Server Installation Manual

Applies to software release v5.6

Form 8147E • March 2020

Server Installation Manual
Revision af01131 (2020-03-23)

Copyright

3200 Sencore Drive, Sioux Falls, SD USA
`www.sencore.com`

About Sencore

Sencore is an engineering leader in the development of high-quality signal transmission solutions for the broadcast, cable, satellite, IPTV, and telecommunications markets. The company's world-class portfolio includes video delivery products, system monitoring and analysis solutions, and test and measurement equipment, all designed to support system interoperability and backed by best-in-class customer support. Sencore products meet the rapidly changing needs of modern media by ensuring the efficient delivery of high-quality video from the source to the home. More information about Sencore is available at the company's website, `www.sencore.com`.

This product can include software developed by the following people and organizations with the following copyright notices:

Contents

1 INSTALLATION AND ACTIVATION

This manual documents the initial installation procedure for the server-based Sencore VideoBRIDGE software. For details on how to activate and configure the included software products, please refer to the individual User's Manuals.

1.1 First-time Installation

Make sure that the server hardware matches the requirements and then follow the procedure outlined below.

For more details, please refer to the CentOS Linux[1] or Red Hat Enterprise Linux[2] Installation Guide.

1. Obtain the latest installation kickstart image from Sencore.

   Installation media is provided both for CentOS Linux and Red Hat Enterprise Linux. If you install the Red Hat Enterprise Linux version, you will need an active subscription for Red Hat Enterprise Linux server.

2. Insert the installation medium into the server:

   - For DVD-based installations, burn the downloaded ISO image to a DVD and insert into the server.
   - For USB-based installation, transfer the downloaded image to a USB mass storage device using a tool such as **dd** (Mac, Unix, Linux) or **USBWriter**[3] (Windows).
   - For installation in a virtualized environment, attach the downloaded ISO image to a virtual DVD-ROM unit.

     Note: Please read the advice on how to configure the virtual machine in section 1.2 to ensure optimal performance.

3. Boot the server and make sure that the primary boot device is set appropriately. If the system fails to boot from the medium, you may need to configure the boot loader for 'legacy BIOS mode'.

4. The installer will run, please follow the on-screen prompts to install the system, taking note of the following:

[1] `https://docs.centos.org/en-US/centos/install-guide/`

[2] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/index`

[3] `https://sourceforge.net/projects/usbwriter/`

- **IMPORTANT:** Leave 'Software selection' at 'Custom software selected'.
- **IMPORTANT:** In the 'Installation Destination', the default partitioning will create a large `/home` partition, which is unused. To avoid this, use the 'I will configure partitioning' option. Then use the 'Click here to create them automatically' and manually reduce the size of (or remove) the `/home` partition, instead giving that space to the `/` partition. Please refer to the Installation Manual[4] for details on disk partitioning.
- We recommend that you configure network settings (IP address, gateway, DNS) within the installer. Post-installation network configuration can be performed using the **nmtui** utility, please refer to A Appendix: Network configuration for details.
- The default installation does not provide any graphical user interface environment. This can be installed later if desired, please refer to the CentOS Linux[5] or Red Hat Enterprise Linux[6] Installation Guide for more details.

5. At the end of the installation procedure, the server is rebooted. Remove the installation media and ensure that the system boots up properly.

6. If you installed the Red Hat Enterprise Linux server flavor, make sure you follow the instructions on how to subscribe the system to the Red Hat Customer Portal[7].

   If you install the CentOS Linux flavor, you may want to enable the Continuous Release repository[8] to be able to get access to security updates as quickly as possible.

7. Enter the selected IP address in your web browser to access the Software Activation page. If your host is using dynamic addressing, you can log in to the account created during installation and issue the command **ip addr** to display the address assigned to the system.

   Continue to chapter 1.4 for details on how to enable the system.

The kickstart will install CentOS Linux 7 or Red Hat Enterprise Linux 7 on the server. The disks will be formatted and all contents lost. Make sure that any important data on the server has been backed up before beginning the procedure.

1.2 Deploying in a Virtualized Environment

It is also possible to deploy the software in a virtualized environment. For optimal performance, check the processor configuration of **cores per socket** on your host server and use the same configuration setting of cores per virtual sockets on the virtual machine.

[4] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/appe-disk-partitions-overview

[5] https://docs.centos.org/en-US/centos/install-guide/

[6] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/index

[7] https://access.redhat.com/solutions/253273

[8] https://wiki.centos.org/AdditionalResources/Repositories/CR

It is also strongly recommended to configure the data network interface card(s) in **pass-through mode** on the host server. This is required for accurate measurements on the Software Probe.

Please follow the steps from chapter 1.1 when installing the software in the virtualized environment. We recommended **disabling** any 'Easy install' or similarly worded option, and *not* selecting the operating system type when initially creating the new virtual machine instance in your virtualization environment. These options may override the installation instructions included in the provided installation image, causing an incomplete installation.

Pre-built images for VMware (vSphere/Workstation/Player) are provided in `OVA` (Open Virtualization Format Archive) format. These images contains a system already installed according to the steps described in the previous chapter, with VMware Tools already installed and activated.

To deploy the image, you need to import it to the virtualization host, please refer to the documentation of your virtualization environment for more details on how to do this.

