VidyoReplay™

Administrator Guide

Version 22.3.0

March 2023

Copyright

Contents

1. Intro

The *VidyoReplay Administrator Guide* includes information about how to configure your server with the System Console, configure system settings as the Super Admin and Tenant Admin, understand the VidyoReplay Library and Manager Access Levels, and work with recordings and webcasts.

For information about the VidyoReplay Virtual Edition (VE), refer to *Install VidyoReplay VE* in the *VidyoReplay* section of the *Vidyo Help.*

What's new

Version 22.3.0

Ability to configure multiple Super users.

More options for downloading recordings via API.

Version 22.2.0

This version is an anchor release.

Record and save in-call chats.

Auto-delete webcasts.

Send email notifications when the NAS is unmounted.

More info

For more information about VidyoReplay, refer to:

- The *VidyoReplay* section of the *Vidyo Help*
- The *VidyoReplay Release Notes*
- The *VidyoPortal and VidyoRouter Administrator Guide*

Support

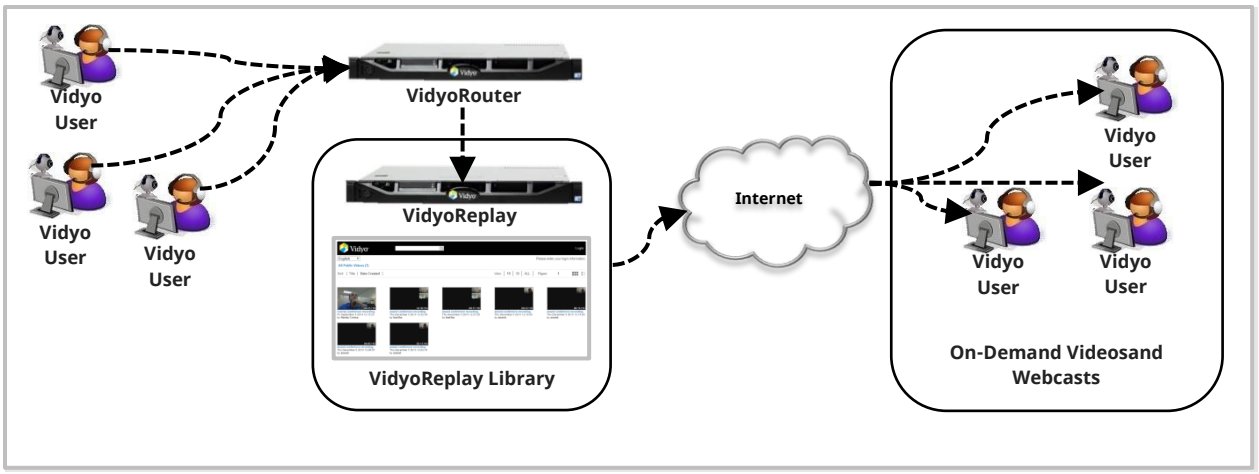
If you need help or have questions, please feel free to do one of the following:

- **Vidyo Resellers and End Users with Plus coverage:** Contact the Vidyo Support Team via email or phone at the locations listed in the Contact Us article.
- **Vidyo End Users without Plus coverage:** Contact your authorized Vidyo Reseller at support@vidyocloud.com.

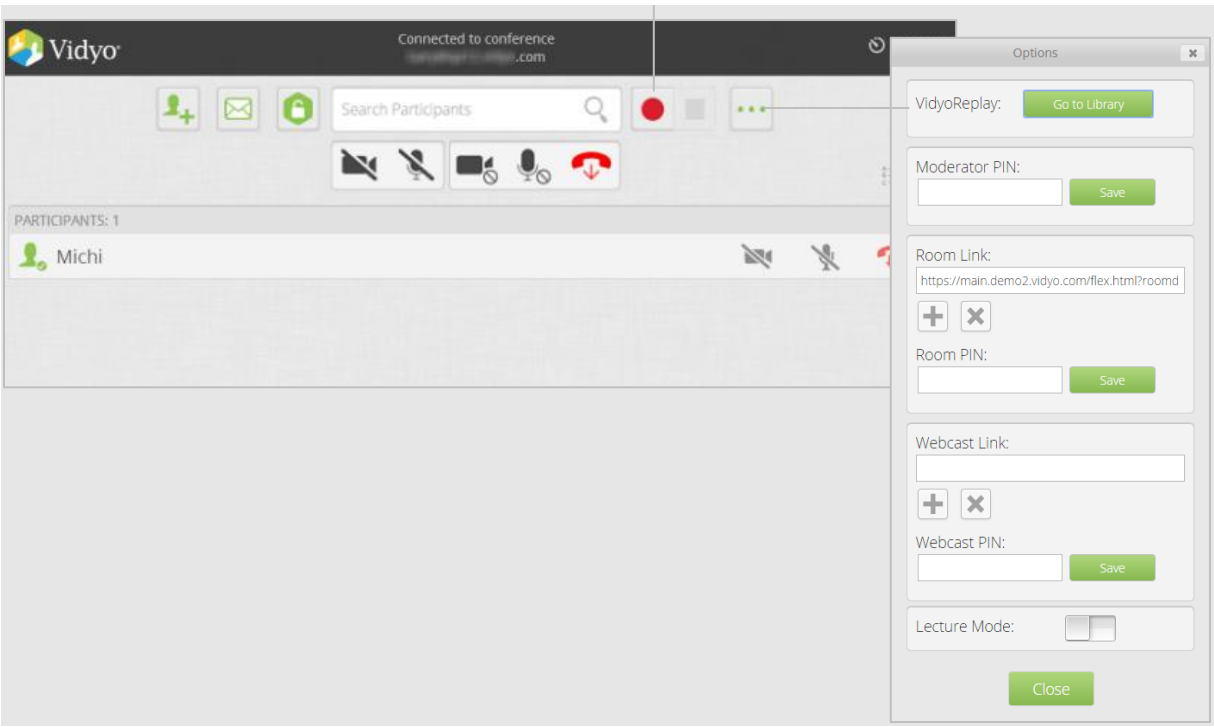
2. Overview

VidyoReplay enables you to record, webcast, store, catalog, and playback videoconferences.

Your users can record videoconferences and start live webcasts of conferences in progress that can be viewed by other people in your organization as well as the general public. All webcasts are also automatically recorded and stored in the VidyoReplay Library. After the recording of your webcast is complete, you can share it by emailing a link to it.



Once you install and configure your VidyoReplay server, the look of the HTML-based Control Meeting screen changes to include the **Record** and **Go to Library** buttons in the following locations:



VidyoReplay specifications

The VidyoReplay component is a rack-mountable 1U server providing conference, webcast, record, and playback capabilities to the Vidyo network.

For more information, refer to the *VidyoPortal and VidyoRouter Administrator Guide* and the *VidyoReplay Release Notes*.

The current VidyoReplay looks like the following:

3. Configuration procedure

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

> Note
>
> If you are clustering VidyoReplays, perform the entire procedure for each VidyoReplay in your cluster.

Make configurations on your VidyoReplay

To make configurations on your VidyoReplay:

1. Configure your network interface settings in the VidyoReplay System Console. The following criteria should be met:
   a. Set your primary network interface (ETH0) and, if you are configuring a NAS, your secondary network interface (ETH1) with IP addresses.
   b. Rack your machine properly.
   c. Successfully Ping your server before proceeding.

   For more information, see 4. Configure your server with the System/Admin Console.
2. Secure your VidyoReplay server (if applicable). See Secure your VidyoReplay system with SSL and HTTPS.
3. Register your VidyoReplay to your VidyoPortal by entering your VidyoPortal address in your VidyoReplay. See Configure the general settings.

Make configurations on your VidyoPortal for your VidyoReplay

To make configurations on your VidyoPortal for your VidyoReplay:

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

   > Note
   >
   > If you are performing an initial VidyoReplay setup, both the VidyoReplay Recorder and VidyoReplay must be added as components in your Vidyo conferencing system. For more information, refer to *Make the VidyoReplay Recorders available* and *Make the VidyoReplay components available* in the *VidyoPortal and VidyoRouter Administrator Guide.*

> When clustering VidyoReplay servers, your username and password must be the same on each VidyoReplay Recorder and VidyoReplay in your system. See Configure the general settings.

2. Assign the VidyoReplay Recorder and VidyoReplay components to a tenant. If you are running a multi-tenant system, assign them to the appropriate tenants.

   For more information, refer to *Make the VidyoReplay components available* in the *VidyoPortal and VidyoRouter Administrator Guide.*

3. Configure groups on your tenant to use your VidyoReplay Recorder and VidyoReplay components.

   For more information, refer to *Add a new group* in the *VidyoPortal and VidyoRouter Administrator Guide.*

> Note
>
> After making these configurations, you can then configure your NAS and/or Clusters on your VidyoReplay, if applicable. See NAS guidelines for your VidyoReplay and VidyoReplay clusters.
>
> You can also customize your Webcast invitations. For more information, refer to *Customize the Invite Text* in the *VidyoPortal and VidyoRouter Administrator Guide.*

4. Configure your server with the System/Admin Console

The Vidyo System Console (also referred to as the Admin Console) enables you to easily and quickly access all the VidyoReplay features.

Immediately after you have physically installed your Vidyo server, you must configure your VidyoReplay as described in this chapter.

For more information about installing the Vidyo server and for Vidyo server specifications, refer to the *VidyoPortal and VidyoRouter Administrator Guide* and the *VidyoReplay Release Notes*.

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

- For security reasons, Vidyo strongly recommends moving your SSH port to the standard 22 which is in the privileged port range. When upgrading from VidyoReplay version 3.1.5 to 19.1.0 or later, your port will be automatically reset to the standard SSH port 22. If you previously had SSH configured to port 2222, you should ensure that you update your firewall rules (if applicable) prior to upgrade. 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 VidyoReplay Admin portal blocking HTTP/HTTPS access from untrusted networks including the Internet.
- Change your VidyoReplay 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 VidyoReplay 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.

Log in and change the default password

The very first time you log into your VidyoReplay 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 VidyoReplay Admin Portal.

To log in to the System 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.

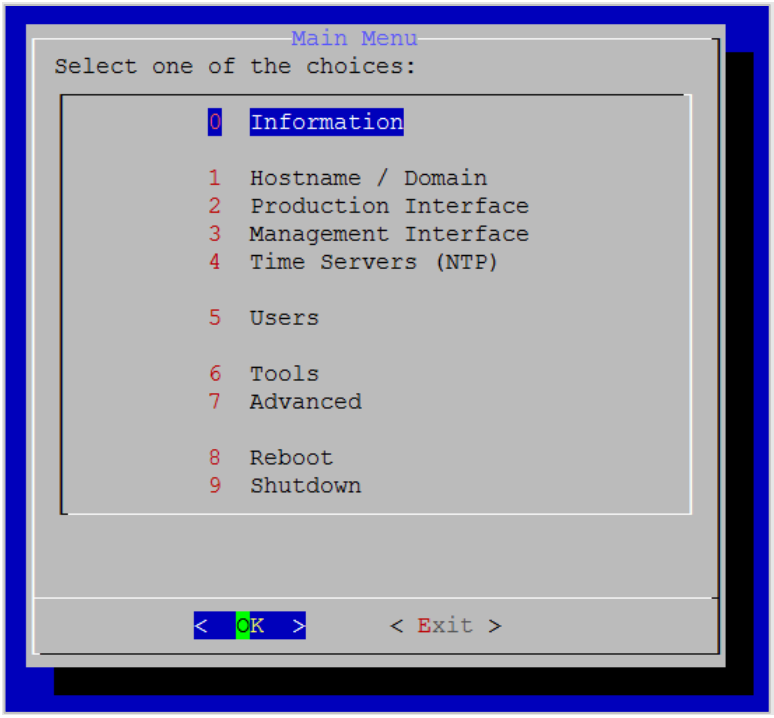
   When selecting a new password, follow these guidelines:

   - 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.



If you need to reset the password, see Change user passwords.

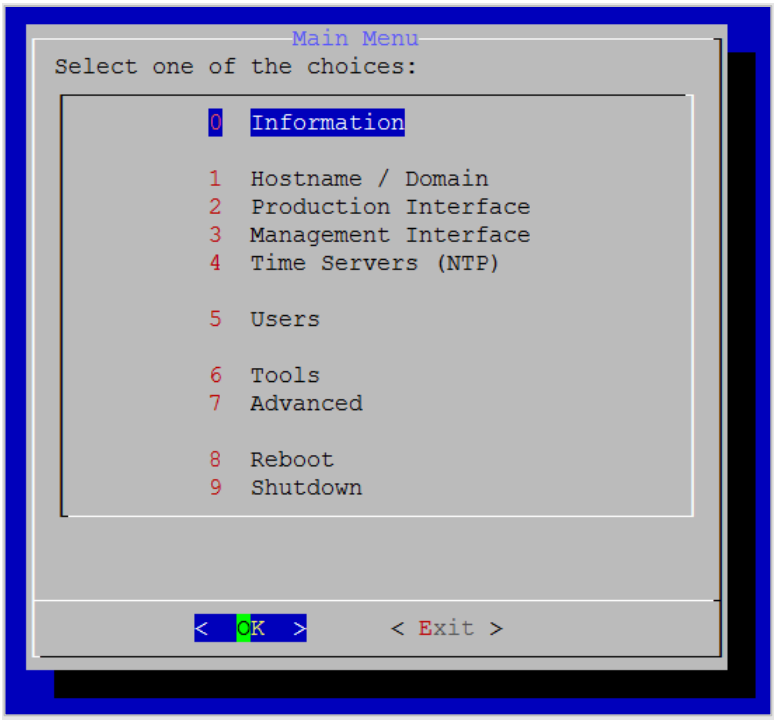
View application and system information

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.

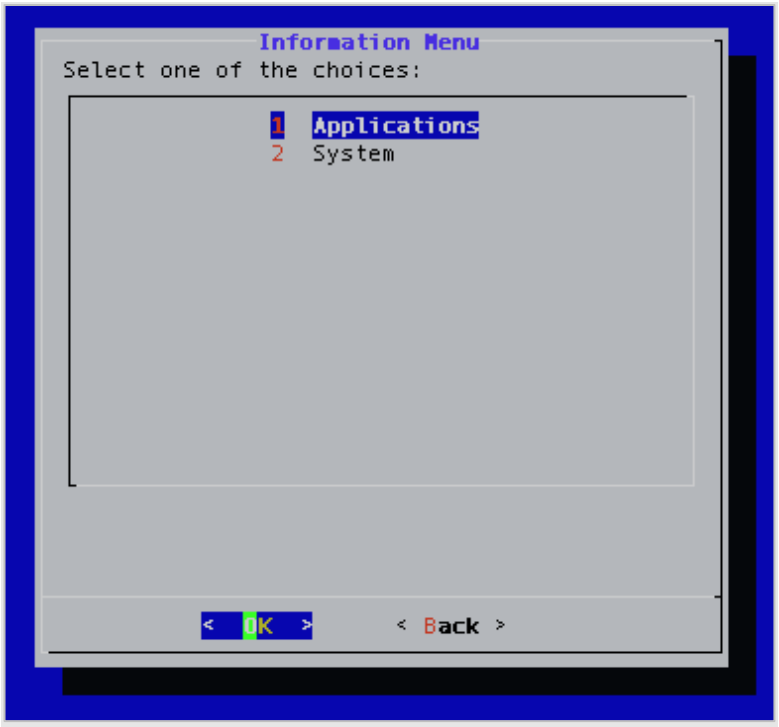
View application information

To view application information:

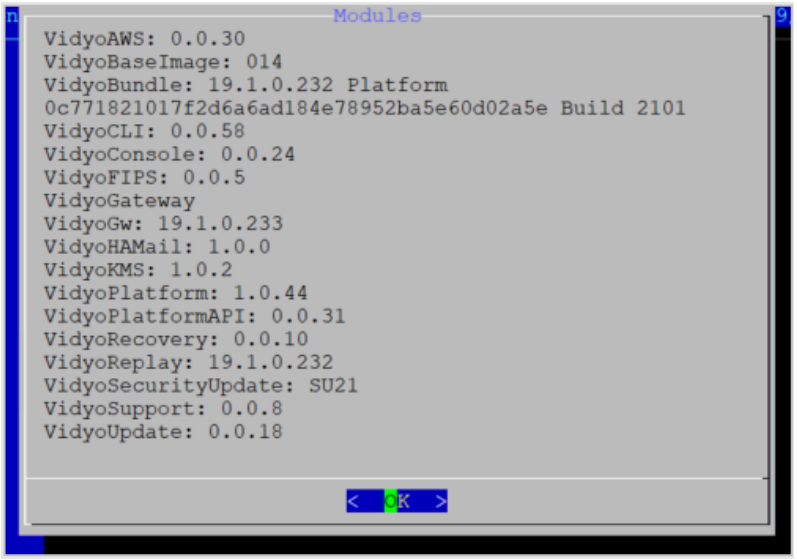
1. Log in to the System Console. The Main Menu displays.



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.

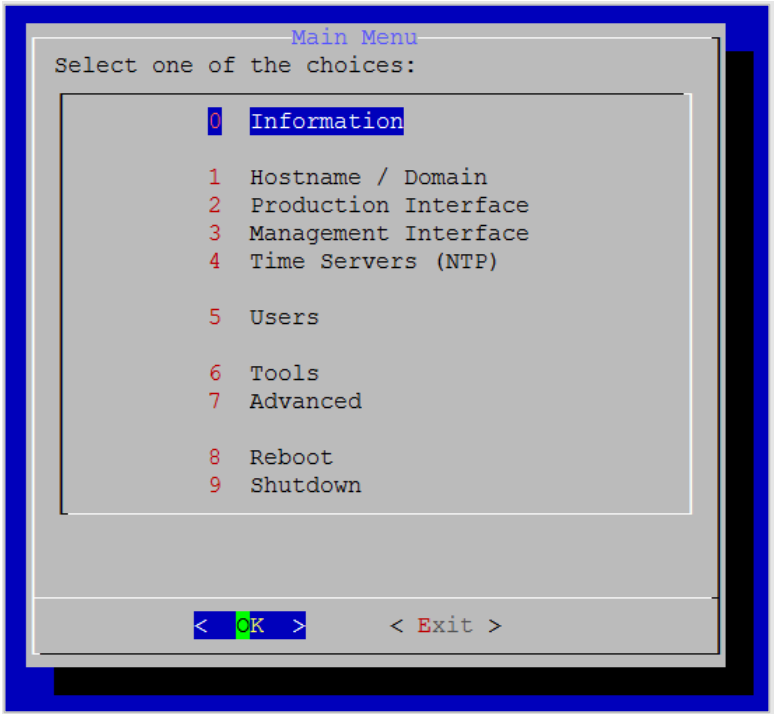


This window displays the list of the platform applications and the version number of each one. This information is mostly internal and useful for troubleshooting by the Vidyo Customer Support team.

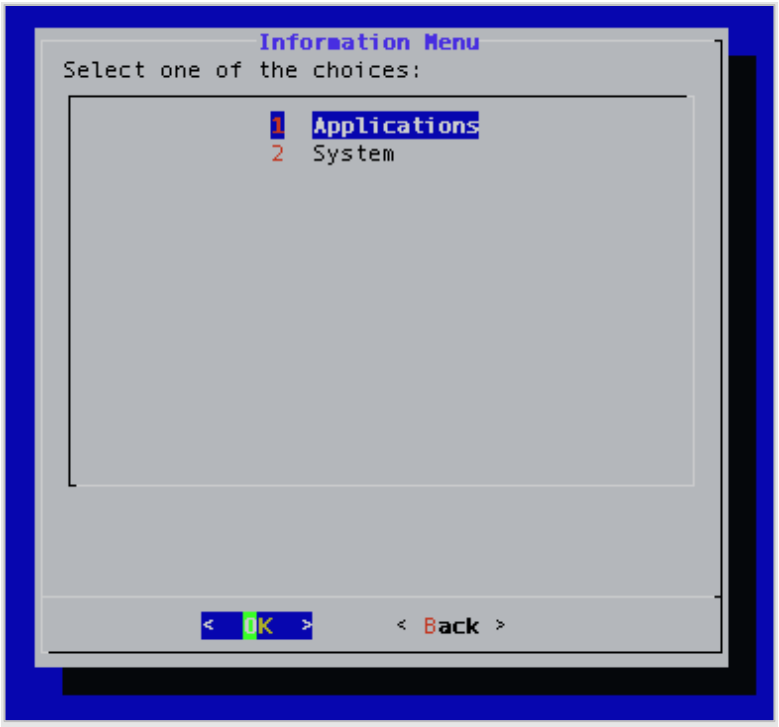
View system information

To view system information:

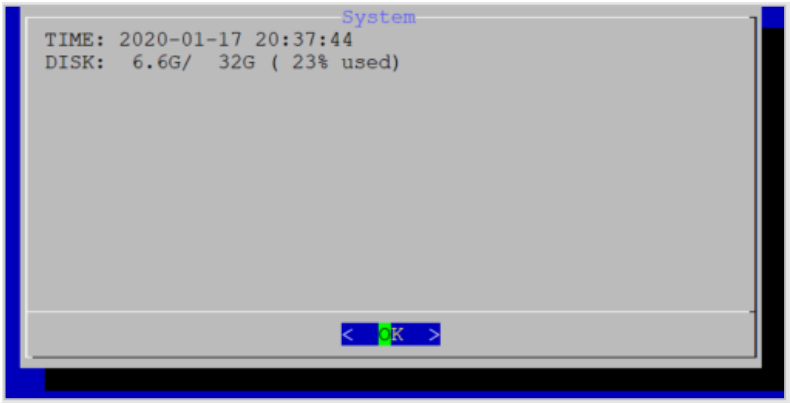
1. Log in to the System Console. Main Menu displays.



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



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



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

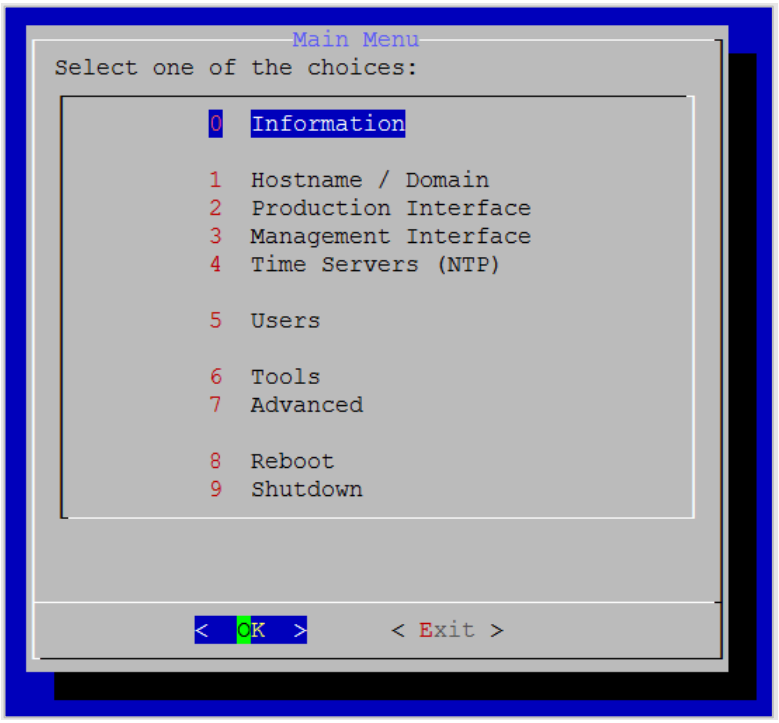
Set the hostname and the domain

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

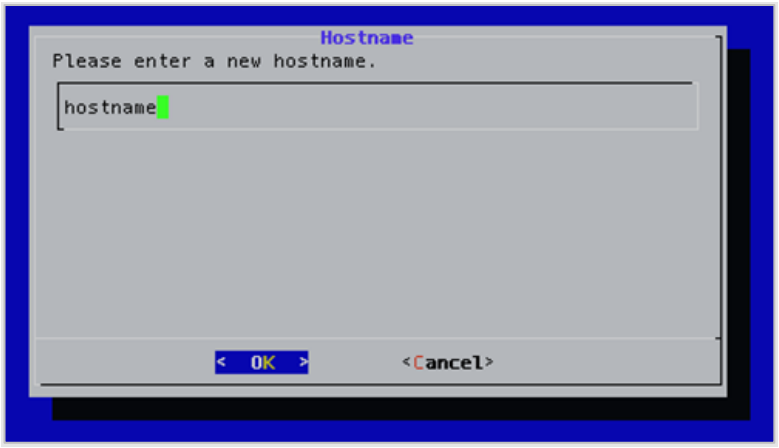
> Note
>
> A network setup must be performed for each of your Vidyo servers.

To set the hostname and the domain:

1. Log in to the System Console. The Main Menu displays.

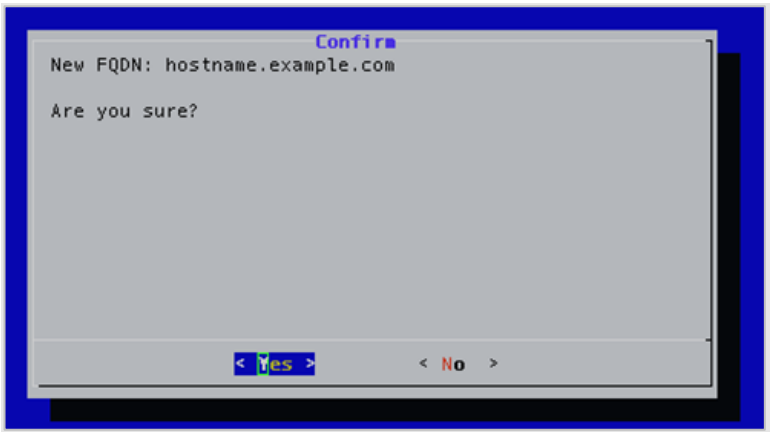


2. Enter **1** to select the Hostname/Domain option.
3. Press the **Enter** key to select **OK**. The *Hostname* window displays.



4. Enter the hostname.
5. Press the **Enter** key to select **OK**. The *Domain* window displays.

6. Enter the domain.
7. Press the **Enter** key to select **OK**. The *Confirm* window displays.



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**.

Configure 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.

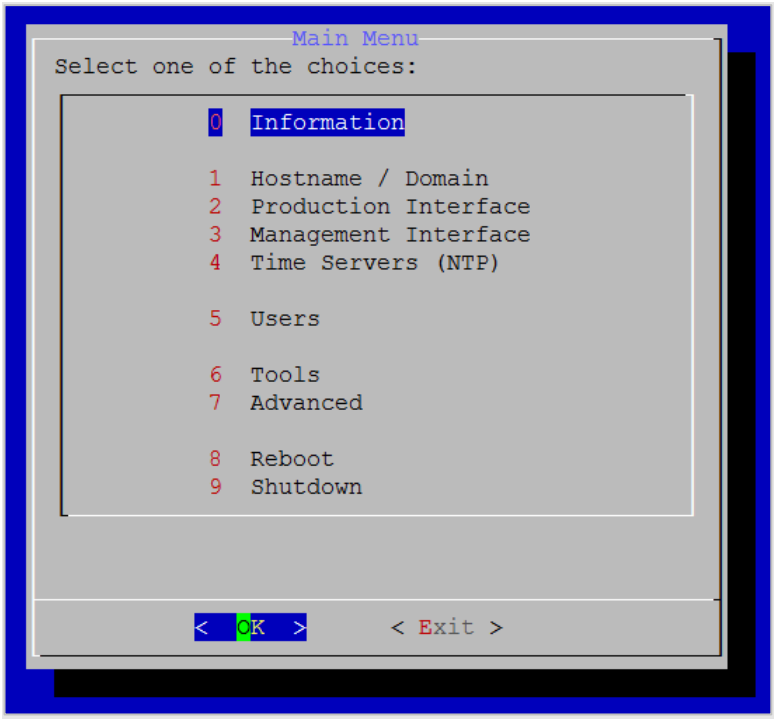
> Note
>
> Vidyo recommends that this feature not replace adding proper network router to your DMZ to handle the proper subnet routes. Static route setup can lead to security vulnerabilities and should only be configured by advanced network administrators. Vidyo is not responsible for any possible security 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.

View the Production Interface active information

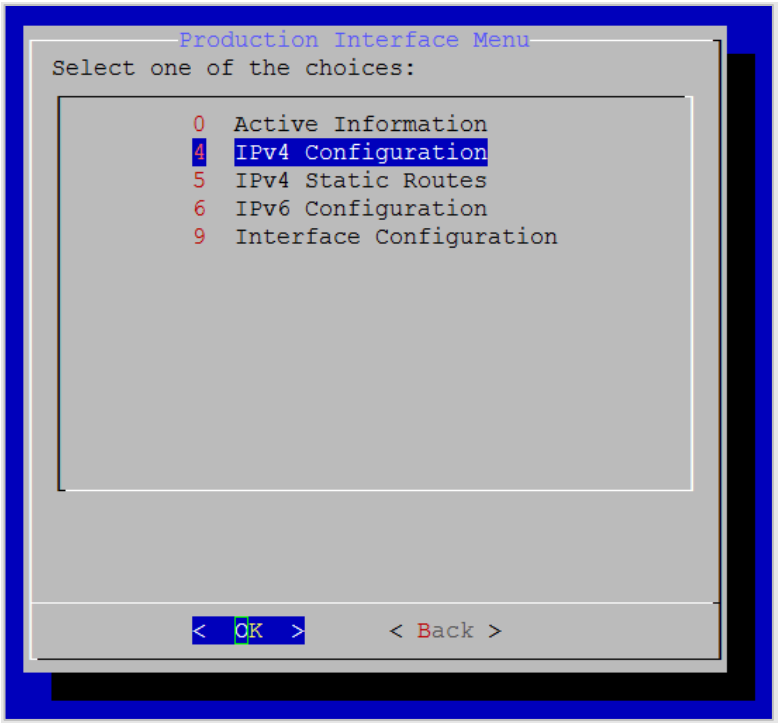
The Production Interface Active Information window provides important information about the Production Interface, such as the currently configured IP address, link status, and duplex settings.

To view the Production Interface active information:

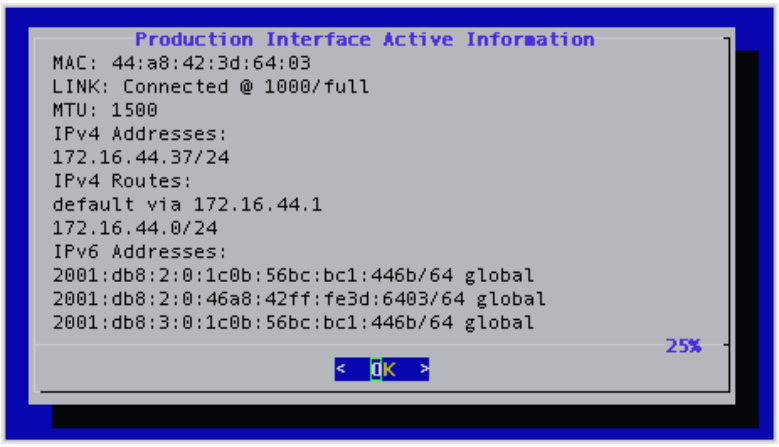
1. Log in to the System Console. The Main Menu displays.



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



4. Enter **0** to select the Active Information option.
5. Press the **Enter** key to select **OK**. The *Product Interface Active Information* window displays.



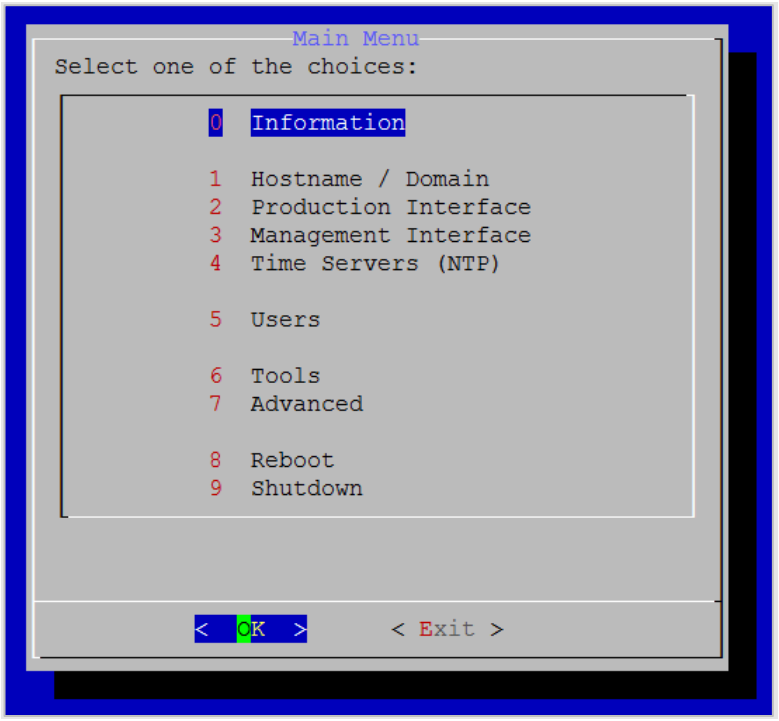
Configure the IPv4 Production Interface

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.

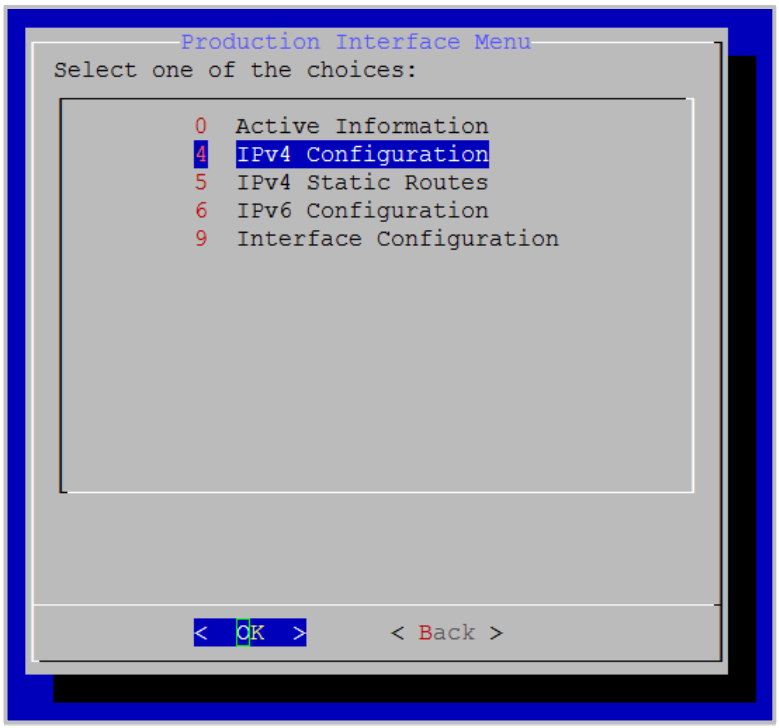
Manually disable and enable the IPv4 Production Interface

To manually disable or enable the IPv4 Production Interface:

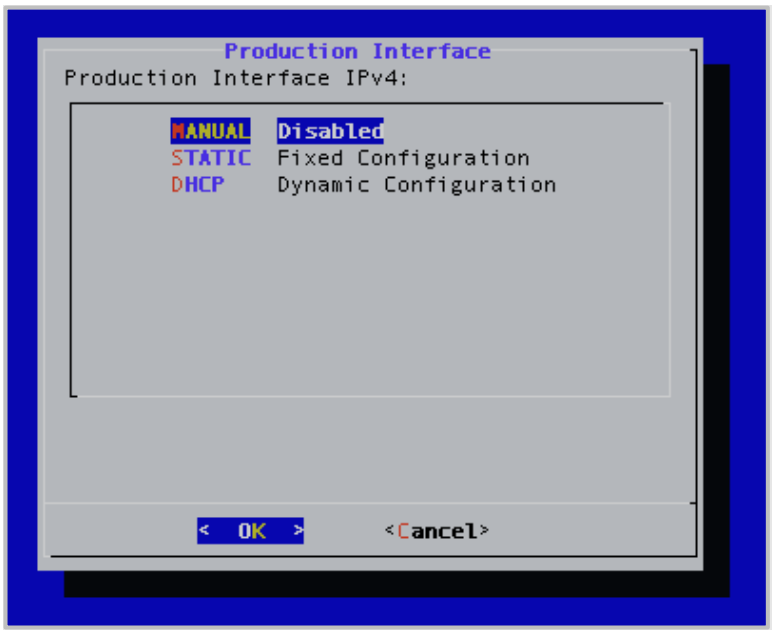
1. Log in to the System Console. The Main Menu displays.



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



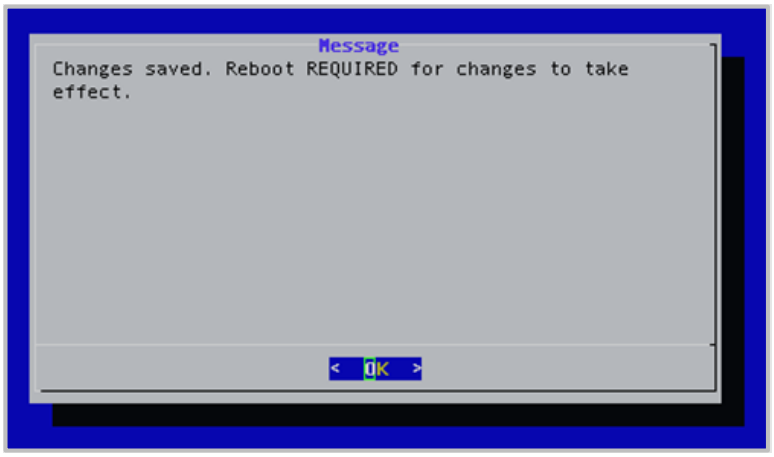
4. Enter **4** to select the IPv4 Configuration option.
5. Press the **Enter** key to select **OK**.



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.

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

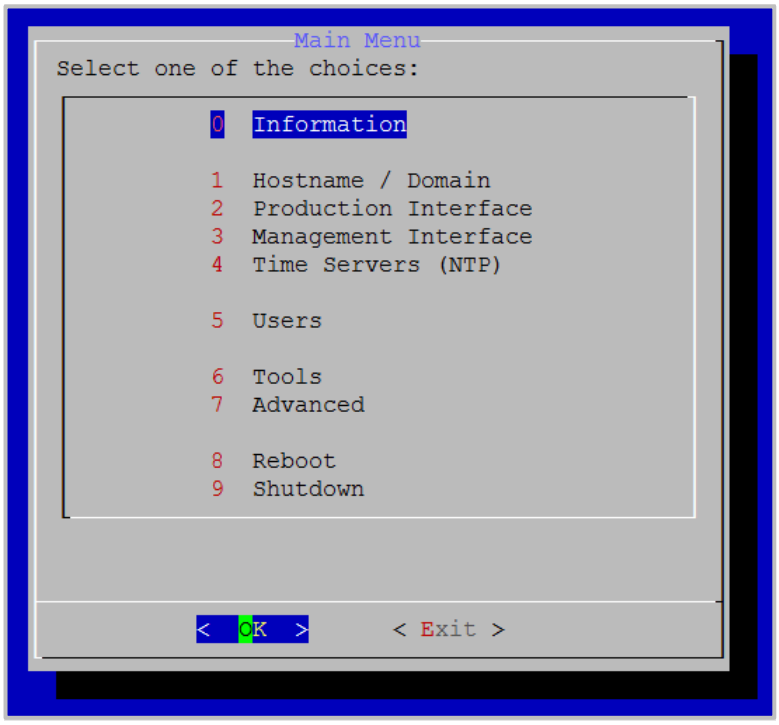


9. Press the **Enter** key to select **OK**.

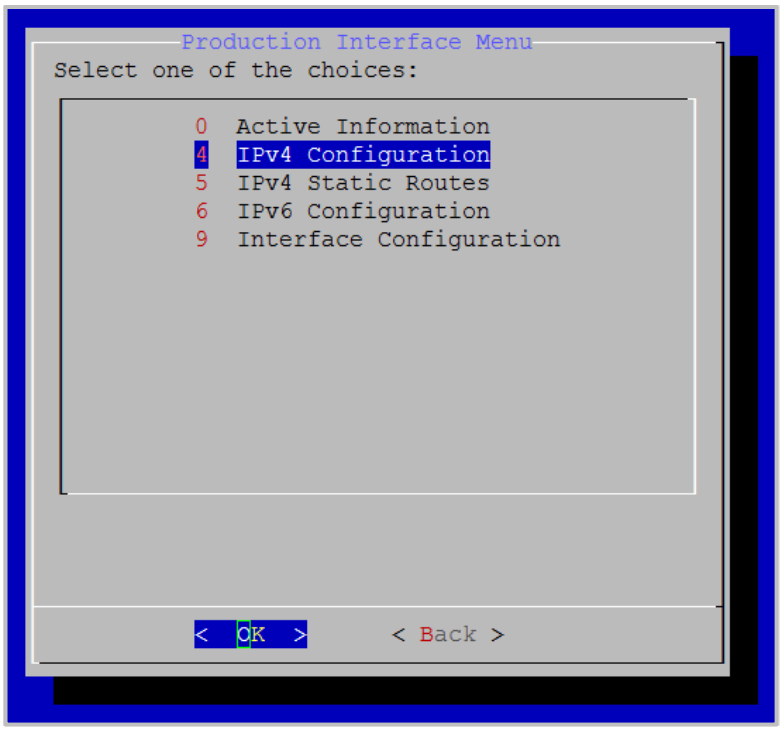
Configure an IPv4 Static Production Interface

To configure an IPv4 Production Interface:

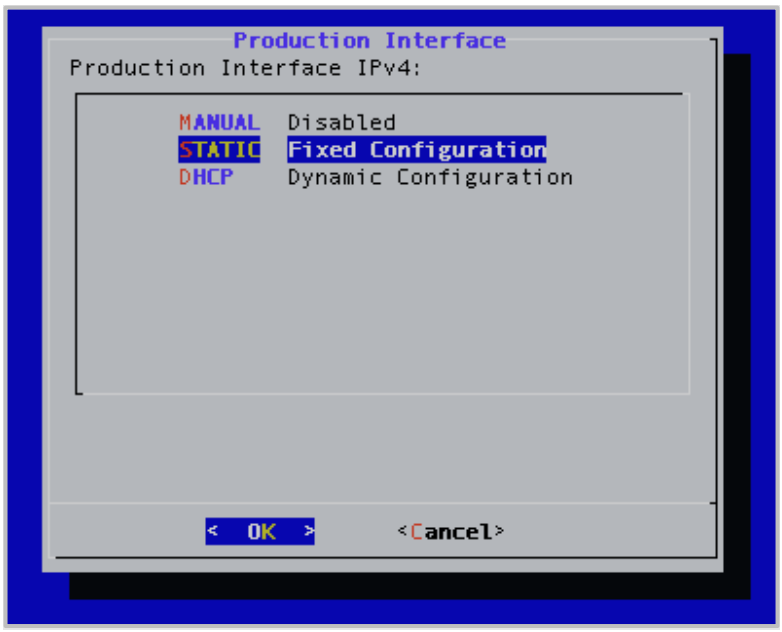
1. Log in to the System Console. The Main Menu displays.



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

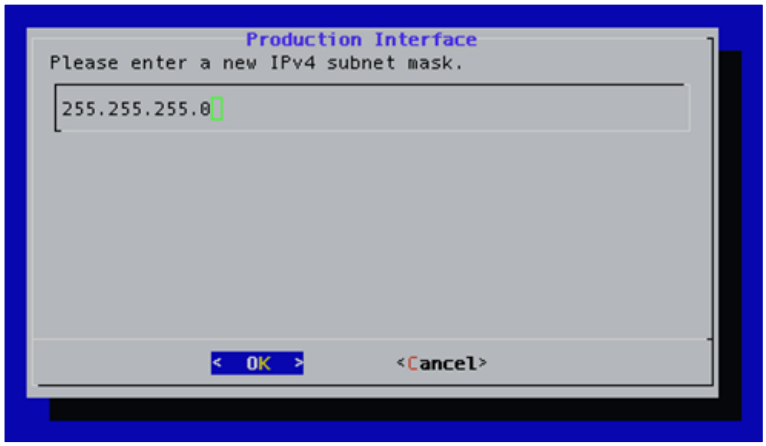


4. Enter **4** to select the IPv4 Configuration option.
5. Press the **Enter** key to select **OK**.



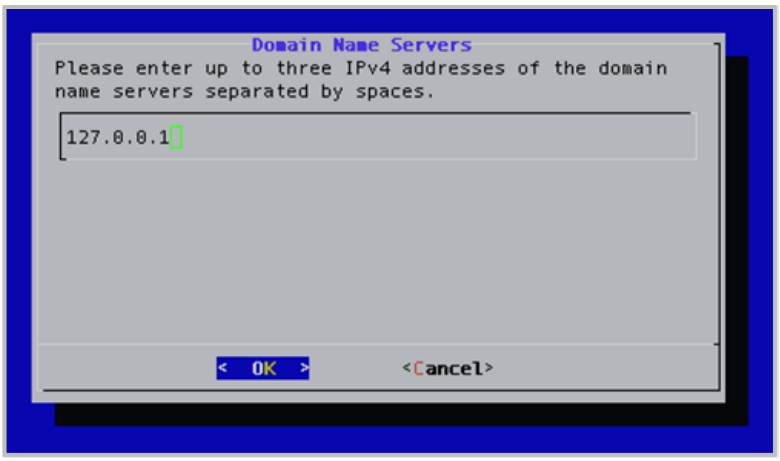
6. Enter **S** to select the STATIC option.
7. Press the **Enter** key to select **OK**.
8. Delete the existing IPv4 address and enter a new one.

9. Press the **Enter** key to select **OK**.
10. Delete the existing IPv4 subnet mask and enter a new one.

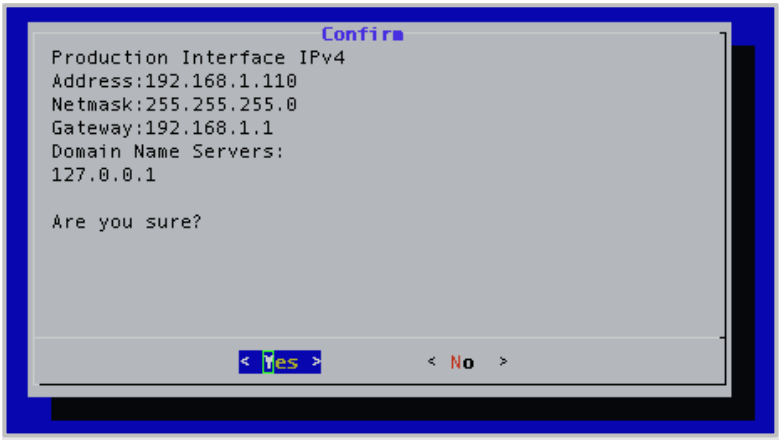


11. Press the **Enter** key to select **OK**.
12. Delete the existing IPv4 Replay and enter a new one.

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



15. Press the **Enter** key to select **OK**. The *Confirm* window displays.



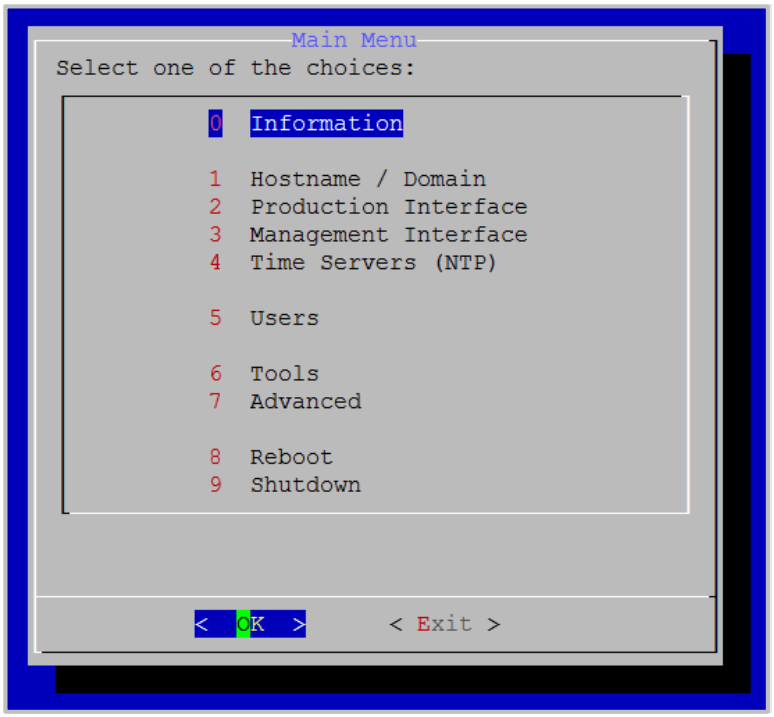
16. Press the **Enter** key to select **Yes**. A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
17. Press the **Enter** key to select **OK**.

    For more information about configuring the Production and Management interfaces, see Configure the Production Interface and Configure the Management Interface.

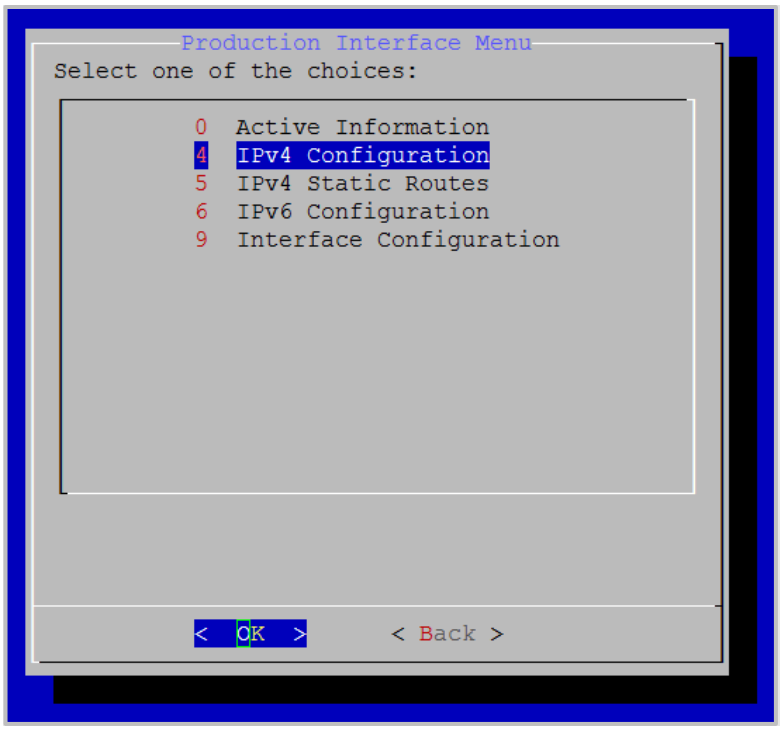
Configure an IPv4 DHCP Production Interface

To configure an IPv4 DHCP Production Interface:

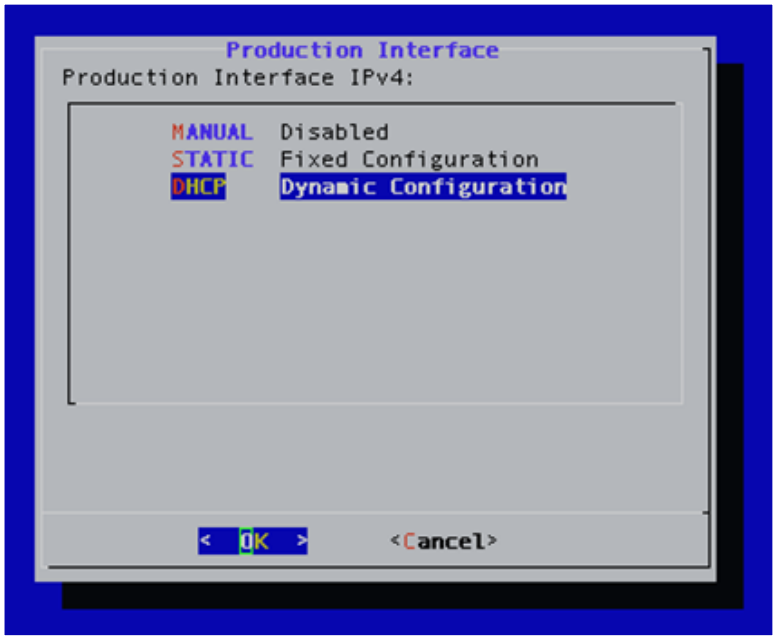
1. Log in to the System Console. The Main Menu displays.



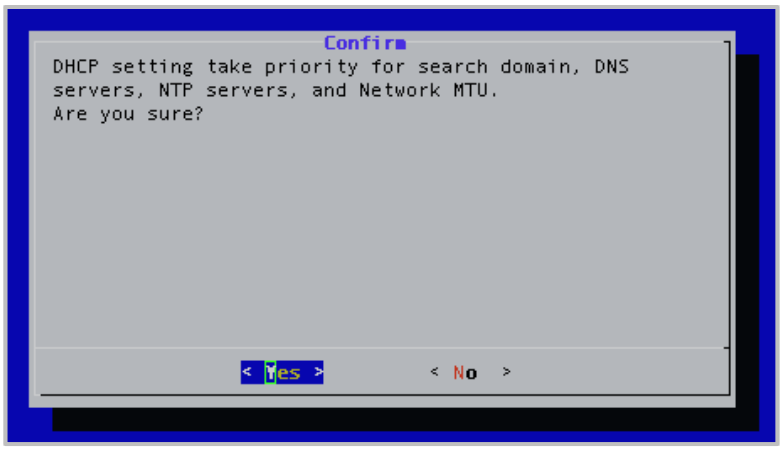
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**. The Production Interface Menu displays.



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



6. Enter **D** to select the DHCP option.
7. Press the **Enter** key to select **OK**. The *Confirm* window displays.



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**.

Configure IPv4 Static routes

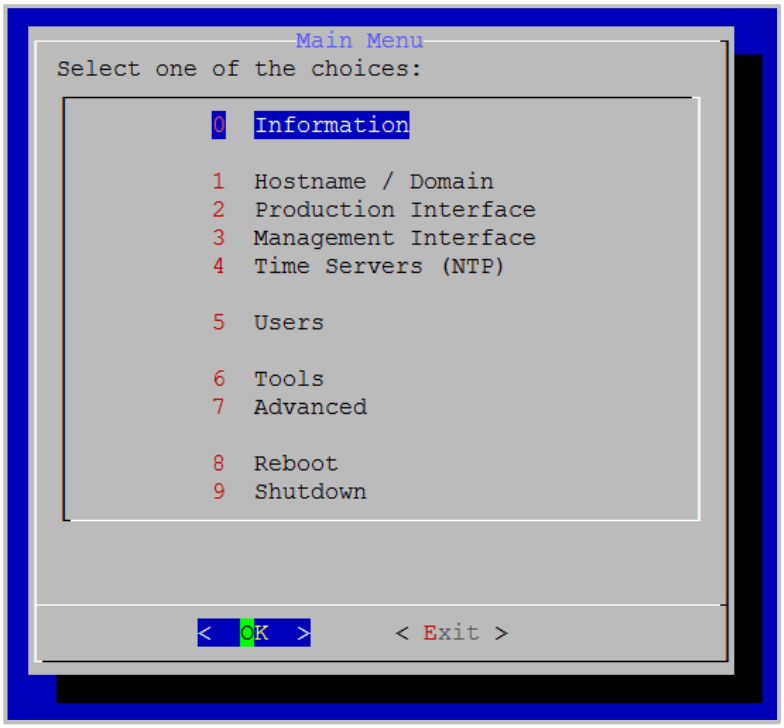
This section describes how to add and remove IPv4 static routes.

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

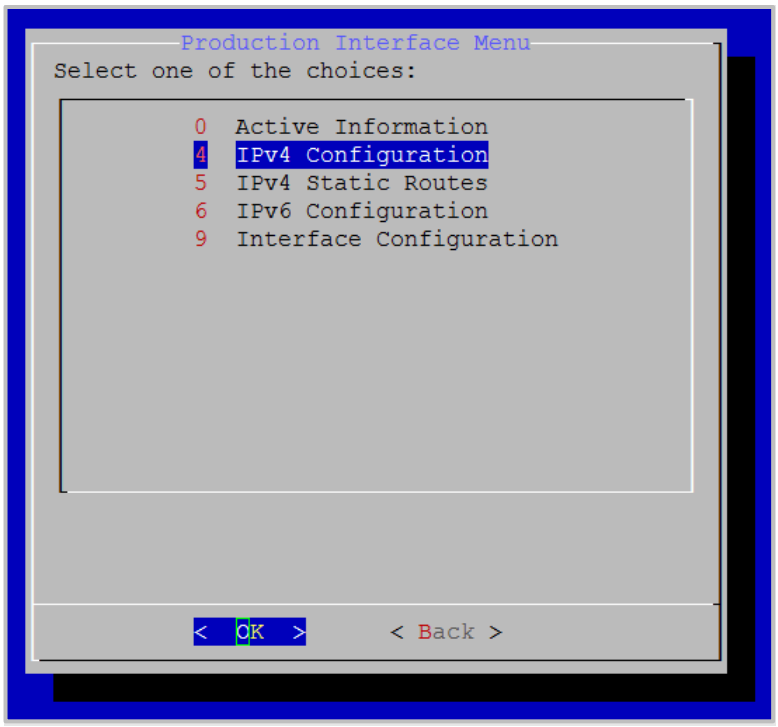
Add IPv4 Static routes

To add IPv4 Static routes:

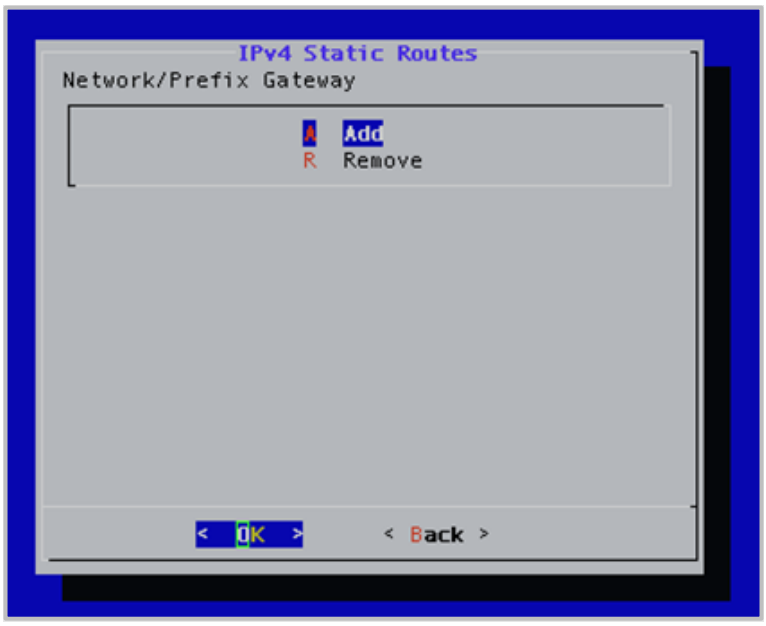
1. Log in to the System Console. The Main Menu displays.



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

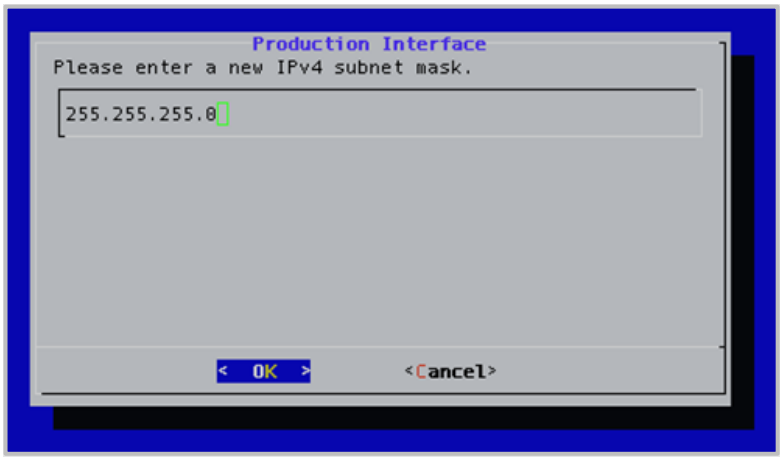


4. Enter **5** to select the IPv4 Static Routes option.
5. Press the **Enter** key to select **OK**. The *IPv4 Static Routes* window displays.



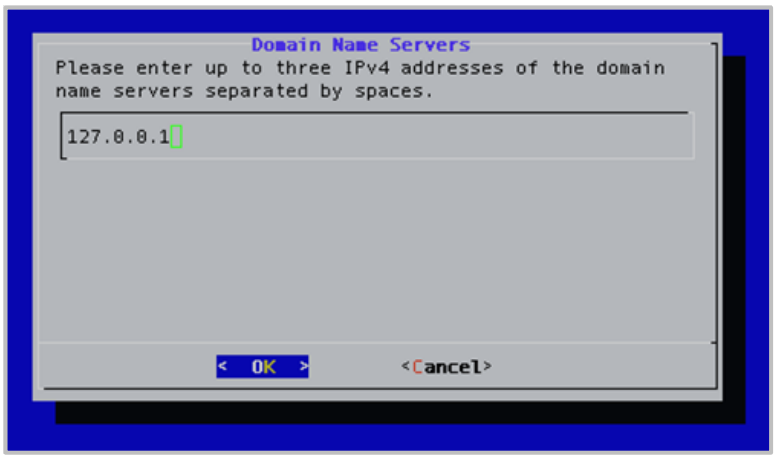
6. Enter **A** to select the Add option.
7. Press the **Enter** key to select **OK**.
8. Delete the existing IPv4 address and enter a new one.

9. Press the **Enter** key to select **OK**.
10. Delete the existing IPv4 subnet mask and enter a new one.

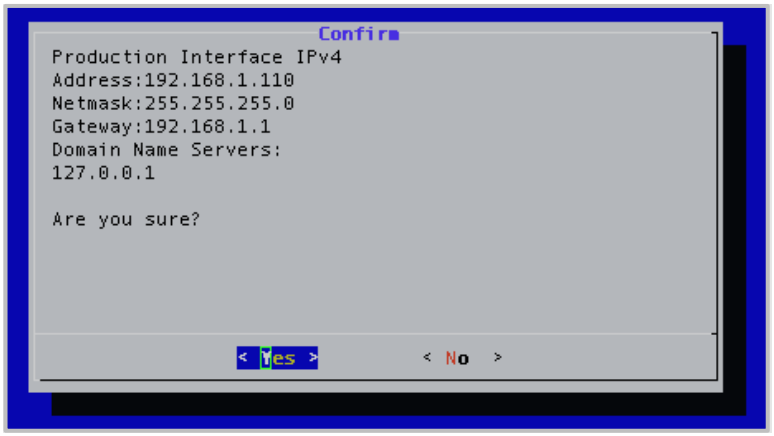


11. Press the **Enter** key to select **OK**.
12. Delete the existing IPv4 gateway and enter a new one.

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



15. Press the **Enter** key to select **OK**. The *Confirm* window displays.



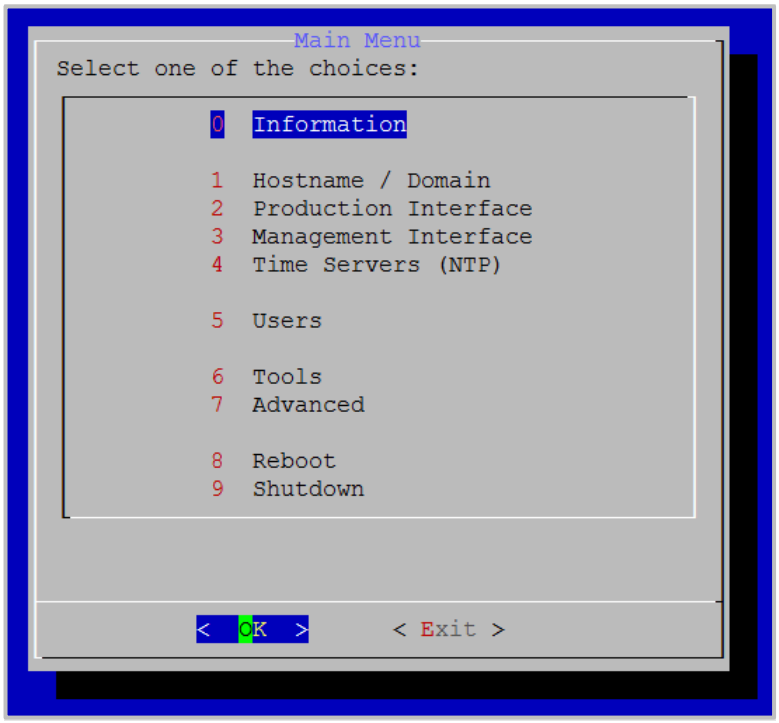
16. Press the **Enter** key to select **Yes**. A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
17. Press the **Enter** key to select **OK**.

    For more information about configuring the Production and Management interfaces, see Configure the Production Interface and Configure the Management Interface.

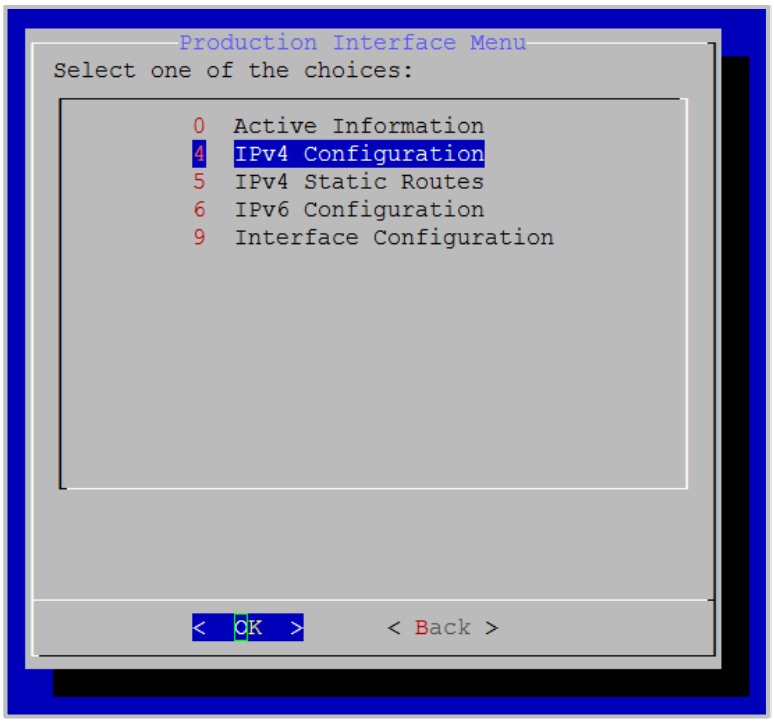
Remove IPv4 Static routes

To remove IPv4 static routes:

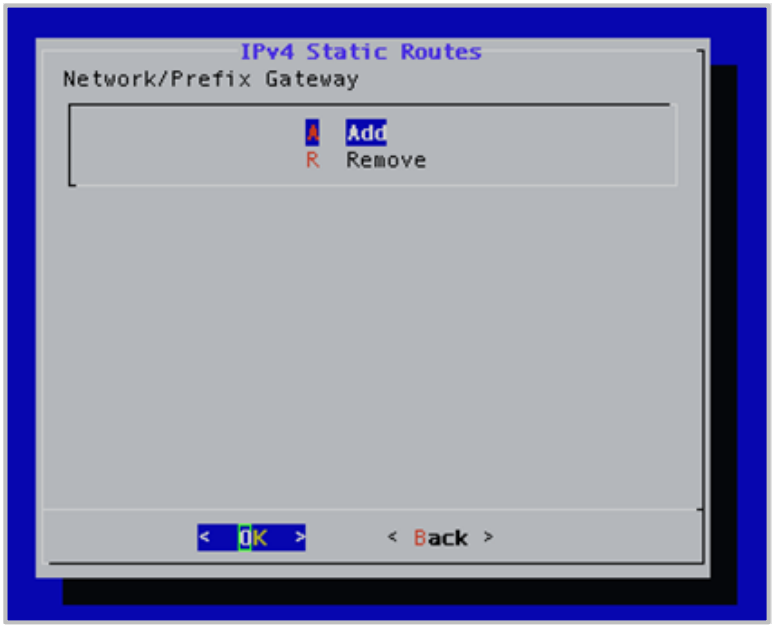
1. Log in to the System Console. The Main Menu displays.



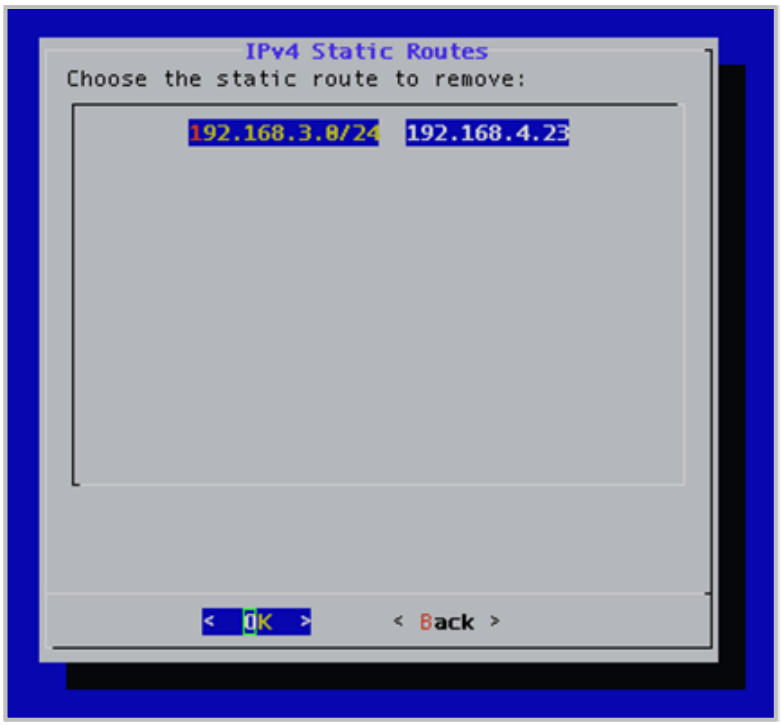
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**. The Production Interface Menu displays.



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



6. Enter **R** to select the Remove option.
7. Press the **Enter** key to select **OK**. The *IPv4 Static Routes* window displays.



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**.

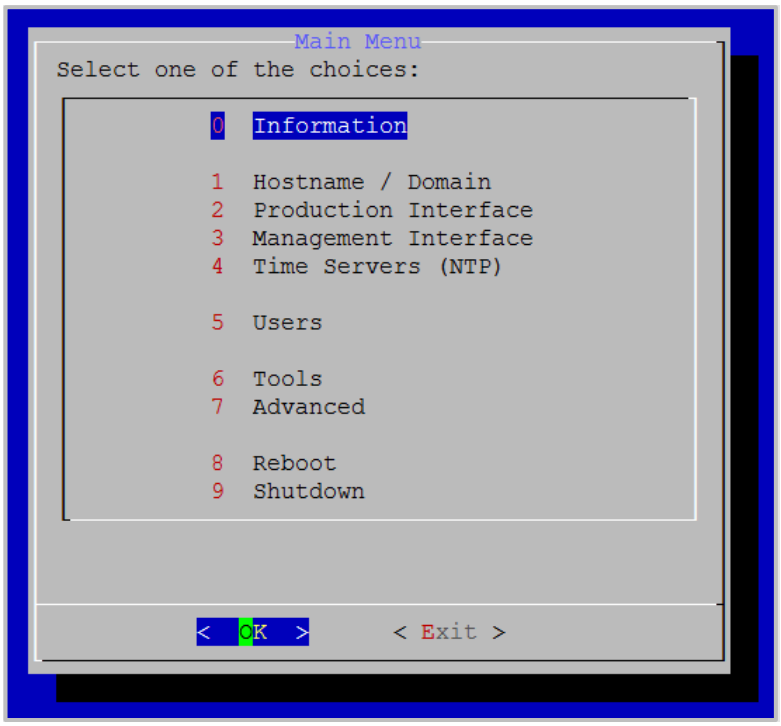
Configure the IPv6 Production Interface

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.

