



HAIVISION

Haivision EMS 1.0
User's Guide

HVS-ID-UG-EMS-10, Issue 01

Edition Notice

© 2015-2023 Haivision. All rights reserved.

This edition and the products it describes contain proprietary and confidential information. No part of this content may be copied, photocopied, reproduced, translated or reduced to any electronic or machine-readable format without prior written permission of Haivision. If this content is distributed with software that includes an end-user agreement, this content and the software described in it, are furnished under license and may be used or copied only in accordance with the terms of that license. Except as permitted by any such license, no part of this content may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Haivision Systems, Inc. Please note that the content is protected under copyright law even if it is not distributed with software that includes an end-user license agreement.

About Haivision

Founded in 2004, Haivision is now a market leader in enterprise video and video streaming technologies. We help the world's top organizations communicate, collaborate and educate. Recognized as one of the most influential companies in video by Streaming Media and one of the fastest growing companies by Deloitte's Technology Fast 500, organizations big and small rely on Haivision solutions to deliver video. Headquartered in Montreal, Canada, and Chicago, USA, we support our global customers with regional offices located throughout the United States, Europe, Asia and South America.

Trademarks

The Haivision logo, Haivision, and certain other marks are trademarks of Haivision. CoolSign is a registered trademark licensed to Haivision Systems, Inc. All other brand or product names identified in this document are trademarks or registered trademarks of their respective companies or organizations.

Disclaimer

The information contained herein is subject to change without notice. Haivision assumes no responsibility for any damages arising from the use of this content, including but not limited to, lost revenue, lost data, claims by third parties, or other damages.

If you have comments or suggestions, please contact infodev@haivision.com.

While every effort has been made to provide accurate and timely information regarding this product and its use, Haivision Systems Inc. shall not be liable for errors or omissions contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Contents

- Edition Notice** **2**
 - About Haivision2
 - Trademarks2
 - Disclaimer2
- Contents** **3**
- About This Document** **5**
 - Conventions5
 - Typographic Conventions and Elements5
 - Action Alerts.....5
 - Obtaining Documentation.....6
 - Getting Service Support6
- Introduction** **8**
 - Haivision EMS Overview8
 - Product Features8
 - Physical Description (Servers)9
- Getting Started** **10**
 - Accessing the EMS Web Interface.....10
 - SSL Encryption13
 - Changing the Default Password13
 - Navigating the Web Interface14
 - The Product Banner.....16
 - Modifying the IP Address17
- Using EMS** **19**
 - Pairing a Makito X Device.....19
 - Device Summaries.....22
 - Organizing and Identifying Devices23
 - Custom Names and Descriptions23
 - Labeling Devices.....24
 - Searching and Filtering Devices26
 - Upgrading Device Firmware28
 - Rebooting and Unpairing Devices31
- Managing System Settings** **34**
 - Managing Certificates34
 - Generating a Certificate Signing Request (CSR)35
 - Importing and Activating a Certificate (CRT).....36
 - Generating a Private Key37
 - Importing a Private Key37
 - Certificate Settings38
 - Managing Licenses40
 - Configuring Network Settings.....41
 - Network Settings44
 - Managing Security.....46
 - Security Settings.....48
 - Installing System Updates.....50
- Reporting** **52**
 - Viewing Reports.....52

System Logs	52
Viewing System Activity.....	53
Warranties	55
1-Year Limited Hardware Warranty.....	55
EXCLUSIONS AND LIMITATIONS	55
OBTAINING WARRANTY SERVICE.....	56
APPLICABLE LAW	56
EULA - End User License Agreement.....	57
READ BEFORE USING	57
SLA - Service Level Agreement.....	57
1. Introduction.....	57
2. Definitions	57
3. Service Levels for the Video Content Management System.....	57
4. Exceptions to Availability for the VCMS	58
5. Credits for Downtime for the VCMS.....	59
6. Support Services for the VCMS	59
7. Service Levels for Haivision Streaming Media Service	60
8. Credits for Outages of Haivision Streaming Media Service.....	60
9. No Secondary End User Support	60
Getting Help	61

About This Document

Conventions


The following conventions are used to help clarify the content.

Typographic Conventions and Elements


<i>Italics</i>	Used for the introduction of new terminology, for words being used in a different context, and for placeholder or variable text.
bold	Used for strong emphasis and items that you click, such as buttons.
Monospaced	Used for code examples, command names, options, responses, error messages, and to indicate text that you enter.
>	In addition to a math symbol, it is used to indicate a submenu. For instance, File > New where you would select the New option from the File menu.
...	Indicates that text is being omitted for brevity.

Action Alerts


The following alerts are used to advise and counsel that special actions should be taken.

 **Tip**

Indicates highlights, suggestions, or helpful hints.

 **Note**

Indicates a note containing special instructions or information that may apply only in special cases.

 **Important**

Indicates an emphasized note. It provides information that you should be particularly aware of in order to complete a task and that should not be disregarded. This alert is typically used to prevent loss of data.

⚠ Caution

Indicates a potentially hazardous situation which, if not avoided, may result in damage to data or equipment. It may also be used to alert against unsafe practices.

⚠ Warning

Indicates a potentially hazardous situation that may result in physical harm to the user.

Obtaining Documentation

This document was generated from the Haivision InfoCenter. To ensure you are reading the most up-to-date version of this content, access the documentation online at <https://doc.haivision.com>. You may generate a PDF at any time of the current content. See the footer of the page for the date it was generated.

Getting Service Support

For more information regarding service programs, training courses, or for assistance with your support requirements, contact Haivision Technical Support using our Support Portal at: <https://support.haivision.com>.

This guide explains how to configure and use Haivision Element Management System (EMS) to remotely discover and manage Haivision Makito X devices.

Introduction

This section provides an overview of EMS, along with a description of the main hardware components and key features.

Topics Discussed

- [Haivision EMS Overview](#)
 - [Product Features](#)
- [Physical Description \(Servers\)](#)

Haivision EMS Overview

Haivision Entity Management System (EMS) is a platform for remotely discovering and managing deployments of Haivision devices.

In the 1.0 release, EMS offers management solutions for Makito X devices. For information on installing, configuring, and managing Makito X devices, please refer to the Makito user documents in the [Haivision InfoCenter](#).

For information on server appliances, see [Physical Description \(Servers\)](#).

Topics Discussed

- [Product Features](#)

Product Features

Key Haivision EMS features include the following:

Discovery and Management

- Discover Haivision Makito X devices on your local network.
- Pair Makito X devices with EMS for robust and secure bidirectional communication.
- Remotely manage multiple devices through one centralized interface.

Organize, Sort, Filter

- Create custom labels to group and organize devices.
- View device status at a glance.
- Search and filter devices.

Detailed Device Information

Device properties such as serial number, uptime, IP address, and more are all viewable from a single interface.

Firmware Upgrade Management

- Device's firmware can be uploaded onto EMS as a central repository.
- Push and apply new firmware simultaneously on devices from a central interface.

Physical Description (Servers)

Your EMS server comes delivered as an enterprise-ready, ultra-compact 1RU appliance made for single-tier architectures.



EMS servers provide two 1 Gb Ethernet (GbE) Network Interface Card (NIC) ports for both traffic and management.

Note

For the system interfaces and LED status indicators, as well as instructions to install and connect to your server, please refer to the [Server Quick Start Guide](#).

Getting Started

! Important

Before proceeding, make sure that the appliance is set up correctly and all necessary network connections are established.

For information on installing and connecting to a physical EMS server, please refer to the [Server Quick Start Guide](#). To install and connect to an EMS virtual machine, refer to the [VMWare Quick Start Guide](#).

Topics Discussed

- [Accessing the EMS Web Interface](#)
 - [SSL Encryption](#)
- [Changing the Default Password](#)
- [Navigating the Web Interface](#)
 - [The Product Banner](#)
- [Modifying the IP Address](#)

Accessing the EMS Web Interface

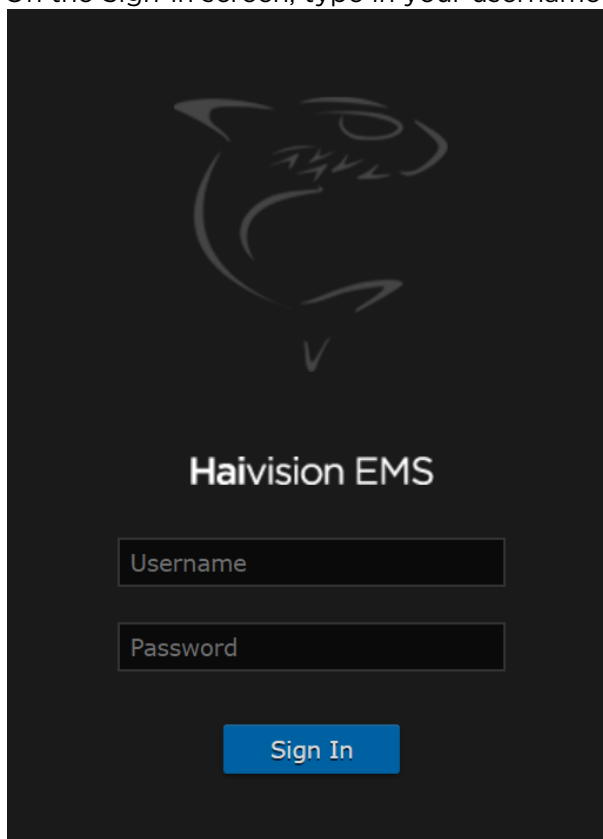
i Note

The URL or IP address as well as your username and initial password are needed to access EMS. To change your password, see [Changing the Default Password](#).