If installed in a VMware vSphere environment, the machine should report back its network configuration to the host environment. Please allow some time for it to do so, and then continue with point 6 as described in the previous chapter.

When logging in to the console of the pre-built images, the default password for the **root** user is **elvis**. The same password is also used for logging in remotely using Secure Shell (ssh). **Please change the password for the root user after finishing the install**, log in and use the `passwd` command to do this.

1.3 Maintaining the underlying Operating System

The software installed on the system is using CentOS Linux or Red Hat Enterprise Linux (depending on the installation image used) as its base system. For information on how to maintain the operating system, including how to update it to install security patches, please refer to the Red Hat Enterprise Linux system documentation (this documentation is also valid for CentOS Linux).

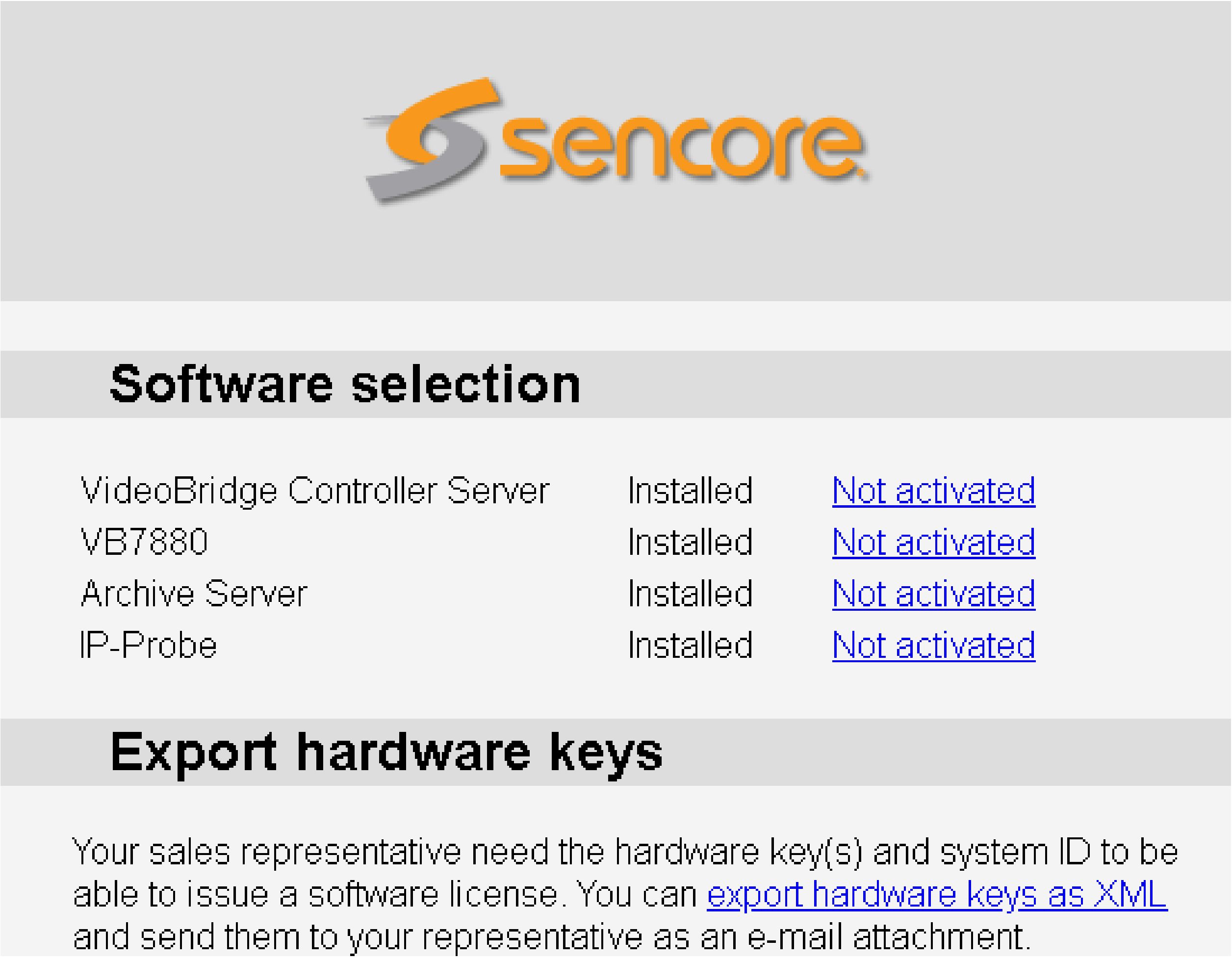
An overview of Red Hat Enterprise system documentation can be found at `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/index.html`

At this point, we recommend you read the *After Installation* chapter of the Installation Guide[9].

1.4 Verifying Correct Initial Setup and Software Activation

Once the software has been installed and restarted all further configuration takes place through the web interface.

[9] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/part-after-installation` (Red Hat)
`https://docs.centos.org/en-US/centos/install-guide/Part_After_Install/` (CentOS)



Software selection

VideoBridge Controller Server	Installed	Not activated
VB7880	Installed	Not activated
Archive Server	Installed	Not activated
IP-Probe	Installed	Not activated

Export hardware keys

Your sales representative need the hardware key(s) and system ID to be able to issue a software license. You can export hardware keys as XML and send them to your representative as an e-mail attachment.