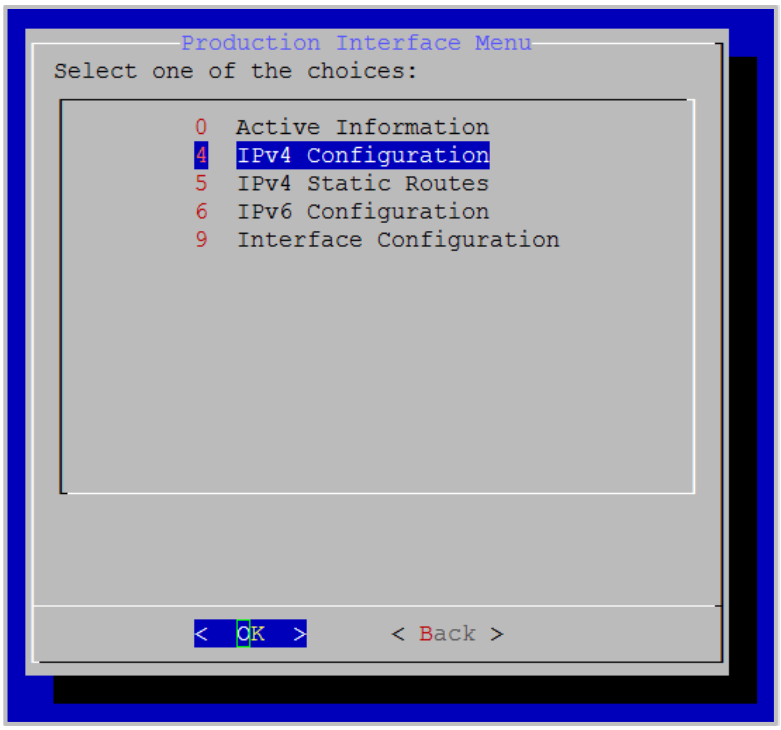
Manually disable and enable the IPv6 Production Interface

To manually disable or enable the IPv6 Production Interface:

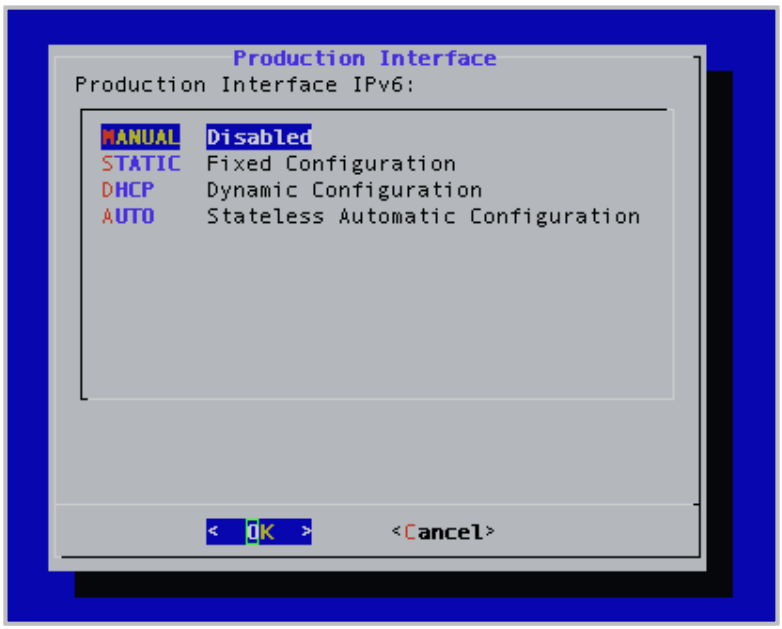
1. Log in to the System Console. The Main Menu displays.



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



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



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

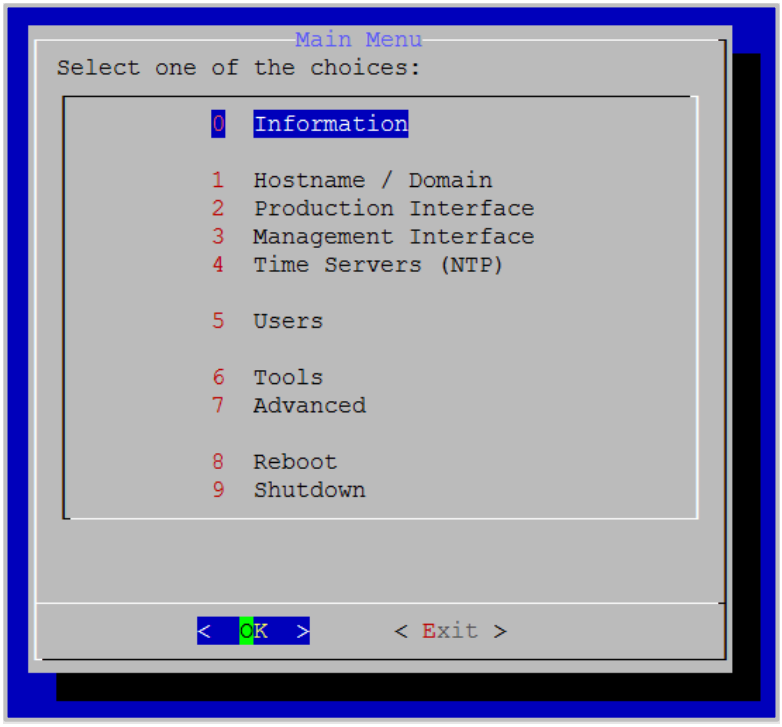
   If the current state of the Production Interface is enabled, you are asked to confirm if you want to disable it. If the current state of the Production Interface is disabled, you are asked to confirm if you want to enable it.

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**.

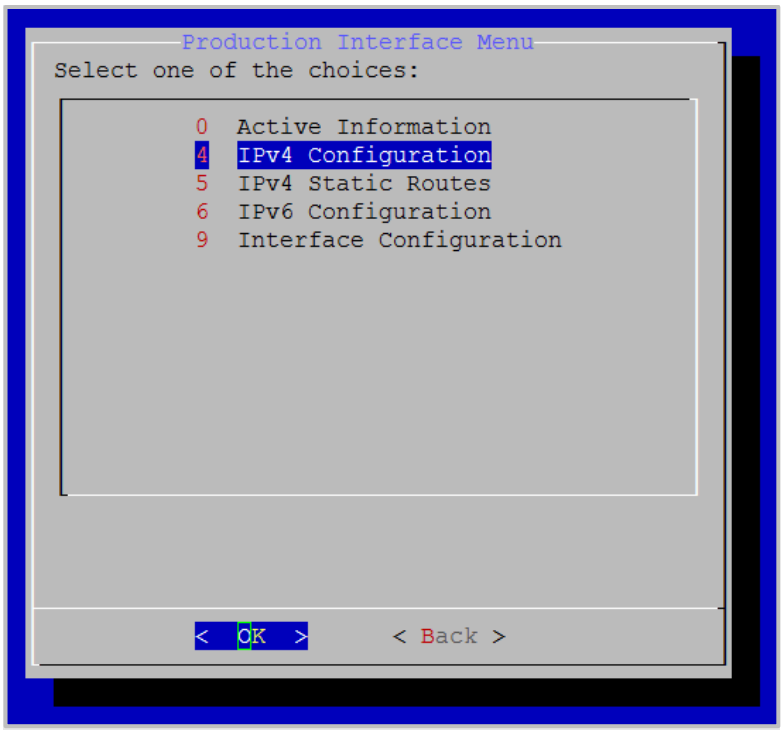
Configure an IPv6 Static Production Interface

To configure an IPv6 static Production Interface:

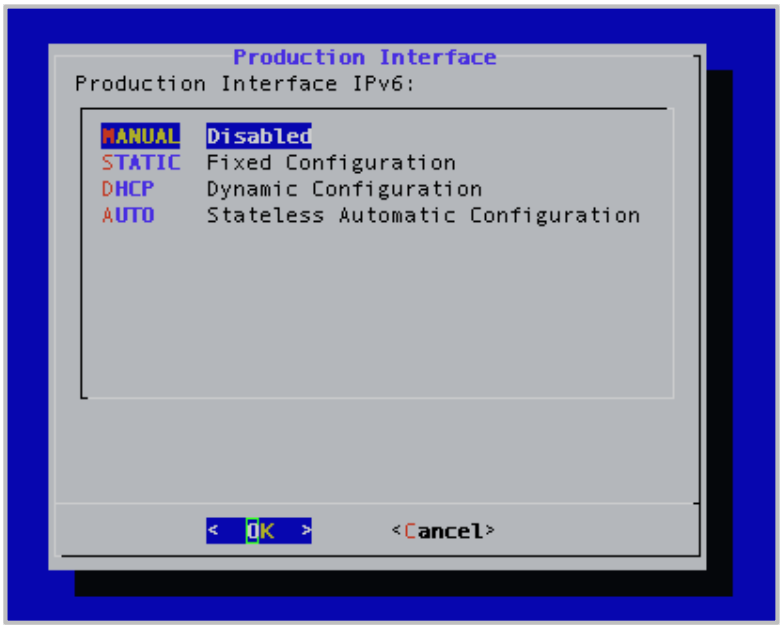
1. Log in to the System Console. The Main Menu displays.



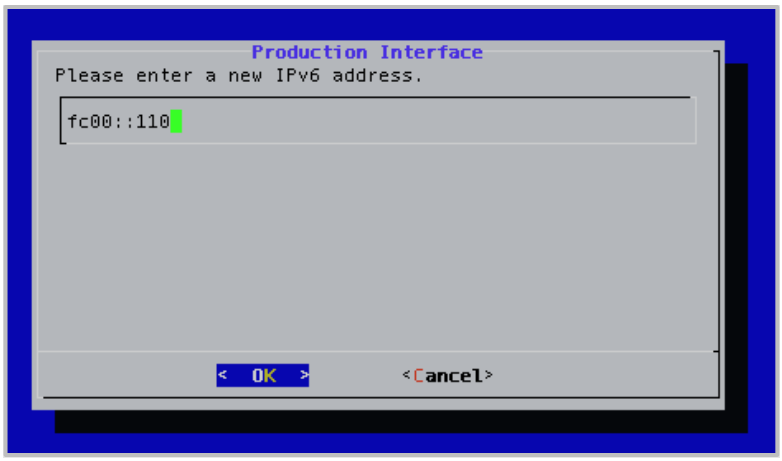
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**. The Production Interface Menu displays.



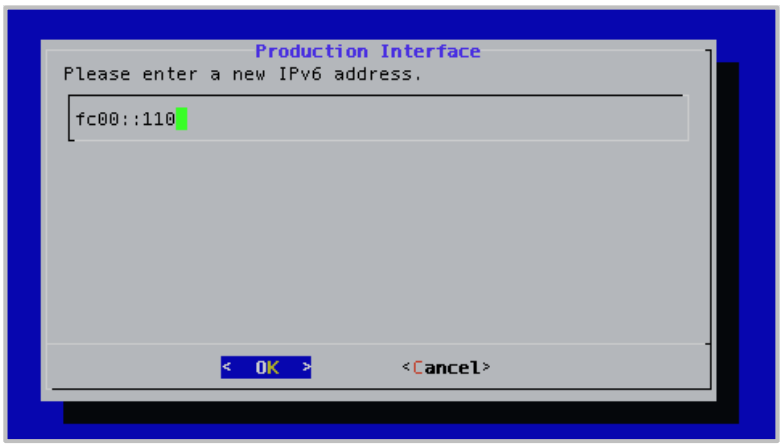
4. Enter **6** to select the IPv6 Configuration option.
5. Press the **Enter** key to select **OK**.



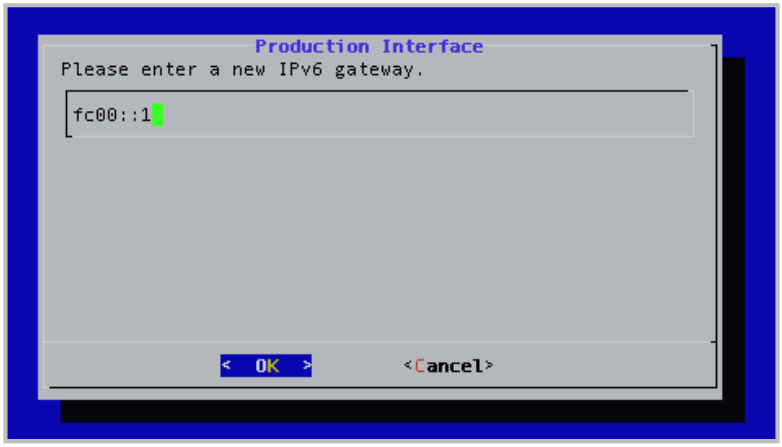
6. Enter **S** to select the STATIC option.
7. Press the **Enter** key to select **OK**.
8. Delete the existing IPv6 address and enter a new one.



9. Press the **Enter** key to select **OK**.
10. Delete the existing IPv6 address and enter a new one.

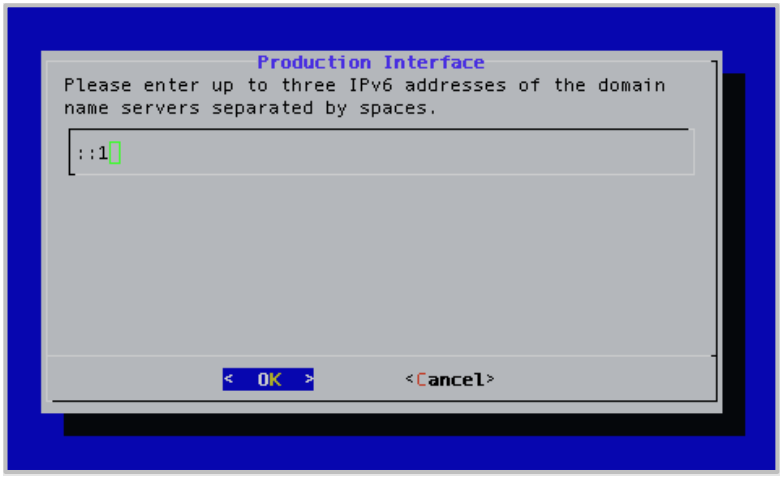


11. Press the **Enter** key to select **OK**.
12. Delete the existing IPv6 gateway and enter a new one.

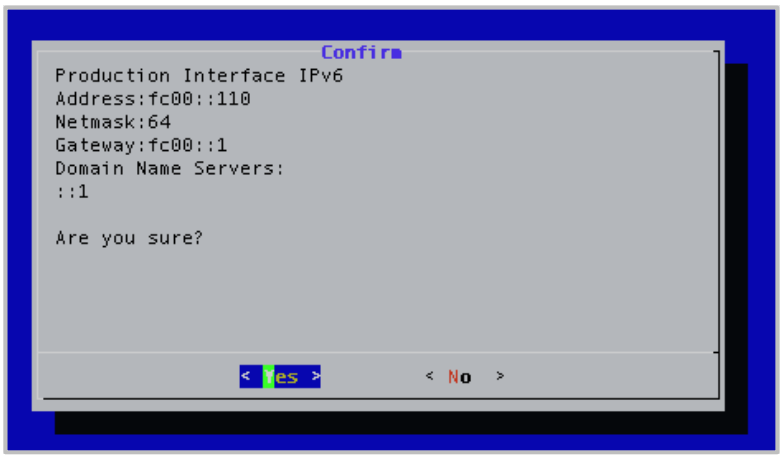


13. Press the **Enter** key to select **OK**.

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

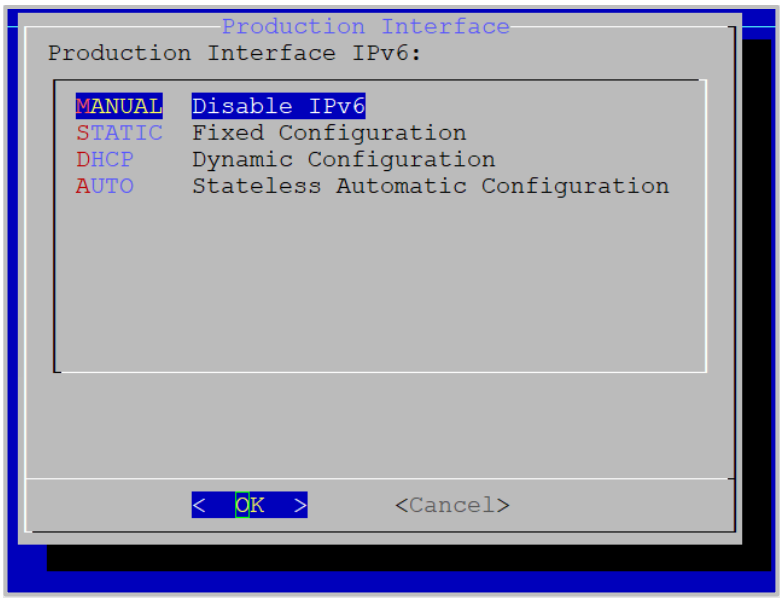


15. Press the **Enter** key to select **OK**. The *Confirm* window displays.



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**.

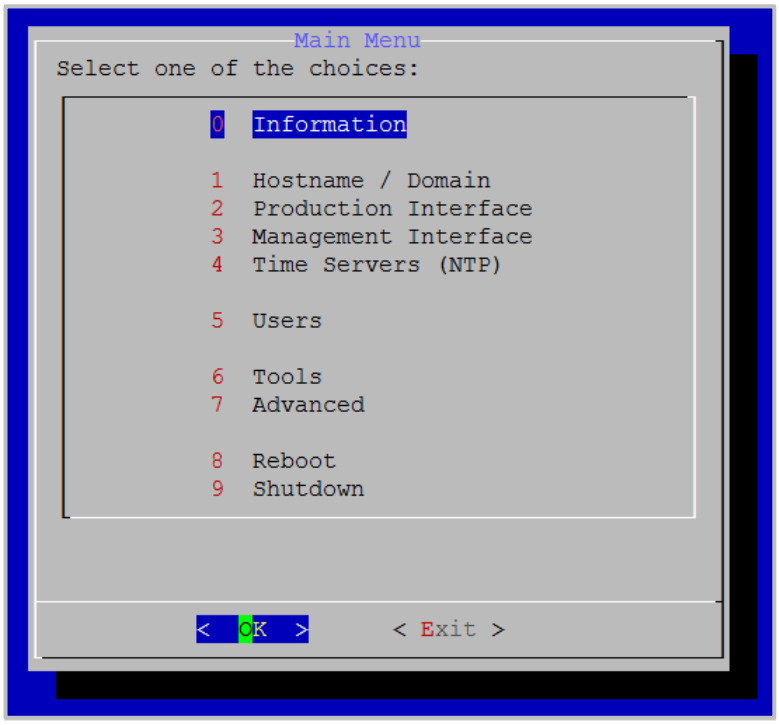
    For more information about configuring the Production and Management interfaces, see Configure the Production Interface and Configure the Management Interface.



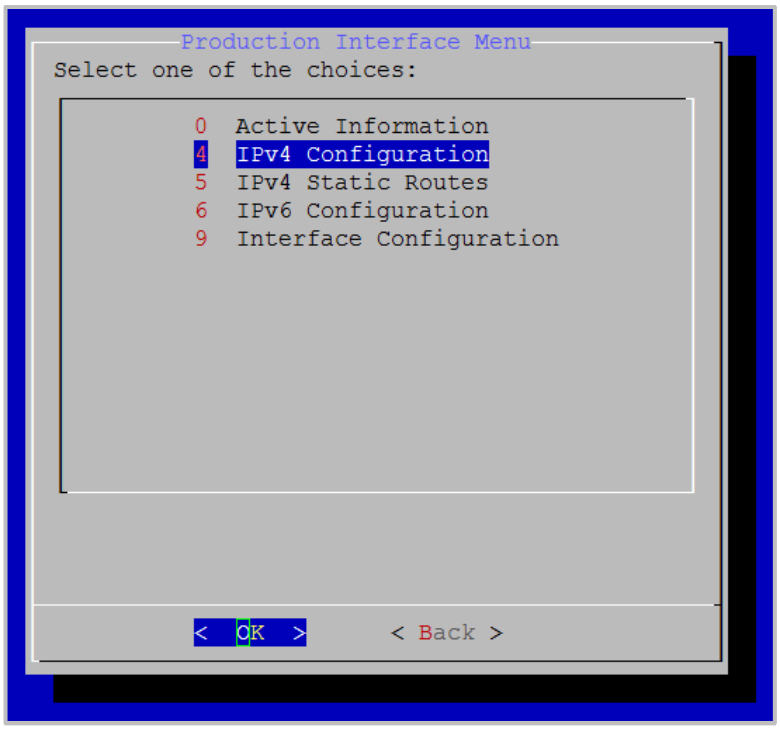
Configure stateless automatic configuration

To configure stateless automatic configuration:

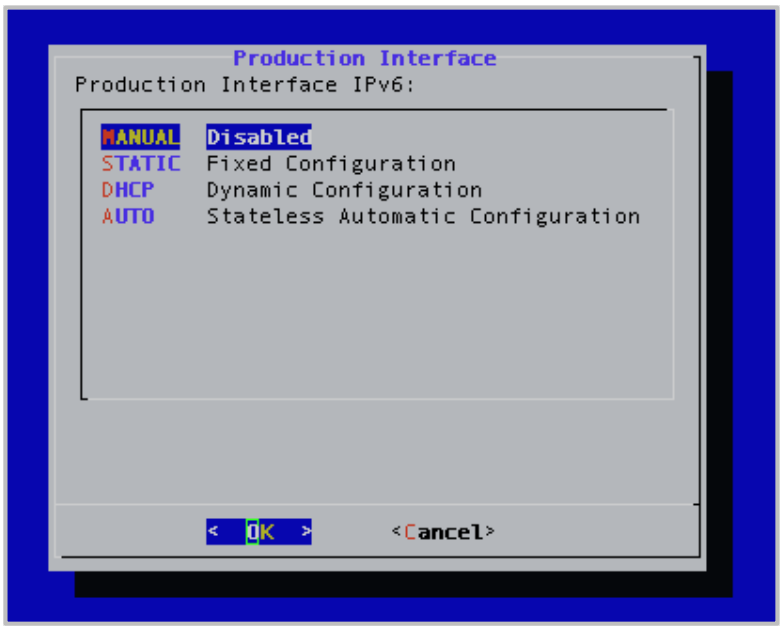
1. Log in to the System Console. The Main Menu displays.



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



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



6. Enter **A** to select the AUTO option.
7. Press the **Enter** key to select **OK**. The *Confirm* window displays.

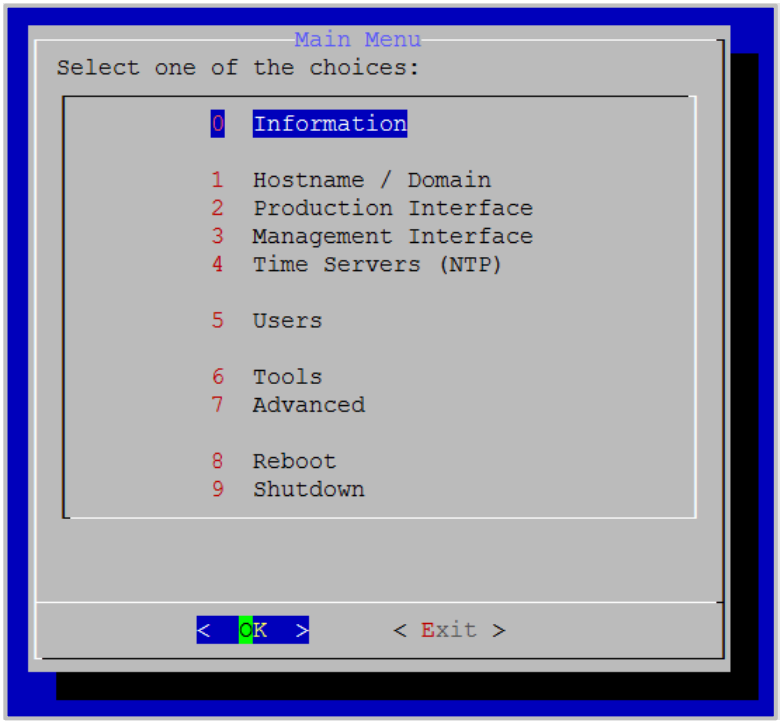
8. Press the **Enter** key to select **Yes**. A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
9. Press the **Enter** key to select **OK**.

Configure the MTU and auto negotiation for the Production Interface

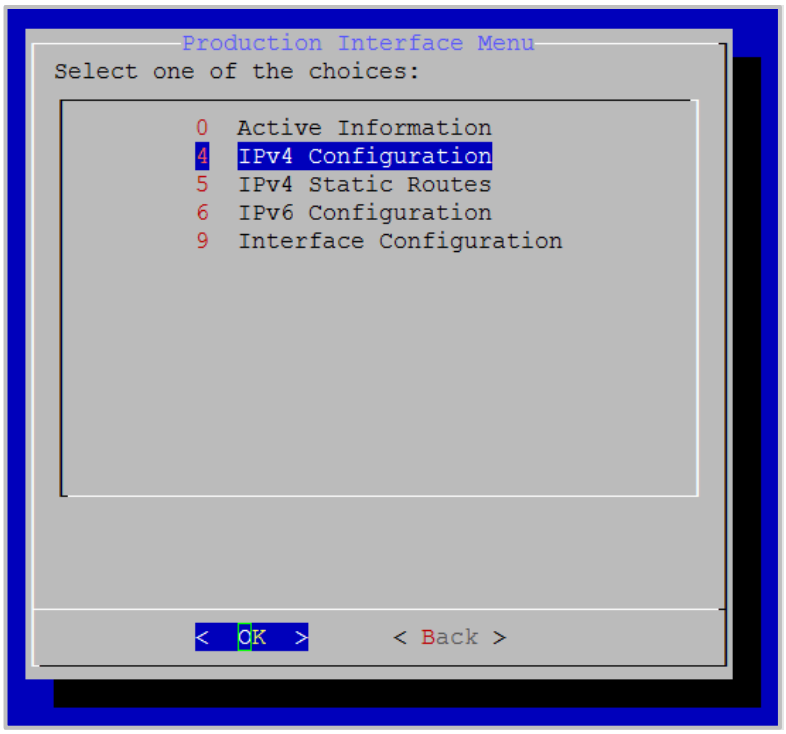
Configure the Maximum Transmission Unit (MTU)

To configure the Maximum Transmission Unit (MTU):

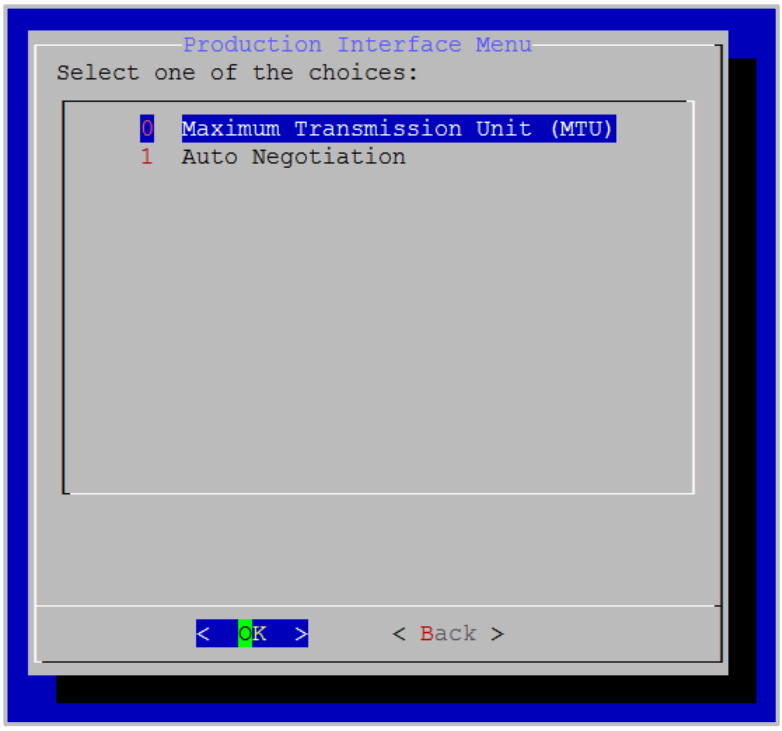
1. Log in to the System Console. The Main Menu displays.



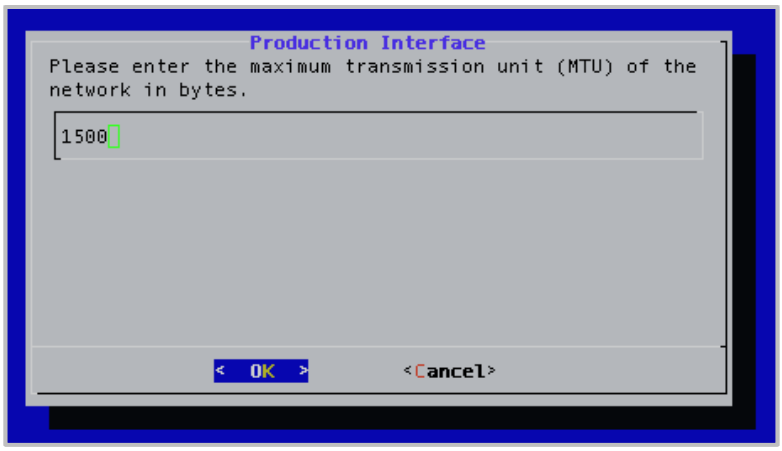
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**. The Production Interface Menu displays.



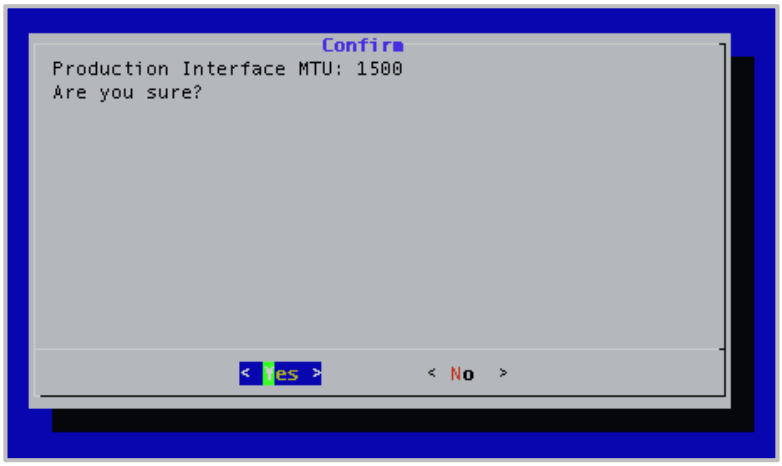
4. Enter **9** to select the Interface Configuration option.
5. Press the **Enter** key to select **OK**. The Production Interface Menu displays.



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



8. Press the **Enter** key to select **OK**. A *Confirm* window displays.

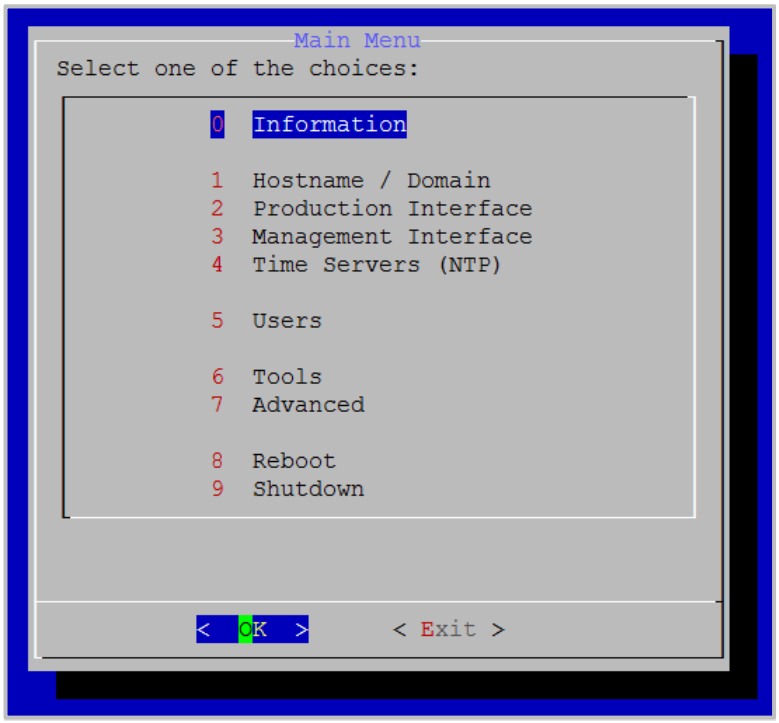


9. Press the **Enter** key to select **Yes**. A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
10. Press the **Enter** key to select **OK**.

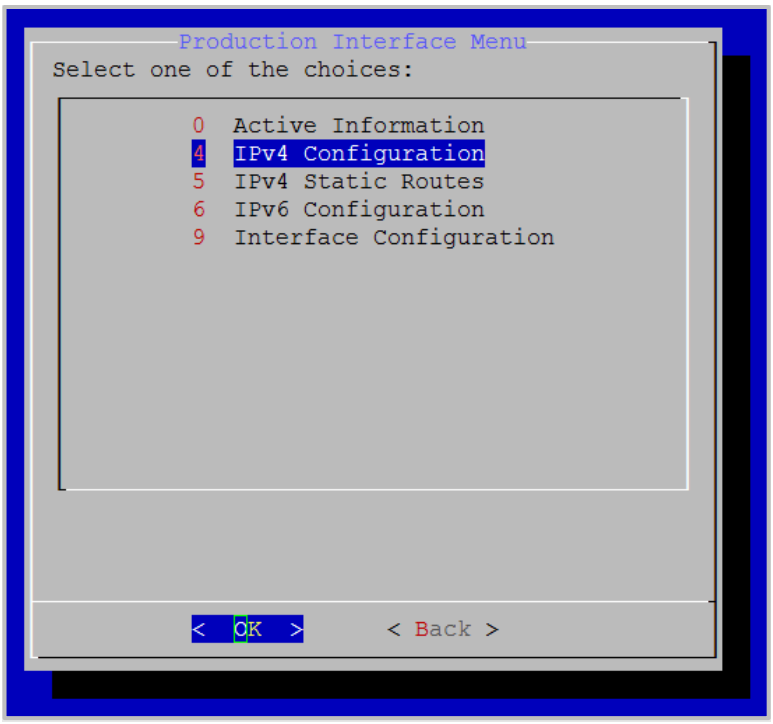
Configure auto negotiation

To configure auto negotiation:

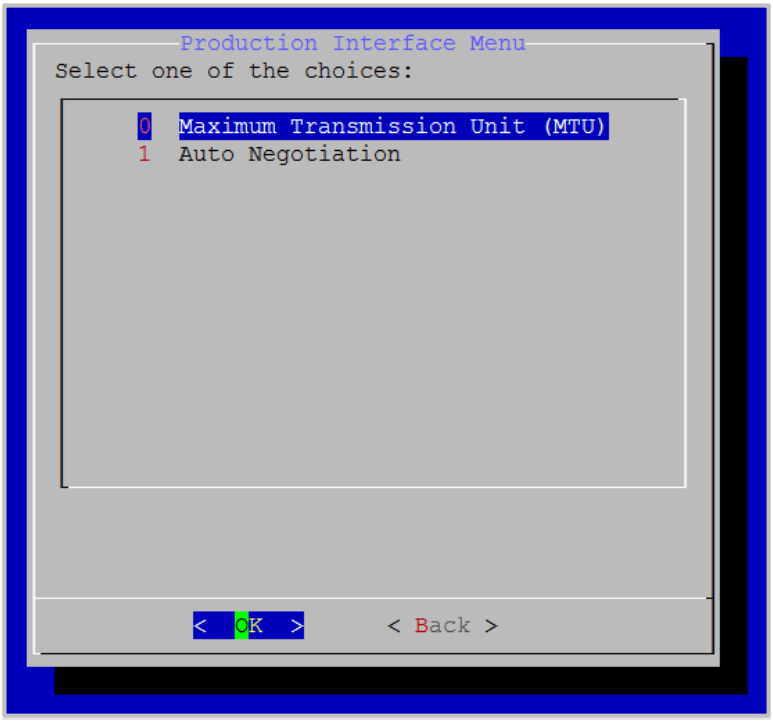
1. Log in to the System Console. The Main Menu displays.



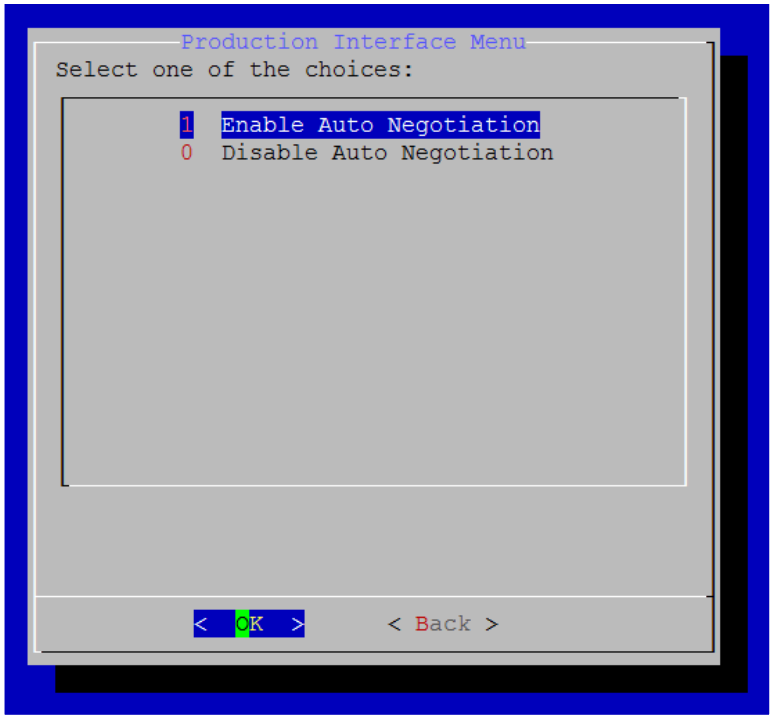
2. Enter **2** to select the Production Interface option.
3. Press the **Enter** key to select **OK**. The Production Interface Menu displays.



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



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



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**.

Configure 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.

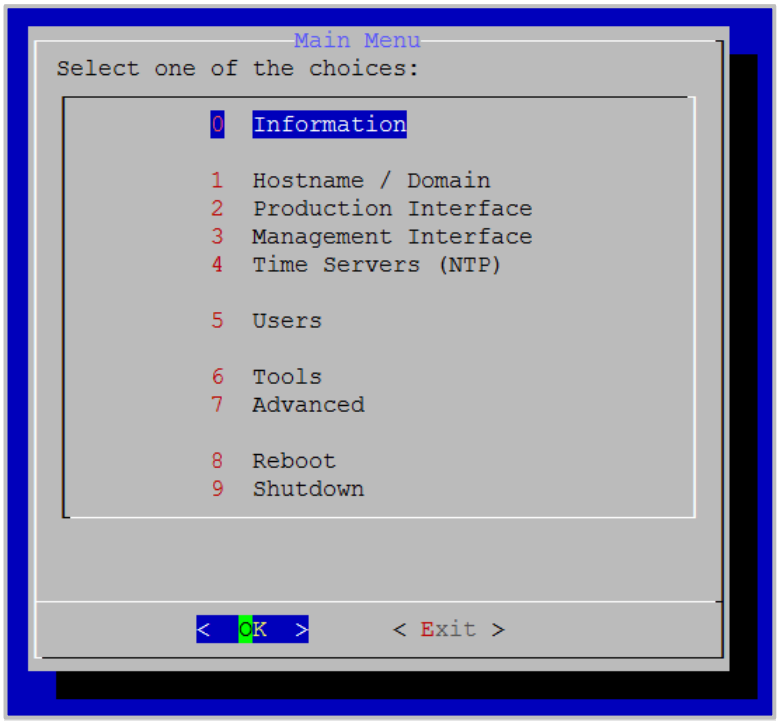
The Management Interface should not be used to transfer any media.

View 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.

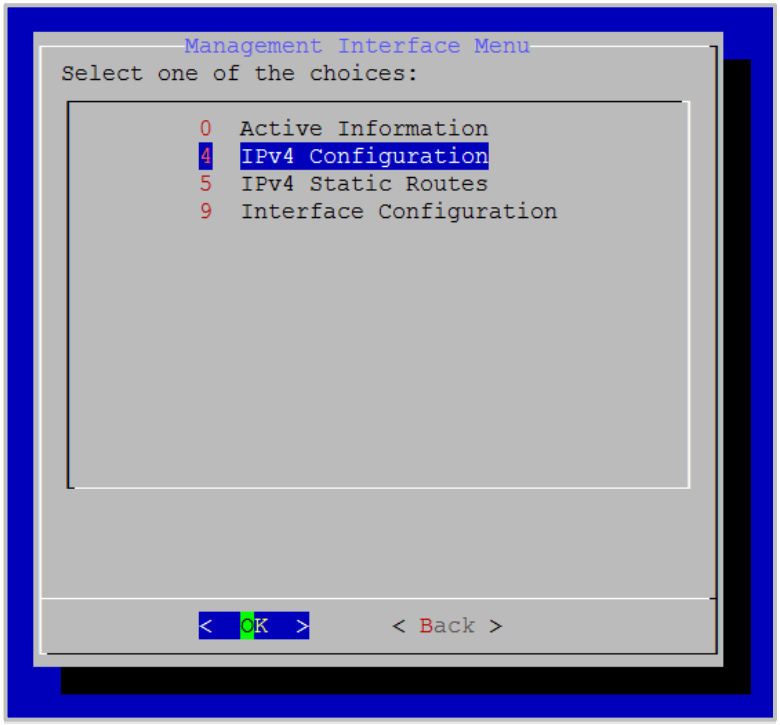
To view the Management Interface active information:

1. Log in to the System Console. The Main Menu displays.

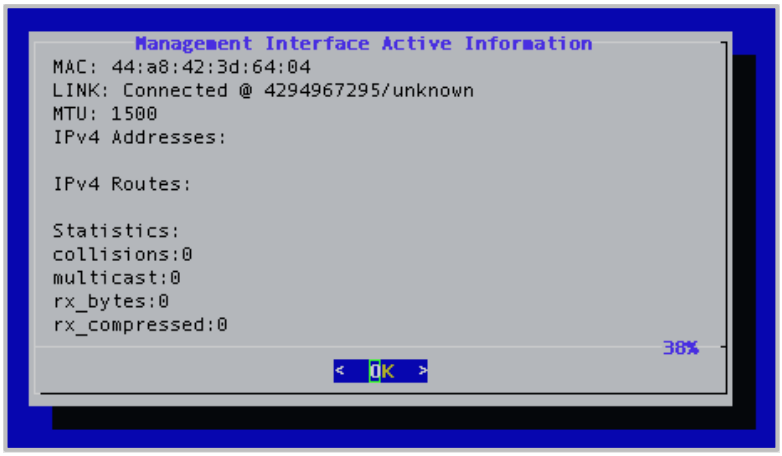


2. Enter **3** to select the Management Interface option.

3. Press the **Enter** key to select **OK**. The Management Interface Menu displays.



4. Enter **0** to select the Active Information option.
5. Press the **Enter** key to select **OK**. The Management Interface Active Information window displays.



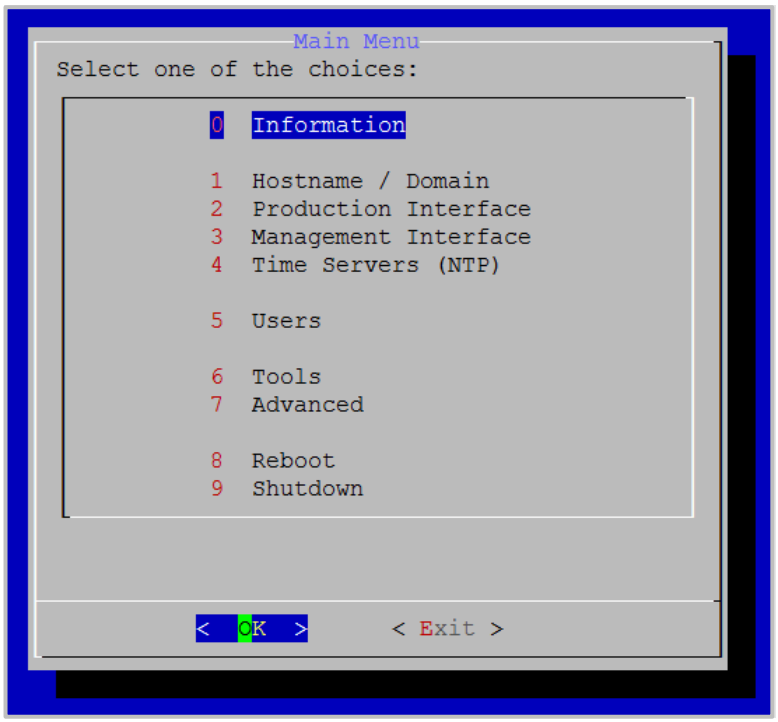
Configure the IPv4 Management Interface

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.

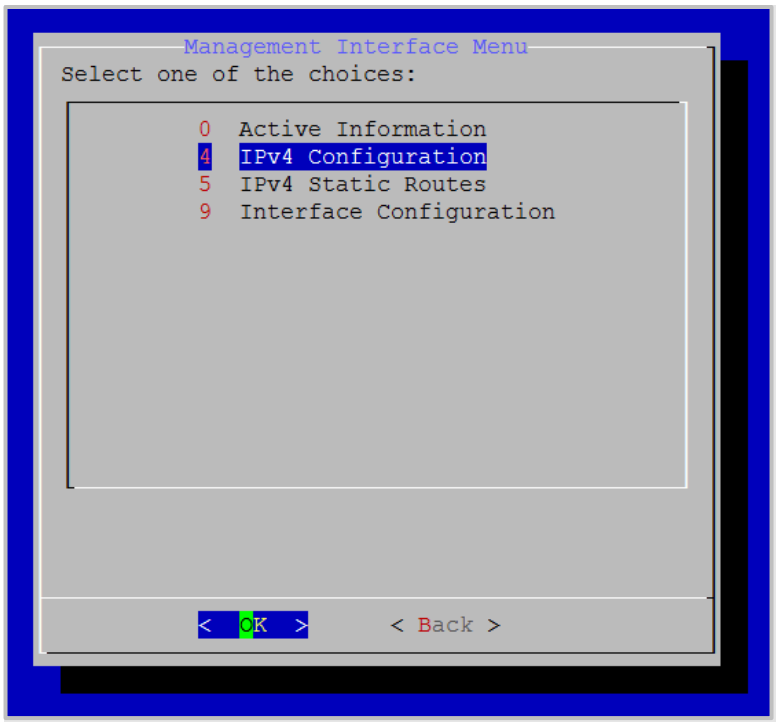
Manually disable and enable the IPv4 Management Interface

To manually disable or enable the IPv4 Management Interface:

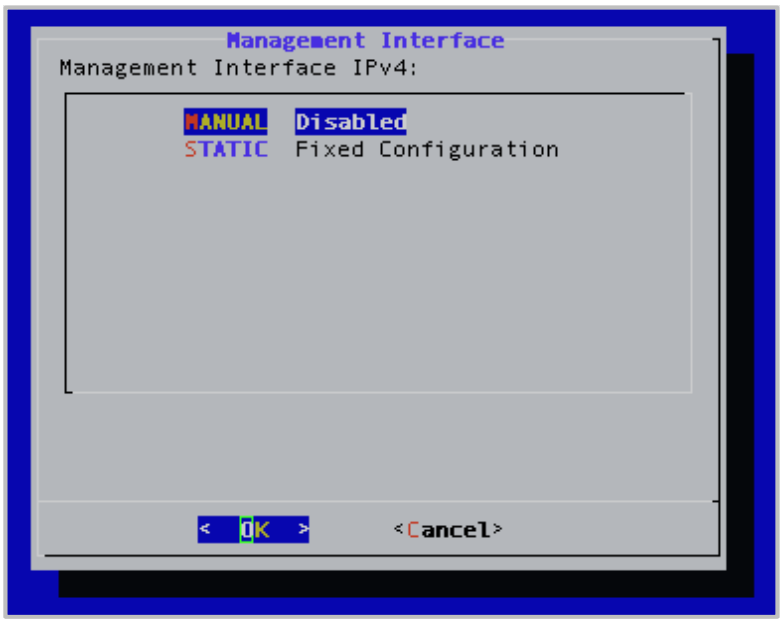
1. Log in to the System Console. The Main Menu displays.



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



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



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

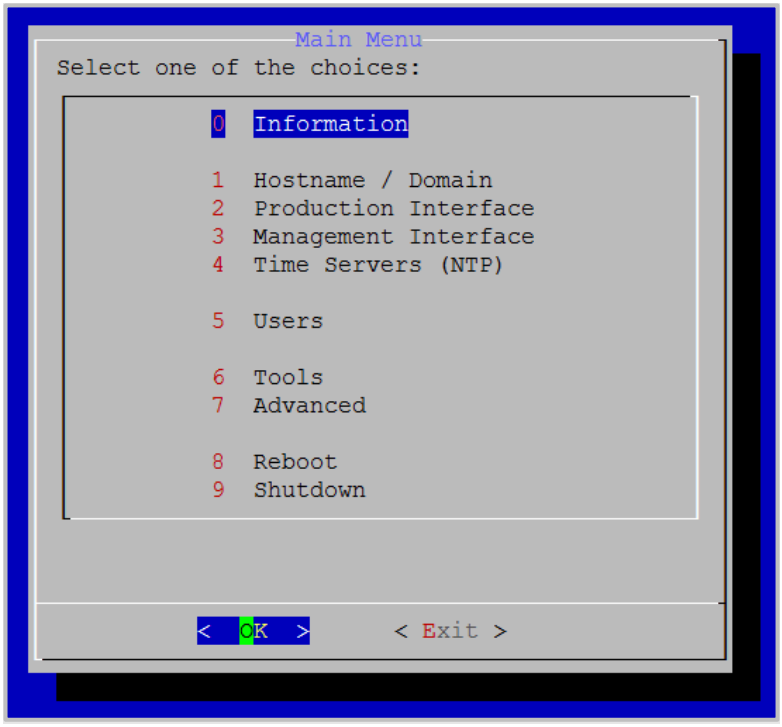
   If the current state of the Management Interface is enabled, you are asked to confirm if you want to disable it; if the current state of the Management Interface is disabled, you are asked to confirm if you want to enable it.

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**.

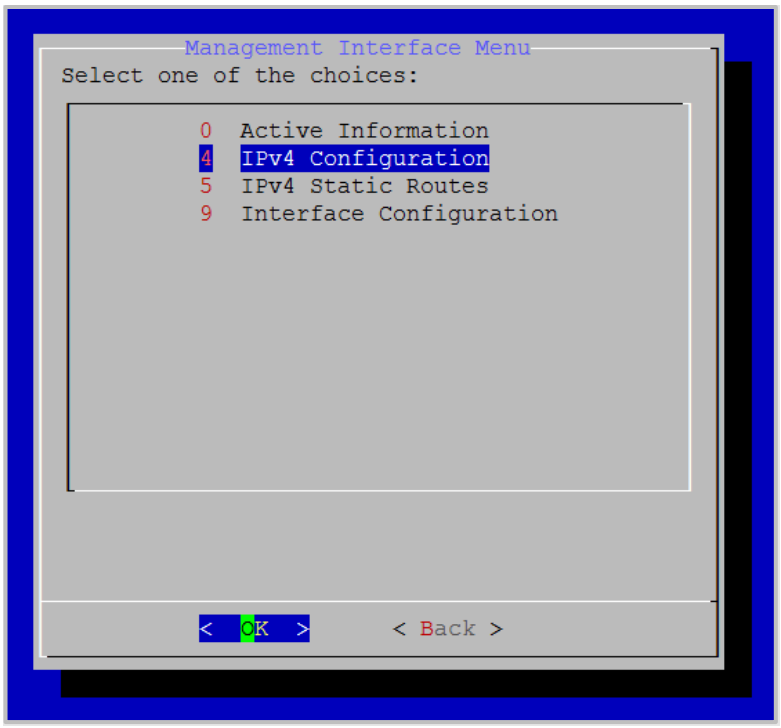
Configure an IPv4 static Management Interface

To configure an IPv4 static Management Interface:

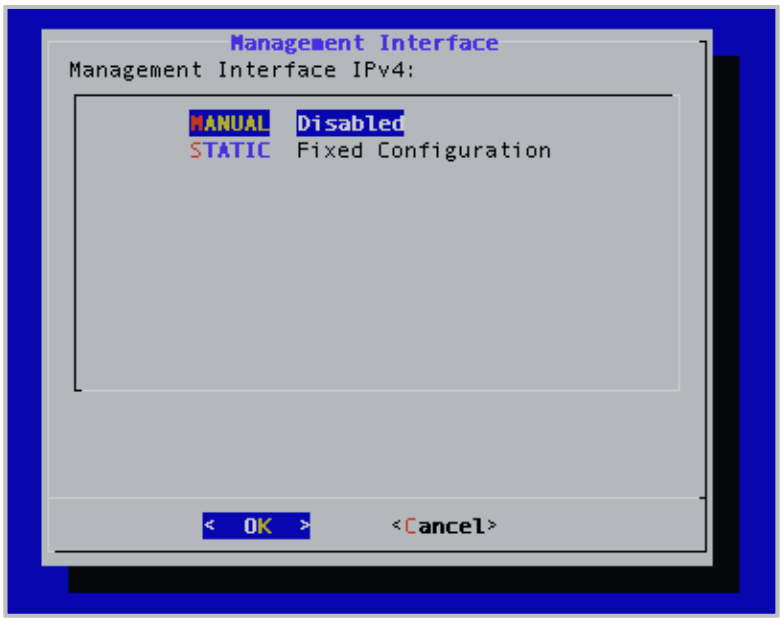
1. Log in to the System Console. The Main Menu displays.



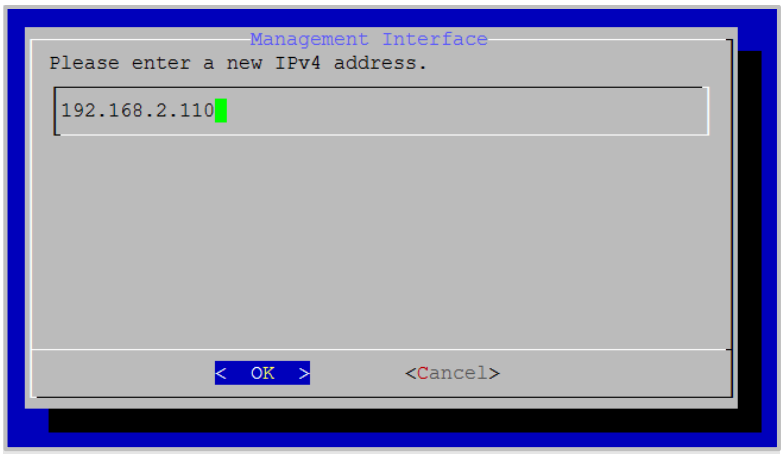
2. Enter **3** to select the Management Interface option.
3. Press the **Enter** key to select **OK**. The Management Interface Menu displays.



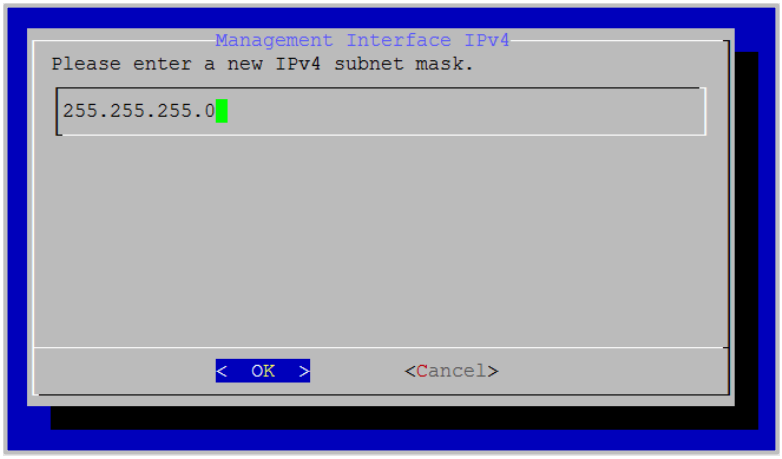
4. Enter **4** to select the IPv4 Configuration option.
5. Press the **Enter** key to select **OK**.
6. Enter **S** to select the STATIC option.



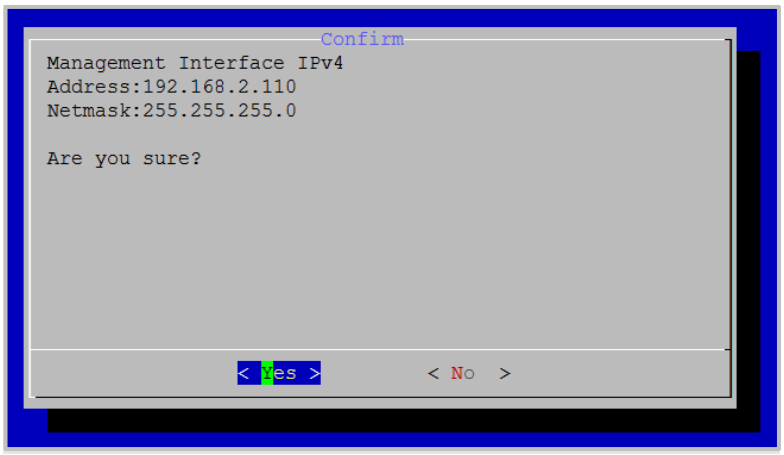
7. Press the **Enter** key to select **OK**.
8. Delete the existing IPv4 address and enter a new one.



9. Press the **Enter** key to select **OK**.
10. Delete the existing IPv4 subnet mask and enter a new one.



11. Press the **Enter** key to select **OK**. The *Confirm* window displays.



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 Configure the Production Interface and Configure the Management Interface.

Configure IPv4 Static Routes

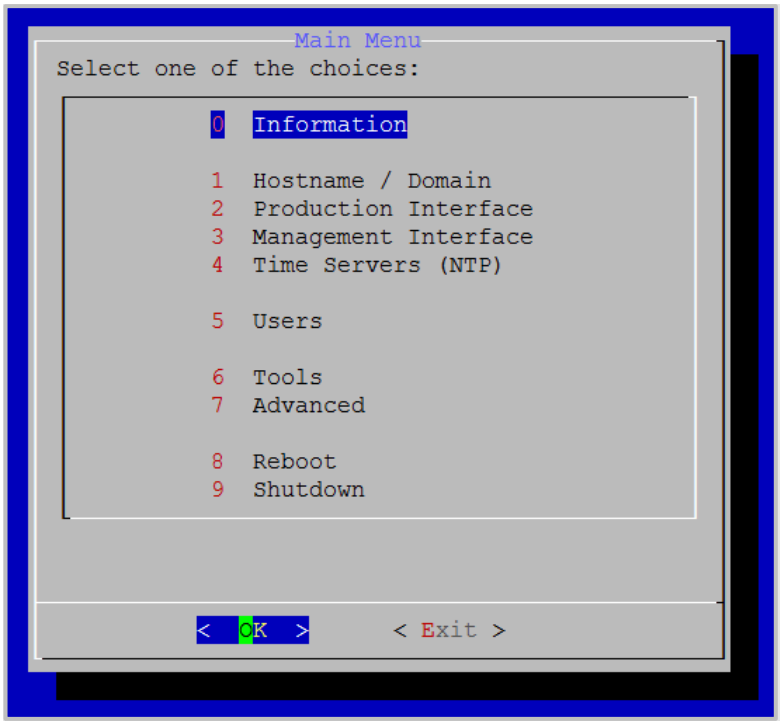
This section describes how to add and remove IPv4 static routes.

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

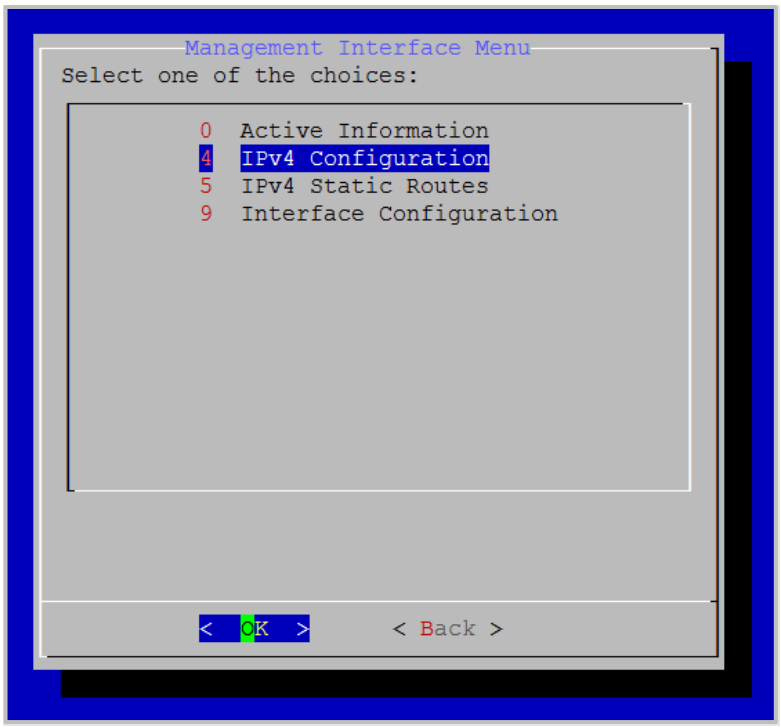
Add IPv4 Static Routes

To add IPv4 Static Routes:

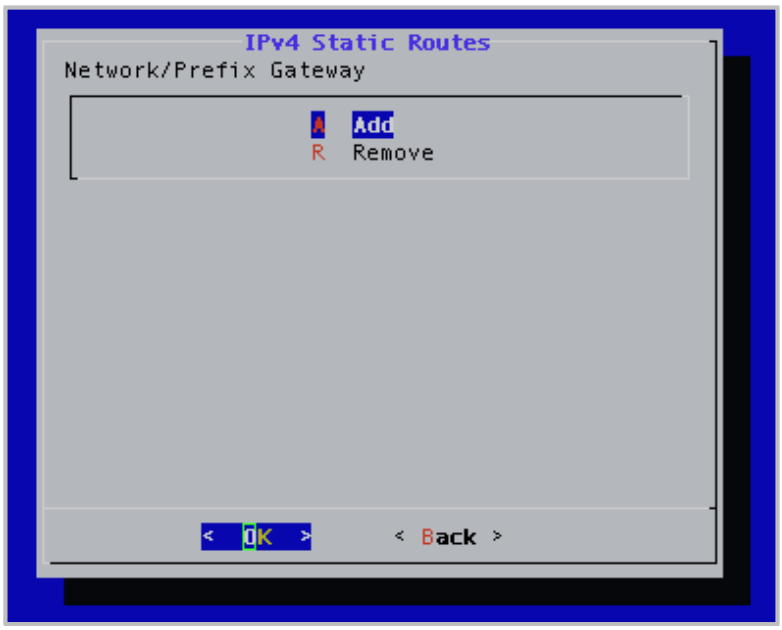
1. Log in to the System Console. The Main Menu displays.



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

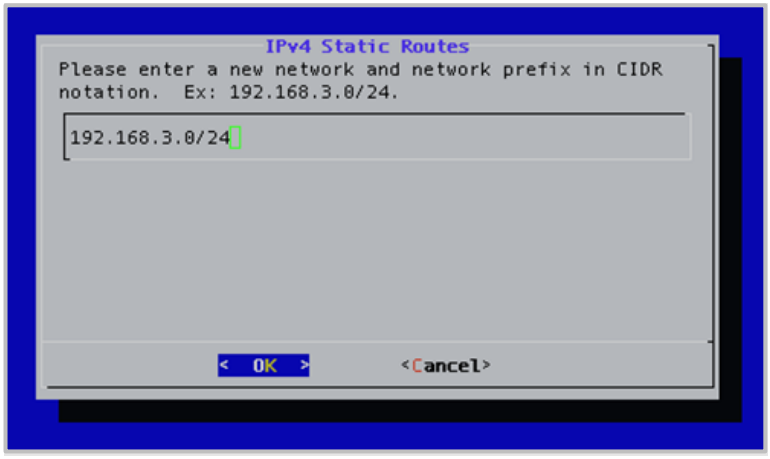


4. Enter **5** to select the IPv4 Static Routes option.
5. Press the **Enter** key to select **OK**. The *IPv4 Static Routes* window displays.

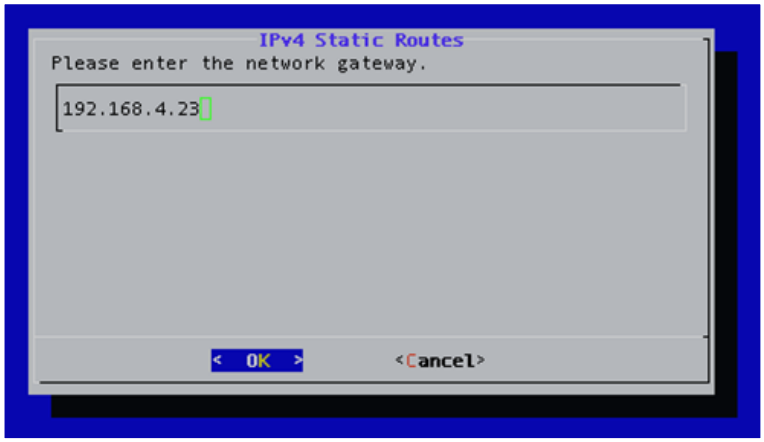


6. Enter **A** to select the Add option.

7. Press the **Enter** key to select **OK**. The *IPv4 Static Route*s window displays.



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.



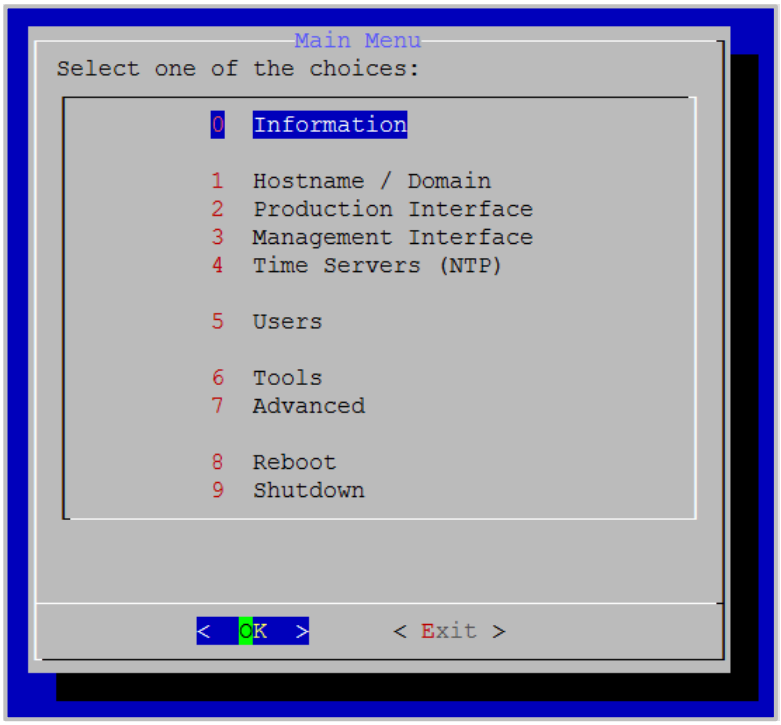
11. Press the **Enter** key to select **OK**. The *Confirm* window displays.

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**.

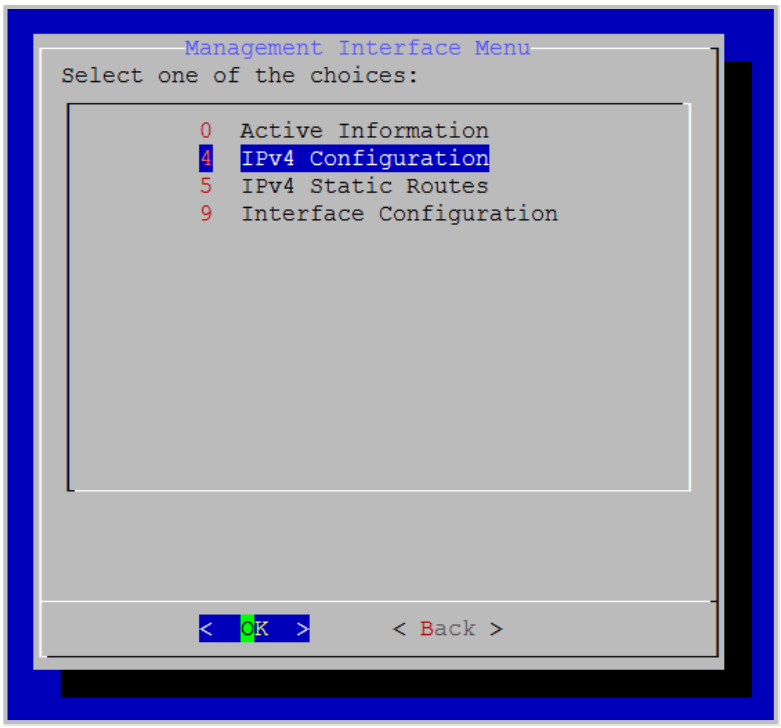
Remove IPv4 Static Routes

To remove IPv4 static routes:

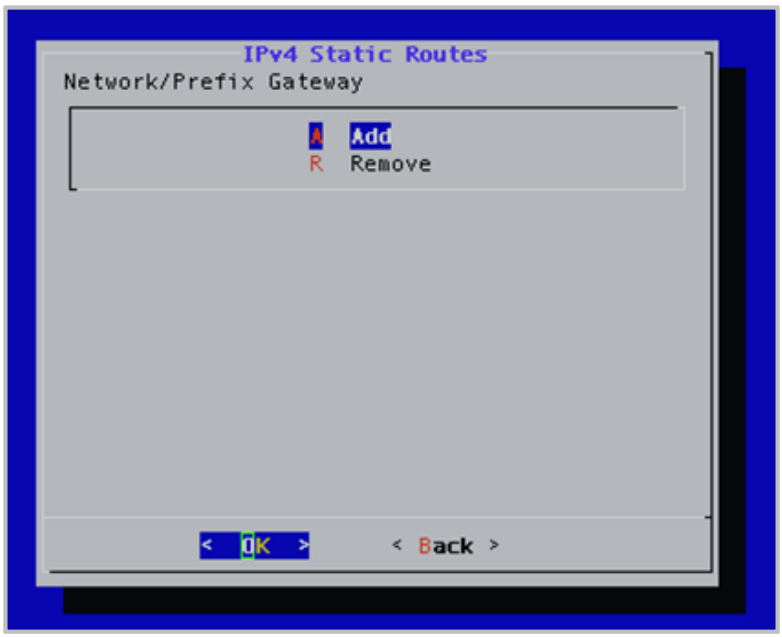
1. Log in to the System Console. The Main Menu displays.



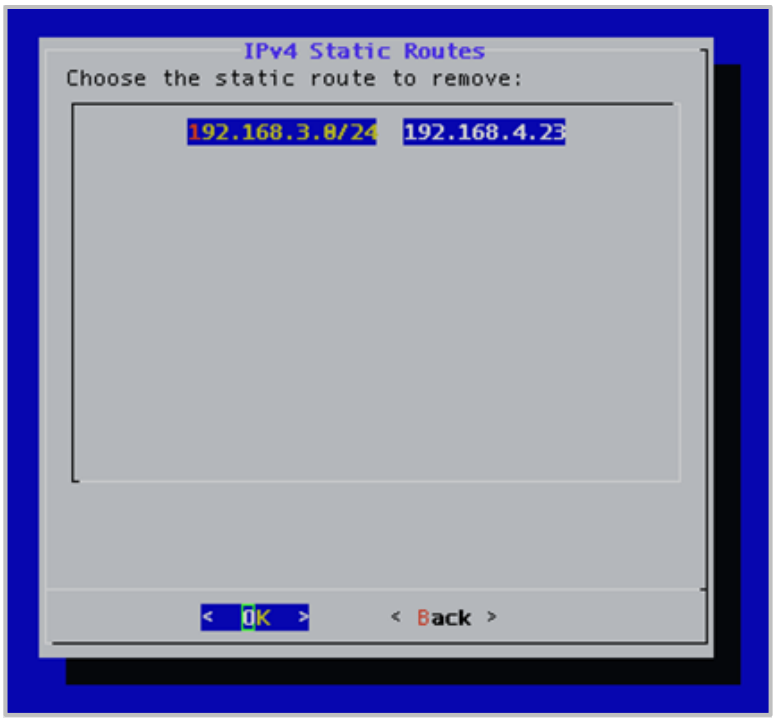
2. Enter **3** to select the Management Interface option.
3. Press the **Enter** key to select **OK**. The Management Interface Menu displays.



