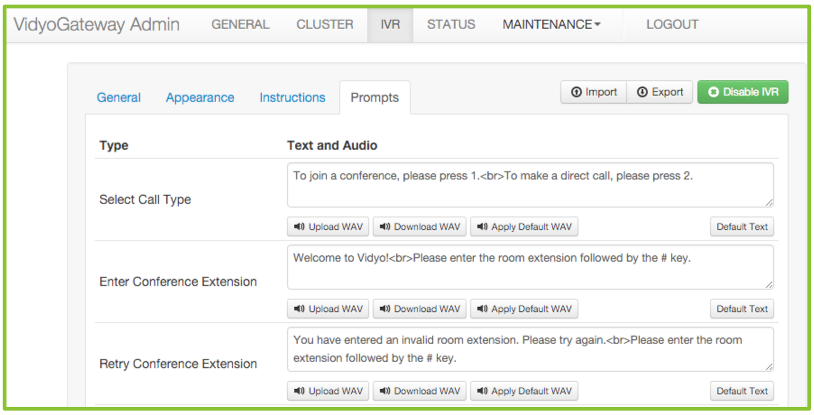
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *IVR* tab.

   The *IVR > General* page displays by default.

3. Click the *Prompts* subtab.



Type	Text and Audio
Select Call Type	To join a conference, please press 1. To make a direct call, please press 2.
Enter Conference Extension	Welcome to Vidyo! Please enter the room extension followed by the # key.
Retry Conference Extension	You have entered an invalid room extension. Please try again. Please enter the room extension followed by the # key.

Note The previous screenshot has been altered to show a condensed listing of the IVR prompt types. For a complete list of IVR prompt types and descriptions, see VidyoGateway IVR Screen Prompt Types.

4. Enter settings for each IVR prompt type using the following corresponding fields:

   - Enter custom prompt type text in the corresponding field.

Note Click and drag the lower-right corner of the **Prompt type** field to adjust the space to the size desired.

   - Click **Default Text** to use the original system text for the corresponding VidyoGateway *IVR* screen prompt type.
   - Click **Upload WAV** to select a custom sound file for use on your VidyoGateway *IVR* screen prompt type.

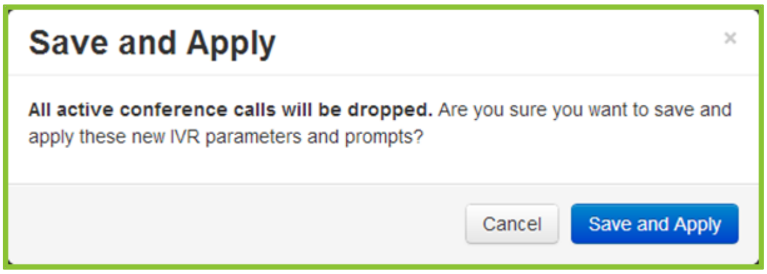
You must upload a 16-bit, mono **.wav** file.

- Click **Download WAV** to save the sound file being currently used as your VidyoGateway IVR screen prompt type.
- Click **Apply Default WAV** to use the original system sound file as your VidyoGateway IVR screen prompt type.

For a complete list of IVR prompt types and descriptions, see VidyoGateway IVR Screen Prompt Types.

5. Click **Save** or **Save and Apply** as desired.

- When you click **Save and Apply**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Apply

All active conference calls will be dropped. Are you sure you want to save and apply these new IVR parameters and prompts?

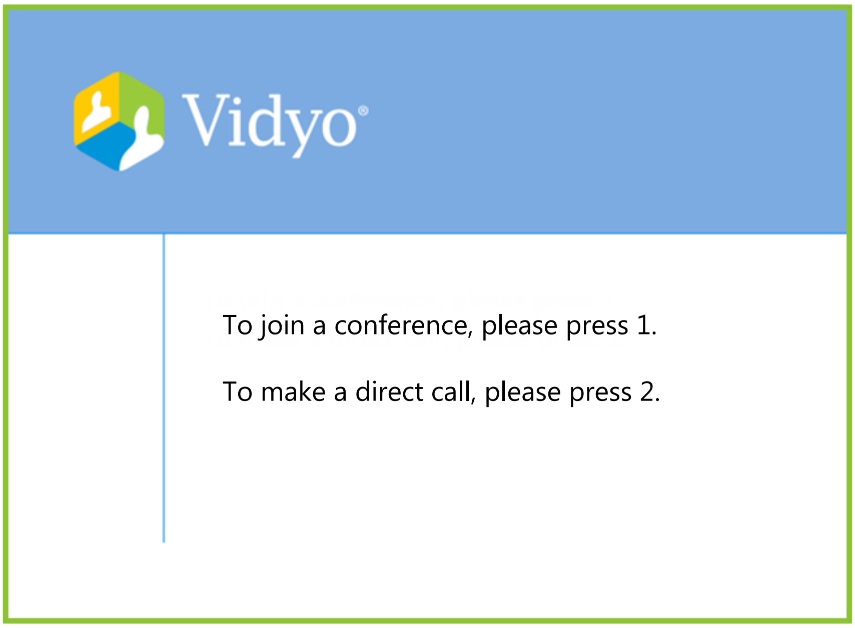
- Settings made while only clicking **Save** accrue and are applied when you subsequently click **Save and Apply** or reboot your VidyoGateway server.

VidyoGateway IVR Screen Prompt Types

VidyoGateway *IVR* screen prompt types include the following:

- The Select Call Type prompt type. If configured as the First Screen Option selection as described on page Configuring Appearance IVR Settings, you first dial in to VidyoGateway and receive this prompt showing choices to join a conference and make a direct call.

- The following screenshot shows the Select Call Type prompt for the VidyoGateway *IVR* screen:



To join a conference, please press 1.

To make a direct call, please press 2.

- The Enter Conference Extension prompt type. If configured as the First Screen Option selection in Configuring Appearance IVR Settings, you first dial in to VidyoGateway and receive this prompt asking you to enter the room extension followed by the # key.
- The Retry Conference Extension prompt type. If you choose to join a conference and enter an invalid room extension, this prompt tells you and asks you to try again by entering the room extension followed by the # key.
- The Retry Room not Accessible (Locked or Full) prompt type. If you lock the room at any point or the room has reached its capacity based on the maximum number of participants set in the VidyoPortal Admin UI, this prompt tells you the conference room is not available and to try again later.
- The Retry Room Generic Error prompt type. If you are unable to join a conference for reasons other than being locked out, this prompt is the generic message indicating you were unable to join the conference and to try again by entering the room extension followed by the # key.
- The Enter Conference Pin prompt type. If you choose to join a conference and enter a room extension followed by the # key, this prompt then instructs you to enter a room pin followed by the # key.
- The Retry Conference Pin prompt type. If you choose to join a conference, enter a room extension followed by the # key, and enter an incorrect room pin followed by the # key, this prompt tells you and asks you to try again by entering the room pin followed by the # key.
- The Enter Direct Call Extension prompt type. If configured as the First Screen Option selection as described on page Configuring Appearance IVR Settings, you first dial in to VidyoGateway and receive this prompt asking you to enter the extension followed by the # key.

- The Retry Direct Call Extension prompt type. If you choose to make a direct call and enter an invalid extension, this prompt tells you and asks you to try again by entering the extension followed by the # key.
- The Retry Direct Call (Offline) prompt type. If you choose to make a direct call, enter an extension, and the remote party is offline, this prompt tells you and asks you to try again by entering the extension followed by the # key.
- The Retry Direct Call (Busy) prompt type. If you choose to make a direct call, enter an extension, and the remote party's line is busy, this prompt tells you and asks you to try again by entering the extension followed by the # key.
- The Retry Direct Call (No Answer) prompt type. If you choose to make a direct call, enter an extension, and the remote party does not answer, this prompt tells you and asks you to try again by entering the extension followed by the # key.
- The Retry Direct Call (Reject) prompt type. If you choose to make a direct call, enter an extension, and the remote party rejects the call, this prompt tells you and asks you to try again by entering the extension followed by the # key.
- The Retry Direct Call (Generic Error) prompt type. If you choose to make a direct call, enter an extension, and it's not connected for any other reason than the previous 4 mentioned, this prompt tells you the remote party could not be reached and asks you to try again by entering the extension followed by the # key.
- The Retry Direct Call (Cancel) prompt type. If you choose to make a direct call, enter an extension, and it's cancelled, this prompt tells you and asks you to try again by entering the extension followed by the # key.
- The Direct Call Ringing prompt type. If you choose to make a direct call, enter an extension, and the line is ringing, this prompt indicates that the line is ringing.
- The Only Participant prompt type. If you choose to join a conference, enter a room extension followed by the # key, enter a room pin followed by the # key, and join successfully, you are shown this prompt if you are the only participant in the conference.

Importing and Exporting VidyoGateway IVR Media and Prompt Settings

You can apply or restore IVR media and prompt settings that have been already saved by importing an existing **`.tar.gz`** file to your VidyoGateway server. You can also save exported settings to a **`.tar.gz`** file for applying to a different VidyoGateway server or just keep it as a backup.

Note Imported and exported settings only apply to media files and prompts. It does not include other IVR configurations.

Importing IVR Media and Prompt Settings

To import IVR media and prompt settings:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *IVR* tab.

   The *IVR > General* page displays by default.

3. Click **Import**.

   The *Import IVR Configuration* pop-up displays.

4. Click **Choose File** to locate the configuration file.

5. Click **Import**.

   A system notification indicates the IVR configuration was imported successfully.

Exporting IVR Media and Prompt Settings

To export IVR media and prompt settings:

1. Log in to the Admin portal using your System Console account.

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

2. Click the *IVR* tab.

   The *IVR > General* page displays by default.

3. Click **Export**.

   Your browser downloads a **`.zip`** file which contains 19 **`.wav`** files, a text file, and a **`.bmp`** file.

Enabling and Disabling VidyoGateway IVR Settings

So far you've been making configurations on the *General*, *Appearance*, *Instructions*, and *Prompt* subtabs and clicking **Save** or **Save and Apply** as desired. However, clicking **Enable or Disable IVR** is what determines whether or not your VidyoGateway *IVR* screen is actually shown to users accessing VidyoConferences via Legacy devices.

To enable or disable VidyoGateway IVR settings:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Click the *IVR* tab.

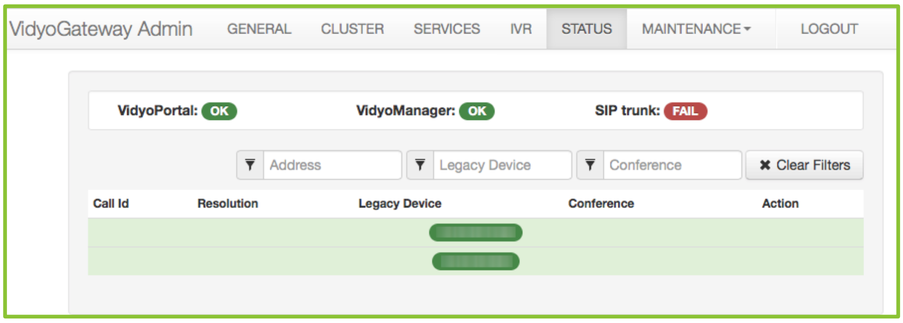
The *IVR > General* page displays by default.

3. Click **Enable IVR**.

   This button toggles between Enable and Disable functions.

Checking the Status of Your VidyoGateway

The *STATUS* page displays the network connectivity status of the VidyoGateway with the VidyoPortal, the VidyoManager, and a SIP Trunk, if configured. The status displays as “OK” or “FAIL” depending on whether the VidyoPortal, VidyoManager, and SIP Trunk are successfully connected.

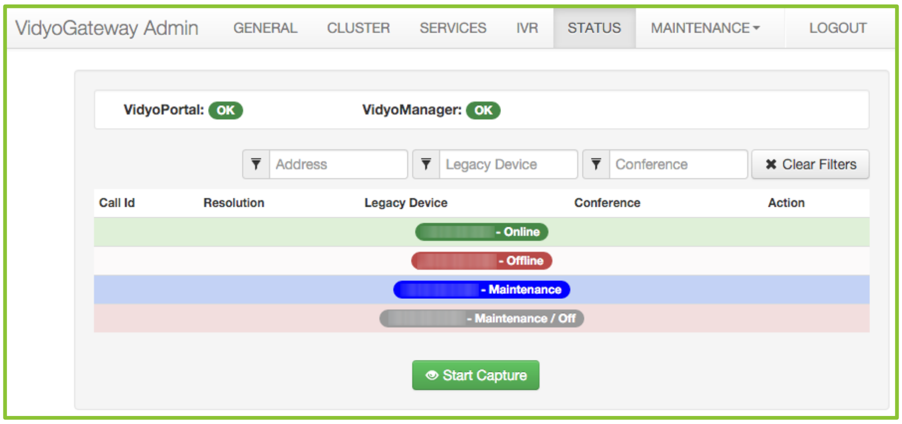


VidyoPortal: OK VidyoManager: OK SIP trunk: FAIL

Call Id	Resolution	Legacy Device	Conference	Action

When accessing the VidyoGateway Admin Pages for the Active Controller, the connection status for each node that is configured for the VidyoGateway cluster on the *CLUSTER > Nodes* subtab display on the *STATUS* page as well. For additional information, see Configuring Nodes for the Active Controller in Cluster Mode.

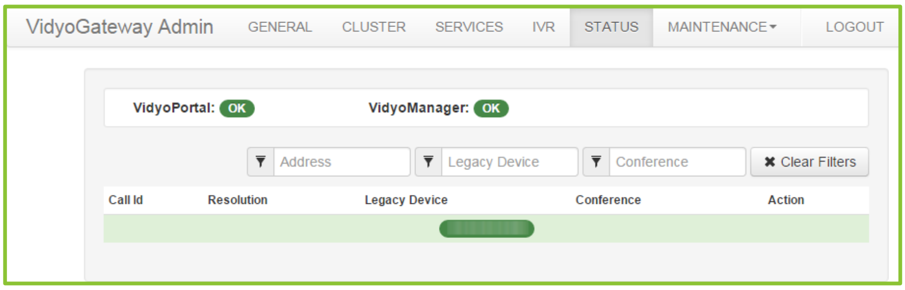
Note When configuring your VidyoGateways as a cluster, you must export the pre-shared key from your Active Controller and import it into your Standby Controller and Cluster Nodes. Otherwise, calls on your Standby Controller or Cluster Nodes will not be visible from the *Status* tab in your Active Controller.



VidyoPortal: OK VidyoManager: OK

Call Id	Resolution	Legacy Device	Conference	Action

If the VidyoGateway is processing calls, the main area of the screen is populated with call information such as Call ID, Resolution, Legacy Device, and Conference.



If the VidyoGateway is not currently processing calls, no results display like the screenshot previously shown.

When results do display on the screen, they can be filtered by the following:

- In the Address filter, you can filter results by IP of Cluster.
- In the Legacy Device filter, you can filter results by IP of Legacy devices.
- In the Conference filter, you can filter by conference room names already set up in your system.

Click **Clear Filters** to instantly remove any parameters you provided.

Viewing Call Statistics

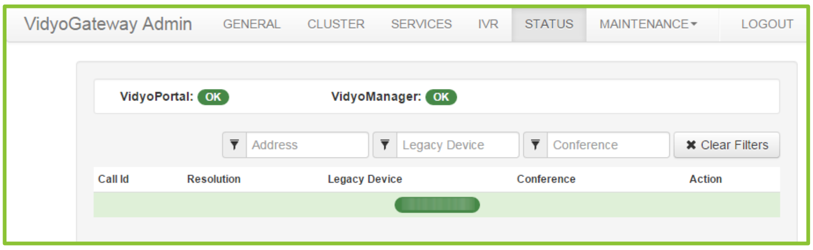
To view call statistics:

1. Log in to the Admin portal using your System Console account.

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

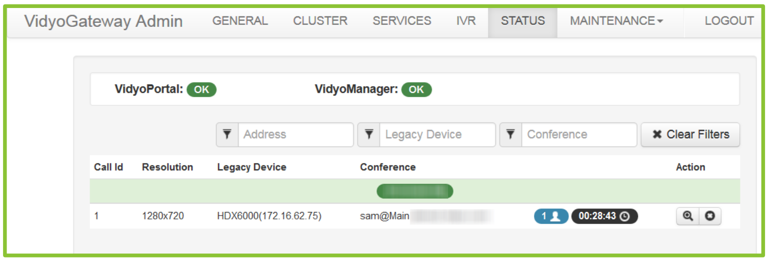
   The *GENERAL* > *VidyoPortal* page displays by default.

2. Click the *STATUS* tab.



   - If the VidyoGateway is not currently processing calls, no results display like the screenshot previously shown.

- If your VidyoGateway is processing calls, the main area of the screen is populated with call information such as Resolution, Legacy Device, Conference, Number of Participants, and Call Duration as follows.



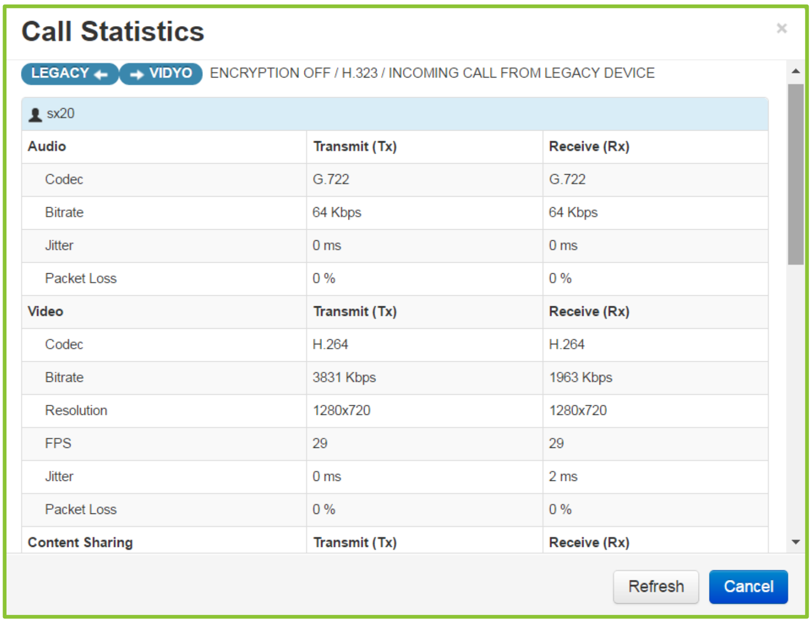
VidyoPortal: OK VidyoManager: OK

Address | Legacy Device | Conference | ✖ Clear Filters

Call Id	Resolution	Legacy Device	Conference		Action
			[redacted]		
1	1280x720	HDX6000(172.16.62.75)	sam@Main [redacted]	1 👤 00:28:43	🔍 ⚙

3. Click the magnifying glass to the right of a specific call row in the main area of the screen.

   The *Call Statistics* pop-up displays.



Call Statistics

LEGACY ⇄ VIDYO ENCRYPTION OFF / H.323 / INCOMING CALL FROM LEGACY DEVICE

👤 sx20

Audio	Transmit (Tx)	Receive (Rx)
Codec	G.722	G.722
Bitrate	64 Kbps	64 Kbps
Jitter	0 ms	0 ms
Packet Loss	0 %	0 %
Video	**Transmit (Tx)**	**Receive (Rx)**
Codec	H.264	H.264
Bitrate	3831 Kbps	1963 Kbps
Resolution	1280x720	1280x720
FPS	29	29
Jitter	0 ms	2 ms
Packet Loss	0 %	0 %
Content Sharing	**Transmit (Tx)**	**Receive (Rx)**

4. The following information is available on the *Call Statistics* pop-up:

   - The Legacy ⟷Vidyo label is shown along with the encryption status, codec, and call direction.
   - The Legacy device shaded table heading displays the name of your device along with the following data between the VidyoGateway and the Legacy device:
     - Audio codec protocols being used for both transmitting and receiving messages.
     - Audio bitrate for both transmitting and receiving values (in Kbps).
     - Audio jitter for both transmitting and receiving values (in ms).
     - Audio packet loss for both transmitting and receiving values (as a percent).
     - Video codec protocols for both transmitting and receiving messages.

        - Video bitrate for both transmitting and receiving values (in Kbps).
        - Video resolution dimensions for both transmitting and receiving values (in pixels).
        - Video frames per second (FPS) for both transmitting and receiving values.
        - Audio jitter for both transmitting and receiving values (in ms).
        - Packet loss for both transmitting and receiving values (as a percentage).
        - Content sharing codec protocols for both transmitting and receiving messages.
        - Content sharing bitrate for both transmitting and receiving values (in Kbps).
        - Content sharing resolution dimensions for both transmitting and receiving values (in pixels).
        - Content sharing frames per second (FPS) for both transmitting and receiving values.
        - Content sharing jitter for both transmitting and receiving values (in ms).
        - Content sharing packet loss for both transmitting and receiving values (as a percentage).
    - The Vidyo ⟷Legacy label is shown along with the encryption status.
    - The Vidyo device shaded table heading displays the name of your device along with data between the VidyoGateway and the VidyoRouter.

5. Click the **X** button on the right of a row to drop the call.
6. Click **Refresh** to reload the statistical data showing on Call Statistics.

Capturing Application Logs

The *STATUS* page allows you to capture logs of calls occurring on your VidyoGateway.

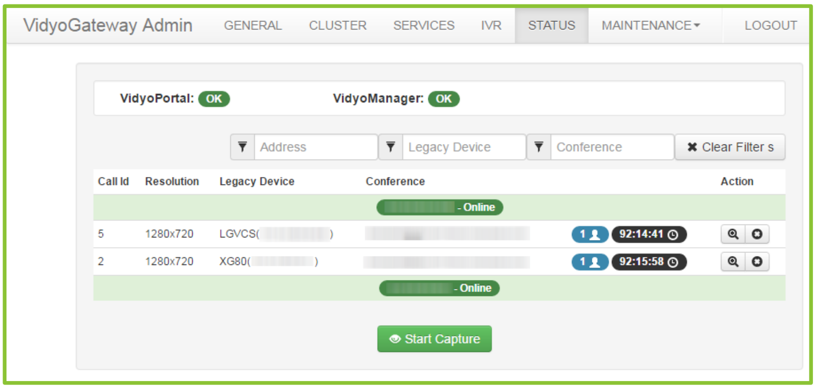
To capture application logs:

1. Log in to the Admin portal using your System Console account.

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

2. Click the *STATUS* tab.

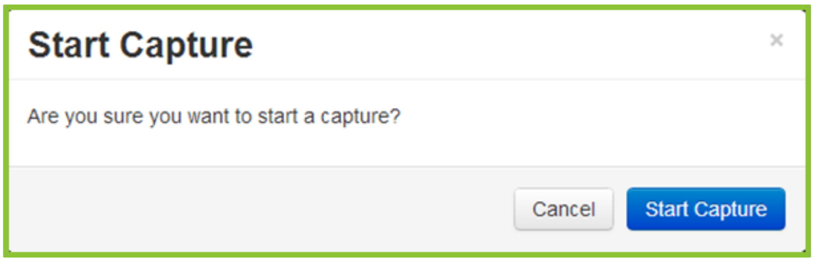
3. Click **Start Capture**.