Figure 1.1: Software Activation

1. Launch a web browser application on the management system.

   Any web browser with support for JavaScript can be used to access the Software Activation interface, one of the following are recommended:

   - Google Chrome
   - Mozilla Firefox
   - Microsoft Edge
   - Microsoft Internet Explorer 11 or higher
   - Apple Safari

2. Type the IP address of the server in the browser URL field and press Enter .

   The network settings should have been set when the operating system was installed. If the web browser is unable to reach the web server, check the server's network settings in the operating system.

3. The Software Activation view should be displayed inside the browser. Software Activation is password-protected, the user name is **admin** and the default password is **elvis**. The page displayed should look similar to figure 1.1.

   The password should be changed from the default. Expand the **More options** heading and follow the instructions under **Change password**[10].

4. If you already have an XML file with license keys for your system, click on the **More options** heading and upload this file under the **Import license keys** option. If you have the license key written down or in an e-mail, instead use the product page described below.

5. If this is a new server, and you need to obtain license keys for the purchased products, please click the link labeled **export hardware keys as XML** and send the downloaded file to your sales representative as an e-mail attachment.

6. None of the installed products are activated by default on the newly installed server. To enable one, use the link labeled **Not activated** next to its name. This will take you to a page giving you the details of the installed software, such as the installed version and the hardware key. If you have a license key that you want to enable and have not yet done so, enter the key in the field labeled **Apply license key** and click the **Add license** button.

7. Click the button labeled **Activate software** and wait for it to finish.

   Please note that it may take some additional time before the user interface of the activated product becomes available. If you receive an error trying to access it, please wait for a few minutes before trying again.

   Note that it is not possible to activate the Software Probe and the VB7880 Advanced Content Extractor on a single system at the same time.

By default, all web communication to and from the host running the installed software is using un-encrypted HTTP communication. Please refer to B Appendix: Enabling HTTPS for information on how to enable HTTPS.

It is **strongly recommended** that the system time is configured to be synchronized against an external NTP server. Please refer to C Appendix: Enabling NTP time synchronization for more information on configuring time synchronization.

1.5 Initial Setup Troubleshooting

If you are having trouble bringing up the Software Activation interface:

- Verify that the client machine and the server are configured on the same subnet and that they have different addresses, or, if you use different subnets, verify that the routing and gateways are set correctly on both the client machine and the server.

[10] If you forget the Software Activation password, you can reset it by logging in as root and issuing the command `/opt/btech/ssg/bin/reset_web_password`

- Make sure that the IP address of the gateway and the network interface are not the same.
- Verify that the appropriate Ethernet link indicators of the PC and the server are lit.
- Verify that web browser proxy settings are not interfering.
- Verify that local firewall settings on the PC are not interfering.
- Try rebooting the server and make sure all services start as expected.
- Clear the browser's cache.
- Verify that the web server is running, by entering the command

  ```
  systemctl status httpd
  ```

  on the server's command line. If it is not running properly, or you are seeing **DNS lookup failure** errors, try issuing the command

  ```
  echo "ServerName localhost" >> /etc/httpd/conf/httpd.conf
  ```

  and then restart the server by issuing the command

  ```
  systemctl restart httpd
  ```

Please refer to A Appendix: Network configuration for more information on server network configuration.

1.6 Upgrading From a Previous Version

The kickstart image is only used for first-time installations. For upgrades, please refer to the software documentation for details on how to perform a software upgrade.

If you want or need to re-install the system, please make sure you first make a backup of all the data you want to keep. See the software documentation for more details about how to do a backup. To copy any installed license keys, navigate to the user interface of the installed software, and use the **Export current license and software maintenance keys** link under the **About — License** tab, where available.

The XML file you can download there can be imported from Software Activation by using the procedure described in chapter 1.4.

1.7 Accessing Software Activation interface

To return to the Software Activation view after having activated a product, navigate your web browser to the address `http://<IP>/ssg`, where `<IP>` is the IP address (or host name, if using DNS) of the server. A link to Software Activation is usually available in the user interface under the **About** view.

1.8 Deactivating

To deactivate a product, you must first access the Software Activation interface (see the previous section) and make sure that it is not set to the default. Expand the **More options** heading and change the setting under **Set default software**.

Once this is done, access the user interface and de-activate it from the **About** view.