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



6. Enter **R** to select the Remove option.
7. Press the **Enter** key to select **OK**. The *IPv4 Static Routes* window displays.



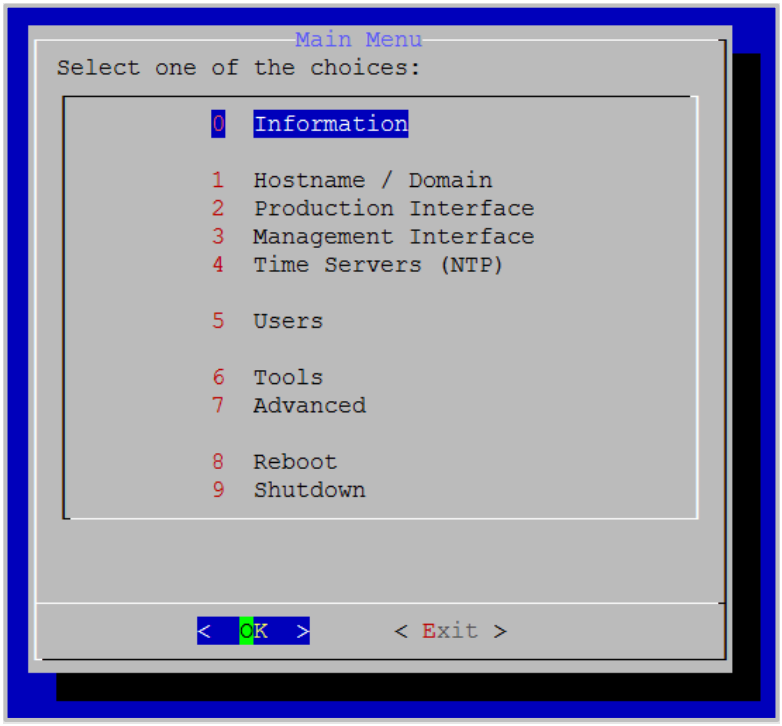
8. Select the static route to remove.
9. Press the **Enter** key to select **OK**. The *Confirm* window displays.
10. Press the **Enter** key to select **Yes**. A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
11. Press the **Enter** key to select **OK**.

Configure the MTU and auto negotiation for the Management Interface

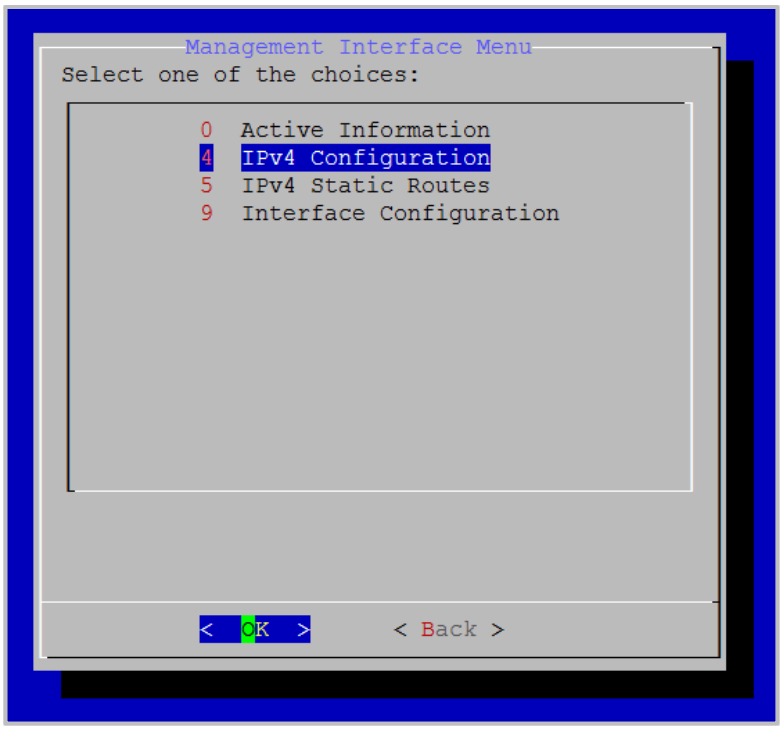
Configure the Maximum Transmission Unit (MTU)

To configure the Maximum Transmission Unit (MTU):

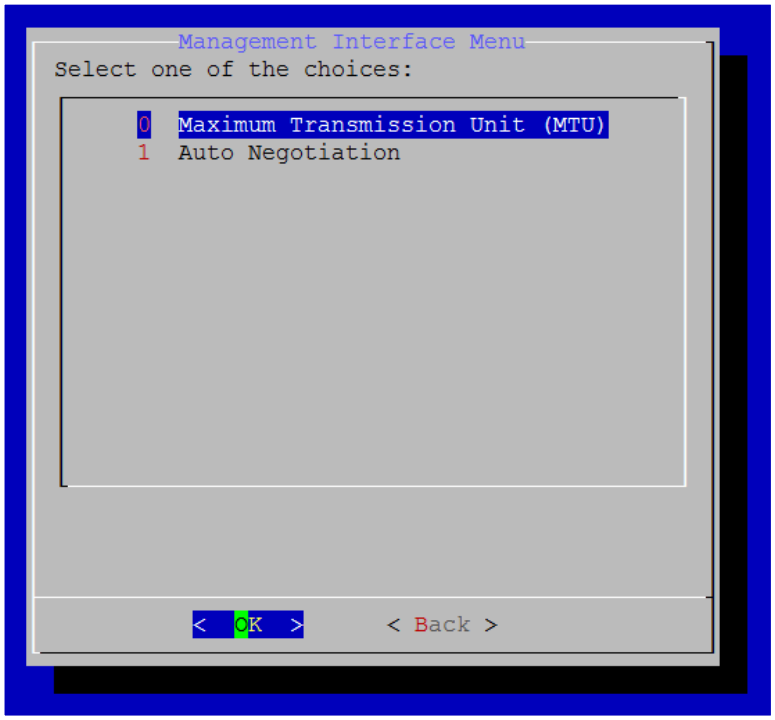
1. Log in to the System Console. The Main Menu displays.



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

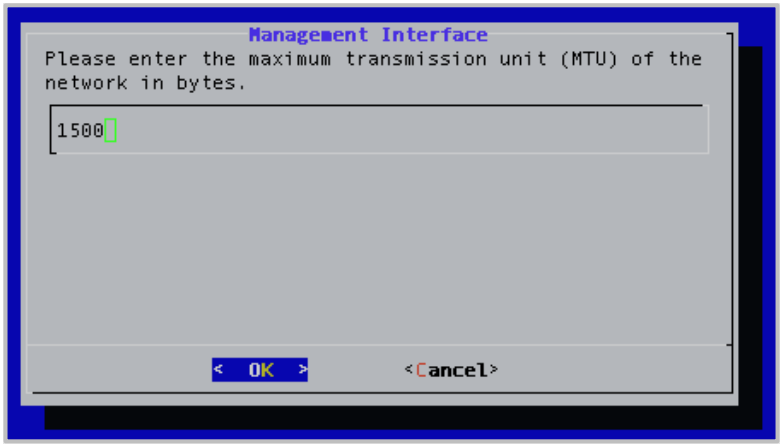


4. Enter **9** to select the Interface Configuration option.
5. Press the **Enter** key to select **OK**.

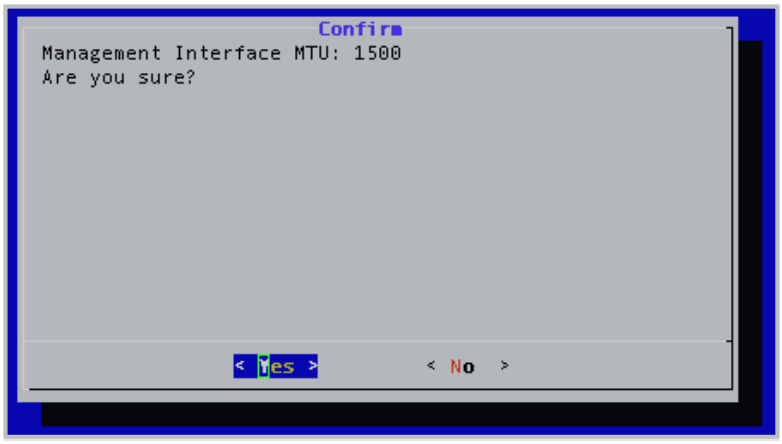


6. Enter **0** to select the Maximum Transmission Unit (MTU) option.
7. Press the **Enter** key to select **OK**.

8. Enter the MTU of the networks in bytes.



9. Press the **Enter** key to select **OK**. A *Confirm* window displays.

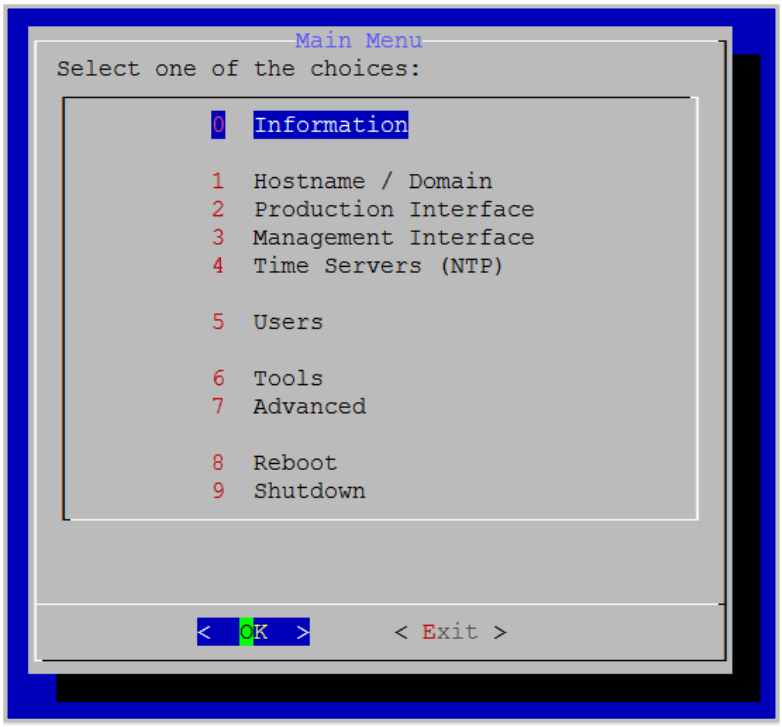


10. Press the **Enter** key to select **Yes**. A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
11. Press the **Enter** key to select **OK**.

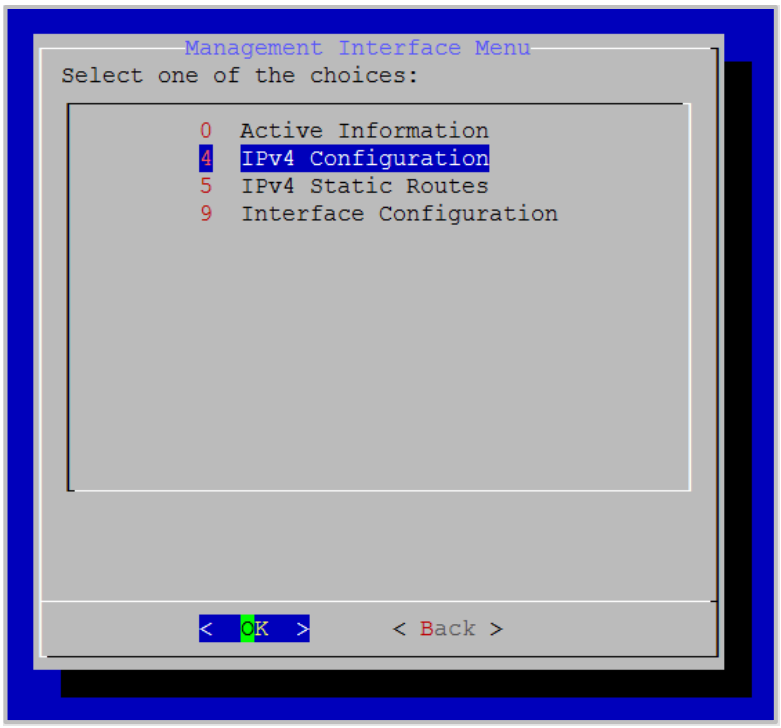
Configure auto negotiation

To configure auto negotiation:

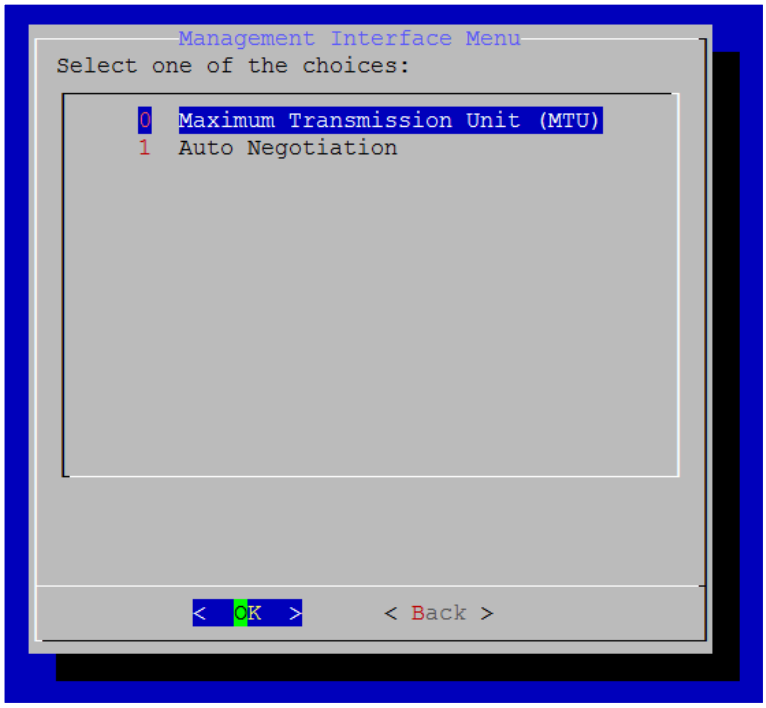
1. Log in to the System Console. The Main Menu displays.



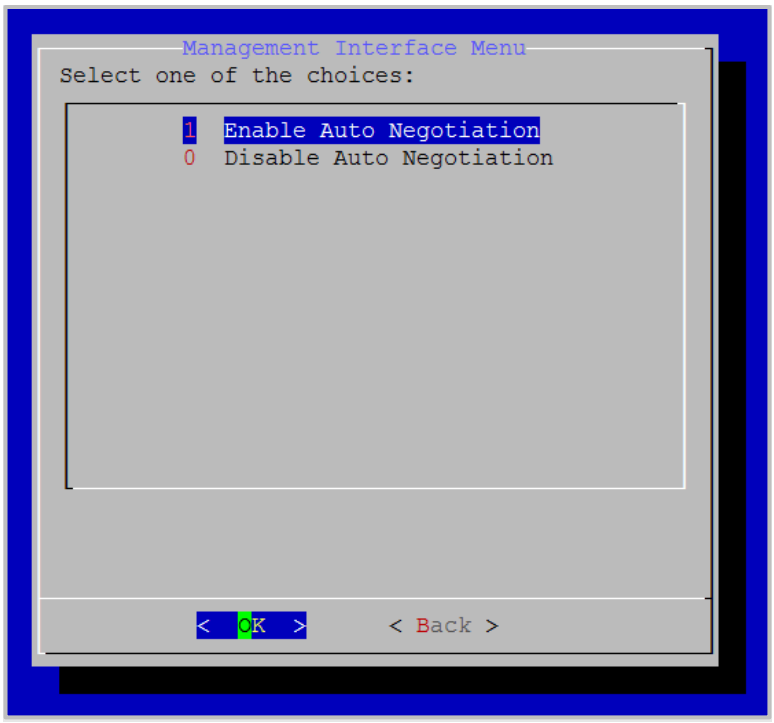
2. Enter **3** to select the Management Interface option.
3. Press the **Enter** key to select **OK**. The Management Interface Menu displays.



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



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

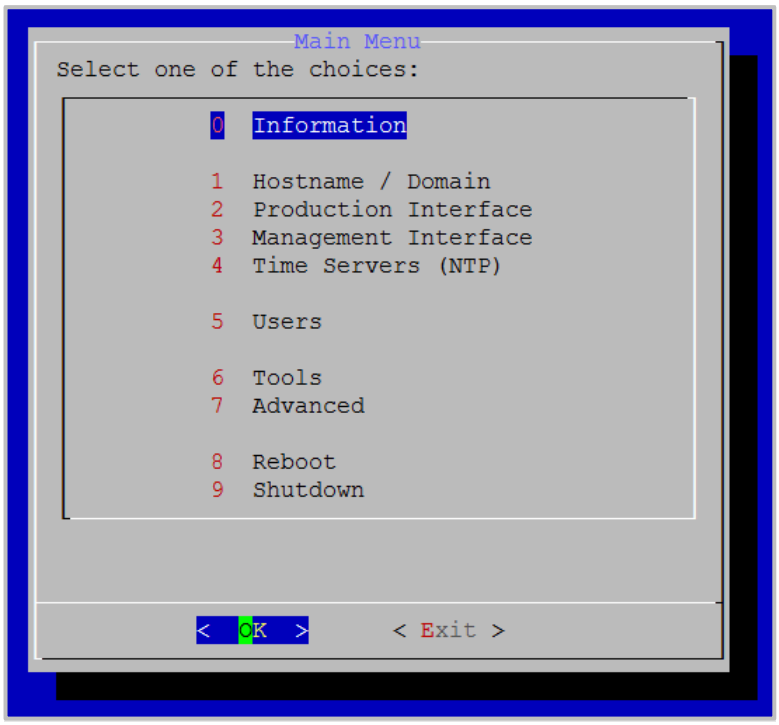


8. Enter **1** to enable Auto Negotiation or enter **0** to disable Auto Negotiation. A *Confirm* window displays.
9. Press the **Enter** key to select **Yes**. A message displays stating “Changes saved. Reboot REQUIRED for changes to take effect.”
10. Press the **Enter** key to select **OK**.

Configure time servers (NTP)

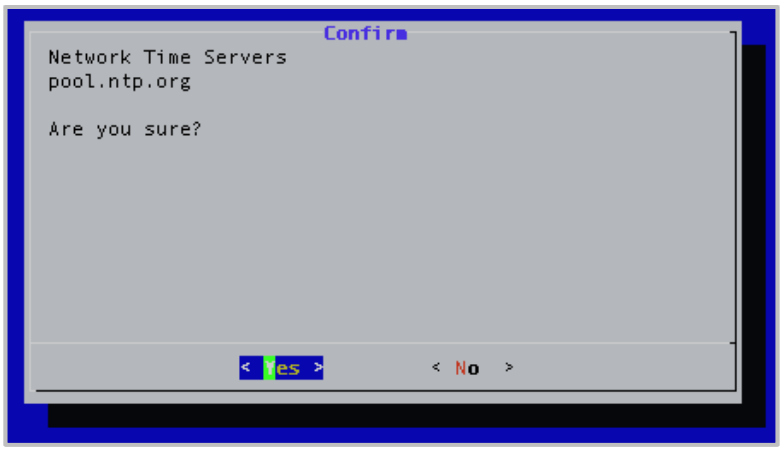
To configure time servers (NTP):

1. Log in to the System Console. The Main Menu displays.



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 name servers 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.



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**.
8. A message displays stating “System time updated.”

Configure users

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

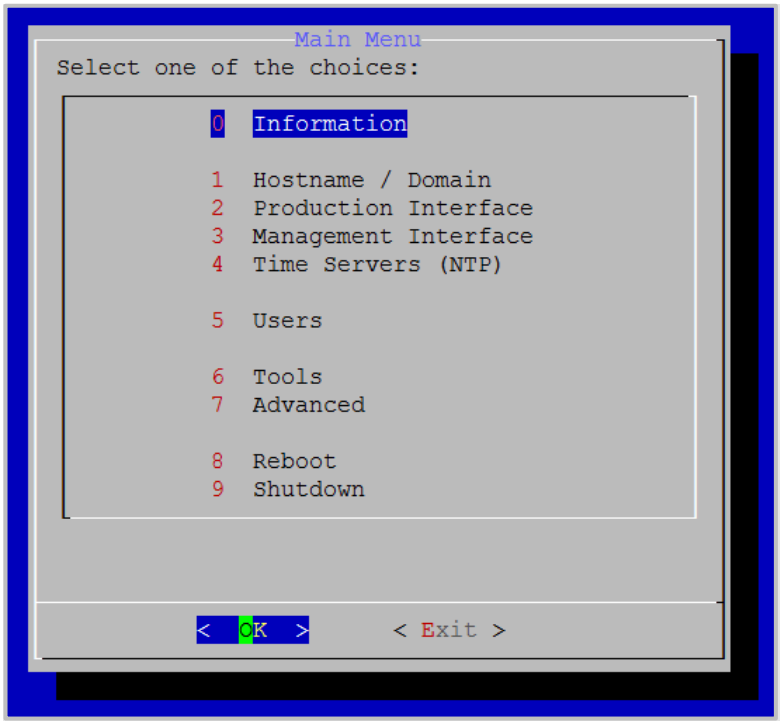
The System Console allows for the creation of up to ten System Console user accounts.

> Note
>
> In addition to accessing the System Console menu, the ten System Console accounts can also access the VidyoReplay 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.

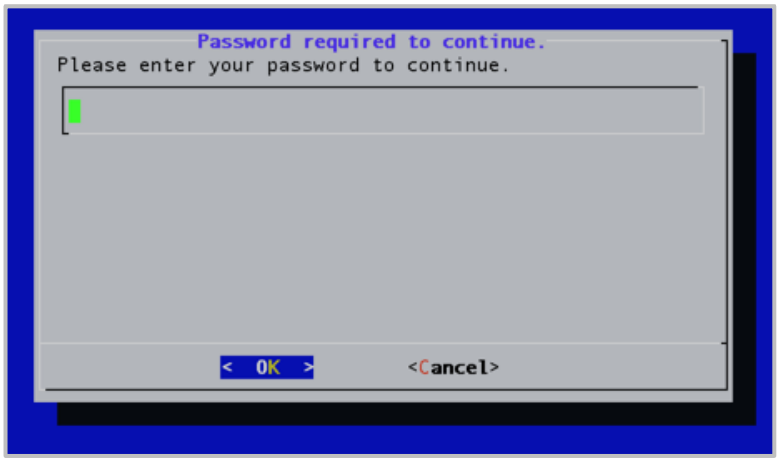
View active user information

To view active user information:

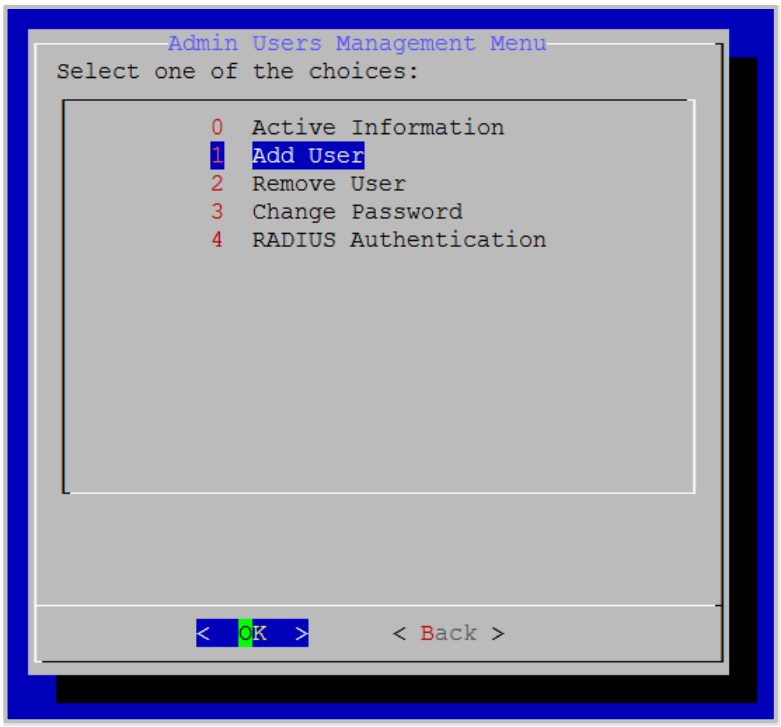
1. Log in to the System Console. The Main Menu displays.



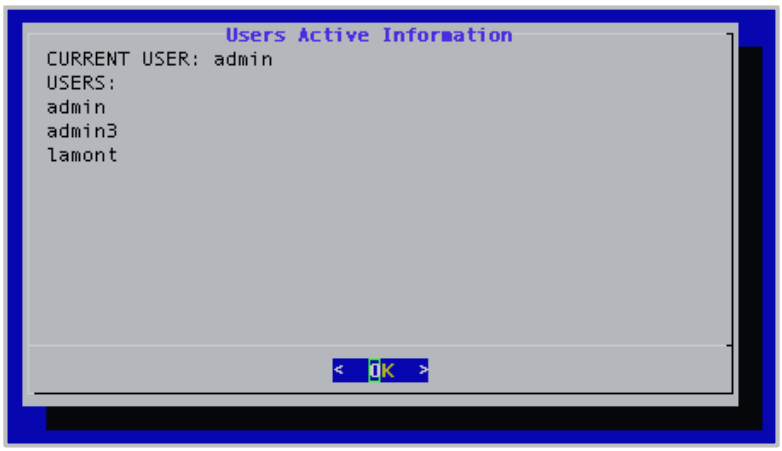
2. Enter **5** to select the Users option.
3. Press the **Enter** key to select **OK**. The *Password required to continu*e window displays.



4. Enter your password.
5. Press the **Enter** key to select **OK**. The Admin Users Management Menu displays.



6. Enter **0** to select the Active Information option.
7. Press the **Enter** key to select **OK**. The *Users Active Information* window displays.

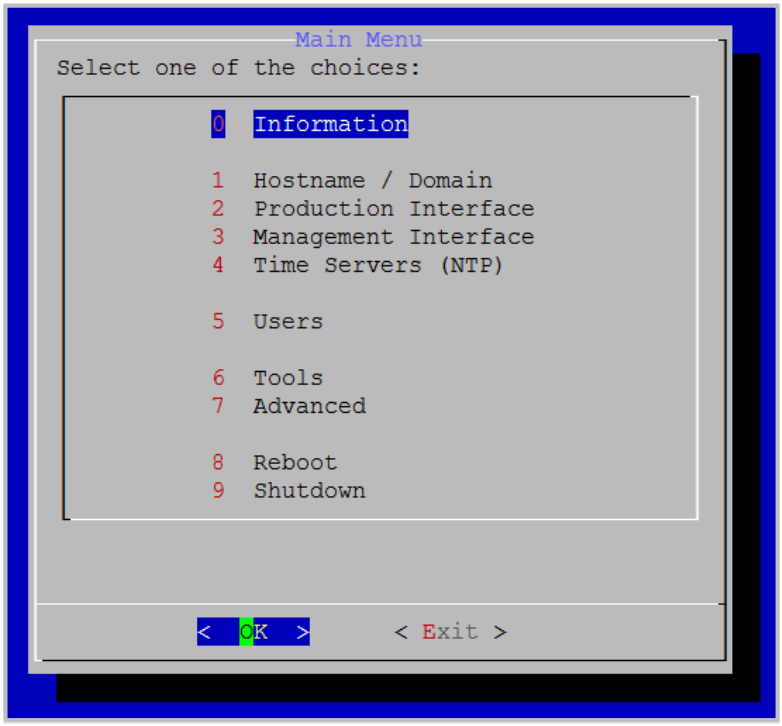


8. Press the **Enter** key to select **OK**.

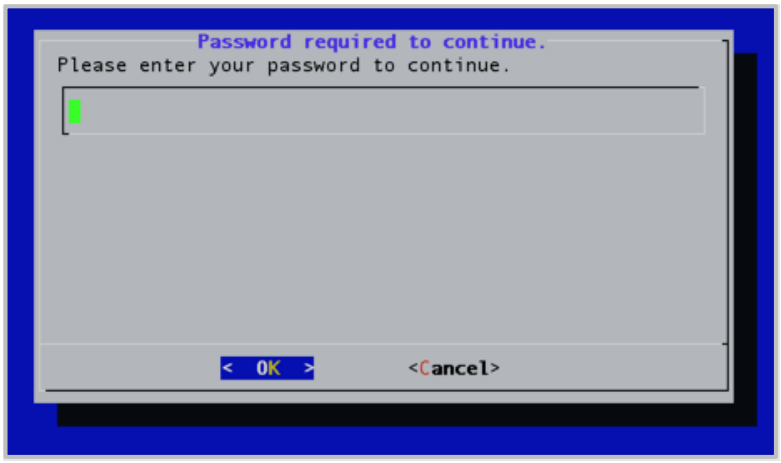
Add users

To add users:

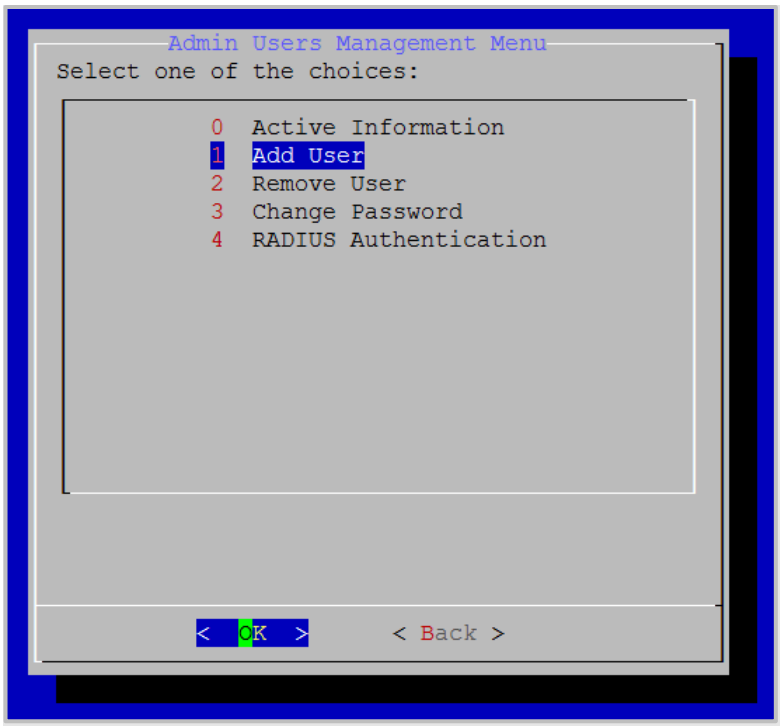
1. Log in to the System Console. The Main Menu displays.



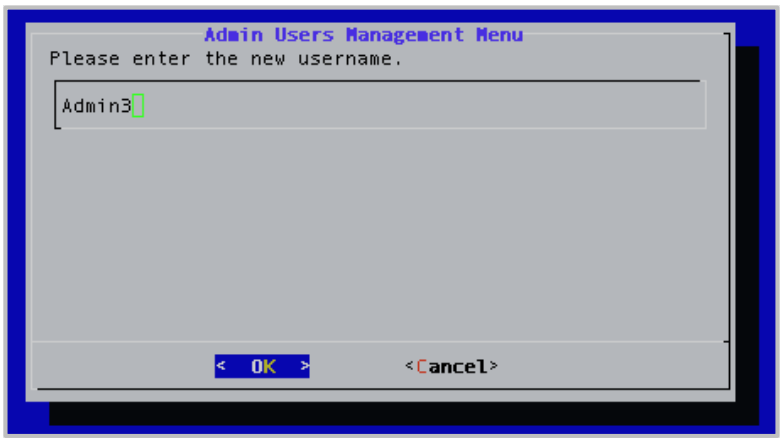
2. Enter **5** to select the Users option.
3. Press the **Enter** key to select **OK**. The *Password required to continue* window displays.



4. Enter your password.
5. Press the **Enter** key to select **OK**. The Admin Users Management Menu displays.

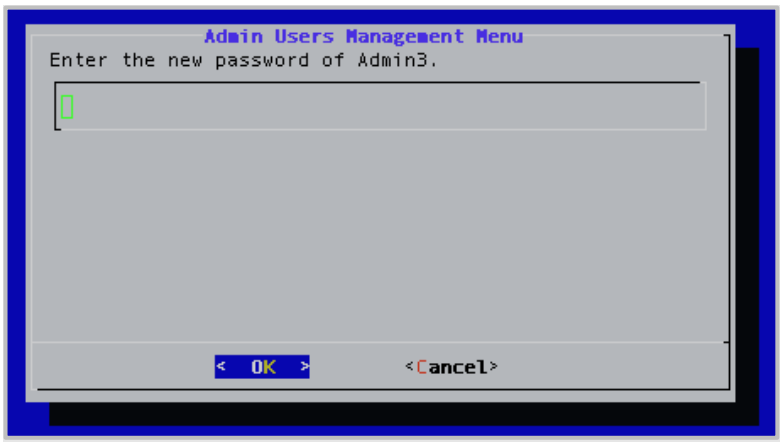


6. Enter **1** to select the Add Users option.
7. Press the **Enter** key to select **OK**.



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.

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

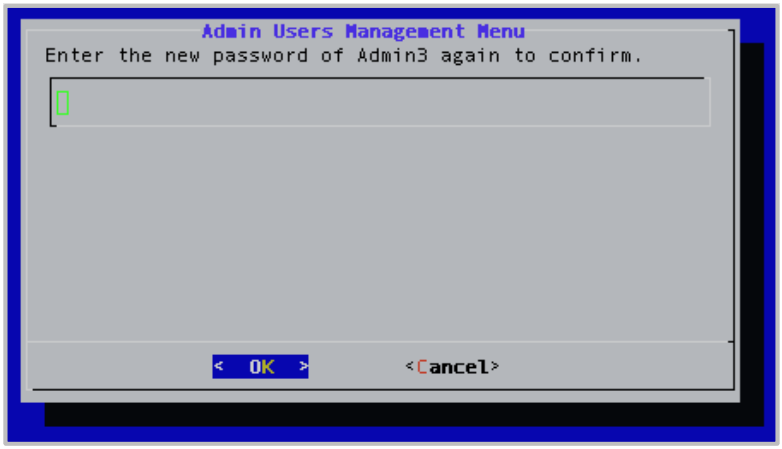


Enter a unique password that follows these password complexity requirements:

- The password should not be based on the dictionary.
- The password should not be too similar to the old password. The default setting is at least three characters 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 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**.



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.

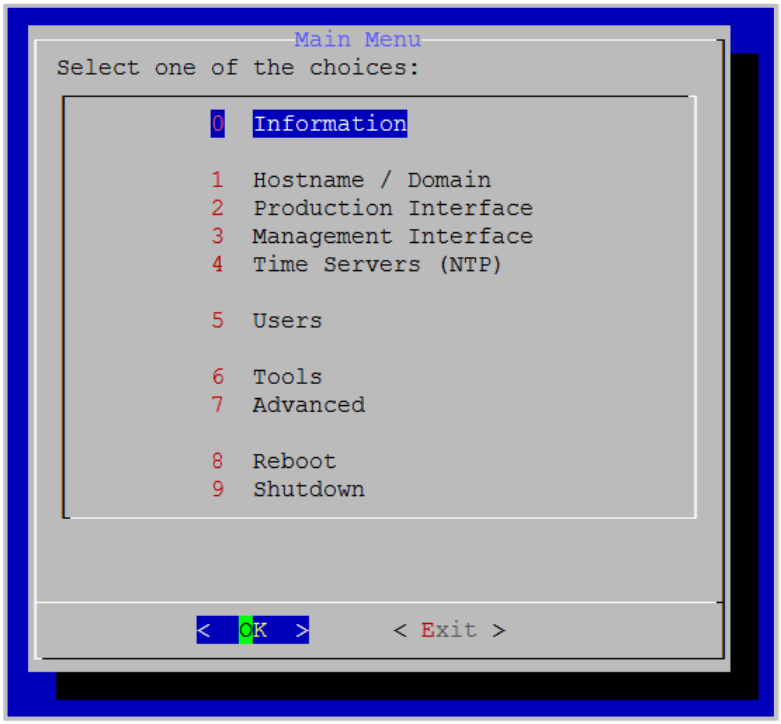
    > Note
    >
    > When you need to reset the password, use option `3. Change Password`. This functionality is only available for local admin accounts. See Change user passwords.

15. Press the **Enter** key to select **OK**. A message displays stating "[User] has been added."
16. Press the **Enter** key to select **OK**.

Remove users

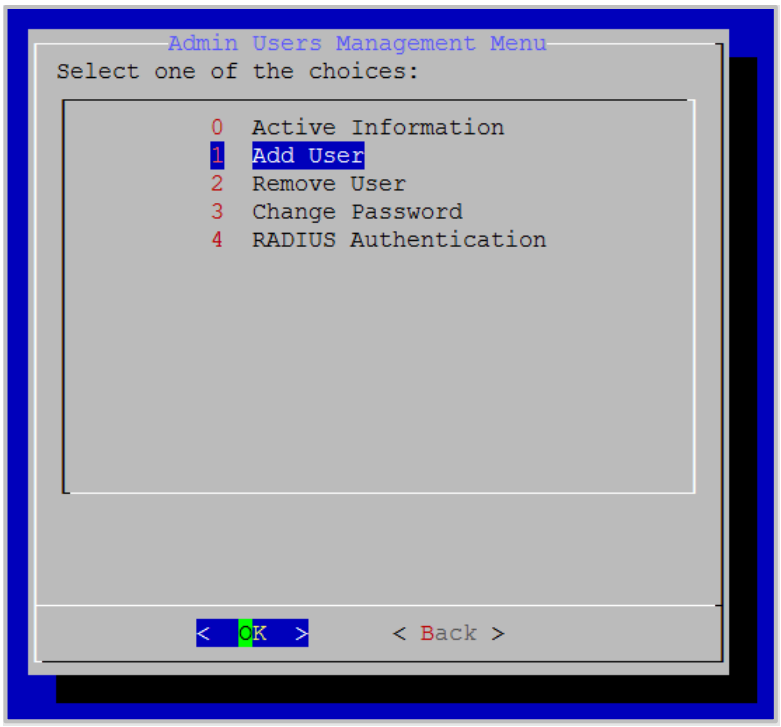
To remove users:

1. Log in to the System Console. The Main Menu displays.

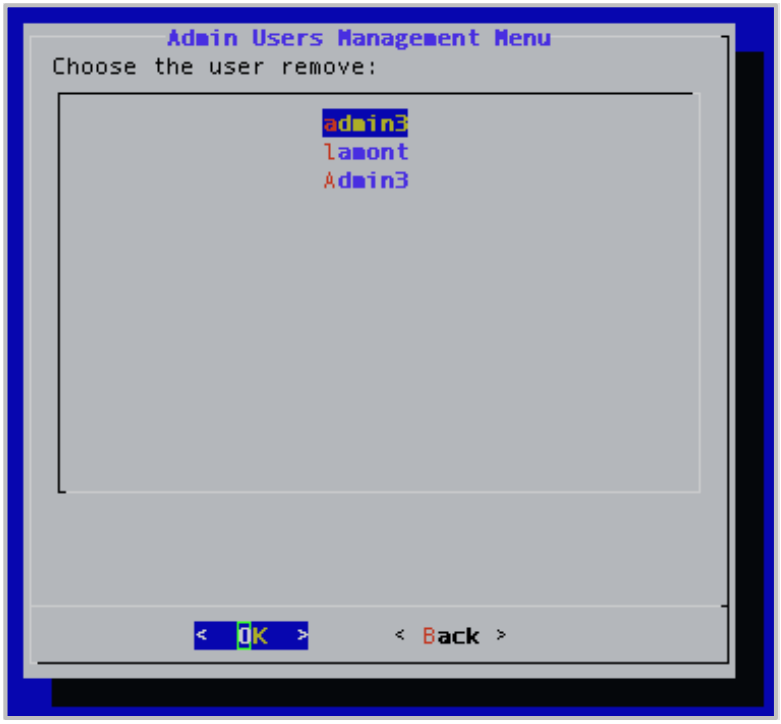


2. Enter **5** to select the Users option.
3. Press the **Enter** key to select **OK**. The *Password required to continue* window displays.

4. Enter your password.
5. Press the **Enter** key to select **OK**. The Admin Users Management Menu displays.



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



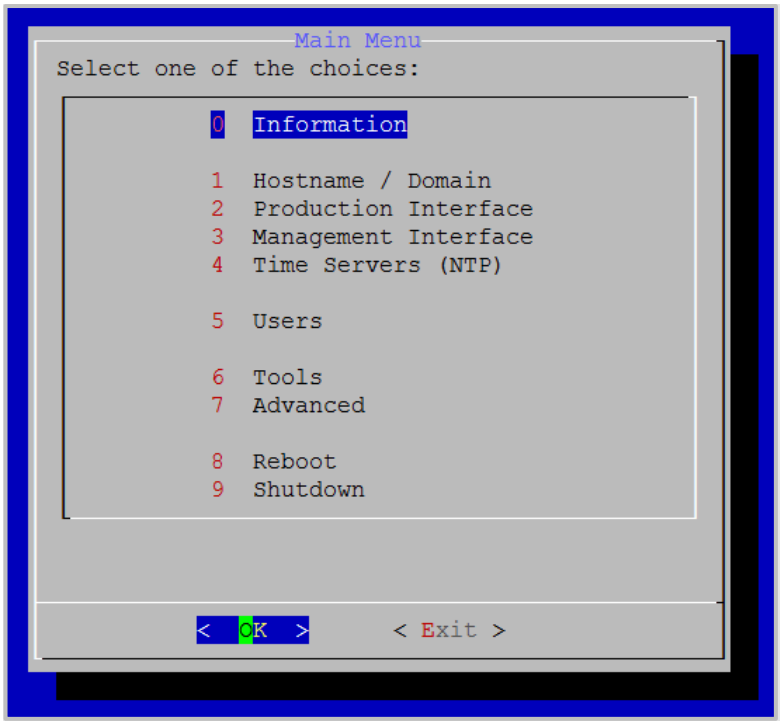
7. Select the user you want to remove.
8. Press the **Enter** key to select **OK**. The *Confirm* window displays.
9. Press the **Enter** key to select **Yes**. A message displays stating “[User] has been removed.”

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

Change user passwords

To change user passwords:

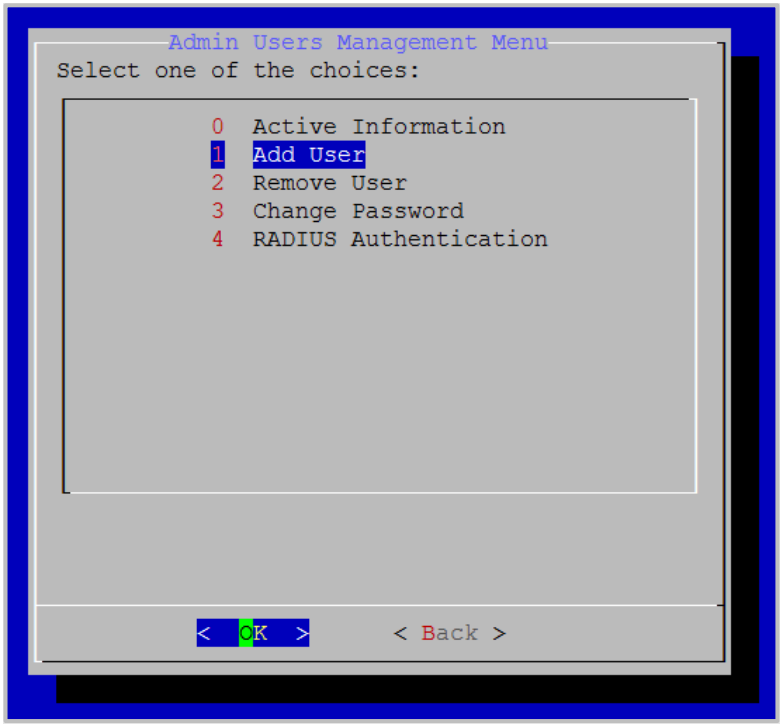
1. Log in to the System Console. The Main Menu displays.



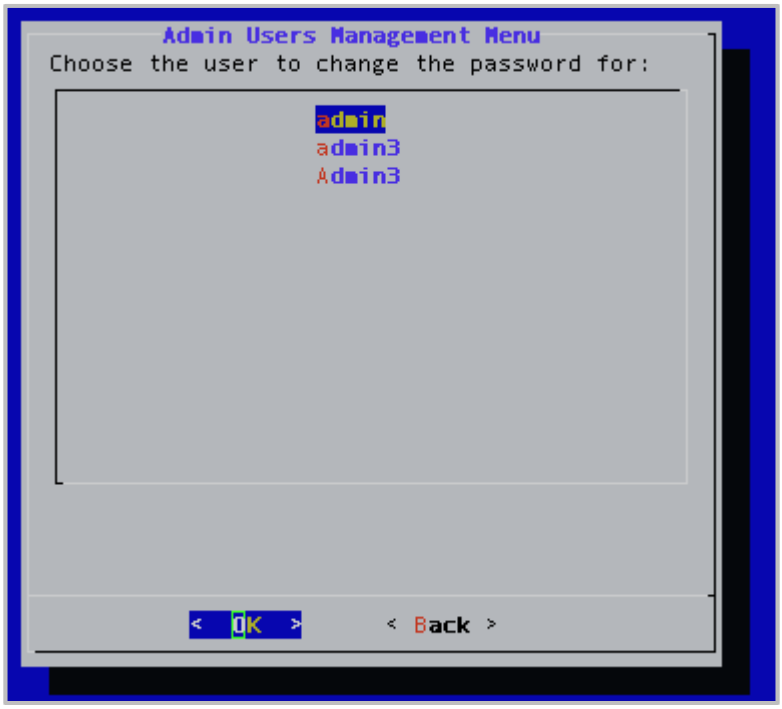
2. Enter **5** to select the Users option.
3. Press the **Enter** key to select **OK**. The *Password required to continue* window displays.

4. Enter your password.

5. Press the **Enter** key to select **OK**. The Admin Users Management Menu displays.

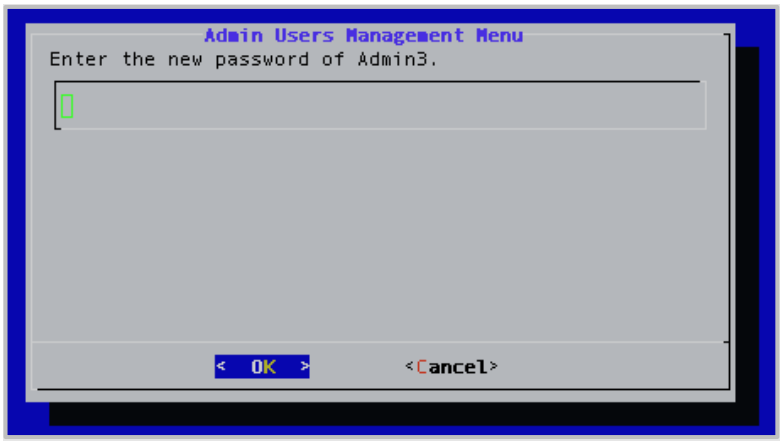


6. Enter **3** to select the Change Password option.
7. Press the **Enter** key to select **OK**.

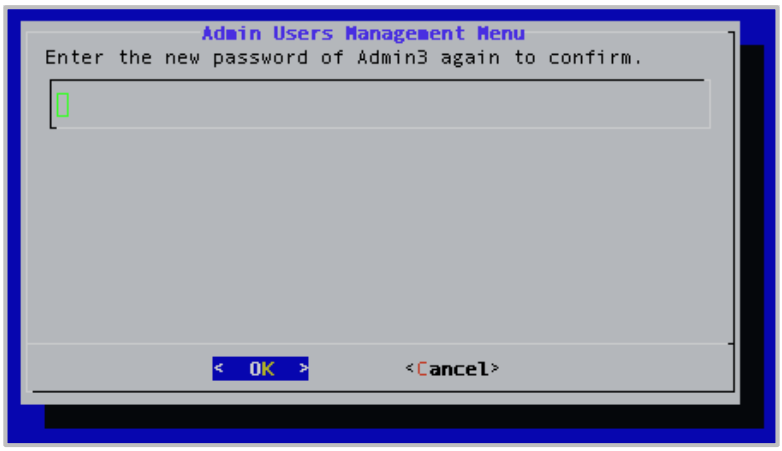


8. Select the user whose password you want to change.

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.



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



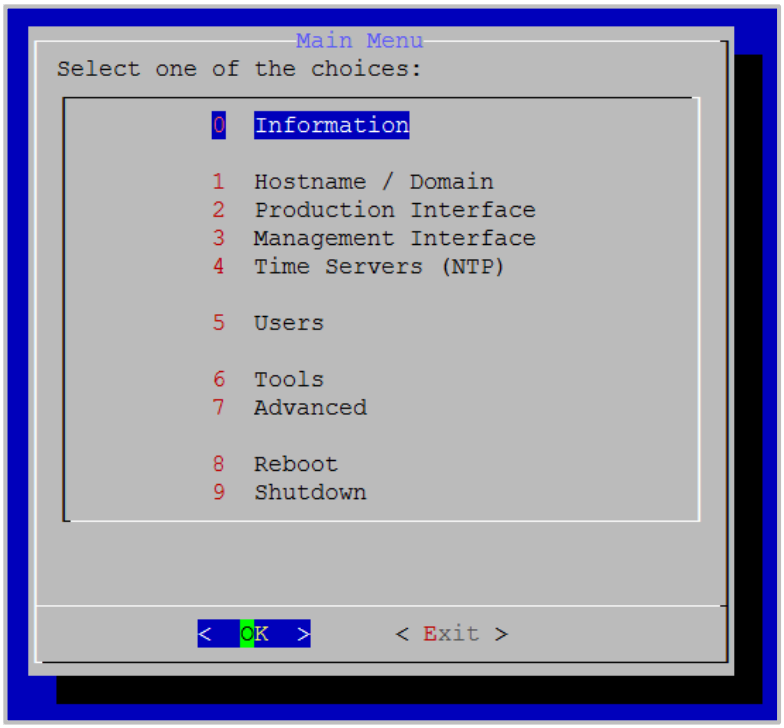
13. Enter the password again to confirm it.
14. Press the **Enter** key to select **OK**. A message displays stating “Password changed for [user].”
15. Press the **Enter** key to select **OK**.

Access tools

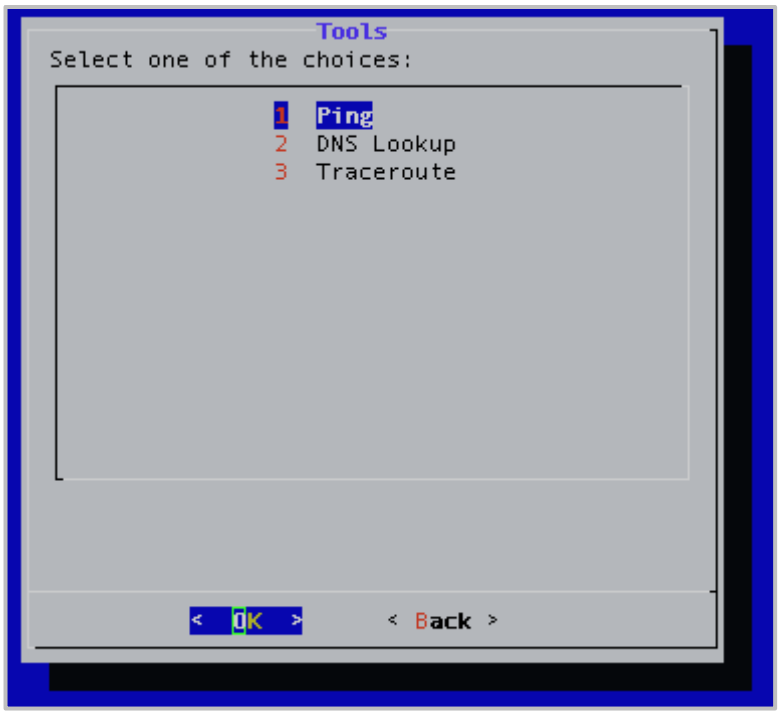
The Tools menu enables you to access the Ping, DNS Lookup, and Traceroute tools.

To access tools:

1. Log in to the System Console. The Main Menu displays.



2. Enter **6** to select the Tools option.
3. Press the **Enter** key to select **OK**. The Tools menu displays.



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**.

Perform advanced configuration

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

Configure FIPS

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

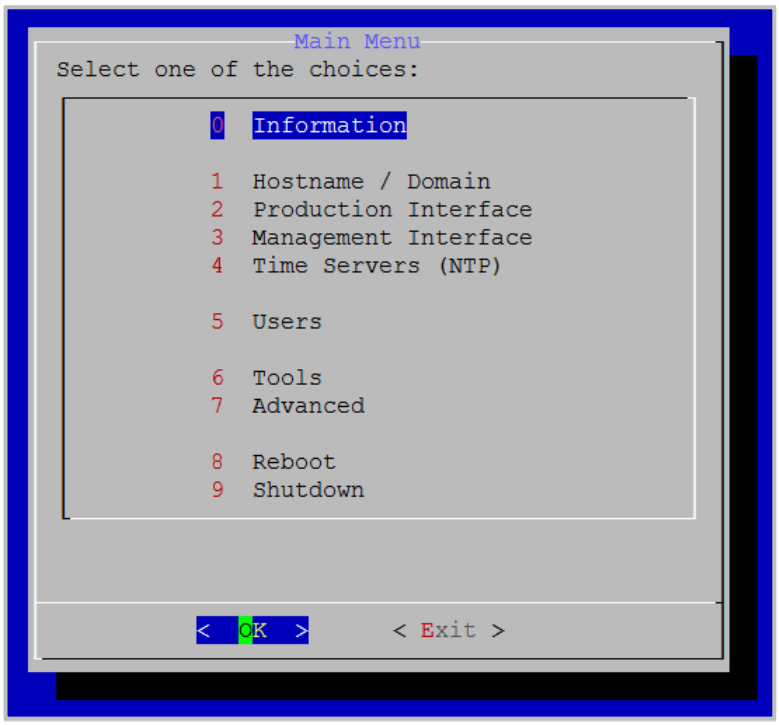
FIPS Certified Modules include the following:

- 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.

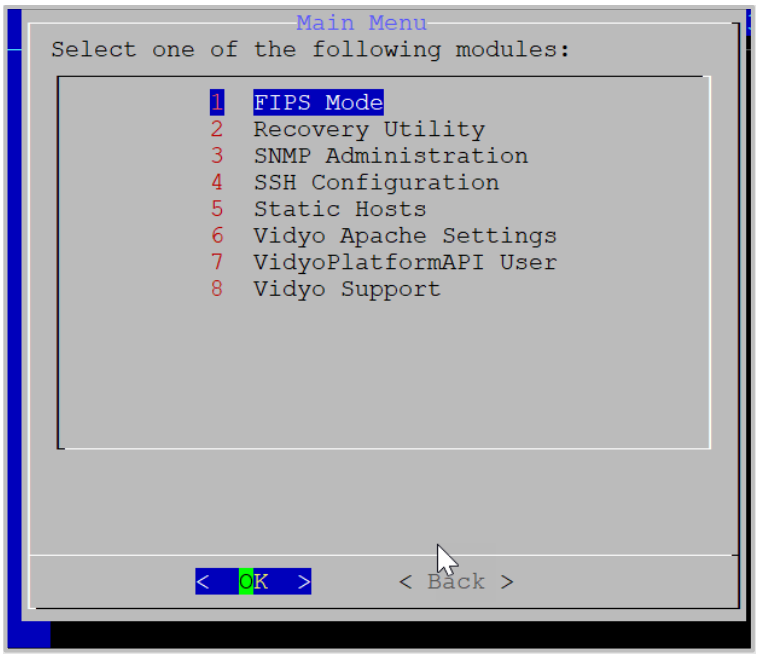
The following steps show you how to enable or disable FIPS mode from the System Console.

To configure FIPS:

1. Log in to the System Console. The Main Menu displays.

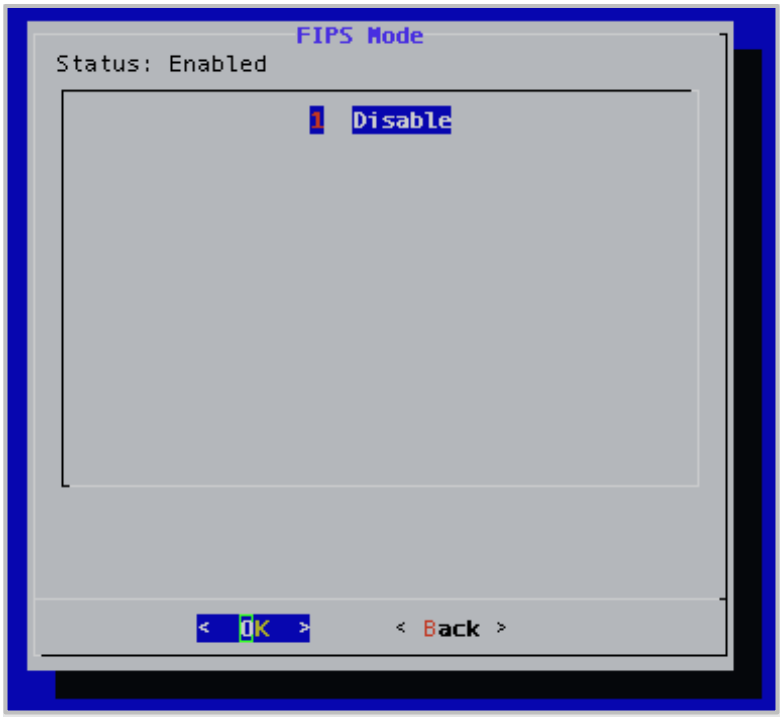


2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **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.



6. Enter **1** to select **Disable**.

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

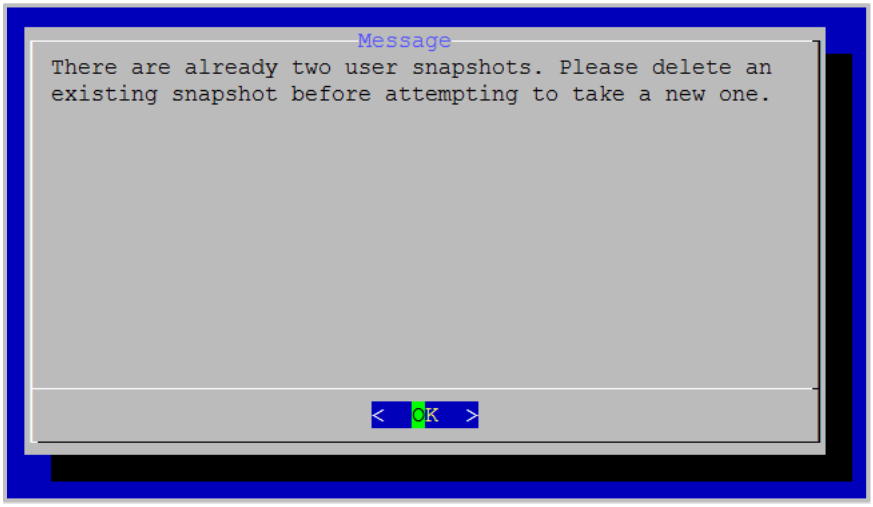
   When your system comes back online, FIPS is then disabled (or enabled) on your Vidyo server.

Run 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.

Take snapshots

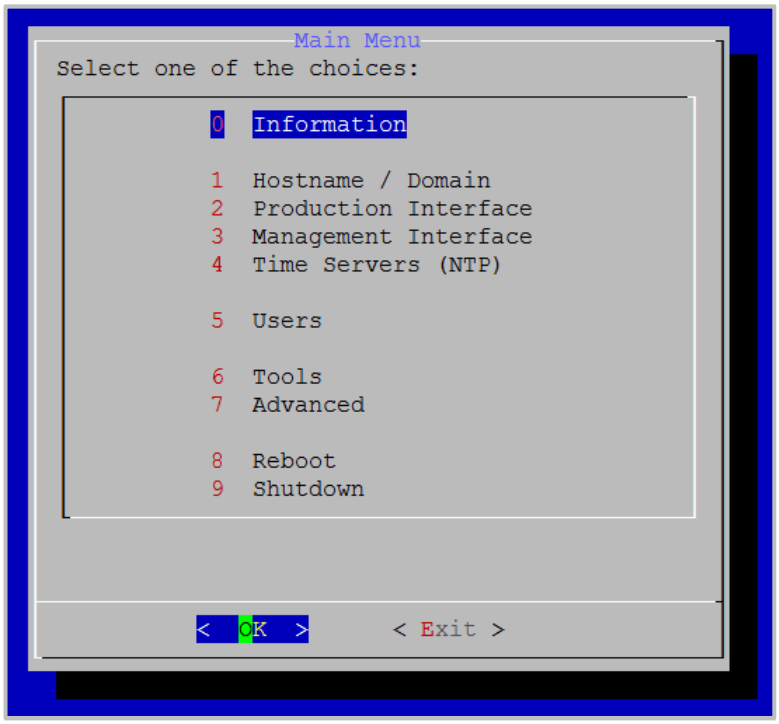
A maximum of two user snapshots are allowed. This limitation does not include snapshots that are automatically generated upon upgrading your VidyoReplay (e.g., VidyoUpdate). When two user snapshots already exist and the user attempts to take a new one, the following message will display:



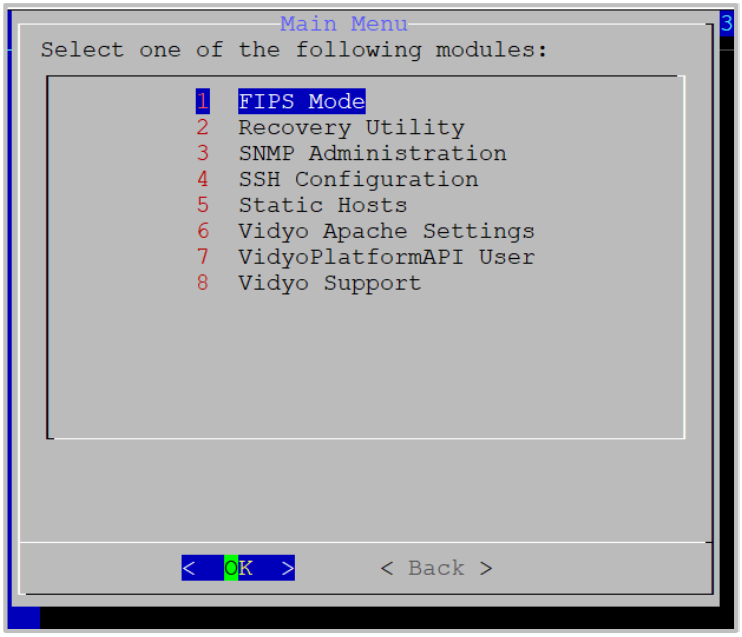
For more information about deleting snapshots, see Delete snapshots.

To take snaphots:

1. Log in to the System Console. The Main Menu displays.

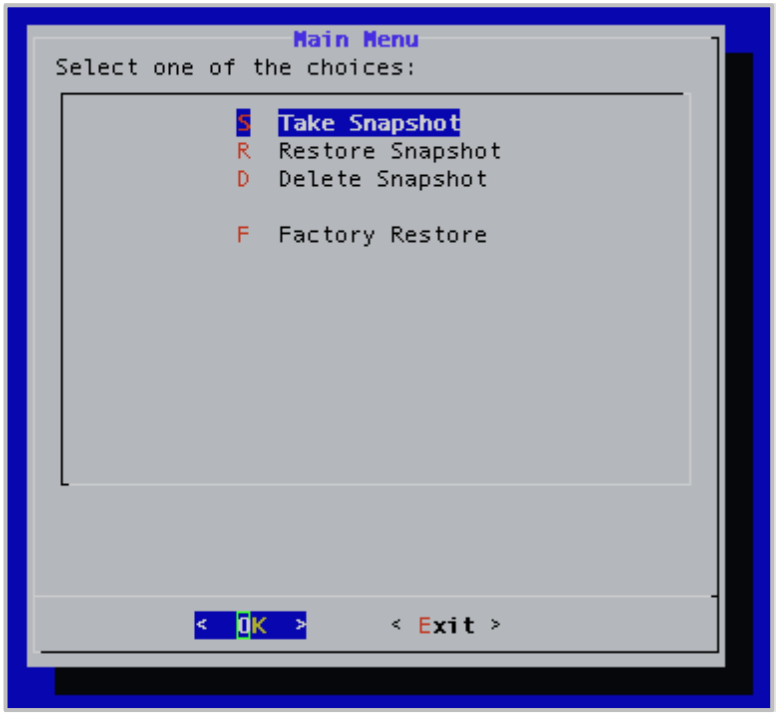


2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.

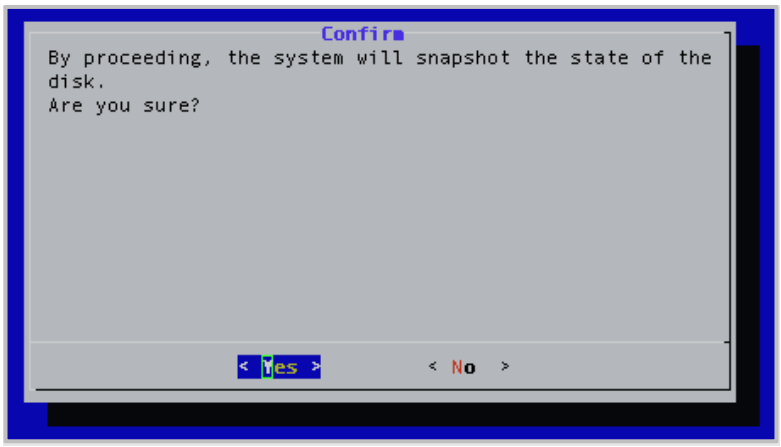


4. Enter **2** to select the Recovery Utility option.

5. Press the **Enter** key to select **OK**. The Recover Utility Main Menu displays.

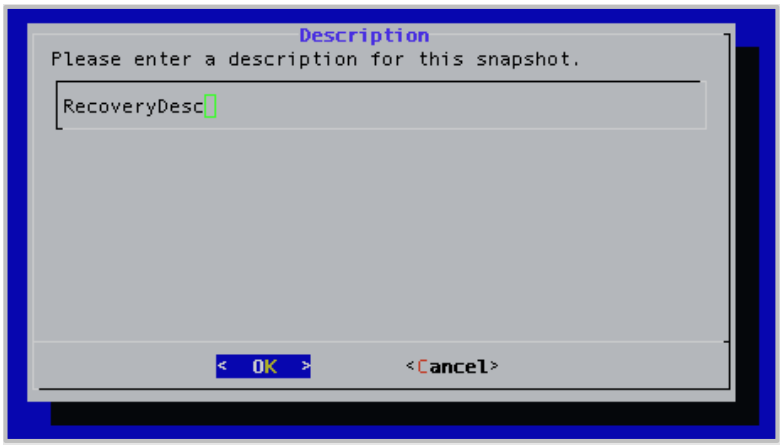


6. Enter **S** to select the Take Snapshot option.
7. Press the **Enter** key to select **OK**. The *Confirm* window displays.



8. Press the **Enter** key to select **Yes**. The *Name* window displays.

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.



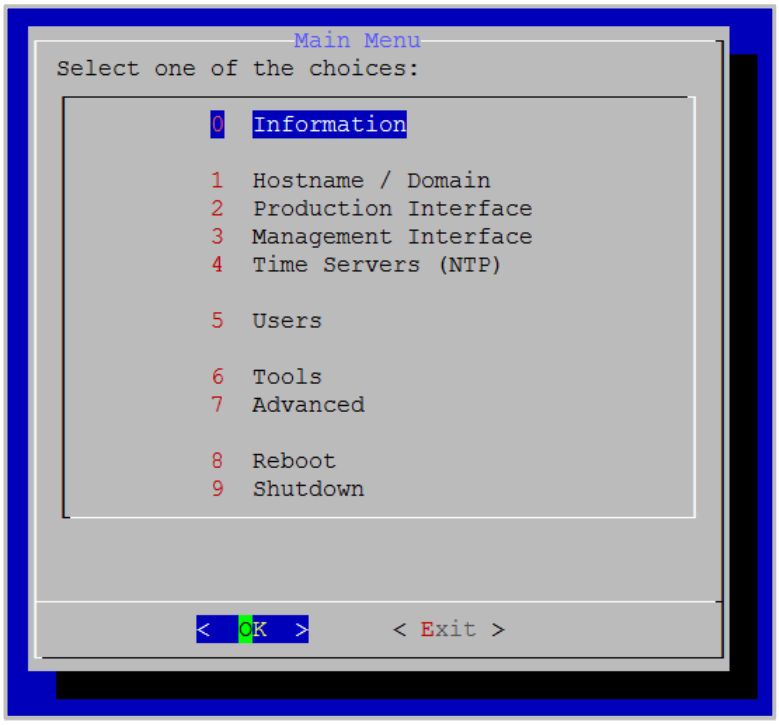
11. Enter a description for the snapshot.
12. Press the **Enter** key to select **OK**. A message displays stating “Snapshot successful.”

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

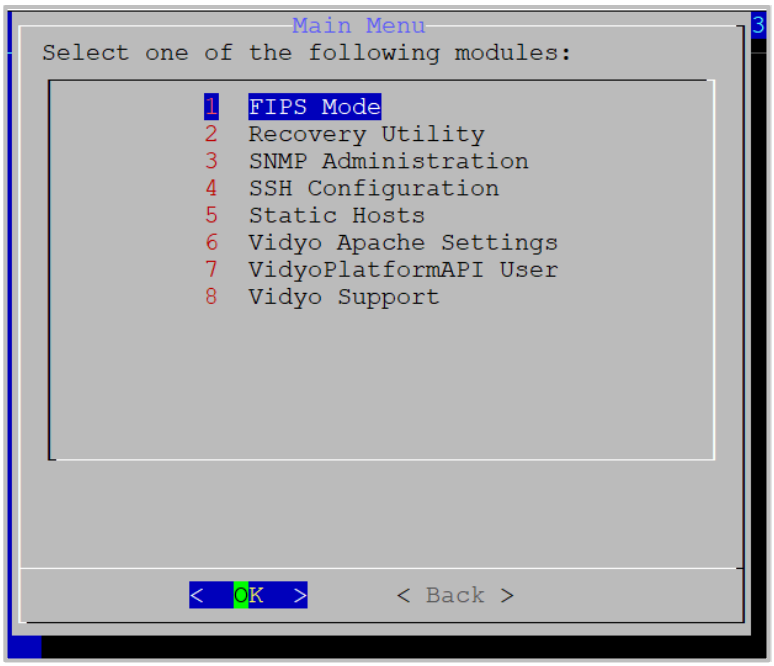
Restore snapshots

To restore snaphots:

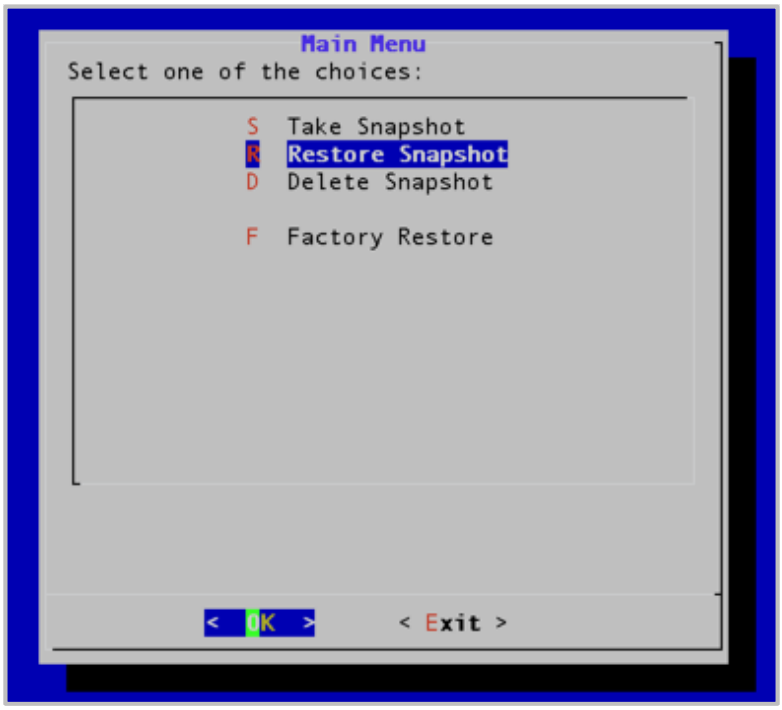
1. Log in to the System Console. The Main Menu displays.