VidyoPortal: OK VidyoManager: OK

Call Id	Resolution	Legacy Device	Conference		Action
[redacted] - Online					
5	1280x720	LGVCS([redacted])	[redacted]	1 92:14:41	
2	1280x720	XG80([redacted])	[redacted]	1 92:15:58	
[redacted] - Online					

The *Start Capture* pop-up displays.



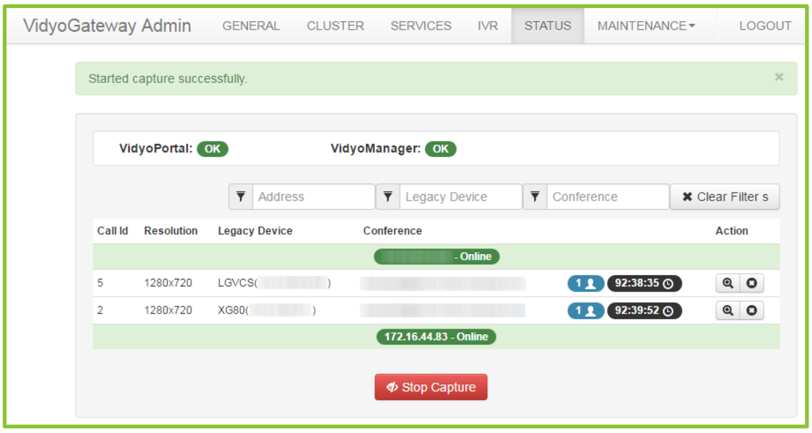
Are you sure you want to start a capture?

4. Click **Start Capture**.

Note Logs of calls taking place on your VidyoGateway are recorded into a file only after you click **Start Capture**.

If the capture is started, a system notification displays indicating it was started successfully.

5. Click **Stop Capture** when you want to stop logging the calls taking place on your VidyoGateway server.

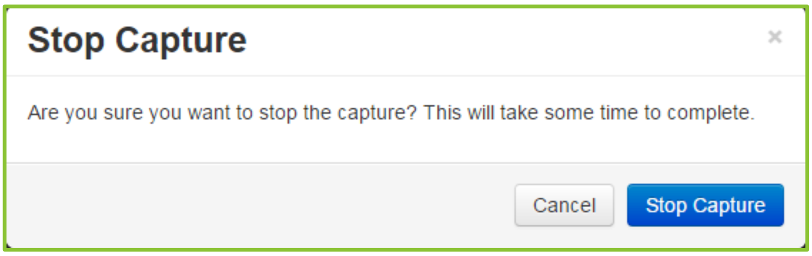


Started capture successfully.

VidyoPortal: OK VidyoManager: OK

Call Id	Resolution	Legacy Device	Conference		Action
[redacted] - Online					
5	1280x720	LGVCS([redacted])	[redacted]	1 92:38:35	
2	1280x720	XG80([redacted])	[redacted]	1 92:39:52	
172.16.44.83 - Online					

The *Stop Capture* pop-up displays.



Stop Capture

Are you sure you want to stop the capture? This will take some time to complete.

6. Click **Stop Capture**.

   If the capture is stopped, a system notification displays indicating it was stopped successfully.

Diagnostics

The *MAINTENANCE > DIAGNOSTICS* page allows you to run and download logs for debugging analysis. Specific user activity audit log files may also be downloaded from the *MAINTENACE > DIAGNOSTICS* page using the **Download Audit Logs** button. For more information about downloading and viewing audit logs, see 6. Auditing.

Downloading Application Logs

To download the single application logs file for debugging purposes:

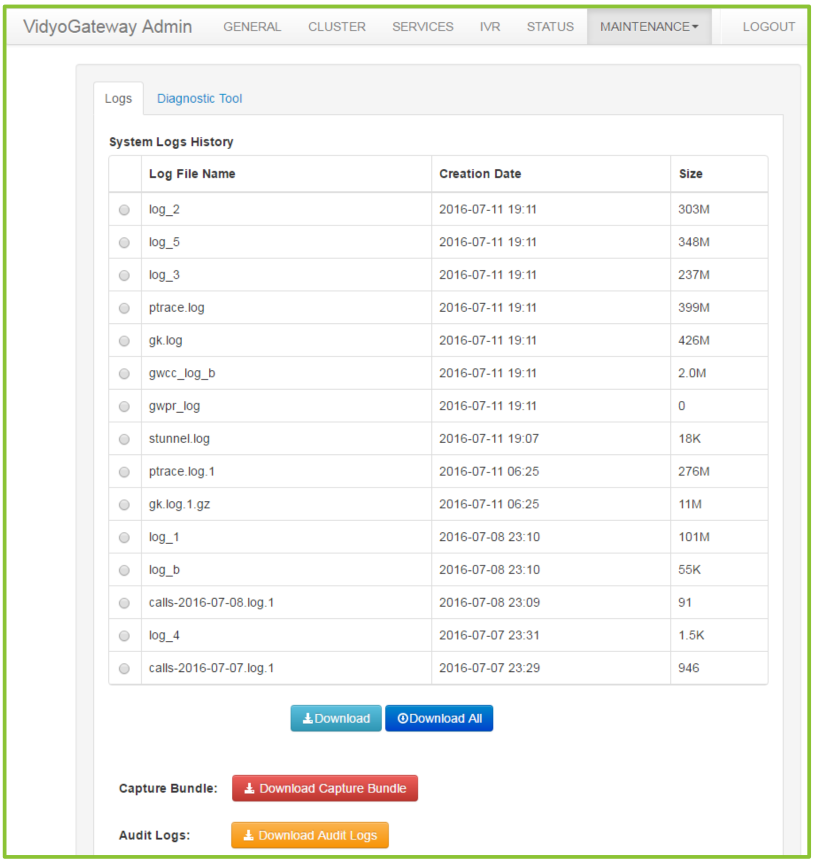
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > DIAGNOSTICS*.

The *MAINTENANCE > DIAGNOSTICS > Logs* page displays by default.



System Logs History

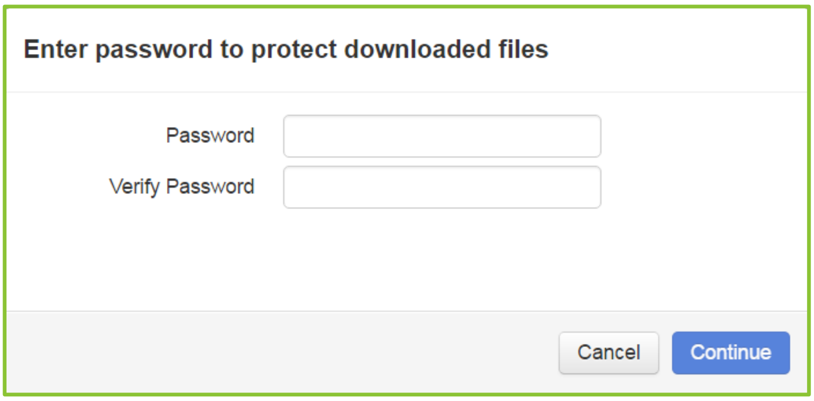
	Log File Name	Creation Date	Size
○	log_2	2016-07-11 19:11	303M
○	log_5	2016-07-11 19:11	348M
○	log_3	2016-07-11 19:11	237M
○	ptrace.log	2016-07-11 19:11	399M
○	gk.log	2016-07-11 19:11	426M
○	gwcc_log_b	2016-07-11 19:11	2.0M
○	gwpr_log	2016-07-11 19:11	0
○	stunnel.log	2016-07-11 19:07	18K
○	ptrace.log.1	2016-07-11 06:25	276M
○	gk.log.1.gz	2016-07-11 06:25	11M
○	log_1	2016-07-08 23:10	101M
○	log_b	2016-07-08 23:10	55K
○	calls-2016-07-08.log.1	2016-07-08 23:09	91
○	log_4	2016-07-07 23:31	1.5K
○	calls-2016-07-07.log.1	2016-07-07 23:29	946

Capture Bundle:

Audit Logs:

3. Click **Download Capture Bundle** to download the capture bundle.

   The *Enter password to protect downloaded files* pop-up displays.



Enter password to protect downloaded files

Password

Verify Password

4. Enter a password in the **Password** field.
5. Re-enter the password in the **Verify Password** field.
6. Click **Continue**.

Your browser downloads a **`.tar.gz`** file containing the log file bundle for debugging analysis.

Note Alternatively, select the the radio button to the left of any logs that need to be downloaded and click **Download**.

You can also click the **Download All** button to download all current logs.

Running Diagnostic Logs

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
- Type of Node and version
- Machine Type
- Node FQDN
- IP Address
- Server Mode
- DNS Server Report
- Etherent Hardware Report
- VidyoGateway Ports
- System Status Report
- Certificate Check

To run diagnostic logs:

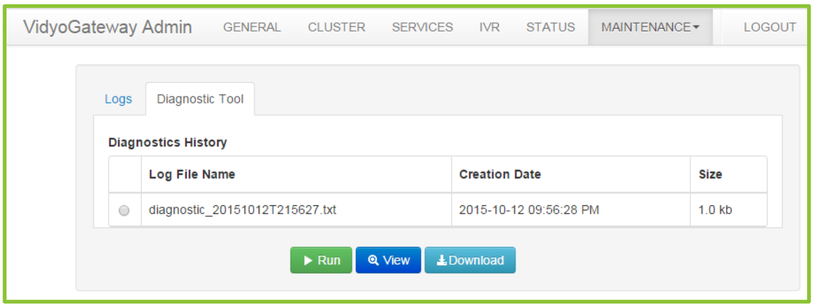
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.
2. Navigate to *MAINTENANCE > DIAGNOSTICS*.

   The *MAINTENANCE > DIAGNOSTICS > Logs* page displays by default.

3. Click the *Diagnostic Tool* subtab.



Diagnostics History

	Log File Name	Creation Date	Size
○	diagnostic_20151012T215627.txt	2015-10-12 09:56:28 PM	1.0 kb

4. Click **Run**.

   Wait a few mintes for the diagnostic file to generate and display in the Diagnostics History table.

Viewing Diagnostic Logs

To view single application logs file for debugging purposes:

1. Log in to the Admin portal using your System Console account.

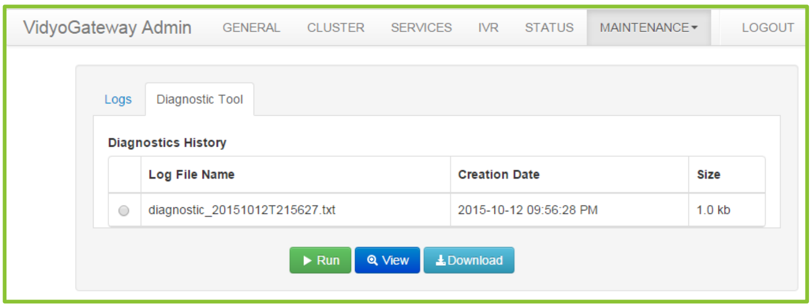
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > DIAGNOSTICS.*

   The *MAINTENANCE > DIAGNOSTICS > Logs* page displays by default.

3. Click the *Diagnostic Tool* subtab.

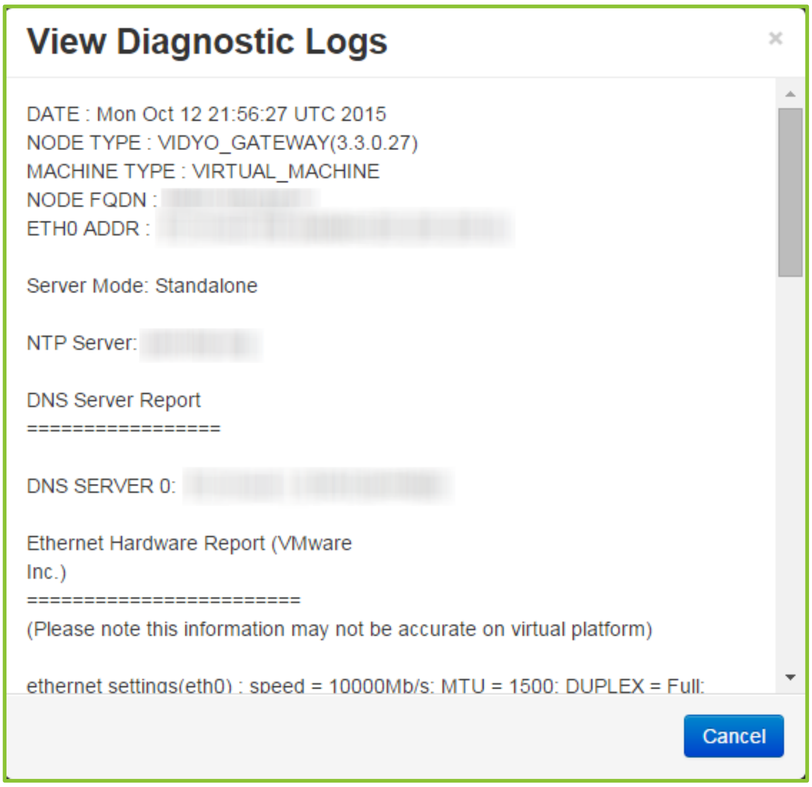


Diagnostics History

	Log File Name	Creation Date	Size
○	diagnostic_20151012T215627.txt	2015-10-12 09:56:28 PM	1.0 kb

4. Select the radio button to the left of the log file that needs to be viewed.
5. Click **View**.

The *View Diagnostic Logs* pop-up displays.



View Diagnostic Logs

```
DATE : Mon Oct 12 21:56:27 UTC 2015
NODE TYPE : VIDYO_GATEWAY(3.3.0.27)
MACHINE TYPE : VIRTUAL_MACHINE
NODE FQDN : [redacted]
ETH0 ADDR : [redacted]

Server Mode: Standalone

NTP Server: [redacted]

DNS Server Report
================

DNS SERVER 0: [redacted]

Ethernet Hardware Report (VMware
Inc.)
=======================
(Please note this information may not be accurate on virtual platform)

ethernet settings(eth0) : speed = 10000Mb/s; MTU = 1500; DUPLEX = Full;
```

6. Click **Cancel** to close the pop-up.

Downloading Diagnostic Logs

To view single application logs file for debugging purposes:

1. Log in to the Admin portal using your System Console account.

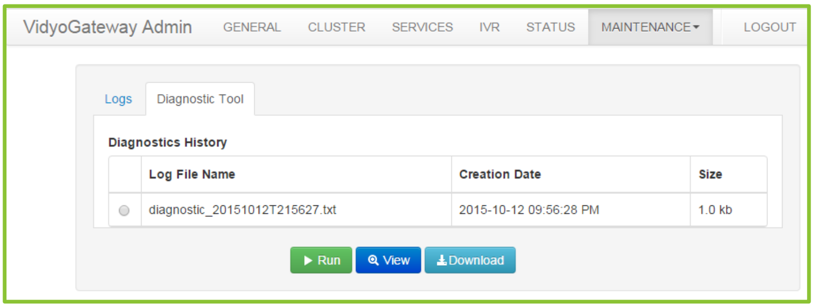
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > DIAGNOSTICS*.

   The *MAINTENANCE > DIAGNOSTICS > Logs* page displays by default.

3. Click the *Diagnostic Tool* subtab.



Diagnostics History

	Log File Name	Creation Date	Size
○	diagnostic_20151012T215627.txt	2015-10-12 09:56:28 PM	1.0 kb

4. Select the radio button to the left of the log file that needs to be viewed.
5. Click **Download**.

   Your browser downloads a **`.tar.gz`** file containing your log file.

Configuring a Public IP Address and Viewing Your VidyoGateway Network Settings

The *MAINTENANCE > NETWORK* page allows you to configure a public IP address and view network settings for your VidyoGateway server.

Configure your network settings using the System Console. For more information, see 3. Configuring Your Server.

Configuring a Public IP Address

Only configure the public IP address on your Controller nodes if you want to dial in to your VidyoGateway using your FQDN.

Note Public IP address configuration is intended for use on a VidyoGateway when it's deployed behind a NAT.

The public IP address should be the address returned by your DNS when looking up the FQDN for your cluster.

Configuring your public IP address only works when the cluster has a private IP address (NAT).

For example, if **`examplecompany.examplegateway.com`** points to 1.2.3.4 and 1.2.3.4 is configured in your firewall as the H.323 address, then you would enter 1.2.3.4 in the **Public IP Address** field.

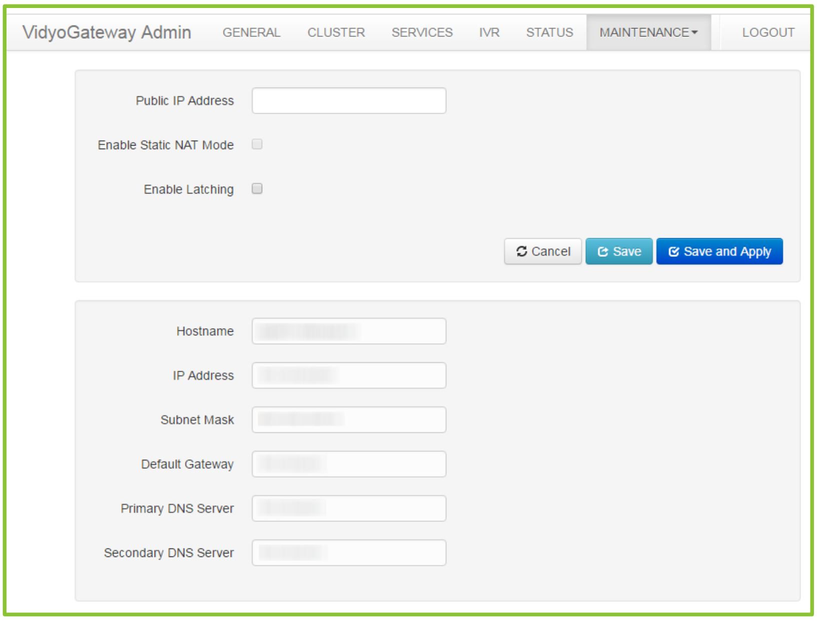
To configure a public IP address:

1. Log in to the Admin portal using your System Console account.

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

The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > NETWORK*.



Public IP Address

Enable Static NAT Mode □

Enable Latching □

Hostname [redacted]

IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

Primary DNS Server [redacted]

Secondary DNS Server [redacted]

3. Enter your public IP Address in the **Public IP Address** field.

4. Select the **Enable Static NAT Mode** checkbox so that the public IP address field is mapped to the Active Controller or standalone VidyoGateway of the external IP address.

   Only one IP address is needed as the media will be proxied from the cluster controller to the clustered nodes. When the checkbox is unchecked, the public IP address is intended for use on a cluster VidyoGateway.

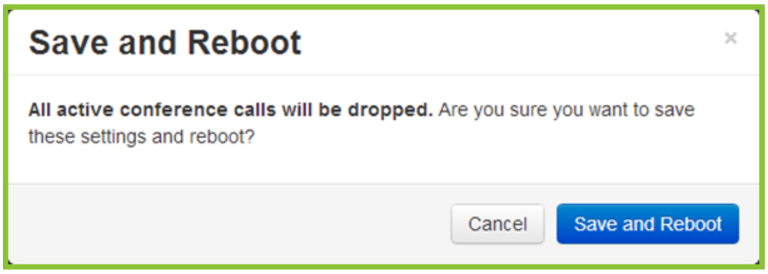
Note The public IP address should be the address returned by your DNS when looking up the FQDN for your cluster. Configuring your public IP address only works when the cluster has a private IP address (NAT).

For example, if examplecompany.examplegateway.com points to 1.2.3.4 and 1.2.3.4 is configured in your firewall as the H.323 address, then you would enter 1.2.3.4 in the **Public IP Address** field.

5. Select the **Enable RTP Latching** checkbox to allow VidyoGateway to work with SIP and H.323 room systems that may be sitting behind a firewall that is not SIP or H.323 aware.

   When latching is enabled, the VidyoGateway uses certain techniques to enable the signaling and media to reach the endpoint through the pinholes it has opened in the firewall. Also, content sharing occurs via the main video instead of BFCP when RTP latching is enabled.

6. Click **Save and Reboot**.
   - Any modifications you make to your Clusters accrue until you click **Save and Reboot**, and then all of your Cluster changes are applied to your VidyoGateway server.
   - When you click **Save and Reboot**, a pop-up informs you that the change drops all of the active conference calls on your VidyoGateway server.



Save and Reboot

All active conference calls will be dropped. Are you sure you want to save these settings and reboot?

Viewing Your VidyoGateway Network Settings

Configure your network settings using the System Console. For more information, see [3. Configuring Your Server]().

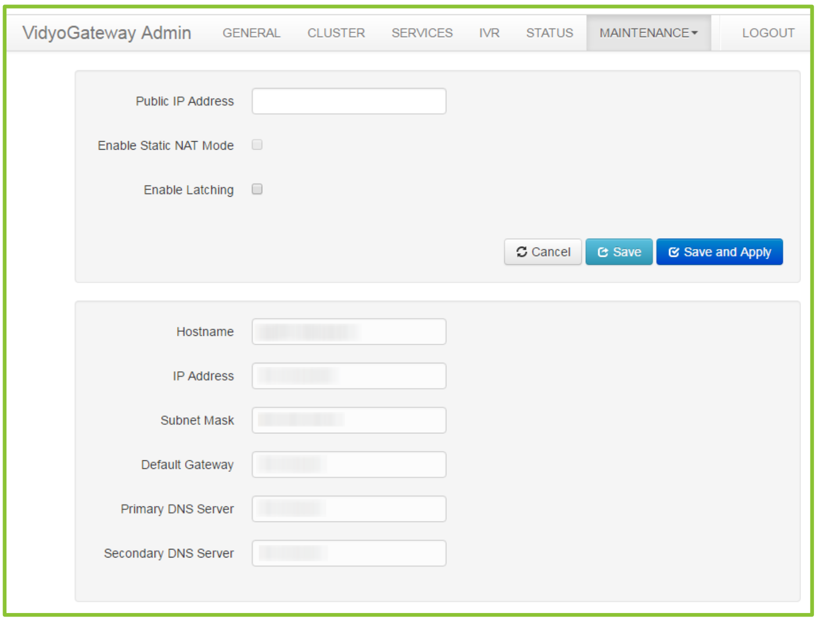
To view your VidyoGateway server network settings:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENACE > NETWORK*.