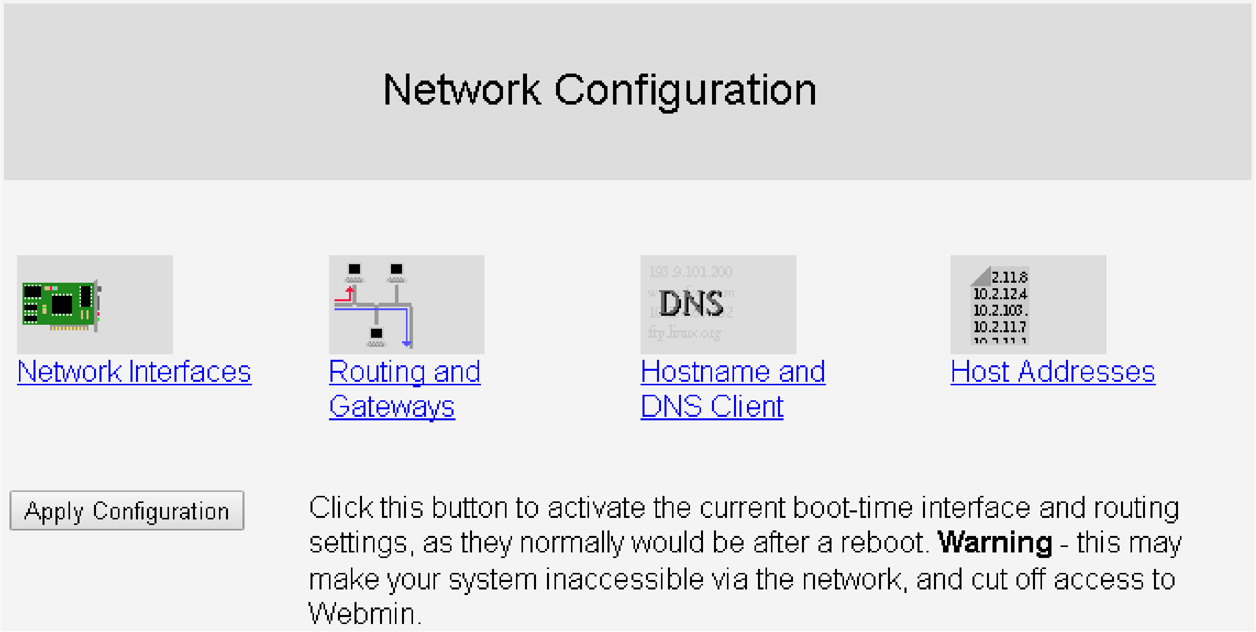
A Appendix: Network configuration

A.1 Web-based configuration

The system ships with a web-based network configuration module. If you are unable to access the system using the web interface, you will need to use the system console. Please see section A.2 for details on how to use the command-line based configuration tool from the console.

To access the web-based configuration module, open the Software Activation interface as described in section 1.4. Click on the **More options** heading and select the **Display and configure the host network configuration** option.

This page displays the current network configuration of the host system. To change the network configuration select the **Change network configuration** option.



Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. **Warning** - this may make your system inaccessible via the network, and cut off access to Webmin.

The web-based network configuration tool is based on WebMin. Further documentation is available in the WebMin documentation[1].

Another alternative is to install the Cockpit web-based interface, which can be used to configure most aspects of the system, including the network settings. Packages for Cockpit are available in the

[1] https://doxfer.webmin.com/Webmin/Network_Configuration

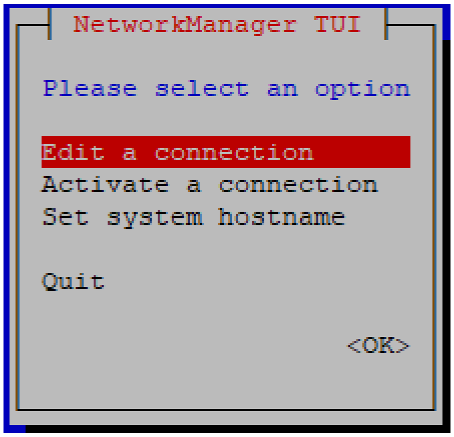
base CentOS/Red Hat Enterprise Linux distribution. For more information on how to install and use Cockpit, please refer to Getting Started With Cockpit[2].

A.2 Command-line based configuration

Changes to network configuration, adding new interface devices and VLANs can be done with the **nmtui** tool. Simply type **nmtui** whilst logged into the server command shell as root[3]. Navigate the nmtui menus using the cursor (arrow) keys and Enter to select. More documentation on using **nmtui** can be found in the Networking Guide[4].

Editing Network interface configuration

To edit a connection first select **Edit a connection** from the nmtui menu:



NetworkManager TUI

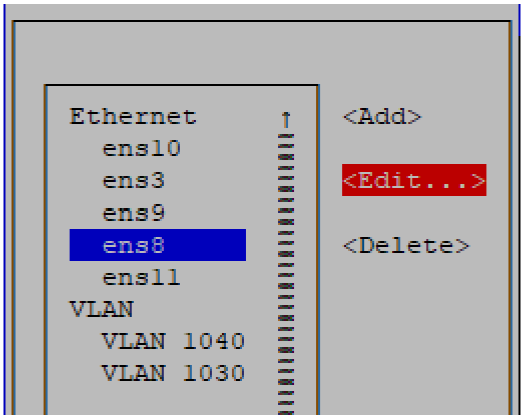
Please select an option

Select the interface to be edited and then select **Edit. . .** from the menu.