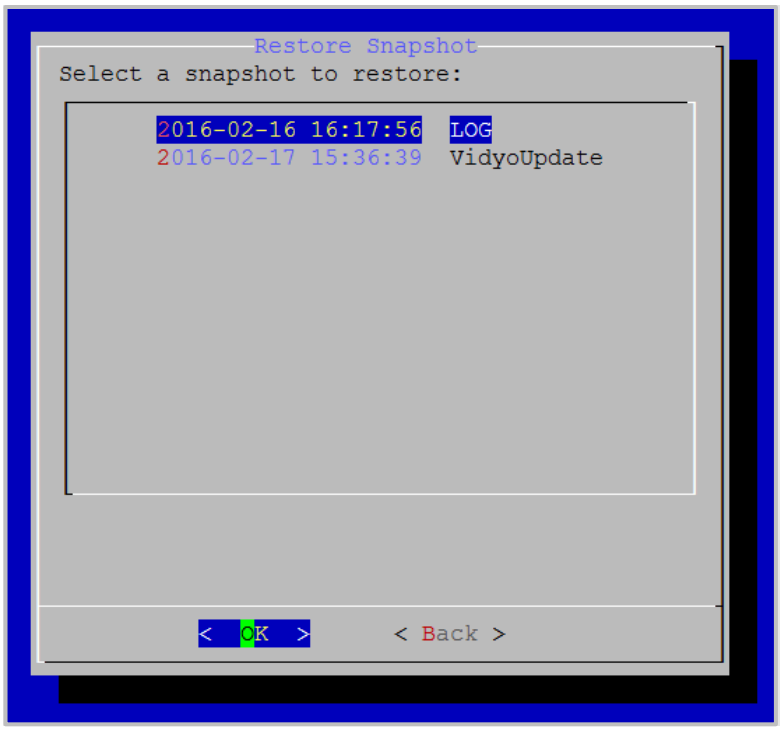
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



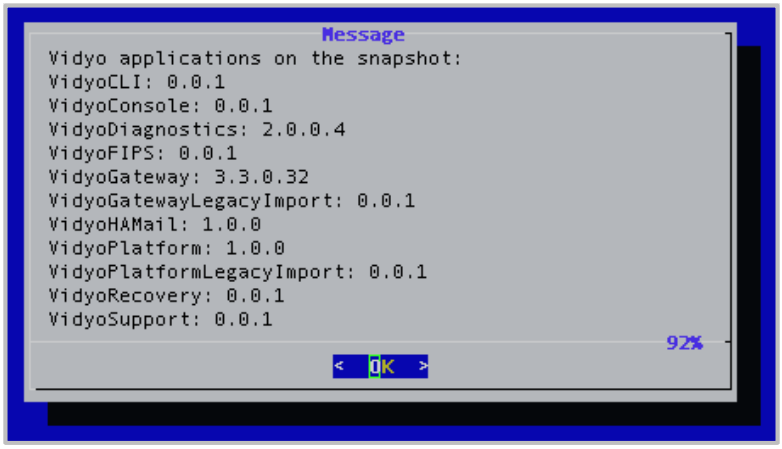
4. Enter **2** to select the Recovery Utility option.
5. Press the **Enter** key to select **OK**. The Recover Utility Main Menu displays.



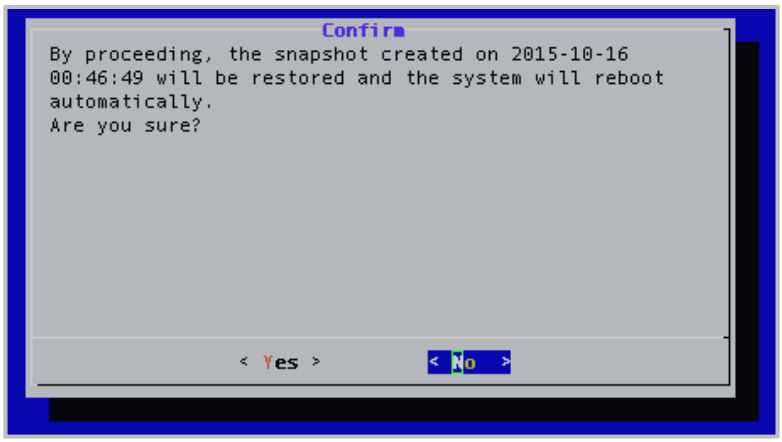
6. Enter **R** to select the Restore Snapshot option.
7. Press the **Enter** key to select **OK**. The *Restore Snapshot* window displays.



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.



11. Press the **Enter** key to select **OK**. The *Confirm* window displays.

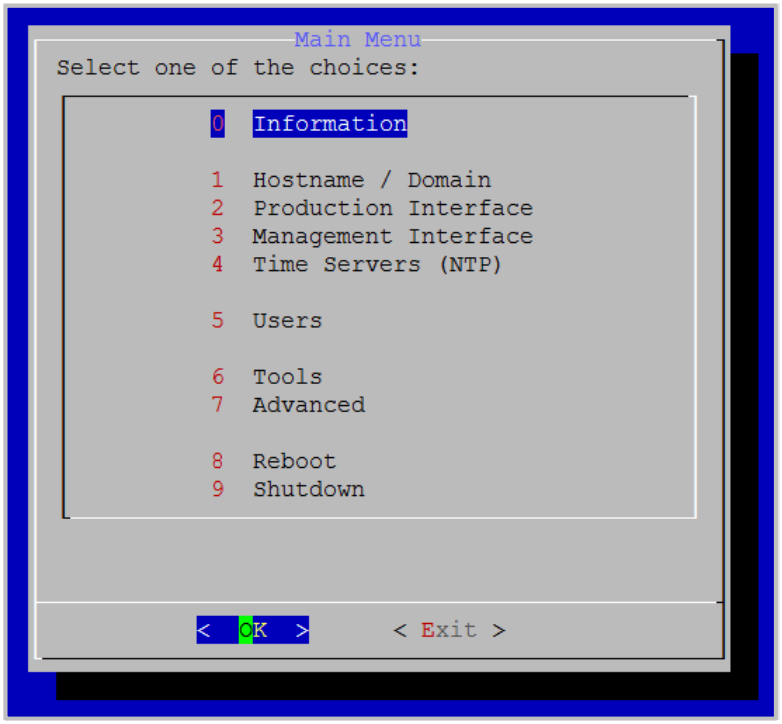


12. Press the **Enter** key to select **Yes**.

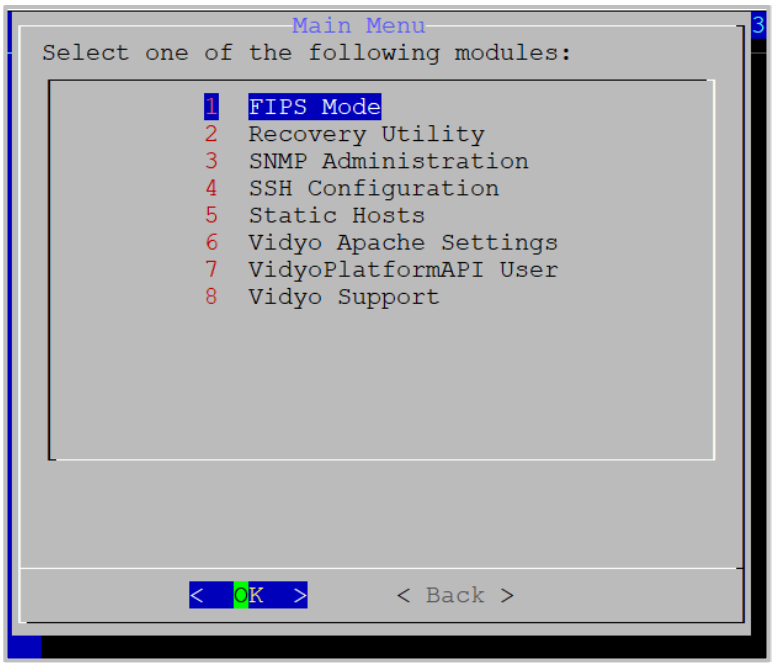
Delete snapshots

To delete snaphots:

1. Log in to the System Console. The Main Menu displays.

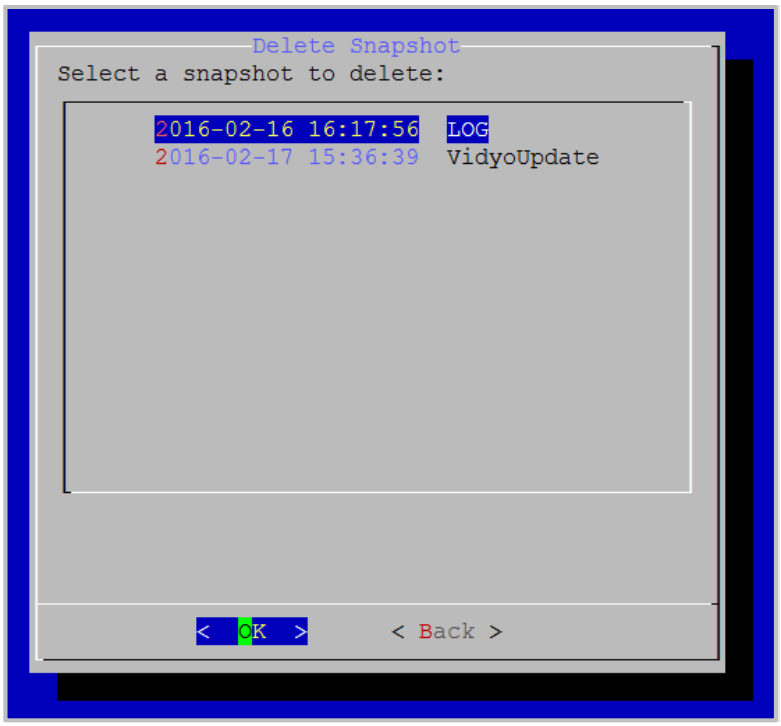


2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.

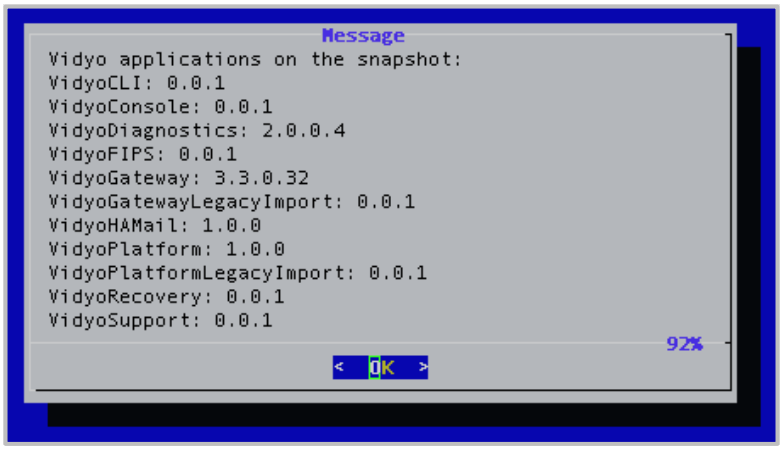


4. Enter **2** to select the Recovery Utility option.
5. Press the **Enter** key to select **OK**. The Recover Utility Main Menu displays.

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



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.



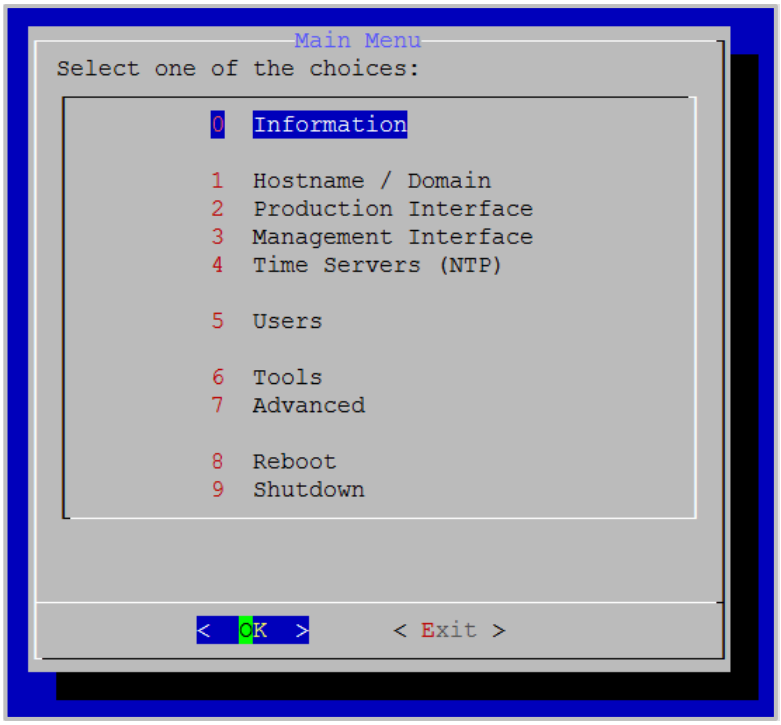
11. Press the **Enter** key to select **OK**. The *Confirm* window displays.

12. Press the **Enter** key to select **Yes**. A message displays stating “Snapshot successfully deleted.”
13. Press the **Enter** key to select **OK**.

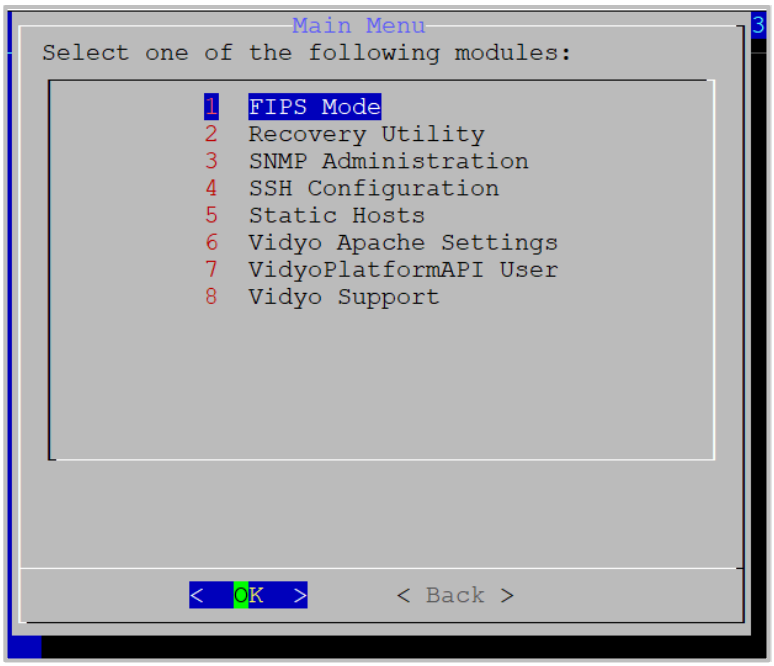
Perform a factory restore

To perform a factory restore:

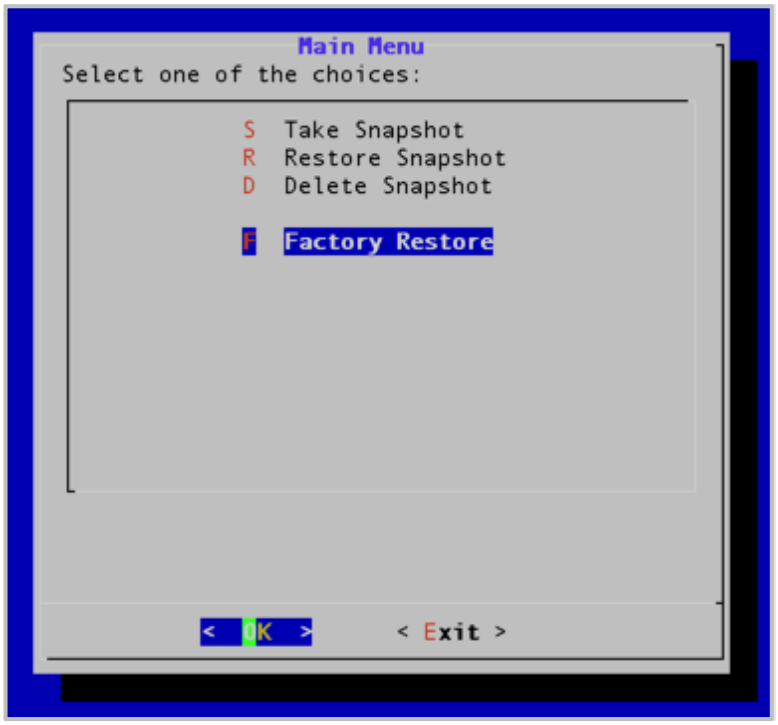
1. Log in to the System Console. The Main Menu displays.



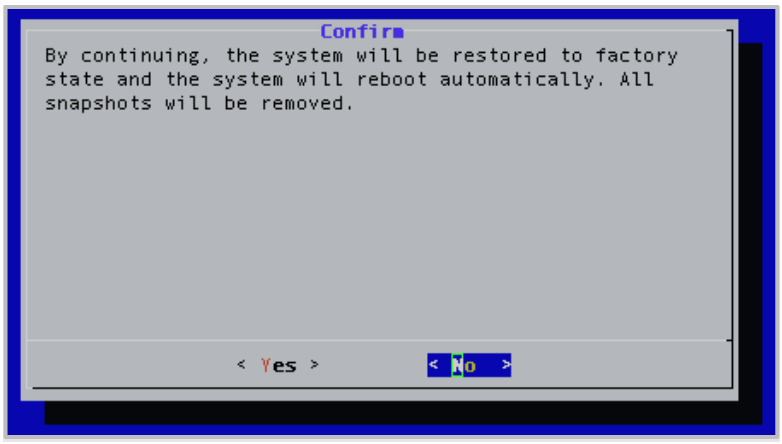
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **2** to select the Recovery Utility option. The Recover Utility Main Menu displays.



5. Enter **F** to select the Factory Restore option.
6. Press the **Enter** key to select **OK**. The *Confirm* window displays.



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

Configure SNMP

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

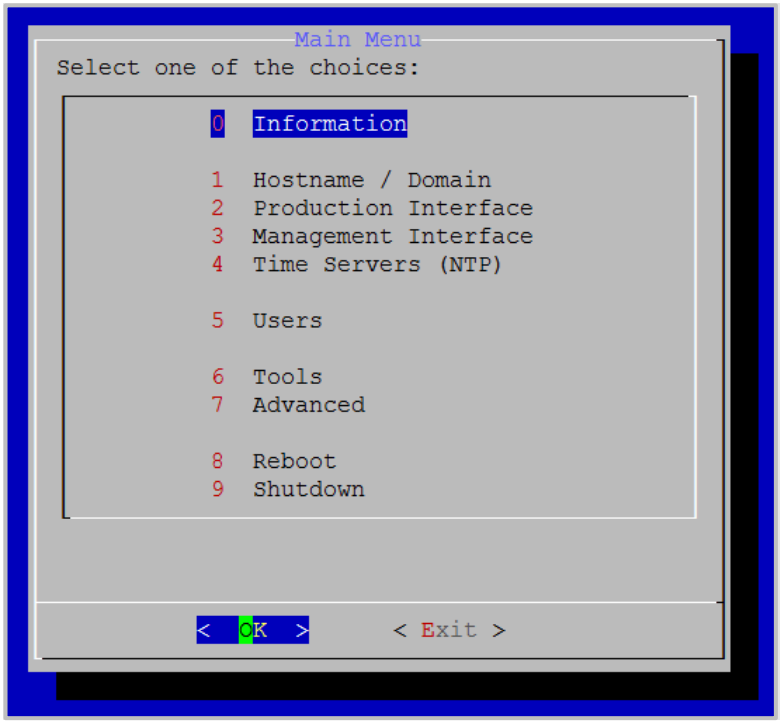
> Note
>
> Some un-configurable object identifiers (OIDs) are standard on all Vidyo Servers. With SNMP traps enabled, they provide notifications if the CPU, disk or memory utilization has reached its threshold (~80% utilization). The specific OIDs are cpuLoadReachedThreshold, diskReachedThreshold, and memoryReachedThreshold.
>
> For more information about Vidyo enterprise notifications, as well as Get, and Set Polling OIDs, download the *Vidyo MIB* file from the *Vidyo Support Centre*.

Enable, disable, and restart SNMP

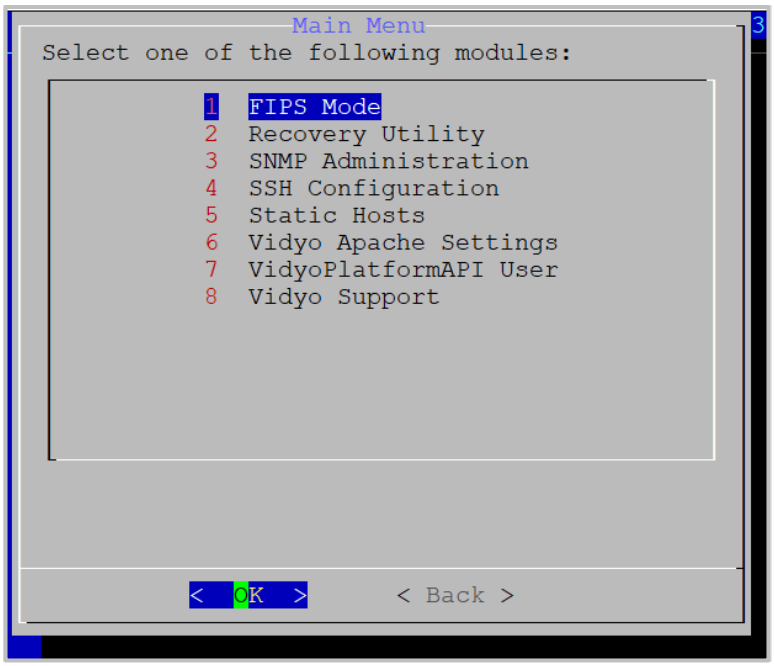
Enable SNMP only after configuring SNMP2 community strings or SNMPv3 users and creating notifications or traps.

To enable, disable, or restart SNMP:

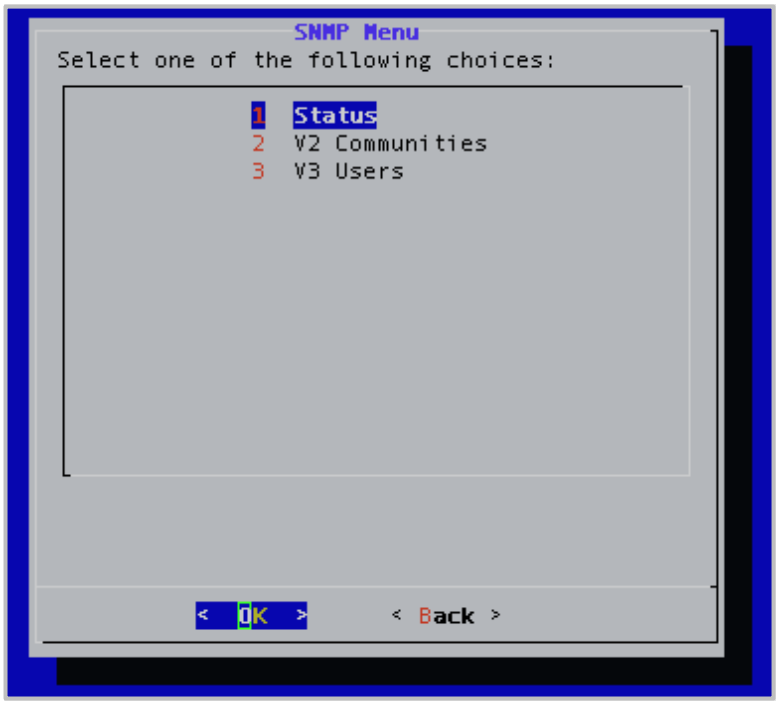
1. Log in to the System Console. The Main Menu displays.



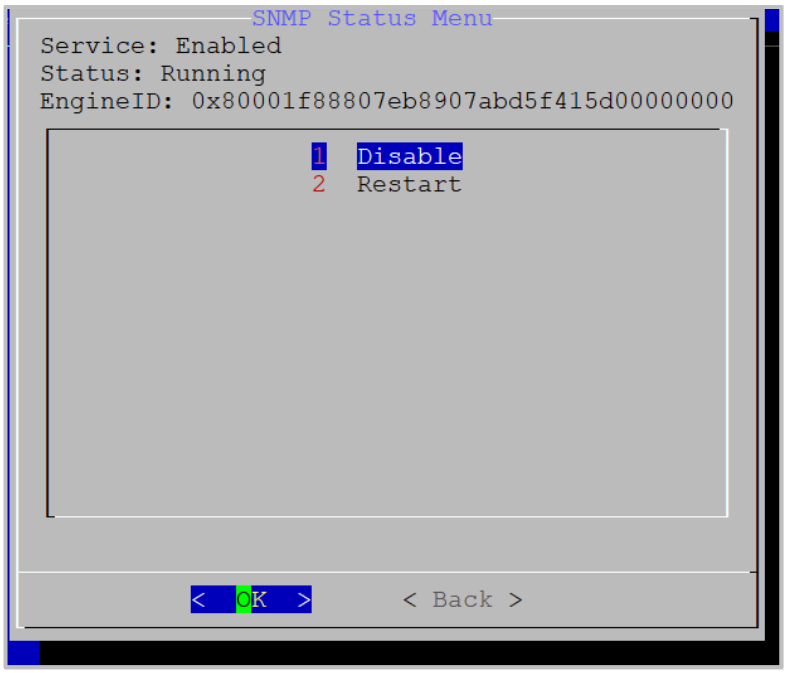
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.



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.



8. Enter **1** to select 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).

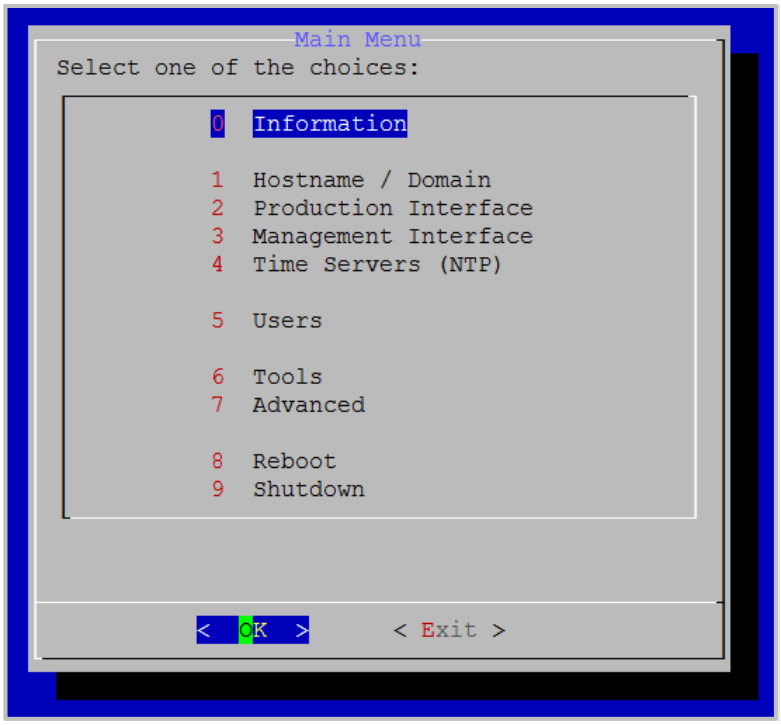
Configure SNMP v2 communities

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.

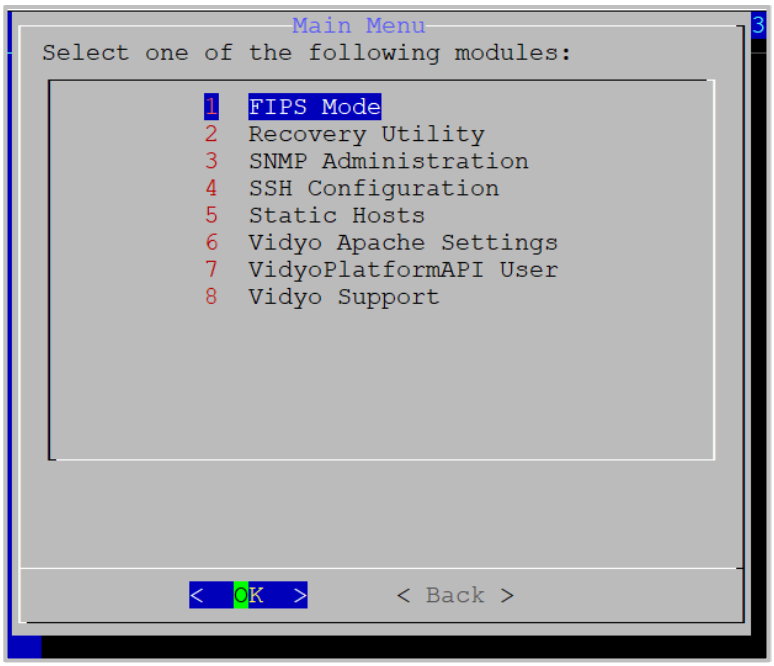
List the SNMP v2 communities

To list the SNMP v2 communities:

1. Log in to the System Console. The Main Menu displays.

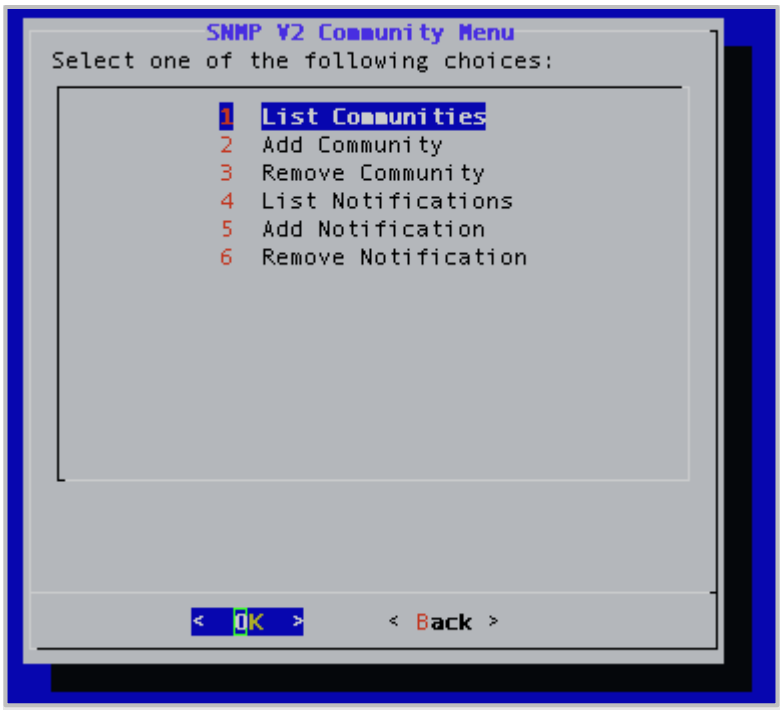


2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**.
6. The SNMP Menu displays.

7. Enter **2** to select the V2 Communities option.
8. Press the **Enter** key to select **OK**. The SNMP V2 Community Menu displays.



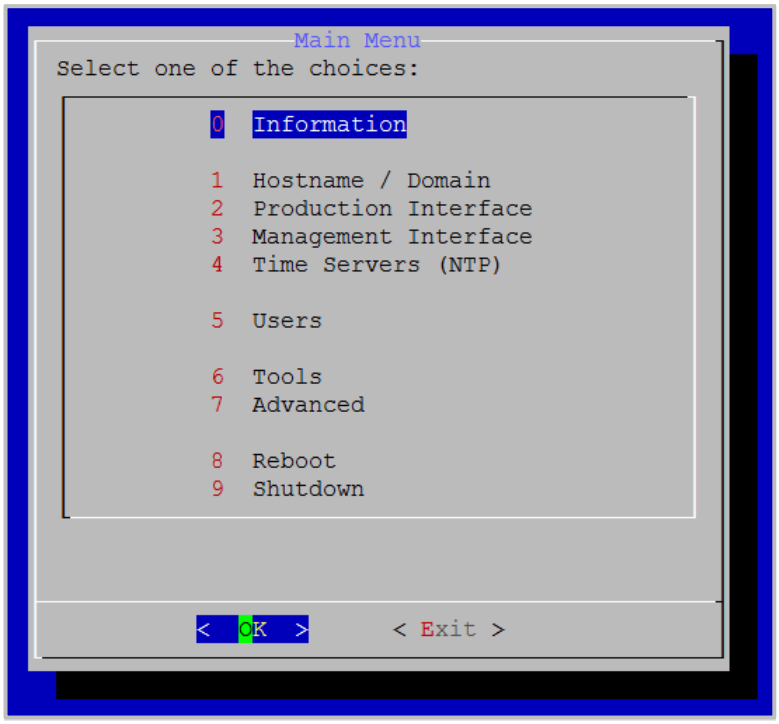
9. Enter **1** to select the List Communities option.
10. Press the **Enter** key to select **OK**. The *V2 Communities* window, which lists the current v2 communities, displays.

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

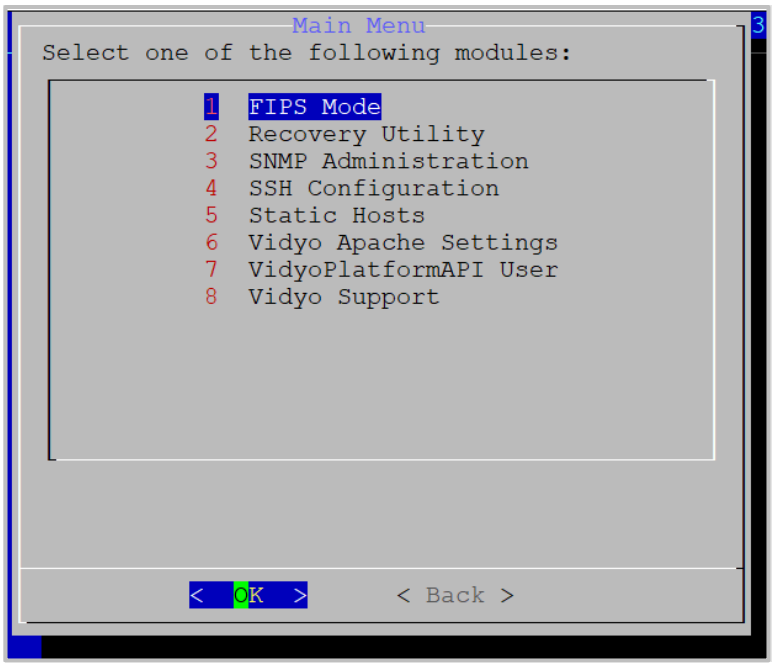
Add SNMP v2 communities

To add SNMP v2 communities:

1. Log in to the System Console. The Main Menu displays.



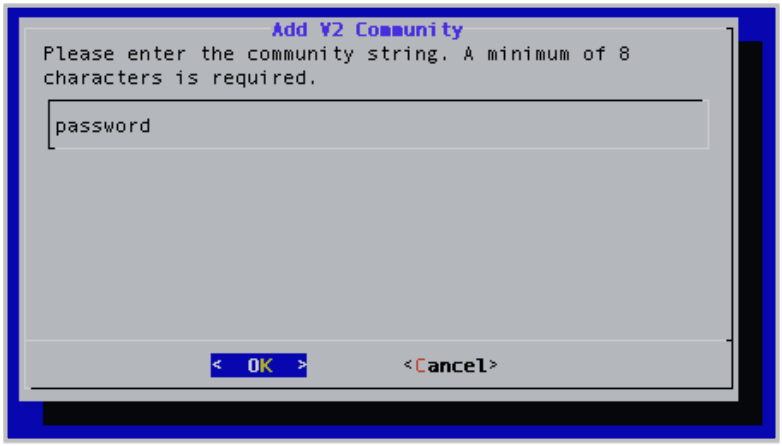
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

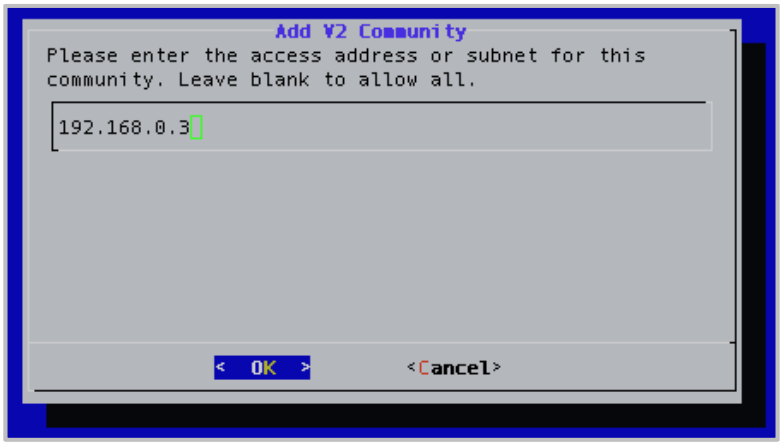
6. Enter **2** to select the V2 Communities option.
7. Press the **Enter** key to select **OK**. The SNMP V2 Community Menu displays.

8. Enter **2** to select the Add Community option.
9. Press the **Enter** key to select **OK**. The *Add V2 Community* window displays.



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.

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.

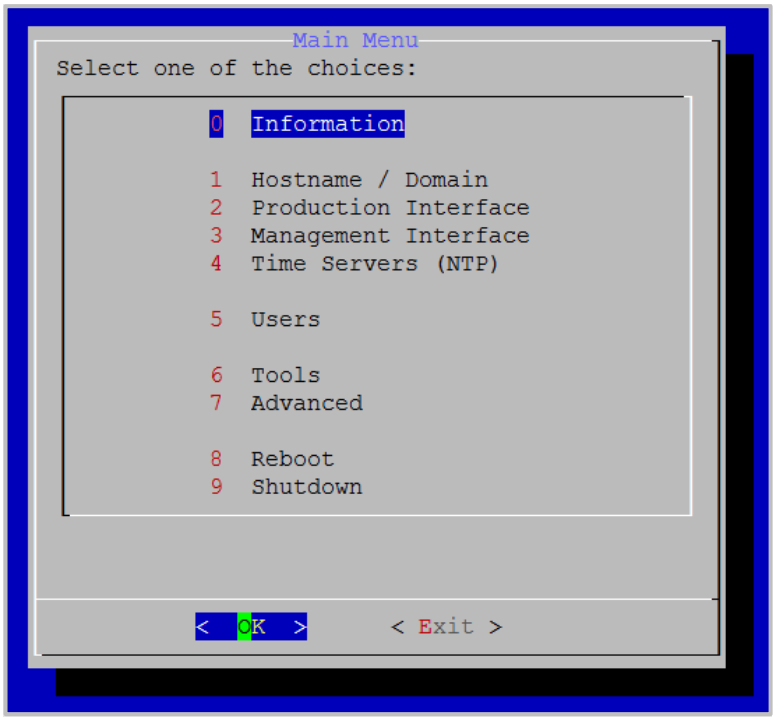


14. Enter the IP address or subnet to access this community, or leave the text box blank if you want to allow access to all.
15. Press the **Enter** key to select **OK**.

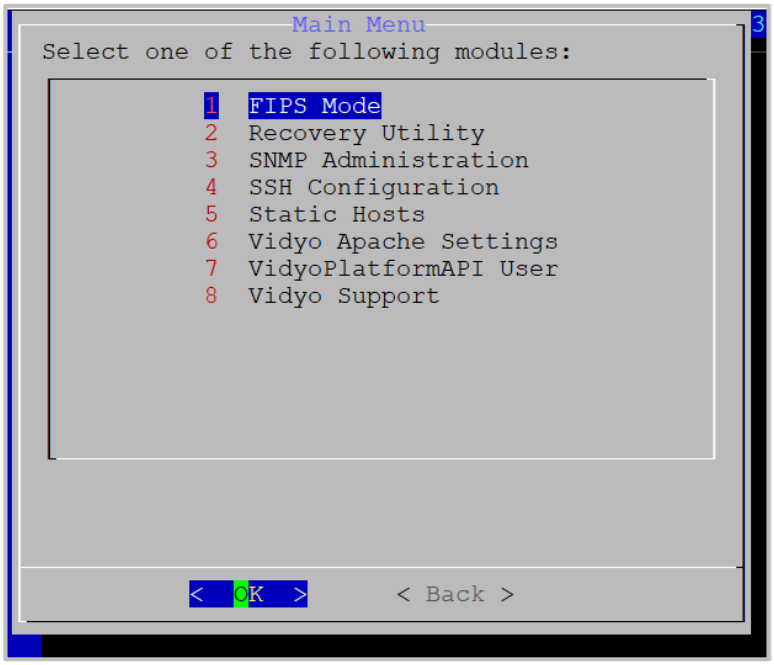
Remove an SNMP community string

To remove an SNMP v2 community:

1. Log in to the System Console. The Main Menu displays.

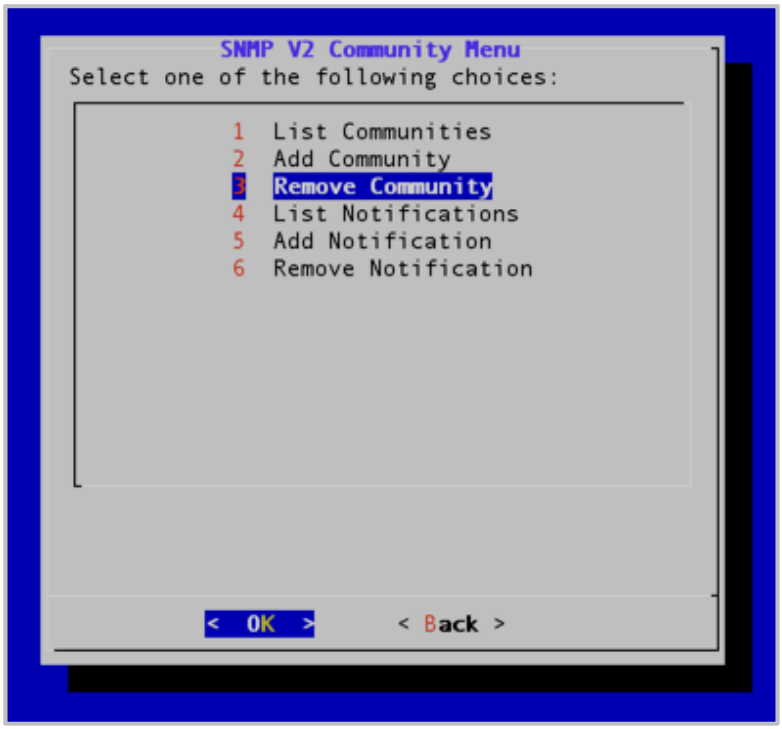


2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.

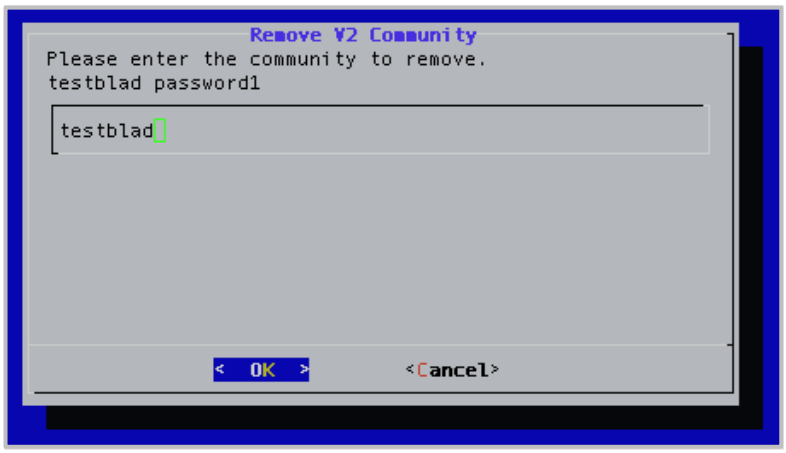


4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

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 **3** to select the Remove Community option.
9. Press the **Enter** key to select **OK**. The *Remove V2 Community* window displays.

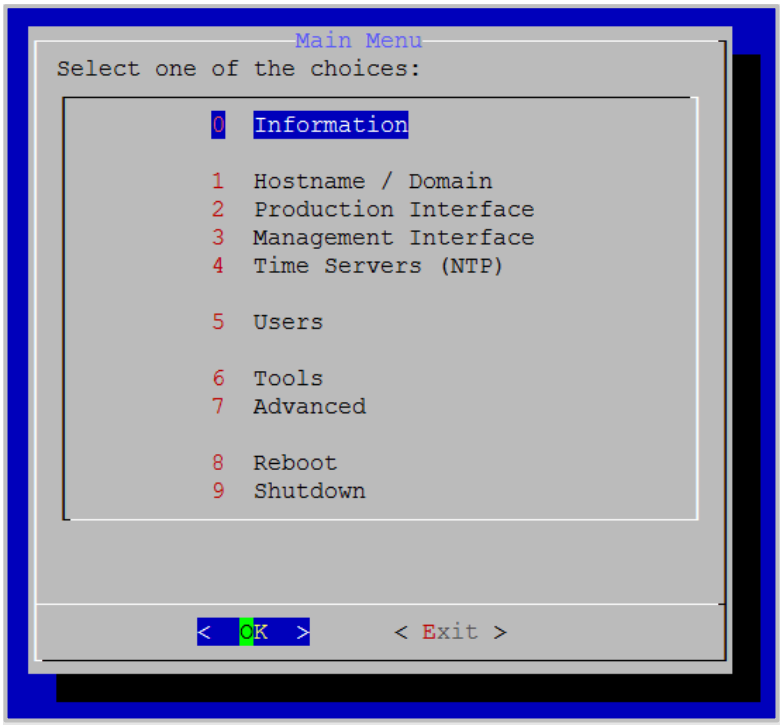


10. Enter the community string of the community you want to remove.
11. Press the **Enter** key to select **OK**.
12. A message displays stating “Successfully removed community.”
13. Press the **Enter** key to select **OK**.

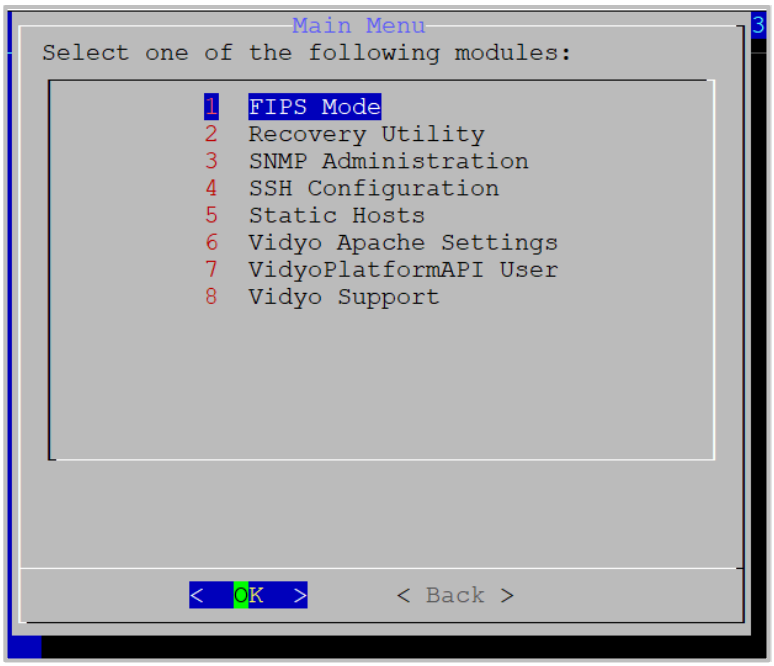
List SNMP v2 notifications

To list an SNMP v2 notification:

1. Log in to the System Console. The Main Menu displays.



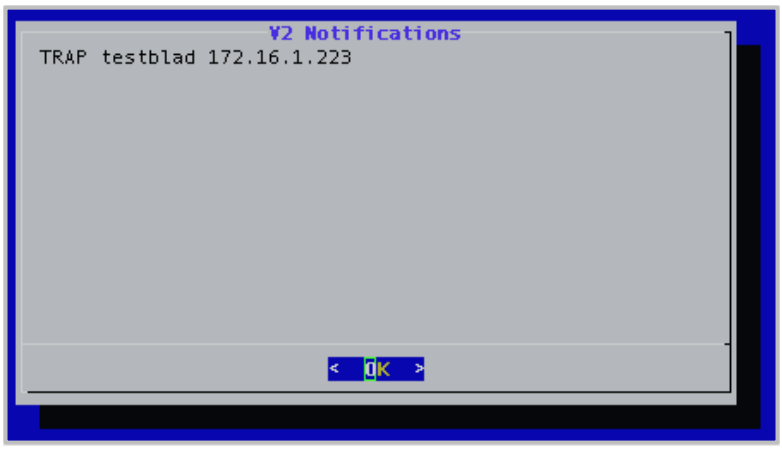
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

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 **4** to select the List Notifications option.
9. Press the **Enter** key to select **OK**. The *V2 Notifications* window displays.

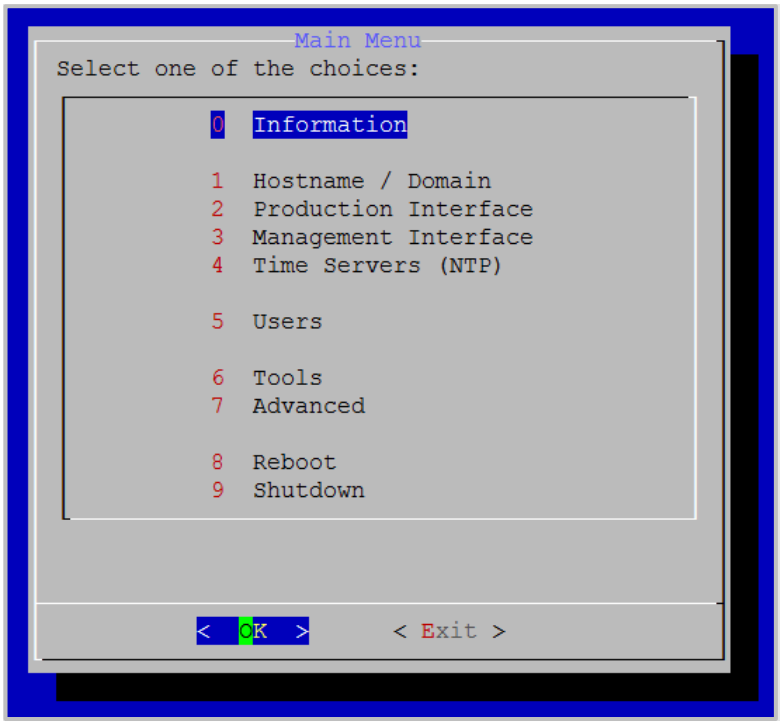


10. Press the **Enter** key to select **OK**.

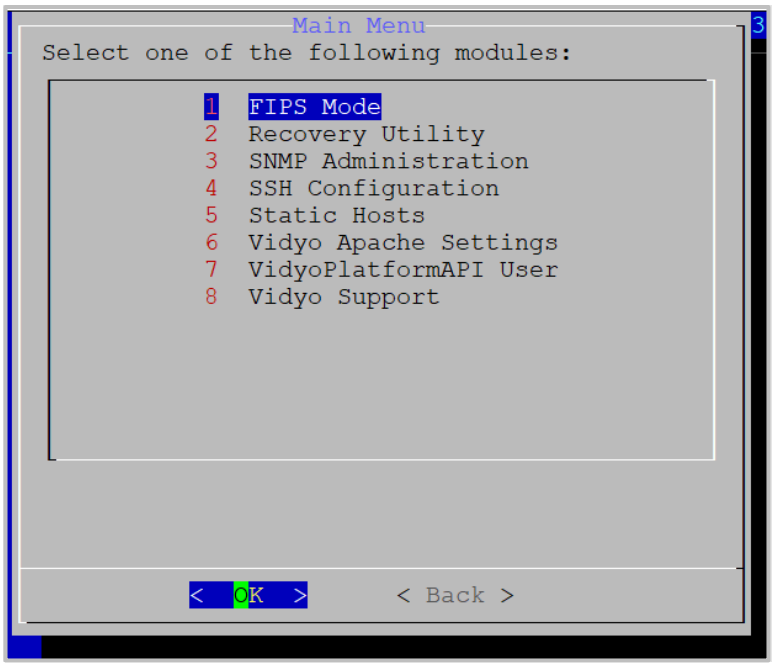
Add SNMP v2 notifications

To add an SNMP v2 notification:

1. Log in to the System Console. The Main Menu displays.



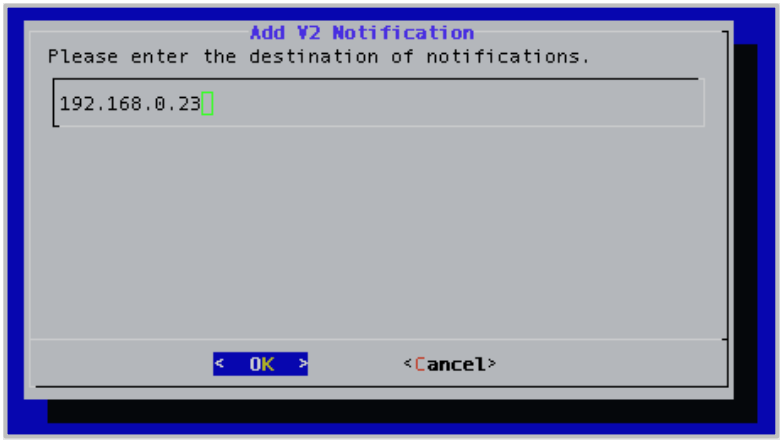
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



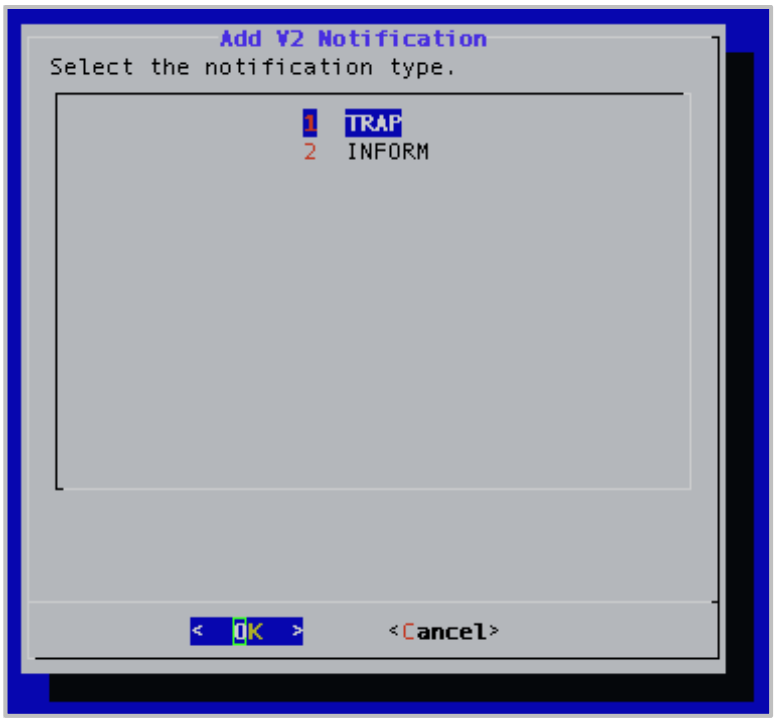
4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

6. Enter **2** to select the V2 Communities option.
7. Press the **Enter** key to select **OK**. The SNMP V2 Community Menu displays.

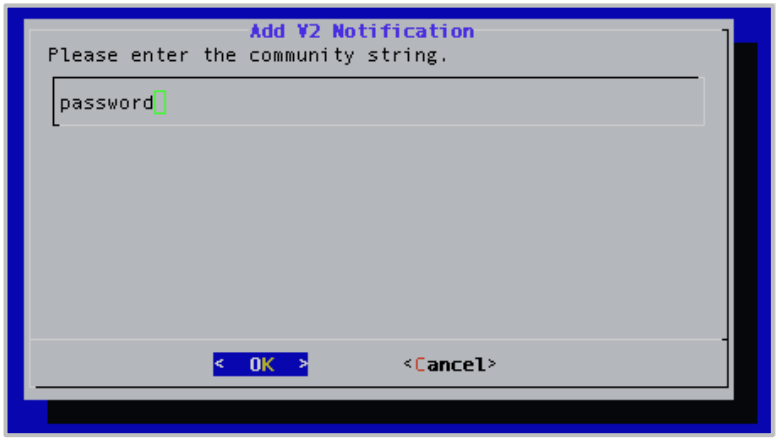
8. Enter **5** to select the Add Notifications option.
9. Press the **Enter** key to select **OK**. The *Add V2 Notification* window displays.



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.



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**.

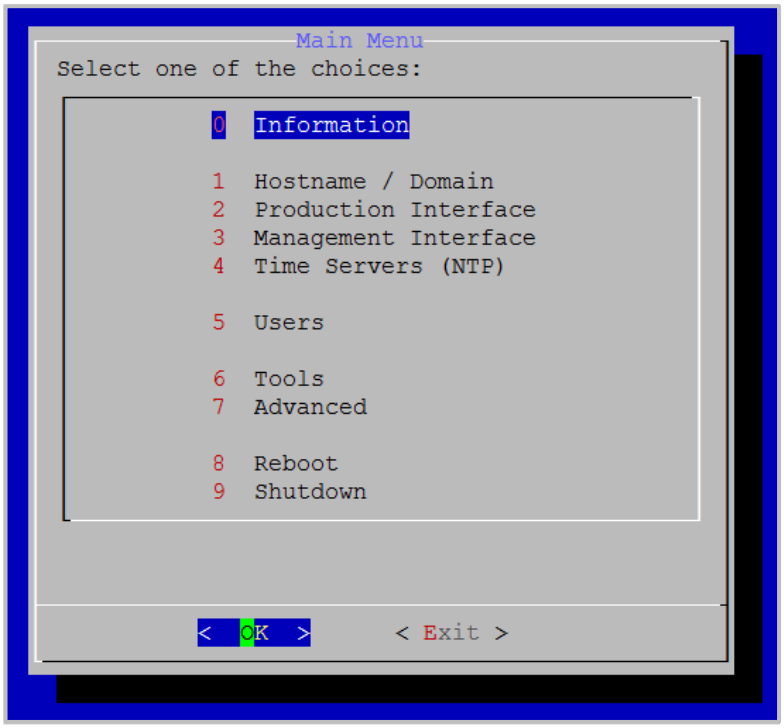


14. Enter the password for the community string.
15. Press the **Enter** key to select **OK**. A message displays stating “Successfully added notification.”
16. Press the **Enter** key to select **OK**.

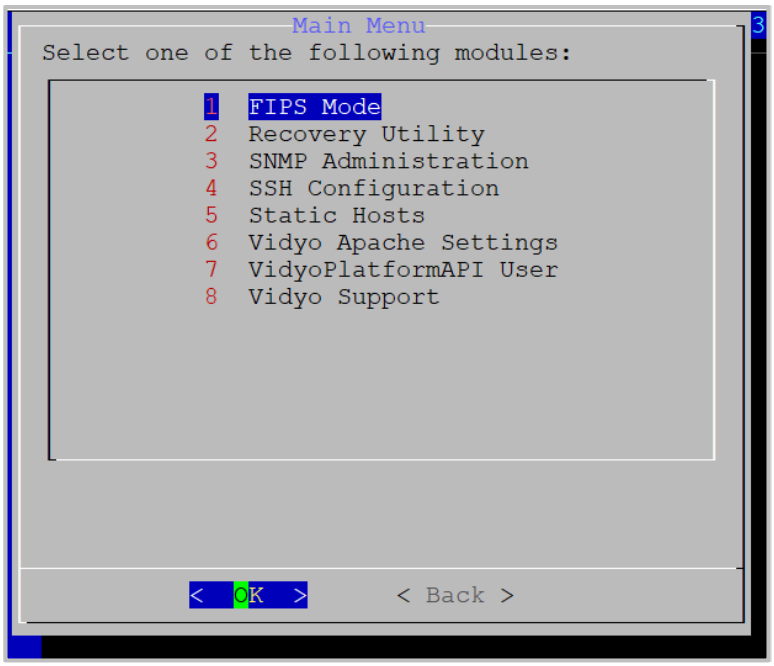
Remove SNMP v2 notifications

To remove an SNMP v2 notification:

1. Log in to the System Console. The Main Menu displays.



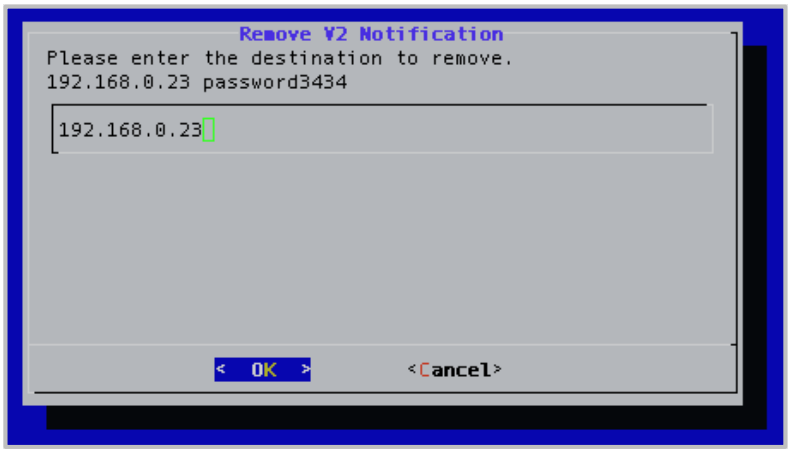
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

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.



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**.

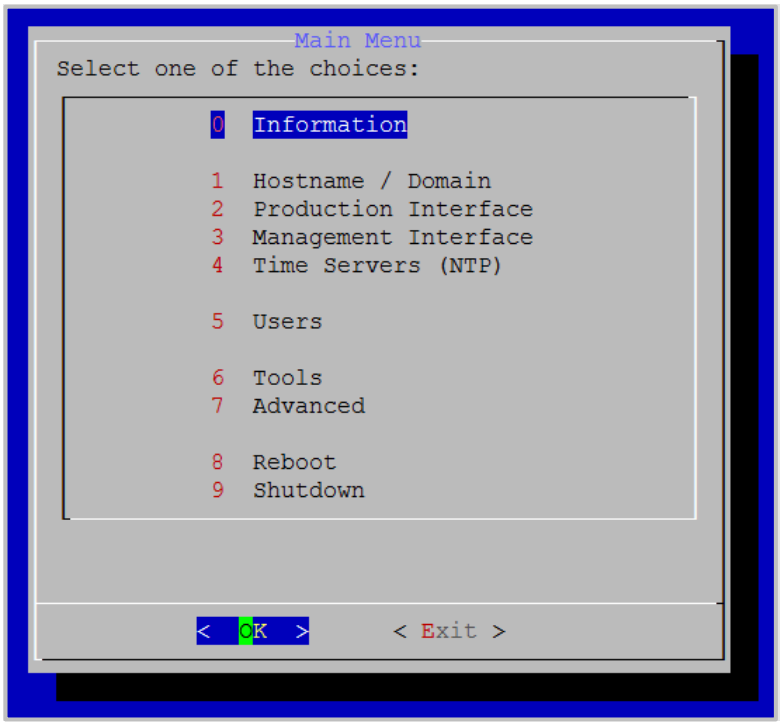
Configure SNMP v3 users

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

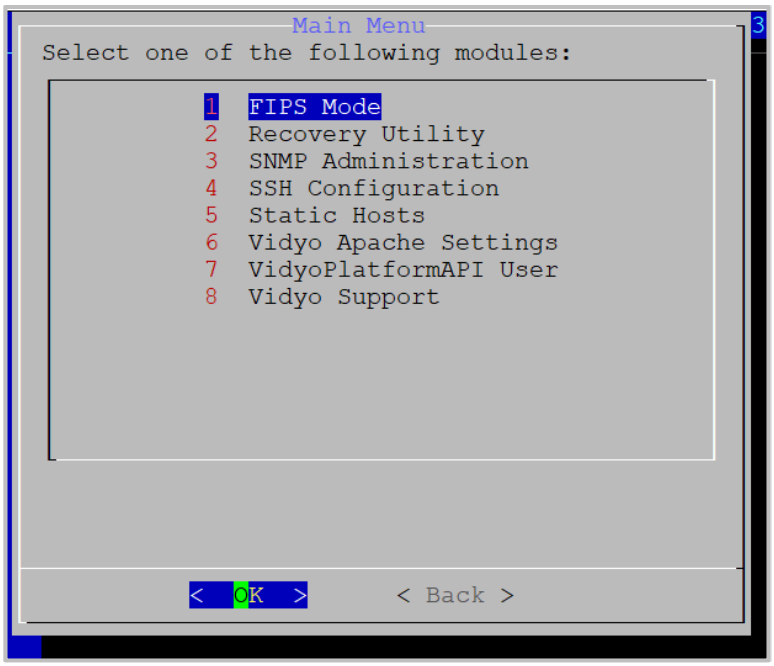
List SNMP v3 users

To list SNMP v3 Users:

1. Log in to the System Console. The Main Menu displays.

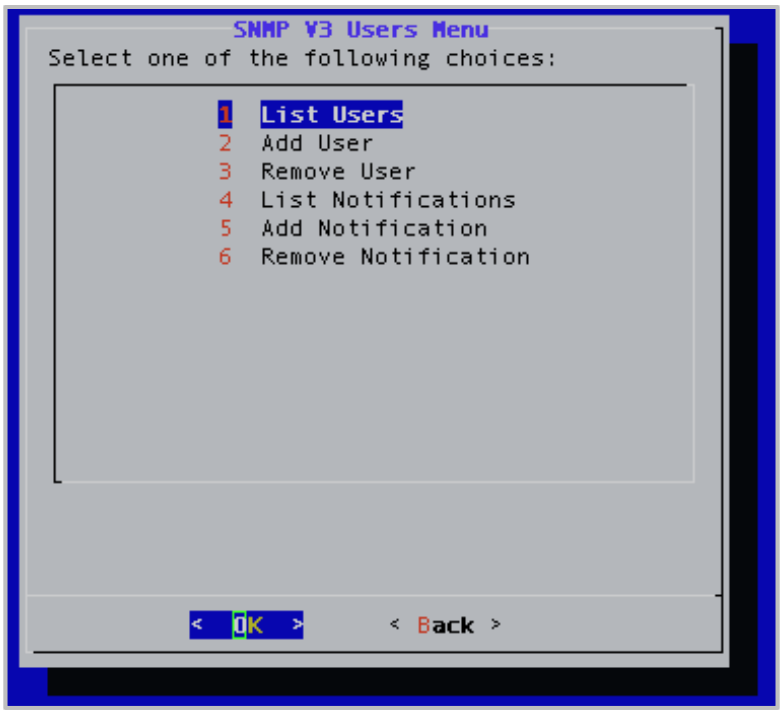


2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

6. Enter **3** to select the V3 Users option.
7. Press the **Enter** key to select **OK**. The SNMP V3 Community Menu displays.



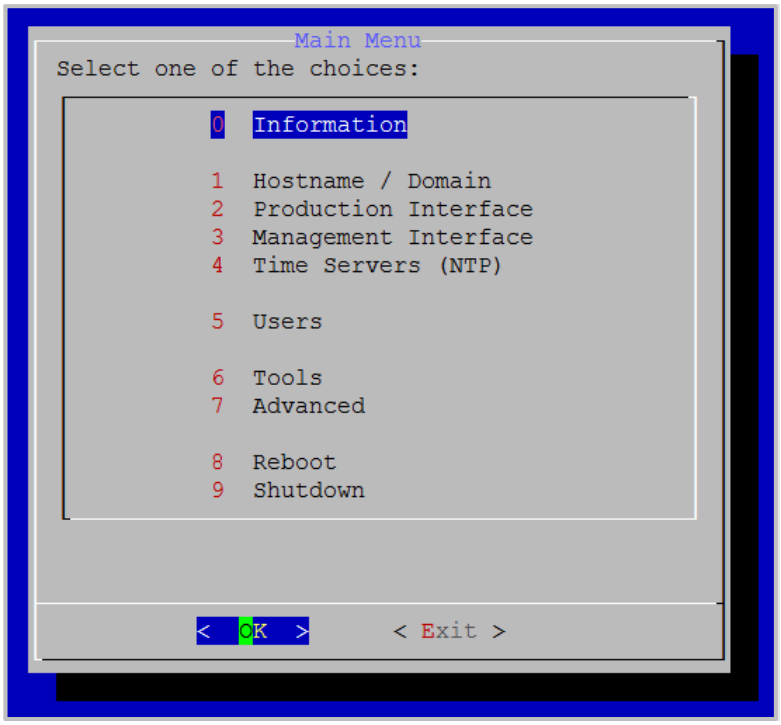
8. Enter **1** to select the List Users option.
9. Press the **Enter** key to select **OK**. The *V3 Users* window, which lists all the V3 users, displays.

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

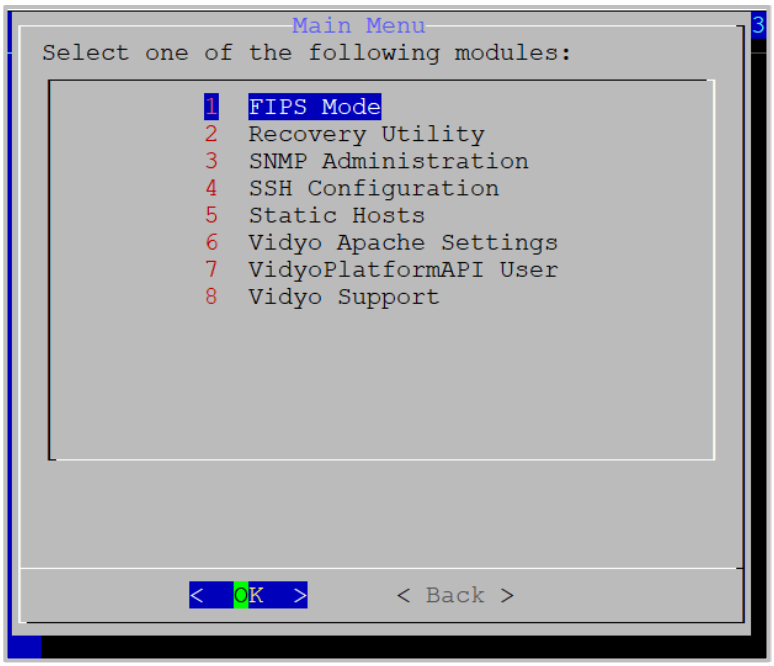
Add SNMP v3 users

To add SNMP v3 Users:

1. Log in to the System Console. The Main Menu displays.



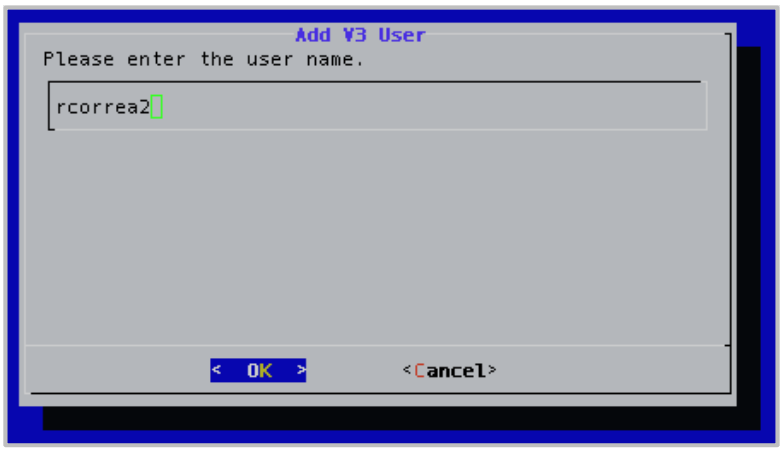
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



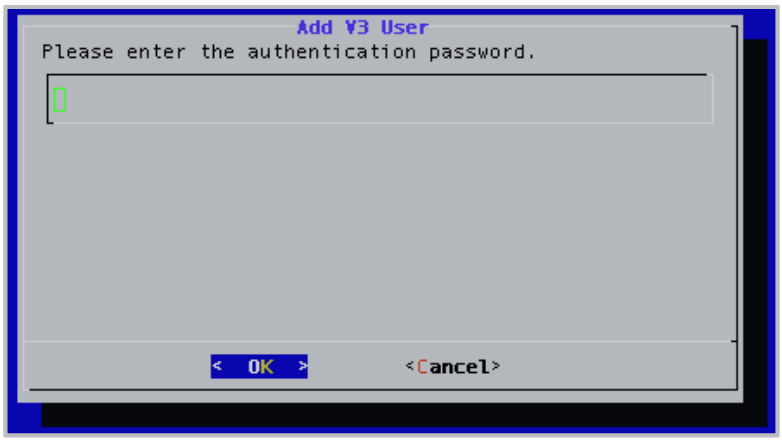
4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

6. Enter **3** to select the V3 Users option.
7. Press the **Enter** key to select **OK**. The SNMP V3 Community Menu displays.