Understanding VidyoGateway Security

This section of the guide shows you how to secure your VidyoGateway. For more information about securing your entire VidyoConferencing system, refer to the security section in the *VidyoConferencing Administrator Guide*.

Before we secure the VidyoGateway, 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 VidyoGateway.

  While support for HTTPS is standardly included in Vidyo products, it does require the purchase and/or acquisition of SSL certificate(s) 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 browsers and VidyoGateway Admin 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 VidyoGateway 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.

Note This feature is first enabled on your VidyoPortal, and then on your VidyoGateway.

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/or acquisition of SSL certificate(s) from a valid CA (Certificate Authority). Once Encryption is enabled, all calls are secured and encrypted for all users and components. Mixing secured and non-secured calls is not currently supported.

Encrypted end-to-end security uses AES-128 encryption to secure the connection between the VidyoPortal and the VidyoRouter.

Confidential information shared during a VidyoConference is protected from hijacking and eavesdropping attempts.

Securing Your VidyoGateway System with SSL and HTTPS

To secure your VidyoGateway system by Enabling HTTPS, you must complete specific configurations done on six sequential subtabs from left to right in the *MAINTENANCE > SECURITY* section of the VidyoGateway Admin Pages. The subtabs include:

1. The *Private Key* subtab for Generating or Uploading an SSL Private Key
2. The *CSR* subtab for Generating an SSL Certificate Signing Request (CSR)
3. The *Server Cert* subtab for Deploying Your Server Certificate
4. The *Server CA Cert* subtab for Deploying Your Server Certification Authority (CA) Certificates
5. The *Ports* subtab (regarding Security) for correctly configuring the HTTPS Port setting to 443

   This subtab is also used for Management Interface configurations. For more information, see Configuring Your Vidyo Server's Management Interface and Port.
6. The *Advanced* subtab for deploying your Client Root CA Certificates.

   The *Advanced* subtab is also used to upload and import Security Settings, and reset Security Settings. For more information, see Importing Client Root CA Certificates from the Advanced Tab, and Importing and Exporting Certificates.
7. Enabling HTTPS on your VidyoGateway.

   Do not use **Enabling HTTPS** and **Enabling HTTPS Only** until you've completed all the previous steps for securing your VidyoGateway system. For more information, see Enabling HTTPS on Your Vidyo Server.

The following ordered sections explain these steps in detail.

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 disable HTTPS.

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 CSR and SSL Server Certificate. This includes importing existing keys, editing 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 an SSL private key:

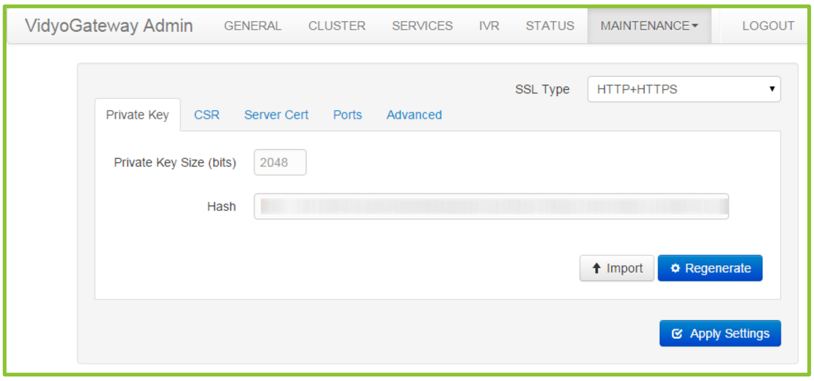
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY.*

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.



SSL Type: HTTP+HTTPS

Private Key Size (bits): 2048

Hash:

3. Click **Import**.

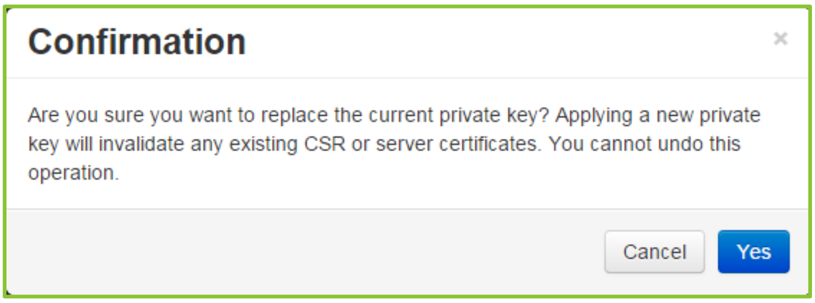
   The *Import Private Key* pop-up displays.

4. Click **Choose File** to locate the private key file.

5. Enter a password in the **Password** field to encrypt data.

6. Click **Import**.

A *Confirmation* pop-up displays.



Confirmation

Are you sure you want to replace the current private key? Applying a new private key will invalidate any existing CSR or server certificates. You cannot undo this operation.

7. Click **Yes**.

   If the upload completes, a system notification displays indicating the private key installed successfully.

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 disable HTTPS.

Changes made to an SSL Private Key require a CSR and SSL Server Certificate. This includes importing existing keys, exporting existing keys, and regenerating new keys.

To regenerate an SSL Private Key:

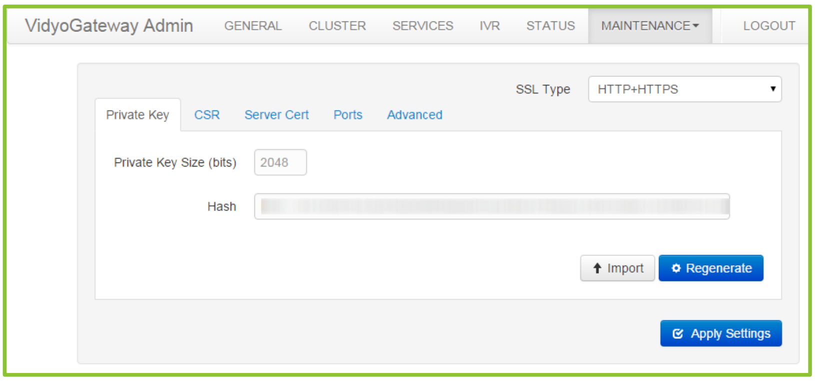
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.



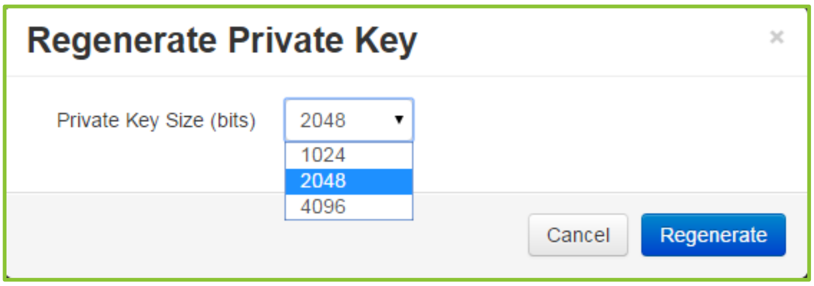
SSL Type: HTTP+HTTPS

Private Key Size (bits): 2048

Hash

3. Click **Regenerate**.

The *Regenerate Private Key* pop-up displays.



Regenerate Private Key

Private Key Size (bits): 2048

4. Select **1024**, **2048**, or **4096** as your **Private Key Size**.

Note Some countries or CAs limit the key size. Observe the limitations in effect in your country. Check with your CA for Key Size requirements.

5. Click **Regenerate**.

   If the change completes, a system notification is shown indicating the private key was regenerated successfully.

Generating 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.

Generating an SSL CSR

To generate an SSL CSR:

1. Log in to the Admin portal using your System Console account.

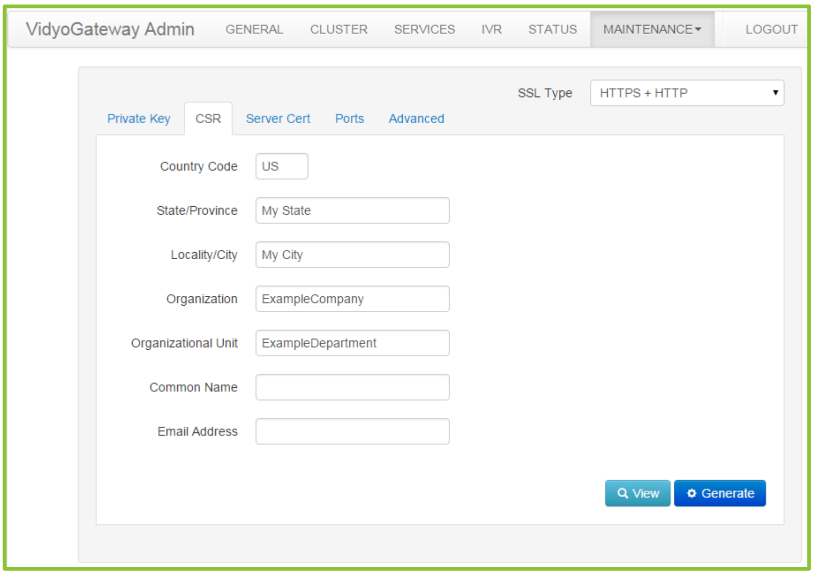
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *CSR* subtab.



SSL Type: HTTPS + HTTP

Country Code: US

State/Province: My State

Locality/City: My City

Organization: ExampleCompany

Organizational Unit: ExampleDepartment

Common Name:

Email Address:

4. 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/City
   - Organization
   - Organization Unit
   - Common Name (the FQDN of the server)
   - Email Address

5. Provide all field information exactly as you registered it with your domain registration provider. You should consider all information on this screen mandatory before you click **Generate/Regenerate**.

Note Click **Cancel** 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 Admin portal using your System Console account.

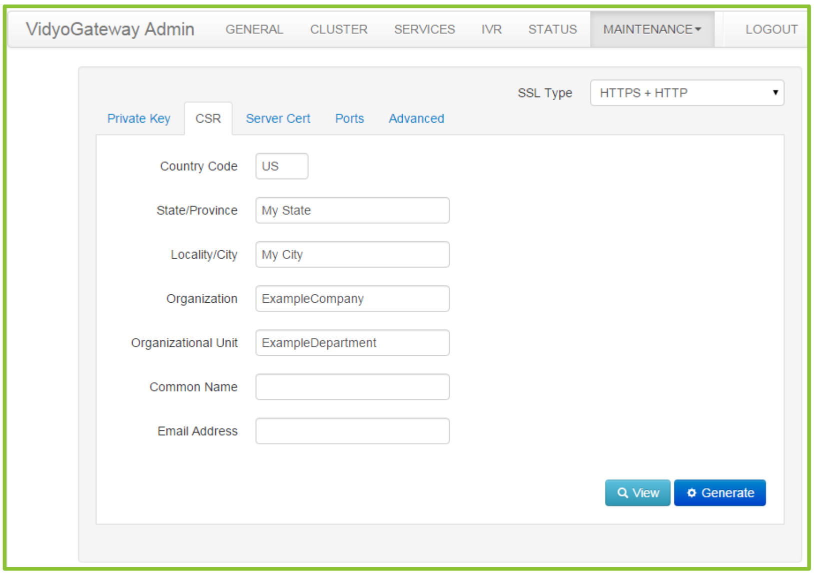
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Naviagate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *CSR* subtab.



SSL Type HTTPS + HTTP

Country Code US

State/Province My State

Locality/City My City

Organization ExampleCompany

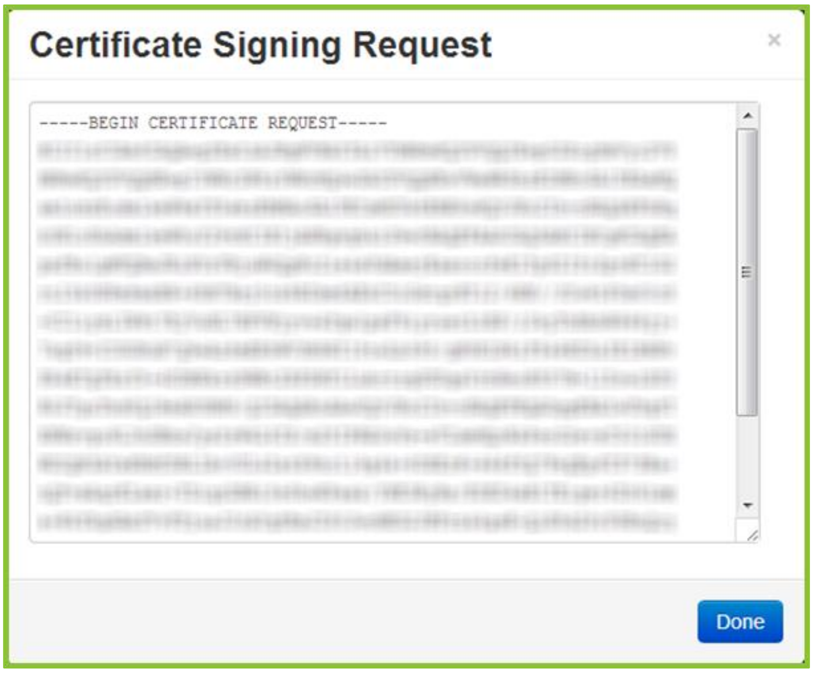
Organizational Unit ExampleDepartment

Common Name

Email Address

4. Click **View**.

The *Certificate Signing Request* pop-up displays.



```
-----BEGIN CERTIFICATE REQUEST-----
```

5. Click **Done**.

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. If neither, the format supported by VidyoGateway is base64 X.509 pem or PKCS#7 (.p7b).

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/or intermediate certificates need to be located, and manually downloaded from the CA's website.

If the root and/or 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/or intermediate certificates available depending on the type of certificate you have ordered. Be sure to locate the appropriate matching root and/or intermediate certificates for your domain certificate. Contact your CA for assistance if you're not sure.

CAs provide different kinds of certificate file(s) 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* tabs. For more information, see Uploading or Editing Your Server Certificate, Appending CA Chain Bundle, and Importing Client Root CA Certificates from the Advanced Tab.
- Bundles (**`.p7b`**, **`.pfx`**, and **`.vidyo`**) are imported and/or exported (only **`.vidyo`** files can be exported) from the *Advanced* subtab. For more information, see Importing and Exporting Certificates.

Uploading or Editing Your Server Certificate

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 Viewing Application and System Information.

If you instead plan on using self-signed certificates, you can click **Generate Self-Signed** to have the server sign its own certificate (self-signed). Clicking **Generate Self-Signed** and confirming removes your currently implemented server certificate.

Editing Your Server Certificate

Changes made to an SSL Private Key require a CSR and SSL Server Certificate. This includes uploading existing keys, editing existing keys, and regenerating new keys.

To edit a server certificate:

1. Log in to the Admin portal using your System Console account.

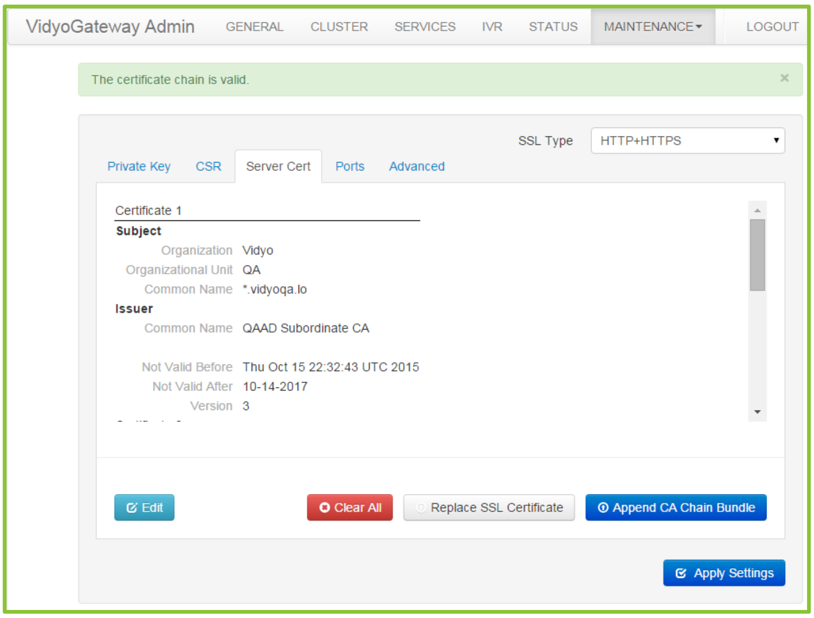
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Server Cert* subtab.



The certificate chain is valid.

SSL Type: HTTP+HTTPS

Certificate 1

Subject

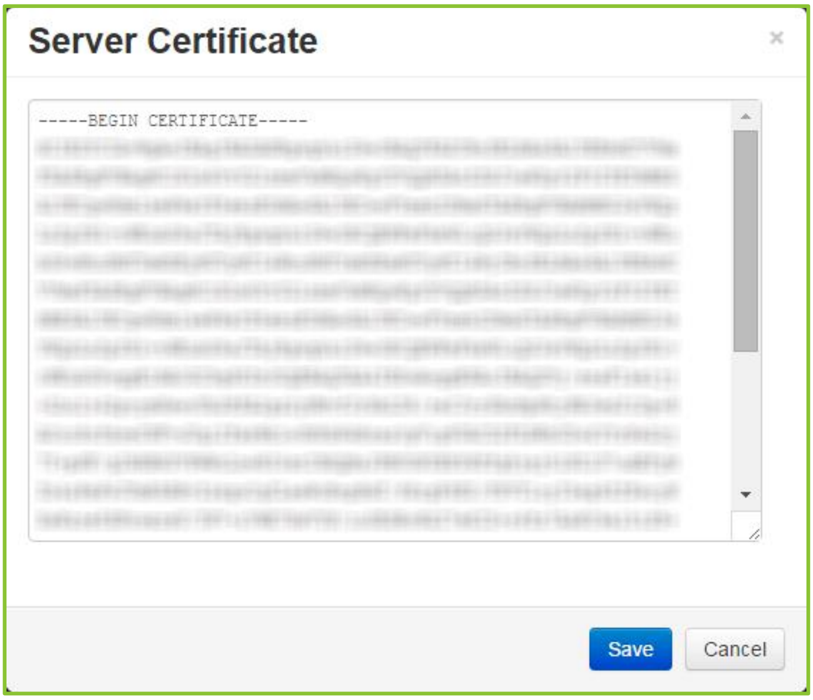
Organization	Vidyo
Organizational Unit	QA
Common Name	*.vidyoqa.lo

Issuer

Common Name	QAAD Subordinate CA
Not Valid Before	Thu Oct 15 22:32:43 UTC 2015
Not Valid After	10-14-2017
Version	3

4. Click **Edit**.

   The *Server Certificate* pop-up displays.



Server Certificate

-----BEGIN CERTIFICATE-----

5. Modify certificate data in the scrollable text region on the pop-up as desired.
6. Click **Save**.

   If the edit completes, a system notification displays indicating the change was successful.

Appending CA Chain Bundle

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 append CA chain bundle:

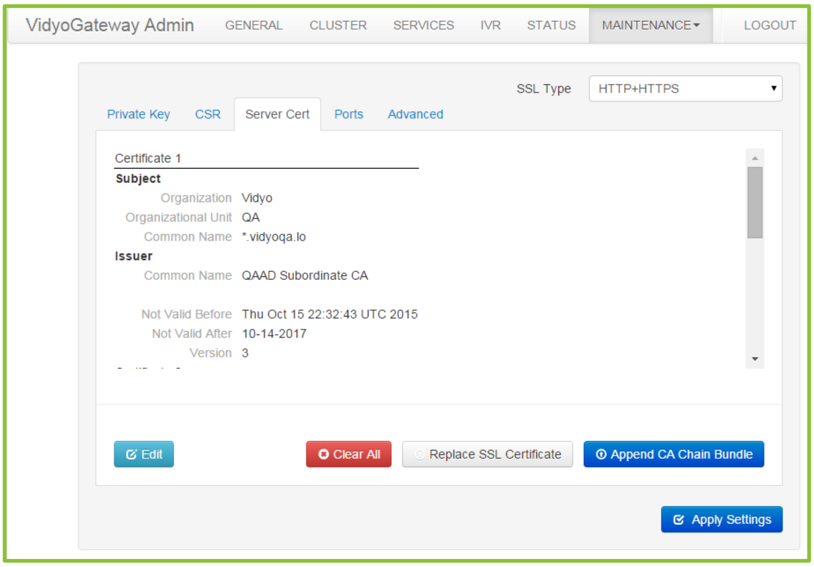
1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.
2. Navigate to *MAINTENANCE > SECURITY.*

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Server Cert* subtab.



SSL Type: HTTP+HTTPS

Certificate 1

Subject

Organization: Vidyo
Organizational Unit: QA
Common Name: *.vidyoqa.lo

Issuer

Common Name: QAAD Subordinate CA

Not Valid Before: Thu Oct 15 22:32:43 UTC 2015
Not Valid After: 10-14-2017
Version: 3

4. Click **Append CA Chain Bundle**.

   The *Append CA Chain Bundle* pop-up displays.

5. Click **Choose File** to locate the file.

6. Click **Upload**.

   A *Confirmation* pop-up displays.

7. Click **Yes**.

Configuring HTTPS Port Settings for Your Admin Pages

The *Applications* tab is also used for Management Interface settings. For more information, see Configuring Your Vidyo Server’s Management Interface and Port.

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.

To configure the HTTPS Port settings for your VidyoGateway Admin Pages:

1. Log in to the Admin portal using your System Console account.

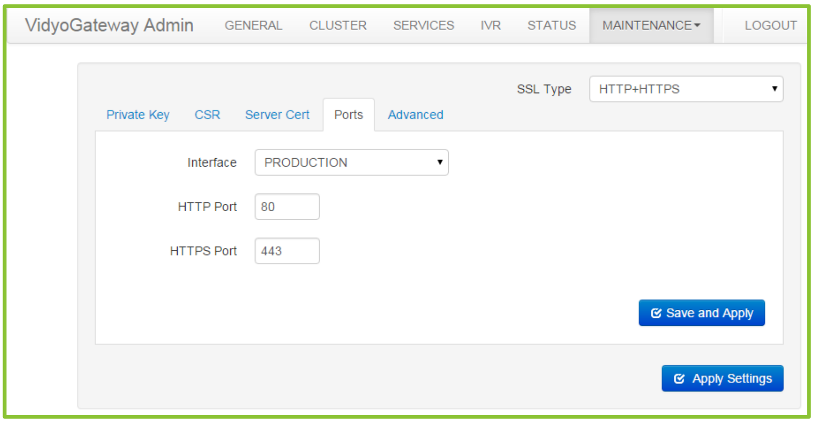
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Ports* subtab.