[2] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/getting_started_with_cockpit/`

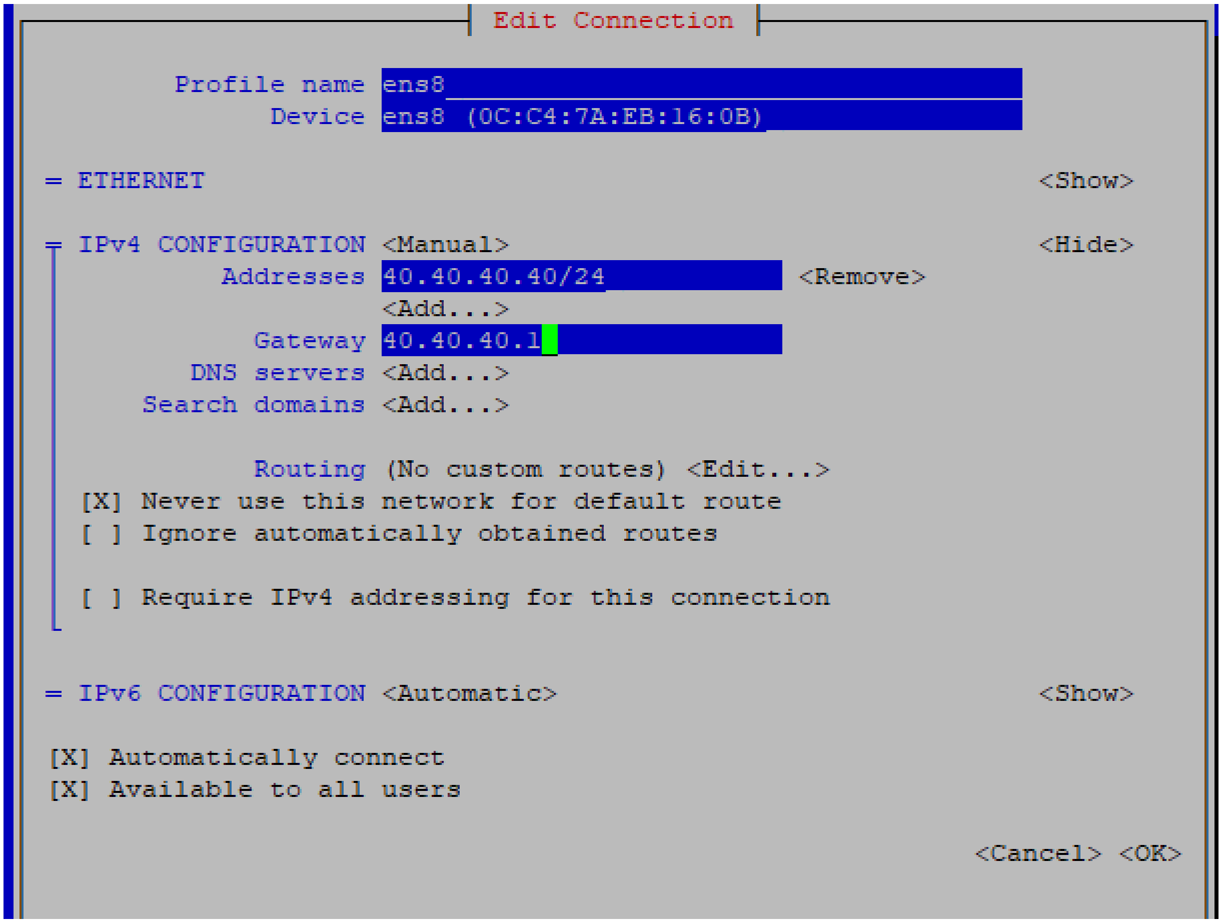
[3] If the **nmtui** tool is not available on your system, you can install it by issuing the command **yum install NetworkManager-tui**

[4] `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/sec-Networking_Config_Using_nmtui.html`



```
Ethernet           ↑   <Add>
   ens10
   ens3                <Edit...>
   ens9
   ens8                <Delete>
   ens11
VLAN
   VLAN 1040
   VLAN 1030
```

Make the necessary changes to IPv4 and IPv6 configuration.



```
                         ┤ Edit Connection ├

           Profile name ens8
                 Device ens8  (0C:C4:7A:EB:16:0B)

═ ETHERNET                                                        <Show>

╤ IPv4 CONFIGURATION <Manual>                                     <Hide>
│          Addresses 40.40.40.40/24            <Remove>
│                    <Add...>
│            Gateway 40.40.40.1
│        DNS servers <Add...>
│     Search domains <Add...>
│
│            Routing (No custom routes) <Edit...>
│ [X] Never use this network for default route
│ [ ] Ignore automatically obtained routes
│
│ [ ] Require IPv4 addressing for this connection
└

═ IPv6 CONFIGURATION <Automatic>                                  <Show>

[X] Automatically connect
[X] Available to all users

                                                            <Cancel> <OK>
```

Selecting **Automatically connect** will ensure the interface is connected next time the system boots.