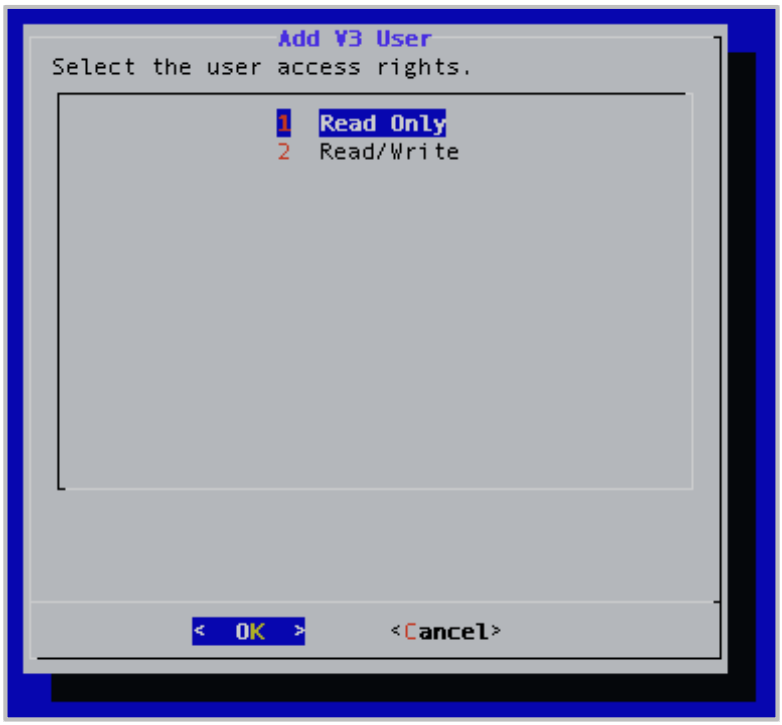
8. Enter **2** to select the Add User option.
9. Press the **Enter** key to select **OK**. The *Add V3 User* window displays.



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.



12. Enter the password for the new V3 user.
13. Press the **Enter** key to select **OK**.
14. The next *Add V3 User* window displays.



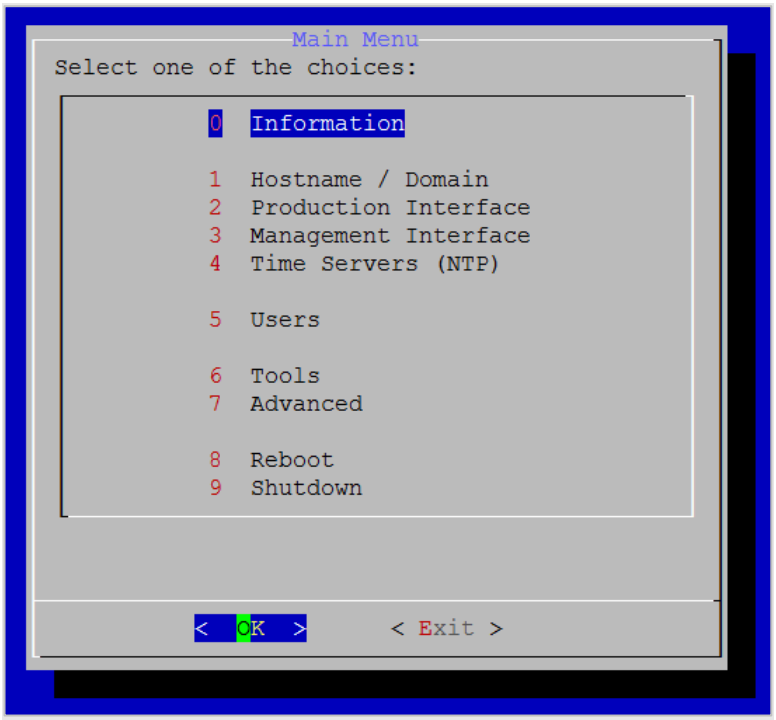
15. Enter **1** if you want the new v3 user's access rights to be read only or enter **2** if you want the new v3 user's access rights to be read and write.
16. Press the **Enter** key to select **OK**.

17. Select the user privacy method: **AES**, **DES**, or **None**.
18. Press the **Enter** key to select **OK**.
19. Enter the privacy password.
20. Press the **Enter** key to select **OK**.

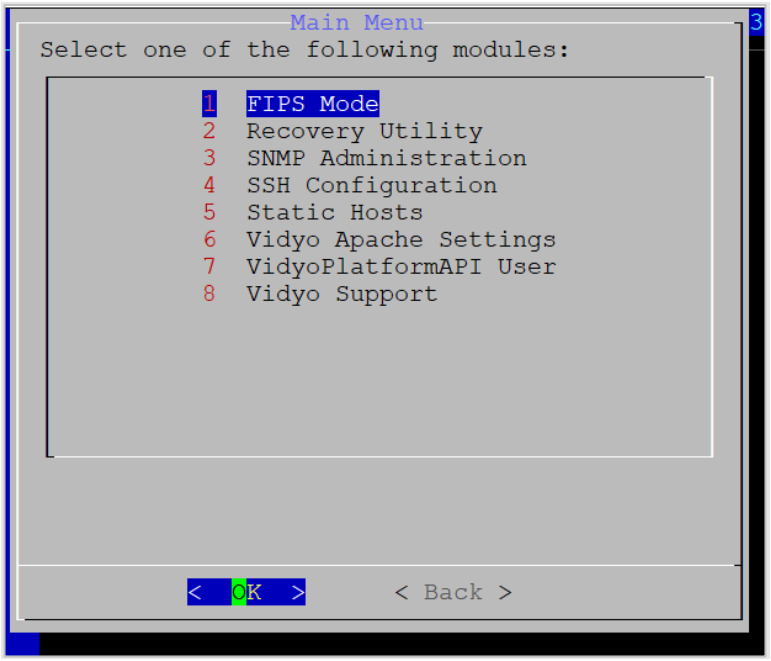
Remove an SNMP v3 user

To remove an SNMP v3 user:

1. Log in to the System Console. The Main Menu displays.



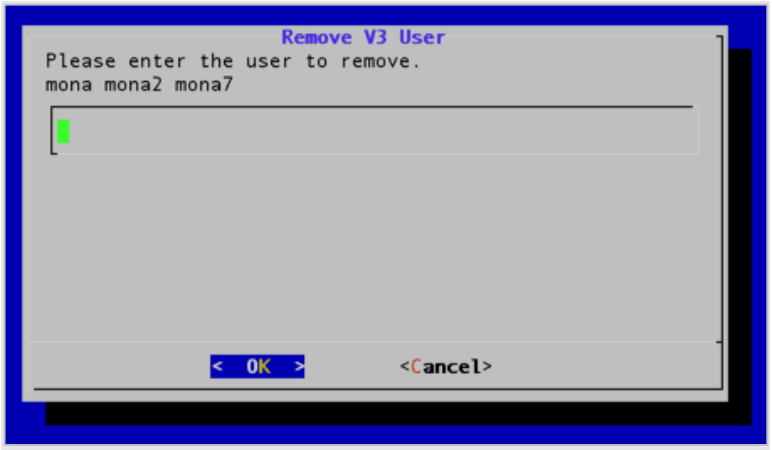
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

6. Enter **3** to select the V3 Users option.
7. Press the **Enter** key to select **OK**. The SNMP V3 Users Menu displays.

8. Enter **3** to select the Remove User option.
9. Press the **Enter** key to select **OK**. The *Remove V3 User* window displays.

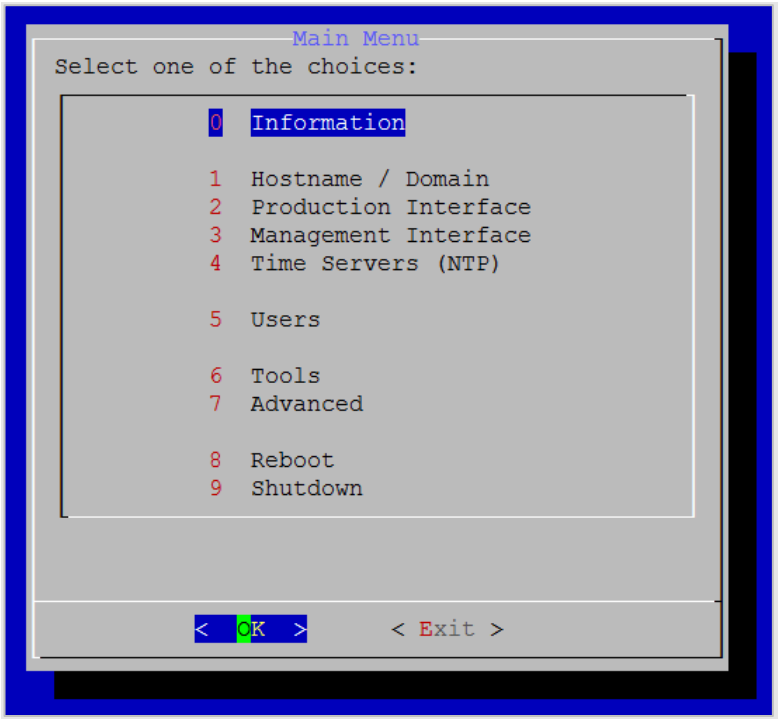


10. Press the **Enter** key to select **OK**. A message displays stating “Successfully removed user.”
11. Press the **Enter** key to select **OK**.

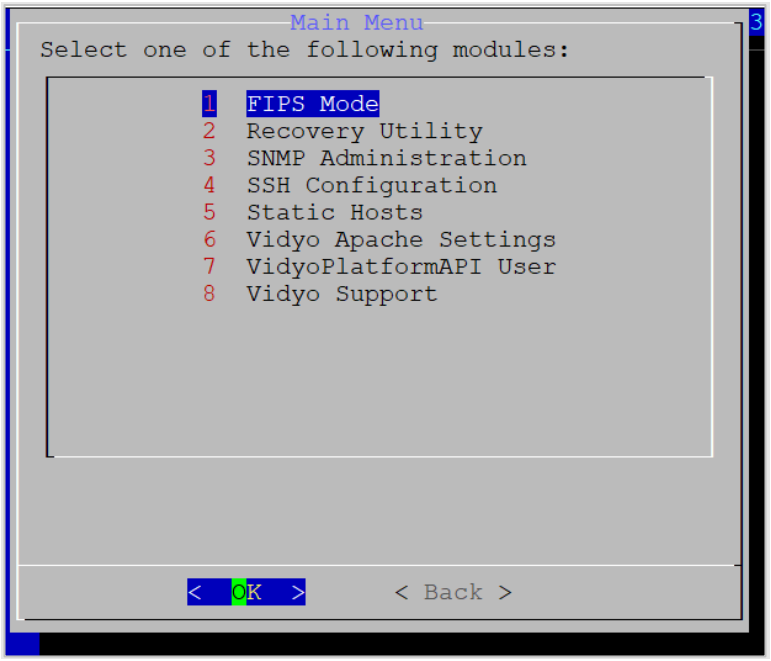
List SNMP v3 notifications

To list an SNMP v3 notification:

1. Log in to the System Console. The Main Menu displays.



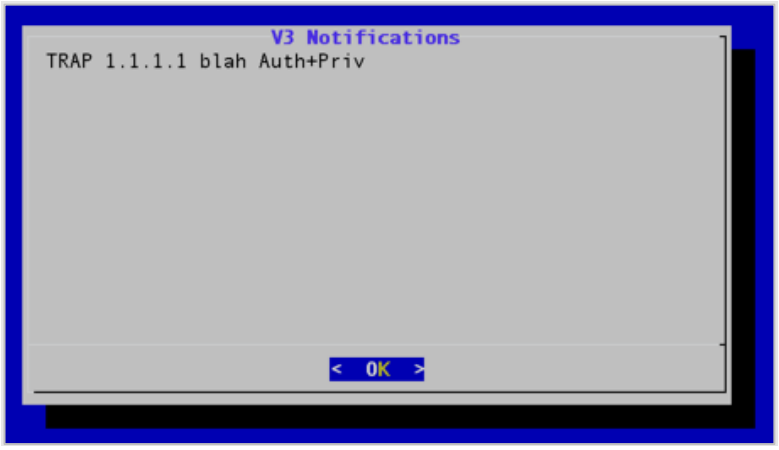
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

6. Enter **3** to select the V3 Users option.
7. Press the **Enter** key to select **OK**. The SNMP V3 Users Menu displays.

8. Enter **4** to select the List Notifications option.
9. Press the **Enter** key to select **OK**. The *V3 Notifications* window displays.

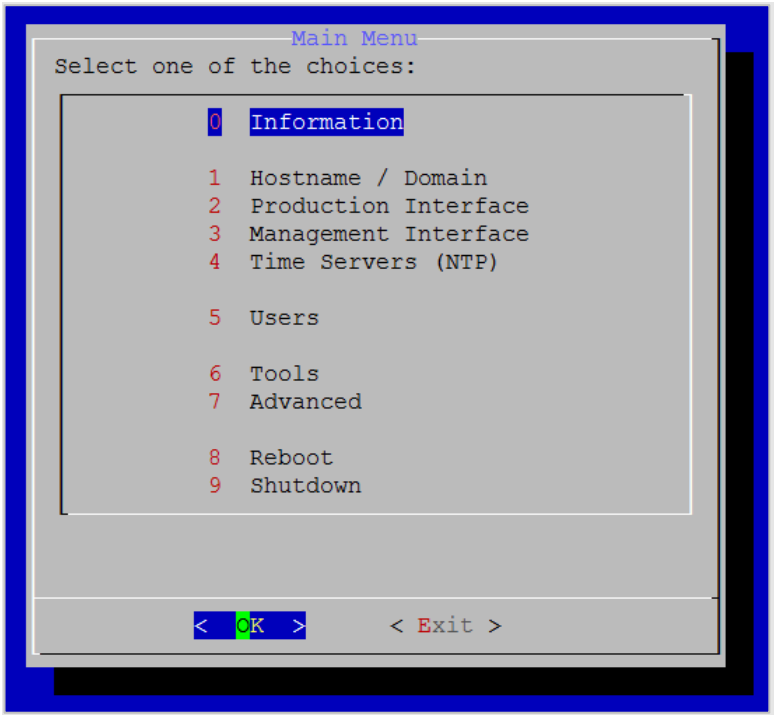


10. Press the **Enter** key to select **OK**.

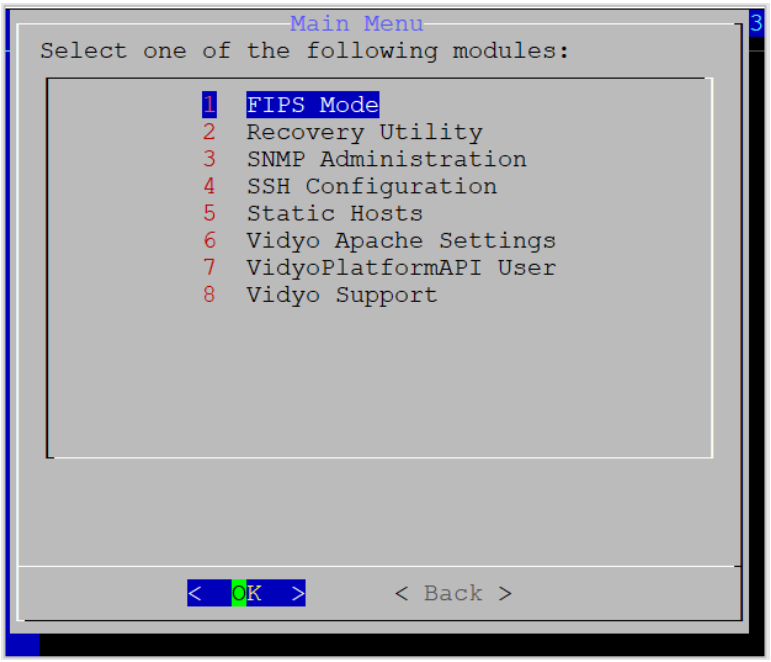
Add SNMP v3 notifications

To add an SNMP v3 notification:

1. Log in to the System Console. The Main Menu displays.



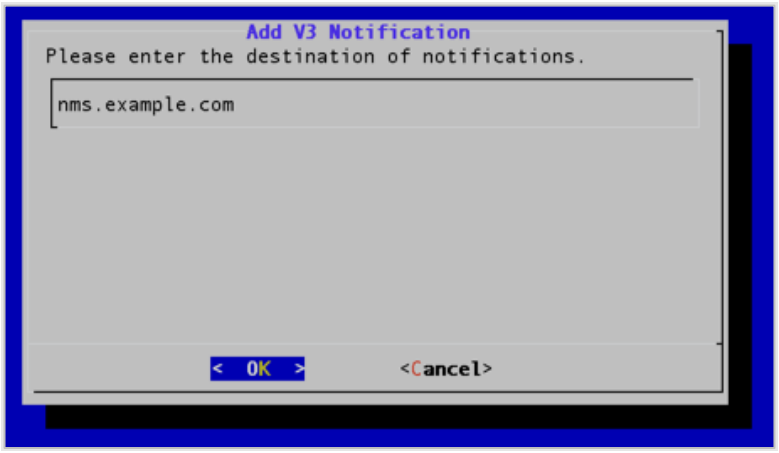
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



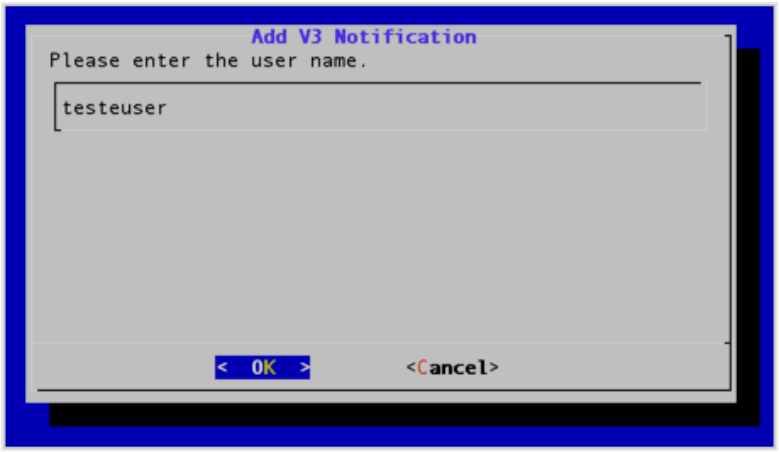
4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

6. Enter **3** to select the V3 Users option.
7. Press the **Enter** key to select **OK**. The SNMP V3 Users Menu displays.

8. Enter **5** to select the Add Notification option.
9. Press the **Enter** key to select **OK**. The *Add V3 Notification* window displays.



10. Enter the IP address or FQDN of the notification's destination.
11. Press the **Enter** key to select **OK**.



12. Enter the user name.
13. Press the **Enter** key to select **OK**.

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**.

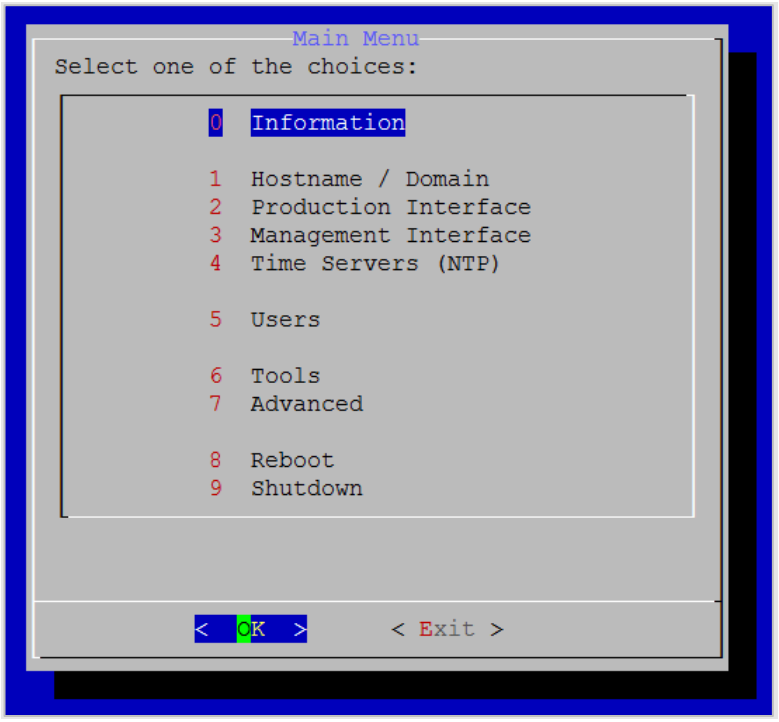
16. Enter the user authentication password.
17. Press the **Enter** key to select **OK**.

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**.

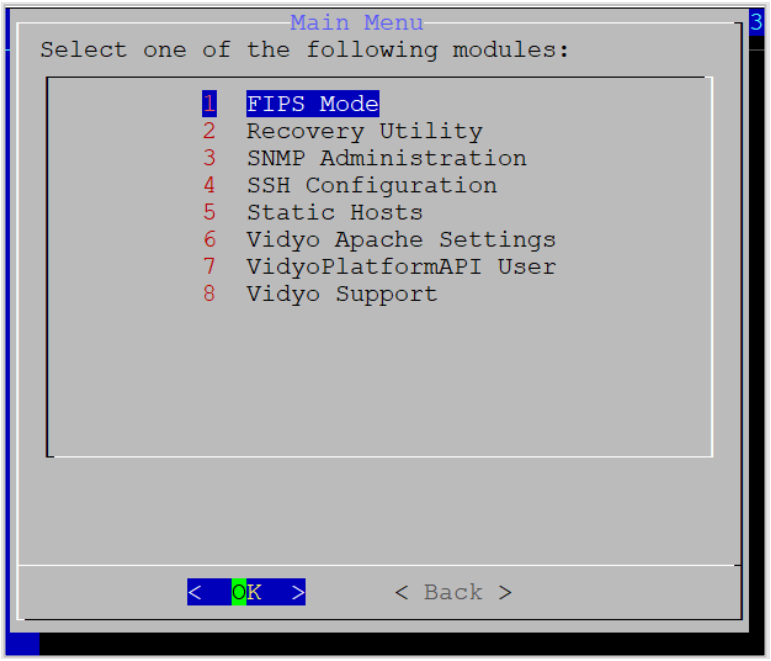
Remove SNMP v3 notifications

To remove an SNMP v3 notification:

1. Log in to the System Console. The Main Menu displays.



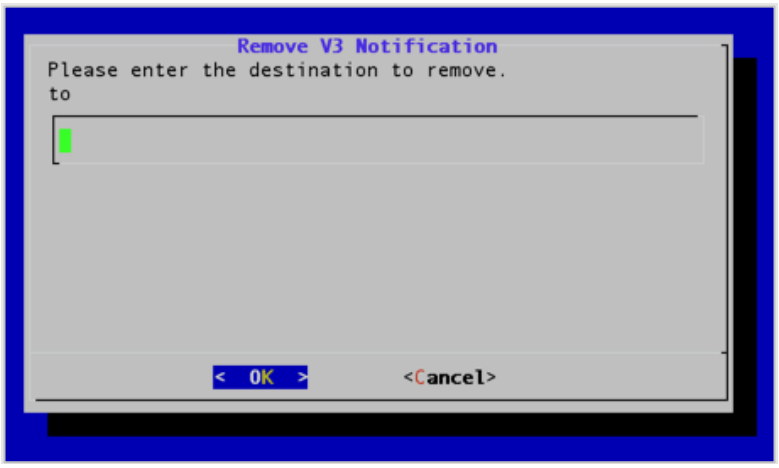
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **3** to select the SNMP Administration option.
5. Press the **Enter** key to select **OK**. The SNMP Menu displays.

6. Enter **3** to select the V3 Users option.
7. Press the **Enter** key to select **OK**. The SNMP V3 Users Menu displays.

8. Enter **6** to select the Remove Notification option.
9. Press the **Enter** key to select **OK**. The Remove V3Notification window displays.

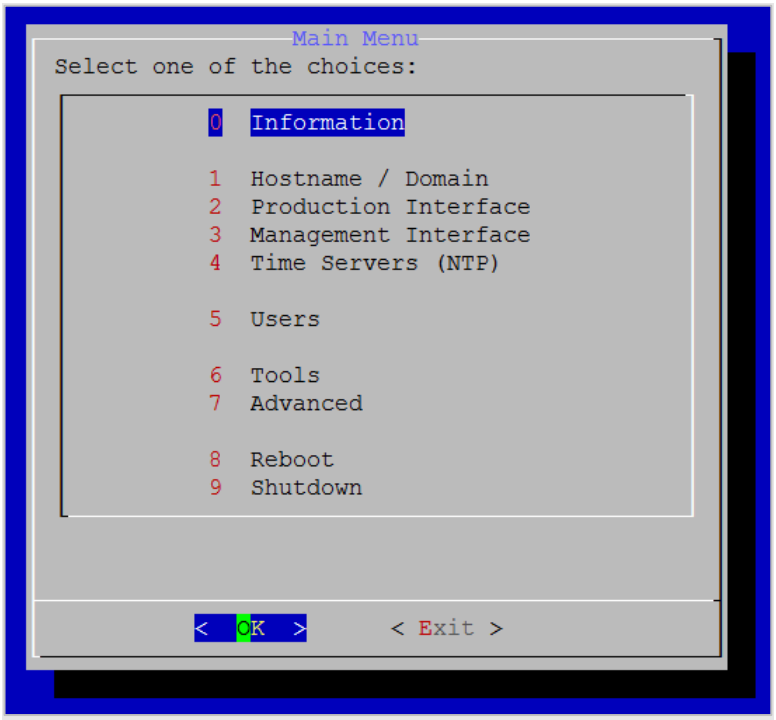


10. Enter the IP address or FQDN of the notification you want to remove.
11. Press the **Enter** key to select **OK**. A message displays stating “Successfully removed notification.”
12. Press the **Enter** key to select **OK**.

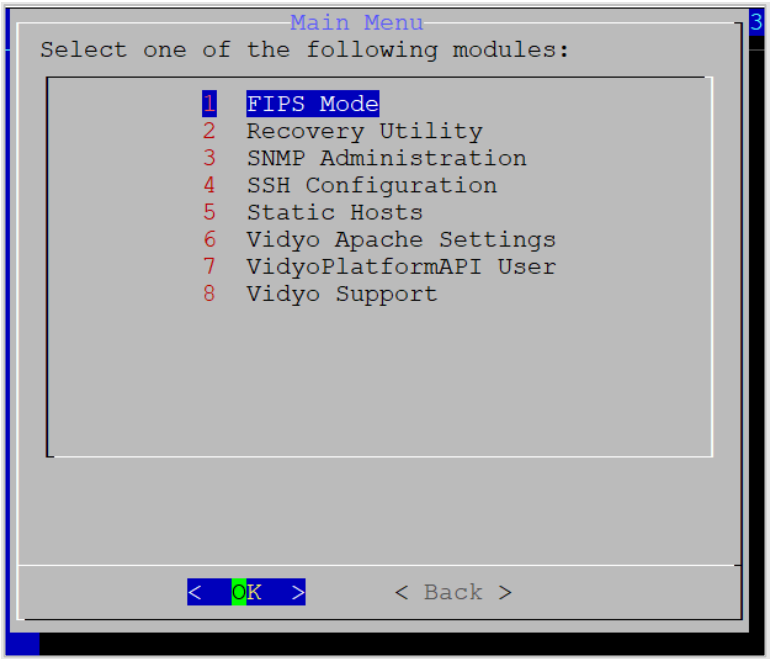
Configure SSH

To configure SSH:

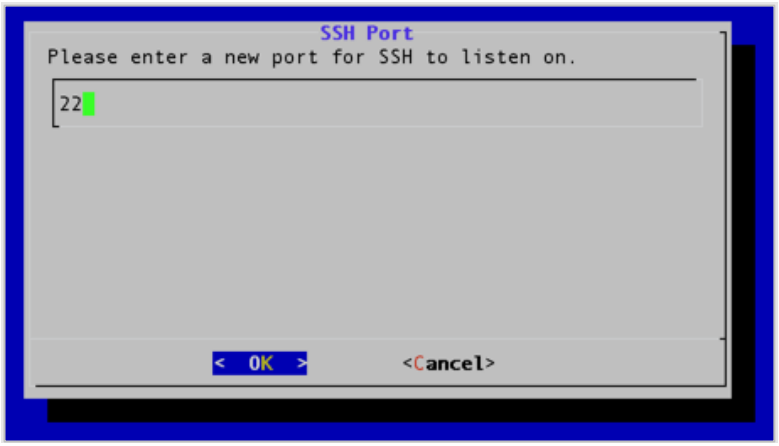
1. Log in to the System Console. The Main Menu displays.



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 **4** to select the SSH Configuration option.
5. Press the **Enter** key to select **OK**. The *SSH Port* window displays.



6. Enter the port number on which SSH can listen.
7. Press the **Enter** key to select **OK**. The *Confirm* window displays.

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**.

Manage static hosts

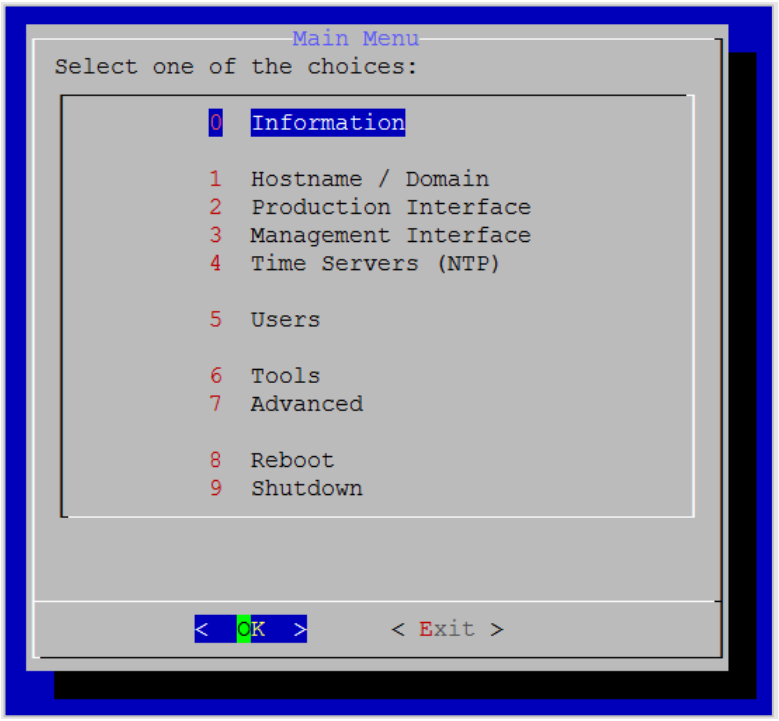
Static Host entries can be added to a single host file on your VidyoPortal. These entries are used to map an IP address to a specific Static Host or FQDN.

> 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.

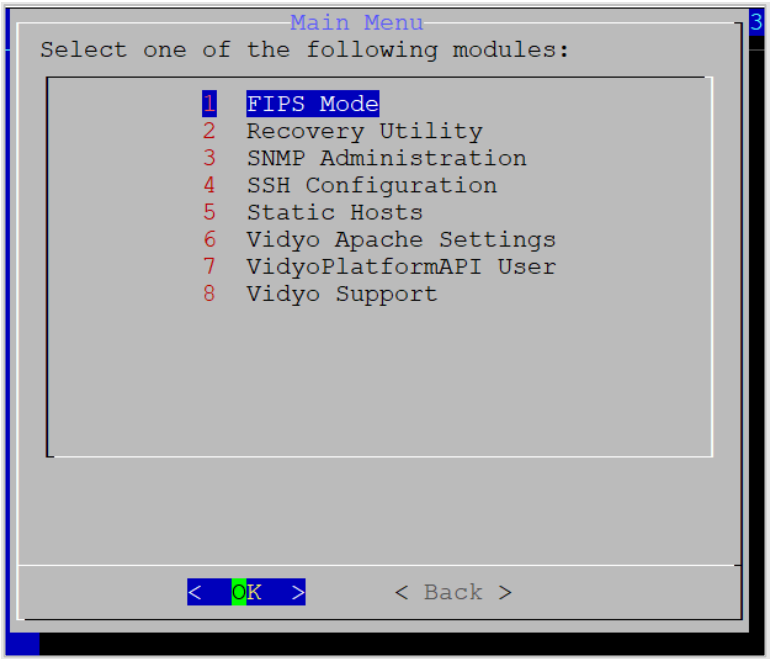
View active information

To view active information:

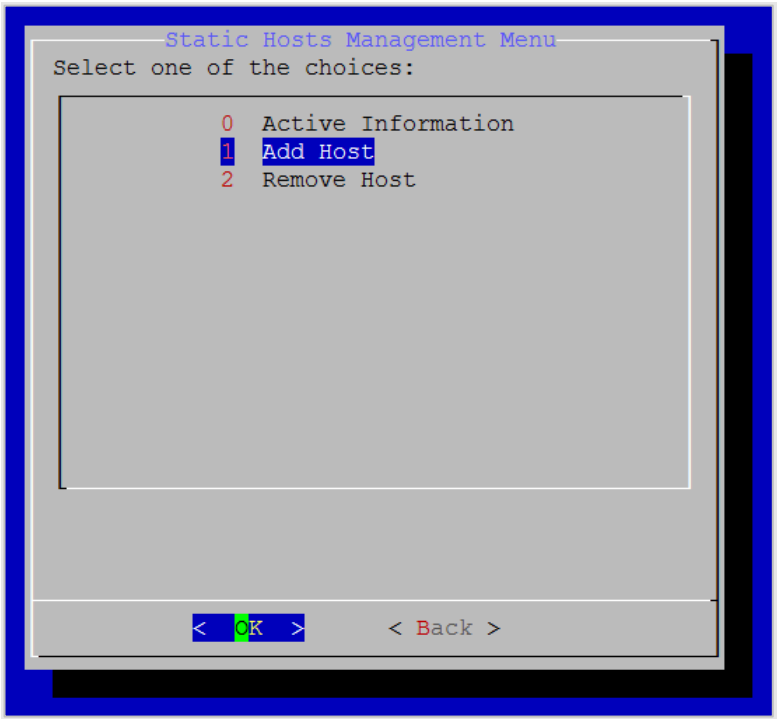
1. Log in to the System Console. The Main Menu displays.



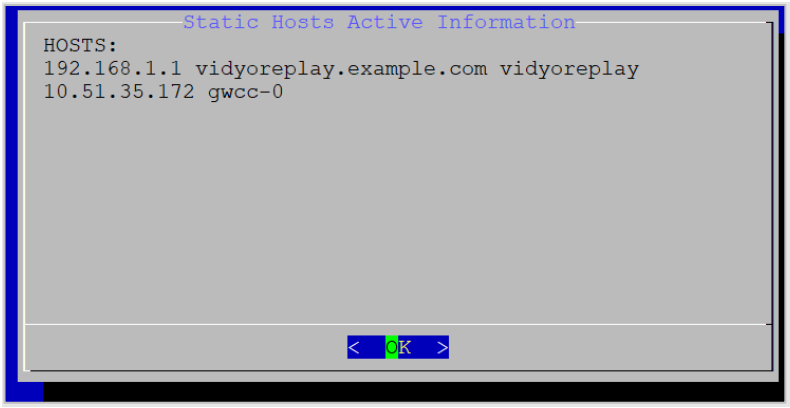
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **5** to select the Static Hosts option.
5. Press the **Enter** key to select **OK**. The Static Hosts Management Menu displays.



6. Enter **0** to select the Active Information option. The *Static Hosts Active Information* window displays.

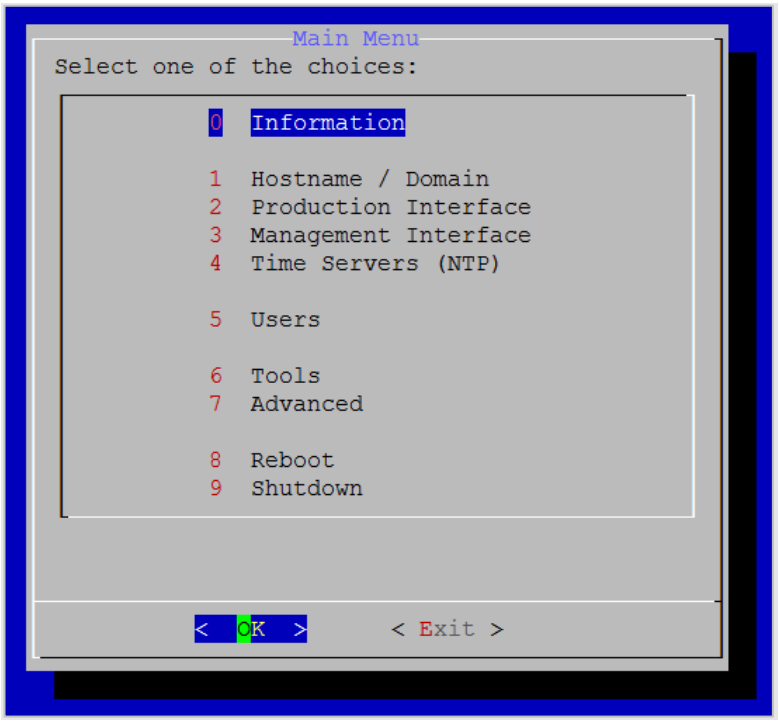


7. Press the **Enter** key to select **OK**.

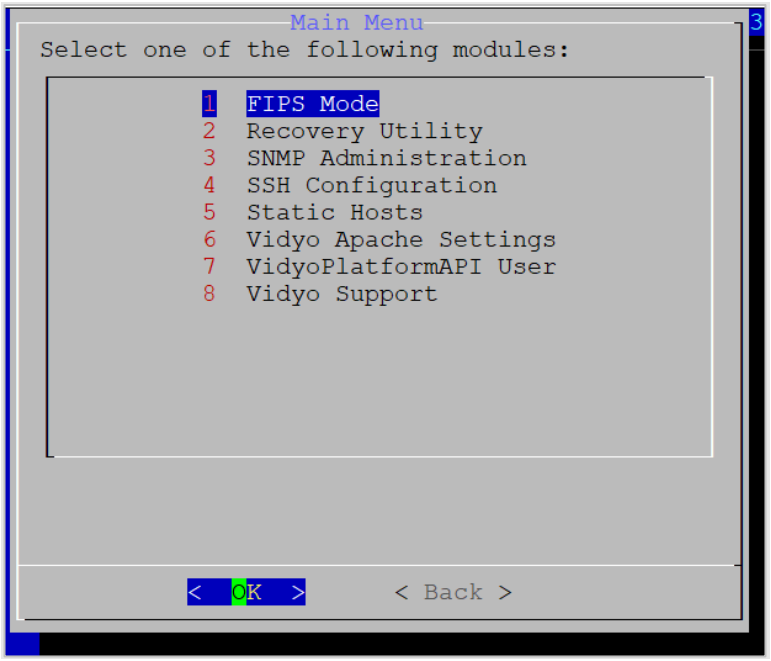
Add static hosts

To view add static hosts:

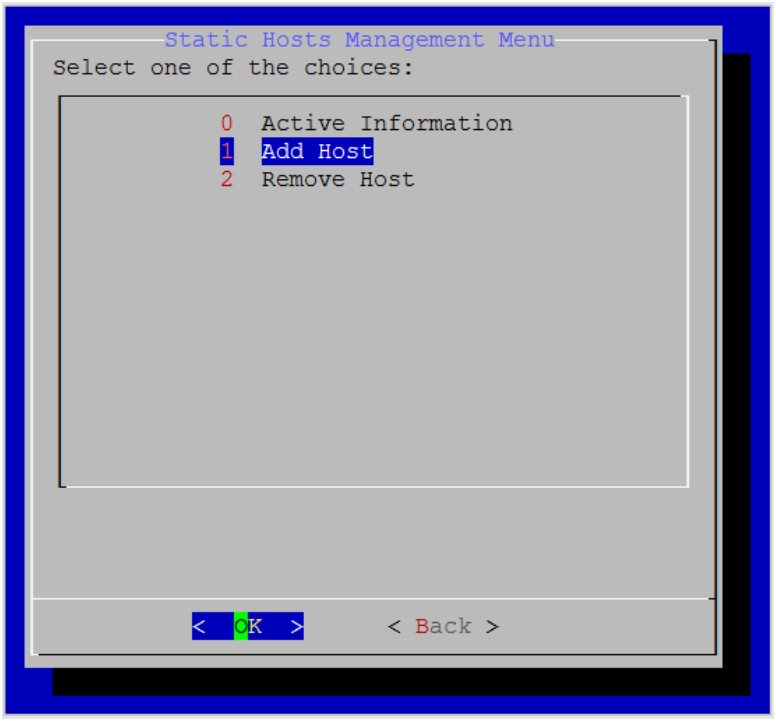
1. Log in to the System Console. The Main Menu displays.



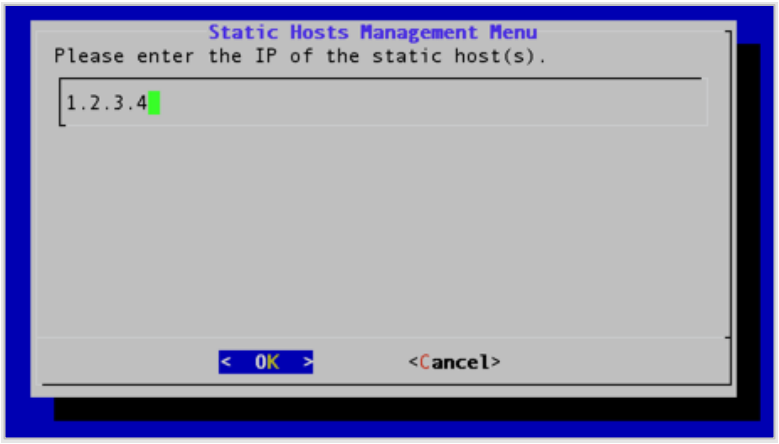
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



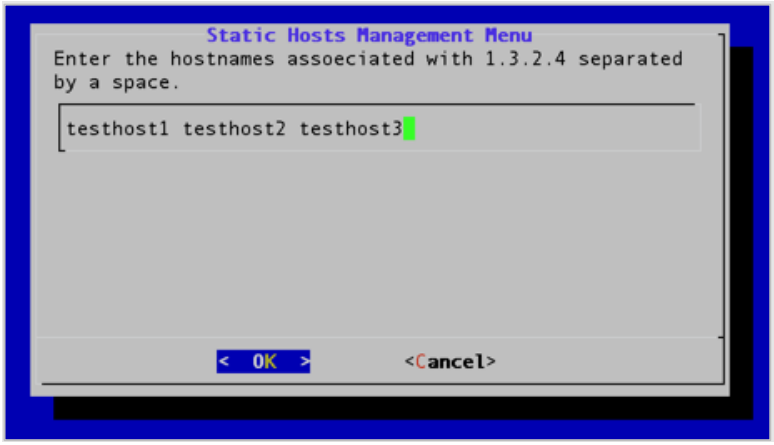
4. Enter **5** to select the Static Hosts option.
5. Press the **Enter** key to select **OK**. The Static Hosts Management Menu displays.



6. Enter **1** to select the Add Host option.
7. Press the **Enter** key to select **OK**. The *Static Hosts Management Menu* window displays.



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.

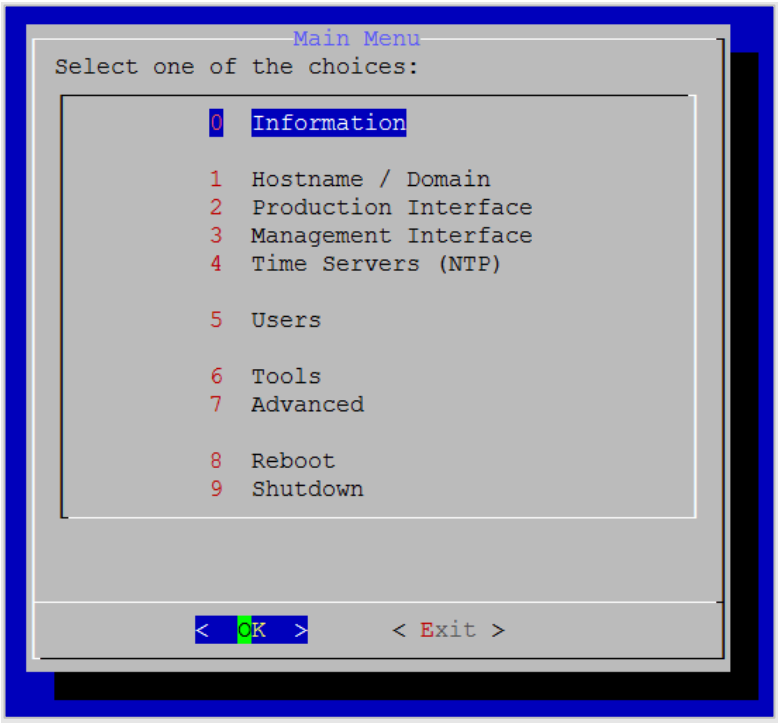


10. Enter the hostname(s) you want to associate with the IP address you just entered.
11. Press the **Enter** key to select **Yes**. The *Message* window displays indicating that the IP address has been added.
12. Press the **Enter** key to select **OK**.

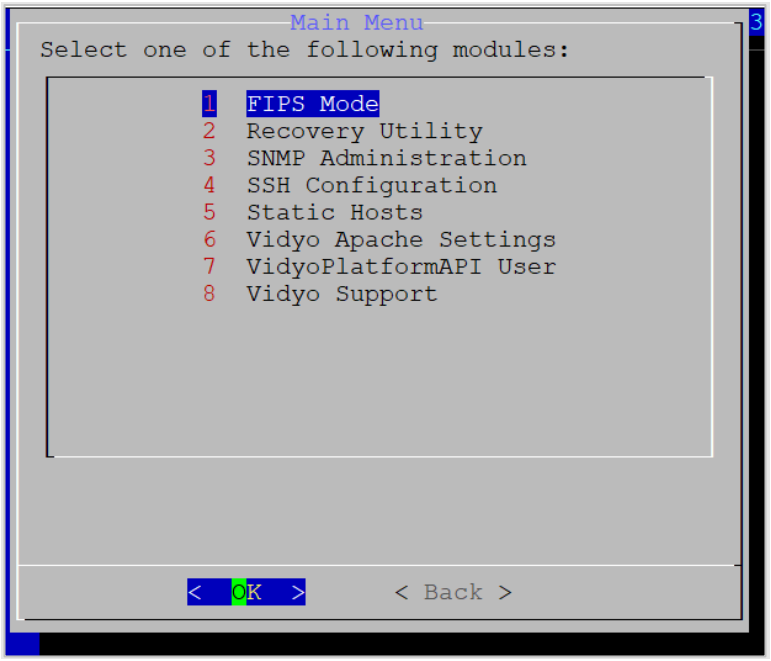
Remove static hosts

To view remove static hosts:

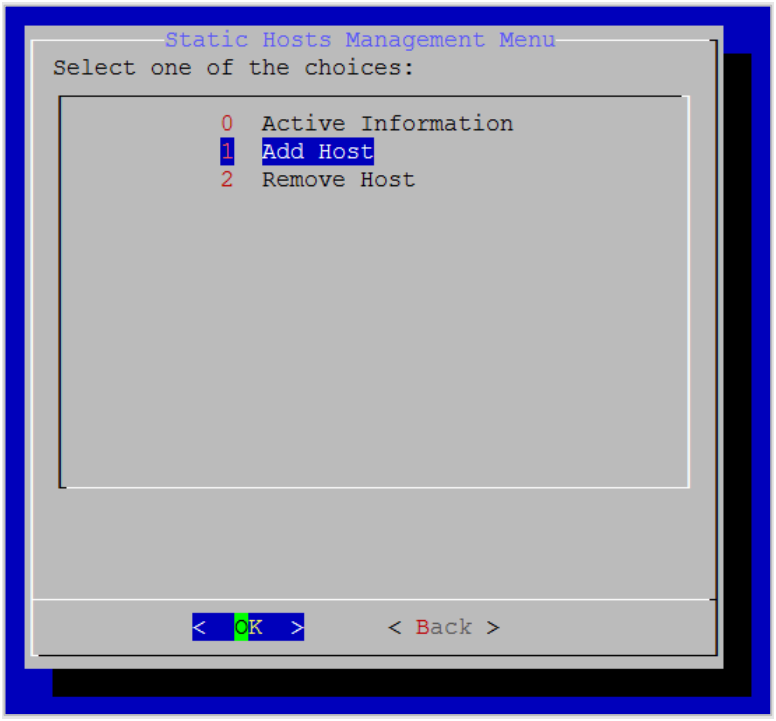
1. Log in to the System Console. The Main Menu displays.



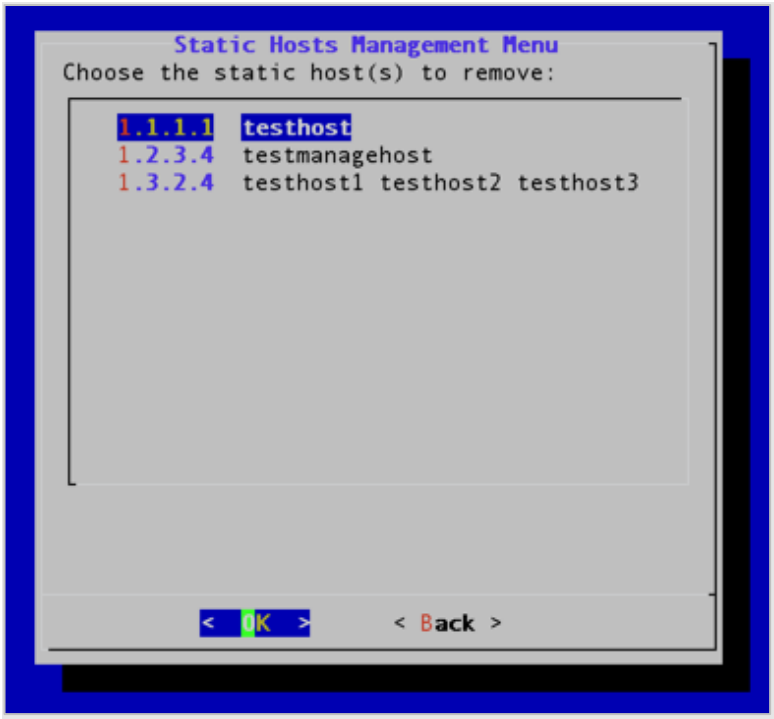
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **5** to select the Static Hosts option.
5. Press the **Enter** key to select **OK**. The Static Hosts Management Menu displays.



6. Enter **2** to select the Remove Host option.
7. Press the **Enter** key to select **OK**. The *Static Hosts Management Menu* window displays.



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.

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**.

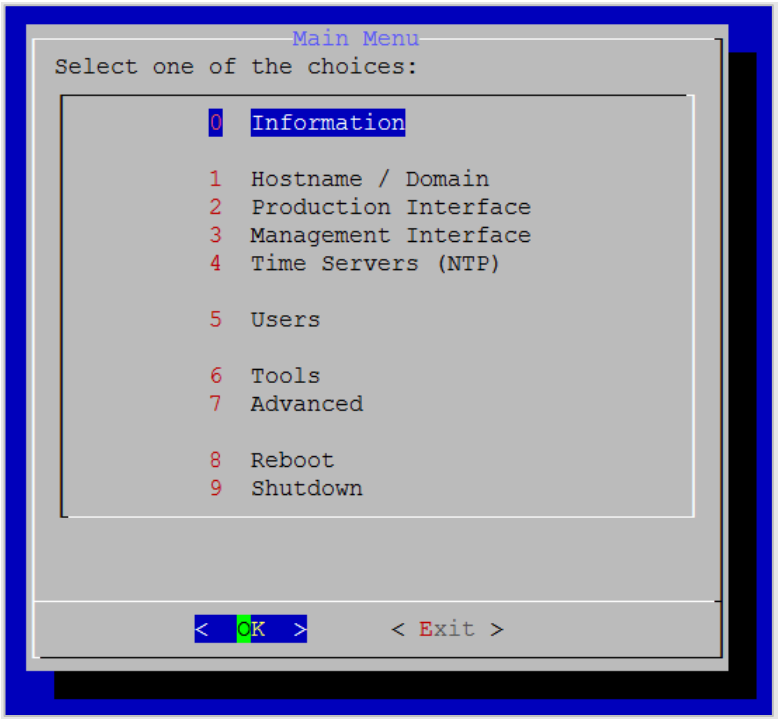
Manage Vidyo Apache settings

This section describes how to view current settings, set modern or intermediate profiles, enable or disable OCSP stapling, and steps to reload Apache.

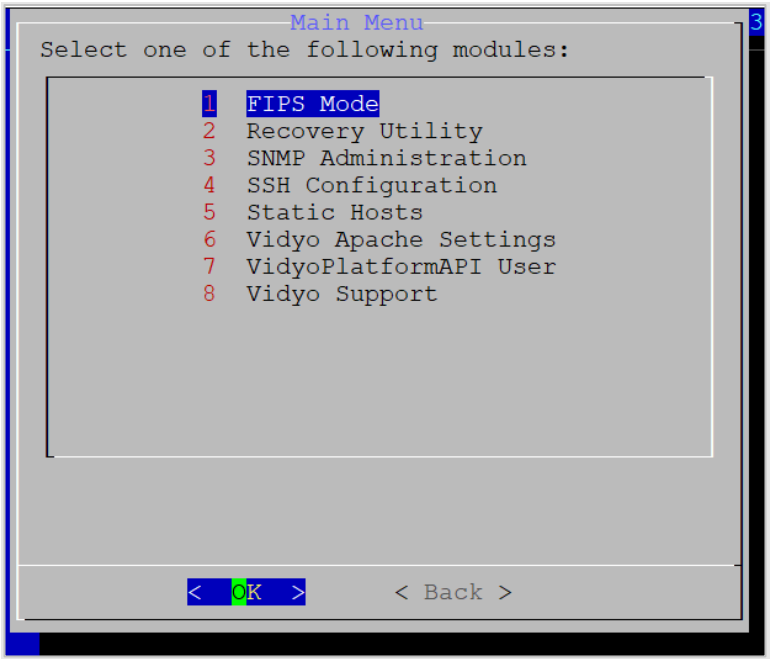
View display current settings

To view display current settings:

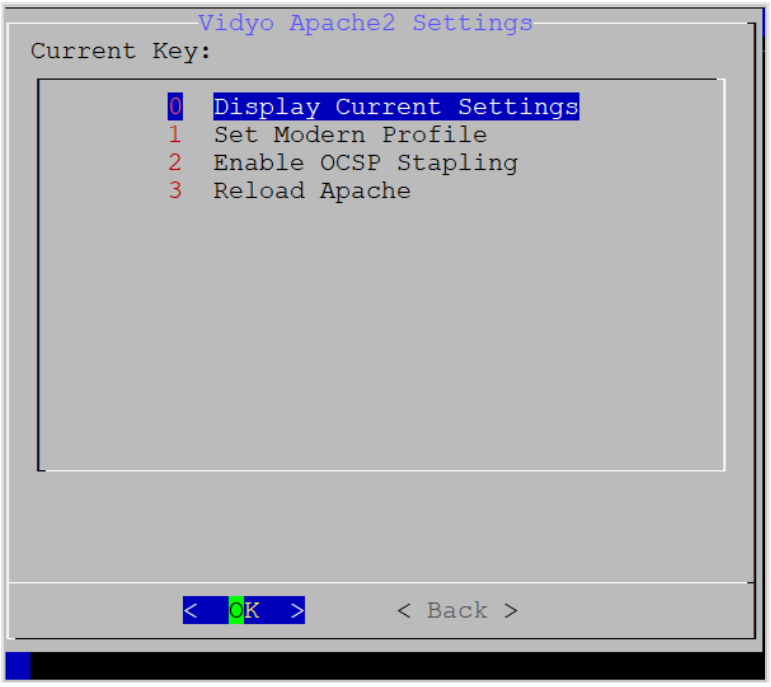
1. Log in to the System Console. The Main Menu displays.



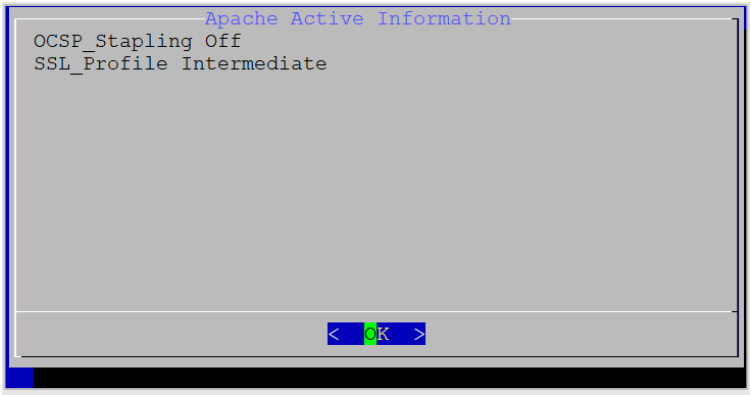
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **6** to select the Vidyo Apache Settings.
5. Press the **Enter** key to select **OK**. The Vidyo Apache2 Settings window displays.



6. Enter **0** to select the Display Current Settings option. The *Apache Active Information* window displays.

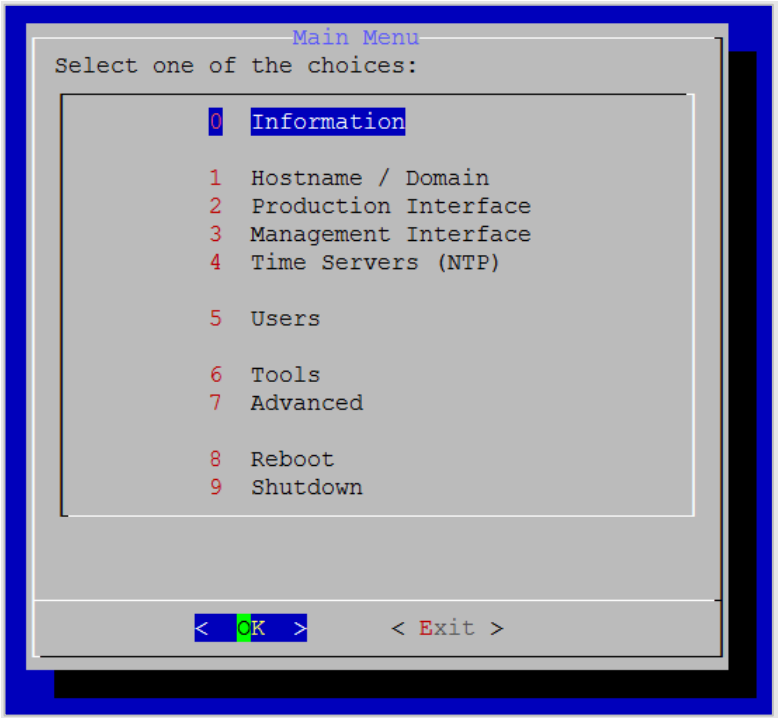


7. Press the **Enter** key to select **OK**.

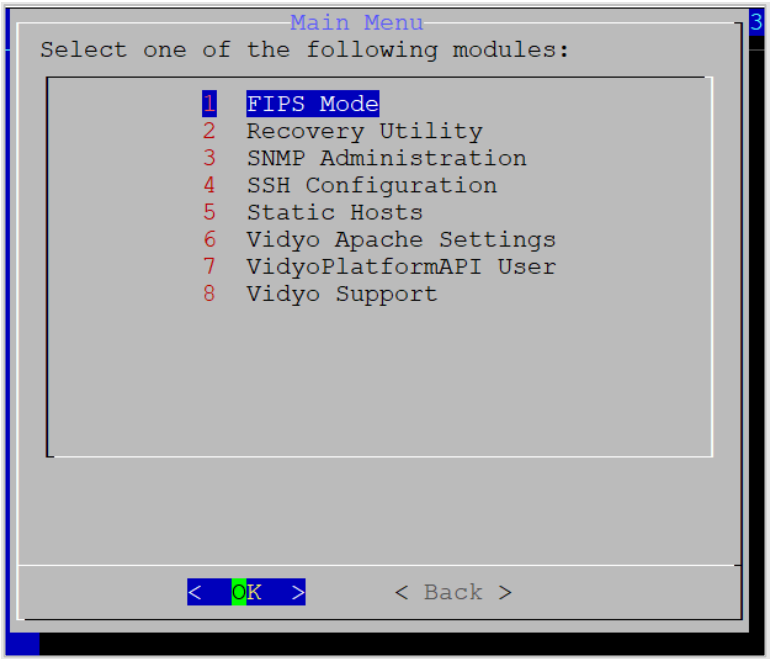
Set modern or intermediate profiles

To set modern profile:

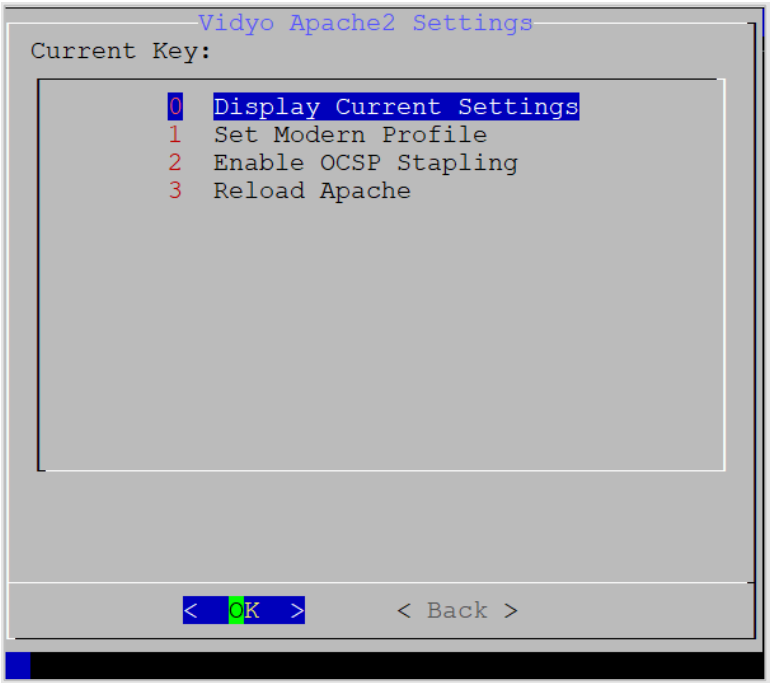
1. Log in to the System Console. The Main Menu displays.



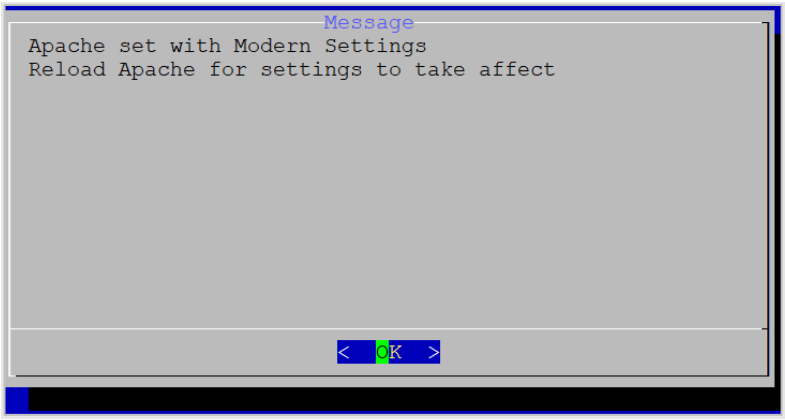
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **6** to select the Vidyo Apache Settings option.
5. Press the **Enter** key to select **OK**. The *Vidyo Apache2 Settings* window displays.



6. Enter **1** to select the Set Modern profile option.
7. Press the **Enter** key to select **OK**. The *Message* window displays.



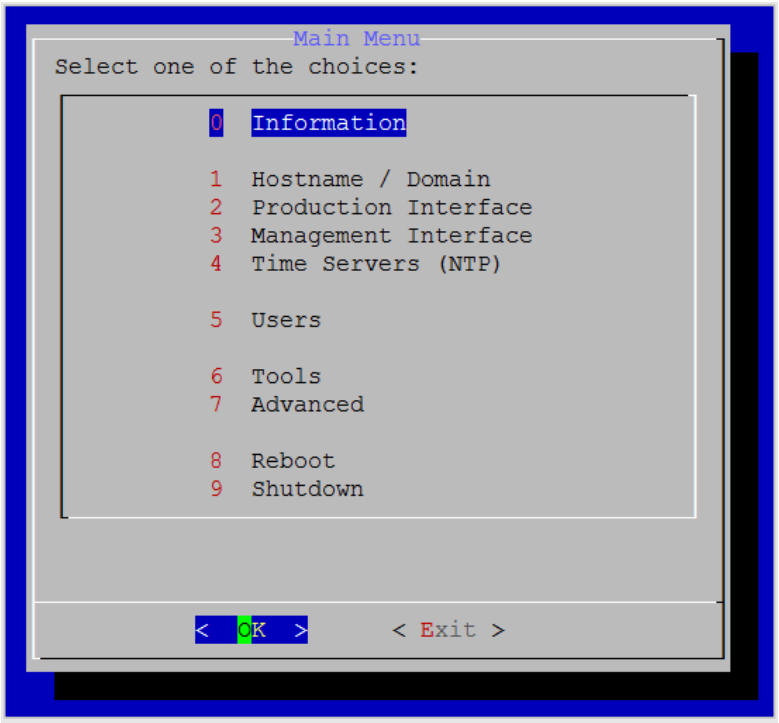
8. Press the **Enter** key to select **OK**.

> Note
>
> When setting profiles, make sure to reload Apache for settings to take effect. Go back to the Vidyo Apache2 Settings window, and then press **3** for the Reload Apache option.
>
> To set Intermediate Profile after Set Modern Profile, go back into the Vidyo Apache2 Settings window and then select Intermediate Profile.

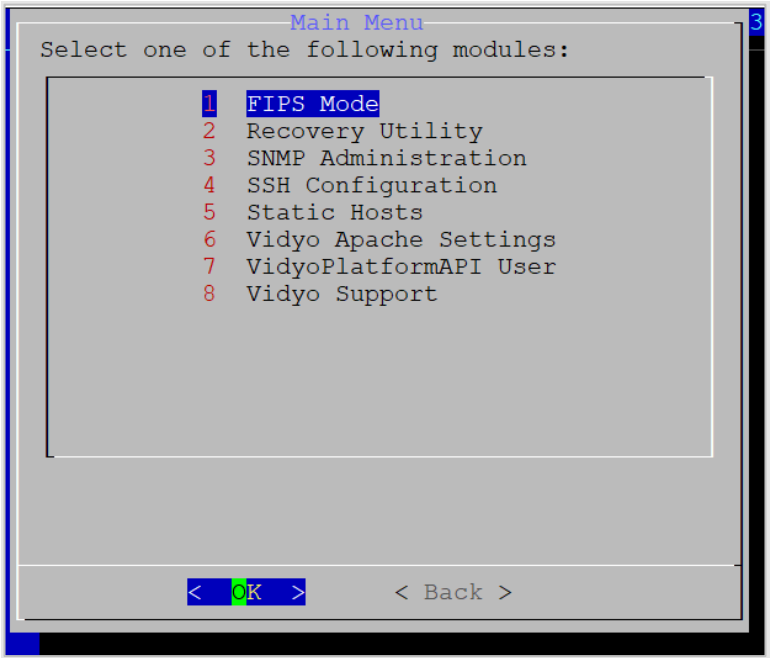
Enable or disable OCSP Stapling

To enable OCSP Stapling:

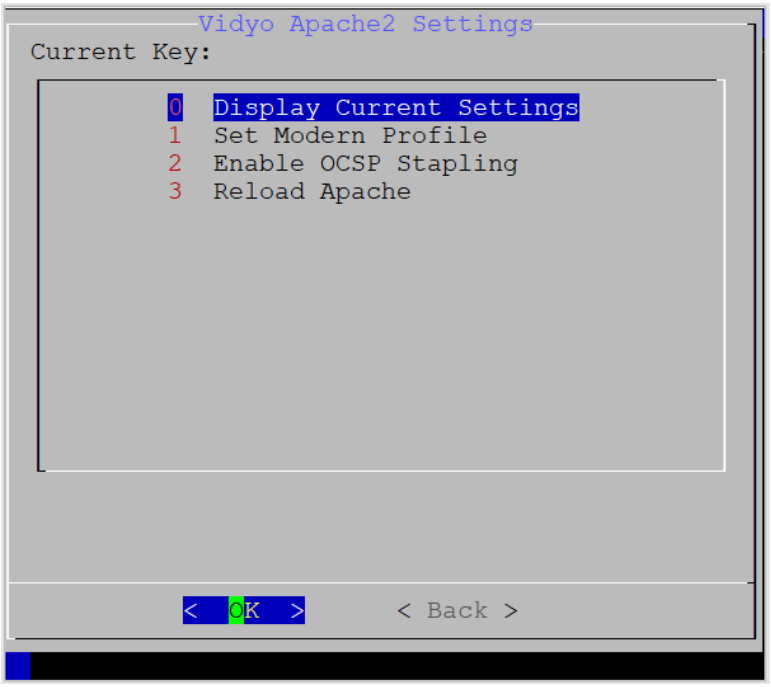
1. Log in to the System Console. The Main Menu displays.



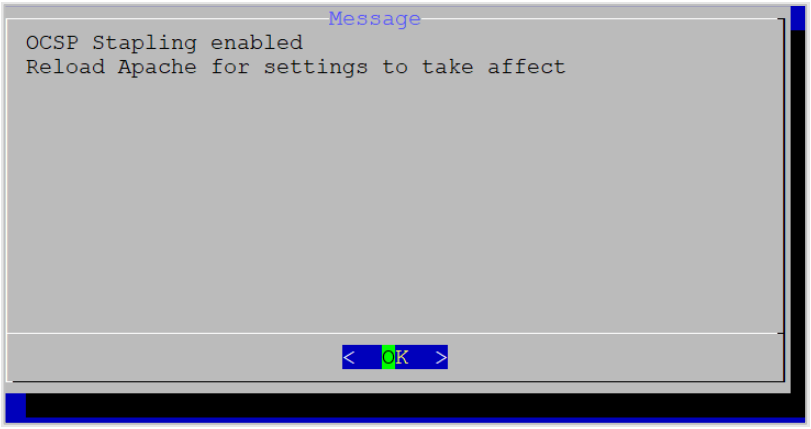
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **6** to select the Vidyo Apache Settings option.
5. Press the **Enter** key to select **OK**. The Vidyo Apache2 Settings Menu displays.



6. Enter **2** to select the Enable OCSP Stapling option. The Message window displays.



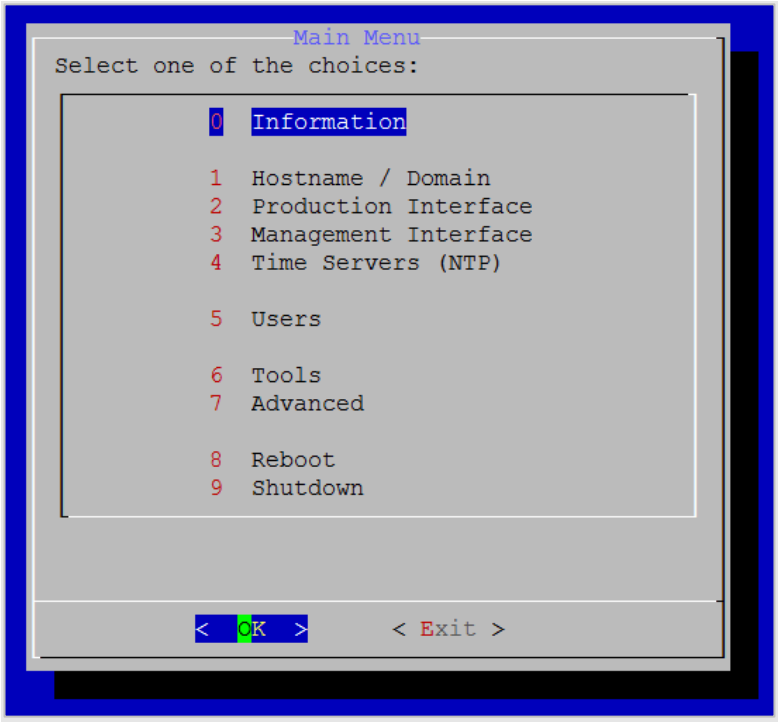
7. Press the **Enter** key to select **OK**.