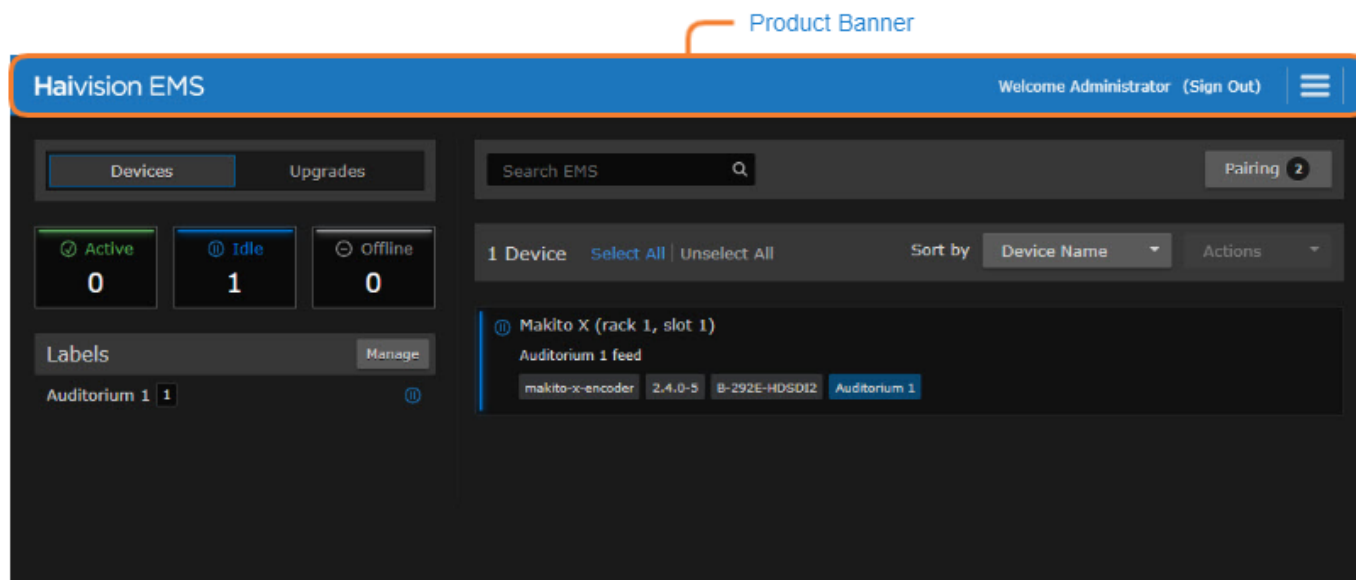
Open a Web browser of your choice, such as Chrome, Firefox, Safari, Microsoft Edge, or Internet Explorer (IE11). To access the Haivision EMS web interface:

1. Type the URL or IP address for EMS in the browser's address and press **Enter**.

2. On the Sign-in screen, type in your username and password and click **Sign In** (or press Enter).



Once you have signed in, the Web interface opens with your account information displayed in the product banner.



⚠ Caution

For security purposes, Haivision strongly advises you to change the default passwords during initial configuration.

! Important

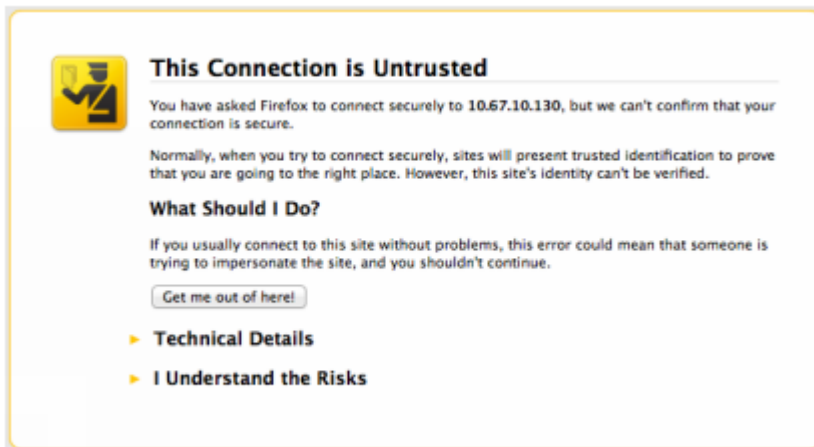
haiadmin is a special "system user" intended primarily for initial setup and system troubleshooting. It is not intended for regular use because it has unrestricted access privileges that cannot be changed. For day-to-day system control and administration, you are strongly advised to create a regular administrative user with a secure password.

To change the current user password, click the username on the banner (next to "Welcome"). For details, see [Changing the Default Password](#).

SSL Encryption

EMS is encrypted to provide secure interactions with your devices. When you sign into the EMS interface, you are automatically redirected to the secure HTTP (HTTPS) site using port 443. When a browser accesses the website, it requests the security certificate to confirm that the site is trusted.

EMS ships with a self-signed Secure Sockets Layer (SSL) certificate key set which works with any configured server hostname. However, web browsers do not consider self-signed certificates to be trusted, because they are not signed by a Certificate Authority. Consequently, when accessing the website with a self-signed certificate, users see a security warning and are prompted for authorization as shown in the example below.



Supplying EMS with an SSL security certificate eliminates the security warning, provides a means for users to verify a website, and ensures that the connection is secure. See [Managing Certificates](#) for more details.

Note

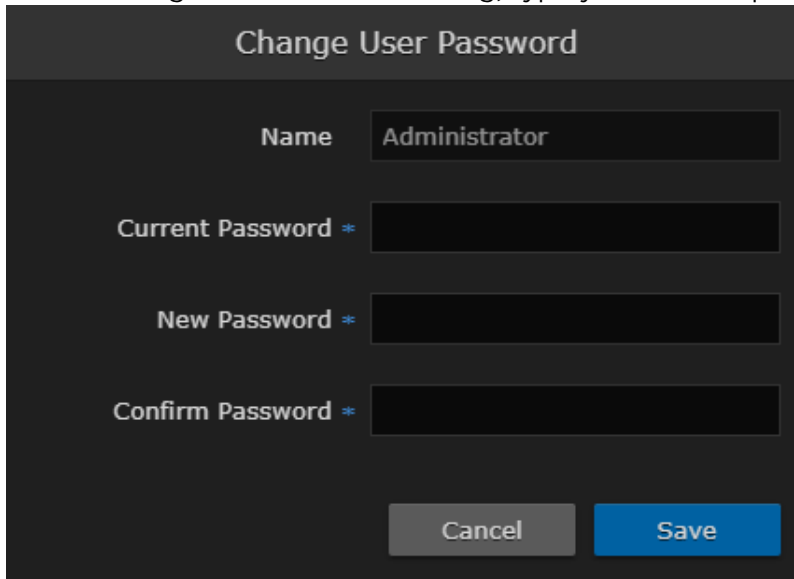
Recent OS updates (particularly MacOS 10.15 and iOS 13, see <https://support.apple.com/en-us/HT210176>) block access to websites with TLS certificates that have a validity window of more than 825 days. Any custom certificate installed should have a validity window of less than 825 days in order to be supported on macOS. Haivision recommends using CA-signed certificates for production systems.

Changing the Default Password

To change the password for the current user:

1. Click the username (e.g., Administrator) on the toolbar (next to "Welcome").

2. On the Change User Password dialog, type your current password in the Current Password field.

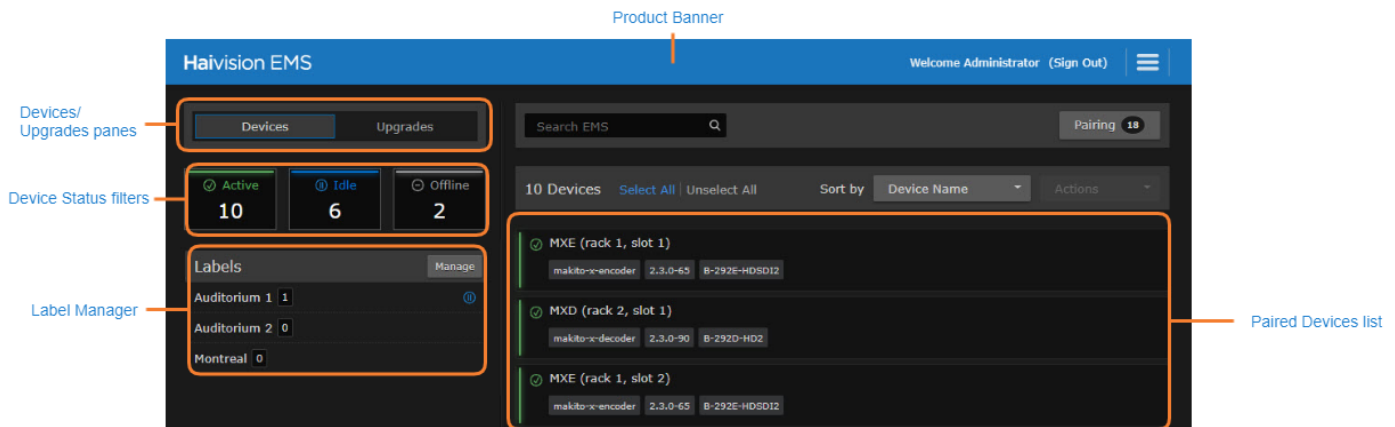


3. Type the new password in the New Password field and again in the Retype Password field.
 4. Click **Save**.

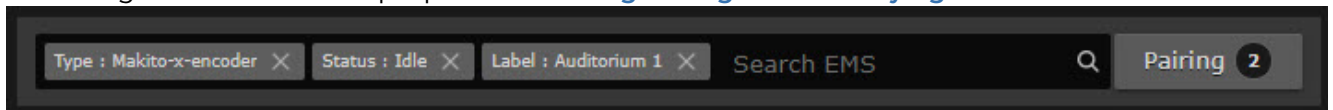
The password change will take effect immediately.

Navigating the Web Interface

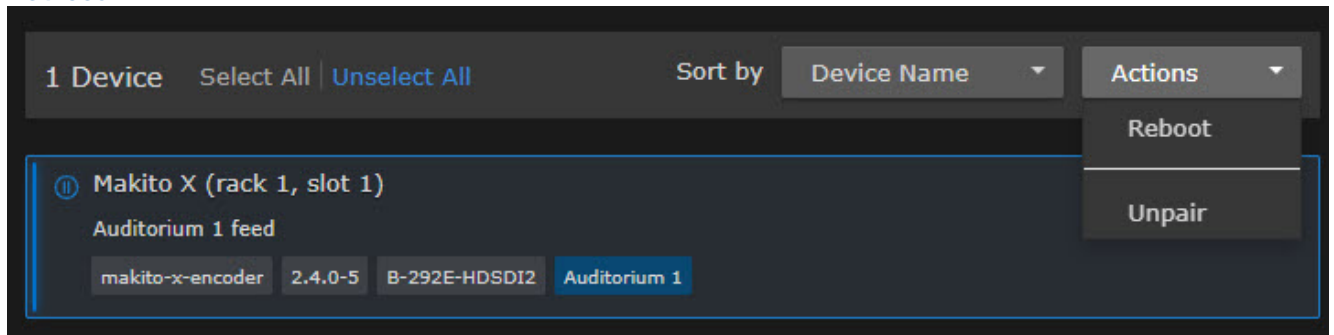
After logging in, the EMS web interface opens to the main screen and shows the Devices pane.