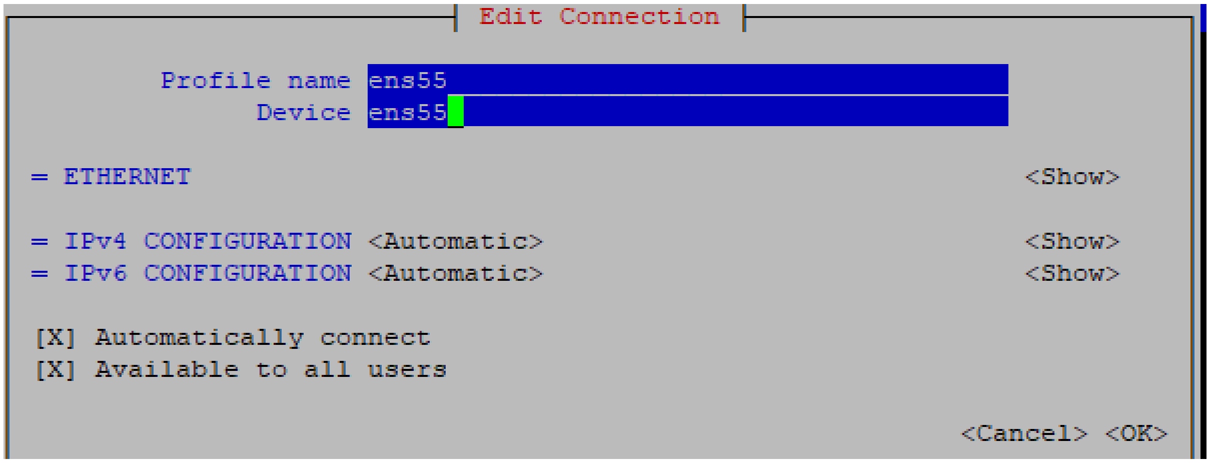
Sometimes it is desirable to select **Never use this interface for default route**, particularly if additional interfaces are only used for monitoring multicast traffic or when setting up a native interface for adding VLANs.

After making changes select **OK** to return the previous menu. Generally, network configuration changes will take effect the next time the interface is activated. This can be done by deactivating and reactivating the interface from the **Activate a connection** menu in nmtui or with the command line **ifdown ifname** followed by **ifup ifname**.

Adding new and VLAN interfaces

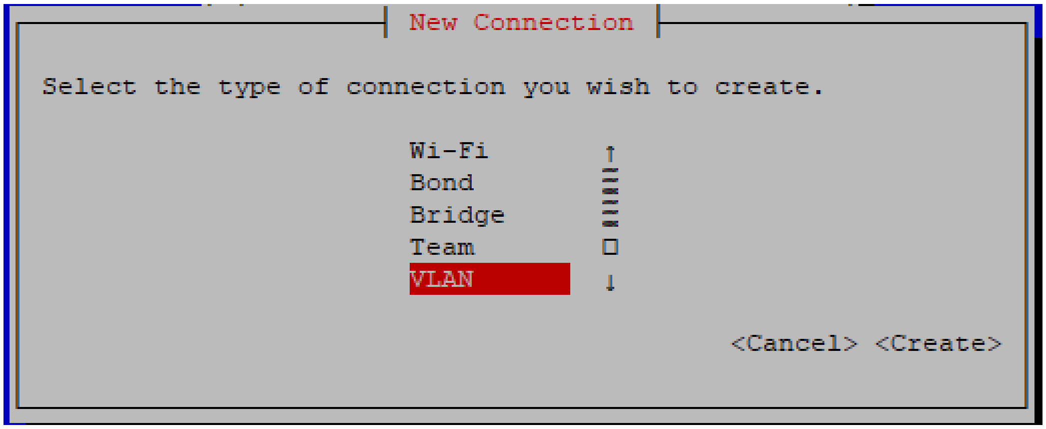
To add a new interface, in the nmtui main menu select **Edit a connection** followed by **Add** and select the interface type from the menu. Typically this is **Ethernet** but may also be used to create VLAN interfaces. Advanced configurations such as Bond and Bridge may be selected if they are required.

To find the system assigned name for a newly added hardware device use the command line **ifconfig** or search in the output of the **dmesg** tool. It can be helpful to keep the nmtui **Profile name** for the device the same as the device name itself, for example:



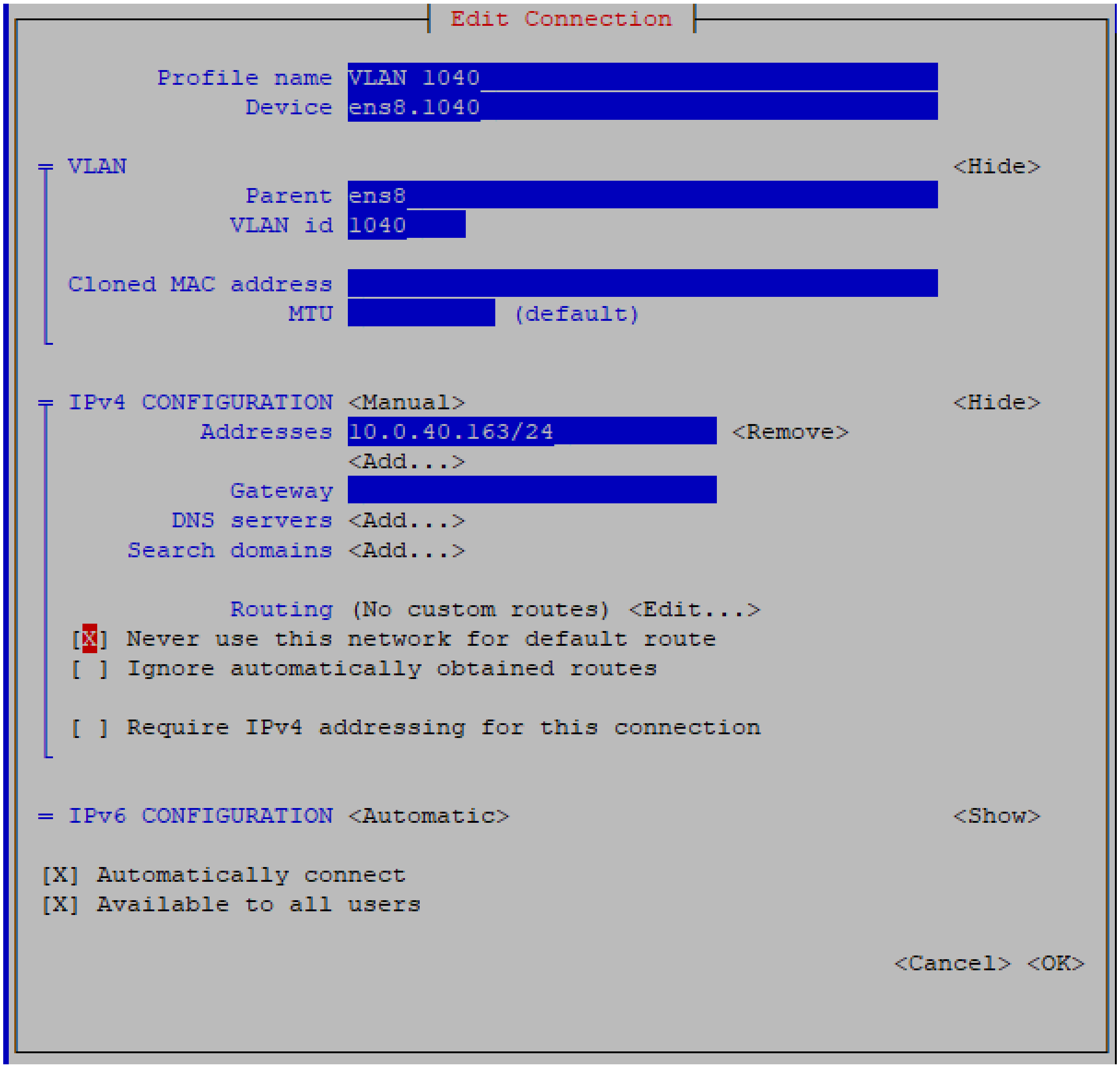
```
                   ┤ Edit Connection ├

        Profile name ens55
              Device ens55

= ETHERNET                                              <Show>

= IPv4 CONFIGURATION <Automatic>                        <Show>
= IPv6 CONFIGURATION <Automatic>                        <Show>

[X] Automatically connect
[X] Available to all users

                                                <Cancel> <OK>
```

To add a VLAN interface from nmtui main menu select **Edit a connection** followed by **Add**. Scroll to the bottom of the list and select VLAN:



```
New Connection

Select the type of connection you wish to create.

        Wi-Fi
        Bond
        Bridge
        Team
        VLAN

                              <Cancel> <Create>
```

Edit the settings for the VLAN interface. The Device field should contain the name of the physical interface to be used for this VLAN and the VLAN number, for example `ens8.1040` means VLAN *1040* on interface *ens8*. The parent and VLAN ID fields should correspond to the values in the name field. In our example *ens8* is the parent and *1040* is the VLAN. Other settings are the same as for normal IPv4/6 interfaces.



```
┌──────────────────────────┤ Edit Connection ├──────────────────────────┐
│                                                                        │
│          Profile name VLAN 1040                                        │
│                Device ens8.1040                                        │
│                                                                        │
│ ╤ VLAN                                                         <Hide>  │
│ │              Parent ens8                                             │
│ │             VLAN id 1040                                             │
│ │                                                                      │
│ │ Cloned MAC address                                                   │
│ │                MTU          (default)                                │
│ └                                                                      │
│                                                                        │
│ ╤ IPv4 CONFIGURATION <Manual>                                  <Hide>  │
│ │           Addresses 10.0.40.163/24            <Remove>               │
│ │                     <Add...>                                         │
│ │             Gateway                                                  │
│ │         DNS servers <Add...>                                         │
│ │      Search domains <Add...>                                         │
│ │                                                                      │
│ │             Routing (No custom routes) <Edit...>                     │
│ │ [X] Never use this network for default route                         │
│ │ [ ] Ignore automatically obtained routes                             │
│ │                                                                      │
│ │ [ ] Require IPv4 addressing for this connection                      │
│ └                                                                      │
│                                                                        │
│ ═ IPv6 CONFIGURATION <Automatic>                               <Show>  │
│                                                                        │
│ [X] Automatically connect                                              │
│ [X] Available to all users                                             │
│                                                                        │
│                                                        <Cancel> <OK>   │
│                                                                        │
└────────────────────────────────────────────────────────────────────────┘
```

After entering the configuration for the VLAN interface select **OK** to return the previous menu, then select **Back** and finally **Activate a connection** to activate the newly created VLAN interface.

B Appendix: Enabling HTTPS

By default, all web communication to and from the host running the installed software is using un-encrypted HTTP communication. To enable HTTPS, the installed Apache server software needs to be configured appropriately.

The guide below is based on the guide from the CentOS Wiki[1]. To install packages, generate keys and update the Apache configuration, you will need to be root so you can either **su** to root or use **sudo** in front of the commands below.