SSL Type: HTTP+HTTPS

Interface: PRODUCTION

HTTP Port: 80

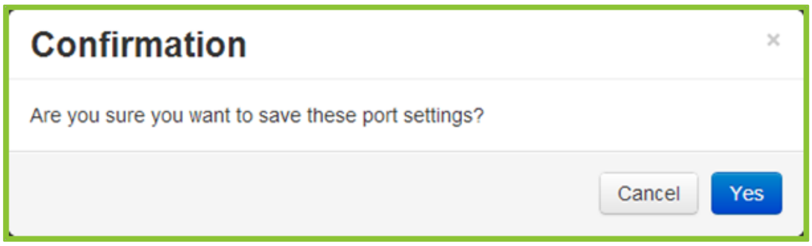
HTTPS Port: 443

The HTTPS port is set to 443 by default. You can change the port value if necessary. Otherwise, leave it as 443.

4. Click **Save and Apply**.

Note Any active calls going through your specific Vidyo server are dropped when you click **Save and Apply**.

A *Confirmation* pop-up displays.



Confirmation

Are you sure you want to save these port settings?

5. Click **Yes**.

If the changes are applied to your Vidyo server, a system notification displays indicating the settings saved successfully.

Importing Client Root CA Certificates from the Advanced Tab

The *Advanced* subtab is used to upload trusted Client Root CA Certificates. This includes all Intermediate and Root Certificates.

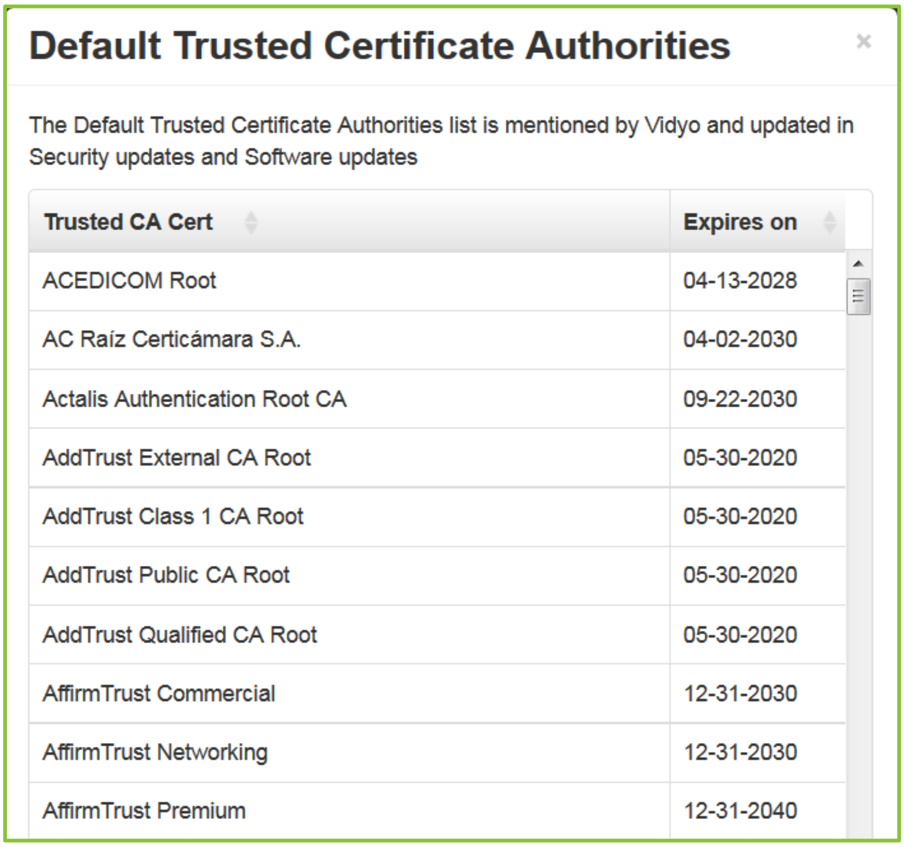
Note If your system requires trusting other secure systems such as VidyoPortals, VidyoRouters, and/or an OCSP Responder, their certificates must also be uploaded in this subtab.

The *Advanced* subtab is also used for OCSP. For more information, see Configuring OCSP.

Importing a Client CA Certificate

Vidyo servers ship with a default trusted Certificate Authority (CA) bundle and is enabled by default. This *Advanced* subtab function allows you to enable or disable the use of this list.

You can view the bundle by clicking the **View** button.



Default Trusted Certificate Authorities

The Default Trusted Certificate Authorities list is mentioned by Vidyo and updated in Security updates and Software updates

Trusted CA Cert	Expires on
ACEDICOM Root	04-13-2028
AC Raíz Certicámara S.A.	04-02-2030
Actalis Authentication Root CA	09-22-2030
AddTrust External CA Root	05-30-2020
AddTrust Class 1 CA Root	05-30-2020
AddTrust Public CA Root	05-30-2020
AddTrust Qualified CA Root	05-30-2020
AffirmTrust Commercial	12-31-2030
AffirmTrust Networking	12-31-2030
AffirmTrust Premium	12-31-2040

To import a client CA cert:

1. Log in to the Admin portal using your System Console account.

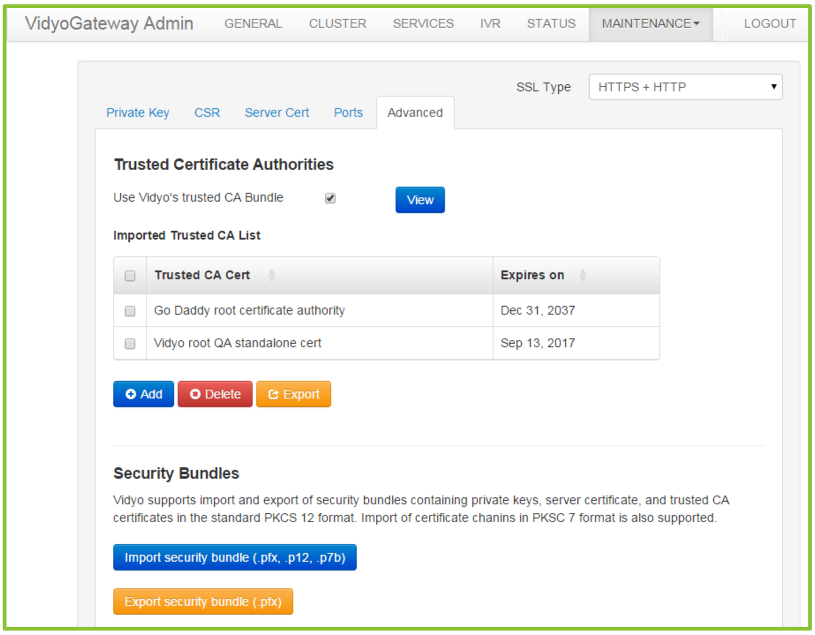
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Advanced* subtab.



SSL Type: HTTPS + HTTP

Trusted Certificate Authorities

Use Vidyo's trusted CA Bundle ☑

Imported Trusted CA List

□	Trusted CA Cert	Expires on
□	Go Daddy root certificate authority	Dec 31, 2037
□	Vidyo root QA standalone cert	Sep 13, 2017

Security Bundles

Vidyo supports import and export of security bundles containing private keys, server certificate, and trusted CA certificates in the standard PKCS 12 format. Import of certificate chanins in PKSC 7 format is also supported.

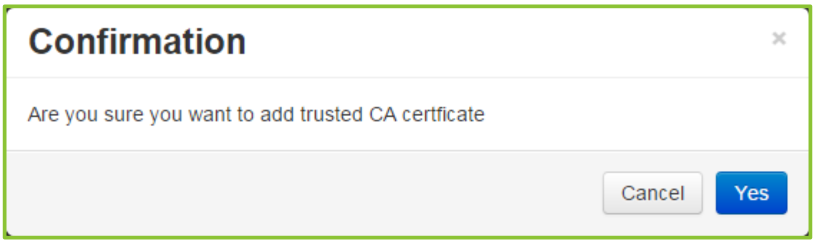
4. Click **Add** in the Trusted Certificate Authorities section.

   The *Add Trusted Certificate Authority* pop-up displays.

5. Click **Choose File** to locate the client CA cert.

6. Click **Upload**.

   A *Confirmation* pop-up displays.



Confirmation

Are you sure you want to add trusted CA certficate

7. Click **Yes**.

   If the changes are applied to your Vidyo server, a system notification displays indicating the settings saved successfully.

Importing and Exporting Certificates

You can also import or export certificate bundles using the *Advanced* subtab.

Importing Certificates from a Certificate Bundle

To import a bundle:

1. Log in to the Admin portal using your System Console account.

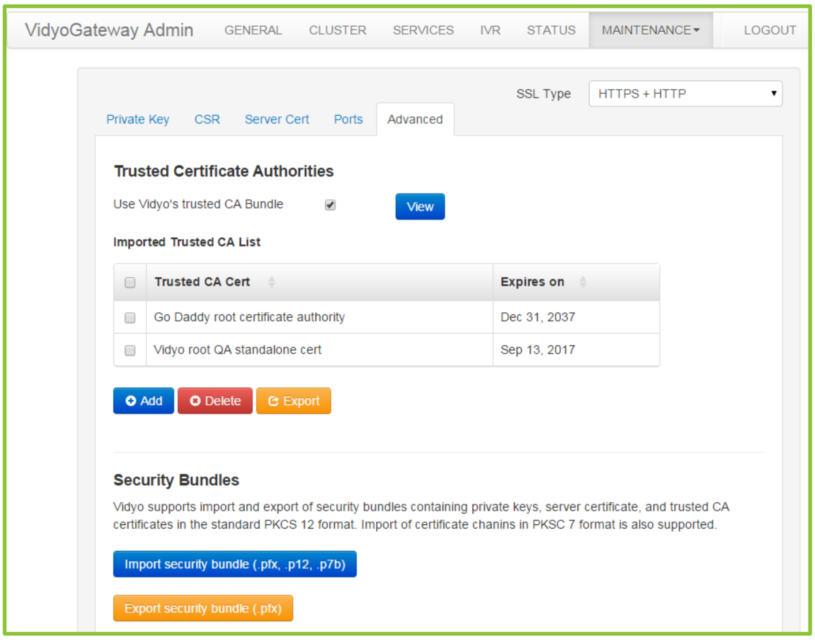
   For more information, see Logging in to the Admin Portal.

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Advanced* subtab.



SSL Type: HTTPS + HTTP

Trusted Certificate Authorities

Use Vidyo's trusted CA Bundle ☑

Imported Trusted CA List

□	Trusted CA Cert	Expires on
□	Go Daddy root certificate authority	Dec 31, 2037
□	Vidyo root QA standalone cert	Sep 13, 2017

Security Bundles

Vidyo supports import and export of security bundles containing private keys, server certificate, and trusted CA certificates in the standard PKCS 12 format. Import of certificate chanins in PKSC 7 format is also supported.

4. Click **Import security bundle (.pfx, .p12, .p7b)** in the Trusted Certificate Authorities section.

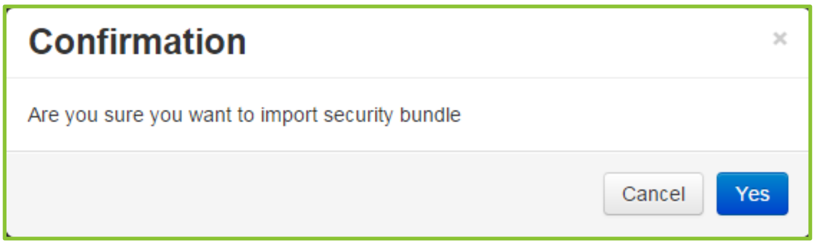
   The *Import Security Bundle* pop-up displays.

5. Click **Choose File** to locate the bundle.

6. Enter the password if using the **`.pfx`** format.

7. Click **Upload**.

A *Confirmation* pop-up displays.



Confirmation

Are you sure you want to import security bundle

8. Click **Yes**.

   If the changes are applied to your Vidyo server, a system notification displays indicating the settings saved successfully.

Exporting a Security Bundle Containing Your Certificate Configuration

To export your security configuration:

1. Log in to the Admin portal using your System Console account.

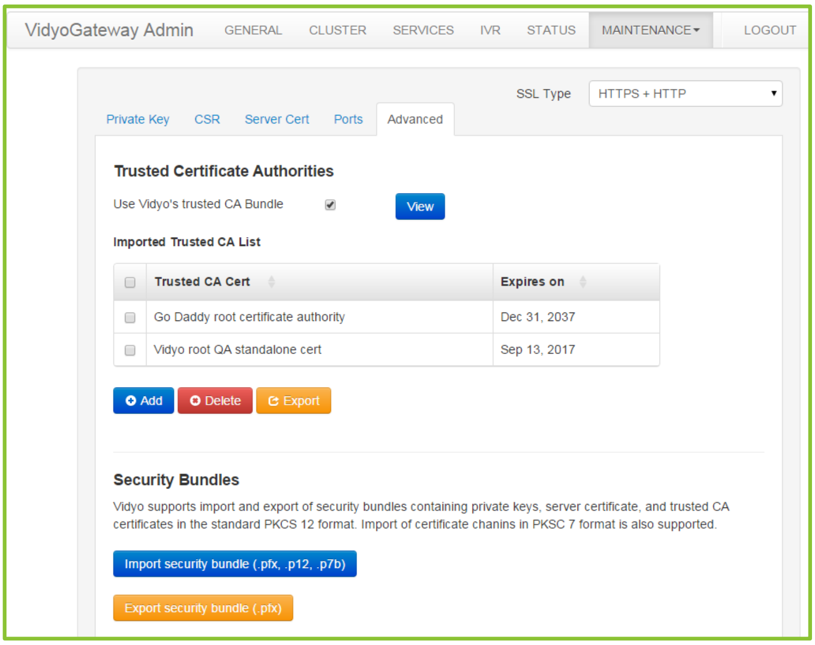
   For more information, see [Logging in to the Admin Portal.]()

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Advanced* subtab.



SSL Type: HTTPS + HTTP

Trusted Certificate Authorities

Use Vidyo's trusted CA Bundle ☑ View

Imported Trusted CA List

□	Trusted CA Cert	Expires on
□	Go Daddy root certificate authority	Dec 31, 2037
□	Vidyo root QA standalone cert	Sep 13, 2017

Security Bundles

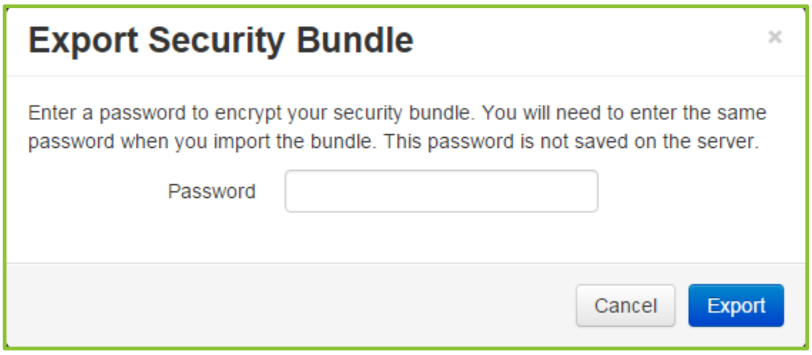
Vidyo supports import and export of security bundles containing private keys, server certificate, and trusted CA certificates in the standard PKCS 12 format. Import of certificate chanins in PKSC 7 format is also supported.

Import security bundle (.pfx, .p12, .p7b)
Export security bundle (.pfx)

4. Click **Export security bundle (.pfx)** in the Trusted Certificate Authorities section.

   The *Export Security Bundle* pop-up displays.

5. Enter a password in the **Password** field.
6. Click **Export**.



Export Security Bundle

Enter a password to encrypt your security bundle. You will need to enter the same password when you import the bundle. This password is not saved on the server.

Password

Your browser downloads a password protected file containing your current security configuration.

Enabling HTTPS on Your Vidyo Server

Note Do not use the **Enable HTTPS** button until you've completed the steps for securing your Vidyo server. Do not **Enable HTTPS Only** mode until you are certain HTTPS is working properly. For more information, see Securing Your VidyoGateway System with SSL and HTTPS.

Enabling HTTPS and HTTP

To Enable HTTPS and HTTP:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.
2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.
3. Select **HTTPS+HTTP** from the **SSL Type** drop-down.

   A *Confirmation* pop-up displays.
4. Click **Yes**.

   If the changes are applied to your Vidyo server, a system notification displays indicating that HTTPS is enabled.

   You can now browse your Vidyo server over HTTPS.
5. Browse to the VidyoGateway Admin Pages to confirm that HTTPS is working properly and that the browser does not post any security errors.

Be sure to include the HTTPS header in the URL (e.g., **`https://[FQDN]`**). Verify that HTTPS 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.

Note You can also verify your signed certificate by displaying information for it in your web browser. See the documentation that came with your web browser for information.

If your browser generates a root certificate error, first check that your operating system has the latest root certificates update applied.

6. Continue with the next procedure if you are successful browsing to your Vidyo server using HTTPS and you do not receive any browser errors.

Note If you are unable to connect to your Vidyo server over HTTPS, see Recovering from an HTTPS Failure.

Enabling HTTPS Only

To Enable HTTPS Only:

1. Log in to the Admin portal using your System Console account.

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

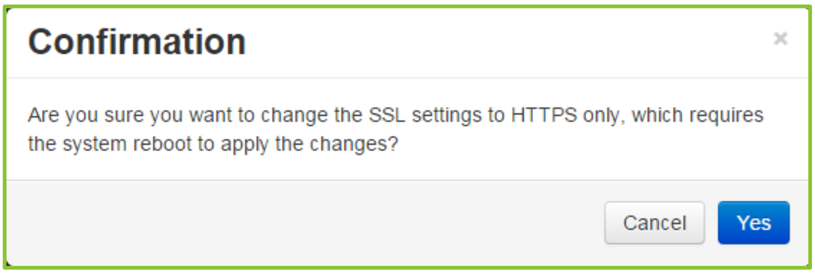
   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Select **HTTPS Only** from the **SSL Type** drop-down.

   A *Confirmation* pop-up displays.



Confirmation

Are you sure you want to change the SSL settings to HTTPS only, which requires the system reboot to apply the changes?

4. Click **Yes**.

   If the changes are applied to your Vidyo server, a system notification displays indicating that HTTPS Only is now enabled.

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 3. Configuring Your Server.

Configuring Your Vidyo Server's Management Interface and Port

Your Vidyo server allows 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 allowing for increased security and firewall protection.

You can move the VidyoGateway Admin Pages to the Management Interface so they are only accessible from that location.

As shown in the following table, the Management Interface is referred to by different names on the physical interface of the server and on the System Console and the VidyoGateway Admin Pages on the *MAINTENANCE > SECURITY > Ports* subtab:

Physical Interface	System Console and VidyoGateway Admin Page Ports Tab
GB1	PRODUCTION
GB2	MANAGEMENT

Note If the Management Interface is enabled, SNMP is only available on the Management Interface.

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

The following sections show you how to enable the management interface in the system console and then move the VidyoGateway Admin Pages to the Management Interface.

Enabling the Management Interface in the System Console

To enable the Management Interface, see Configuring the IPv4 Management Interface.

Moving Your VidyoGateway Admin Page to the Management Interface

Now you can explicitly move access to your VidyoGateway Admin Pages to the Management Interface.

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

To move your VidyoGateway Admin Page to the Management Interface:

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

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

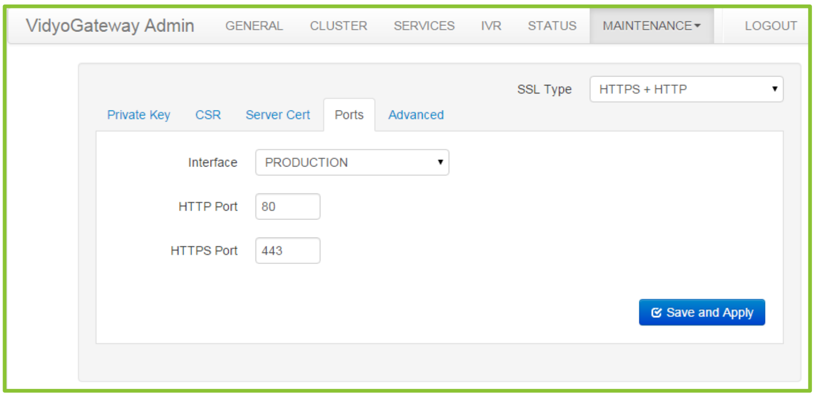
   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Ports* subtab.

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

   SSL Type: HTTPS + HTTP
   Interface: PRODUCTION
   HTTP Port: 80
   HTTPS Port: 443

   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**.

Note After clicking **Save and Apply**, your changes are applied immediately; therefore, if your *VidyoGateway Admin Page* is moved, you are logged out and it is no longer accessible from the Production Interface (PRODUCTION).

Configuring OCSP

Enabling OCSP from the VidyoGateway

To enable OCSP in the VidyoGateway:

1. Log in to the Admin portal using your System Console account.

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

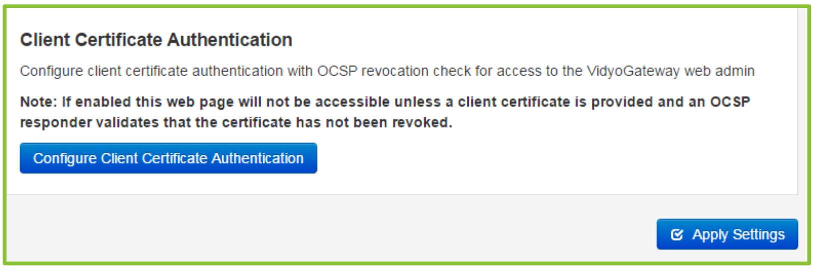
   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.

3. Click the *Advanced* subtab.

4. Click the **Configure Client Certificate Authentication** button in the Client Certificate Authentication section.

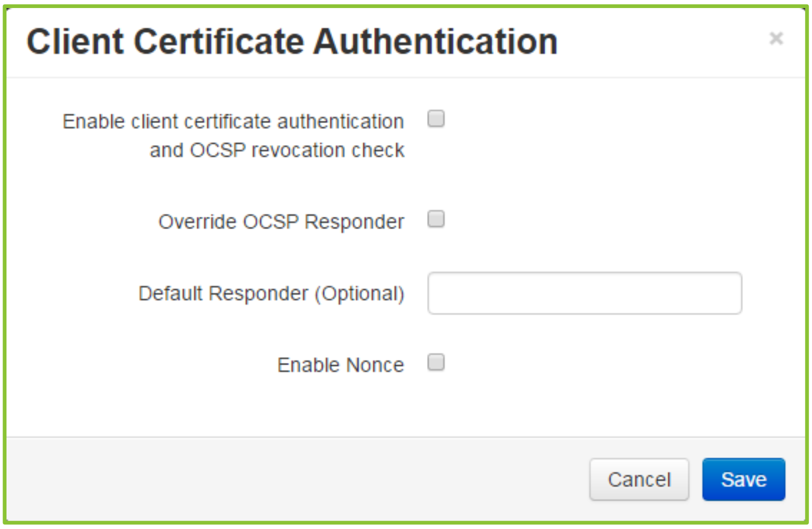


Client Certificate Authentication

Configure client certificate authentication with OCSP revocation check for access to the VidyoGateway web admin

Note: If enabled this web page will not be accessible unless a client certificate is provided and an OCSP responder validates that the certificate has not been revoked.