- The product banner includes links for managing and navigating EMS. See [The Product Banner](#).
- When a new device is paired with EMS, it will appear in the device list. See [Pairing a Makito X Device](#).
- The device list can be switched between Device mode and Upgrade mode. In Upgrade mode, devices can be selected for firmware updates. See [Upgrading Device Firmware](#).
- The Search bar, Device Status filters, and Label Manager can be used to filter the device list according to various device properties. See [Organizing and Identifying Devices](#).



- Selecting a device makes the More Actions drop-down menu available. The More Actions menu provides options for rebooting or unpairing devices from EMS. See [Rebooting and Unpairing Devices](#).

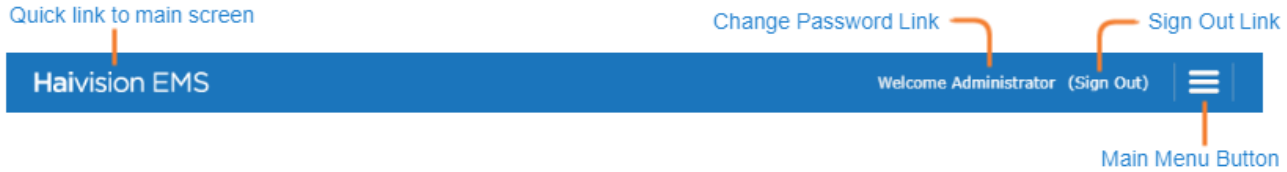


Related Topics

- [The Product Banner](#)

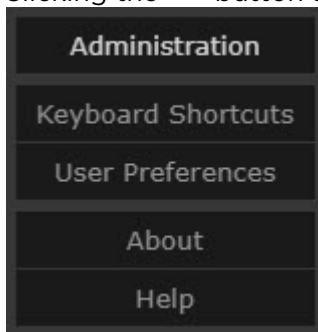
The Product Banner

All screens on the EMS web interface include the product banner, shown below.

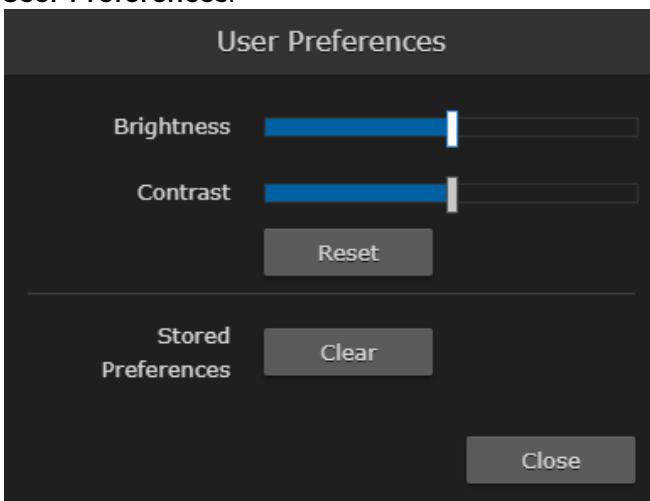


The following options are available from the product banner:

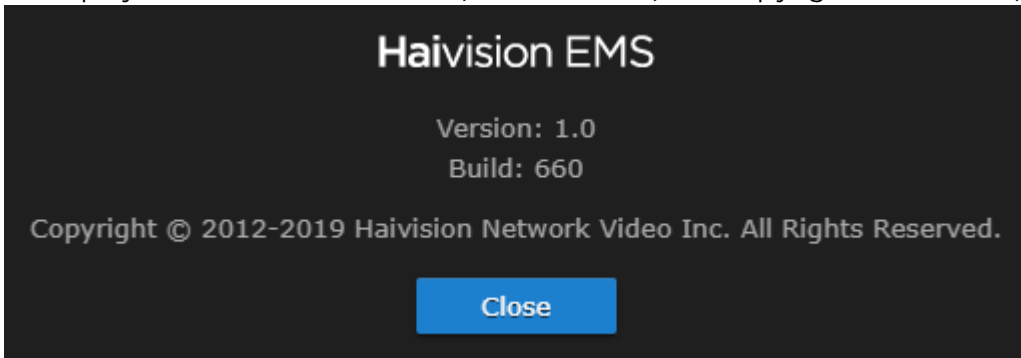
- To access the home screen from anywhere within the web interface, click on the Haivision EMS logo.
- To change your password, click on your username.
- To sign out of the web interface, click the **Sign Out** link.
- Clicking the **☰** button allows you to access other pages or options within the interface.



- Select **Administration** to configure and manage EMS. See [Managing System Settings](#) for details regarding the various administration pages.
- To view a list of shortcuts relevant to the page you are currently browsing, select **Keyboard Shortcuts** (or press the ? key).
- To adjust the brightness and contrast or reset the EMS stored preferences in your browser, select **User Preferences**.



- To display the current EMS version, build number, and copyright information, select **About**.



- To open the Haivision InfoCenter website that contains the EMS documentation, select **Help**.

Tip

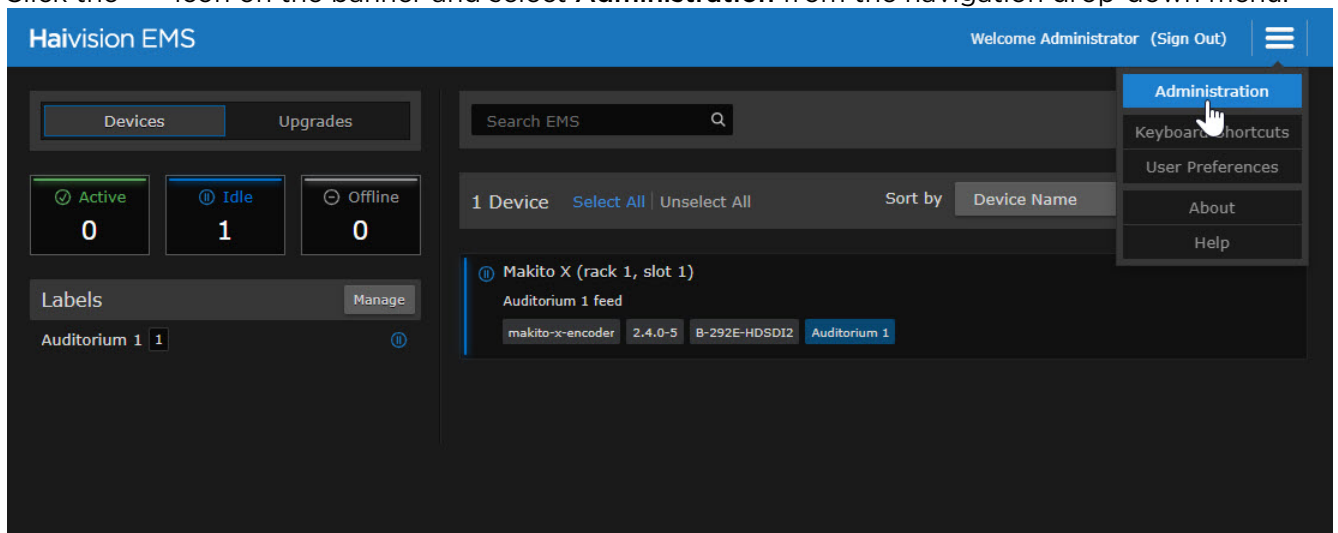
If your device does not have access to the Internet, a bundled version of the documentation opens in your browser. However, always visit the [Haivision InfoCenter](#) for the most up-to-date information.

Modifying the IP Address

Tip

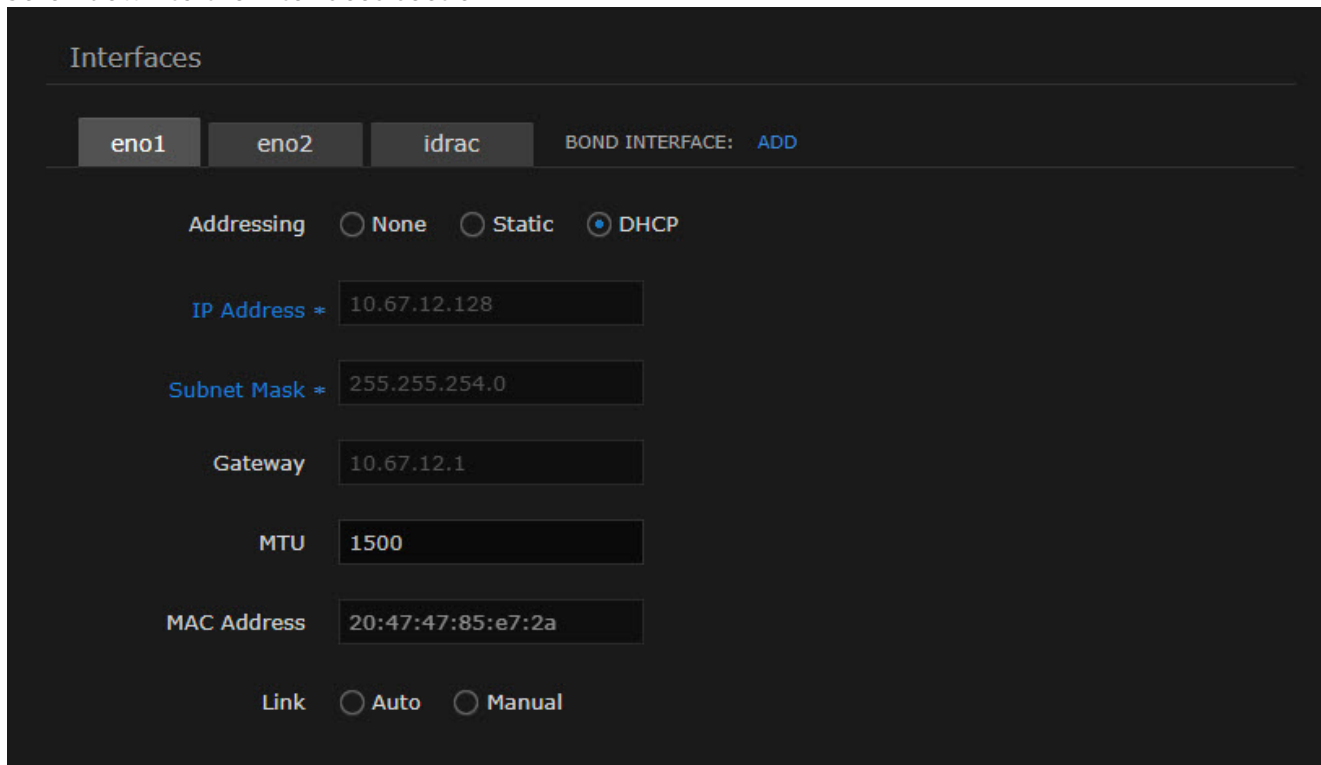
You can also modify network settings by connecting directly to the Console UI. To do so, connect a keyboard and monitor to the server (refer to the [Server Quick Start Guide](#)). You can also access the Console UI remotely using a secure shell (SSH) connection. For more information, see [Using the Console UI with Haivision Hardware](#).