> Note
>
> After enabling OCSP Stapling, make sure to reload Apache for settings to take effect. Go back to the Vidyo Apache2 Settings window, and then press **3** for the Reload Apache option.
>
> To disable OCSP Stapling after enabling, go back into the VIdyoApache2 Settings window and then select, Disable OCSP Stapling.

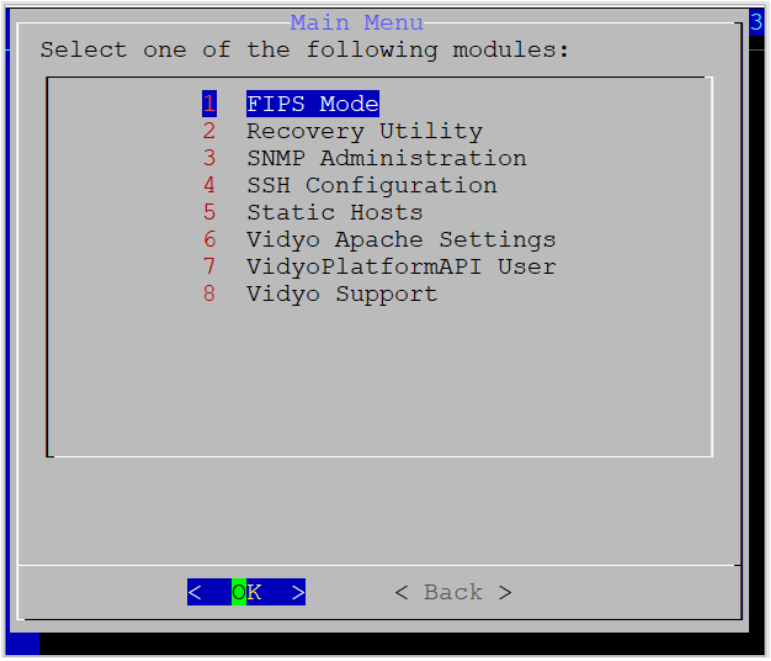
Reload Apache

To reload Apache:

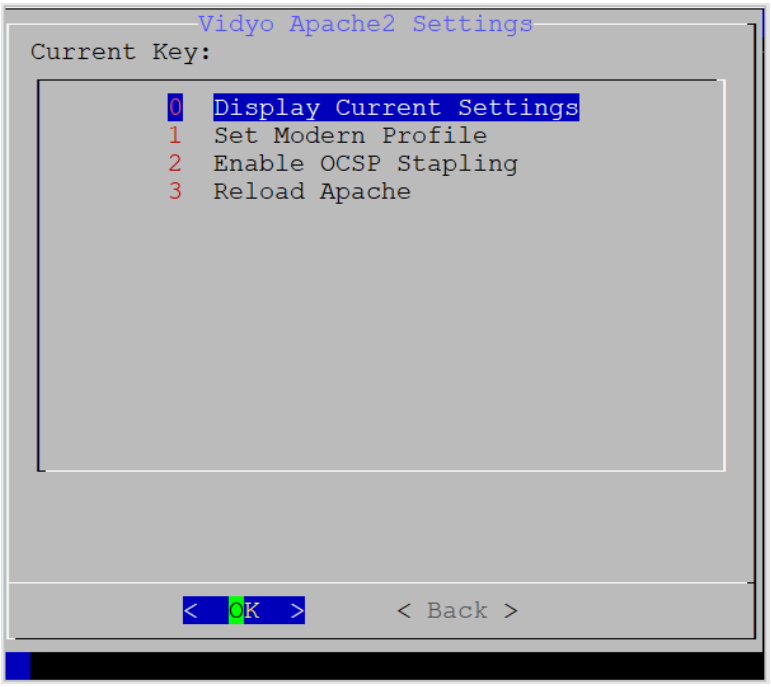
1. Log in to the System Console. The Main Menu displays.



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 **6** to select the Vidyo Apache Settings.
5. Press the **Enter** key to select **OK**. The Vidyo Apache2 Settings Menu displays.



6. Enter **3** to select the Reload Apache option. The Message window displays, “Apache reloaded with Settings”.

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

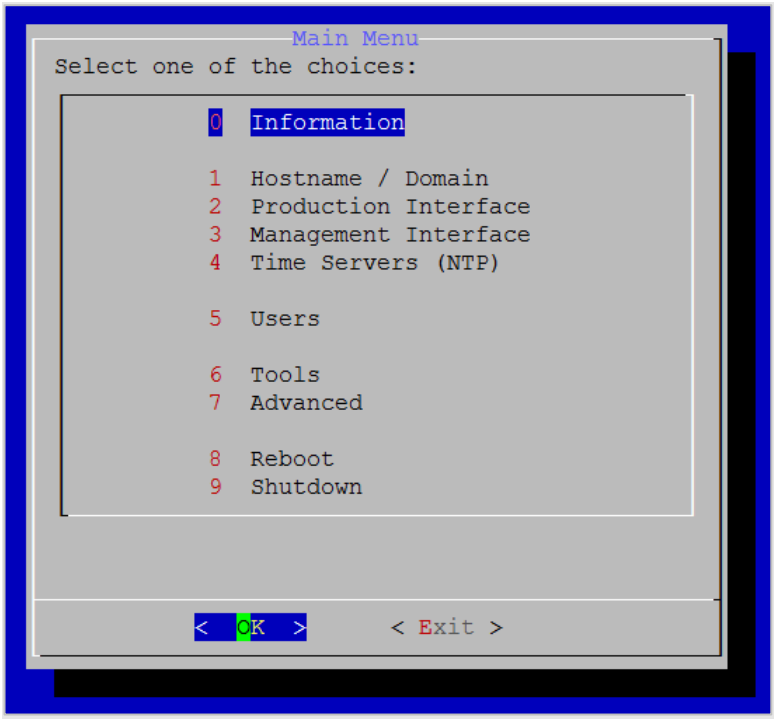
Manage VidyoPlatformAPI users

This section describes how to display a list of your API users as well as how to add, remove, and update API users.

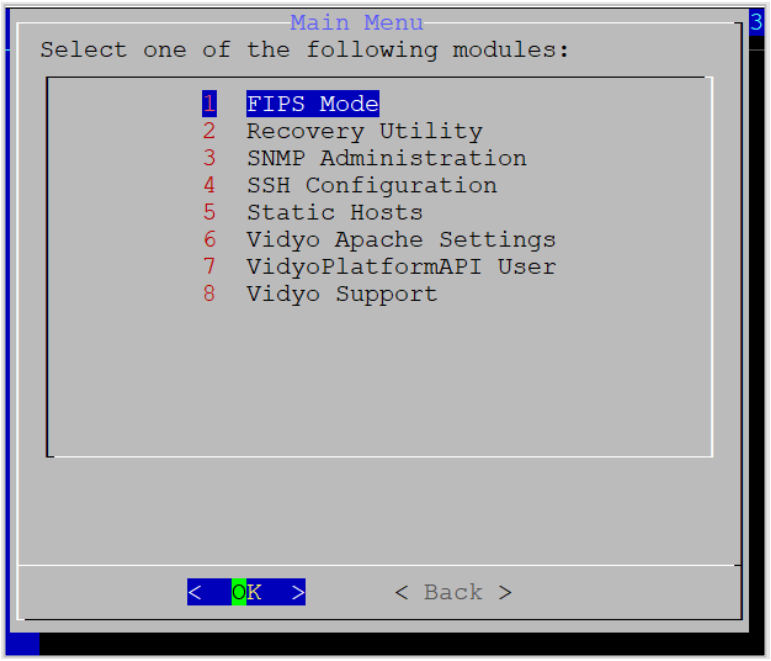
List API users

To list API users:

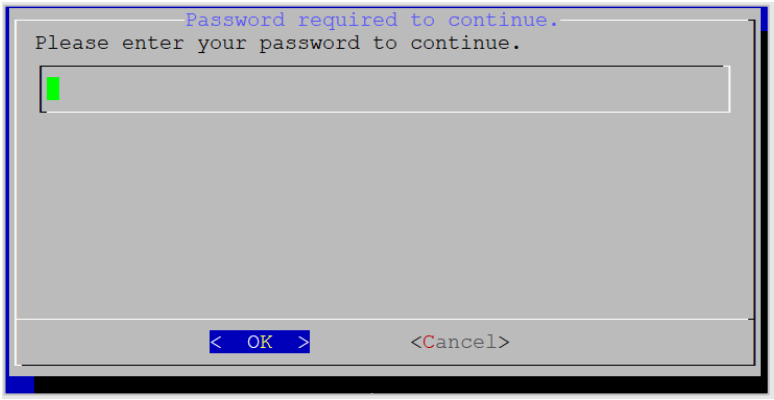
1. Log in to the System Console. The Main Menu displays.



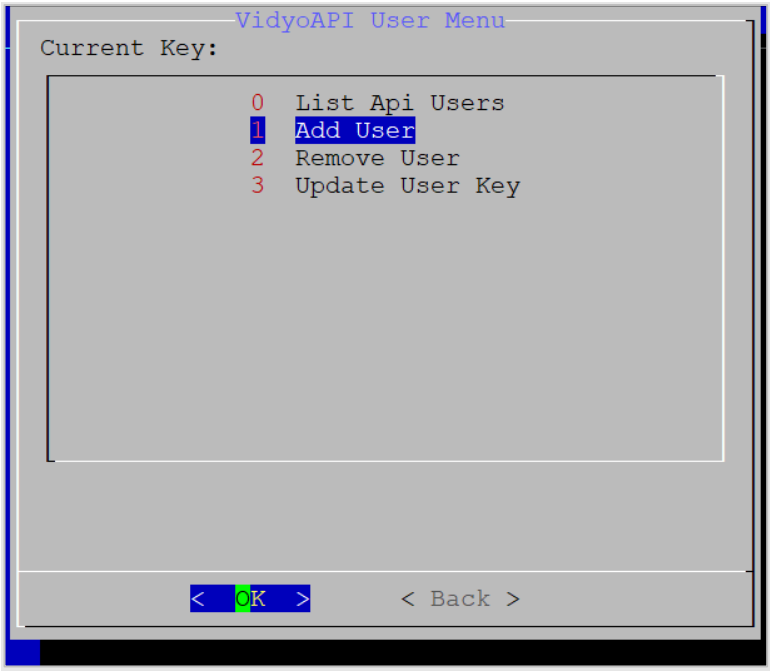
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **7** to select the VidyoPlatformAPI User option.
5. Press the **Enter** key to select **OK**. The *Password required to continue* window displays.



6. Enter your password and then press the **Enter** key to select **OK**. The *VidyoAPI User Menu* window displays.

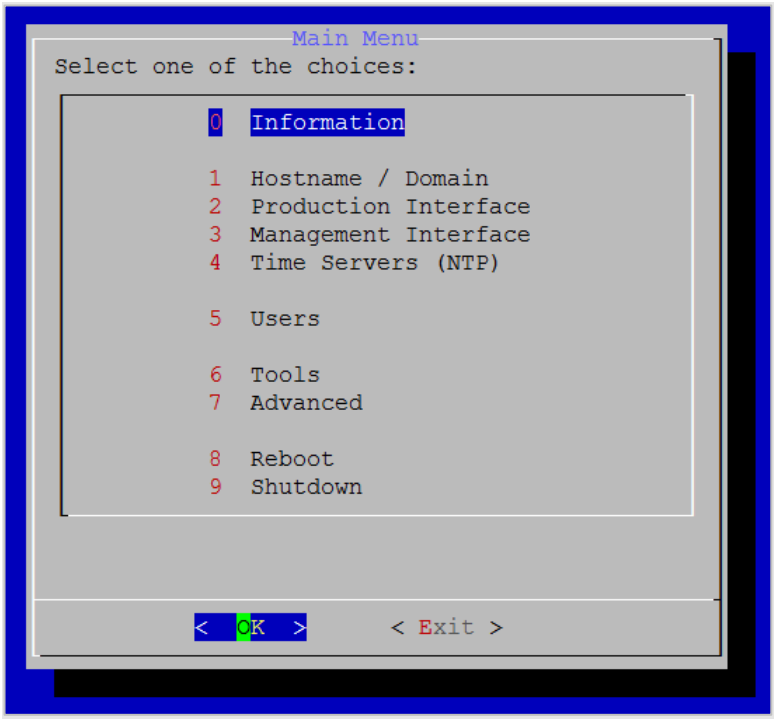


7. Enter **0** to select the List Api Users option and the press the **Enter** key to select **OK**. The *User Active Information* window displays the current user(s).
8. Press the **Enter** key to select **OK**.

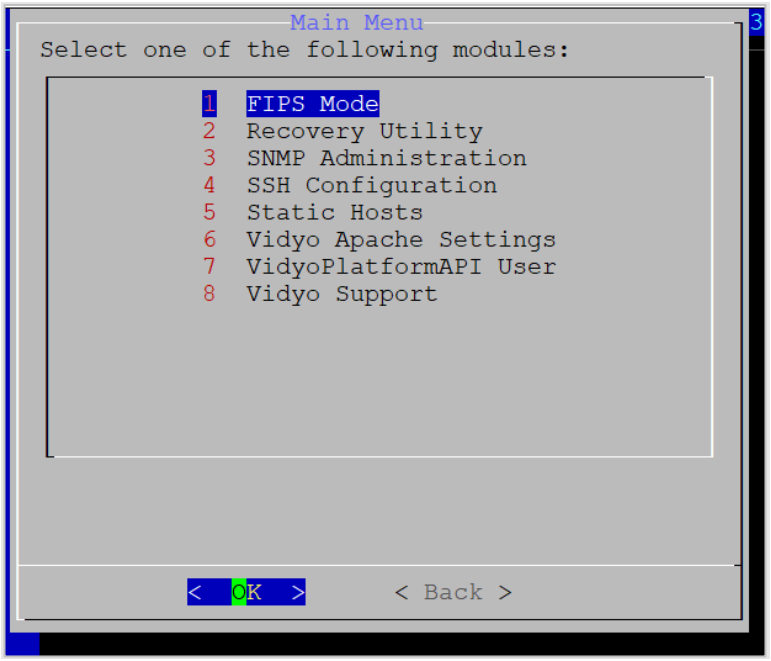
Add and remove users

To add and remove API users:

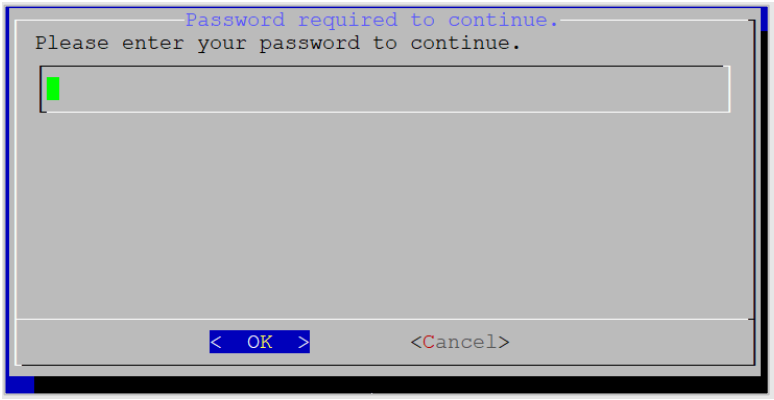
1. Log in to the System Console. The Main Menu displays.



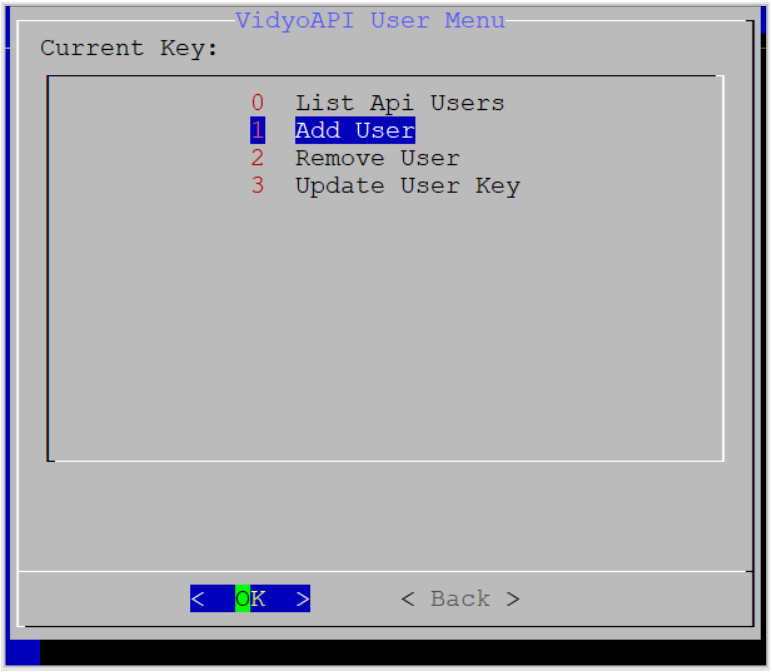
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



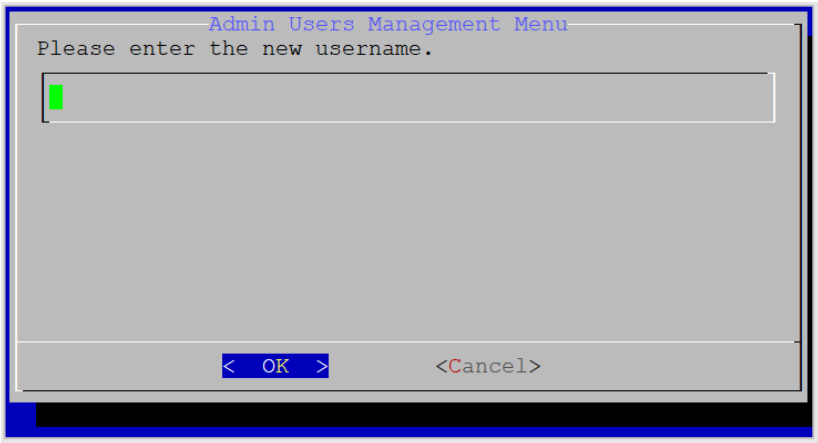
4. Enter **7** to select the VidyoPlatformAPI User option.
5. Press the **Enter** key to select **OK**. The *Password required to continue* window displays.



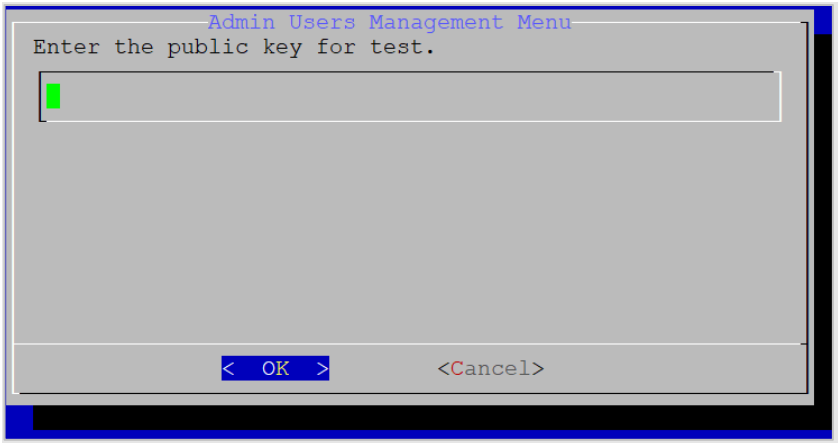
6. Enter your password and then press the **Enter** key to select **OK**. The *VidyoAPI User Menu* window displays.



7. Enter **1** to select the Add User option, and the press the **Enter** key to select **OK**. The *Admin Users Management Menu* window displays this message, “Please enter the new username”.



8. Enter a username and then press the **Enter** key to select **OK**. The *Admin Users Management Menu* window displays this message, “Enter the public key for test.”



9. Enter a public key for a text and then press the **Enter** key to select **OK**. The Message window displays this message, “User has been added”.
10. Press the **Enter** key to select **OK** and then the Message window confirms the user was added.

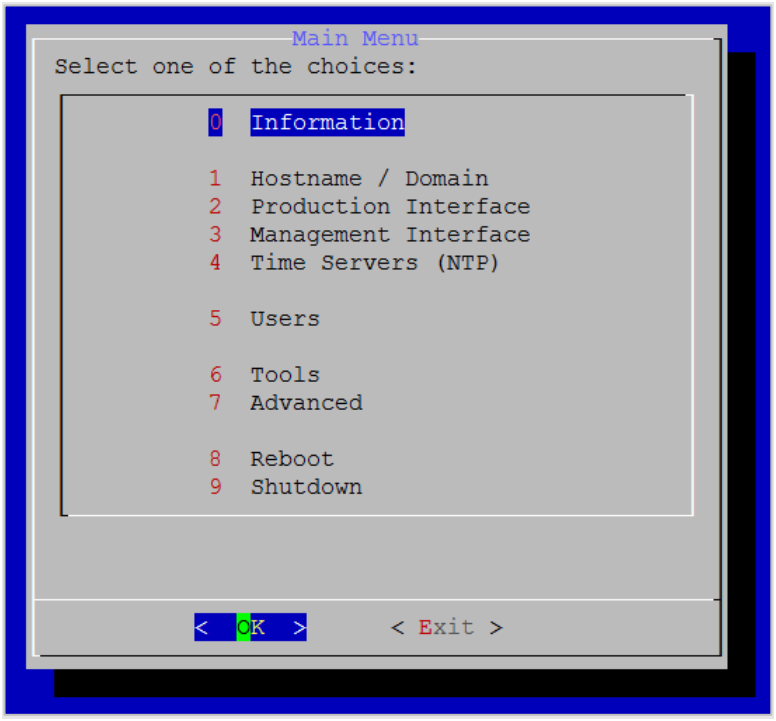
Note

To remove a user, follow the same steps above, except select **2** to Remove User. Then, choose the user to remove and the press **Enter** key to select **OK**. When the Confirm window displays this message, “Remove Api user “test”, Are you sure?”, then press the **Enter** key to select **Yes**. The system will then display a message that the user was successfully removed.

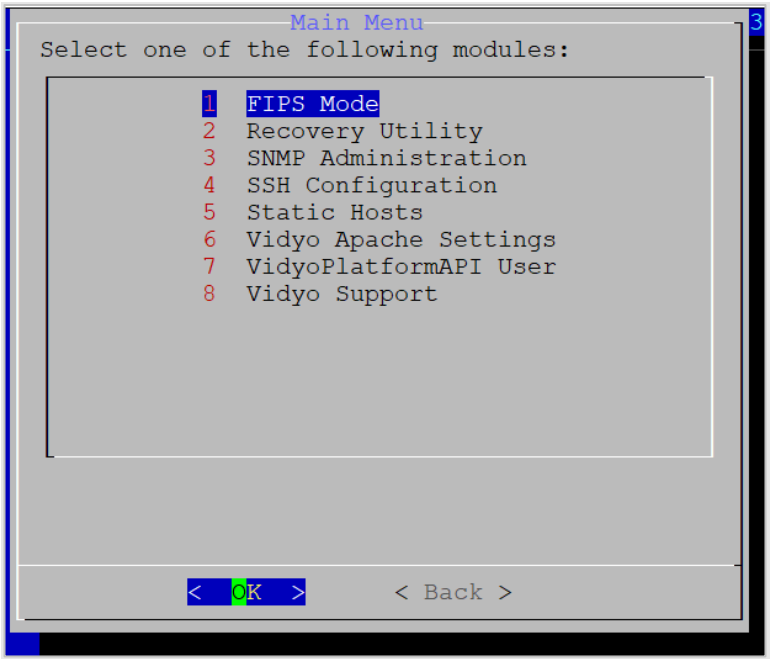
Update user key

To update user key:

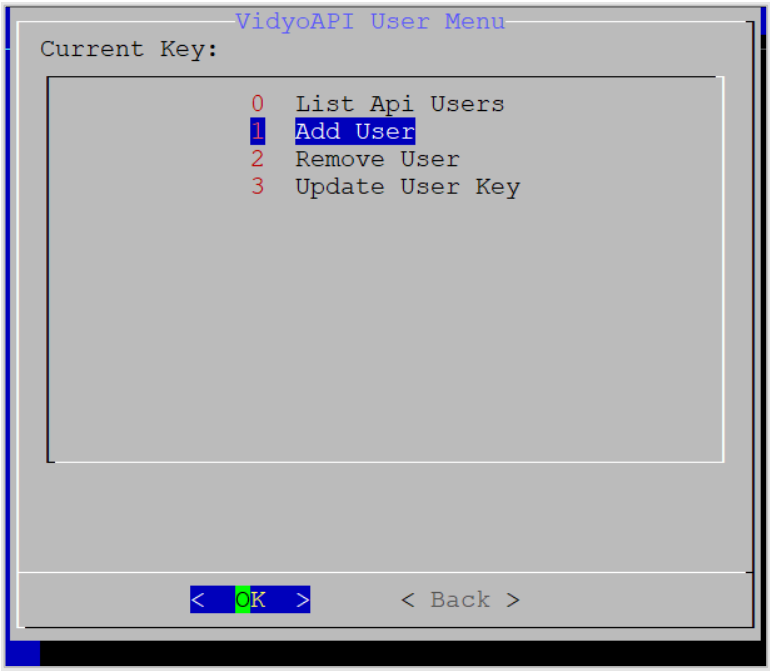
1. Log in to the System Console. The Main Menu displays.



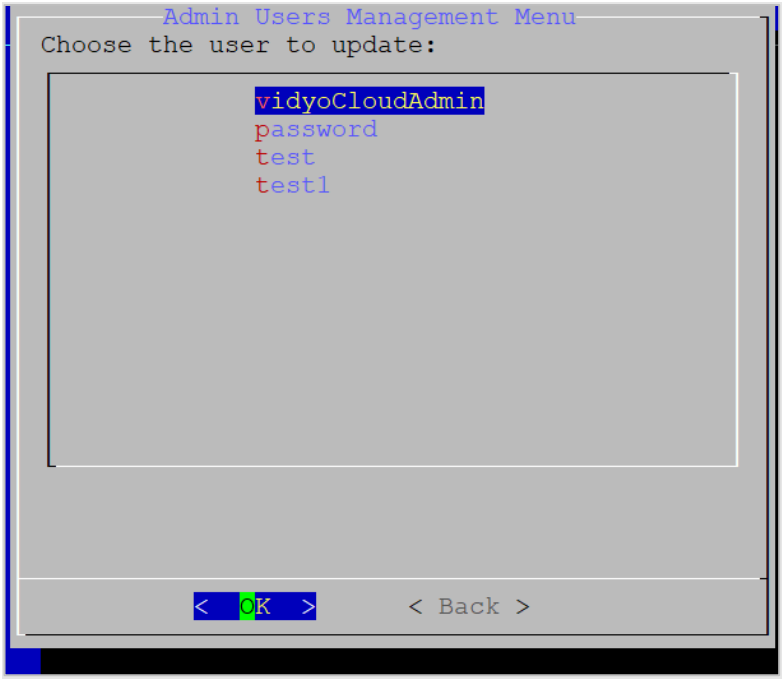
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



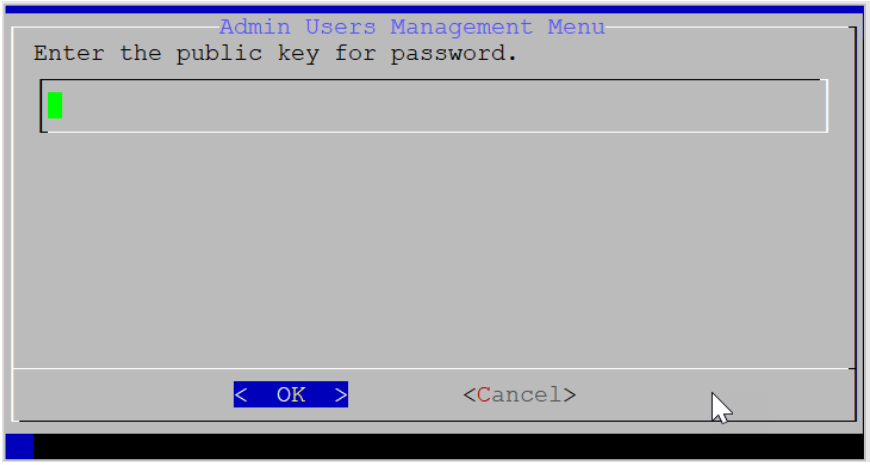
4. Enter **7** to select the VidyoPlatformAPI User option.
5. Press the **Enter** key to select **OK**. The *VidyoAPI User Menu* displays.



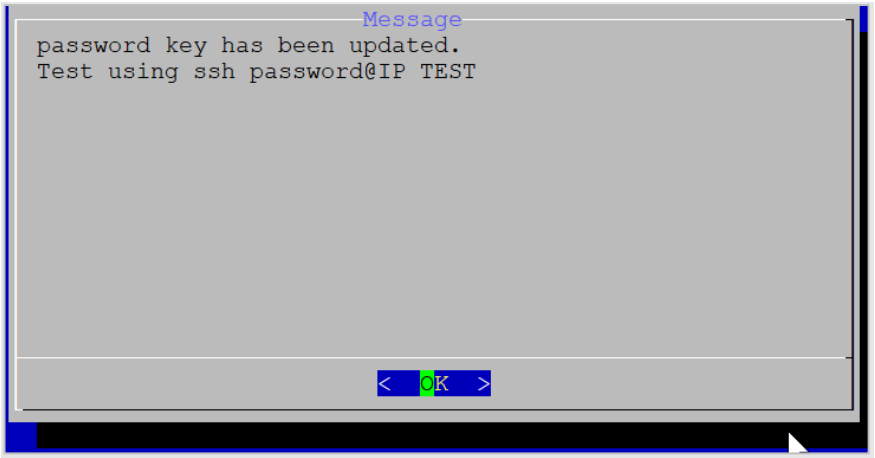
6. Enter **3** to select the Update User Key option, and then press the **Enter** key to select **OK**. The *Admin Users Management Menu* window displays.



7. Choose the user to update in the list and then press the **Enter** key to select **OK**. The *Admin Users Management Menu* window displays.



8. Enter the public key for password and then press the **Enter** key to select **OK**. The *Message* window displays the updated password key.



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

Configure remote Vidyo Support access

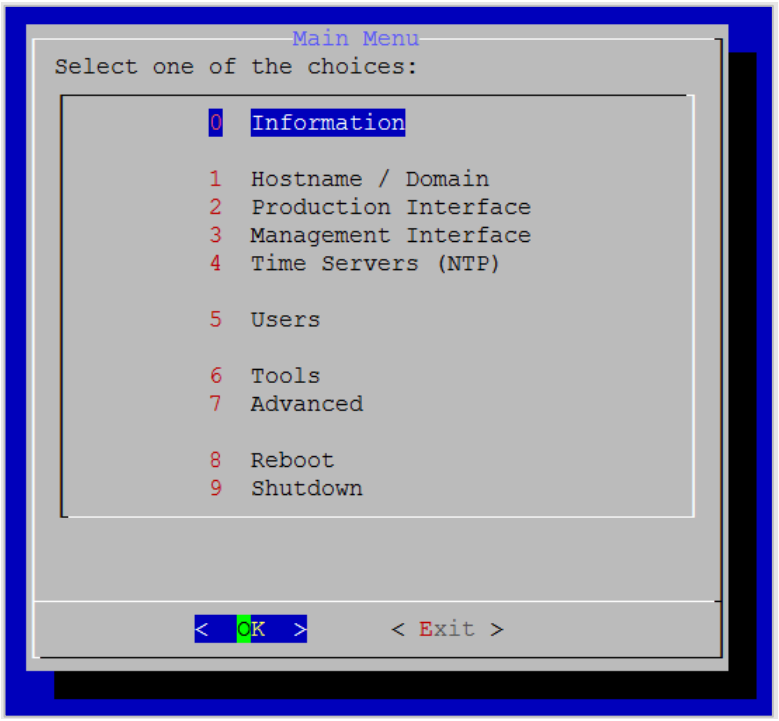
This section describes how to generate a one-time encrypted password that enables the Vidyo Customer Support team to remotely access your VidyoReplay system in a secure manner. The encrypted password that is generated expires at midnight UTC the day after it is generated.

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

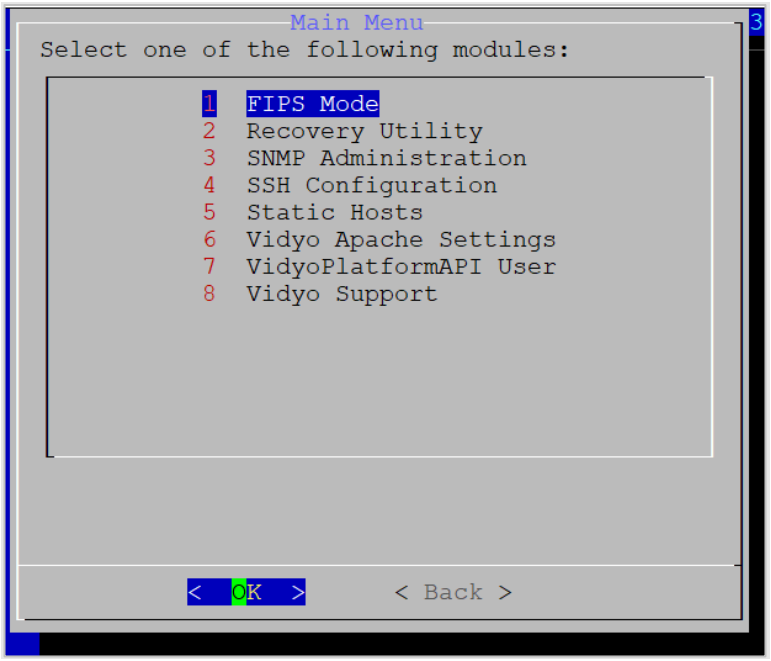
Enable remote Vidyo Support access

To enable remote Vidyo Support access:

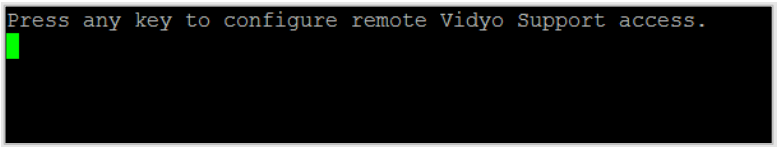
1. Log in to the System Console. The Main Menu displays.



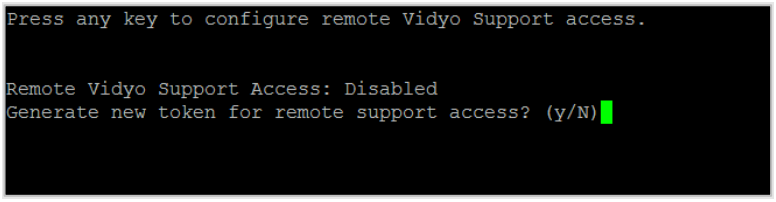
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



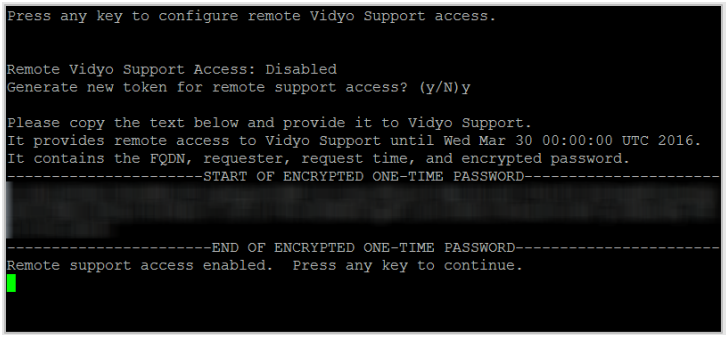
4. Enter **8** to select the Vidyo Support option.
5. Press the **Enter** key to select **OK**. The following message displays:



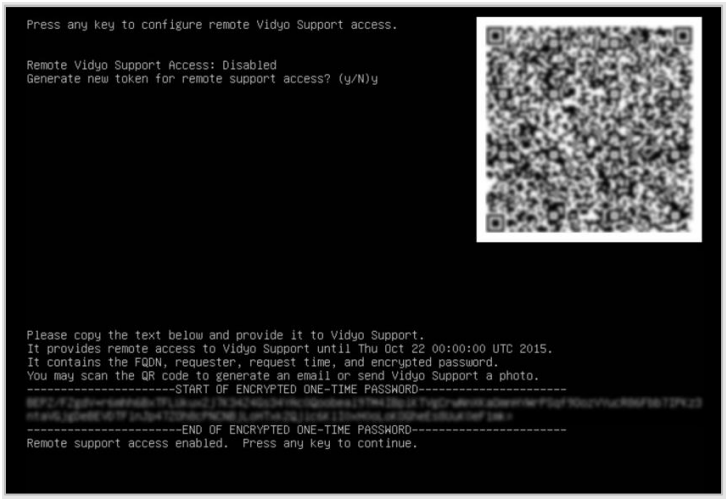
6. Press any key on your keyboard.
7. Enter **y** to generate a new token for remote support access.



8. Press the **Enter** key.
   - If you are accessing the System Console via SSH, a one-time encrypted password is generated as shown:



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



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.

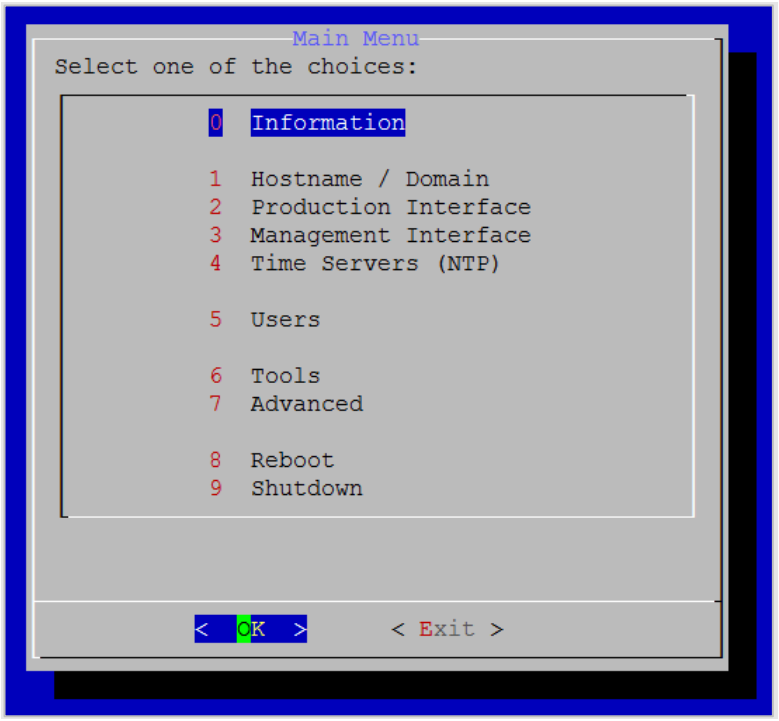
> **Note**
>
> The password that is generated expires at midnight UTC the day after it is generated.

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

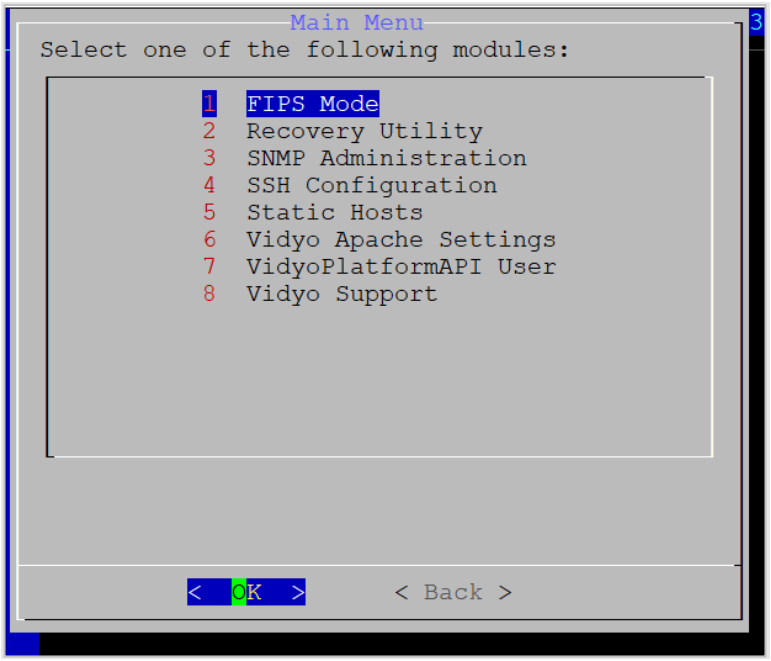
Disable remote Vidyo Support access

To disable remote Vidyo Support access:

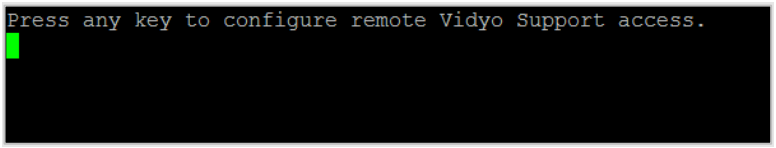
1. Log in to the System Console. The Main Menu displays.



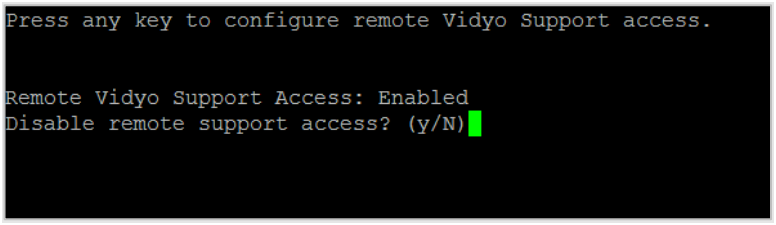
2. Enter **7** to select the Advanced option.
3. Press the **Enter** key to select **OK**. The Main Menu for the Advanced configuration displays.



4. Enter **8** to select the Vidyo Support option.
5. Press the **Enter** key to select **OK**. The following message displays:



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

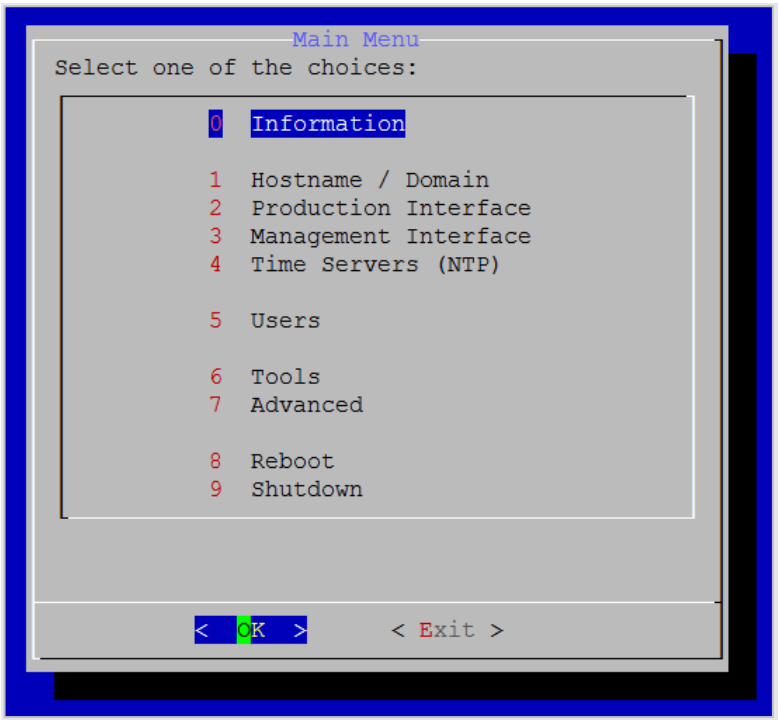


8. Press the **Enter** key. A message indicates that remote access is disabled.
9. Press any key to return to the Advanced Main Menu.

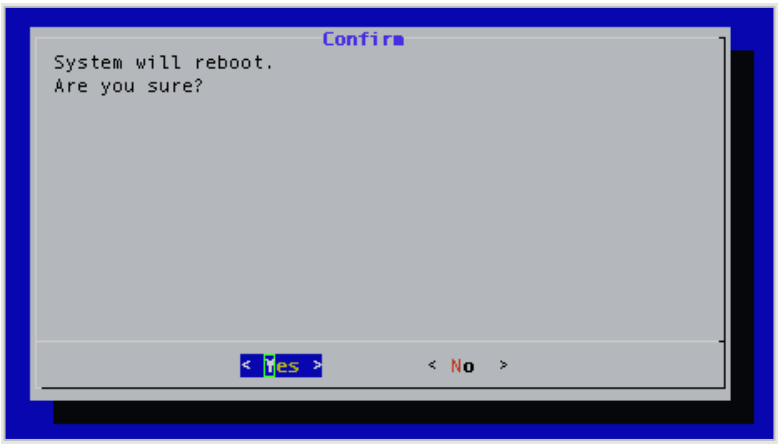
Reboot the System Console

To reboot the System Console:

1. Log in to the System Console. The Main Menu displays.



2. Enter **8** to select the Reboot option.
3. Press the **Enter** key to select **OK**. The *Confirm* window displays.

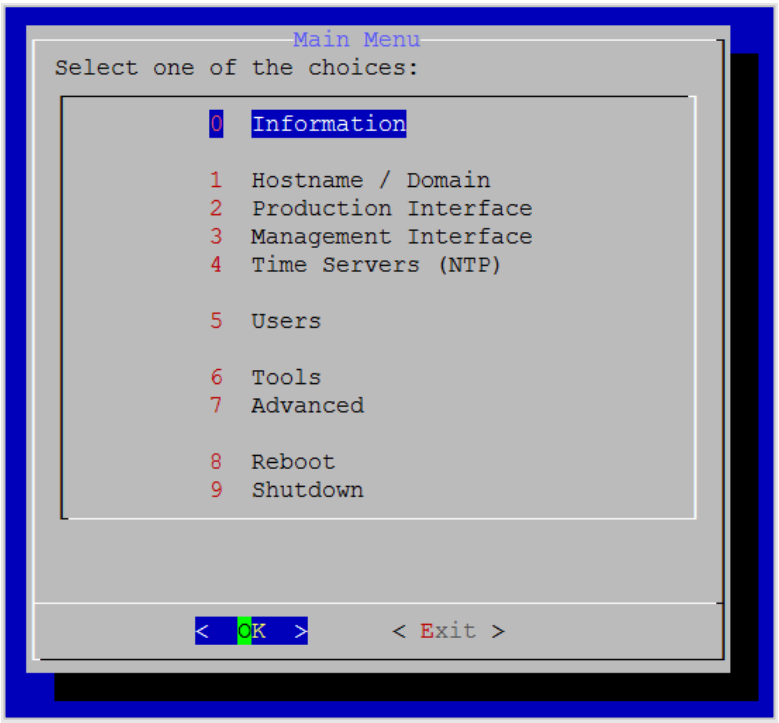


4. Press the **Enter** key to select **Yes**.

Shut down the System Console

To shut down the System Console:

1. Log in to the System Console. The Main Menu displays.



2. Enter **9** to select the Shutdown option.
3. Press the **Enter** key to select **OK**. The *Confirm* window displays

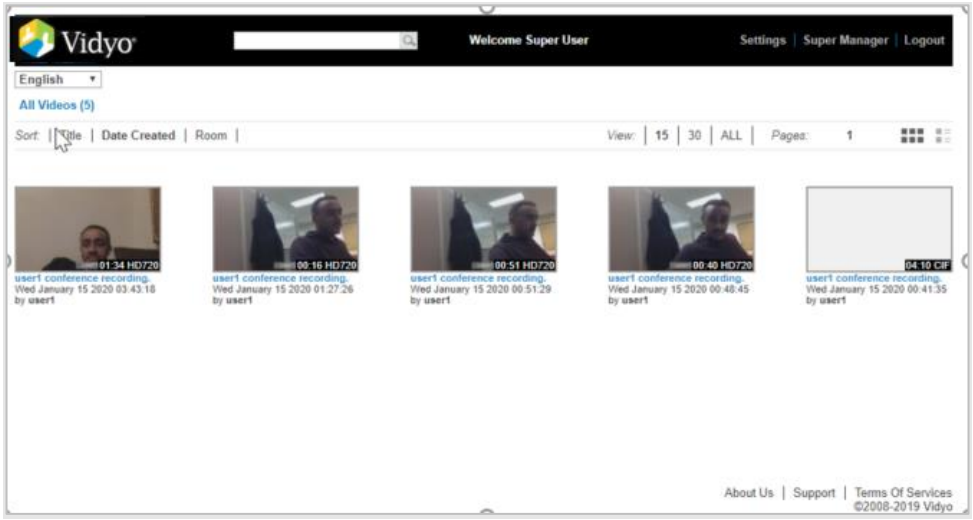
4. Press the **Enter** key to select **Yes**.

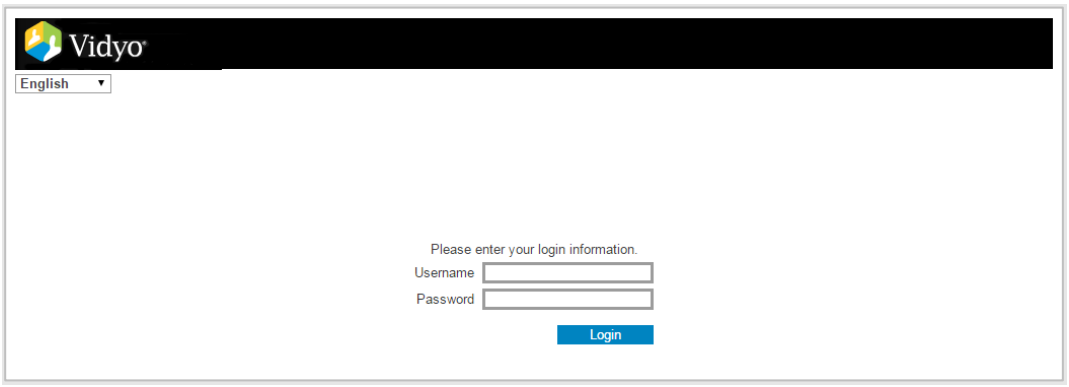
Log in to VidyoReplay

Now that you have connected your VidyoReplay server to the network and added both your VidyoReplay Recorder and your VidyoReplay on your VidyoPortal, you must log in as the Super Admin and configure your VidyoReplay to ensure that it can function within your VidyoConferencing system.

To log in to your VidyoReplay:

1. Enter the URL or IP address for the VidyoReplay in the address bar of a web browser. The URL of your VidyoReplay is typically a domain name: `[vidyoreplay.example.com]`. The VidyoReplay Public Library displays.



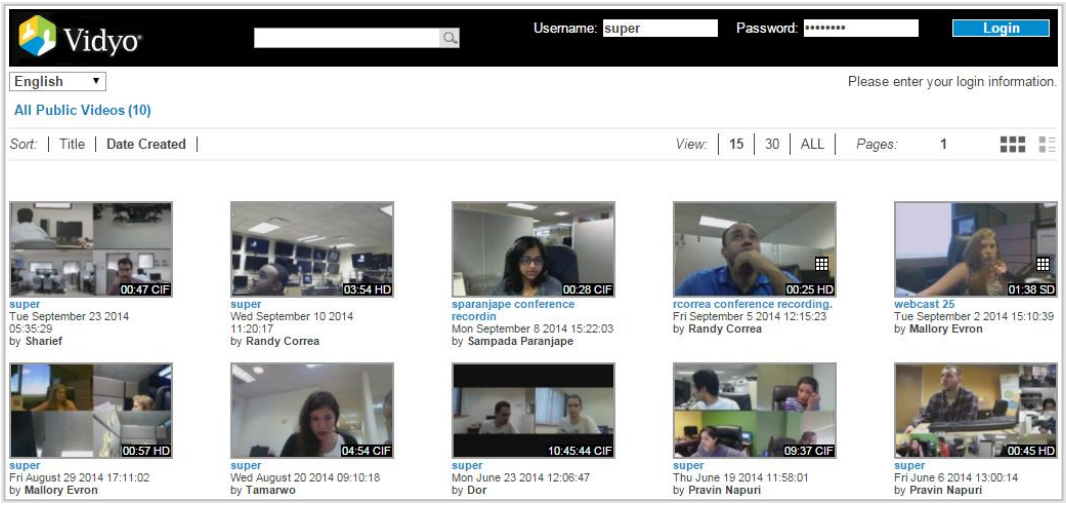
> **Note**
>
> Only recordings with Public selected as the **Who can watch** option display on this screen. Otherwise a blank login screen displays. See 7. VidyoReplay Library and Manager access levels and Add or edit recording properties.
>
> 
>

2. Log in to the VidyoReplay using the default Super account:

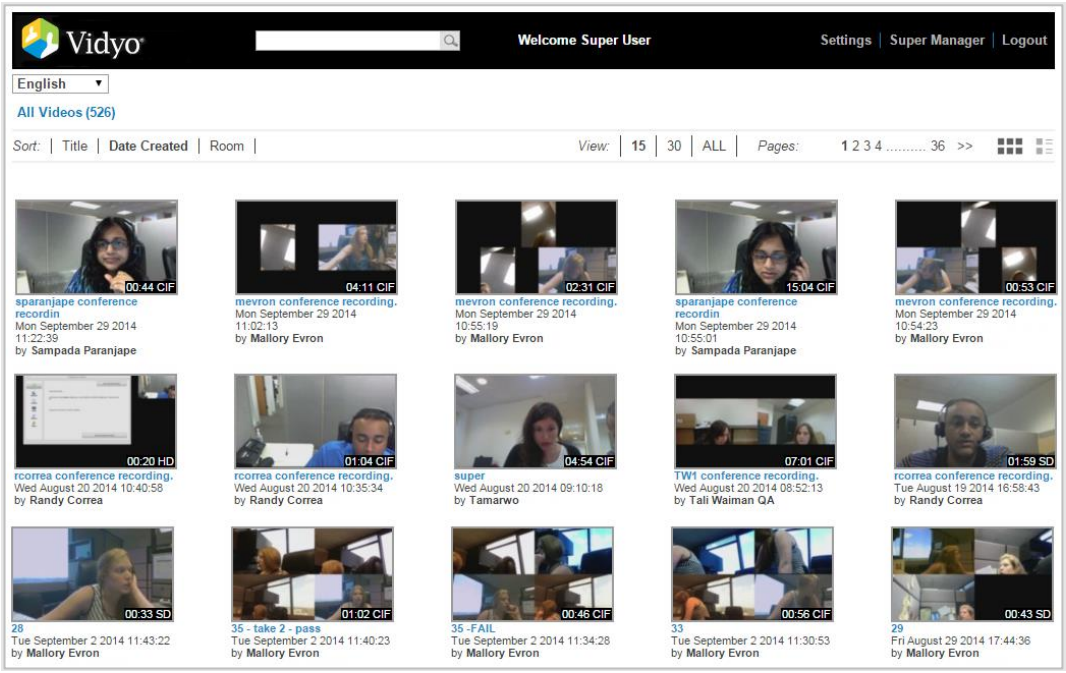
   User Name: `super`

   Password: `password` (case sensitive)

   > **Note**
   >
   > You should change this password from the default. See Configure the general settings.



3. Click **Login**. Your VidyoReplay Personal Library displays.



> **Note**
>
> Recordings or webcasts display in your VidyoReplay Library based on Access Levels. See 7. VidyoReplay Library and Manager access levels.

Set the language for the Super Admin interface

The VidyoReplay's Super Admin interface is available in these 15 languages:

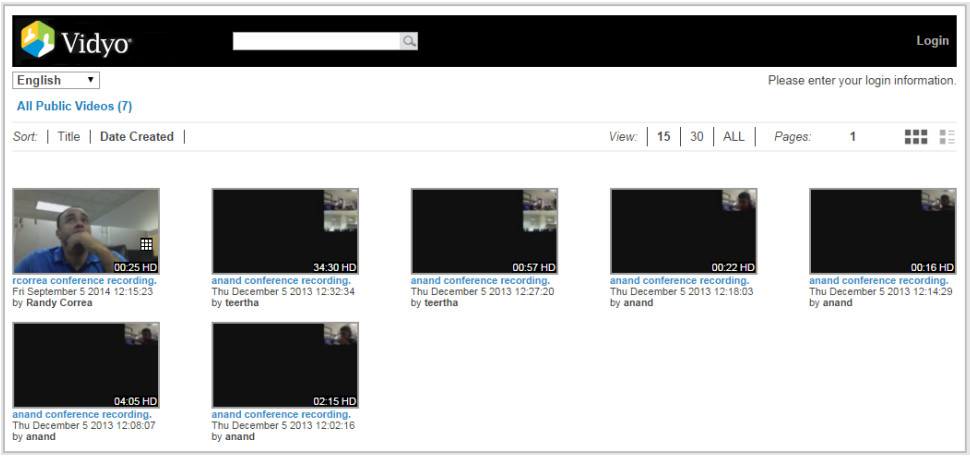
- Chinese (Simplified)
- Chinese (Traditional)
- English
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish
- Thai
- Turkish

Set the language of your Super Admin Pages using the drop-down on the upper left corner of the Super Admin Login page (before or after logging into the system).

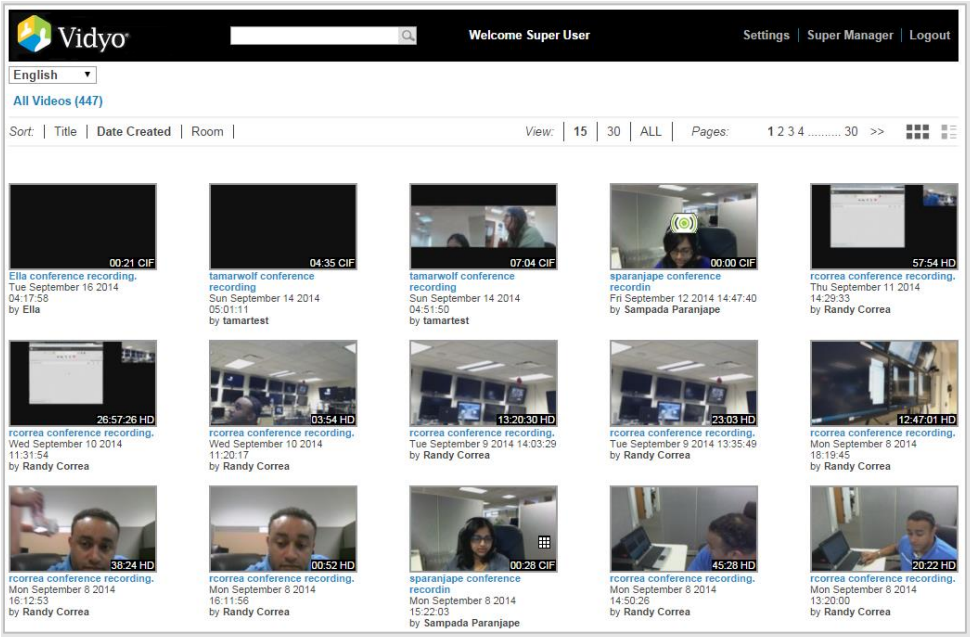
> **Note**
> Interfaces are immediately modified after selecting your preferred language or color scheme using the drop-downs.

To set your preferred language using the drop-down on the upper left corner of the VidyoReplay:

1. Select your desired language using the language drop-down on the upper-left corner of the VidyoReplay in any of the following states:
   - Prior to logging in to VidyoReplay.



- After logging in to VidyoReplay.



5. Configure system settings as the Super Admin

This section describes how to configure the VidyoReplay system settings. The first procedure shows you how to access these settings.

When you make changes to the system settings as described in this chapter and then click **Save** or **Save & Apply**, the VidyoReplay server reboots.

> Note
>
> After you have configured your system, you should provide users with a link to the VidyoReplay along with their username, and password. You can also provide them with information about creating, viewing, and managing recordings and webcasts. See 8. View and manage recordings and webcasts.

Access system settings

To access VidyoReplay settings:

1. Log in to the VidyoReplay using the default Super account. See Log in to VidyoReplay.
2. Click the **Settings** link. The VidyoReplay system settings display.

   Tabs are shown along the top, which include the following: *General*, *Cluster*, *Recorder*, *Security*, *Customization*, *Cleanup*, *Maintenance,* and *Users*. Settings are made on these tabs to configure different areas of your system. The following sections cover these tabs in more detail.

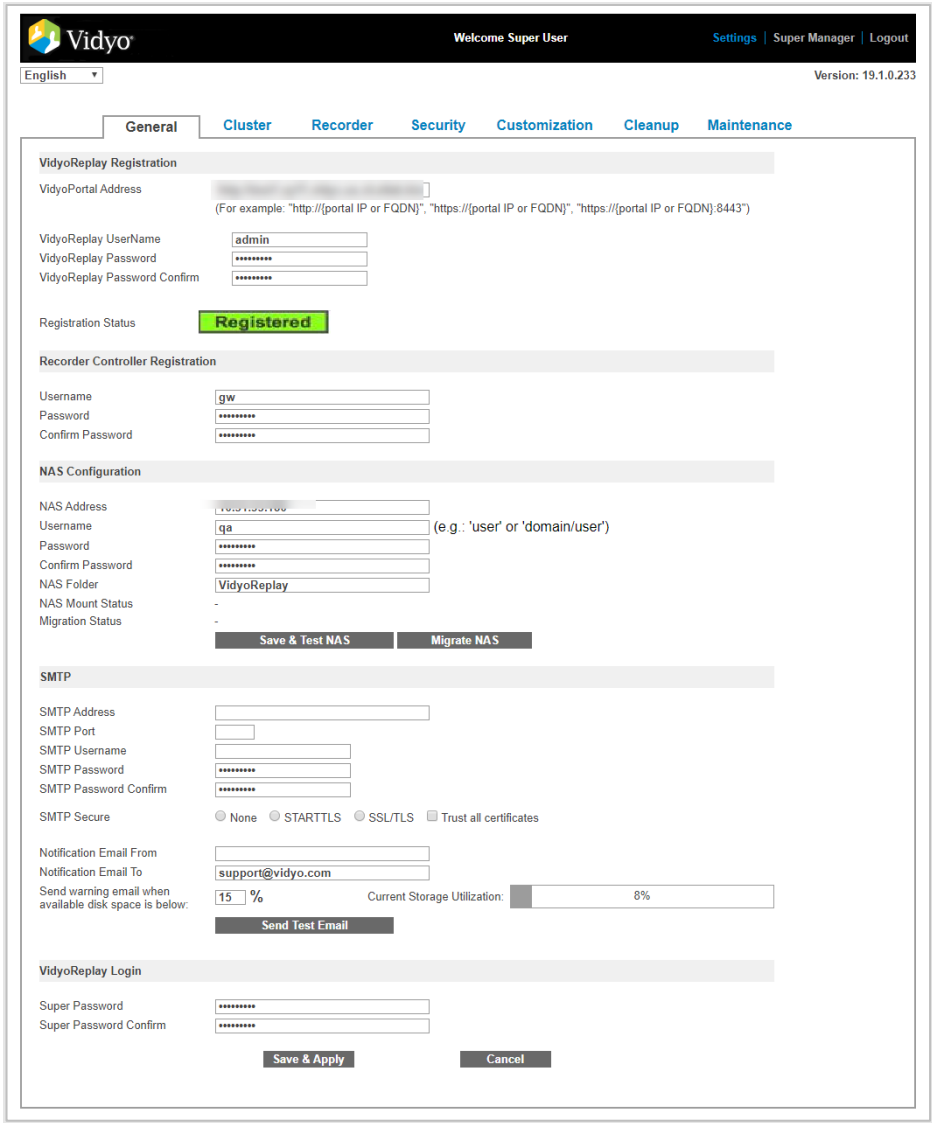
> Note
>
> The tabs display or are hidden based on the server (Standalone versus Active Controller, Standby Controller, or Recorder or in a VidyoReplay cluster) from which you are accessing settings. Notes are included on these topics if the settings vary.

Configure the general settings

In the VidyoReplay version 19.1.0 or later, you can migrate your local recordings from this General Settings tab.

To configure the general settings:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *General* tab.



4. In the **VidyoPortal Address** field, enter the IP or FQDN address (fully qualified domain name) of your VidyoPortal. The library needs this address so it can connect to its associated VidyoPortal.

> **Note**
>
> You must add your VidyoReplay and VidyoReplay recorder as components on your VidyoPortal. See 3. Configuration procedure.
>
> When clustering VidyoReplay servers, your username and password must be the same on each VidyoReplay Recorder and VidyoReplay in your system. See Configure the general settings.

5. Change the **VidyoReplay UserName** and **VidyoReplay Password** in their respective fields to match the account you set up for the VidyoReplay on the VidyoPortal, and then verify the password.

The **Registration Status Display** field shows “Registered” if your VidyoReplay is able to communicate with your VidyoPortal.

> Note
>
> The **Registered** field is read-only and verifies that the VidyoPortal and VidyoReplay have authenticated to each other successfully.

6. In the Recorder Controller Registration section, enter the username, password, and confirm the password of your VidyoReplay Controller.
7. In the NAS Configuration section, enter the following:
   a. In the NAS Address, enter the IP address of your NAS.
   b. Enter the username, password, and confirm the password of your NAS.
   c. Enter the NAS folder name to use on your NAS.
   d. View the NAS Mount Status indicators to see the current state of your VidyoReplay server’s NAS configuration.
   e. View the Migration Status in the Migration Status field.
   f. Click the **Save & Test NAS** button to migrate your local recordings.
   g. Click the **Migrate NAS button** to migrate your local recordings. You no longer need to use the Vidyo Console to migrate local recordings. After you click this button, check that the statuses update correctly in the NAS Mount Status and Migrations Status fields.

      NAS Mount Status indicators include the following:

      - No error (green indicator)
      - No route to host: Network issue or NAS device might be down (red indicator)
      - Connection refused: NAS service might not be running (red indicator)
      - Permission denied: NAS username/password might be incorrect (red indicator)
      - No such device or address: NAS folder might not be available (red indicator)
      - Permission denied: NAS read error (red indicator)
      - Permission denied: NAS write error (red indicator)
      - Unknown error
      - Mount in progress

Note

- The Alarm column of the Components Table in your VidyoPortal alerts you if your VidyoReplay is in Maintenance mode, shows any NAS error statuses (if NAS is used), and indicates if your database replication is OFF. For more information, refer to *Use the Components table* in the *VidyoPortal and VidyoRouter Administrator Guide*.
- The SMB and CIFS protocols are supported for mounting your NAS.
- Your NAS username must have both read and write access to the NAS folder.
- A standalone VidyoReplay handles all recordings and playbacks/webcasts internally; however, you can connect it to NAS, if desired.
- To use a cluster configuration, your VidyoReplays must be connected to a NAS. See NAS guidelines for your VidyoReplay.

8. In the SMTP section, enter the following:
   - In the **SMTP Address** field, enter the IP address of your SMTP server.
   - In the **SMTP Port** field, enter your SMTP port.
   - Enter the username, password, and confirm the password of your SMTP server.
   - In the SMTP Secure options, select from **None**, **STARTTLS**, and **SSL/TLS**.
   - Select the **Trust all certificates** checkbox, if desired.
   - In the **Notification Email From** and **Notification Email To** fields, enter email addresses.

     The email address you provide here is notified in the event of a failover.

     VidyoReplay also sends notifications to this email address if your NAS unmounts. This allows you to get alerted quickly, thereby preventing issues that could occur if your NAS unmounts without your knowledge.

Note

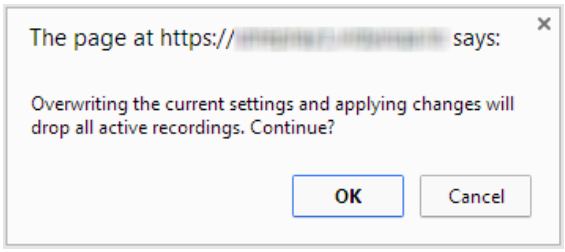
- The notification email address is only configurable on Controller 1 and Controller 2 nodes and not from the VidyoReplay Recorder.
- The system needs a “From” address because many email systems block or send to the spam folder all emails that don’t have “From” addresses. The “To” address is the email address of the Admin or other IT person who receives notifications from the library. (The two addresses may be identical.)

   - In the **Send warning email when available disk space is below** field, enter a percentage.
   - The Current Storage Utilization percentage bar shows how much space is being utilized on your VidyoReplay.
   - Click **Send Test Email** if you want to make sure the email is configured correctly.

9. If you want to change the VidyoReplay Super Admin's password, you can change it in the **Super Password** field and confirm it in the **Super Password Confirm** field.

10. Click **Save & Apply**.

    When you click **Save & Apply**, a dialog box informs you that overwriting the settings and applying changes drops all active recordings on your server.



    When you click **OK**, the VidyoReplay server reboots.

NAS guidelines for your VidyoReplay

This section provides some guidelines for your NAS to work with your clustered VidyoReplay configuration.

> Note
>
> The SMB and CIFS protocols are supported for mounting your NAS. A standalone VidyoReplay handles all recordings and playbacks/webcasts internally; however, you can connect it to NAS, if desired.
>
> Your NAS username must have both read and write access to the NAS folder. To use the cluster configuration, your VidyoReplays must be connected to NAS. See VidyoReplay clusters.
>
> You can always confirm the status of your NAS by viewing the NAS Status indicators on the *General* tab. See Configure the general settings.

Configure VidyoReplay to use your NAS

After properly setting up your NAS, the VidyoReplays in your cluster must now be configured to use it.

Always confirm your VidyoReplay as being correctly configured to use your NAS by viewing the NAS Status on the *General* tab. See Configure the general settings.

To configure VidyoReplay to use your NAS:

1. Configure your secondary network interface (ETH1) for your NAS.
2. Configure your address, username, password, NAS folder in the *General* tab. See Configure the general settings.
3. Configure your VidyoReplay servers in to a cluster configuration. See VidyoReplay clusters.
4. View the NAS Status in the *General* tab. See Configure the general settings.
5. You may now move any of your local `.mp4` or `.flv` files to your NAS, if desired.

VidyoReplay clusters

A VidyoReplay can be configured as a single Standalone VidyoReplay (a single component acting as both Controller and VidyoReplay Recorder) or as a cluster setup with an Active Controller, Standby Controller, and VidyoReplay Recorder.

This section explains various VidyoReplay cluster configurations used to support as many recordings required prior to going through the *Cluster* tab in the VidyoReplay Admin Pages. Think of a VidyoReplay cluster as a large, single VidyoReplay system.

For information about configuring clusters, see Configure clusters.

> **Note**
>
> With Clustering enabled on your VidyoReplay, 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 VidyoReplay.

Clustering benefits

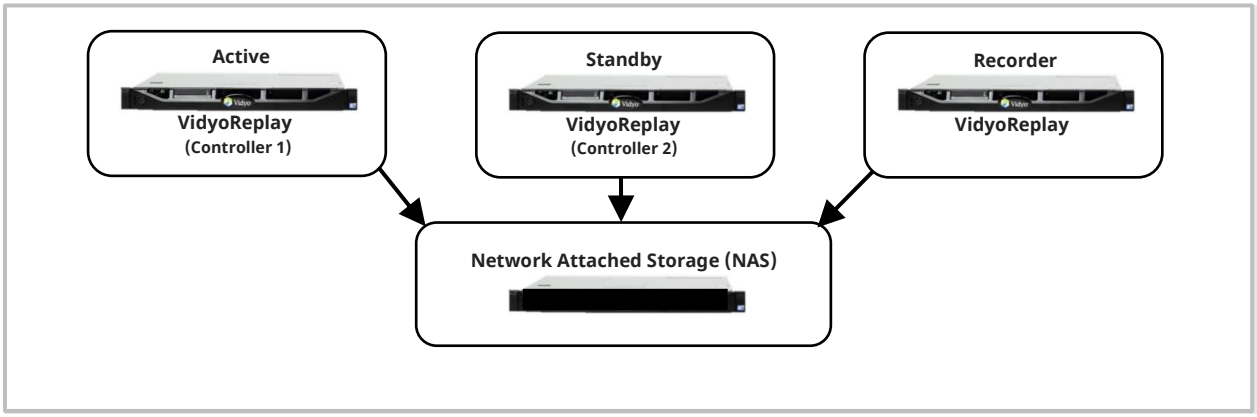
VidyoReplay clustering enables you to scale your VidyoReplay capacity to a higher volume of simultaneous recordings by deploying multiple VidyoReplays per VidyoPortal and per tenant. By clustering, you are enabling the multiple VidyoReplays to balance the recording load, thereby increasing your scalability. Clustering also provides the same benefit when playing back recordings from your NAS via the shared controller IP address on your active controller.