   The *Client Certificate Authentication* pop-up displays.



Client Certificate Authentication

Enable client certificate authentication and OCSP revocation check □

Override OCSP Responder □

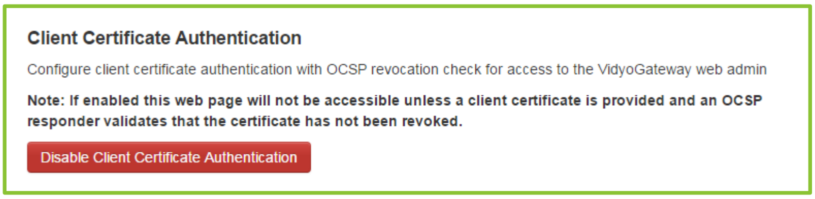
Default Responder (Optional)

Enable Nonce □

5. Select the **Enable client certificate authentication and OCSP revocation** check.

6. Select the **Override OCSP Responder** checkbox and and enter the **IP or FQDN address** of the new responder in **Default Responder (optional)** field if you want to override the OCSP responders specified in the Client, Intermediate, and Root certificate.
7. Select **Enable Nonce** if necessary.
8. Click **Save**.
9. Click **Apply Settings** in the Client Certificate Authentication section.

   The **Configure Client Certificate Authentication** button changes to the **Disable Client Certificate Authentication** button.

   Client Certificate Authentication

   Configure client certificate authentication with OCSP revocation check for access to the VidyoGateway web admin

   Note: If enabled this web page will not be accessible unless a client certificate is provided and an OCSP responder validates that the certificate has not been revoked.

   For VidyoGateway, this will immediately require OCSP certificate verification for the VidyoGateway Admin Pages.

Note The server must have access to the OCSP Responders specified in the certificates or the overridden Responder. Also, be sure that the configured DNS server can resolve the FQDNs of all the OCSP Responders.

Disabling OCSP from the VidyoGateway

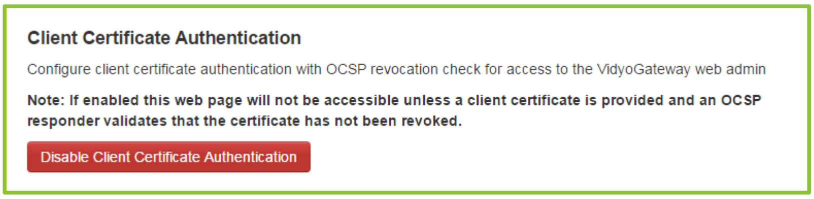
To disable OCSP from the VidyoGateway:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.
2. Navigate to *MAINTENANCE > SECURITY*.

   The *MAINTENANCE > SECURITY > Private Key* page displays by default.
3. Click the *Advanced* subtab.
4. Click the **Disable Client Certificate Authentication** button in the Client Certificate Authentication section.

   Client Certificate Authentication

   Configure client certificate authentication with OCSP revocation check for access to the VidyoGateway web admin

   Note: If enabled this web page will not be accessible unless a client certificate is provided and an OCSP responder validates that the certificate has not been revoked.

A confirmation message displays at the top of the window stating “Disabled client certification authentication.”

The **Disable Client Certificate Authentication** button changes to the **Configure Client Certificate Authentication** button.

Disabling OCSP from the System Console

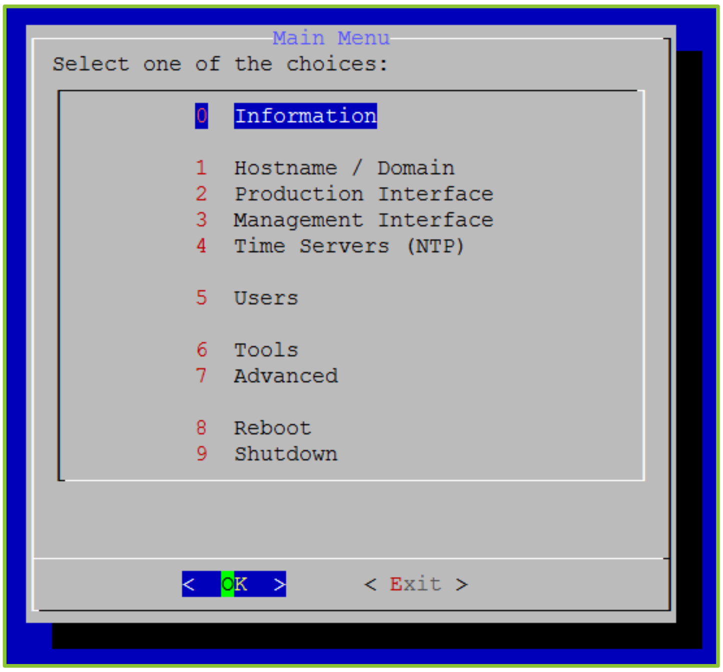
In the event that you are locked out of the VidyoGateway Admin Pages, follow the steps below to disable OCSP.

To disable OCSP from the System Console:

1. Log in to the Admin portal using your System Console account.

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

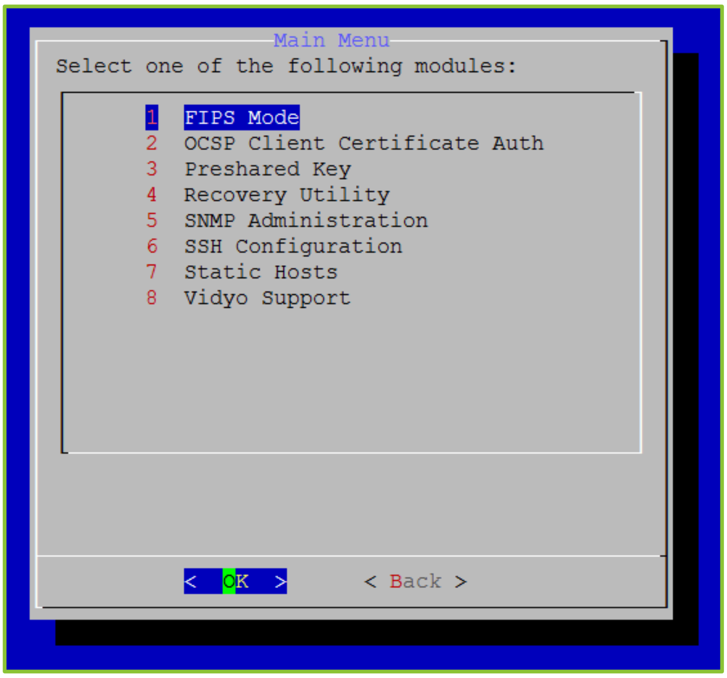
   The Main Menu displays.



```
                    Main Menu
Select one of the choices:

          0  Information

          1  Hostname / Domain
          2  Production Interface
          3  Management Interface
          4  Time Servers (NTP)

          5  Users

          6  Tools
          7  Advanced

          8  Reboot
          9  Shutdown


        <  OK  >          < Exit >
```

2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**.

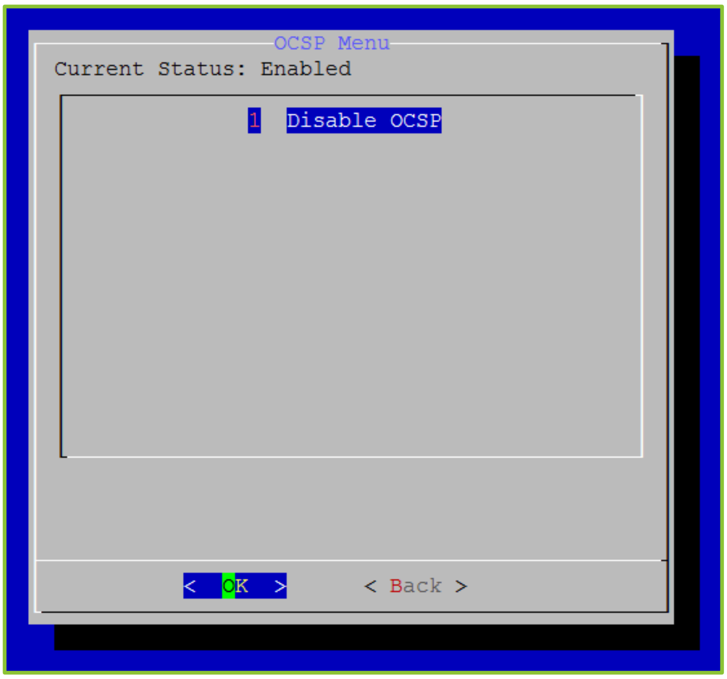
The Main Menu for the Advanced configuration displays.



```
Main Menu
Select one of the following modules:

        1   FIPS Mode
        2   OCSP Client Certificate Auth
        3   Preshared Key
        4   Recovery Utility
        5   SNMP Administration
        6   SSH Configuration
        7   Static Hosts
        8   Vidyo Support

            <  OK  >         < Back >
```

4. Enter **2** to select the OCSP Client Certificate Auth option.
5. Press the **Enter** key to select **OK**.

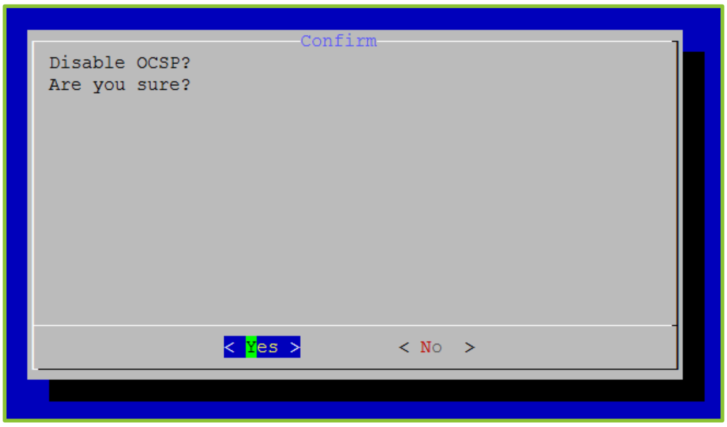
The OCSP Menu displays.



```
OCSP Menu
Current Status: Enabled

                1   Disable OCSP

            <  OK  >         < Back >
```

6. Enter **1** to select the Disable OCSP option.
7. Press the Enter key to select OK.

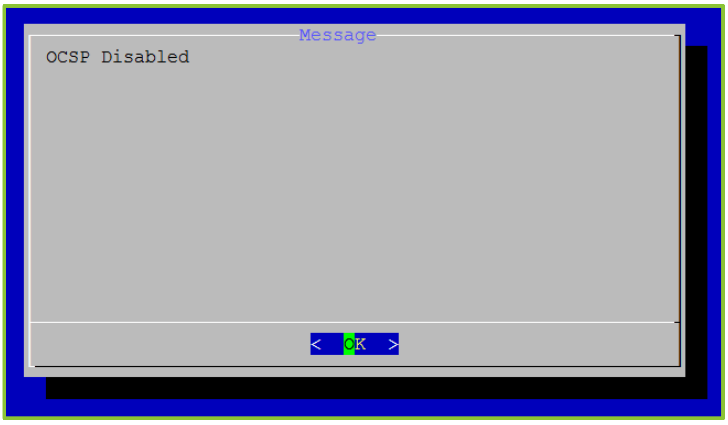
   A confirmation prompt displays.



```
Disable OCSP?
Are you sure?
```

8. Press the Enter key to select Yes.

   A message displays stating “OCSP Disabled.”



```
OCSP Disabled
```

9. Press the Enter key to select OK.

   The OCSP Menu displays.

Upgrading Your VidyoGateway

When you receive a software update from Vidyo, you install it using the *UPGRADE* page.

Note Once the VidyoGateway is upgraded, a downgrade is not possible.

For specific information about upgrading your VidyoGateway, refer to the VidyoGateway Release Notes for your corresponding software release version.

For information about upgrading your entire VidyoConferencing system, refer to the VidyoConferencing Administrator Guide.

To upgrade your VidyoGateway:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

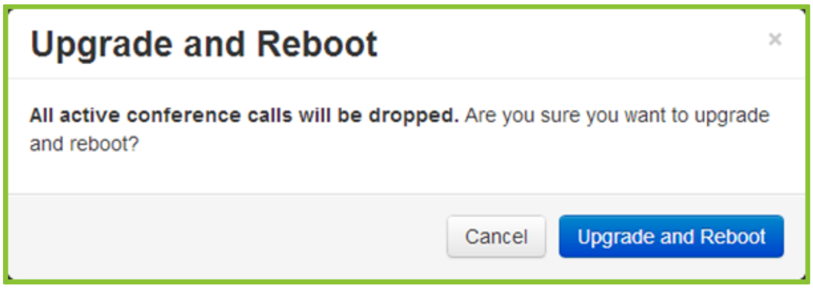
2. Navigate to *MAINTENANCE > UPGRADE.*

   The current software version is shown in the **Software Version** field.

3. Click **Choose File** to locate the VidyoGateway installation file.

4. Click **Upgrade and Reboot**.

   The *Upgrade and Reboot* pop-up displays to inform you that the change drops all of the active conference calls on your VidyoGateway server.



Upgrade and Reboot

All active conference calls will be dropped. Are you sure you want to upgrade and reboot?

5. Click **Upgrade and Reboot** to confirm.

   After your VidyoGateway server reboots, return to the *Maintenance > Upgrade* tab and confirm that the upgraded software version is the one currently being used by your system.

Shutting Down or Rebooting Your VidyoGateway

You can either shutdown or reboot your VidyoGateway server manually using the *SHUTDOWN / REBOOT* page.

Shutting Down Your VidyoGateway Server

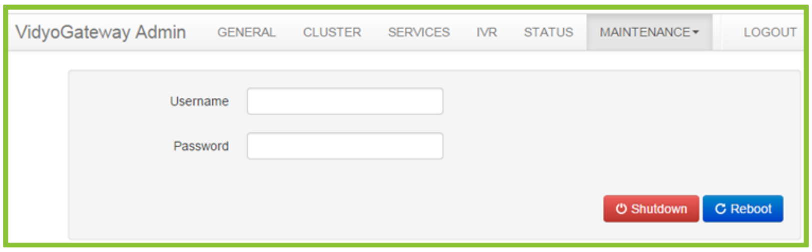
To shut down your VidyoGateway server:

1. Log in to the Admin portal using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

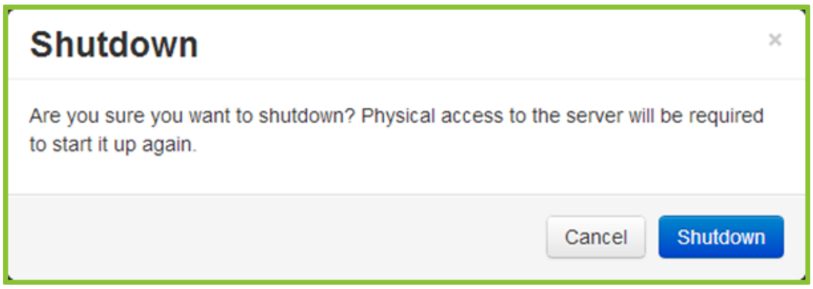
2. Navigate to *MAINTENANCE > SHUTDOWN / REBOOT.*



3. Enter your username and password.

4. Click **Shutdown**.

   The *Shutdown* pop-up displays to inform you that you will need physical access to the server in order to start your VidyoGateway server up again. Shutting down certainly drops all of the active conference calls on your VidyoGateway server as well.



Shutdown

Are you sure you want to shutdown? Physical access to the server will be required to start it up again.

5. Click **Shutdown** to confirm.

Rebooting Your VidyoGateway Server

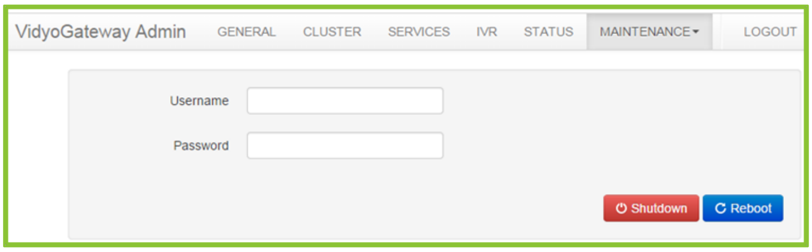
To reboot your VidyoGateway server:

1. Log in to the Admin portal using your System Console account.

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

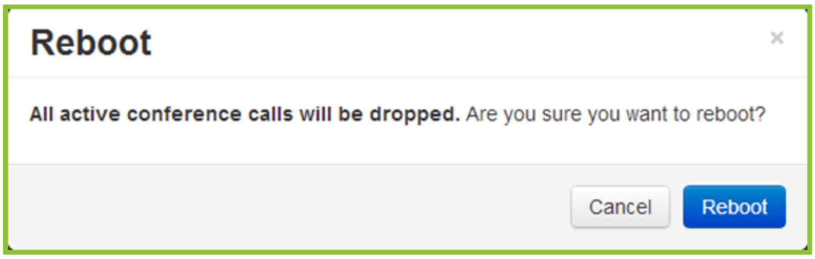
   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > SHUTDOWN / REBOOT*.



3. Enter your username and password.
4. Click **Reboot**.

   The *Reboot* pop-up informs you that the reboot drops all of the active conference calls on your VidyoGateway server.



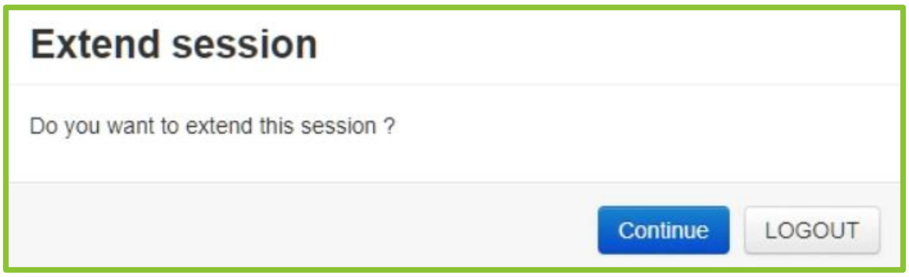
Reboot

All active conference calls will be dropped. Are you sure you want to reboot?

5. Click **Reboot** to confirm.

Extending Your VidyoGateway Session

After four minutes of inactivity, the *Extend session* pop-up displays. Click **Continue** to extend your session for 15 minutes; otherwise, click **LOGOUT** to log out of your VidyoGateway.



Extend session

Do you want to extend this session ?

Logging Out of Your VidyoGateway

You can manually log out of your VidyoGateway server using the *Logout* tab.

To log out of your VidyoGateway server:

1. Log in to the Admin portal using your System Console account.

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

The *GENERAL > VidyoPortal* page displays by default.

2. Click the *LOGOUT* tab.

   You are immediately logged out of your VidyoGateway server.

6. Auditing

Your VidyoGateway can capture audit log information showing specific user activity on your server. The audit log information is downloaded in plain text format in a `.tar.gz` file.

For more information about downloading and viewing logs for debugging analysis and viewing the statistics of a single call, see Diagnostics.

Downloading Audit Logs from Your VidyoGateway

To download Audit logs from your VidyoGateway:

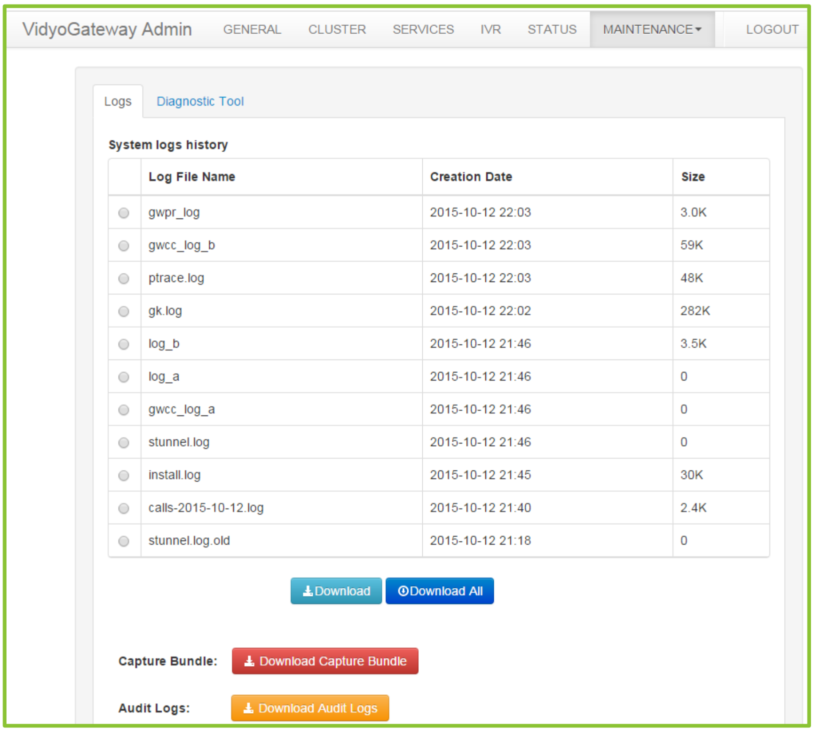
1. Log in to your VidyoGateway using your System Console account.

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

   The *GENERAL > VidyoPortal* page displays by default.

2. Navigate to *MAINTENANCE > DIAGNOSTICS*.

   The *MAINTENANCE > DIAGNOSTICS > Logs* page displays by default.



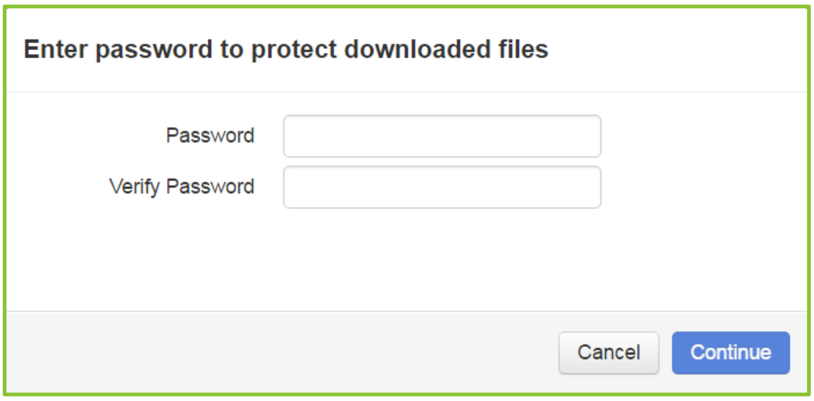
System logs history

	Log File Name	Creation Date	Size
○	gwpr_log	2015-10-12 22:03	3.0K
○	gwcc_log_b	2015-10-12 22:03	59K
○	ptrace.log	2015-10-12 22:03	48K
○	gk.log	2015-10-12 22:02	282K
○	log_b	2015-10-12 21:46	3.5K
○	log_a	2015-10-12 21:46	0
○	gwcc_log_a	2015-10-12 21:46	0
○	stunnel.log	2015-10-12 21:46	0
○	install.log	2015-10-12 21:45	30K
○	calls-2015-10-12.log	2015-10-12 21:40	2.4K
○	stunnel.log.old	2015-10-12 21:18	0

3. Select the radio button to the left of the log that needs to be downloaded.

4. Click the **Download Audit Logs** button to download the file.

The *Enter password to protect downloaded files* pop-up displays.