- Click the  icon on the banner and select **Administration** from the navigation drop-down menu.



- On the Administration page, click **System Settings** on the toolbar and then click **Network** on the sidebar.

3. Scroll down to the Interfaces section.



The screenshot shows the 'Interfaces' configuration page in HAIVISION. At the top, there are tabs for 'eno1', 'eno2', and 'idrac'. To the right, it says 'BOND INTERFACE: ADD'. Below the tabs, the 'Addressing' section has three radio buttons: 'None', 'Static', and 'DHCP' (which is selected). Below this are input fields for 'IP Address *' (10.67.12.128), 'Subnet Mask *' (255.255.254.0), 'Gateway' (10.67.12.1), 'MTU' (1500), and 'MAC Address' (20:47:47:85:e7:2a). At the bottom, the 'Link' section has two radio buttons: 'Auto' and 'Manual'.

4. On the Network Configuration page, for the first network interface (`eno1` in the above example), either:
- Select DHCP to enable Dynamic Host Configuration Protocol,
-or-
 - Enter a valid IP address, subnet mask, and gateway to work in your environment.
5. Click **Save Settings**, and then click **Reboot**.
6. After the system has rebooted, sign in again to continue.

Using EMS

Note

Makito X must be properly configured for management through the EMS interface. For information on configuring Makito X devices, please refer to the relevant user documents on the [Haivision InfoCenter](#).

Topics Discussed

- [Pairing a Makito X Device](#)
- [Device Summaries](#)
- [Organizing and Identifying Devices](#)
 - [Custom Names and Descriptions](#)
 - [Labeling Devices](#)
 - [Searching and Filtering Devices](#)
- [Upgrading Device Firmware](#)
- [Rebooting and Unpairing Devices](#)

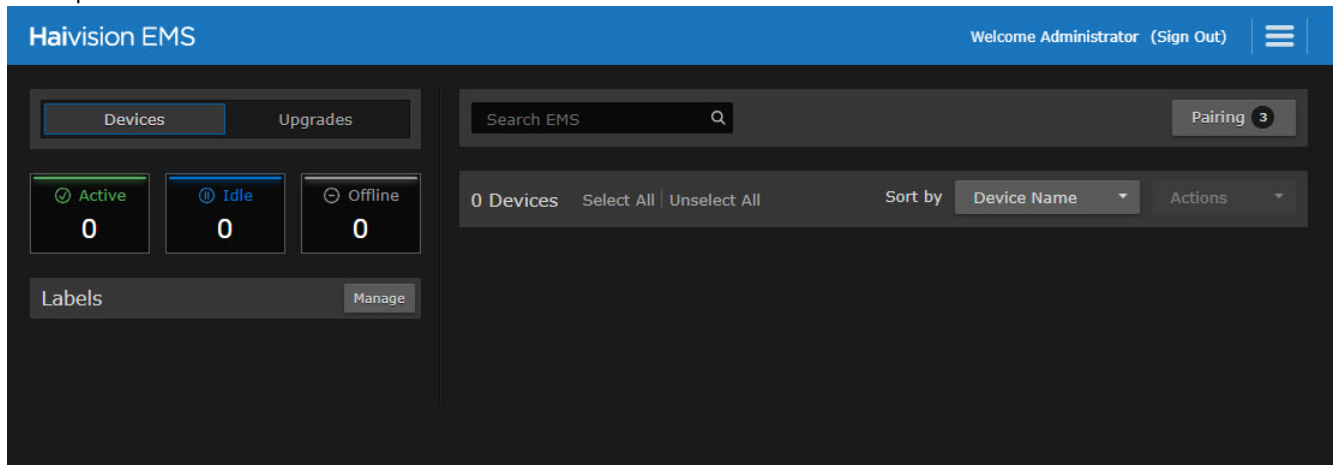
Pairing a Makito X Device

Note

For device discovery to work, mDNS must be enabled on each of the devices you wish to pair.

To discover and pair a Makito X device with EMS:

1. Ensure the Devices pane is selected. If any devices available for pairing are discovered on the network, the number of devices will appear on the Pairing button, as shown in the following example.



2. Click **Pairing**.
3. Enter the address of EMS into the Address field.
4. Generate a new passcode and click **Copy to clipboard**.

Pair Devices

Use the information below to pair each compatible device with EMS. Pairing must be completed from the device's admin console. Links to unpaired devices are listed on the right for your convenience.

Criteria for Passcode Generation

EMS Address:

EMS Port:

Valid For: 3 days

Generate Passcode

Active Passcode

Expires: November 10, 2019 (3 days)

Passcode:

CM2qoO4FUncKDDEwLjY3LjEyLjEyoBCzRVJ
 kCkBmZDZiM2Q2MzZkMmE1ZDc3MTYzMTF
 hMzM5ODQ0ZTNhMzdmNGFjODk5NDc5Mjg
 4YjIxMjc5ZGJkNjBkODQzOTExEiBkOTQ3MT

[Copy To Clipboard](#)

Discovered devices: Unpaired (3) | [All \(3\)](#)

NOTE: mDNS on the device must be enabled for discovery to work

Austin MXE

makito-x-encoder 2.4.0-5 :: Jul 31 2019

Hostname	haivision-ace.local ↗
Type	makito-x-encoder
IP Address	10.67.12.212 ↗
Serial number	HAI-031340030127
Firmware version	2.4.0-5 :: Jul 31 2019

MakitoX (haivision-ace)

makito-x-encoder 2.3.0-65 :: Jan 22 2019

MX4E-HAI-031922020046

makito-x-encoder 1.0.0-62 :: May 29 2019

Close

5.
Note
 Administrator privileges are required to complete the pairing process on Makito devices.

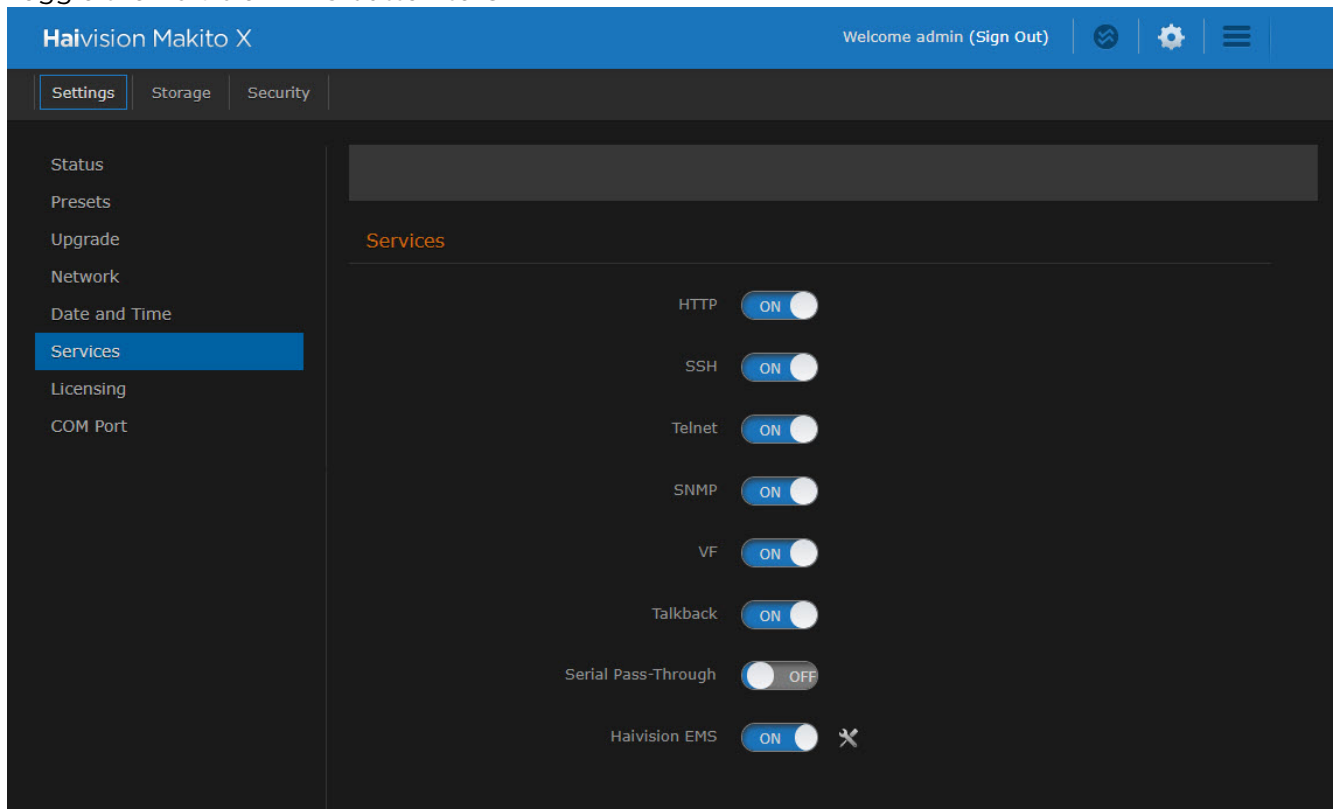
6. Click the icon to access the Administration settings and select **Services**.