For more information about the Shared Controller IP Address, see Configure clusters.

For more information about configuring your NAS, see NAS guidelines for your VidyoReplay.

When creating clusters, you need to assign a Controller 1 role to one of your VidyoReplays and designate the other VidyoReplays as a Controller 2 and/or Recorder. Any VidyoReplay can be a Controller 1, Controller 2, or VidyoReplay Recorder in your VidyoReplay cluster.

When your VidyoReplay cluster is properly implemented, Controller 1, Controller 2, and the VidyoReplay Node assume statues of Active, Standby, and additional Recorder to balance the recording and playback load.



> **Note**
>
> The VidyoReplay Recorder is not required in the diagram.
>
> A NAS must be used as your storage when clustering VidyoReplays. For more information about NAS, see NAS guidelines for your VidyoReplay.
>
> Also when clustering VidyoReplay servers, your username and password must be the same on each VidyoReplay Recorder and VidyoReplay in your system. See Configure the general settings.

Configure clusters

The *Cluster* tab provides options to configure your VidyoReplay server as a Standalone, Controller 1, Controller 2, or Recorder Node. The following sections cover these configurations in more detail.

Each VidyoReplay server in your cluster must align to the following requirements:

- A public IP addresses must be used. This means none of the VidyoReplay servers in your cluster can be NATed.
- If they are behind a Firewall, it must permit Legacy ports for each VidyoReplay server in your Cluster. This is usually configured as a set range of IP addresses in your Firewall.
- Each VidyoReplay server in your cluster must all be physically located in the same data center. The Clustering functionality does not support VidyoReplays located in separate data centers.
- Each VidyoReplay 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. See Configure Controller 1, Configure Controller 2, and Configure your Recorder.

> Note
>
> Cluster configurations are only supported using IPv4. IPv6 clustering is not currently supported.
>
> VidyoReplay 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 VidyoReplay Controller (Controller 1 or Controller 2) takes possession of the shared IP address.

The *Cluster Configuration* screen allows you to specifically designate your VidyoReplays as a Standalone, Controller 1, Controller 2, or Recorder Node. You can also provide additional data for each component depending on the VidyoReplay role.

As a reminder, when your VidyoReplay cluster is properly implemented, Controller 1, Controller 2, and VidyoReplay Node assume statuses of Active, Standby, and additional Recorder/s to balance the recording and playback load.

When the Active Controller is configured properly, the following takes place in the event of a failover:

1. Recordings being recorded or played are stopped as the Standby Controller takes the IP address of the Active Controller.
2. The new Active Controller sends out the email notification alert to the Notification Email From and To address provided in the *General* tab. See Configure the general settings.
3. The course of action varies at this point based on whether the original Active Controller that failed is repairable and can be returned to your system setup.

Clustering procedure

In a VidyoReplay cluster, the volume of incoming recordings is load balanced among each of your servers in a logical manner. When you change the status of a VidyoReplay in your cluster, the system automatically adjusts the statues of the other VidyoReplays to keep your system intact.

> Note
>
> You can perform upgrades, cleanups, and configuration changes to your specific nodes in your VidyoReplay cluster by setting the server status to Maintenance and administering your machine.
>
> The Alarm column of the Components Table in your VidyoPortal alerts you if your VidyoReplay is in Maintenance mode, shows any NAS error statuses (if NAS is used), and indicates if your database replication is OFF.

For more information, refer to *Use the Components table* in the *VidyoPortal and VidyoRouter Administrator Guide*.

> Note
>
> In the VidyoReplay 19.1.0 or later release, the High Availability subtab is no longer available; however, you can invoke the “force standby mode” by rebooting the server. Then, the standby controller will take over the virtual IP.

Perform the steps from the following sections to create your VidyoReplay Cluster.

To create a VidyoReplay cluster:

1. Make sure you’ve assigned a hostname to Controller 1. Reboot your machine after assigning the hostname. See Set the hostname and the domain.
2. Configure Controller 1 to use your NAS. See Configure VidyoReplay to use your NAS.
3. Access Controller 2 and assign a different hostname to it. Reboot your machine after assigning the hostname.
4. Configure Controller 2 to use your NAS. See Configure VidyoReplay to use your NAS.
5. Access your Recorder and assign a different hostname to it. Reboot your machine after assigning the hostname.
6. Configure your Recorder to use your NAS. See Configure VidyoReplay to use your NAS.
7. Perform the cluster configuration settings on Controller 1 and then reboot. See Configure Controller 1.

   > Note
   >
   > You must add your VidyoReplay and VidyoReplay recorder as components on your VidyoPortal. See 3. Configuration procedure.
   >
   > When clustering VidyoReplay servers, your username and password must be the same on each VidyoReplay Recorder and VidyoReplay in your system. See Configure the general settings

8. Perform the cluster configuration settings on Controller 2. Reboot your machine after the configuration. See Configure Controller 2.

9. Perform the cluster configuration settings on your Recorder. Reboot your machine after the configuration. See Configure your Recorder.

Return a repaired controller to your system setup

The original Active Controller returns to the system setup and is acting as the Standby Controller.

Replace an irreparable controller 1 to your system setup

Vidyo recommends you replace the original Controller 1 role with a Recorder Node role (if you have one in your system setup). The Recorder node is then recognized as a Standby Controller, but is mislabeled as a Recorder.

> Note
>
> If desired, you can easily reconfigure your controllers to bear the correct Controller 1, Controller 2 labeling. However, this is not required and the system is fully functional in this state.

Some people setup VidyoReplay systems with a single Standalone VidyoReplay (a single component acting as both Controller and Recorder). Other clients designate a Controller 1, Controller 2, and Recorder Nodes. You can think of the latter as a large, single VidyoReplay system.

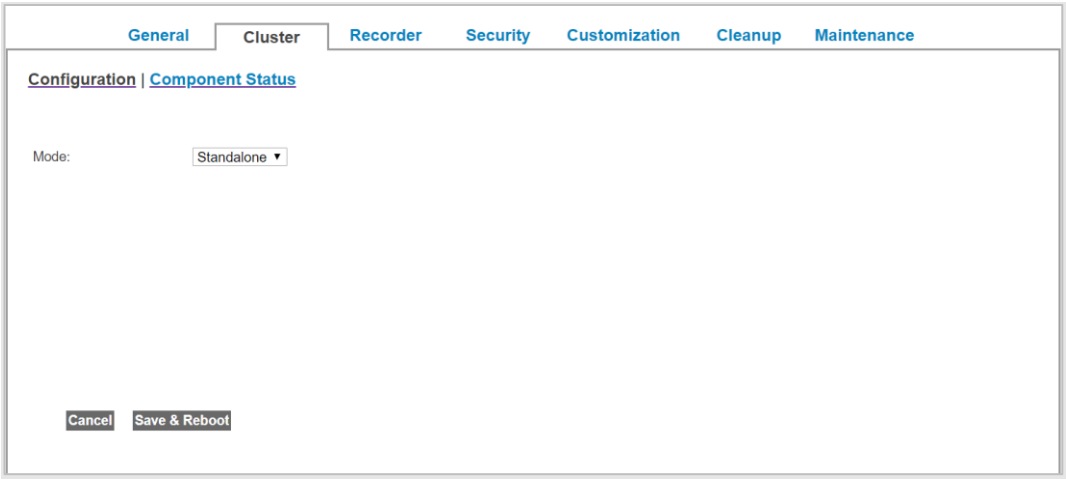
The following sections show you how to configure each VidyoReplay component type using the *Cluster* tab.

Configure your standalone VidyoReplay

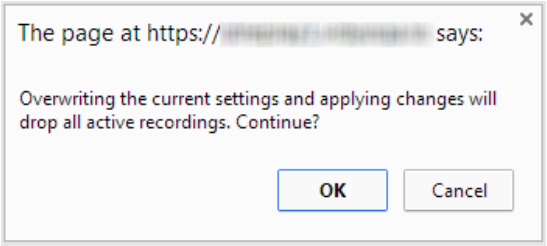
Your server is set as a Standalone VidyoReplay by default. Unless it’s changed, you don’t need to modify the configuration.

To configure your Standalone VidyoReplay:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Cluster* tab.
4. Click the **Configuration** link.
5. Select **Standalone** from the **Mode** drop-down.



6. Click **Save & Reboot**. When you click **Save & Reboot**, a dialog box informs you that overwriting the settings and applying changes drops all active recordings on your server.



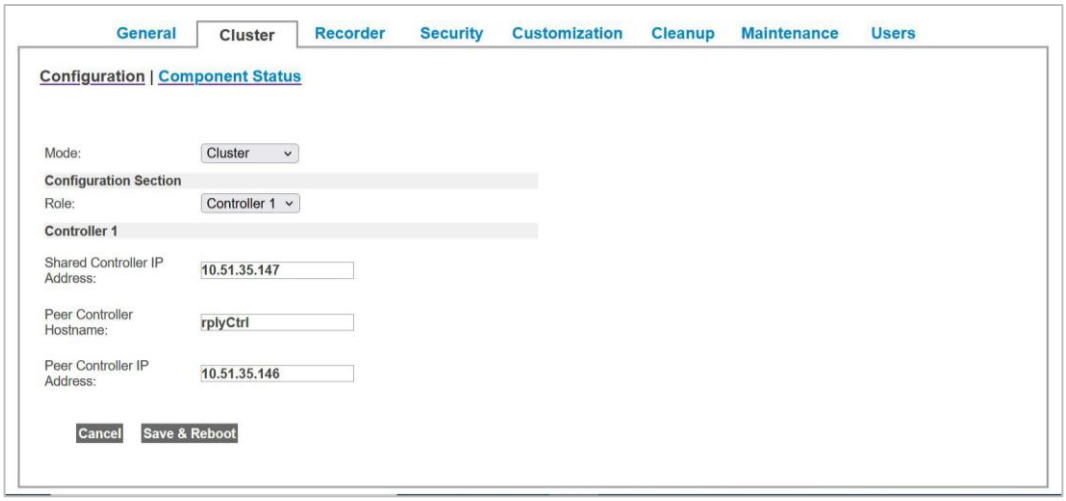
When you click **OK**, the VidyoReplay server reboots.

Configure Controller 1

Before configuring clusters, be sure to review Clustering procedure.

To configure Controller 1:

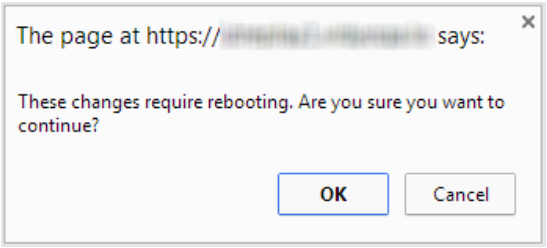
1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Cluster* tab.
4. Click the **Configuration** link.
5. In the **Mode** drop-down, select **Cluster**.
6. In the **Role** drop-down, select **Controller 1**.



7. In the additional fields, configure Controller 1 as follows:
   - Enter a **Shared Controller IP Address**.

     > Note
     >
     > Provide the IP address exactly as it's shown in the System Console and do not provide an FQDN in this field.

   - Enter a **Peer Controller Hostname**.
   - Enter a **Peer Controller IP Address**.
8. Click **Save & Reboot**. When you click **Save & Reboot**, a dialog box informs you that overwriting the settings and applying changes drops all active recordings on your server.



When you click **OK**, the VidyoReplay server reboots.

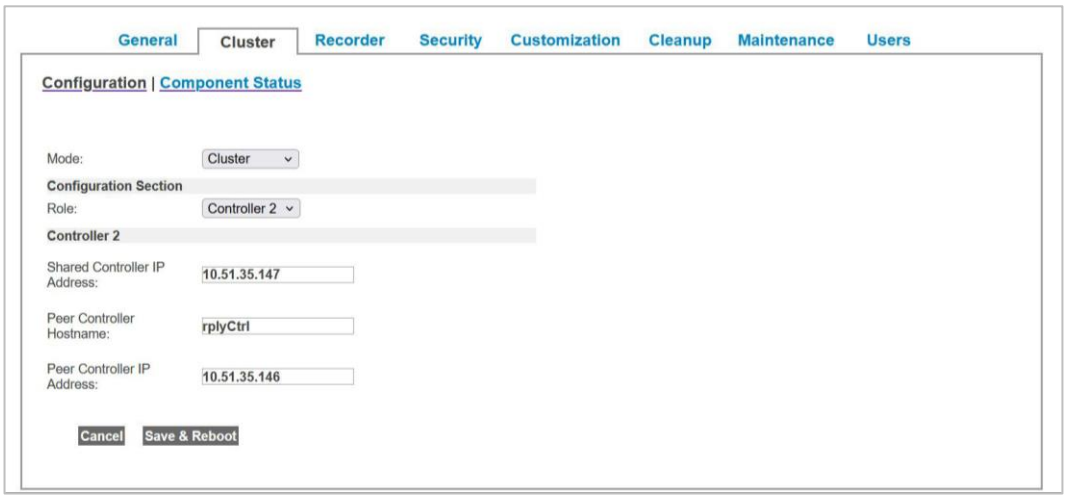
Configure Controller 2

Before configuring clusters, be sure to review Clustering procedure.

To configure Controller 2:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Cluster* tab.
4. Click the **Configuration** link.
5. In the **Mode** drop-down, select **Cluster**.

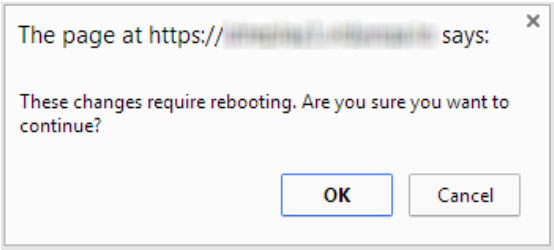
6. In the **Role** drop-down, select **Controller 2**.



7. In the additional fields, configure Controller 2 as follows:
   - Enter a **Shared Controller IP Address**.

     > Note
     >
     > Provide the IP address exactly as it's shown in the System Console and do not provide an FQDN in this field.

   - Enter a **Peer Controller Hostname**.
   - Enter a **Peer Controller IP Address**.
8. Click **Save & Reboot**. When you click **Save & Reboot**, a dialog box informs you that overwriting the settings and applying changes drops all active recordings on your server.



When you click **OK**, the VidyoReplay server reboots.

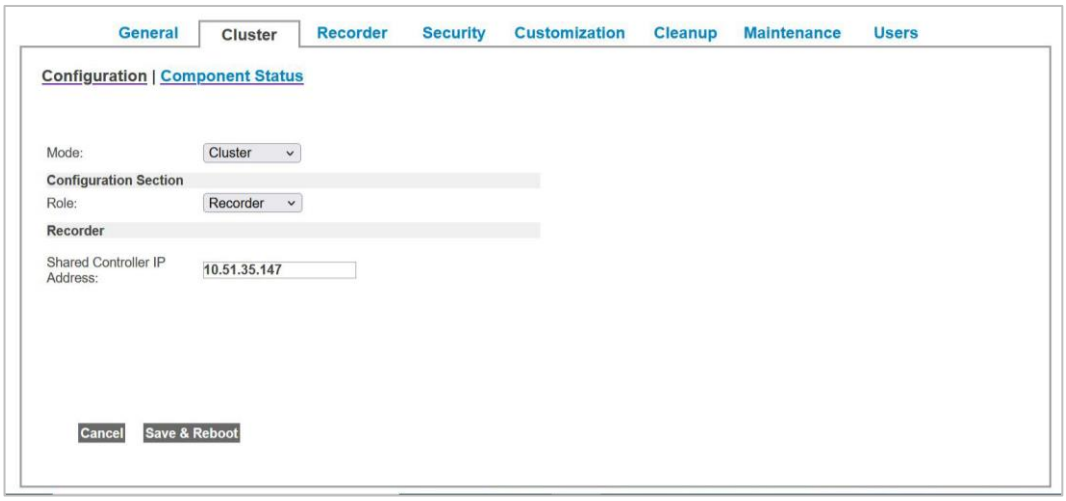
Configure your Recorder

Before configuring clusters, be sure to review Clustering procedure.

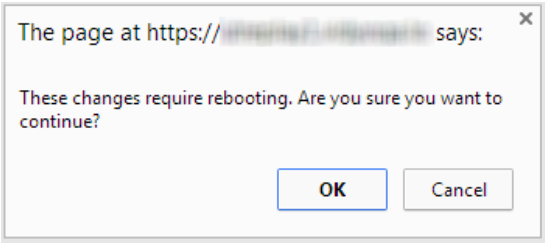
To configure your Recorder:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Cluster* tab.

4. Click the **Configuration** link.
5. In the **Mode** drop-down, select **Cluster**.
6. In the **Role** drop-down, select **Recorder**.



7. Enter a **Shared Controller IP Address**. Provide the IP address exactly as it's shown in the System Console and do not provide an FQDN in this field.
8. Click **Save & Reboot**. When you click **Save & Reboot**, a dialog box informs you that overwriting the settings and applying changes drops all active recordings on your server.



When you click **OK**, the VidyoReplay server reboots.

View VidyoReplay component statuses

You can view the component statuses and other details of the VidyoReplay servers in your system using the **Component Status** link.

Additionally, in VidyoReplay version 19.1.0 or later, you can turn Maintenance mode on or off per node in this window as well as view details about each component including Status (up, online, or maintenance), Local IP Address, NAS Status (up or down), number of Calls, and Actions (Maintenance mode on or off).

To view VidyoReplay component statuses:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Cluster* tab.
4. Click the **Component Status** link. A tabular display appears and lists your servers along with corresponding components, statuses, local IP addresses, shared IP addresses, and database statuses.

> **Note**
>
> To stop incoming recordings or prior to upgrading, turn a node to Maintenance Mode: Off (from within the Maintenance tab).

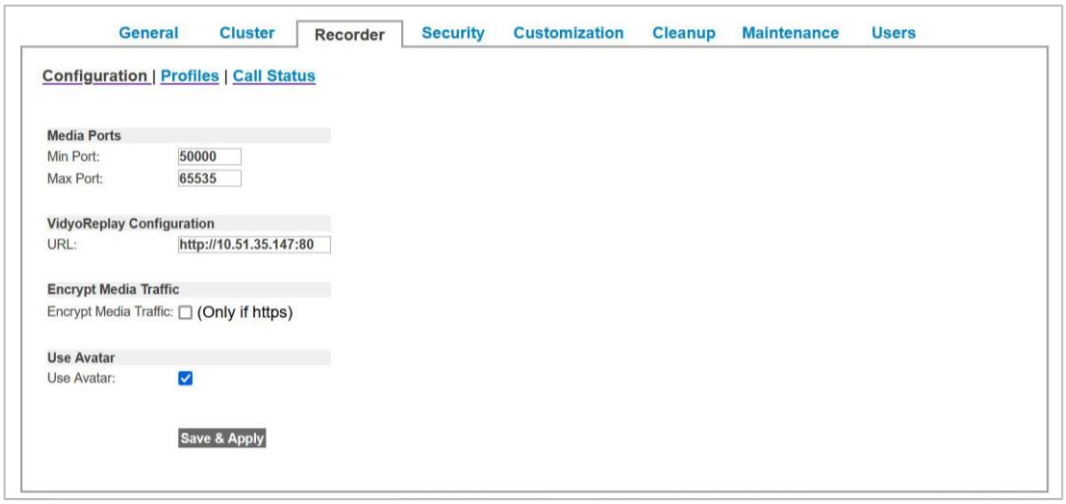
Configure the VidyoReplay Recorder

Your VidyoReplay Recorder is configured using the Configuration, Profiles, and Call Status links.

Set VidyoReplay Recorder main configurations

To set your VidyoReplay Recorder main configurations:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Recorder** tab.
4. Click the **Configuration** link.

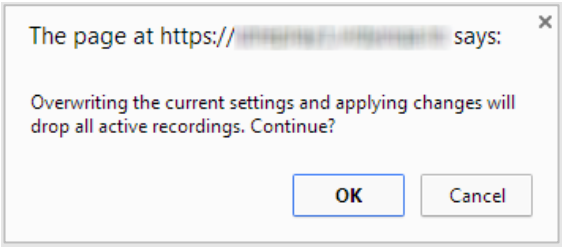


5. In the Media **Min Port** and **Max Port** fields, enter the UDP ports used for media transport between the VidyoReplay and the VidyoRouter. You must specify a minimum range of 1000.
   - In the Media **Min Port** field, enter the lower limit of the port range. The default (and recommended) value is 1024.
   - In the Media **Max Port** field, enter the upper limit of the port range. The default (recommended and maximum) value is 65535.
6. In the **URL** field, enter the IP address of your VidyoReplay Recorder. Provide the FQDN of your VidyoReplay Recorder exactly as it's shown in the System Console.

   When clustering VidyoReplay servers, the URL field must be the Shared Controller FQDN.
7. Select the **Encrypt Media Traffic** checkbox to only allow calls in which the media is encrypted and secured via the secure real-time transport protocol (SRTP).
8. When you leave this checkbox unselected, recordings without SRTP media encryption are permitted on the VidyoReplay.
9. Select the **Use Avatar** checkbox if you want an avatar with the first three letters of a participant's name to appear on their tile when their video source is muted (that is, when that participant is in audio-only mode).

10. Leave the checkbox unselected if you do not want a participant's video tile to display at all when their video source is muted.

    Click **Save & Apply**. When you click **Save & Apply**, a dialog box informs you that overwriting the settings and applying changes drops all active recordings on your server.



    When you click **OK**, the VidyoReplay server reboots.

Manage VidyoReplay Recorder profiles

The **Profiles** link allows you to manage and configure profiles for various recording types on your VidyoReplay.

VidyoReplay profiles specify details such as descriptive text, the profile type, resolution, recording mode, FPS, bandwidth, the maximum number of participants, layout, and whether the profile is active. Profiles are used when initiating a recording or webcast.

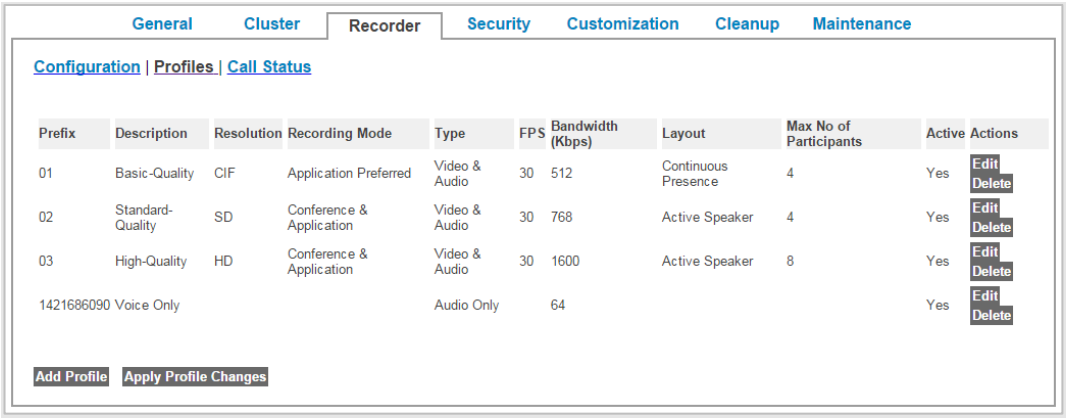
The VidyoReplay comes with preconfigured profiles for a variety of resolutions. These defaults allow you to record without the need to create your own profiles. You can modify these profiles or add new ones.

> Note
>
> When a VidyoReplay server is made part of a cluster, all the profiles must be identical between the cluster nodes. Therefore, any manually entered profiles should be created on each node. For more information about clustering, see VidyoReplay clusters.
>
> Four default profiles are provided for Basic-Quality CIF, Standard-Quality SD, High-Quality HD, and Audio.

View and manage VidyoReplay Recorder profiles

To view and manage VidyoReplay Recorder profiles:

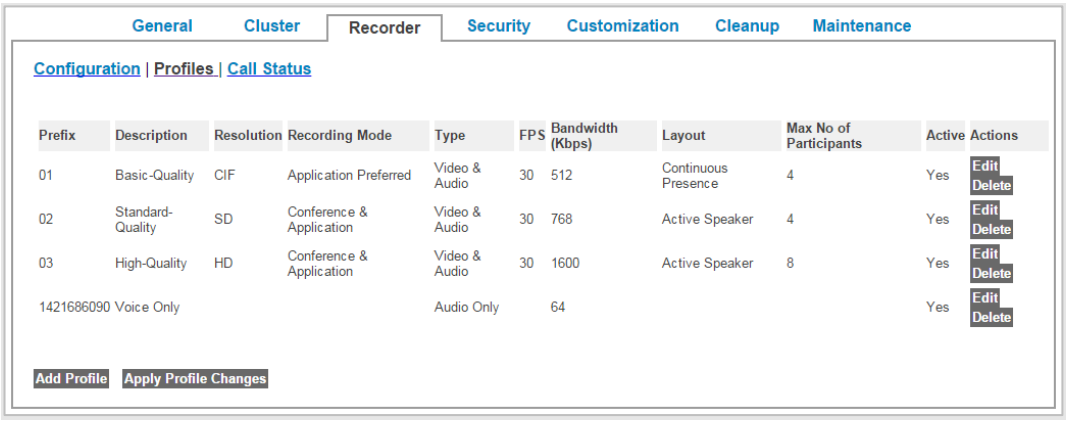
1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Recorder** tab.
4. Click the **Profiles** link.



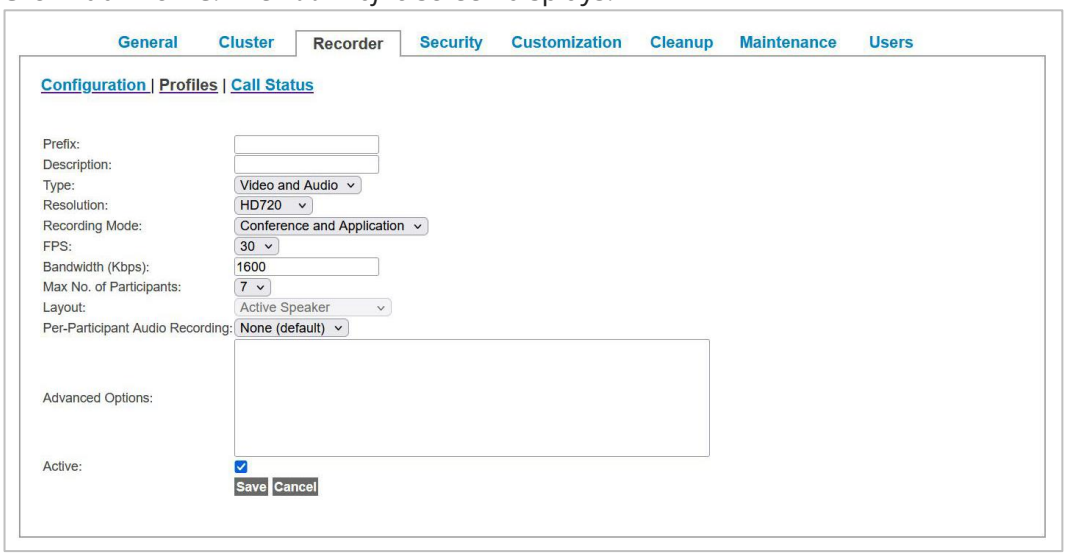
Add a VidyoReplay Recorder profile

To add a VidyoReplay Recorder profile:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Recorder** tab.
4. Click the **Profiles** link.



5. Click **Add Profile**. The *Add Profile* screen displays.



6. In the **Description** field, enter a descriptive recorder profile name for your new profile.

   For example, if you are planning to use the Per-Participant Audio Recording feature, you could enter “PPA-aac_SD” to indicate per-participant audio of type AAC is enabled for a standard definition recording.

7. In the **Type** drop-down, select **Video and Audio** or **Audio Only**.

   > Note
   >
   > If you select **Audio Only**, the **Resolution**, **Recording Mode**, **FPS**, **Max No. of Participants**, and **Layout fields** disappear, and the **Bandwidth** field is read-only and is fixed at 64 kbps.

8. In the **Resolution** drop-down, select **HD1080**, **HD720**, **SD**, or **CIF** as your resolution.

   The setting determines the maximum resolution used for your profile.

   > Note
   >
   > If you select **HD1080**, **HD720**, or **SD** as your profile resolution, the Recording Mode is set to **Conference and Application** and the Layout is fixed as **Active Speaker**.
   >
   > If you select **CIF** as your profile resolution, the Recording Mode is set to **Application Preferred** and the Layout is set to **Continuous Presence**.

9. In the Recording Mode drop-down, select **Conference and Application**, **Conference Only**, or **Application Preferred**.

   > Note
   >
   > The recording mode is initially selected in this drop-down based on the Resolution selected in the following manner: Conference and Application = HD1080 or HD720, Conference and Application = SD, Application Preferred = CIF.

10. In the **FPS** drop-down, select **5**, **10**, **15**, **20**, **25**, or **30** as your frames per second.
11. In the **Bandwidth (kbps)** field, enter a numeric value (in kbps) for the maximum bandwidth available for your profile.

> **Note**
>
> The number that displays in this field is based on the Resolution selected in the following manner: 3072kbps = HD1080, 1600 kbps = HD720, 768 kbps = SD, 512 kbps = CIF.
>
> If you select the **Audio Only** option from the **Type** drop-down, the **Bandwidth** field is read-only and is fixed at 64 kbps.

12. In the **Max No. of Participants** drop-down, select **1**, **2**, **3**, **4**, **5**, **6**, **7**, or **8** as your specified maximum number of participants to be shown.

> **Note**
>
> The maximum number of participants is initially selected in this drop-down based on the Resolution selected in the following manner: 8 = HD1080 or HD720, 4 = SD, 4 = CIF.

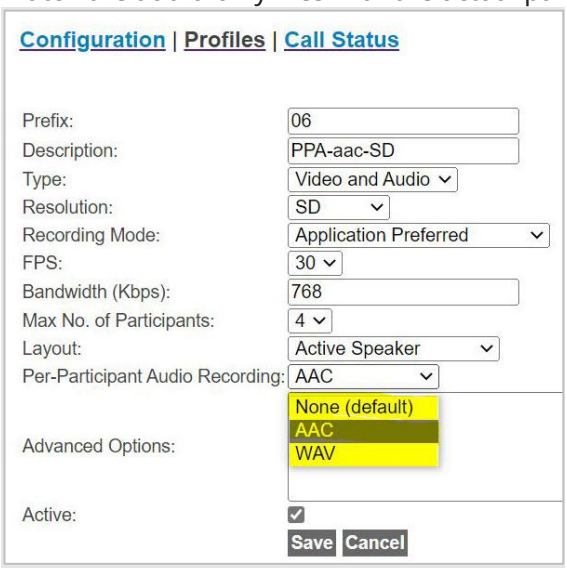
13. In the **Layout** drop-down, select **Continuous Presence** or **Active Speaker** as your mode.
    - Select **Continuous Presence** to display all participants in equal-sized windows.
    - Select **Active Speaker** to display the most recent speaker in a larger window than other users.

    > **Note**
    >
    > If you select the **Conference and Application** option from the **Recording Mode** drop-down, the **Layout** field is read-only and is fixed as **Active Speaker**.
    >
    > If you select **HD1080**, **HD720**, or **SD** in the **Resolution** drop-down, the **Layout** field is read-only and is fixed as **Active Speaker**.
    >
    > If you select **CIF** in the **Resolution** drop-down, the **Layout** field is read-only and is fixed as **Continuous Presence**.

14. In the **Per-Participant Audio Recording** drop-down, select **None (default)**, **AAC**, or **WAV.**

    This feature enables each participant in a conference to have separate conference recordings as well as separate audio-only files. When enabled, an additional directory is created in the file system that contains the recordings. The directory contains the audio-only recordings as well as a meta.dat file. This metadata file includes events within the conference recording, such as “user joined”, “user left”, “user silence”, and “user speaking”.

If a participant leaves and re-joins a conference, two audio-only files are created. In order to match the audio-only files with the actual participants, you must consult the meta.dat file.



- Select **None (default)** if you do not want to allow any extra audio-only files to be created.
- Select **AAC** to allow additional MPEG audio-only files (.M4A) to be created. This option uses the AAC codec. AAC codecs require more CPU, but the resulting audio-only files are small.
- Select **WAV** to allow additional WAV audio-only files (.WAV) to be created. This option uses the PCM codec. WAV format results in about 10.5 MB of storage for each minute.

15. In the **Advanced Options** field:
    - Enter **chatRecording:on** if you want to record and save chat messages from your VidyoConnect calls. See Record and save in-call chats.
    - Enter **deleteWebcast:on** if you want to delete the webcast recording at the end of the VidyoConnect call. See Auto-delete webcasts.
16. Select the **Active** checkbox to make your profile and all its settings available for use on your system.

    Deselect the checkbox to make it unavailable for use on your system.
17. Click **Save**. The VidyoReplay server reboots.

Record and save in-call chats

You can record and save the chat messages from your VidyoConnect calls by creating a profile with **chatRecording:on** enabled. When this profile is selected, an additional file is created during the recording. That file is a CSV file which contains the chat messages as well as other information, such as the timestamp, username, and internal ID. The file looks like this:

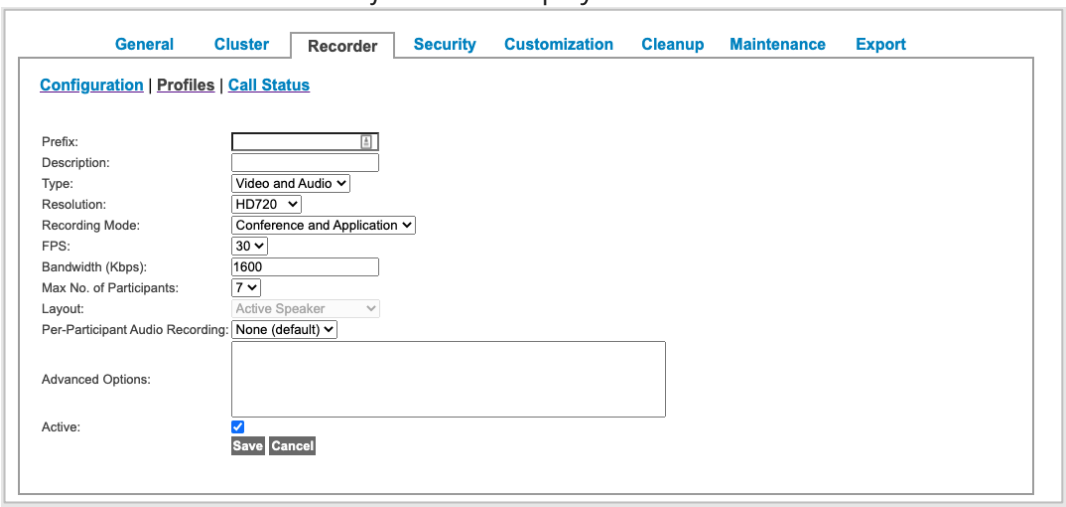
```
1575af13-dd58-5562-894e-20a9e28a92a1.chat                                                                    2561/2561          100%
20220616160334 |Marius |scip:CsAPI1654849160-113f4-7b7fec32ad0b3cc6-b5dd6badb6538269;transport=TLS     |HELLO
20220616160349 |Marius |scip:CsAPI1654849160-113f4-7b7fec32ad0b3cc6-b5dd6badb6538269;transport=TLS     |waiting for the automatedXY to join
20220616160409 |Marius |scip:CsAPI1654849160-113f4-7b7fec32ad0b3cc6-b5dd6badb6538269;transport=TLS     |2 joined already - but no audio ... yet
20220616160505 |Guestautomated7@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-1145a-df302ab096636530-9bfcd42f6a22d231;transport=TLS     |Switching loudest speaker to: autom
20220616160506 |Marius |scip:CsAPI1654849160-113f4-7b7fec32ad0b3cc6-b5dd6badb6538269;transport=TLS     |all joined (io automated)
20220616160520 |Guestautomated1@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-1145b-990f0fac2ebd9b63-639204b07182275c;transport=TLS     |Switching loudest speaker to: autom
20220616160535 |Guestautomated10@v:neo.alpha.vidyo.com |scip:CsAPI1654849160-1145e-8303662461efac16-39ae6d2c2341f17a;transport=TLS     |Switching loudest speaker to: autom
20220616160551 |Guestautomated4@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-1145f-da3e62147059fae7-a5d4fdd425902eac;transport=TLS     |Switching loudest speaker to: autom
20220616160606 |Guestautomated2@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-11460-90c1b4cb86af3469-7694d70e26434d56;transport=TLS     |Switching loudest speaker to: autom
20220616160621 |Guestautomated9@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-11461-4e87034310713cb-3a31b790477d1ad;transport=TLS     |Switching loudest speaker to: autom
20220616160637 |Guestautomated6@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-11462-a7437a84610ef04-ac91cdcfa616cfd0;transport=TLS     |Switching loudest speaker to: autom
20220616160652 |Guestautomated5@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-11463-536c6b061bbbc282-557a87442e0d54be;transport=TLS     |Switching loudest speaker to: autom
20220616160707 |Guestautomated8@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-11466-aab8ffd9504efd98-a5160f511a5ebb47;transport=TLS     |Switching loudest speaker to: autom
20220616160723 |Guestautomated3@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-11467-ff498bf903d30984-64f988b3ee80039d;transport=TLS     |Switching loudest speaker to: autom
20220616160738 |Guestautomated7@v:neo.alpha.vidyo.com  |scip:CsAPI1654849160-1145a-df302ab096636530-9bfcd42f6a22d231;transport=TLS     |Ok, we are leaving the call, but we
20220616160742 |Marius |scip:CsAPI1654849160-113f4-7b7fec32ad0b3cc6-b5dd6badb6538269;transport=TLS     |...they are leaving. So stop recording.
```

When a user goes to the VidyoReplay Library and downloads a recording that had the in-call chat recorded, they receive a ZIP file that contains the recorded call in MP4 format, a thumbnail image, and the CSV file containing the chat. Note that the VidyoReplay Library does not provide any visual indication of which recordings include the chat message and which don't.

To record and save in-call chats:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Recorder** tab.
4. Click the **Profiles** link.

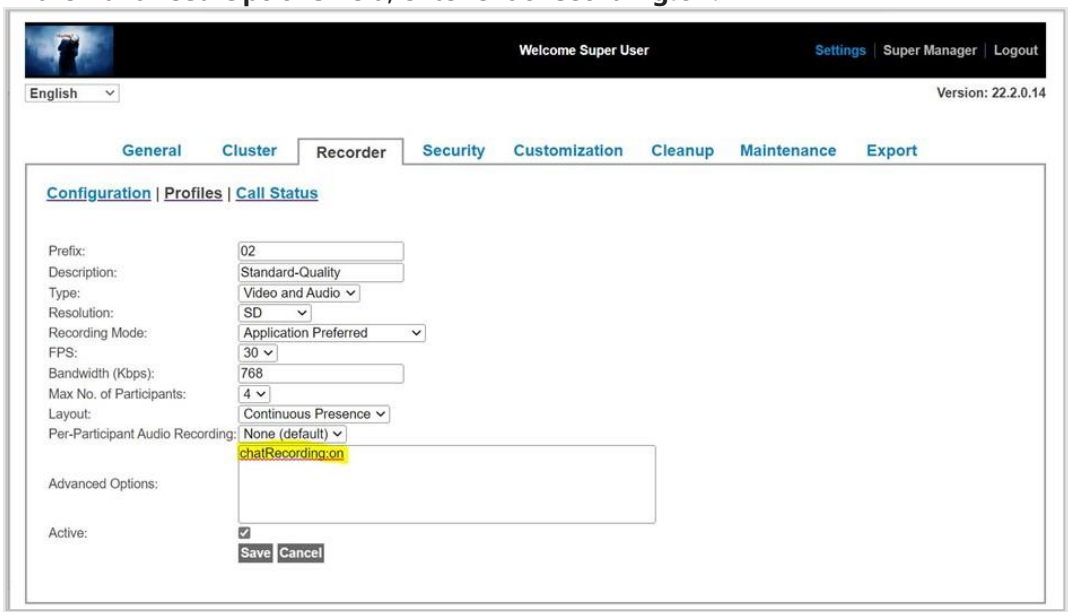
   Click **Add Profile**. The *Add Profile* screen displays.



5. In the **Description** field, enter a descriptive profile name which identifies that the in-call chat will be recorded.

   For example, if you are adding chat recording to your Standard-Quality profile, you could enter "Standard-Quality-chat".
6. Complete the **Type**, **Resolution**, **Recording Mode**, **FPS**, **Bandwidth**, **Max No. of Participants**, **Layout**, and **Per-Participant Audio Recording** fields as described in the previous section, Add a VidyoReplay Recorder profile.

7. In the **Advanced Options** field, enter **chatRecording:on**.



8. Select the **Active** checkbox to make your profile and all of its settings available for use on your system.

   Click **Save**. The VidyoReplay server reboots.

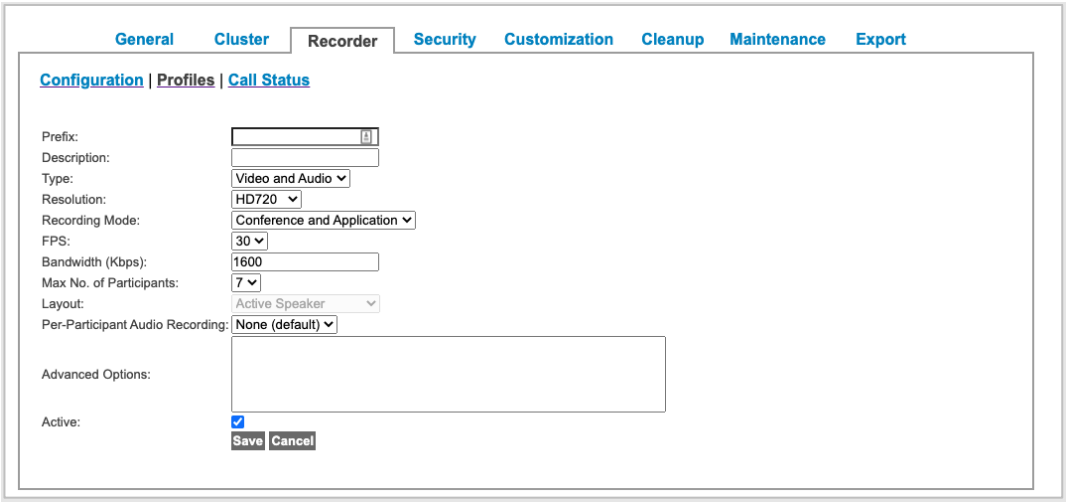
Auto-delete webcasts

You can delete your webcast recordings by creating a profile with **deleteWebcast:on** enabled. When this profile is selected, the webcast recording is not available in the VidyoReplay Library once the webcast finishes. Therefore, it cannot be viewed, played, searched, or downloaded.

> Note
>
> To enable users who have slow connections to view the entire webcast, the recording does remain available for about 30 seconds after the webcast ends.

To auto-delete webcasts:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Recorder** tab.
4. Click the **Profiles** link. Click **Add Profile**. The *Add Profile* screen displays.

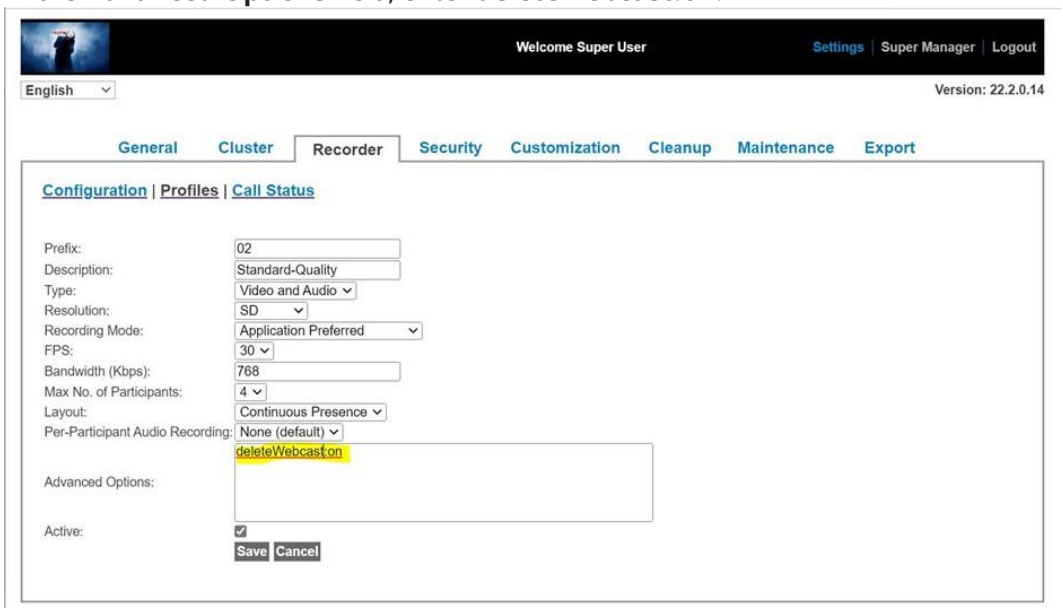


5. In the **Description** field, enter a descriptive profile name which identifies that the webcast will be deleted at the end of the call.

   For example, if you are auto-deletion of your webcasts to your Standard-Quality profile, you could enter “Standard-Quality-delete”.

6. Complete the **Type**, **Resolution**, **Recording Mode**, **FPS**, **Bandwidth**, **Max No. of Participants**, **Layout**, and **Per-Participant Audio Recording** fields as described in the previous section, Add a VidyoReplay Recorder profile.

7. In the **Advanced Options** field, enter **deleteWebcast:on**.



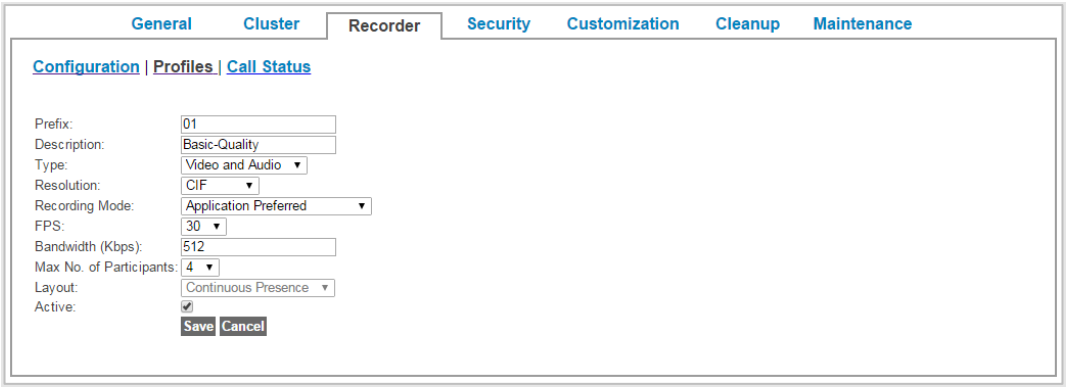
8. Select the **Active** checkbox to make your profile and all of its settings available for use on your system.

   Click **Save**. The VidyoReplay server reboots.

Edit a VidyoReplay Recorder profile

To edit a VidyoReplay Recorder profile:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Recorder** tab.
4. Click the **Profiles** link.
5. Click the corresponding **Edit** button to the right of the list of profiles. The *Edit Profile* screen displays.



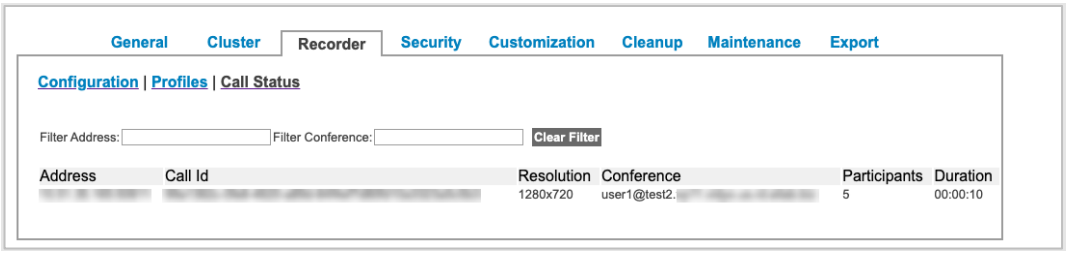
6. Edit configuration settings for your profile. The settings are the same as the ones used when adding a VidyoReplay recorder profile. See Add a VidyoReplay Recorder profile.
7. Click **Save**. The VidyoReplay server reboots.

View VidyoReplay Recorder statuses

The **Status** link allows you to view the recordings and playbacks occurring on your VidyoReplay.

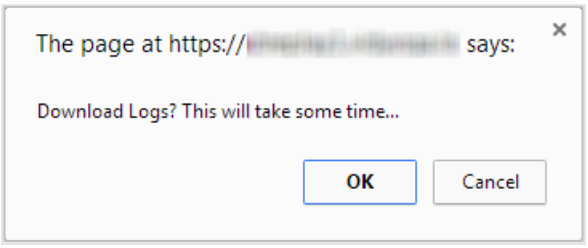
To view VidyoReplay Recorder statuses and to download logs:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Recorder** tab.
4. Click the **Call Status** link.



If the VidyoReplay is processing recordings, the main area of the screen is populated with call information such as Address, Status, Call ID, Resolution, Conference, Participants, and Duration.

5. Click **Clear** to instantly remove any parameters you provided.
6. Click **Download Logs**. A dialog box asks you if you to confirm that you want to download the logs as it may take some time.



7. Click **OK**. Your browser downloads a `.tar.gz` file containing your log file for debugging analysis.

Secure your VidyoReplay system with SSL and HTTPS

To secure your VidyoReplay system by Enabling SSL and HTTPS Only, you must complete specific configurations done on six sequential tabs from left to right in the Security section of the Super Admin Portal. The tabs include:

- *SSL Private Key* Tab – This tab is for Generating or Uploading an SSL Private Key.
- *SSL CSR* Tab – This tab is for Generating an SSL Certificate Signing Request (CSR).
- *Server Certificate* Tab – This tab is for Deploying Your Server Certificate.
- *Server CA Certificates* Tab – This tab is for Deploying Your Server Certification Authority (CA) Certificates.
- *Advanced* Tab – This tab is for deploying your Client Root CA Certificates.

> Note
>
> The *Advanced* tab is also used to Upload and Import Security Settings, and Reset Security Settings. See Import or export certificates from the Advanced tab and Reset your security configuration to factory defaults.

- Enable an SSL Type from the drop down in the top left of the window. The HTTPS+HTTP option is the default).

> Caution
>
> Do not use the **Enable SSL Type** drop down until you've completed the steps for securing your videoconferencing system.

The following ordered sections explain these steps in detail.

Upload and regenerate an SSL private key

The following procedures show you how to upload 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.

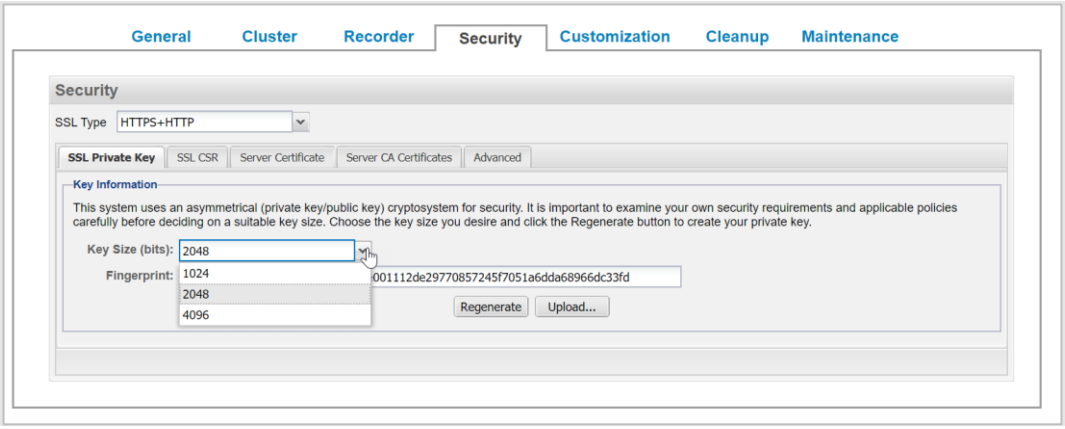
Upload an SSL private key

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.

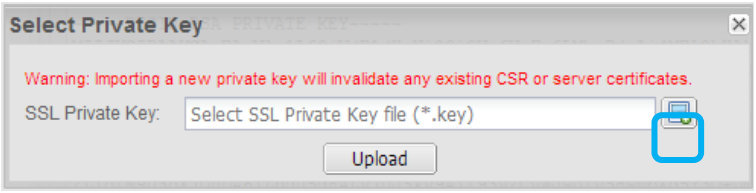
> Note
>
> In order to import an SSL Private Key, you must first disable HTTPS.
>
> You can only import encrypted and password protected private keys that were exported from servers that also encrypted and password protected the private keys.
>
> Changes made to an SSL Private Key require a CSR and SSL 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 `.pfx` bundle format. See Import certificates from a certificate bundle.

To import an SSL private key:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *SSL Private Key* subtab.



5. Click **Upload**.
6. In the *Select Private Key* dialog box, click the **Select File** ( ) icon.



7. Select your private key file and click **Upload**.
8. If the upload is successful, the *File Upload Success* dialog box displays. The tab then loads the Private Key information in the lower part of the screen.

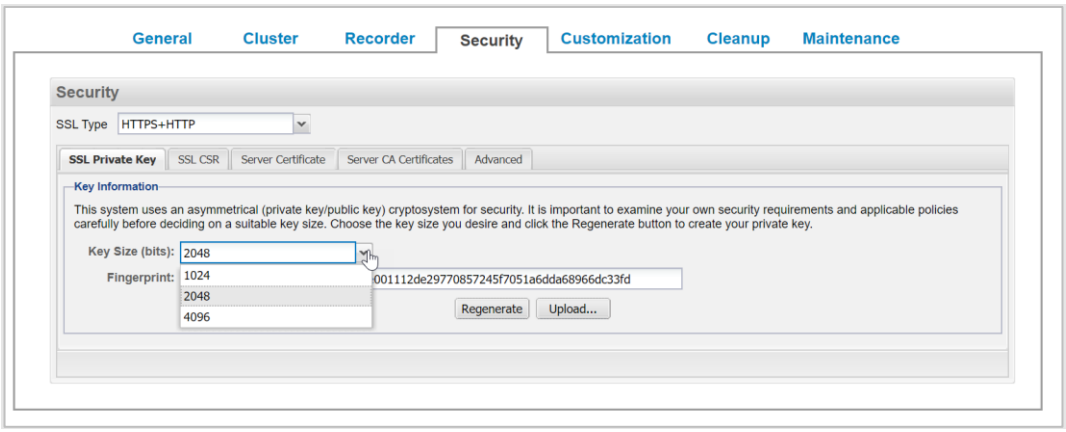
Generate an SSL private key

This system uses an asymmetrical (private key and public key) cryptosystem for security. Choose the desired key size and click the **Regenerate** button to create your private key.

> Note
>
> 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 VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *SSL Private Key* subtab.



5. In the **Key Size** field, specify a **1024**, **2048**, or **4096** key size.

   > Note
   >
   > Some countries or CAs limit the key size. Observe the limitations in effect in your country. Check with your CA for Key Size requirements.

6. Click **Regenerate**. A confirmation window displays this message, “Are you sure you want to generate a new private key? This will require new SSL CSR and server certificates.”

7. Click **Yes**.

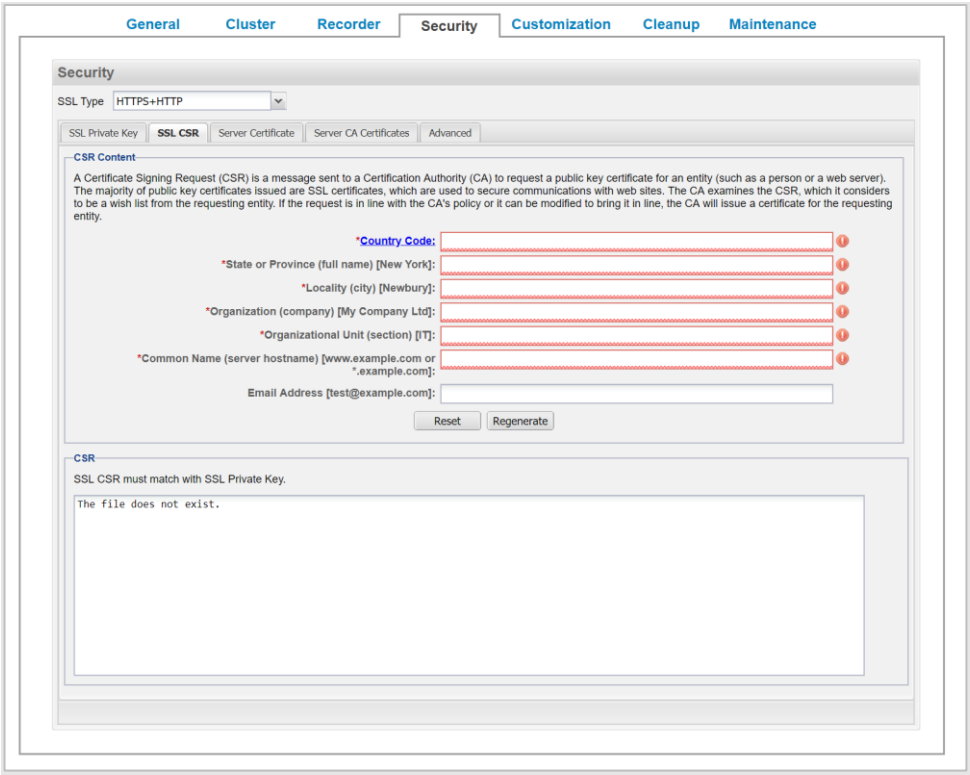
Generate and view an SSL CSR

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.

Generate an SSL CSR

To generate an SSL CSR:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *SSL CSR* subtab.



5. Check with your CA and carefully enter correct values for the following:
   - Country Code (the 2 character ISO 3166 country code)
   - State or Province Name
   - Locality
   - Organization Name
   - Organization Unit
   - Common Name (the FQDN of the server)
   - Email Address

   > **Note**
   >
   > If using a Subject Alternate Name (SAN) certificate, the alternate names are added by the Certificate Authority when a certificate is ordered and the Common Name you're providing here in the Certificate Details portion of the screen is used to provide your base Common Name (CN) for your SAN certificate. See Use a wildcard certificate in a multi-tenant system.

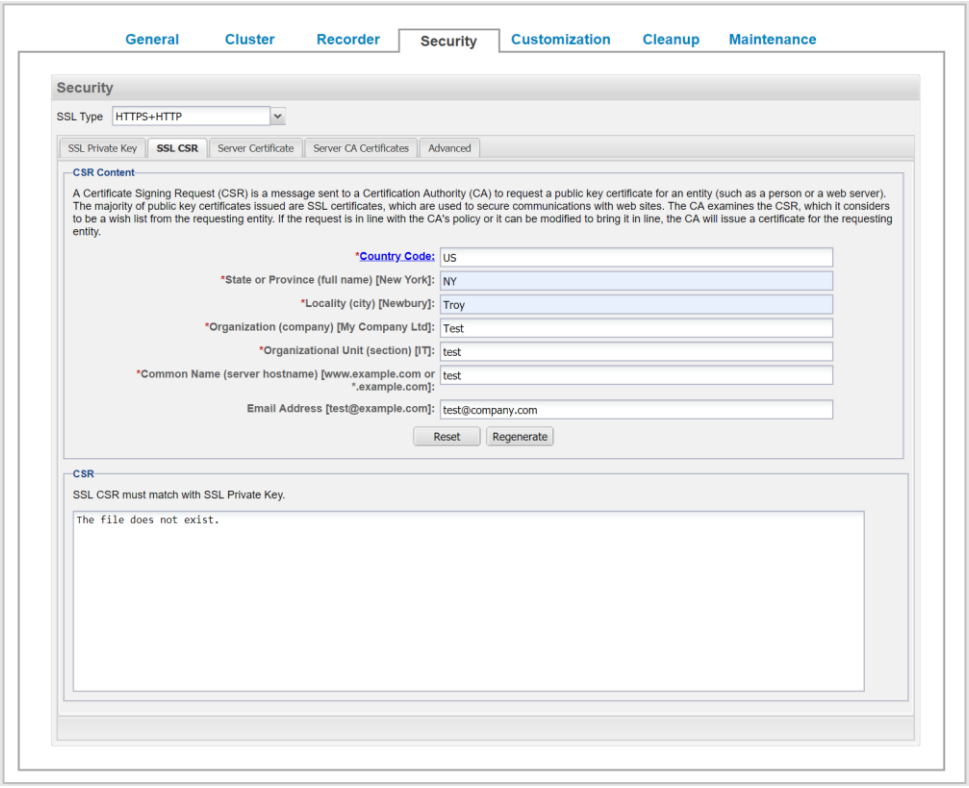
6. Provide all field information exactly as you registered it with your domain registration provider. You should consider all information on this screen mandatory before you click **Generate** or **Regenerate CSR**.

   > **Note**
   >
   > Click **Reset** to reload any previously saved field information.
   >
   > Your SSL CSR is generated based on the SSL Private Key you entered during Upload an SSL private key or Generate an SSL private key.

View an SSL CSR

To view an SSL CSR:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *SSL CSR* subtab.



5. View the lower portion of the screen labeled CSR, as desired.

Use a wildcard certificate in a multi-tenant system

If you are running a multi-tenant system, all Tenant URLs must be in the same domain, and each use a unique sub-domain. You then also use a wildcard or SAN SSL certificate. For a wildcard certificate, you must substitute an asterisk (*) wildcard character for the tenant sub-domain name (or sub-sub-domain name) in the Common Name, so the name of each tenant automatically matches the fully qualified domain name (FQDN) for the certificate.

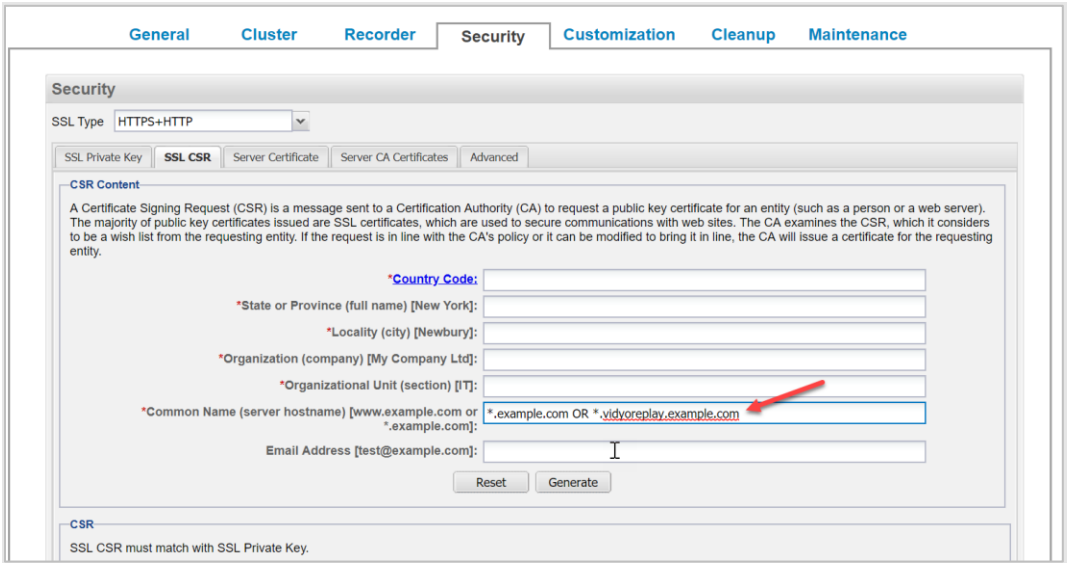
For example: ***.example.com** or ***.vidyoreplay.example.com**.

> Note
>
> If using a Subject Alternate Name (SAN) certificate, the alternate names are added by the Certificate Authority when a certificate is ordered and the Common Name you're providing here

> in the Certificate Details portion of the screen is used to provide your base Common Name (CN) for your SAN certificate.
>
> Microsoft refers to their own version of SAN certificates as Unified Communications (UC) certificates.

Vidyo recommends that you use sub-sub-domain names so that you can also use a wildcard DNS entry in your domain name server to resolve tenant URL addresses without requiring a separate entry for each tenant, and also avoid having to create a new DNS entry each time a new tenant is added.

Wildcard certificate entry examples include: `*.example.com` or `*.vidyoreplay.example.com`



Certificates received from your certificate authority

Most CAs instantly send certificates and returns to at least a domain (server) certificate and may return a root and one or more intermediate certificates in separate files. However, some authorities may provide the certificate data in a single email. You must copy the certificate data from the email into separate, respective files.

> Note
>
> When selecting the certificate type from your CA, be sure to select Apache2 or Tomcat.

Your certificate authority may provide three types of files:

- The domain certificate file. This is often named or titled server certificate.
- One or more intermediate certificate files. This is optional.
- The root certificate file.

Again, the certificate authority may send you these files, or require you to download them from their website. The certificates are not clearly identified most times, requiring you to identify each file type.

As mentioned, if your certificate authority provides certificate files in an email message, you must copy and paste the appropriate text for each certificate type into a separate file and save it with the correct extension, as described in the next section. Be sure to use a text editor that doesn't append carriage returns at the end of each line.

Vidyo recommends the following guidelines to identify certificate files from your CA:

- The domain file normally contains your server's common name or FQDN.
- Intermediate files often contain the character string "inter" somewhere in the file name. Once you identify which ones are the intermediates, you can then identify the root certificate file by process of elimination.
- The remaining file is the CA's root certificate file.

The CA may also only return the domain (server) certificate, and if needed or required, the root and intermediate certificates need to be located, and manually downloaded from the CA's website.

If the root and intermediate certificates were not provided to you, your Vidyo server includes a default bundle of common CA root and intermediate certificates. If you are using a mainstream CA, the root and intermediate certificates may not be needed.

> Note
>
> Some CAs have several root and intermediate certificates available depending on the type of certificate you have ordered. Be sure to locate the appropriate matching root and intermediate certificates for your domain certificate. Contact your CA for assistance if you're not sure.

CAs provide different kinds of certificate files to customers. Regardless, the following certificates should be a part of what your CA provides to you:

- Domain Certificate (may have a `.domain`, `.crt`, or `.cer` extension).
- Intermediate Certificate(s) (optional, may be one or more, and may have an `.inter`, `.crt`, or `.cer` extension).
- A Root Certificate (may have a `.root`, `.crt`, or `.cer` extension).

Certificate files versus bundles

Your CA may instead provide you with a `.p7b` file, which may contain Root and Intermediate or Root, Intermediate, and Server Certificate content. Check with your CA to find out exactly where each certificate is located. Your Vidyo server accepts the `.pem`, `.crt`, `.cer`, `.der`, `.p7b`, and `.pfx` formats. The `.pfx` format additionally includes the private key which may be password protected.

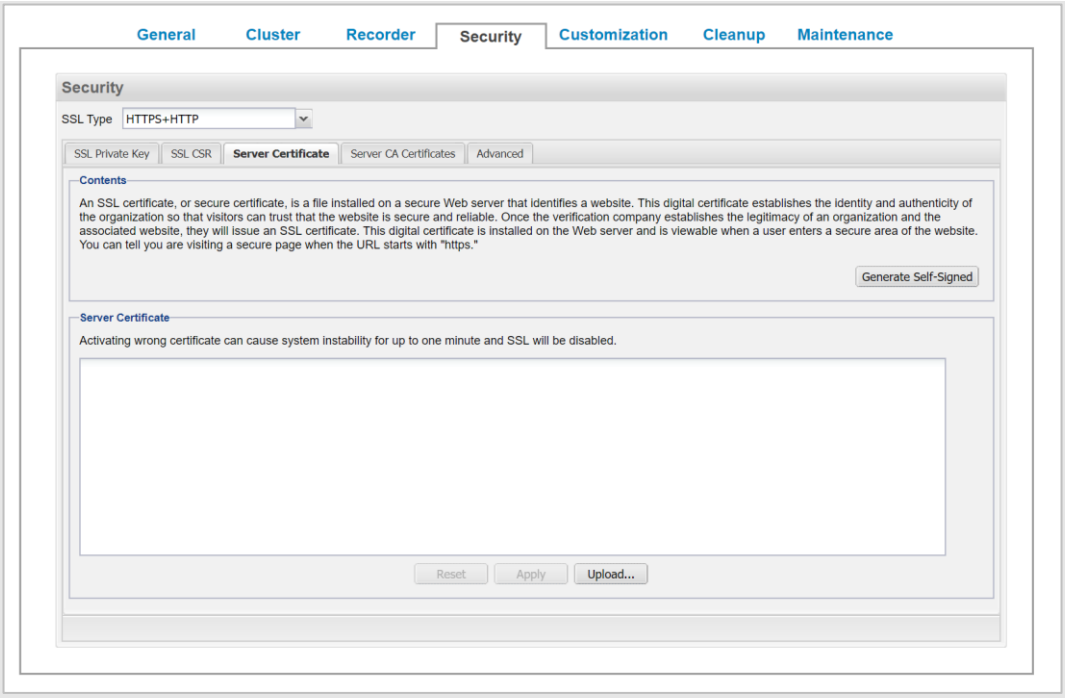
- Certificate Files (`.pem`, `.crt`, `.cer`, and `.der`) are imported using the *Server Certificate*, *Server CA Certificates*, and *Advanced* tabs. See Deploy your server certificate, Deploy your server CA certificates (intermediates), and Import Client Root CA Certificates from the Advanced tab.
- Bundles (`.p7b`, `.pfx`,) are imported and exported (only `.pfx` files can be exported) from the *Advanced* tab. See Import Client Root CA Certificates from the Advanced tab.

Deploy your server certificate

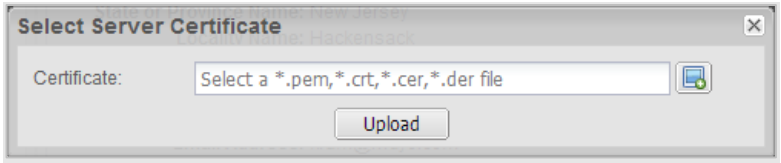
- Perform the steps in this procedure after you receive certificate files back from your certification authority.
- An unsigned (self-issued) certificate does not provide a guarantee of security to your users.
- Your Vidyo server checks certificates for validity based on the certificates issued date range. Therefore, make sure that the time zone of your server is configured correctly prior to applying your certificate.
- If you instead plan on using self-signed certificates, you can click **Generate Self-Signed** to have the server sign its own certificate (self-signed). Clicking Generate Self-Signed and confirming removes your currently implemented server certificate.

To upload your server certificate file:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *Server Certificate* subtab.



5. Click **Upload**.
6. In the *Select Server Certificate* dialog box, click the **Select File** ( ) icon.



7. Select your server certificate file on your computer (may also be referred to as the Domain Certificate by your Certificate Authority) or local network and click **Upload**.

   If the upload is successful, the *File Upload Success* dialog box displays.