Enter password to protect downloaded files

Password

Verify Password

5. Enter a password in the **Password** field.
6. Re-enter the password in the **Verify Password** field.
7. Click **Continue**.

   Your browser downloads the audit log file.

Note Click the **Download All** button to download all the logs.

For more information about capturing logs, downloading single application logs for debugging, or viewing call statistics, see Diagnostics.

Understanding Audit Log Content

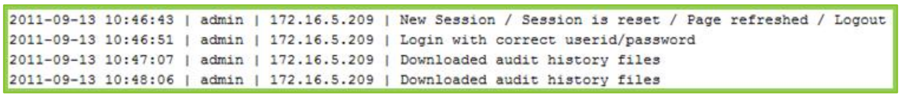
Content Captured in the Audit Log

VidyoGateway	
Login	
Login Successful	Logoff
Login Unsuccessful	
Config	
Save	Save and Apply
Services	
Add Service	Modify Service
Delete Service	

VidyoGateway	
Upgrade Gateway	
Upload and install	
Certificate	
Upload	
Restart	
Restart	Shutdown

Sample Audit Log Content

This is how an Audit log for the VidyoRouter, VidyoGateway, and VidyoManager in .txt format looks as viewed in a text editor after being decompressed. From left to right the data logged are: Timestamp, User ID, IP Address, and Description.



```
2011-09-13 10:46:43 | admin | 172.16.5.209 | New Session / Session is reset / Page refreshed / Logout
2011-09-13 10:46:51 | admin | 172.16.5.209 | Login with correct userid/password
2011-09-13 10:47:07 | admin | 172.16.5.209 | Downloaded audit history files
2011-09-13 10:48:06 | admin | 172.16.5.209 | Downloaded audit history files
```

7. Integrating VoIP Phones and IP PBXs

At times you may want to add voice-only participant(s) into a VidyoConference through an existing VoIP phone system. This section provides an overview of integrating VidyoGateway with VoIP phones and IP-based PBX systems.

Each VidyoGateway supports up to 50 simultaneous voice-only connections. Additional capacity can be achieved by clustering VidyoGateways (as described in the previous section).

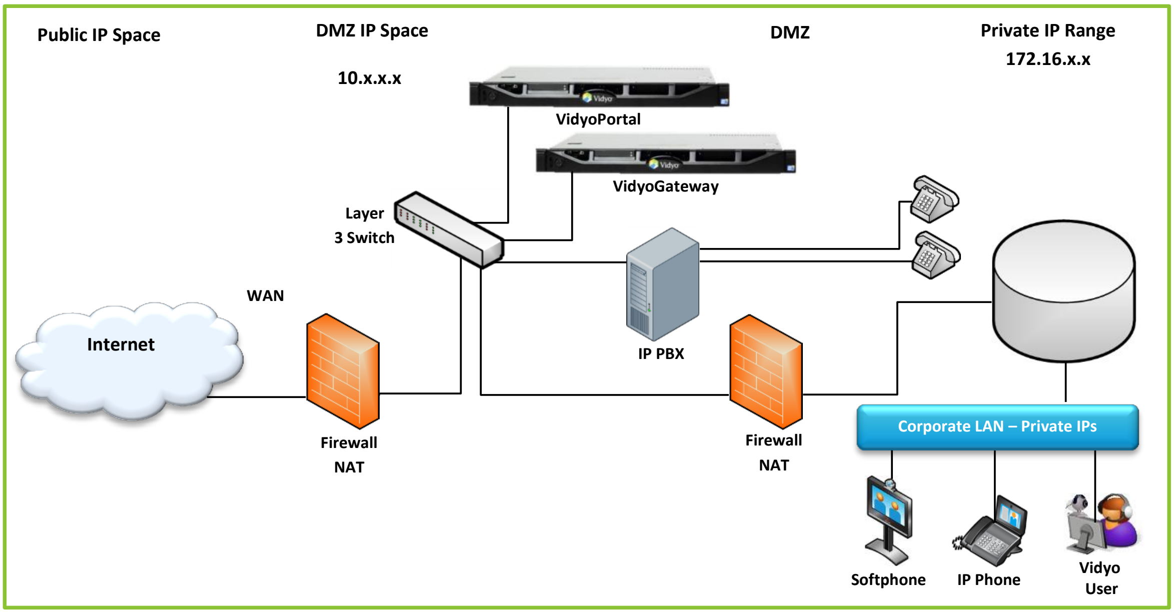
The VidyoGateway supports G.711 and G.722 (narrowband and wideband) audio codecs commonly used by VoIP systems, and the SPEEX codec used on the Vidyo side. The VidyoGateway supports H.323 and SIP signaling as well as Vidyo's signaling format, which is based on SIP but enhanced to enable additional capabilities.

As calls are placed in either direction, the VidyoGateway performs transcoding between codecs, converts signaling, and enables Vidyo endpoints and VoIP phones to participate in the same conference or point-to-point call.

For more detailed information about how to integrate VoIP phones and IP PBXs, refer to *Integrating VoIP Phones and IP PBX's with VidyoGateway* Vidyo Technical Note. This Technical Note provides details on SIP trunk configuration using the Trixbox CE and the Cisco Unified Call Manager (CUCM).

Network Topology

The diagram below illustrates a typical network topology for VoIP integration with VidyoConferencing. Elements include VidyoPortal™, VidyoRouter, VidyoGateway, an IP PBX, analog POTS phones, VoIP soft phones, dedicated IP phones, VidyoDesktop™, and VidyoRoom endpoints.



Connecting to VidyoConferences from VoIP Phones

If you are using a soft phone or IP phone that supports the ability to place calls directly using a SIP dial string, you can call into a VidyoConference directly (without needing an IP PBX). The SIP dial string must include three components:

- The voice-only service prefix of the VidyoGateway.
- The extension of the endpoint or meeting room you are calling.
- The address of the VidyoGateway.

For example: This dial string 91234@10.10.99.1 would route a voice call (9) to extension 1234 to the VidyoGateway at IP address 10.10.99.1. Depending on the configuration of the VidyoGateway service prefix, the call connects to either the Vidyo user’s meeting room or ring the endpoint with extension 1234 directly.

Connecting to VidyoConferences Via an IP PBX

IP PBX systems allow for various call routing rules that determine how calls are connected. There are many different possible permutations for setting up how calls are connected from telephone to the VidyoConference. This section describes two common methods for call routing on the IP PBX.

- Connecting to an IP PBX with a Direct Dial Number: With this method, the IP PBX is configured with a dedicated PSTN telephone number that is exclusively used for voice participants joining VidyoConferences. This number brings callers into an IVR (interactive voice response) system hosted on the IP PBX that prompts them for the Vidyo user extension. Once the caller has entered the extension, the IP PBX forwards the call out the SIP trunk to the VidyoGateway. Ideally, the extension entered at the IVR prompt matches the destination Vidyo extension and the IP PBX prepends the VidyoGateway voice-only prefix.
- Connecting to an IP PBX with an Extension Dial: A second method is to treat each Vidyo user as another extension—similar to a desk phone extension. You do this by assigning a block of extensions to the VidyoGateway trunk. When creating a user account on the Vidyo system, each user is assigned one of the valid extensions. When users then call into the PBX from a telephone and have the option to enter an extension, they can enter one of the Vidyo extensions which then routes the call through the SIP trunk to the VidyoGateway. The IP PBX is configured to route any extension in this range to the VidyoGateway with the VidyoGateway voice-only prefix prepended.

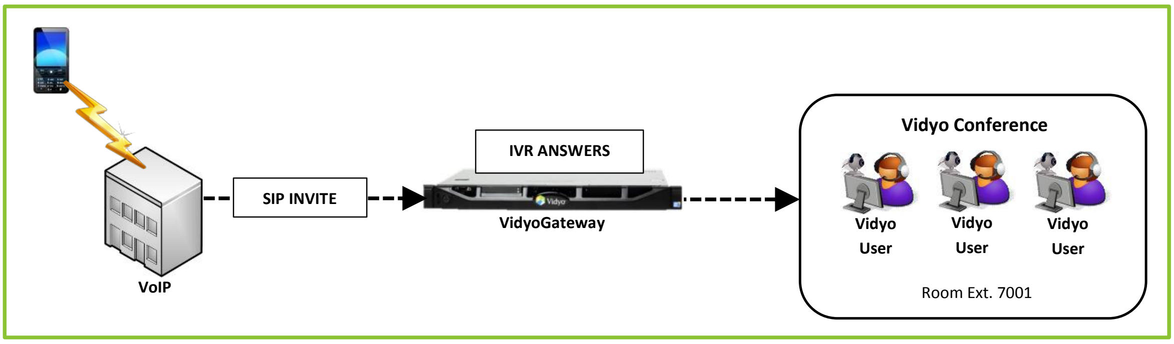
8. Integrating Direct Phone Calls with IVR Functionality

Phones can be used with the IVR functionality using either SIP invites from your VoIP provider or integrating VidyoGateway with your IP PBX.

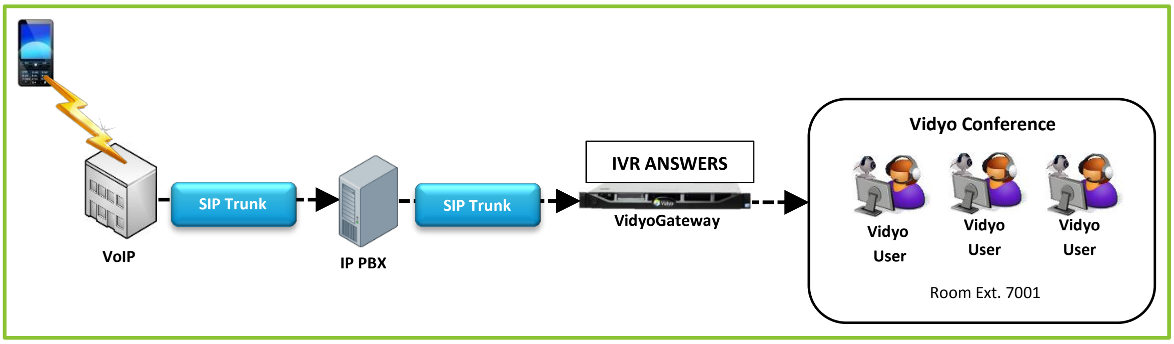
Phone Setups Using the IVR Functionality

The following diagrams provide examples of each setup when using the IVR functionality with a VoIP provider.

- This first setup shows a configuration to your VidyoGateway using SIP invites coming directly from your VoIP provider.



- This second setup shows a configuration to your VidyoGateway using a configured SIP trunk on your IP PBX.



9. Using VidyoGateway Virtual Edition (VE)

The VidyoGateway Virtual Edition (VE) allows you to enjoy the benefits of the VidyoGateway within a virtual environment. The advantages of using virtual appliances include:

- All the features and functionality of the physical appliance.
- The simplicity and efficiency of a software-based virtual appliance.
- Leveraging your investment in VMware vSphere infrastructure.

This chapter describes how to configure the VidyoGateway VE.

Understanding VidyoGateway VE Requirements

You can run multiple Virtual Edition Vidyo servers (of any combination) on the same physical host when using VidyoGateway version 3.2 and later. 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 guidelines (such as sharing physical hosts with multiple virtual machines), your virtual machines must adhere to the virtual machine configurations listed in this section.

The guidelines provided here apply to VMware ESXi 5.0 and later. In the future, as additional virtualization platforms are tested, Vidyo will provide updated guidelines.

Based on our testing, the following recommendations should be taken into account when planning a virtual infrastructure:

- 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.
- 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.

Virtual Machine Provisioning Requirements

VidyoGateway 3.5.1 determines the capacity based on the CPU Resource Reservation. When reserving resources and configuring the Virtual Machine, the configurations in the table below must be adhered to in order to ensure optimal performance:

VidyoGateway Version 3.5.1 Capacity	VM Configuration		Resource Reservation	
	RAM [GB]	Storage [GB]	CPU [GHz]	RAM [GB]
1 HD/2 SD/4 CIF/ 10 voice	2	50	2	2
2 HD/1 FHD/4 SD/8 CIF/ 20 voice	2	50	4.4	2
4 HD/2 FHD/9 SD/ 15 CIF/50 voice	6	50	8.8	6
5 HD/2 FHD/12 SD/ 25 CIF/75 voice	8	50	12	6
8 HD/4 FHD/18 SD/ 50 CIF/100 voice	12	50	20	12

VidyoGateway Version 3.5.1 Capacity	VM Configuration		Resource Reservation	
	RAM [GB]	Storage [GB]	CPU [GHz]	RAM [GB]
10 HD/5 FHD/20 SD/ 50 CIF/125 voice	15	50	25	15

Note The number of vCPU should be configured as the minimum number that is necessary in order to achieve the required CPU reservation.

There is no longer a minimum host CPU speed; however, different numbers of vCPU will be required to achieve the resource reservation based on the host CPU speed.

To take advantage of the resources available in more powerful servers, multiple Virtual Edition VidyoGateways may be deployed on the same physical host. VidyoGateways of differing capacity may be added to the same cluster.

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)
- 1 Dell R620, dual Intel Xeon E5-2667 v2 3.30 GHz 8-Core, 32 GB with the following installations:
    - 2 VidyoGateway (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 VidyoGateway VE Support of VMware Features

The following list includes VMware features and explains both if and how they are currently supported by VidyoGateway VE:

□ You can store and deploy backup copies of your VidyoGateway VE appliance using vSphere’s export and import features.

□ While your VidyoGateway 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, vNIC and removing virtual hardware resources are not currently supported.

□ VidyoGateway software updates are managed in the same manner as the regular appliance. Always take snapshots (while your VidyoGateway VE appliance is powered off) before updating. For more information, see Upgrading Your VidyoGateway.

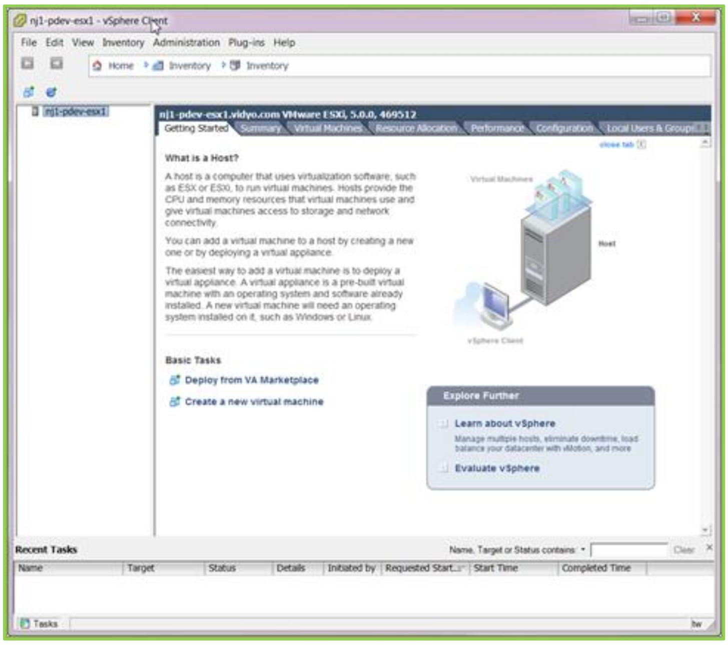
□ Advanced features, such as vMotion, high availability, fault tolerance, and distributed resource manager are not currently supported.

Installing VidyoGateway VE

Note The virtual appliance's filename reflects the appliance type and the software version. The following screenshots refer to the deployment of a VidyoGateway virtual server appliance with the latest software version at the time of release. Please refer to the *VidyoGateway Release Notes* for more detailed information regarding release versions.

To install the VidyoGateway VE:

1. Log in to the vSphere client (provided with VidyoGateway VE) on your system.



What is a Host?

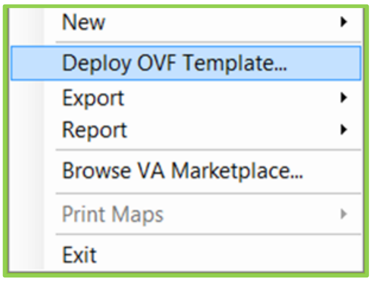
A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

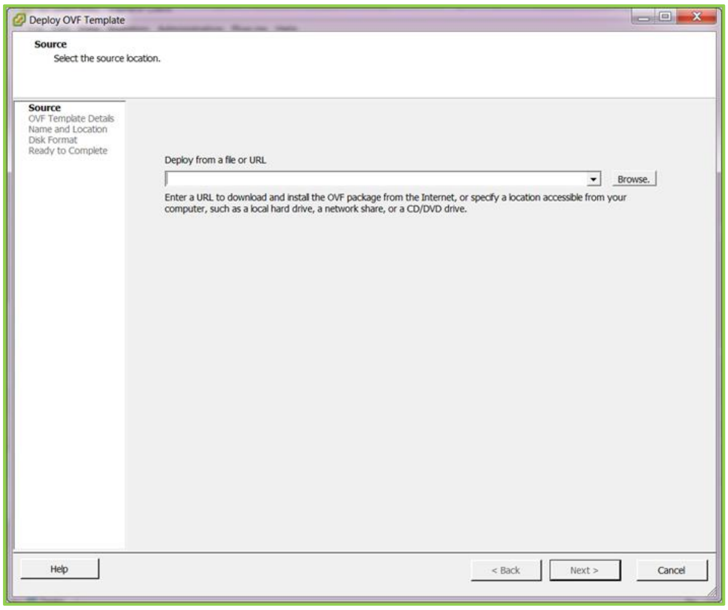
The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more

2. Select **Deploy OVF Template** from the File menu.



The *Source* dialog box opens.

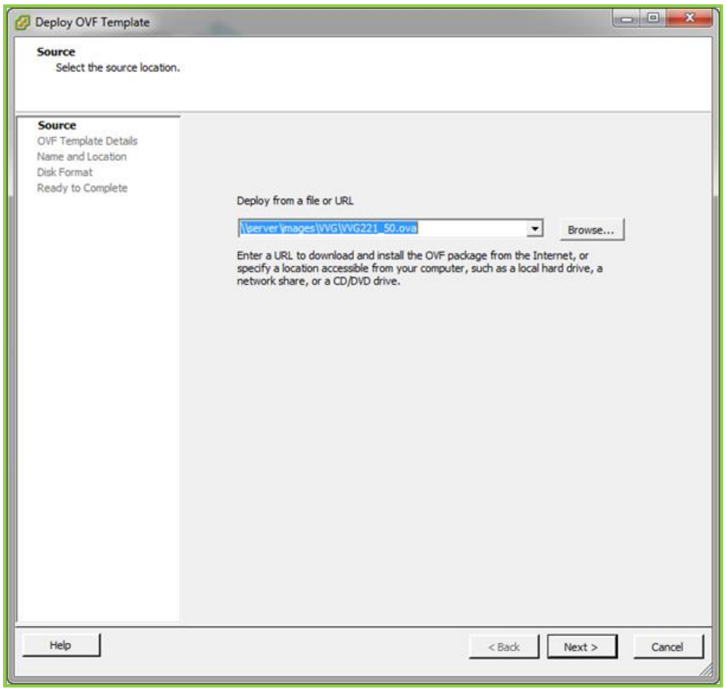


Source
Select the source location.

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

3. Click **Browse** and select the **`.ova`** file from your file system.



Source
Select the source location.

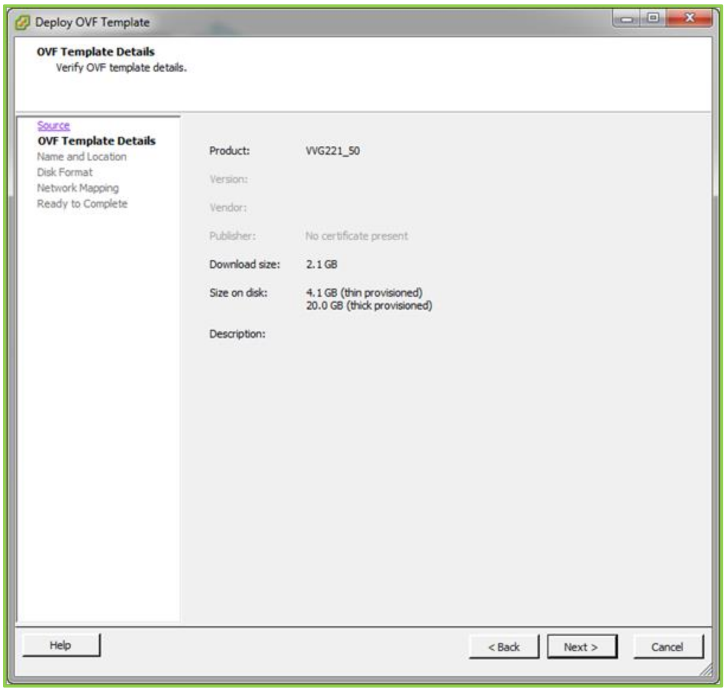
Deploy from a file or URL

\\server\images\VVG\VVG221_50.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

4. Click **Next**.

The dialog box changes to *OVF Template Details*.



OVF Template Details

Verify OVF template details.