Haivision EMS 1.0
User's Guide

20

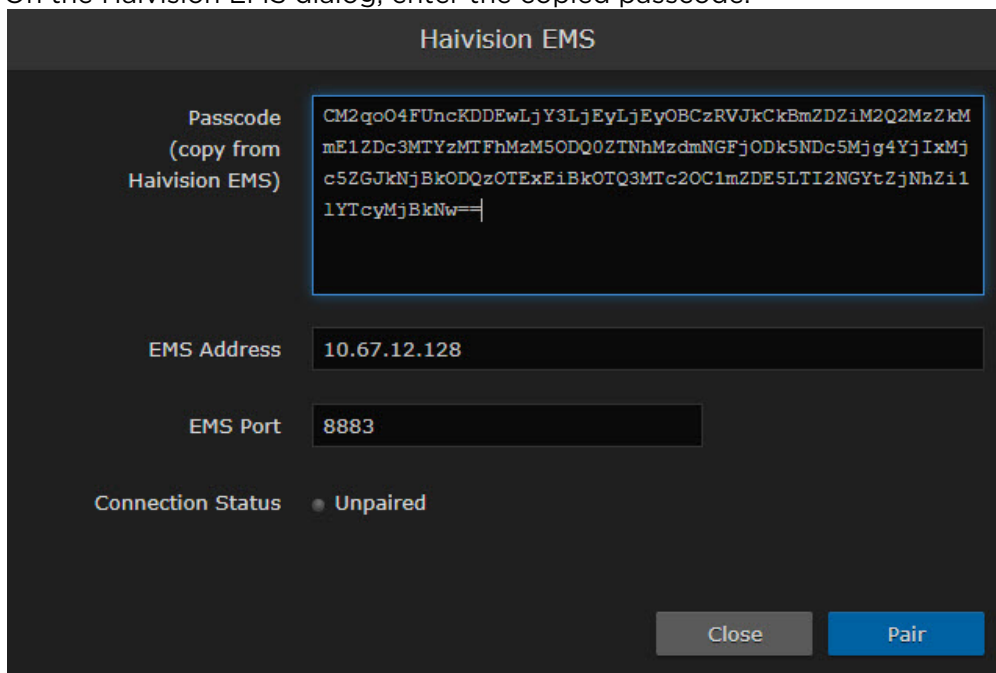
Generated on: 2024-02-15 13:20:44
HVS-ID-UG-EMS-10, Issue 01

7. Toggle the Haivision EMS button to **On**.



8. Click the  icon to open the Haivision EMS dialog.

9. On the Haivision EMS dialog, enter the copied passcode.



Note

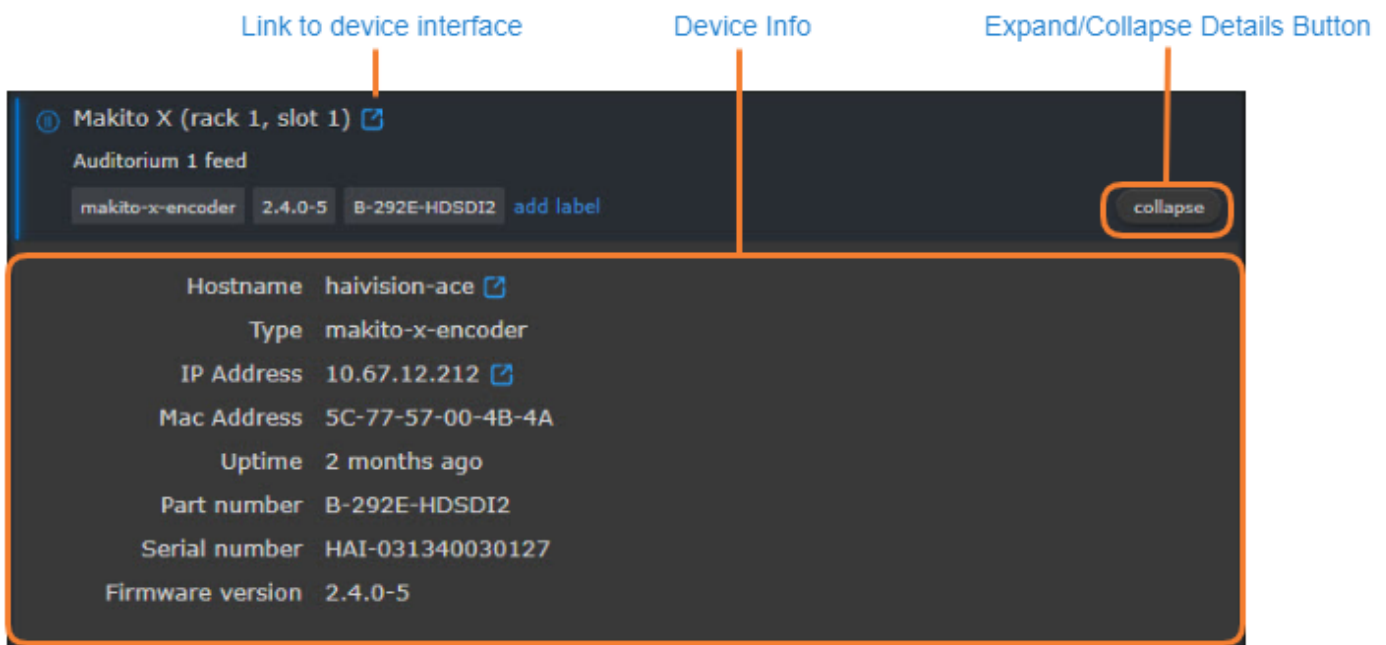
On a new device, the EMS Address and Port fields are blank. When a pairing code is pasted in, the address and port are automatically filled in to reflect the IP and port contained in the pairing code. If needed, the port number can be changed to accommodate network security requirements.

10. Click **Pair**.

Once connected, the device becomes available for management from the EMS interface.

Device Summaries

Once a device is paired with EMS, links to the device's interface and an expandable information pane become available.



Clicking the link icon next to the device's name or IP address will take you to its web interface.

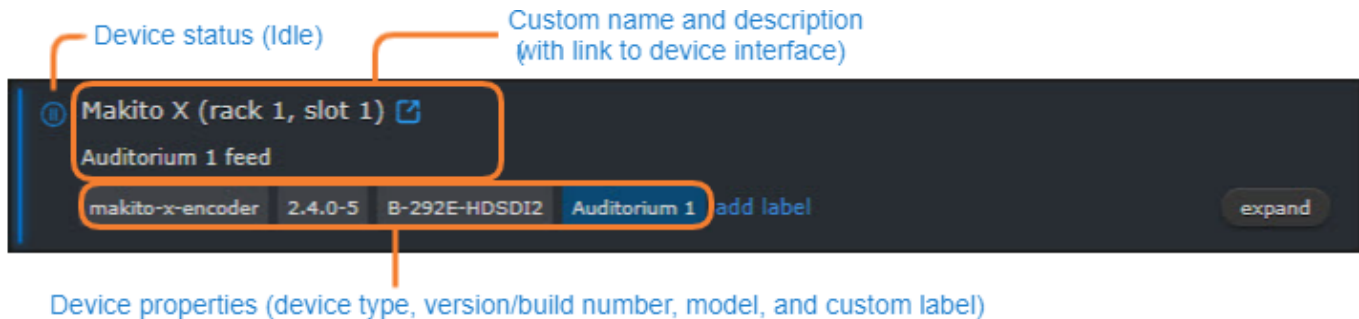
Hovering the mouse over a device reveals the Expand/Collapse button. Click **Expand** to reveal detailed device information.

Field	Description
Hostname	The device's hostname as it appears on the network.
Type	The device type.
IP Address	The device's IP address with a link to its web interface. Devices with multiple IP addresses have each address listed separately.
MAC Address	The unique hardware identifier assigned to the device.
Uptime	How long the device has been online.

Field	Description
Part number	The device model number.
Serial number	The unique serial identifier assigned to the device.
Firmware version	The currently installed firmware package version.

Organizing and Identifying Devices

EMS offers different ways to identify, organize, search, and filter paired devices.



Once a device is paired with EMS, the following information is displayed:

- Name (defaults to the device hostname).
- Status color/icon (Active, Idle, or Offline).
- Device type (e.g., makito-x-encoder or makito-x-decoder).
- Model (e.g., B-292D-HD2)

Topics Discussed

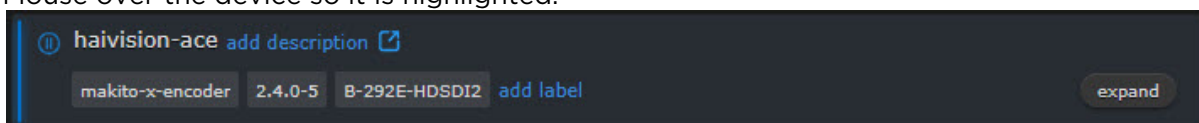
- [Custom Names and Descriptions](#)
- [Labeling Devices](#)
- [Searching and Filtering Devices](#)

Custom Names and Descriptions

When a device is first paired, the device's name defaults to its hostname. This can be changed and a custom description can be added to make identification easier.

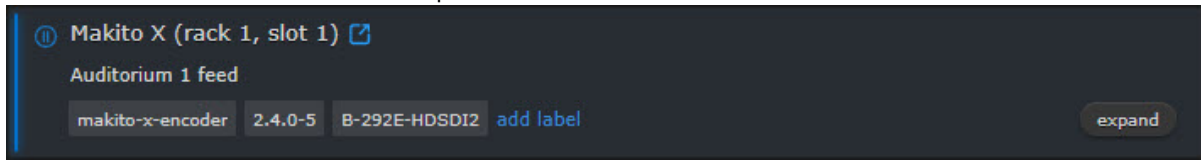
To rename a device or add a custom description:

1. Mouse over the device so it is highlighted.



2. Click the title field or click **Add Description**.

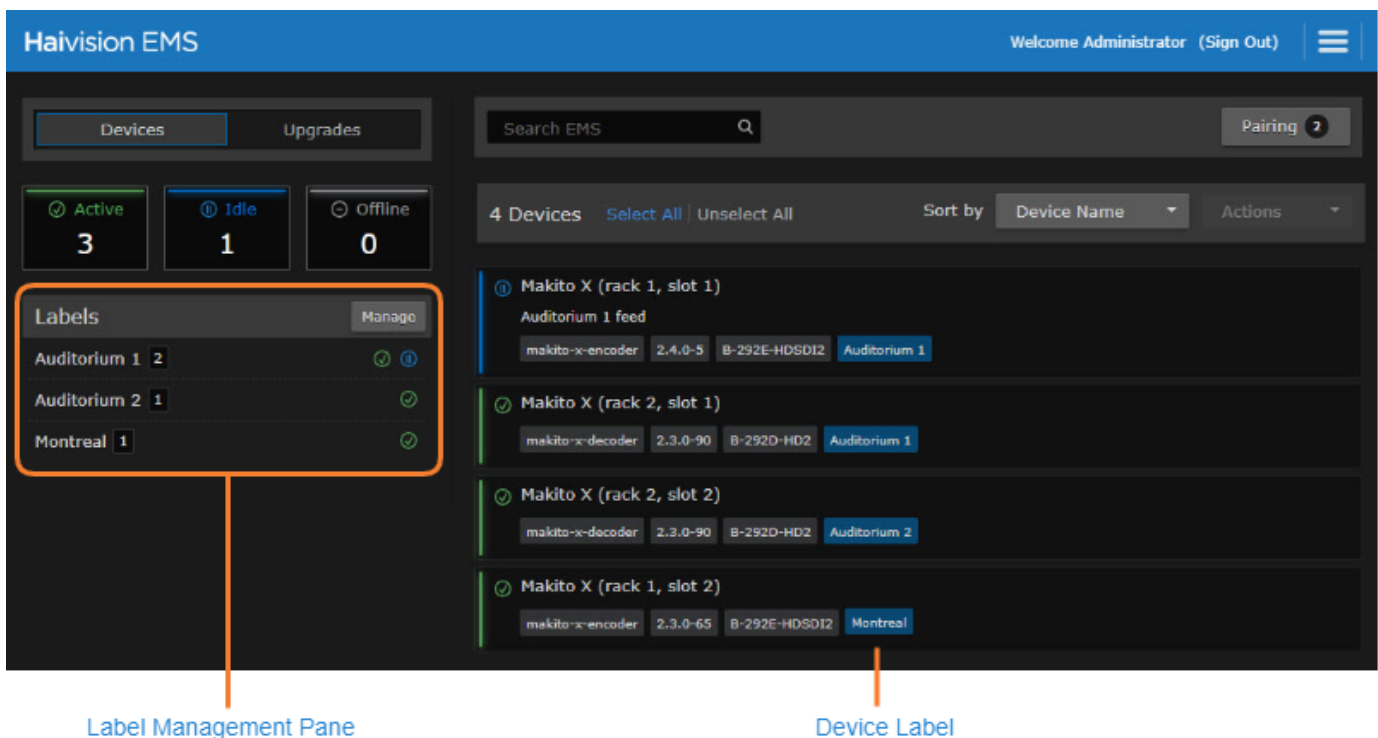
3. Enter the desired name or description.



Note
Renaming a device does not change its hostname.

Labeling Devices

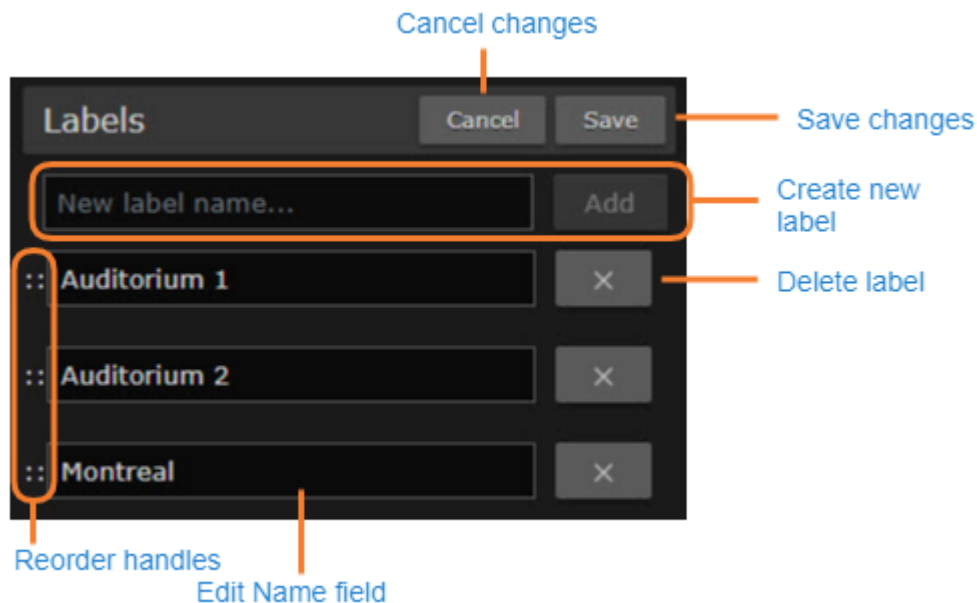
EMS has the ability to create, customize, and assign labels to paired devices to make organization easier.



The Label Management pane shows label names, number of devices under that label and device states (Active, Idle or Offline).

To create or edit labels:

1. Click **Manage** on the Labels pane.



From here you can:

- Create new labels.
- Rename existing labels.
- Reorder labels.

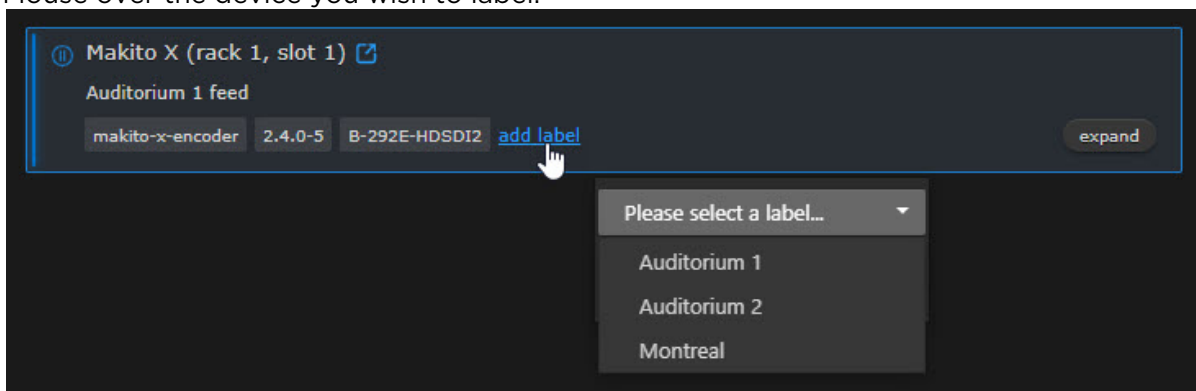
Note

Deleting a label only removes it from the list and any devices it has been applied to. It does not unpair any devices with that label.

2. Click **Save**.
New labels will be added to the end of the list.

To add a label to a device:

1. Mouse over the device you wish to label.



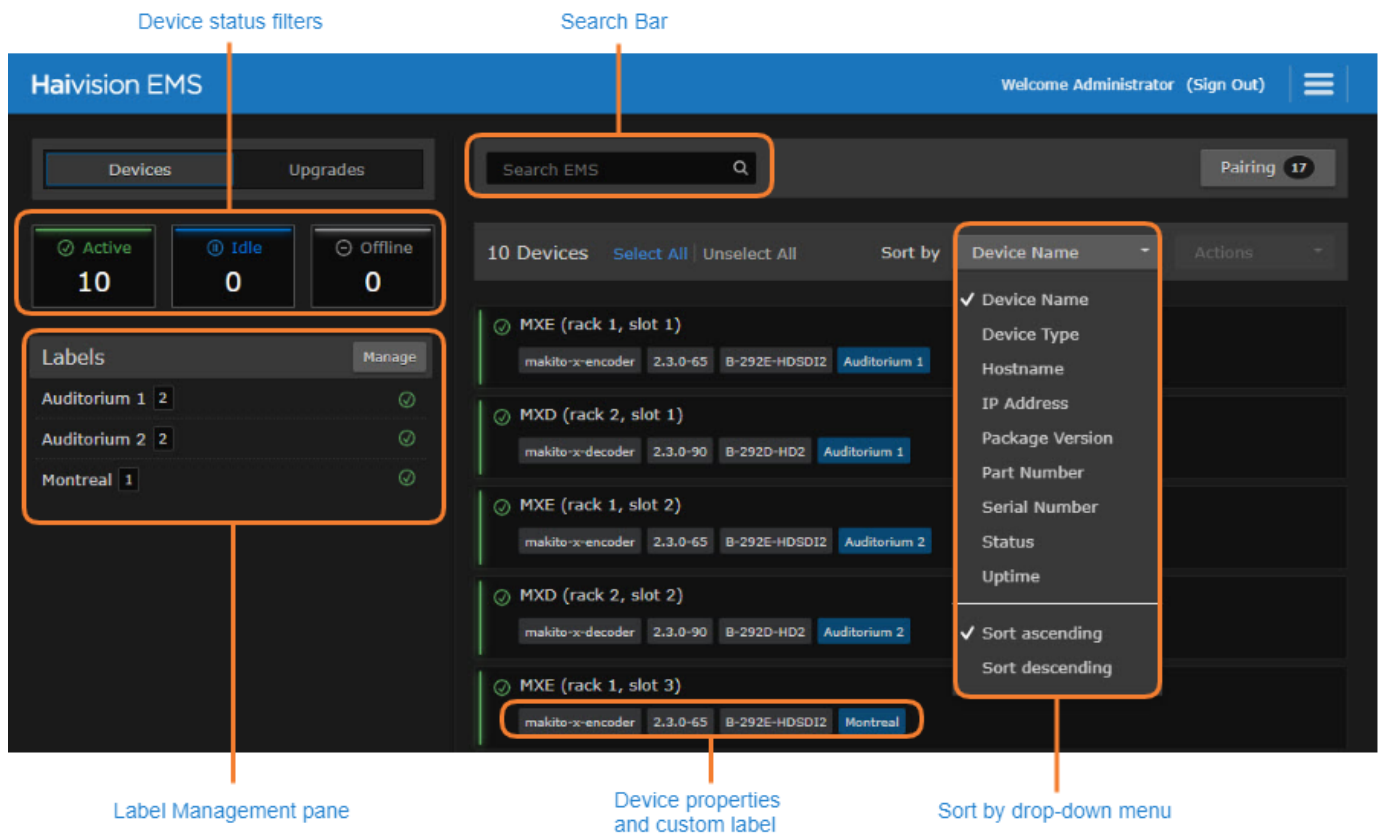
2. Click **Add Label**.
3. Click **Please select a label...** and select from the drop-down.
4. Click **Save**.

Tip

Devices can also be selected from the device list and dragged and dropped onto the desired label in the labels pane. Hold **Ctrl** to select multiple devices.