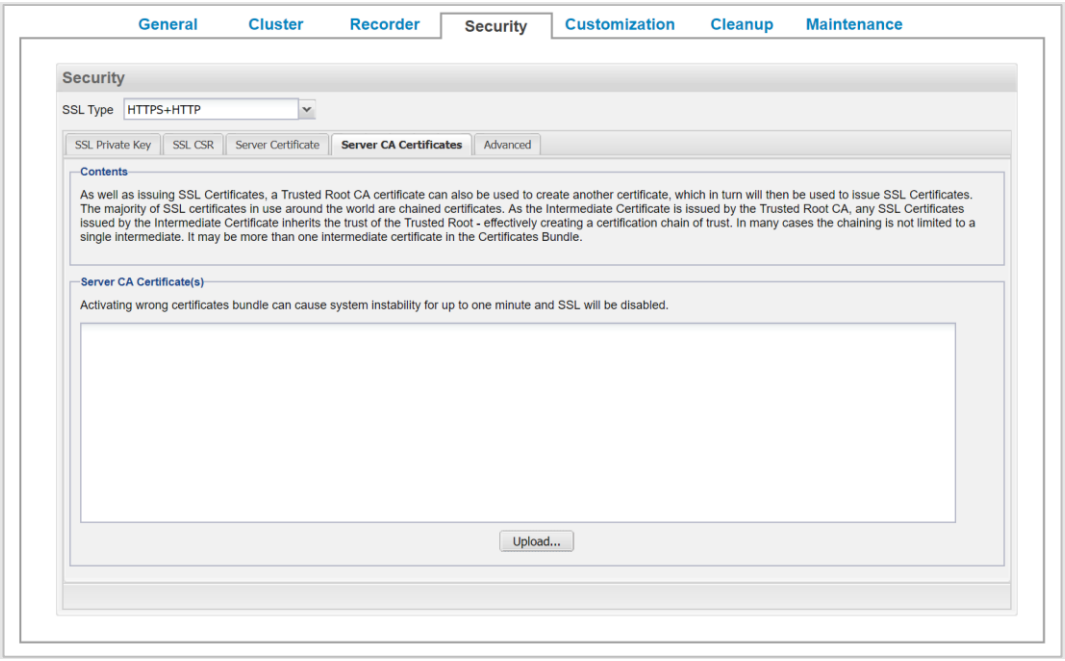
   The tab then loads the Certificate Information, Issuer, Subject, and the Certificate itself in the screen.

Deploy your server CA certificates (intermediates)

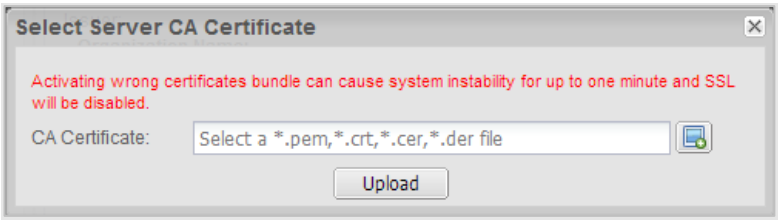
In addition to issuing SSL Certificates, a Trusted Root CA certificate can also be used to create another certificate, which in turn can be used to issue SSL Certificates. The majority of SSL certificates in use around the world are chained certificates of this type. As the Intermediate Certificate is issued by the Trusted Root CA, any SSL Certificates issued by the Intermediate Certificate inherits the trust of the Trusted Root – effectively creating a certification chain of trust. In many cases the chaining is not limited to a single intermediate. More than one intermediate certificate may be part of a Certificates Bundle.

To upload your server CA certificates (intermediates) files:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *Server CA Certificates* subtab.



5. Click **Upload**.
6. In the *Select Server CA Certificate* dialog box, click the **Select File** ( ) icon.



7. Select your server CA certificate file on your computer (may also be referred to as the Intermediate Certificate by your Certificate Authority) or local network and click **Upload**.

> Note
>
> A single file may contain multiple intermediate certificates.
>
> You can additionally upload the Root CA in this location in order to present the certificate to your clients along with the certificate chain. However, this is not recommended as standard security practice.

If the upload is successful, the *File Upload Success* dialog box displays.

The tab then loads the Certificate Information, Issuer, Subject, and the Certificates in the screen.

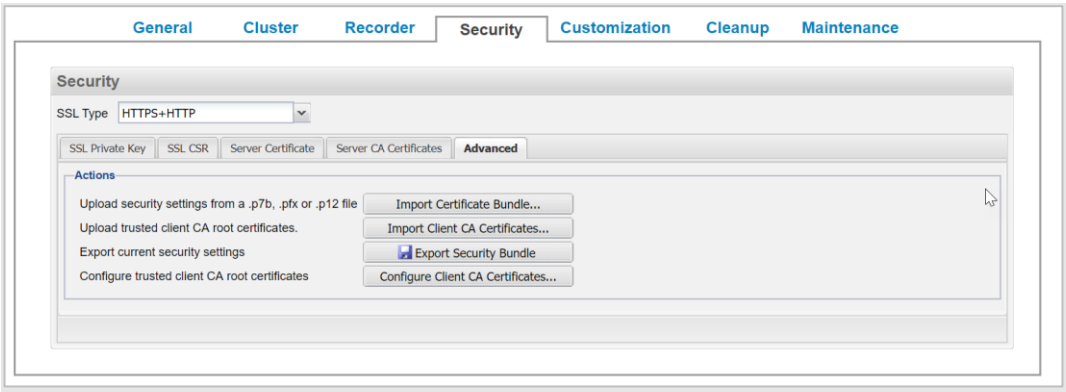
Import Client Root CA Certificates from the Advanced tab

The *Advanced* tab is used to upload trusted Client Root CA Certificates. This includes all Intermediate and Root Certificates.

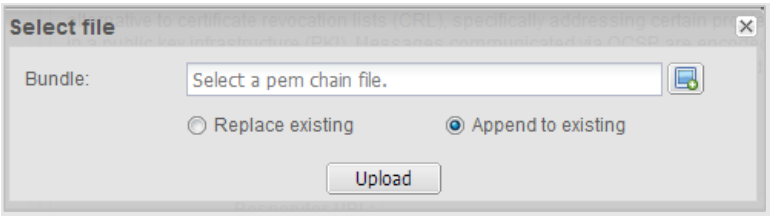
> Note
>
> If your system requires trusting other secure systems such as LDAPS and Secure SMTP Server, their certificates must also be uploaded in this tab.
>
> The *Advanced* tab is also used to Upload and Import Security Settings and to Reset Security Settings. See Import or export certificates from the Advanced tab and Reset your security configuration to factory defaults.

To upload Client Root CA Certificates from the Advanced tab:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *Advanced* subtab.



5. Click **Import Client CA Certificates**.
6. In the *Select file* dialog box, select either the **Replace existing** or **Append to existing** radio buttons.
   - Replace existing – Replaces any previously uploaded Client Root CA Certificates.
   - Append to existing – Any uploaded Client Root CA Certificates are added to your existing ones.
7. Click the **Select File** ( ) icon to locate the server certificate file on your computer (may also be referred to as the Domain Certificate by your Certificate Authority) or local network.



> **Note**
> A single file may contain multiple Client Root CA Certificates.

8. Click **Upload** to upload the client root CA certificate file. An Uploading file progress bar is shown while the system applies your certificates.

   If the upload is successful, a *Confirmation* dialog box displays indicating that your “Upload successful. Do you want to reboot the server now?”

9. Click **Yes**.

Enable SSL Types

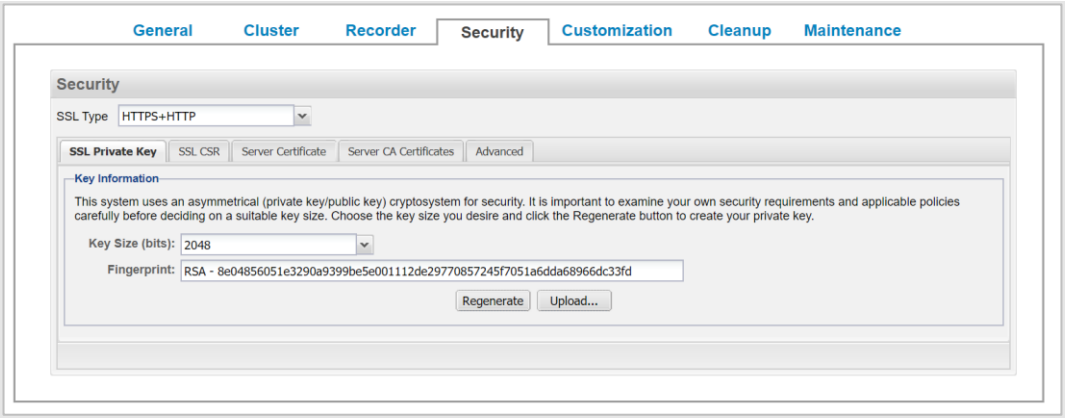
When you have completed the steps for securing your VidyoConferencing system, then you can select your SSL Type. Do not Enable HTTPS Only mode until you are certain HTTPS is working properly.

See Secure your VidyoReplay system with SSL and HTTPS.

Enable an SSL Type

To enable an SSL Type:

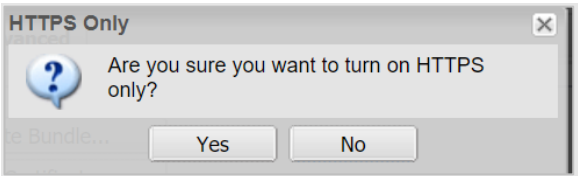
1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.



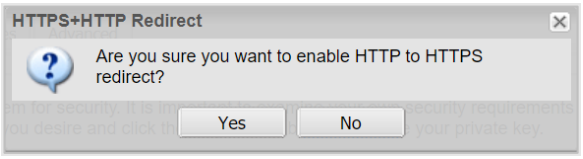
4. From the SSL Type drop down select any of the following three options:
   - **HTTPS+HTTP (default)** – This is the default option already enabled.
   - **HTTPS Only** - Before you enable HTTPS Only, you must configure your components to work with HTTPS on your VidyoPortal. For more information, refer to *Configure your components to work with HTTPS* in the *VidyoPortal and VidyoRouter Administrator Guide.*

     If you don’t configure your components to work with HTTPS first, you can still enable **HTTPS Only**, however, this may result in “DOWN” component statuses.

- When you select this option, a pop-up will display this message, “Are you sure you want to turn on HTTPS only?”



- HTTPS+HTTP Redirect
  - When you select this option, a pop-up will display this message, “Are you sure you want to enable HTTP to HTTPS redirect?”



  - Click **Yes** and your SSL setting is set.

> **Note**
>
> Browse to your VidyoReplay Admin portal to confirm that HTTPS is working properly and that the browser does not post any security errors. Be sure to include the HTTPS header in the URL (e.g., `https://[FQDN]`). Verify that HTTPS 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.
>
> 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.

If you are successful browsing to your Vidyo server using HTTPS and you do not receive any browser errors, continue with the next procedure.

> **Note**
>
> If you are unable to connect to your Vidyo server over HTTPS, see Secure your VidyoReplay system with SSL and HTTPS.

Import or export certificates from the Advanced tab

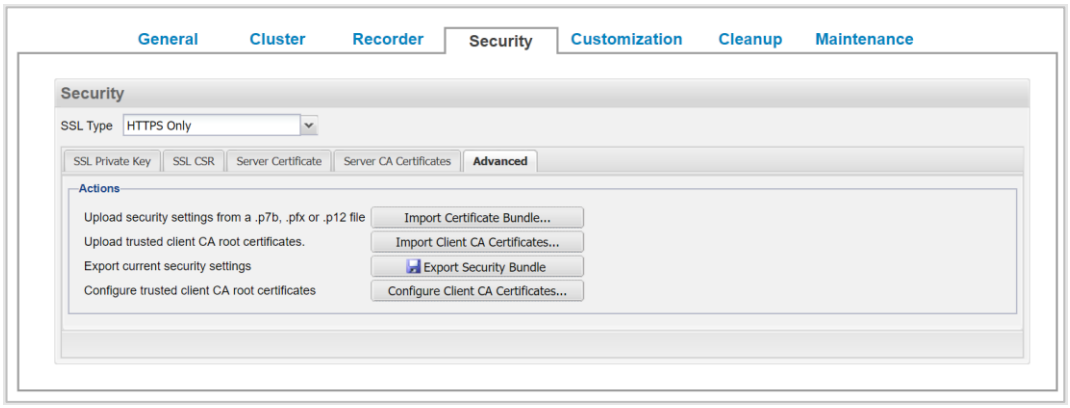
You can also import or export certificate bundles using the *Advanced* tab.

Import certificates from a certificate bundle

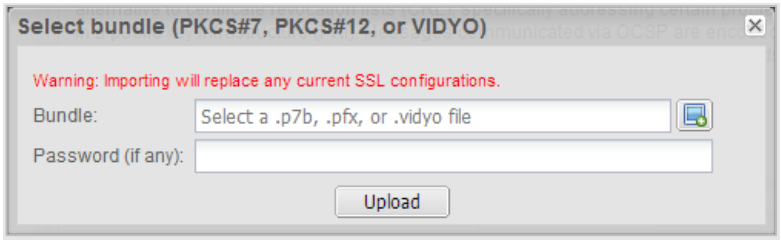
You can import from `.p7b` and `.pfx` standard formats.

To upload security settings from a certificate bundle:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *Advanced* subtab.



5. Click **Import Certificates Bundle**.
6. In the *Select bundle* dialog box, click the **Select File** ( ) icon to locate the bundle file.
7. If using the `.pfx` format, enter the password.



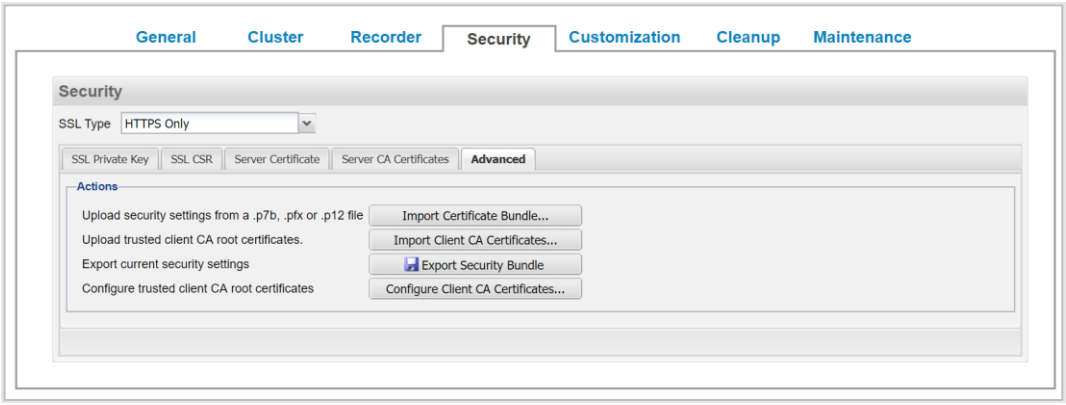
8. Click **Upload** to upload the bundle file. If the upload is successful, the *File Upload Success* dialog box displays.

> Note
>
> Depending on which bundle format you used, the appropriate Private Key, Server Certificate, Server CA Certificates, and Client Root CA Certificates data is loaded in to your Vidyo server.

Export a security bundle containing your certificate configuration

To export a security bundle containing your certificate configuration:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *Advanced* subtab.

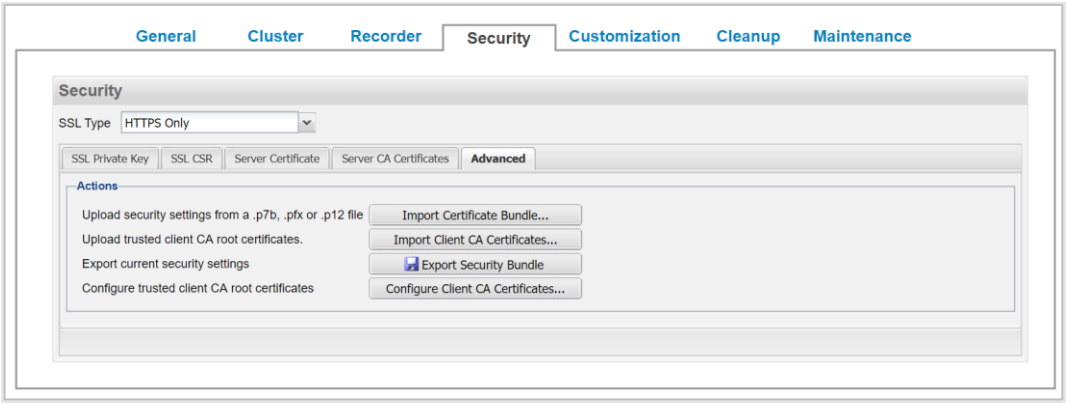


5. Click **Export Security Bundle**. Your browser then downloads `security_bundle.pfx` file to your computer which contains your security configuration for transfer or backup purposes.

Reset your security configuration to factory defaults

To reset your security configuration to the factory defaults:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Security* tab.
4. Click the *Advanced* subtab.



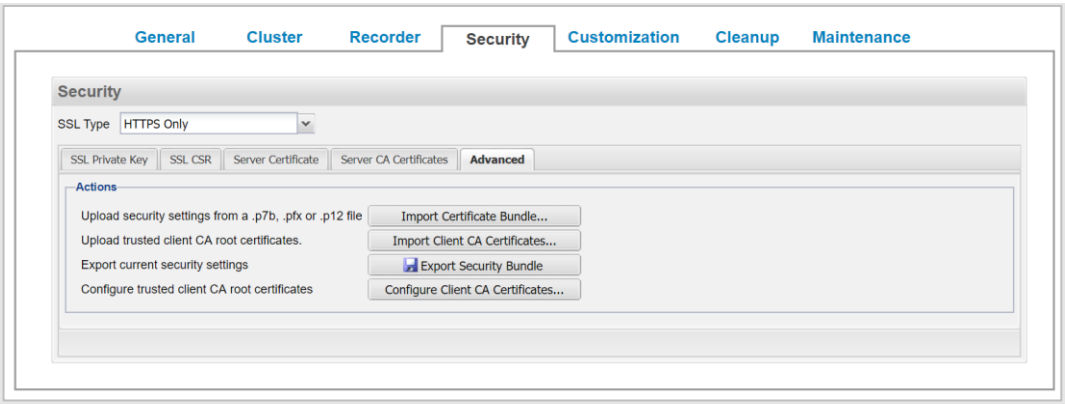
5. Click **Reset Security**. Your security configuration is then restored to the factory default settings.

Configure client CA certificates

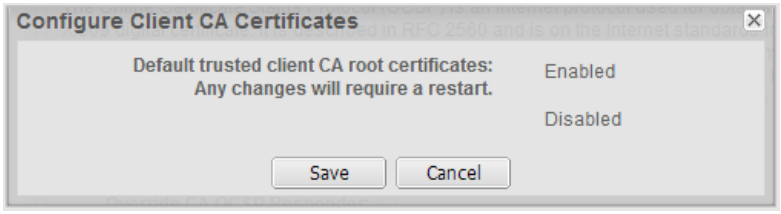
Vidyo servers ship with a default trusted CA list and is enabled by default. This *Advanced* tab function allows you to enable or disable the use of this list.

To configure client CA certificates:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Security** tab.
4. Click the **Advanced** subtab.



5. Click **Configure Client CA Certificates**. The *Configure Client CA Certificates* dialog box displays.



6. Click **Save**. The VidyoReplay server reboots. After rebooting, your CA root certificates are applied.

Configure customizations

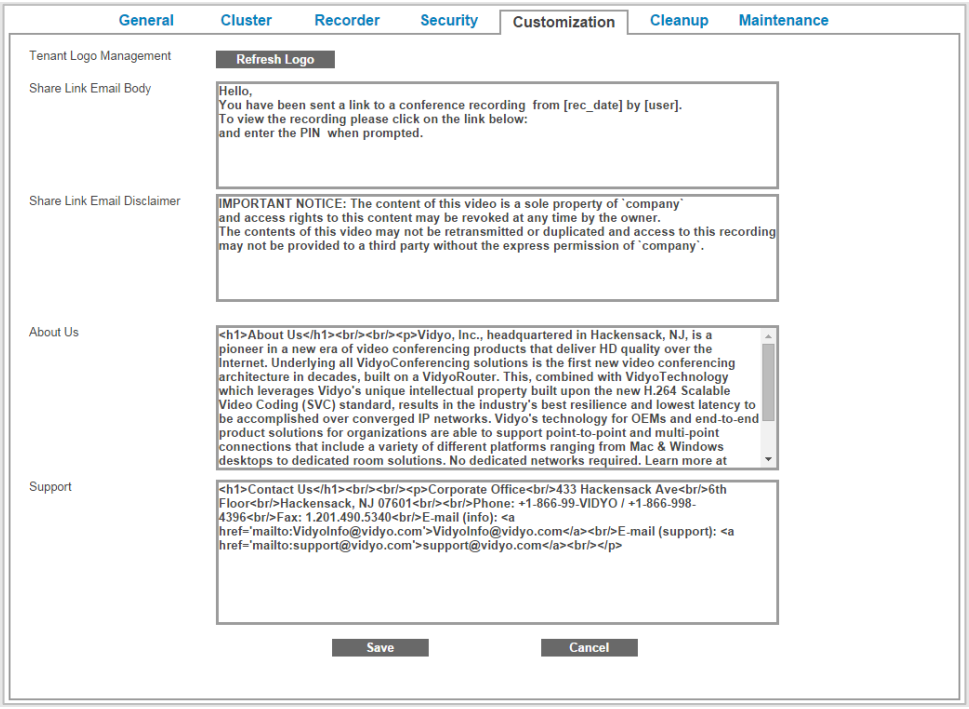
You can use the *Customization* tab to reset the logo and modify the default share link, about us, and support information for all tenants.

> **Note**
>
> You can only access the *Customization* tab from a Standalone VidyoReplay or from the Active or Standby Controllers in a VidyoReplay cluster.

Super Admins establish your company's logo, and provide **Share Link Email Body**, **Share Link Email Disclaimer**, **About Us**, and **Support** field information using the VidyoPortal. Tenant Admins can refresh a logo updated on the VidyoPortal by the Super Admin. Also, Super Admins may allow Tenant Admins to override **Share Link Email Body**, **Share Link Email Disclaimer**, **About Us**, and **Support** field information.

To configure your customizations:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Customization** tab.



4. Click **Refresh Logo** to update the logos on all tenants in your system with the one configured on your VidyoPortal in the Super Admin portal.
5. In the **Share Link Email Body** field, change the default text, if desired.
6. In the **Share Link Email Disclaimer** field, change the default text, if desired.

> **Note**
> This is an invitation to watch a pre-recorded webcast or other pre-recorded video from the VidyoReplay Library, not to participate in a live webcast.

7. In the **About Us** field, change the default text, if desired.
8. In the **Support** field, change the default text, if desired.
9. Click **Save**. A system notification indicates that the “Settings were updated successfully”.

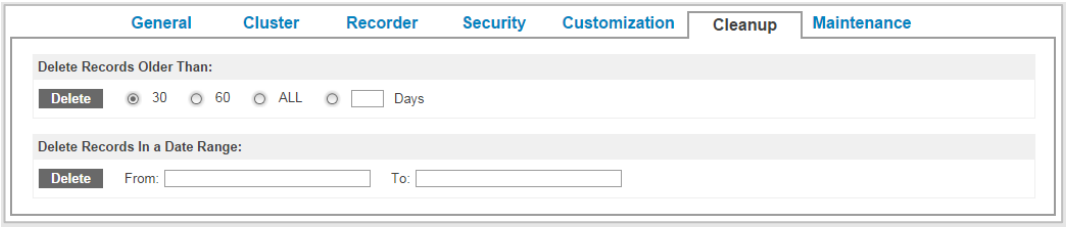
Clean up the VidyoReplay Library

The *Cleanup* tab allows the Super Admin to delete older video recordings to free up system space.

> **Note**
> You can only access the *Cluster* tab from a Standalone VidyoReplay or from the Active Controller in a VidyoReplay cluster.

To clean up the VidyoReplay Library:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Cleanup** tab.

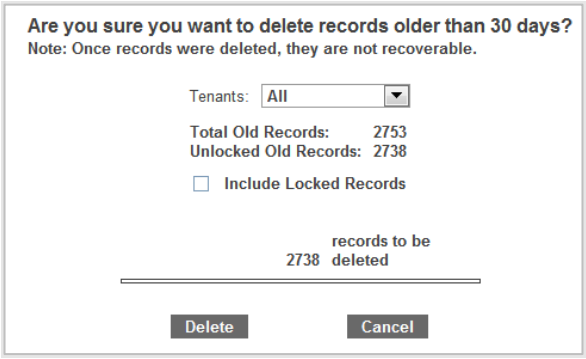


4. To delete records older than a certain number of days, do the following:
   a. Select **30**, **60**, **All**, or enter a custom number of days.
   b. Click **Delete**.

   The *Tenants and Locked Records* confirmation dialog box displays.
5. To delete recordings in a date range, do the following:
   a. Enter the first date in the **From** field.
   b. Enter the end date in the **To** field.
   c. Click **Delete**.

   The *Tenants and Locked Records* confirmation dialog box displays.
6. In the **Tenants** drop-down, select **All**, **Default**, or a specific tenant for deletion.

7. Select the **Include Locked Records** checkbox to delete the locked videos from the ones chosen.



8. Click **Delete**.

Maintain your VidyoReplay

In the Maintenance tab, you can upgrade, restart, and download logs from your VidyoReplay. In version 19.1.0 and later, you can also upgrade your VidyoReplay quickly and easily without first having to switch your system into Maintenance mode.

> Note
>
> To move nodes into Maintenance mode, see View VidyoReplay component statuses.

Upgrade your VidyoReplay

If you are upgrading to VidyoReplay version 22.3.0 or later (which has the multiple Super users feature), follow the instructions in Upgrade your VidyoReplay cluster to version 22.3.0 or later.

Upgrade your VidyoReplay cluster

To upgrade your VidyoReplay cluster:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Maintenance* tab and the Upgrade subtab displays by default.

4. Click **Choose File**.
5. Locate the `.vidyo` file on your computer or network location.
6. Click **Open**.
7. Click **Upload & Install**.

Upgrade your VidyoReplay cluster to version 22.3.0 or later

VidyoReplay version 22.3.0 or later offers the ability to have multiple Super users. Because of this feature, the procedure for upgrading is slightly different due to the database changes required when there are multiple Super users.

Before performing this procedure, be sure to review the following:

- For information about multiple Super users, see Configure multiple Super users.
- For information about clusters, see VidyoReplay clusters and Configure clusters.
- For information about how to turn Maintenance mode on or off, see View VidyoReplay component statuses.

To upgrade a VidyoReplay cluster to version 22.3.0 or later:

1. Upgrade all the VidyoReplay recording nodes in the cluster as described in the previous section, Upgrade your VidyoReplay.
2. Log in to the Active Controller (Controller 1) and put the Standby Controller (Controller 2) in Maintenance mode.
3. Log out of the Active Controller (Controller 1).
4. Log in to the Standby Controller (Controller 2) and perform the upgrade. When the upgrade completes, the system reboots.

   > Note
   >
   > At this point in the procedure, login via the UI is not possible.

5. Log in to the Active Controller (Controller 1) and take the Standby Controller (Controller 2) out of Maintenance mode.
6. Put the Active Controller (Controller 1) in Maintenance mode and perform the upgrade. When the upgrade completes, this Controller (Controller 1) will become the Standby Controller.

   > Note
   >
   > At this point in the procedure, login via the UI is not possible.

7. Log in to Controller 2 (which is now the Active Controller) and take Controller 1 (which is now the Standby Controller) out of Maintenance mode.
8. Log out of Controller 2. You can now log in via the UI to any Controller.

Restart or shut down your VidyoReplay

To restart your VidyoReplay you no longer need to take it out of Maintenance mode.

To restart or shutdown VidyoReplay:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Maintenance* tab.
4. Click the **Restart** link.

5. Enter a username and password, and then click **Restart**. The VidyoReplay system will restart.

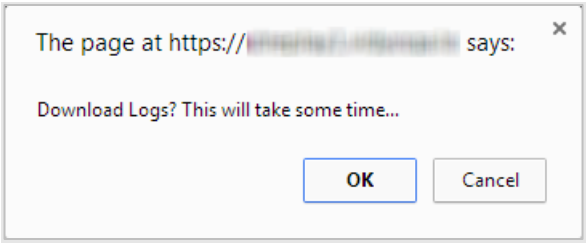
View VidyoReplay Recorder statuses and download logs

The **Status** link allows you to capture logs of recordings occurring on your VidyoReplay. You can download and view logs for debugging analysis and view the statistics of a single recording. You can also view the data directly on the VidyoReplay if desired.

To view VidyoReplay Recorder statuses and to download logs:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the *Maintenance* tab.
4. Click the **Download Logs link**.

5. Click **Download Logs**. A dialog box asks you if you to confirm that you want to download the logs as it may take some time.



6. Click **OK**. Your browser downloads a `.tar.gz` file containing your log file for debugging analysis.

Configure multiple Super users

With VidyoReplay version 22.3.0 and later, you can configure multiple Super users. This feature also:

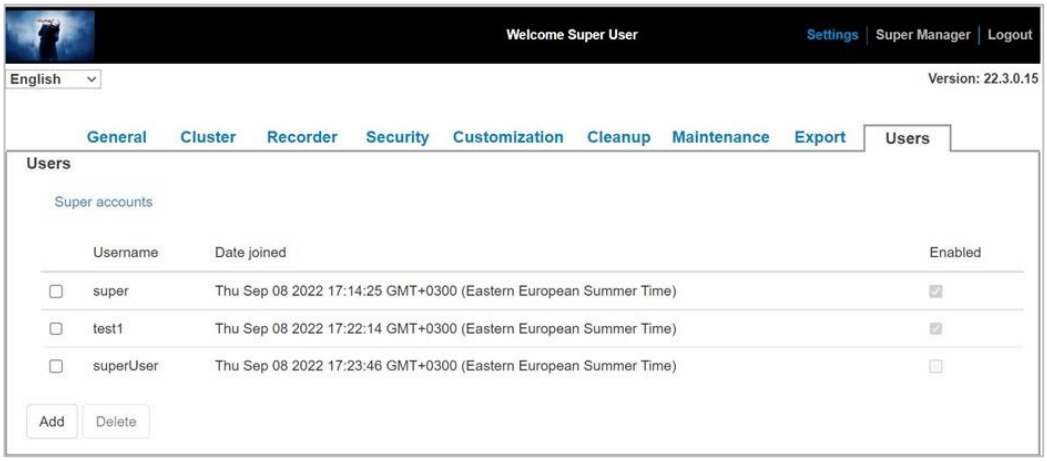
- Enables you to add users with Super permissions as well as edit and delete them.
- Allows you to further strengthen the installation by maintaining more strict control over passwords for users with Super permissions.

> Note
> Due to database changes required when there are multiple Super users, the procedure for upgrading an existing VidyoReplay cluster is different starting with VidyoReplay version 22.3.0. See the Upgrade your VidyoReplay cluster to version 22.3.0 or later section.

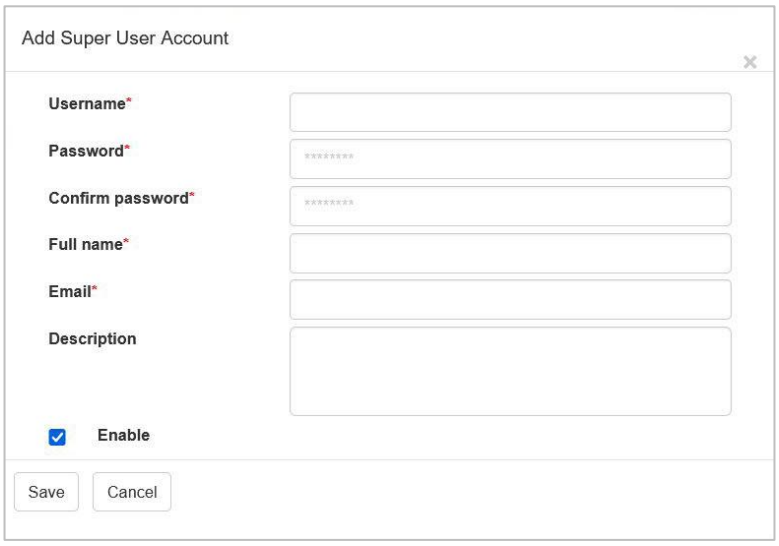
Add a Super user

To add a Super user:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Users** tab.



4. Click **Add**. The “Add Super User Account” pop-up appears.



5. Enter the username, password, and other information about the new Super user.

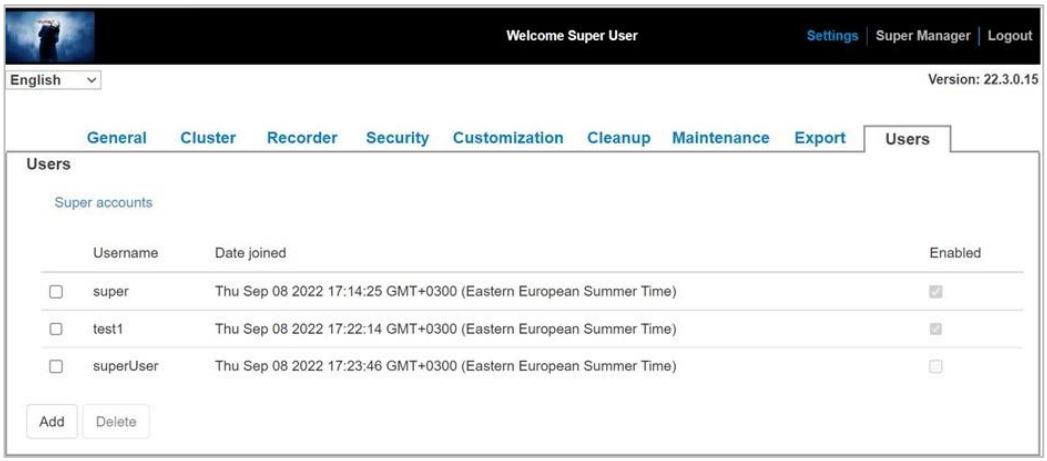
   All fields are mandatory except for the Description field. By default, the new user is enabled; therefore, the Enable checkbox is already selected.

6. Click **Save**. The new Super user is added to the database and is displayed in the list of users on the Users tab.

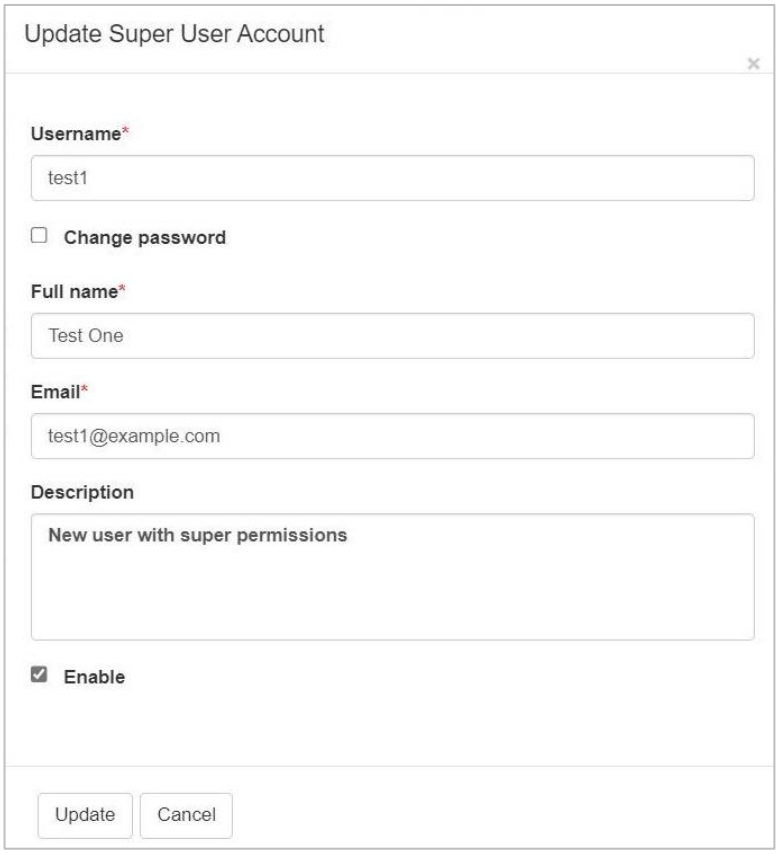
Edit a Super user

To edit a Super user:

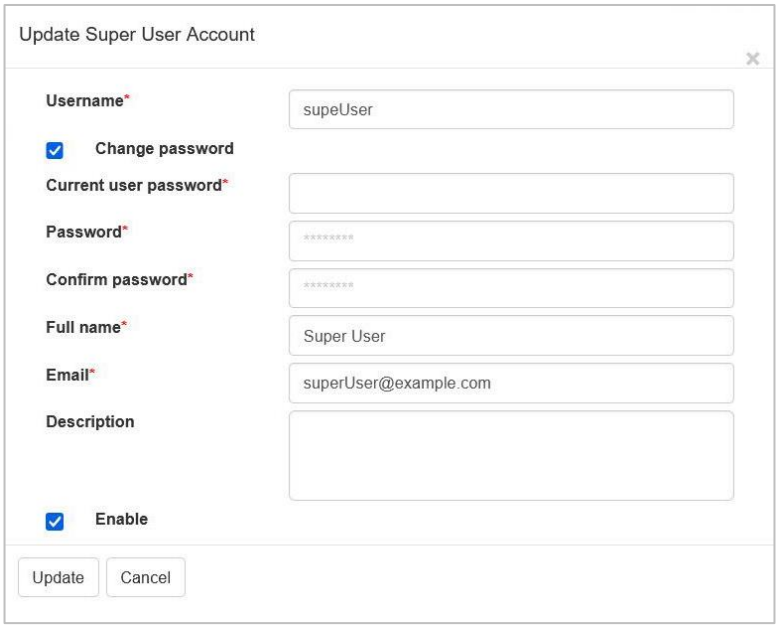
1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Users** tab.



4. Hover your cursor over the username of the user you want to edit. The cursor changes from an arrow to a hand when you hover over the username.
5. Click to select the user. The “Update Super User Account” pop-up appears.



6. Edit the username, full name, and other information about the Super user.
7. If you select the **Change password** checkbox, the pop-up redisplays with these additional fields: Current user password, Password, and Confirm password.



a. Enter the user's current password in the **Current user password** field.

   If you are changing your own password, enter the password that you want to change. If you are helping another Super user who has forgotten their password to reset it, enter your current password.

b. Enter the new password for the user in the **Password** field.

c. Enter the new password again in the **Confirm password** field.

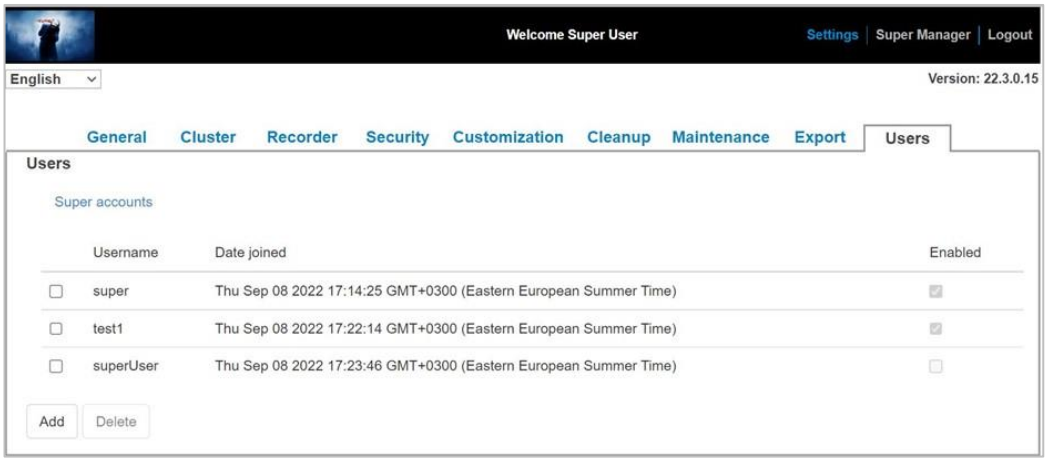
8. Click **Save**. The changes are stored in the database.

   If a user's password was changed, that user will be able to log in with the new password (as long as that user is enabled).

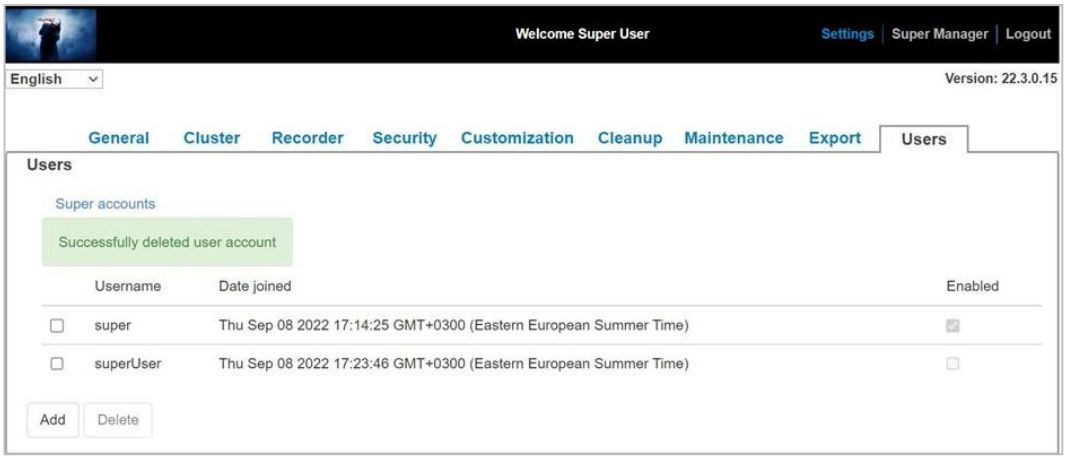
Delete a Super user

To delete a Super user:

1. Log in to the VidyoReplay using the default Super account.
2. Click the **Settings** link.
3. Click the **Users** tab.



4. Select the checkbox next to the name of the Super user that you want to delete.
5. Click **Delete**. The Users page refreshes and indicates that the user account was successfully deleted.



6. Configure your system as the Tenant Admin

Super Admins configure the system (and establish tenants if running a multi-tenant system). Then, they create Tenant Admins who can manage their assigned tenant or tenants.

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

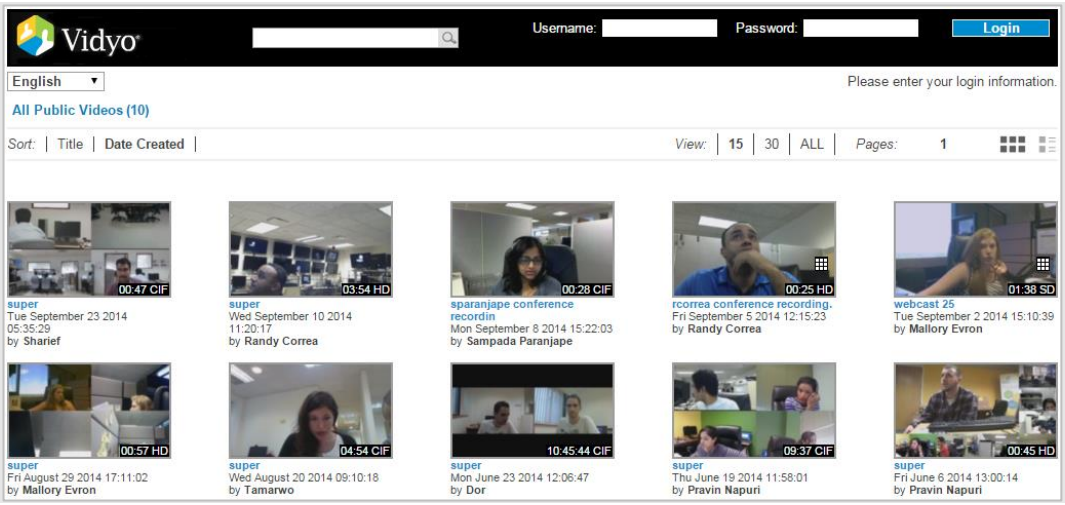
Log in as a Tenant Admin

To administer your tenant, you must log in to your VidyoReplay using a Tenant Admin account.

To log in to your VidyoReplay as a Tenant Admin:

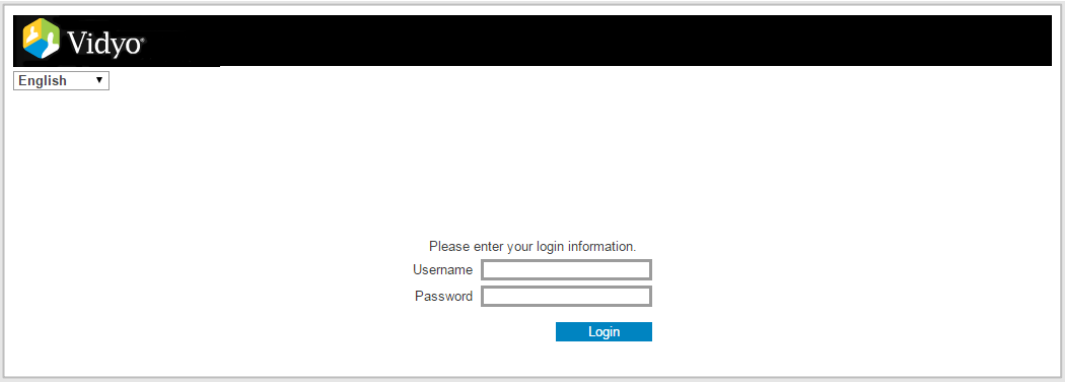
1. Log in to your VidyoRepaly using your Tenant Admin account. The URL of your VidyoReplay is typically a domain name: `[vidyoreplay.example.com]`

   The VidyoReplay Public Library displays.



   > **Note**
   >
   > Only recordings with Public selected as the **Who can watch** option display on this screen. Otherwise a blank login screen displays.

For more information, see 7. VidyoReplay Library and Manager access levels and Add or edit recording properties.



2. Enter the default Admin user name and password.
   - User Name: `admin`
   - Password: `password` (case sensitive)
3. Click **Login**.

> Note
> You should change this password from the default.

For more information, refer to *Manage users as the Tenant Admin* in the *VidyoPortal and VidyoRouter Administrator Guide*.

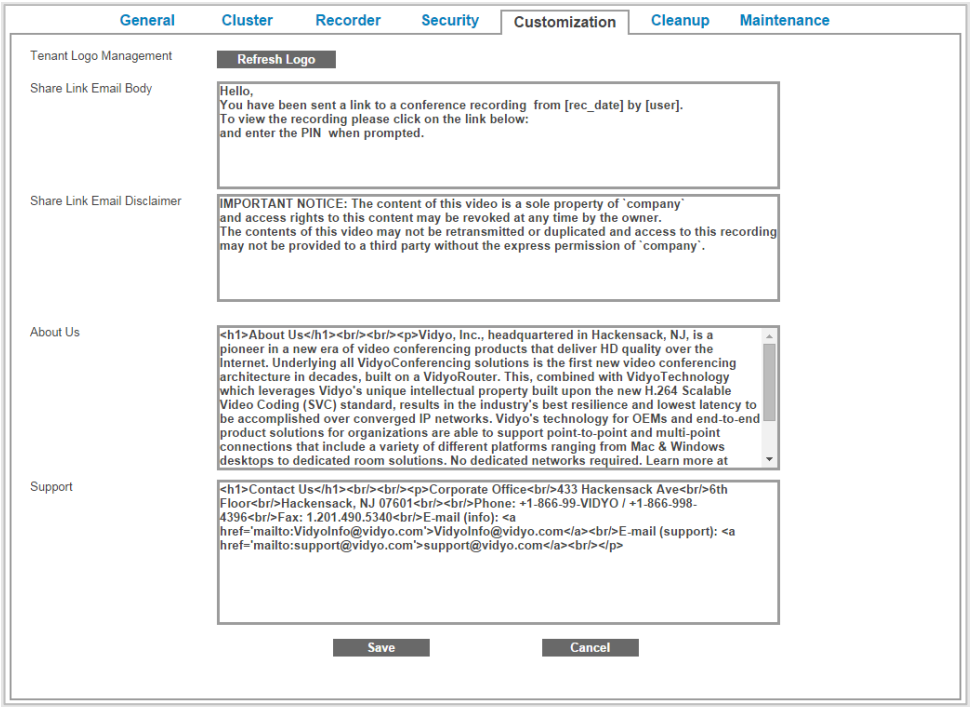
Configure customizations

You can use the *Customization* tab to reset the logo and modify the default share link, about us, and support information for all tenants.

Super Admins establish your company's logo, and provide Share Link Email Body, Share Link Email Disclaimer, About Us, and Support field information using the VidyoPortal. Tenant Admins can refresh a logo updated on the VidyoPortal by the Super Admin. Also, Super Admins may allow Tenant Admins to override Share Link Email Body, Share Link Email Disclaimer, About Us, and Support field information.

To configure your customizations:

1. Log in to the VidyoReplay using the Admin account.
2. Click the **Settings** link.
3. Click the **Customization** tab.



4. Click **Refresh Logo** to update the logos on all tenants in your system with the one configured on your VidyoPortal in the Super Admin portal.

   For more information, refer to *Upload custom logos on your tenant* in the *VidyoPortal and VidyoRouter Administrator Guide*.

5. In the **Share Link Email Body** field, change the default text if desired.
6. In the **Share Link Email Disclaimer** field, change the default text if desired.
7. In the **About Us** field, change the default text if desired.
8. In the **Support** field, change the default text if desired.
9. Click **Save**. A system notification indicates that the “Settings were updated successfully”.

> Note
>
> This is an invitation to watch a pre-recorded webcast or other pre-recorded video from the VidyoReplay Library, not to participate in a live webcast.

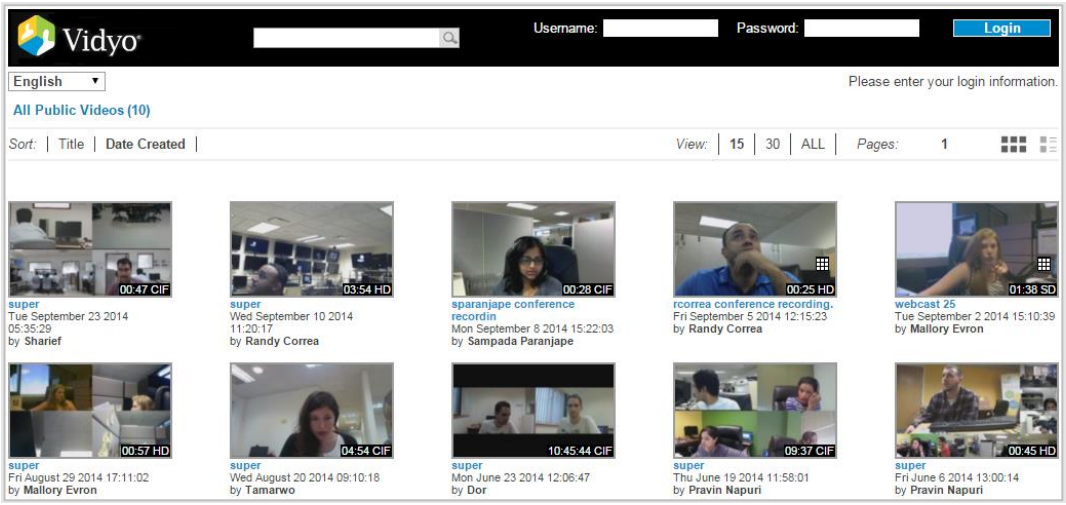
7. VidyoReplay Library and Manager access levels

All recordings and webcasts are stored in the VidyoReplay Library and can also be accessed via the VidyoReplay Manager. This section provides information for our VidyoConnect™ customers on user account access levels and how they affect what displays in the VidyoReplay Library and the VidyoReplay Manager.

VidyoReplay Library access levels

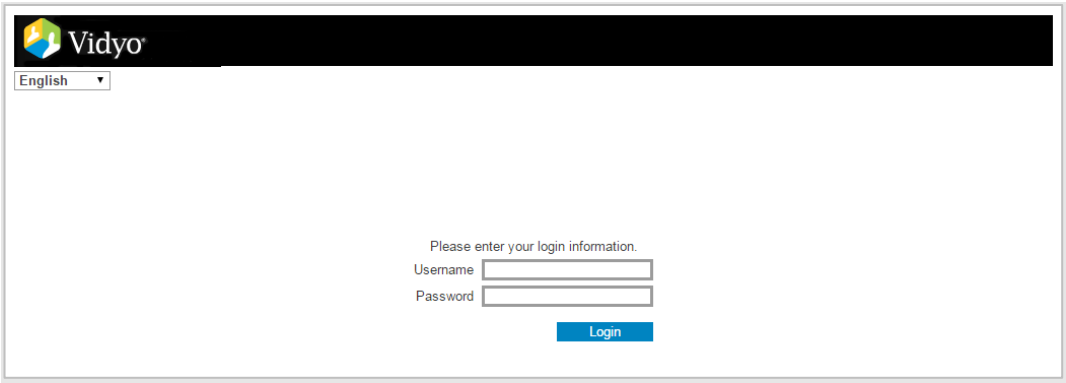
All completed recordings and webcasts are classified at one of three VidyoReplay Library access levels:

- **Private**: Only the user who created the recording or the Super Admin can view it.
- **Organization**: Only the user who created the recording, the Super Admin, or the people within your organization can view it.
- **Public**: Anyone with an invitation can watch the recording. This collection of recordings and webcasts is referred to as the VidyoReplay Public Library and is shown when first accessing VidyoReplay, but before logging in to the system.



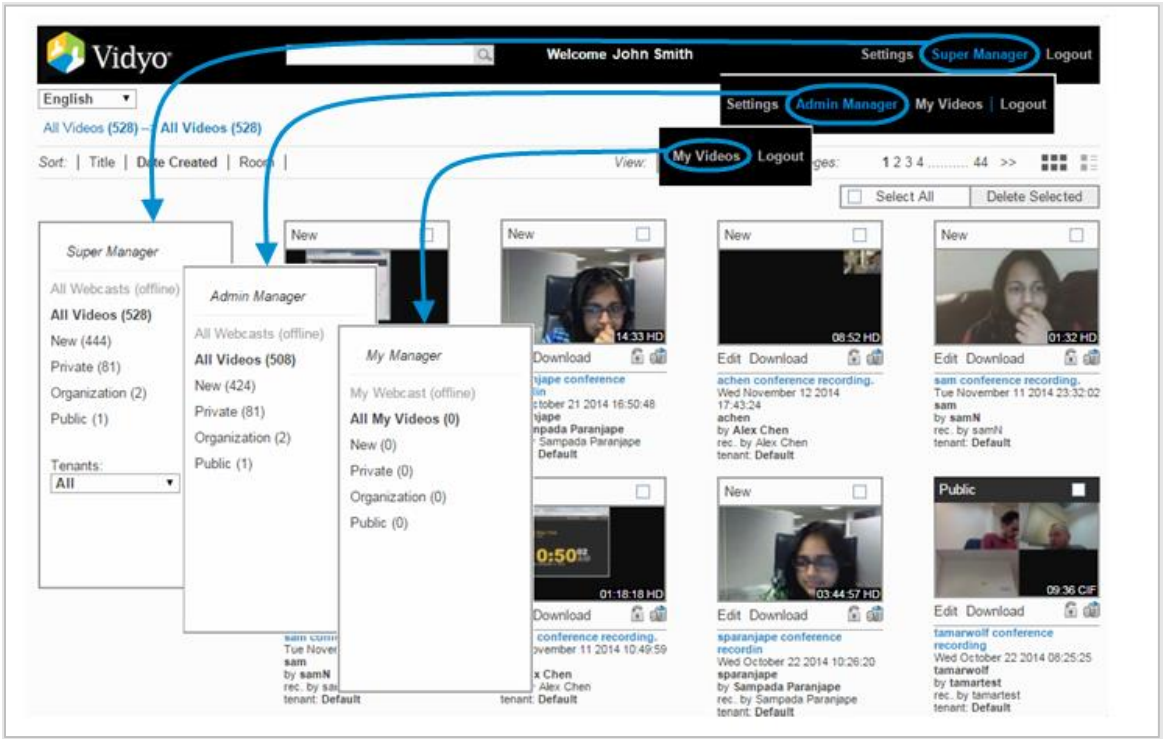
> Note
>
> Only recordings with Public selected as the **Who can watch** option display on this screen. Otherwise a blank login screen displays.

For more information, see Add or edit recording properties.



VidyoReplay Manager access levels

The following screenshot shows the different Manager links (on the upper-right) and the Manager sections of the screen (left) when logging in with Super Manager, Admin Manager, and User accounts:



The functionality of the Managers varies as follows:

- **Super Manager**: All videos marked for Private, Organization, and Public are visible. The Super Manager can also use the Tenants drop-down to filter the results based on a selected tenant.
- **Admin Manager**: Only videos on the Admin Manager's specific tenant that are marked for Private, Organization, and Public are visible.
- **My Manager**: Only videos that are marked for the user as Private, Organization, and Public are visible.

Access your VidyoReplay Library

You can access your VidyoReplay library when creating recordings and webcasts. For details, refer to *Record a meeting* in the *Use VidyoConnect* section of the *Vidyo Help*.

Access your VidyoReplay Manager

To access your VidyoReplay Manager:

1. Log in to the VidyoReplay using the link, username, and password provided by your system administrator.
   - If you are logging in as the Super Manager, see Log in to VidyoReplay.
   - If you are logging in as a Tenant Admin, see Log in as a Tenant Admin.

   Your VidyoReplay Library displays.
2. Click the **Manager** link that displays on the upper-right corner of the screen based on your account. See VidyoReplay Manager access levels.

   Your VidyoReplay Manager displays on the left side of the screen.

8. View and manage recordings and webcasts

The section covers how users view and manage recordings and webcasts from the VidyoReplay Manager.

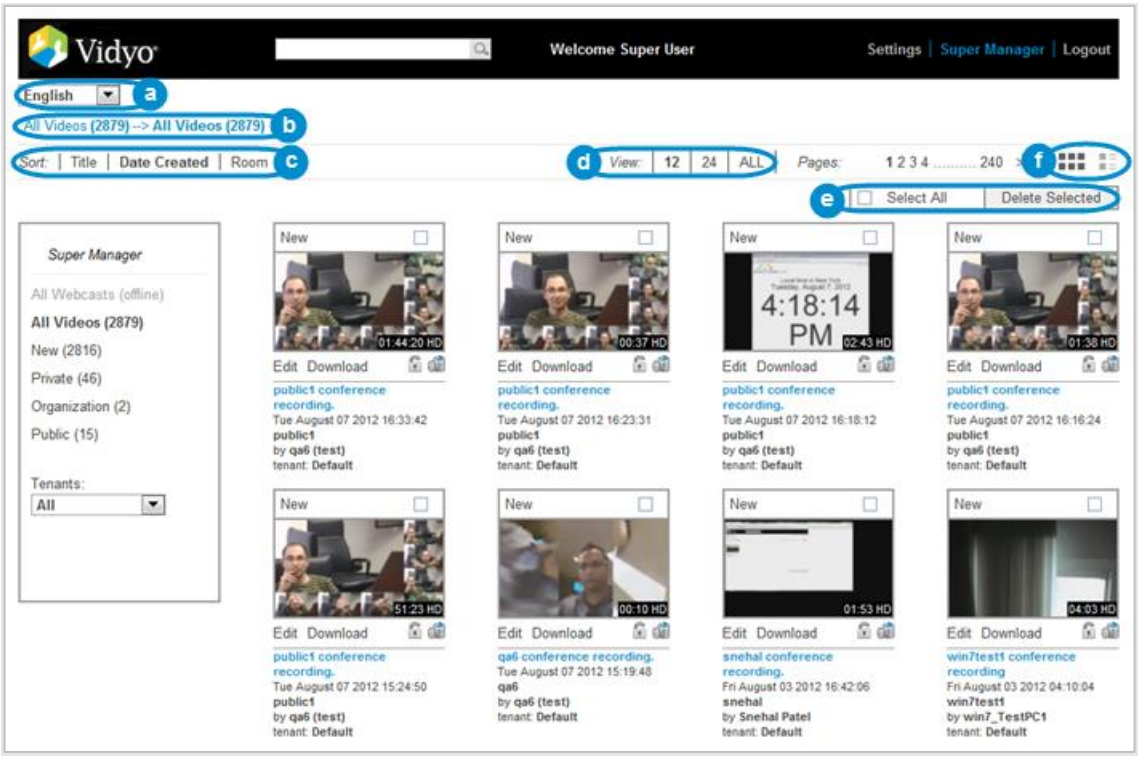
For information about creating recordings and webcasts, refer to *Record a meeting* in the *Use VidyoConnect* section of the *Vidyo Help*.

For information on configuring conference settings, refer to *Configure settings via the Control Meeting page* in the *VidyoPortal and VidyoRouter Administrator Guide.*

Sort, view, and select your recordings

To sort, view, and select your recordings:

1. Access your VidyoReplay Library or VidyoReplay Manager. See Access your VidyoReplay Library or Access your VidyoReplay Manager.
2. From the VidyoReplay Library or Manager, you can sort, view, and select your recordings using the following tools along the top of the screen.



a. Change your language preference by selecting your language of choice from the drop-down box in the upper left-hand corner.

b. You can use the “breadcrumbs” to navigate your VidyoReplay if desired. Breadcrumbs also show total number of recordings and/or webcasts in parenthesis based on selections you make in the VidyoReplay Library or Manager.

c. Sort by Title, Date Created, or the Room from which the recording originated (this is generally the host’s personal room or it could be a VidyoRoom™ appliance, which is typically used in conference rooms).

d. Choose to view 12, 24, or ALL the videos. If all of the videos won’t fit on a single page, you can go to other pages (**1** 2... >>).

e. To delete more than one video at a time, select the checkbox on each video that you want to delete, or use the **Select All** checkbox to select all of your recordings (except ones that are locked) and then click **Delete Selected**.

> Caution
>
> Deleting a video cannot be undone.

Delete locked recordings from the *Cleanup* tab. See Clean up the VidyoReplay Library.

f. Change from grid to list view using the Change Layout buttons.

Use thumbnail recording tools

To use thumbnail recording tools:

1. Access your VidyoReplay Manager.
2. From the VidyoReplay, the following tools are available beneath corresponding thumbnail images of your recordings:

a. The thumbnail banner indicates the **Who can watch** selection for the recording. The options include Public, Organization, and Private. See 7. VidyoReplay Library and Manager access levels and Add or edit recording properties.

b. Click **Edit** to enter or change recording properties. See Add or edit recording properties.

c. Information such as the recording title, date created, and owner of recording display in the lower region.

d. Click **Download** and the recording is automatically downloaded as an **.mp4** (**.m4a** for audio only) file.

e. Use the **Lock**, **Share**, and **Delete** icons as follows:

- Click  to protect your recording from accidental deletion.
- Click  to send a pre-written email message containing the link to the recording in your default email program. There you can address it to as many people as you like, add personalized text, and then send the email to people you wish to view your recorded video.
- Click  to get rid of the recording.

f. The length and resolution of the recording appear on the lower-right corner of the thumbnail.

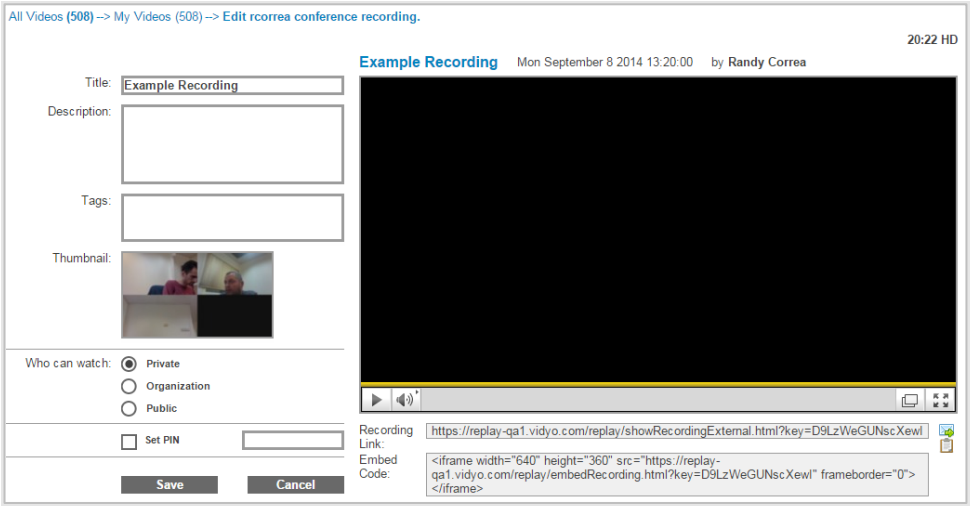
g. Use the thumbnail checkbox to select multiple recordings in the VidyoReplay Manager.

Add or edit recording properties

To add or edit recording properties:

1. Access your VidyoReplay Manager.
2. Click the word **Edit** under the video you wish to edit.

The *Recording Properties* page displays.



By default all of your videos are named "`[your username] conference recording`".

3. In the **Title** field, change the title of your recording, if desired.
4. In the **Description** field, provide a brief description of your recording.
5. In the **Tags** field, enter the words people might use to search for your recording.

   > Note
   >
   > Separate each tag entered by a comma and a space.

6. Select from the following **Who can watch** options:
   - **Private**: Select this option for your recording so it only displays in your VidyoReplay Library and Manager.
   - **Organization**: Select this option if you only want people in your organization (e.g., your company) to see the recording in their VidyoReplay Library and Manager.
   - **Public**: Select this option if you want the recording to display on the VidyoReplay Public Library.

     > Note
     >
     > Only videos with Public selected for this option display in the VidyoReplay Public Library. The VidyoReplay Public Library displays when you access the VidyoReplay, but have not yet logged in to the system. If no recordings have Public selected for this option, a blank login screen displays.
     >
     > For more information, see 7. VidyoReplay Library and Manager access levels and Add or edit recording properties.

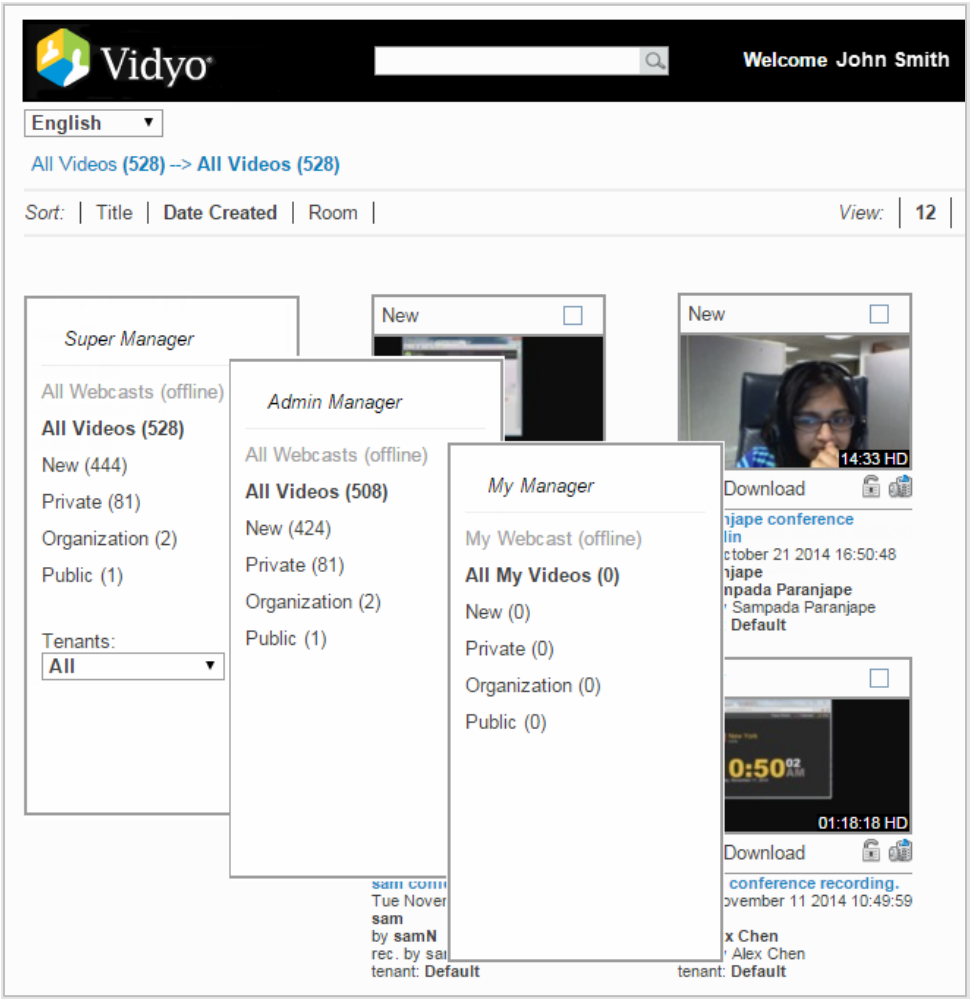
7. For added security, select the **Set PIN** checkbox and enter a PIN code.

   > Note
   >
   > Provide the PIN to users you want to view your recording.

8. Click **Share** to send a pre-written email message containing the link to the recording in your default email program. There you can address it to as many people as you like, add personalized text, and then send the email to people you wish to view your recorded video.
9. Click **Copy** to capture the link to your recording in your clipboard. This link can then be sent via any messaging system.
10. Copy the code that displays in the **Embedded Code** field to embed your recording in a separate webpage of your choice.
11. Click **Save**.

VidyoReplay Manager

Specific VidyoReplay Manager controls display if you access it using a Super, Admin, or User account. See VidyoReplay Manager access levels.



- You can filter by webcasts by clicking All Webcasts while live webcasts are occurring on your VidyoReplay.
- You can filter by All Videos, New, Private, Organization, or Public videos if desired.

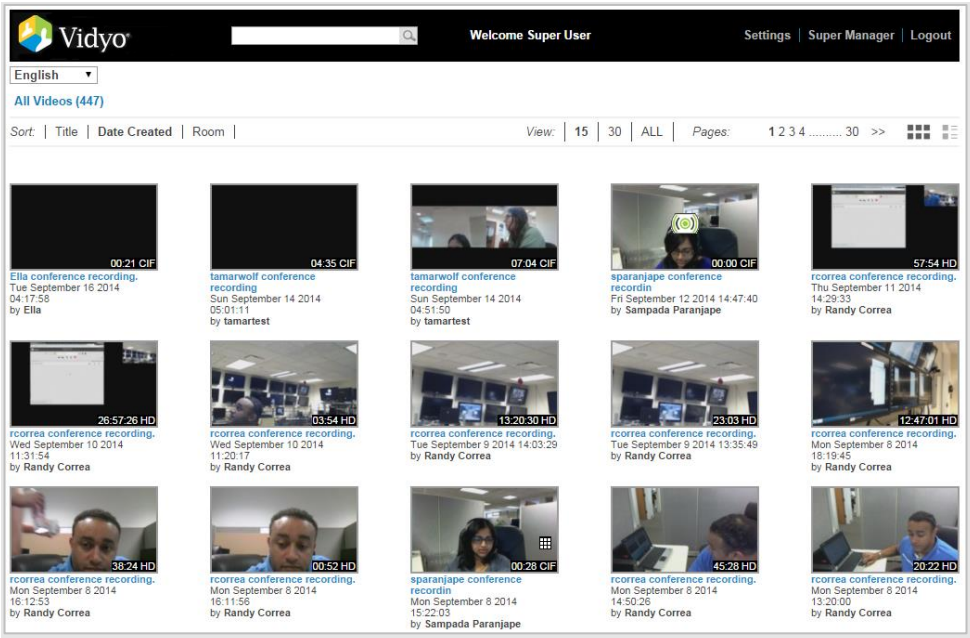
> **Note**
>
> The number in parentheses next to the various options indicates how many recordings match the specific filter.

- The Super Manager can filter results based on a selected tenant. By selecting **Default**, only the videos created by the users that the Default Tenant manages display.

Search for a recording or webcast

To search for a recording or webcast:

1. Access your VidyoReplay Library or VidyoReplay Manager.
2. Type all or part of the title or a tag into the search box at the top of the screen.



3. Click the **Search (** **) icon**.
4. Recording and Webcast results display in the main content part of the screen.

> **Note**
>
> Webcasts display with a flashing green icon in the center of its preview image.

5. Click a Recording or Webcast to access its content.

> **Note**
>
> Recordings or webcasts display in your VidyoReplay Library based on Access Levels. See 7. VidyoReplay Library and Manager access levels.

Appendix A. 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 consider 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-40B	DEV-RM-HD40-B-SA-0A	66,640 hours
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

Product	Part Number	MTBF
VidyoH20 for Google+ Hangouts	DEV-SRV-H20-XL-N3-0A	121,400 hours
VidyoOne	DEV-SRV-ONE-N2-0B	29,900 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