Product: VVG221_50

Version:

Vendor:

Publisher: No certificate present

Download size: 2.1 GB

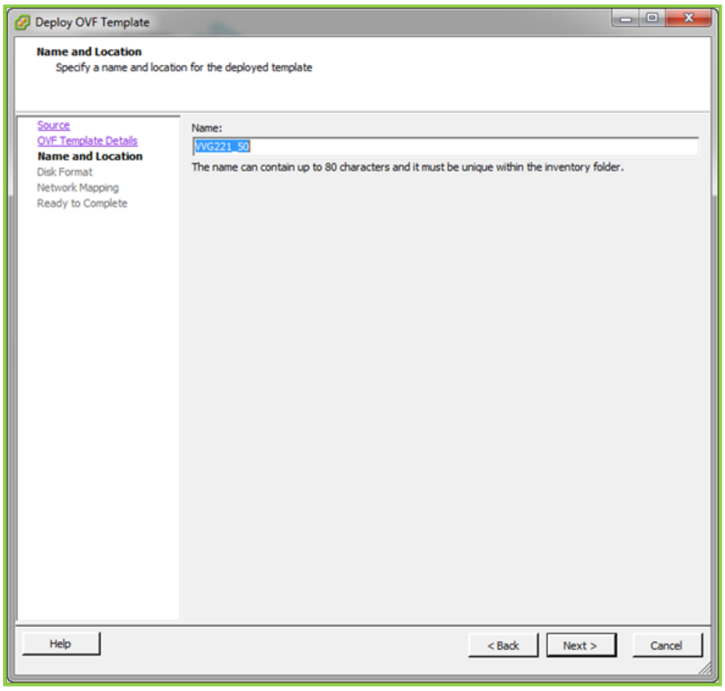
Size on disk: 4.1 GB (thin provisioned)
20.0 GB (thick provisioned)

Description:

This screen is read-only. If you need to change anything, click Back.

5. Click Next.

The dialog box changes to *Name and Location*.



Name and Location

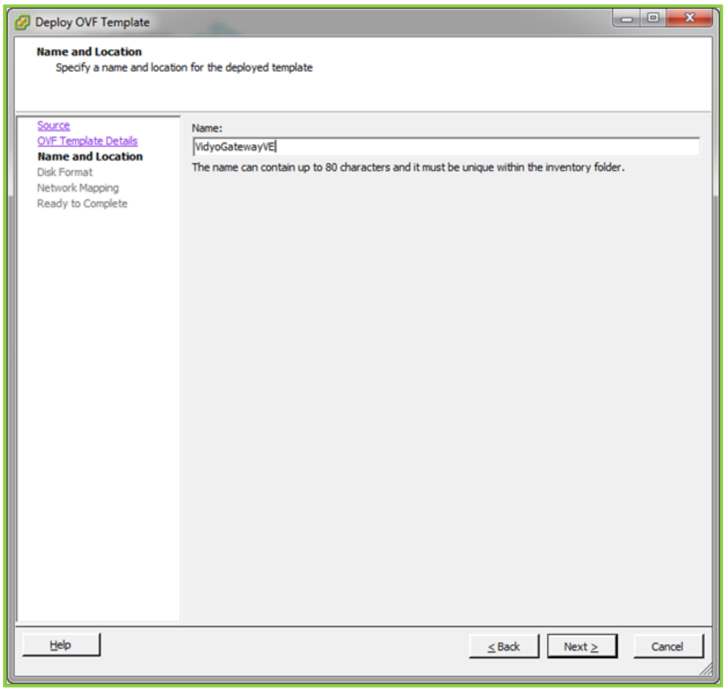
Specify a name and location for the deployed template

Name: VVG221_50

The name can contain up to 80 characters and it must be unique within the inventory folder.

The name displayed is a copy of the **.ova** filename as the vSphere default.

6. Type in a more descriptive name if desired.



Name and Location
Specify a name and location for the deployed template

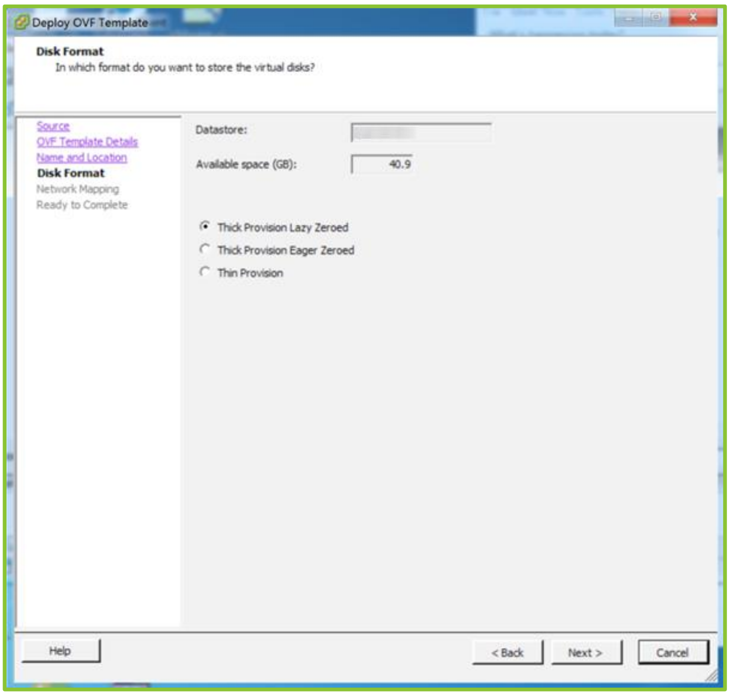
Name:
VidyoGatewayVE

The name can contain up to 80 characters and it must be unique within the inventory folder.

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.



Disk Format

In which format do you want to store the virtual disks?

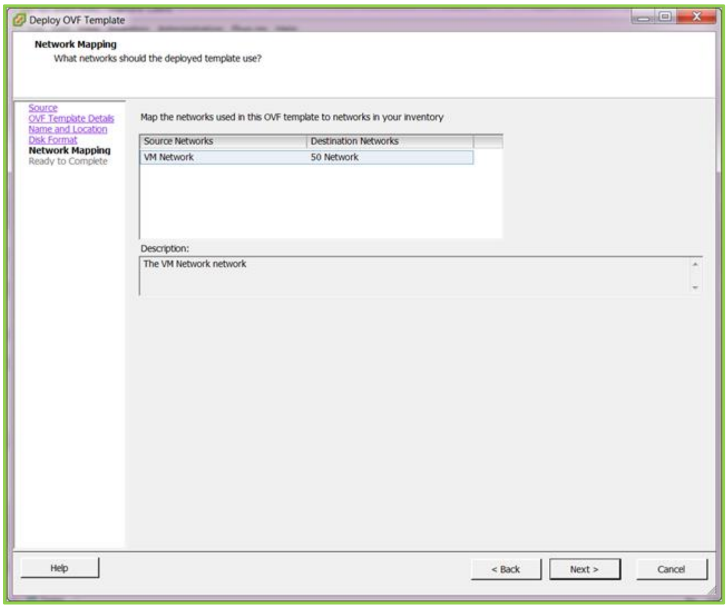
Datastore:

Available space (GB): 40.9

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

9. Click **Next**.

The dialog box changes to *Network Mapping*.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	50 Network

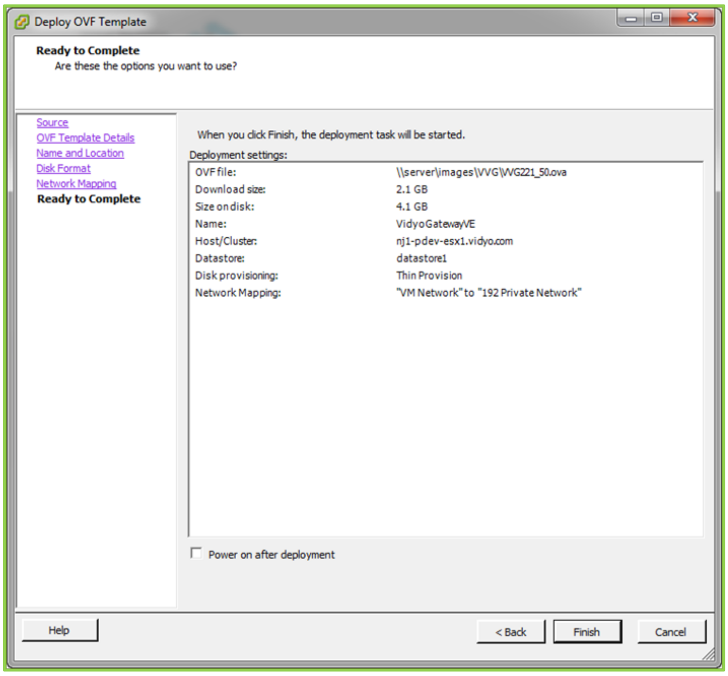
Description:

The VM Network network

10. Select the one network available for the VidyoGateway VE to use.

11. Click **Next**.

The dialog box changes to *Ready to Complete*.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

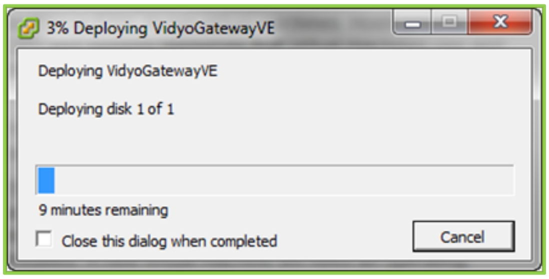
OVF file:	\\server\images\VVG\VVG221_50.ova
Download size:	2.1 GB
Size on disk:	4.1 GB
Name:	VidyoGatewayVE
Host/Cluster:	nj1-pdev-esx1.vidyo.com
Datastore:	datastore1
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "192 Private Network"

□ Power on after deployment

12. Select the **Power on after deployment** checkbox to start your VidyoGateway immediately after you take the next step.

13. Click **Finish**.

    The *Deploying VidyoGatewayVE* dialog box displays.



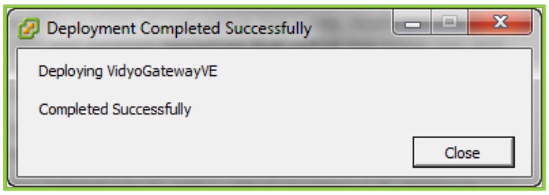
Deploying VidyoGatewayVE

Deploying disk 1 of 1

9 minutes remaining

□ Close this dialog when completed

The *Deployment Completed Successfully* dialog box displays.

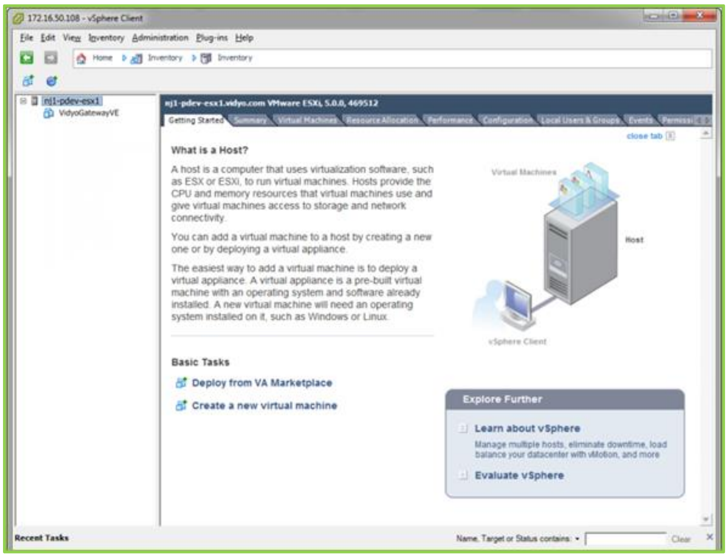


Deploying VidyoGatewayVE

Completed Successfully

14. Click **Close**.

The *vSphere Client* window displays.


172.16.50.108 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
nj1-pdev-esx1
VidyoGatewayVE
nj1-pdev-esx1.vidyo.com VMware ESXi, 5.0.0, 469512
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissi
close tab
Virtual Machines
Host
vSphere Client
Recent Tasks
Name, Target or Status contains: ▾
Clear

What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Basic Tasks

- Deploy from VA Marketplace
- Create a new virtual machine

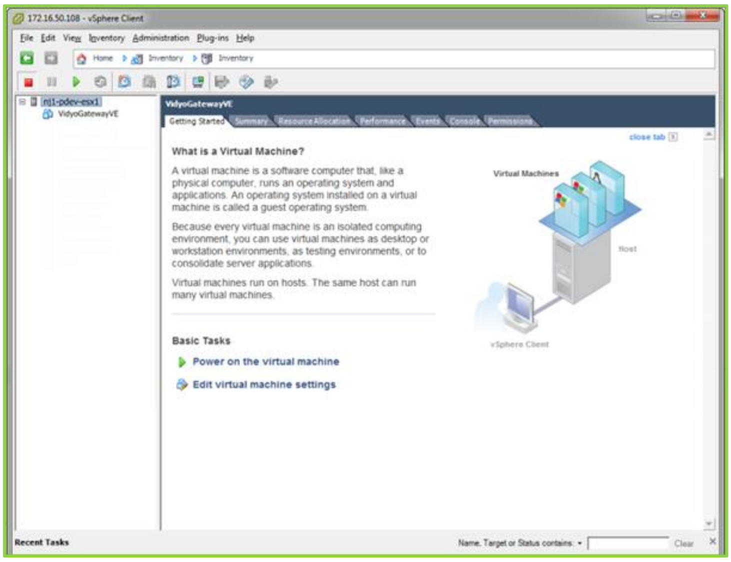
Explore Further

- Learn about vSphere

  Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more
- Evaluate vSphere

15. Click the + sign to the left of the ESXi host name.
16. Click *VidyoGateway VE* in the left-side pane.

    The tabs change.


172.16.50.108 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
nj1-pdev-esx1
VidyoGatewayVE
VidyoGatewayVE
Getting Started Summary Resource Allocation Performance Events Console Permissions
close tab
Virtual Machines
Host
vSphere Client
Recent Tasks
Name, Target or Status contains: ▾
Clear

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

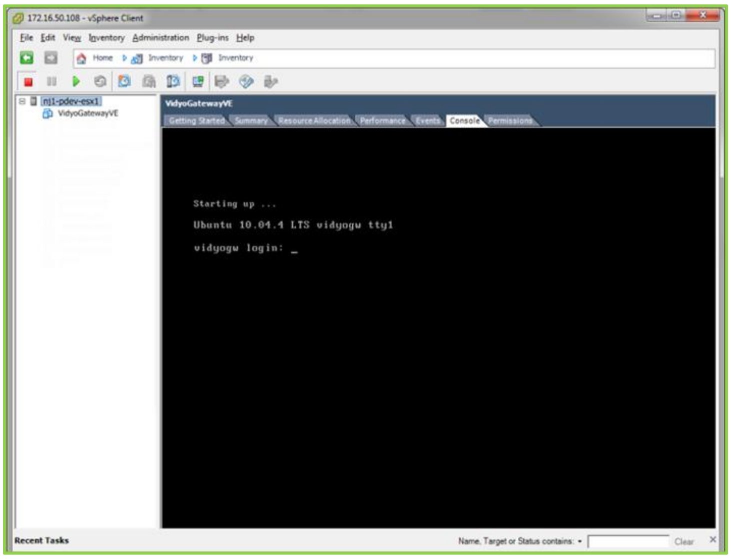
Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

- Power on the virtual machine
- Edit virtual machine settings

17. Click the *Console* tab.

The VidyoRouter VE System Console displays.



```
Starting up ...

Ubuntu 10.04.4 LTS vidyogw tty1

vidyogw login: _
```

18. Log in as Admin.

    If you haven't changed your password yet, use the default password we have provided for you.

    You can now configure your VidyoGateway VE network settings as described in Viewing Application and System Information and in the "Adding VidyoGateways" section in the *VidyoConferencing Administrator Guide*.

Appendix A. Definitions

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

For more standard VidyoConferencing definitions, refer to the *VidyoConferencing Administrator Guide.*

- AGC – Automatic Gain Control. In a VidyoConference with VidyoGateway version 2.2, AGC automatically controls the gain of a signal by reducing the volume if the signal is strong and raising it when the signal is weaker, thereby keeping the audio output at a near constant level.
- AVC – Advanced Video Coding. AVC is also known as MPEG-4 Part 10 or H.264. See also Protocol (H.264/AVC).
- CIF Protocol – Common Intermediate Format. A video format used in videoconferencing systems that supports both NTSC and PAL signals. CIF is part of the ITU H.261 videoconferencing standard. It specifies a data rate of 30 frames per second (fps), with each frame containing 288 lines and 352 pixels per line.
- Codec – Short for coder/decoder or, because codecs are commonly used for compression, compressor/decompressor; a codec is any technology for compressing and decompressing data. Some popular codecs for computer video include MPEG, Indeo, and Cinepak.
- Cluster – A group of VidyoGateways used for increased capacity. One VidyoGateway is designated the Controller. In addition to handling calls itself, the Controller also controls a number of Standby VidyoGateways.
- Controller – A VidyoGateway that in addition to handling calls allocates capacity for a number of Standby VidyoGateways.
- Firewall – A system designed to prevent unauthorized access to or from a private network.
- Gatekeeper – A management tool for H.323 multimedia networks. Depending on the demands of the specific network, the gatekeeper oversees authentication, authorization, telephone directory, and PBX (private branch exchange) services, as well as call control and routing.
- HD (High Definition) – A video format with a 1280 x 720 resolution and a 16 to 9 aspect ratio. (There are other HD formats but this is the one referred to in this document.)
- Legacy System – In this guide, any videoconferencing system based on the SIP or H.323 protocol.
- MCU – Multipoint Control Unit. A device in videoconferencing that connects two or more audiovisual terminals together into one single videoconference call. The MCU collects information about the capabilities of the systems at each of the videoconference endpoints and sets the conference to the lowest common denominator so that everyone can participate.
- NAT – Network Address Translation. An Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for

external traffic. A NAT box located where the LAN meets the Internet and makes all necessary IP address translations.

- Prefix – A unique identifier for a call service.
- Point-to-Point Call (Direct Call) – A videoconference that takes place between just two users. No additional participants can join a point-to-point call.
- Protocols
  - H.235 – The H.3xx encryption protocol over H.323 connections for secured videoconferencing. Vidyo supports AES 128 bits.
  - H.239 – The standard used in H.323 and H.320 videoconferencing that enables two simultaneous media channels in a single video conference. The second channel is used for data presentation. For example, it's possible to see a speaking person within a main video screen and see their computer screen with diagrams, documents, screenshots, and so on.
  - H.245 – A control signaling protocol for the exchange of end-to-end messages between communicating H.323 and H.234 endpoints/terminals.
  - H.264/AVC – Also called Advanced Video Coding (AVC). A simple and straightforward video codec that provides enhanced compression performance and a network-friendly video representation.
  - H.264/SVC – Also called Scalable Video Coding. A new video compression standard that enables a video stream to be broken into multiple resolutions, quality levels, and bit rates. Vidyo uses this technology in its video conferencing products.
  - H.323 – A standard that addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences. The H.323 protocol provides audio-visual communication sessions on any packet network.
  - SIP – Session Initiation Protocol. A signaling protocol used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP).
- QoS – Quality of Service. A networking term that specifies a guaranteed throughput level.
- SD (Standard Definition) – A video format with a 640 x 360 resolution and a 16 to 9 aspect ratio. (Traditional broadcast television SD has a different format. The definition given here is the one referred to in this document.) Starting with version 2.2, VidyoGateway provides a better SD experience by supporting an adaptive aspect ratio for SD calls. With this feature, the aspect ratio automatically changes as needed when you are in an SD call.
- Standby VidyoGateway – One of a cluster of VidyoGateways that are controlled by a single Controller VidyoGateway.
- TCS4 – Terminal Control String. A special routing method for incoming H.320 video calls. TCS4 allows direct inward dialing (DID) to an endpoint on the IP network through the gateway when DID is not available. H.323 endpoints on the IP network register with the gatekeeper using extension numbers. When an ISDN terminal dials one of the gateway phone numbers followed

by a TCS4 extension, the call is routed directly to the corresponding IP endpoint registered with that extension.

Appendix B. Legacy TCS4 Delimiters

	TCS4 Delimiter	Alphanumeric	Dialing String
Polycom	##	Yes	192.168.1.110##35001
Polycom PVX v8.0.4	@		035001@192.168.1.110
LifeSize	##	Yes	192.168.1.110##35001
Tandberg MXP	(Does not use a delimiter1.)		35001@192.168.1.110
Tandberg C series	(Does not use a delimiter2.)		35001@192.168.1.110
Tandberg 2500 vB3.9			192.168.1.110,035001
Tandberg MCU 8+8			192.168.1.110,035001
Sony	#	No	192.168.1.110#35001
Codian	!	No	192.168.1.110!35001

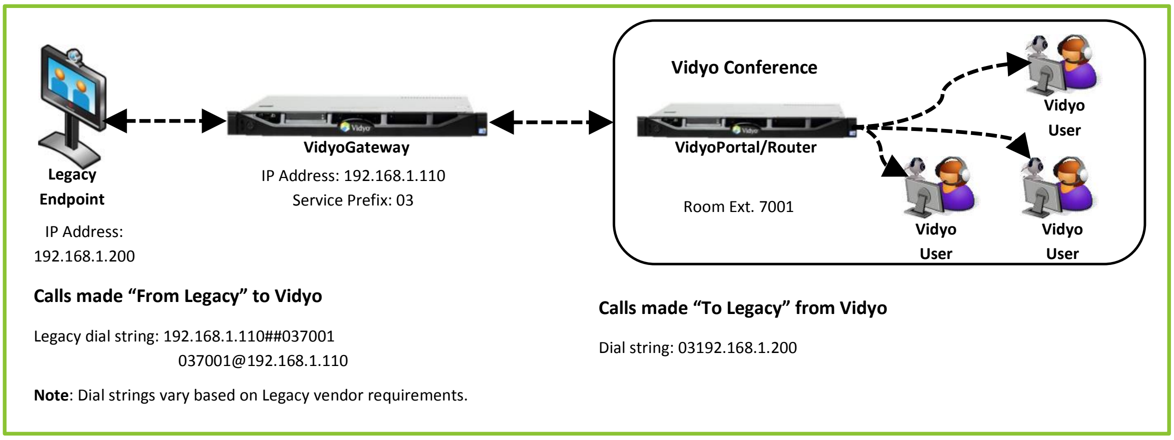
[1] The Tandberg MXP platform doesn't support TCS4 delimiters when dialing over IP. To dial from a Tandberg MXP into a VidyoConference, dial the VidyoGateway service prefix followed by the Vidyo user's extension then @ and the IP address of the VidyoGateway as shown in the Tandberg MXP Dialing String entry shown previously.

[2] As of release version TC4.1.2, it's now possible to dial using the format name@domain or name@IPAdress without being registered to a gatekeeper.

Note Vidyo users must use a comma as the delimiter when dialing into Legacy MCUs and/or border controllers acting as H.323 gatekeepers. For more information on dialing summaries, see the next chapter.