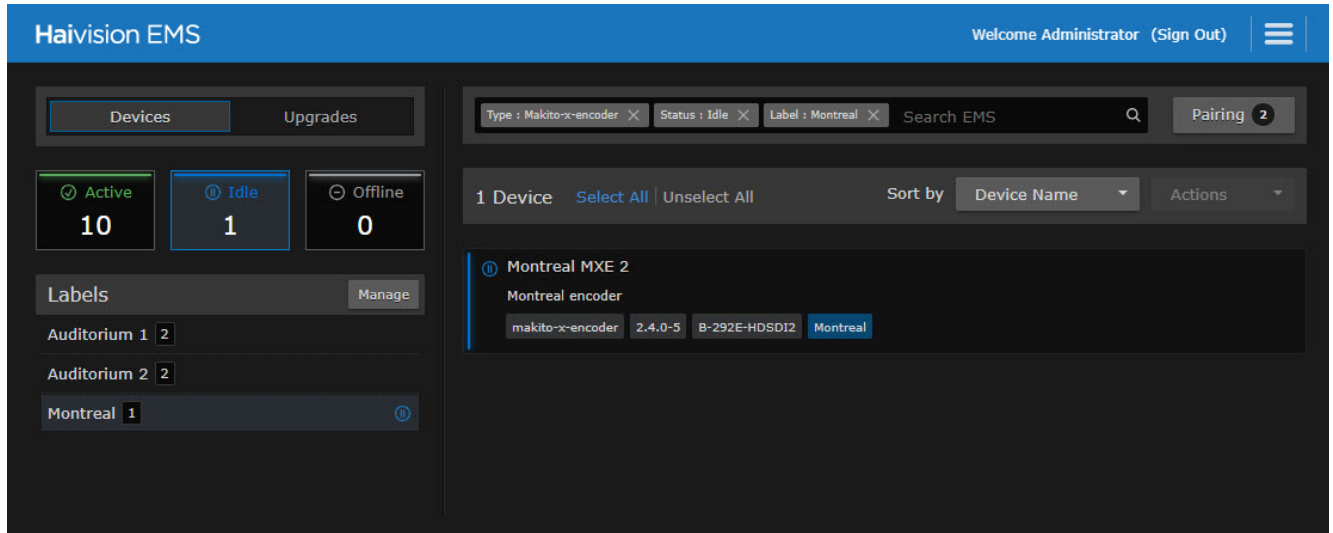
Searching and Filtering Devices

Devices can be searched for, filtered, and sorted according to their properties, status, or applied labels.



To filter the device list based on properties, status, or labels:

1. Click any device status (Online, Idle or Offline), properties, or labels you wish to filter or type them into the Search field.



Note

Multiple properties or labels can be applied to a search query at once, but only one device status can be applied at a time.

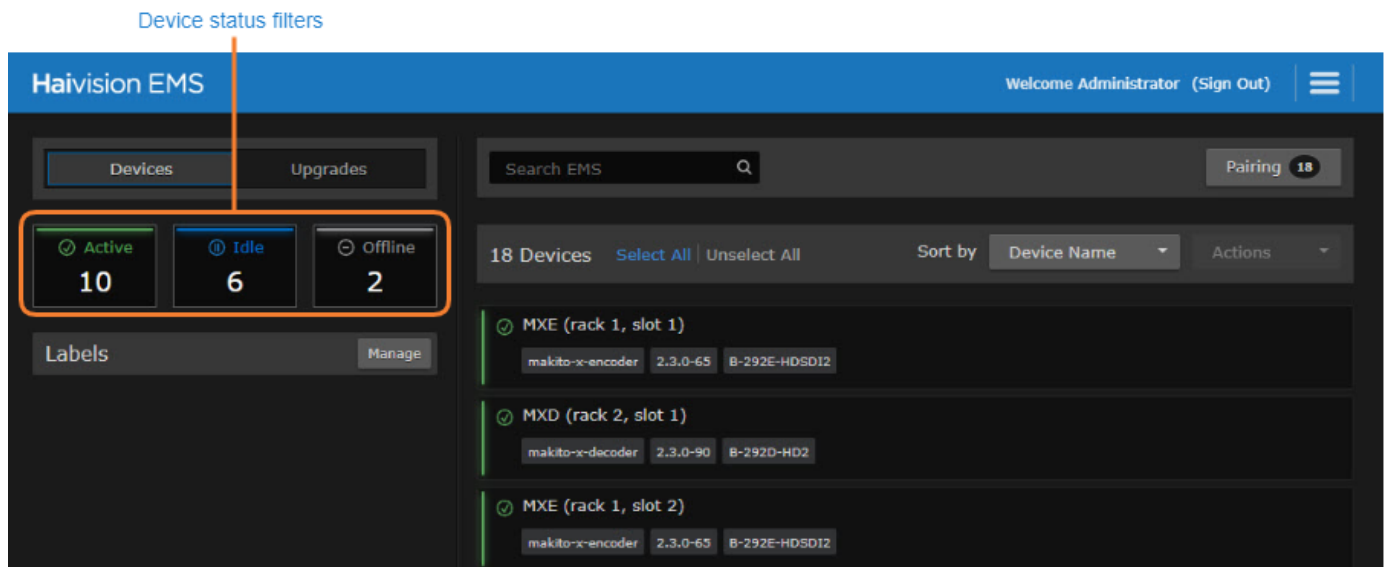
2. Click the X icon to remove a property from your search query.

Related Topics

- [Labeling Devices](#)

Device Status

The status of paired devices (Active, Idle, and Offline) is viewable from the Web interface. The device status icons indicate how many devices are in each state. Clicking a status icon filters the device list to only show devices with the corresponding status.



- Active devices are online and have at least 1 active stream.
- Idle devices are online and not streaming.
- Offline devices are disconnected from EMS.

A device's status changes from Active or Idle to Offline within 5 seconds of a network or power interruption.

Upgrading Device Firmware

i Note

Please refer to the user documentation of the device you are upgrading for device-specific upgrade instructions.

To upgrade a managed device to a new firmware version:

1. Select **Upgrades** from the left-hand pane.

The screenshot shows the Haivision EMS interface. The top navigation bar includes 'Haivision EMS' and 'Welcome Administrator (Sign Out)'. The left-hand pane has 'Upgrades' selected. The main area shows a search bar, a 'Start Installation' button, and a list of devices. One device, 'Makito X (rack 1, slot 1)', is selected and highlighted with a blue border. The device details show 'Auditorium 1 feed', 'makito-x-encoder', '2.4.0-3', 'B-292E-HDSID2', and 'Auditorium 1'.

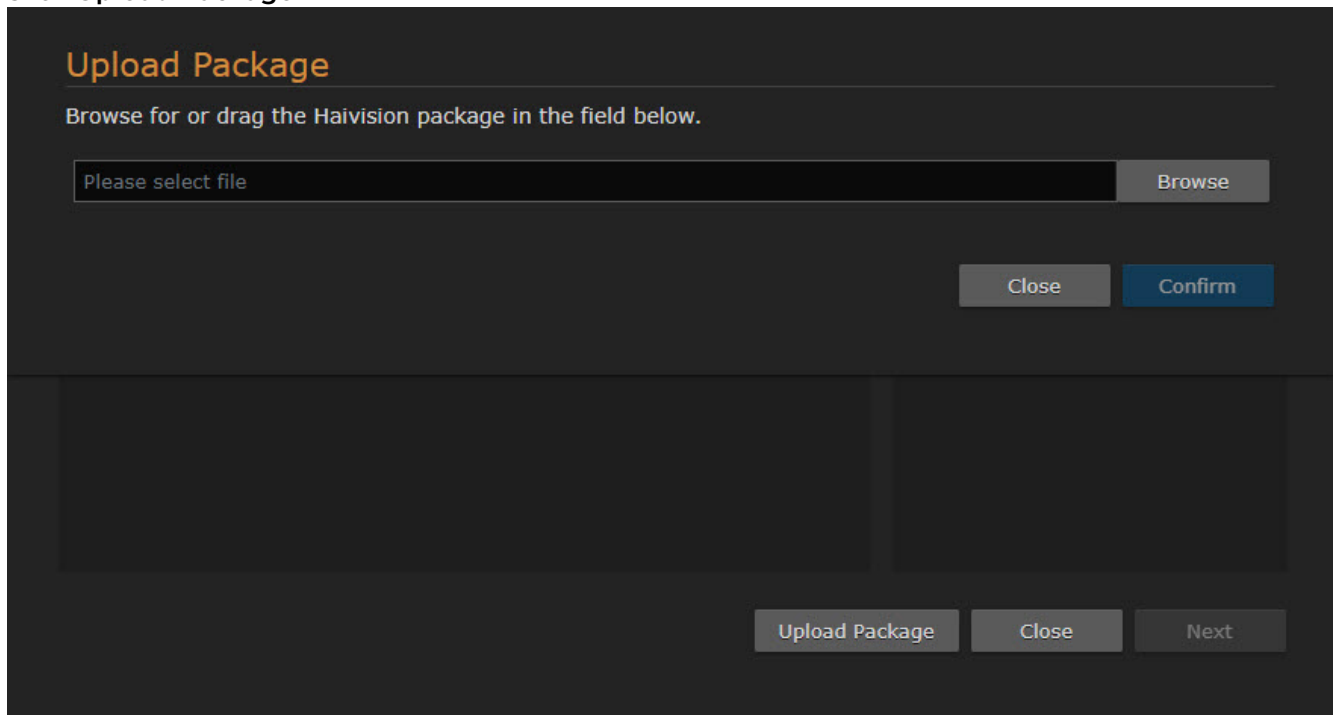
- 2.