If the system is available on a publicly visible host name, you can use EFF's Certbot to deploy a Let's Encrypt certificate. Please see the section **Using Certbot with Let's Encrypt** below.

Installing packages requires an active Internet connection. If you are using Red Hat Enterprise Linux, you will need an active subscription to install packages.

Getting the required software

To enable SSL on Apache, you will need to install the `mod_ssl` package, if not installed already. To install the package, issue the following command:

```
yum install mod_ssl
```

Generating a certificate

If you have an internal certificate authority, use that to create a certificate. Otherwise follow the steps below to generate a self-signed certificate. Please note that modern browsers display a warning message when connecting to a web server running a self-signed certificate. This message can usually be suppressed by installing the certificate in the browser.

First generate a private key, which we call **ca.key**:

```
openssl genrsa -out ca.key 2048
```

Second, create a certificate signing request (CSR) in **ca.csr**:

```
openssl req -new -key ca.key -out ca.csr
```

[1] `https://wiki.centos.org/HowTos/Https`

Third, we self-sign the key:

```
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
```

We now have the necessary files, but we need to copy them to the correct locations in the file system:

```
cp ca.crt /etc/pki/tls/certs
cp ca.key /etc/pki/tls/private/ca.key
cp ca.csr /etc/pki/tls/private/ca.csr
```

Configuring the web server

The Apache SSL configuration file, **/etc/httpd/conf.d/ssl.conf**, needs to be updated to make use of the generated certificate. Open it using a text editor, for example:

```
vi +/SSLCertificateFile /etc/httpd/conf.d/ssl.conf
```

Change the paths to match where the Key file (**ca.crt**) and Certificate Key (**ca.key**) are stored. If you've used the method above, the configuration should be:

```
SSLCertificateFile /etc/pki/tls/certs/ca.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
```

We also need to forward the configuration from the HTTP host to the HTTPS host. This is done by adding the following line anywhere in the `VirtualHost` declaration in the **ssl.conf** file, you can for instance add this next to the lines above:

```
RewriteOptions Inherit
```

Quit and save the file and then restart Apache by issuing the command

```
systemctl restart httpd
```

All being well you should now be able to connect to the system using HTTPS. If there was an error, the command output should give you some hints on where to look.

Disabling HTTP access

To configure the server to redirect any access arriving over HTTP to the HTTPS server, the simplest way is to create the file `/etc/httpd/conf.d/001-http-to-https.conf`[2]:

```
cat <<'EOM' > /etc/httpd/conf.d/001-http-to-https.conf
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L,NE]
EOM
```

After creating the file, restart Apache by issuing the command

```
systemctl restart httpd
```

If this does not work, please consult the Apache documentation or the Apache Wiki[3]. It is also possible to completely disable the HTTP port, if it is not needed.

Using Certbot with Let's Encrypt

If the system is available on a publicly visible host name, you can use EFF's Certbot to deploy a Let's Encrypt certificate. Some preparations are needed before running Certbot.

To enable SSL on Apache, you will need to install the `mod_ssl` package, if not installed already. To install the package, issue the following command:

```
yum install mod_ssl
```

Next, we need to configure Apache *VirtualHost* configurations for HTTP and HTTPS. The HTTPS one is configured in the Apache SSL configuration file, **/etc/httpd/conf.d/ssl.conf**, and needs to be updated slightly:

Open it using a text editor, for example:

```
vi +/VirtualHost /etc/httpd/conf.d/ssl.conf
```

Add the following line after the `<VirtualHost _default_:443>` line:

[2] `https://wiki.apache.org/httpd/RewriteHTTPToHTTPS`

[3] `https://wiki.apache.org/httpd/RedirectSSL`

```
RewriteOptions Inherit
```

Finally, we need to create a VirtualHost for the HTTP part, this one is kept simple and can be created by issuing the following command:

```
cat <<'EOM' > /etc/httpd/conf.d/002-http-virtualhost.conf
<VirtualHost _default_:80>
RewriteOptions Inherit
</VirtualHost>
EOM
```

Now the configuration should be ready for adding the Let's Encrypt certificate. Please follow the Certbot guide[4] for information on how to do that.

[4] https://certbot.eff.org/lets-encrypt/centosrhel7-apache

C Appendix: Enabling NTP time synchronization

It is strongly recommended that the server running the Sencore VideoBRIDGE software be synchronized against an external NTP server.

If not set up correctly, alarms may be displayed with incorrect timestamps and out out alignment with other monitoring devices in the system.

NTP synchronization against public servers on the Internet is usually enabled automatically if they were detected during the operating system installation. It is possible to change the servers to use, for instance to set it to use a local NTP server, by changing the configuration in the file `/etc/chrony.conf` manually.

The VideoBRIDGE Controller will also act as NTP server, if available. Please refer to the individual User's Manuals for information on how to set up the Sencore VideoBRIDGE software and hardware to synchronize towards the VBC server.

For more details on configuring the date and time settings, please refer to the System Administrator's Guide, chapters *Configuring the Date and Time*[1] and *Using chrony*[2].

[1] `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/chap-Configuring_the_Date_and_Time.html`

[2] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-using_chrony`