Appendix C. Deployment Examples

Deployment Example 1: Adding a Legacy user to a VidyoConference OR a single Legacy user calling into a VidyoConference



Calls made “From Legacy” to Vidyo

Legacy dial string: 192.168.1.110##037001
037001@192.168.1.110

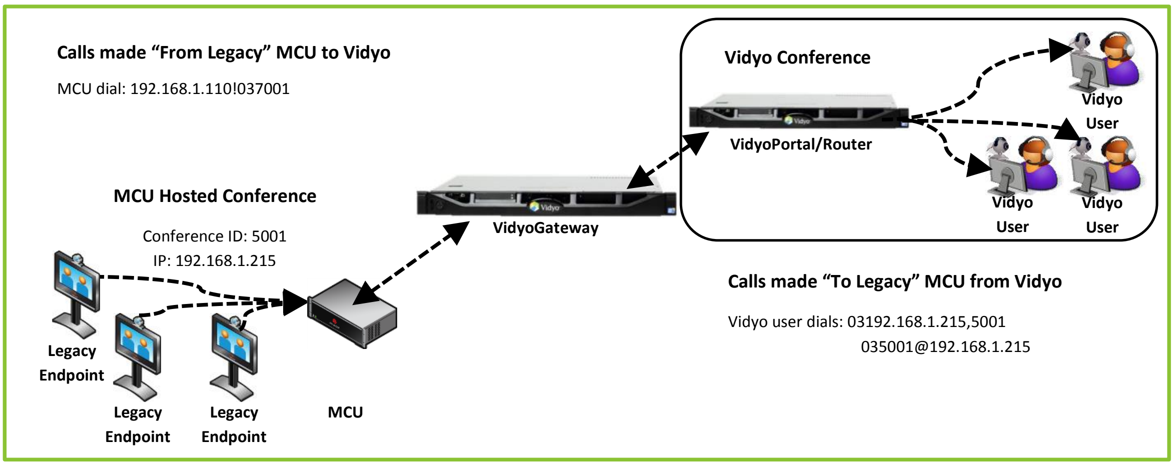
Note: Dial strings vary based on Legacy vendor requirements.

Calls made “To Legacy” from Vidyo

Dial string: 03192.168.1.200

Deployment Example 2: Legacy MCU calling into a VidyoConferencing room OR a VidyoConferencing room is calling into an MCU-hosted conference.

Note There is a single stream between the MCU and VidyoGateway.



Calls made “From Legacy” MCU to Vidyo

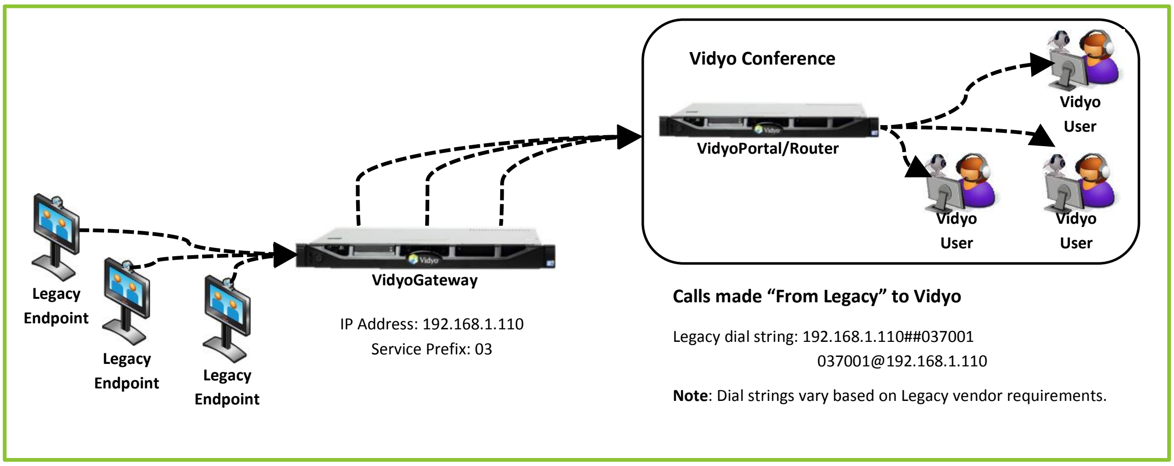
MCU dial: 192.168.1.110!037001

Calls made “To Legacy” MCU from Vidyo

Vidyo user dials: 03192.168.1.215,5001
035001@192.168.1.215

Deployment Example 3: Multiple Legacy users calling into an MCU-hosted VidyoConference.

Note the three separate video streams between the VidyoGateway and VidyoRouter. This deployment (where the call is hosted on the VidyoRouter rather than on the MCU) is the recommended deployment.

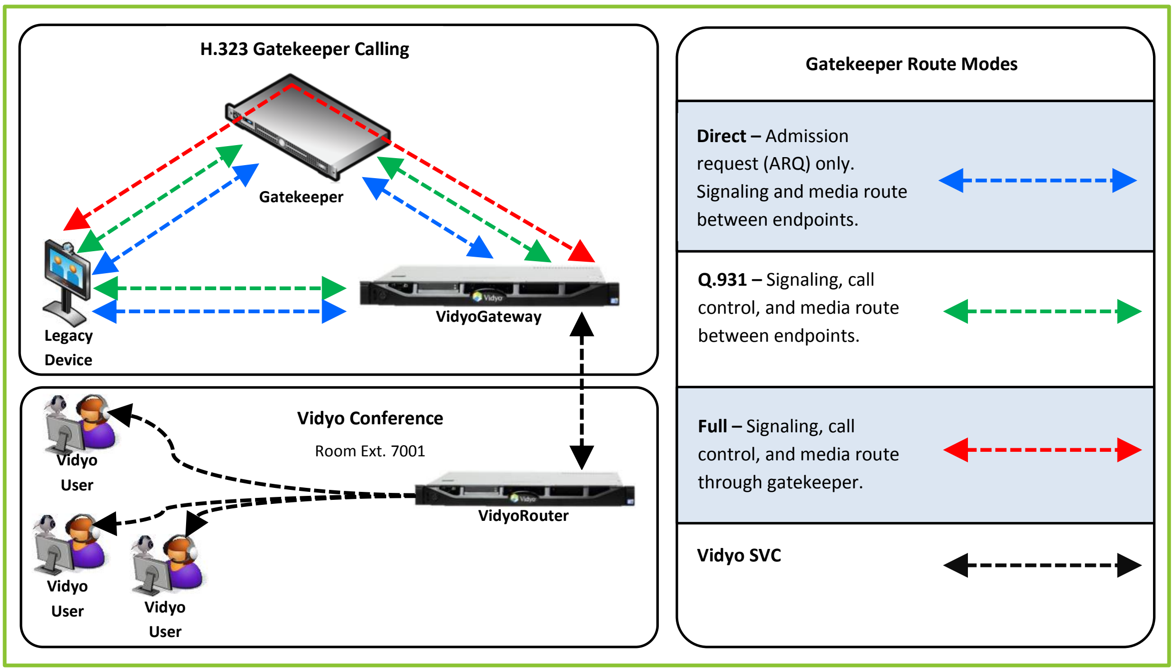


Calls made “From Legacy” to Vidyo

Legacy dial string: 192.168.1.110##037001
037001@192.168.1.110

Note: Dial strings vary based on Legacy vendor requirements.

Deployment Example 4: VidyoGateway in a deployment that has an H.323 gatekeeper.



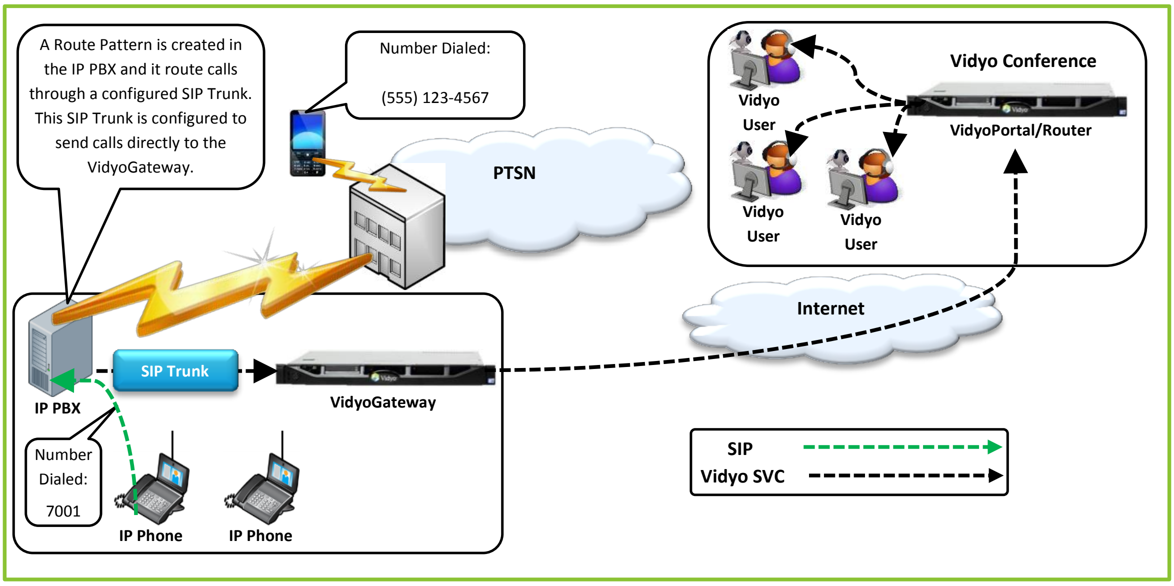
Direct – Admission request (ARQ) only. Signaling and media route between endpoints.

Q.931 – Signaling, call control, and media route between endpoints.

Full – Signaling, call control, and media route through gatekeeper.

Vidyo SVC

Deployment Example 5: Integrating Vidyo with VoIP/mobile devices/landlines in a deployment that includes an IP PBX.

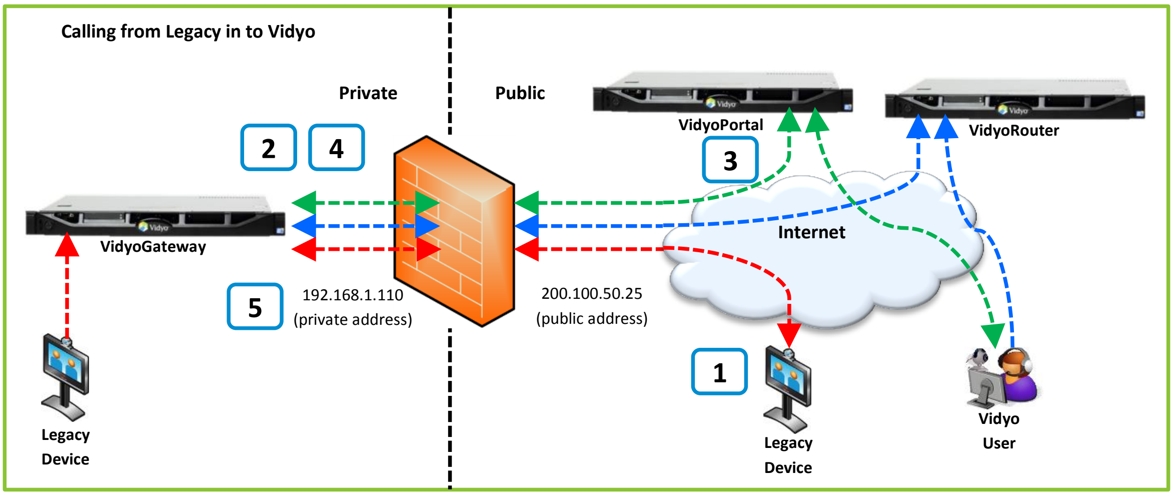


Appendix D. NAT/Firewall Traversal

There are two possibilities in which a call must traverse a firewall: when the VidyoGateway is behind a NAT/firewall and when the Legacy device is behind a firewall.

- When the VidyoGateway resides on the public network with a native public IP address and when the Legacy device is behind a NAT/firewall, the Legacy device must open the required H.323 or SIP ports (whichever are being used).
- When the VidyoGateway is behind a firewall and/or within a DMZ, you must configure your firewall with a STATIC NAT (an external IP address routed to the VidyoGateway native private address) and open the required ports in both directions.
- Configure your NAT Public IP Address. For more information, see Configuring a Public IP Address.

The following diagram illustrates the call flow from a Legacy endpoint calling Vidyo users when the VidyoGateway is behind a NAT/firewall.

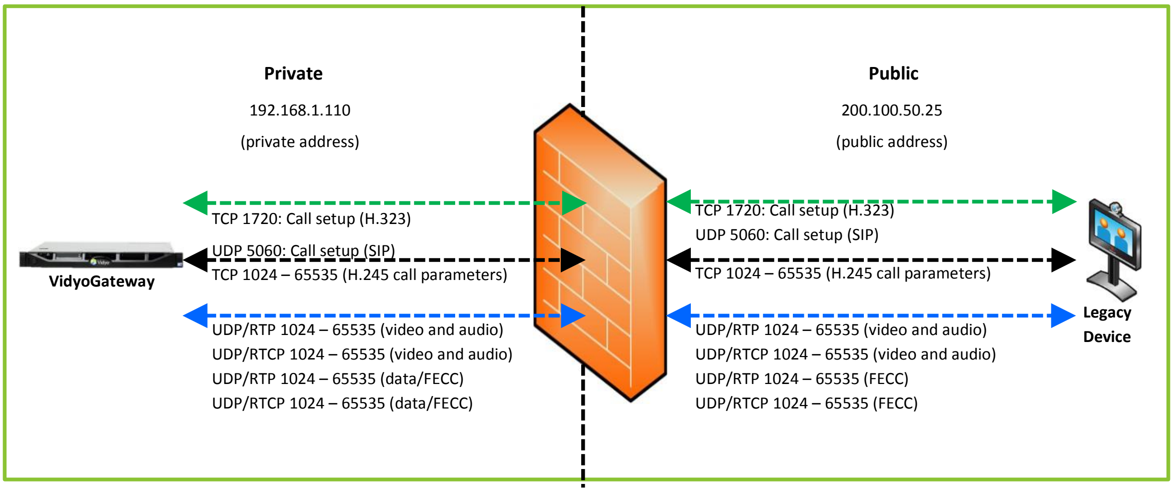


The following list explains each number in the “Calling from Legacy to Vidyo” illustration above.

1. The Legacy device calls the VidyoGateway public-facing IP address.
2. The VidyoGateway sends commands to the VidyoPortal.
3. VidyoManager (on the VidyoPortal) sends the VidyoGateway the VidyoRouter address to use for calls.
4. The VidyoGateway establishes a TCP session (17990) with the VidyoRouter. H.264 SVC media streams (audio/video) are sent over UDP between the VidyoGateway and VidyoRouter.

5. The VidyoGateway sends a connect message to the Legacy device. Capabilities are exchanged between both devices. Video and audio is negotiated and sent between the two systems.

The following diagram illustrates an H.323 firewall configured with a STATIC NAT.

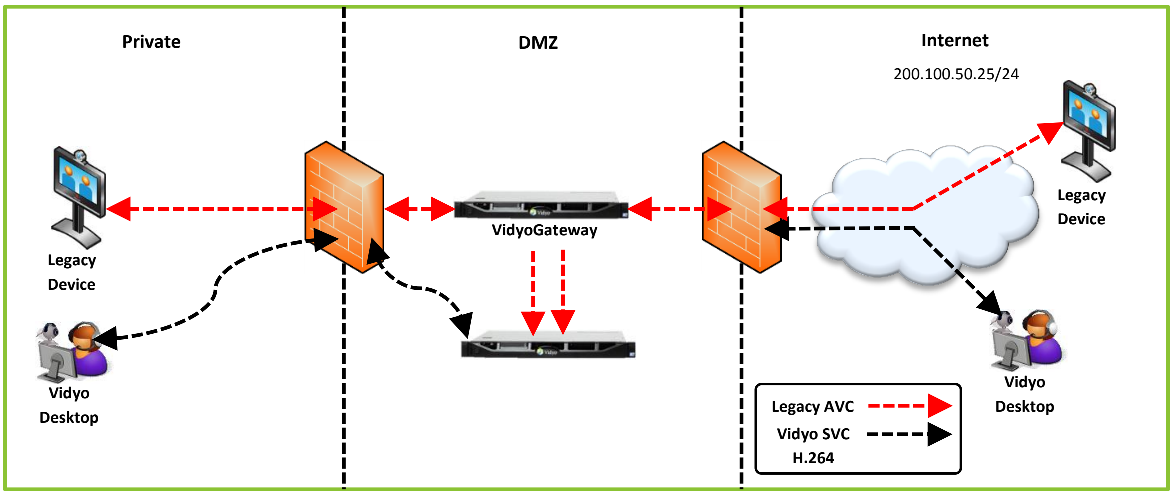

Private
192.168.1.110
(private address)
Public
200.100.50.25
(public address)
VidyoGateway
TCP 1720: Call setup (H.323)
UDP 5060: Call setup (SIP)
TCP 1024 – 65535 (H.245 call parameters)
UDP/RTP 1024 – 65535 (video and audio)
UDP/RTCP 1024 – 65535 (video and audio)
UDP/RTP 1024 – 65535 (data/FECC)
UDP/RTCP 1024 – 65535 (data/FECC)
TCP 1720: Call setup (H.323)
UDP 5060: Call setup (SIP)
TCP 1024 – 65535 (H.245 call parameters)
UDP/RTP 1024 – 65535 (video and audio)
UDP/RTCP 1024 – 65535 (video and audio)
UDP/RTP 1024 – 65535 (FECC)
UDP/RTCP 1024 – 65535 (FECC)
Legacy
Device

These are the port requirements between the VidyoGateway and Legacy devices:

Port(s)	Type	Description	Direction
53	UDP	DNS	→
1718	UDP	H.323 gatekeeper discovery	↔
1719	UDP	H.323 gatekeeper registration	↔
1720	TCP	H.323 call setup	↔
5060 (configurable)	UDP/TCP	SIP call signaling	↔
5061 (configurable)	TLS	SIP call signaling	↔
1024 – 65535	Dynamic TCP	H.323 Call control (H.245) **Note** The H245 port range is configurable. It should be set to at least four times the number of simultaneous H.323 calls in the cluster.	↔

Port(s)	Type	Description	Direction
1024 – 65535	Dynamic UDP	Media RTP/RTCP to/from Legacy Note Port range is configurable. Vidyo recommends configuring 20 ports per call. Therefore for expected capacity of 50 calls, plan so that the Min Port is at least 1,000 less than the Max Port.	↔

The following diagram illustrates the call flow of Legacy and Vidyo desktop users when a VidyoGateway and VidyoPortal/VidyoRouter are deployed in a DMZ environment.



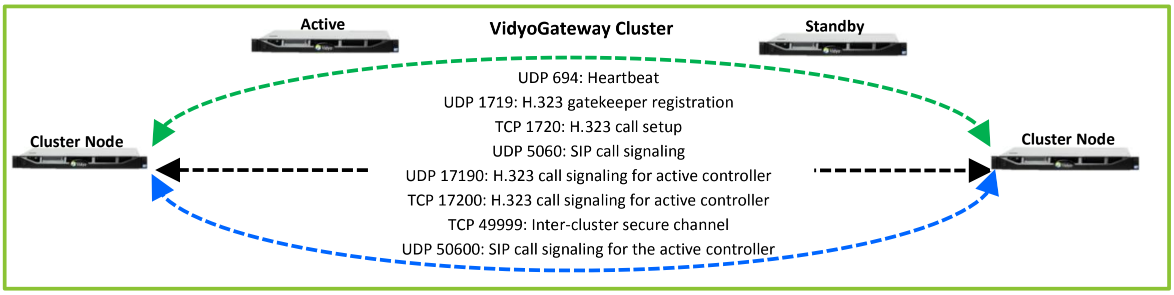
These are the additional port requirements between the VidyoGateway and the VidyoPortal/VidyoRouter:

Port(s)	Type	Description	Direction
53	UDP	DNS	→
80	TCP	Local Web GUI access SOAP messaging between VidyoPortal.	↔

Port(s)	Type	Description	Direction
443	TCP	Secure connection to VidyoPortal (https:). **Note** Required for Vidyo Encryption. Therefore if this port is open, no need for port 80	⟷
17990	TCP	VidyoRouter session control (SCIP).	→
17992	TCP	VidyoManager (EMCP).	→
50000 – 65535	Dynamic UDP	Media stream (H.264 SVC) to VidyoRouter **Note** Port range is configurable. Vidyo recommends configuring 50 ports per call. Therefore for expected capacity of 50 concurrent calls, plan so that the Min Port is at least 2,500 less than the Max Port.	⟷

For information on specifying ports in the VidyoGateway, see “Configuring HTTPS Port Settings for Your VidyoGateway Admin Pages” on page 126.

The following diagram illustrates the port requirements between VidyoGateway cluster nodes.



UDP 694: Heartbeat
UDP 1719: H.323 gatekeeper registration
TCP 1720: H.323 call setup
UDP 5060: SIP call signaling
UDP 17190: H.323 call signaling for active controller
TCP 17200: H.323 call signaling for active controller
TCP 49999: Inter-cluster secure channel
UDP 50600: SIP call signaling for the active controller

Port requirements between the VidyoGateway cluster nodes.

Port(s)	Type	Description	Direction
694	UDP	Heartbeat between the cluster controllers	↔
1719	UDP	H.323 gatekeeper registration	↔
1720	TCP	H.323 call setup	↔
5060	UDP	SIP call signaling for the VidyoGateway nodes	↔
17190	UDP	H.323 call signaling for the active controller	↔
17200	TCP	H.323 call signaling for the active controller	↔
49999	TCP	VidyoGateway inter-cluster secure channel	↔
50600	UDP	SIP call signaling for the active controller	↔

Appendix E. 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.

Product	Part Number	MTBF
HD-2	PKG-RM-HD2-GROUP, DEV-RM-HD2-SA	61,115 hours
HD-3	PKG-RM-HD3-NTPM-GROUP, PKG-RM-HD3-GROUP, DEV-RM-HD3-SA, DEV-RM-HD3-NTPM-SA	179,500 hours
HD-40B	DEV-RM-HD40-B-SA-0A	66,640 hours
HD-40C	DEV-RM-HD40-C-SA-0A	61,825 hours

Product	Part Number	MTBF
HD-100D	DEV-RM-HD100-D9020-SA-0A & DEV-RM-HD100-D-NTPM-SA-0A	75,400 hours
HD-230	DEV-RM-HD230-NTPM-SA-0A & DEV-RM-HD230-SA-0A	80,520 hours
VidyoGateway	DEV-SRV-GW-N2-0B	29,900 hours
VidyoGateway XL	DEV-SRV-GW-XL-N3-0A	121,400 hours
VidyoOne	DEV-SRV-ONE-N2-0B	29,900 hours
VidyoPanorama 600	DEV-SRV-PAN600-N2-0A	109,186 hours
VidyoPortal	DEV-SRV-PT-N2-0B	29,900 hours
VidyoPortal XL	DEV-SRV-PT-XL-N3-0A	116,700 hours
VidyoReplay	DEV-SRV-REP-N3-0A	116,700 hours
VidyoRouter	DEV-SRV-RTR-N2-0B	29,900 hours
VidyoRouter XL	DEV-SRV-RTR-XL-N3-0A	103,600 hours