i Note

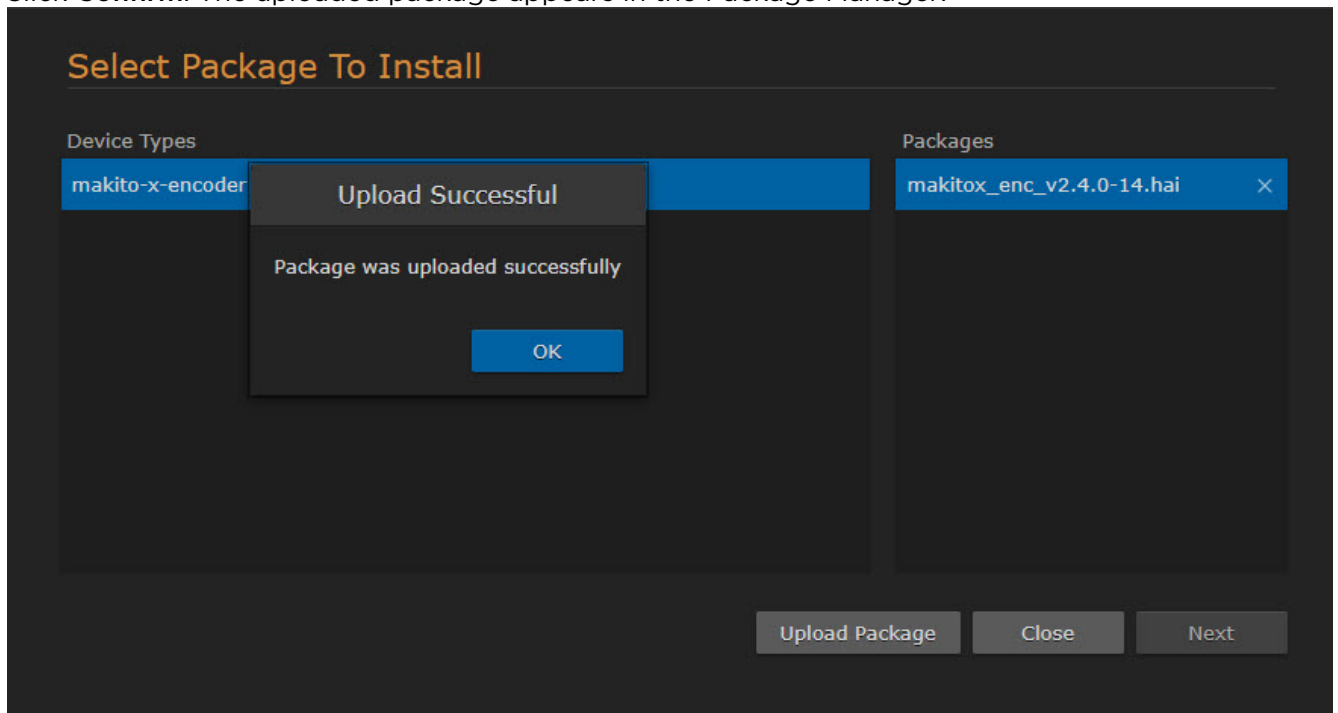
Multiple devices can be upgraded at once but they must be of the same device type (e.g., Makito X Encoder).

3. Click **Start Installation**. The Package Manager will open.

- Click **Upload Package**.



- Click **Browse** and select the desired firmware package.
- Click **Confirm**. The uploaded package appears in the Package Manager.



- Select the desired upgrade package from the Packages pane.
- Click **Next**.

9.

Note

If the package selected does not match one or more of the device types selected in step 2, those devices will not appear in the confirmation dialog and will not be upgraded.

Confirm Package Installation

Warning

Please consult your package installation notes before proceeding.

Be sure that the selected devices are not in use before commencing.

The installation process may take up to 10 minutes to complete and will restart the device.

Package name `makitox_enc_v2.4.0-14.hai`
 Size 90796300 Bytes

Selected devices (1)

ⓘ Makito X (rack 1, slot 1)

Auditorium 1 feed

`makito-x-encoder` `2.4.0-5` `B-292E-HDSDI2` `Auditorium 1`

2.4.0-5 → 2.4.0-14

Cancel
Start Installation

10. Click **Start Installation**.

The status of the upgrade will be shown in the device list and the device(s) will reboot.

Haivision EMS Welcome Administrator (Sign Out) ☰

Devices | **Upgrades**

✔ Active
0

ⓘ Idle
1

⊖ Offline
0

Labels Manage

Auditorium 1 1 ⓘ

Search EMS Start Installation

Select devices to install

1 Device | Select All | Unselect All | Sort by Device Name | Actions

ⓘ Makito X (rack 1, slot 1)

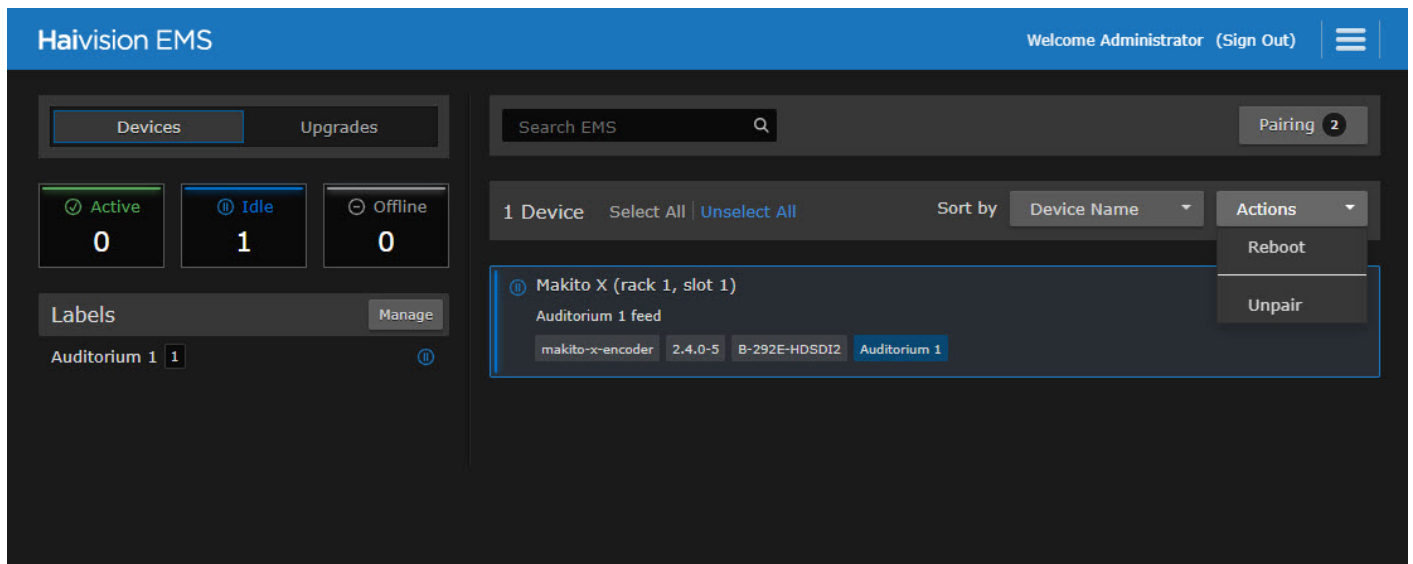
Auditorium 1 feed

`makito-x-encoder` `2.4.0-5` `B-292E-HDSDI2` `Auditorium 1`

Installation status: 🌟 Downloading package to device (24%) cancel

Rebooting and Unpairing Devices

Selecting a device enables the Actions drop-down menu. From here, you can reboot and unpair devices.

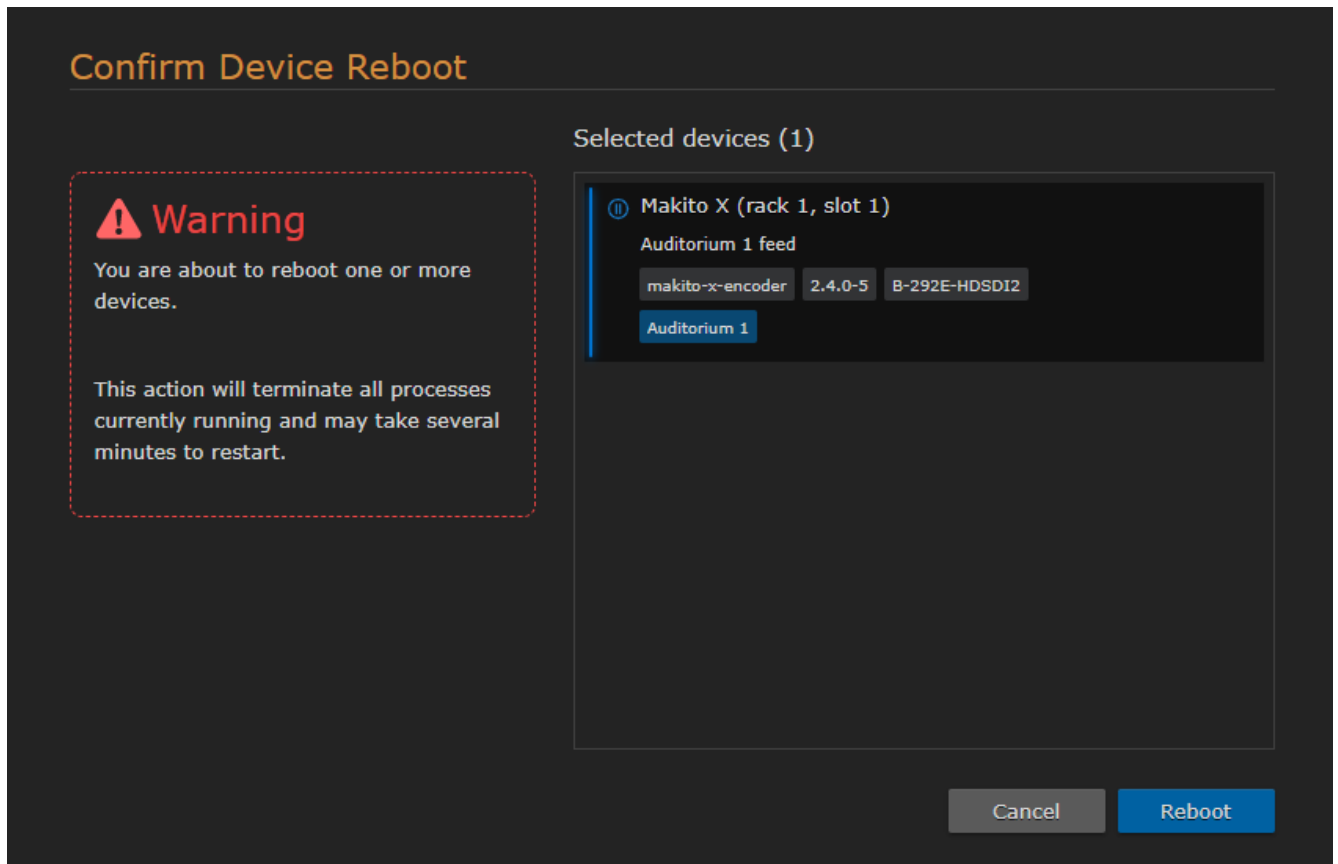


To reboot a paired device:

1. Select the device(s) you wish to reboot.
2. Click the **Actions** drop-down menu and select **Reboot**.
- 3.

Note

Any offline devices in your original selection will not appear in the confirmation dialog and will not be booted.



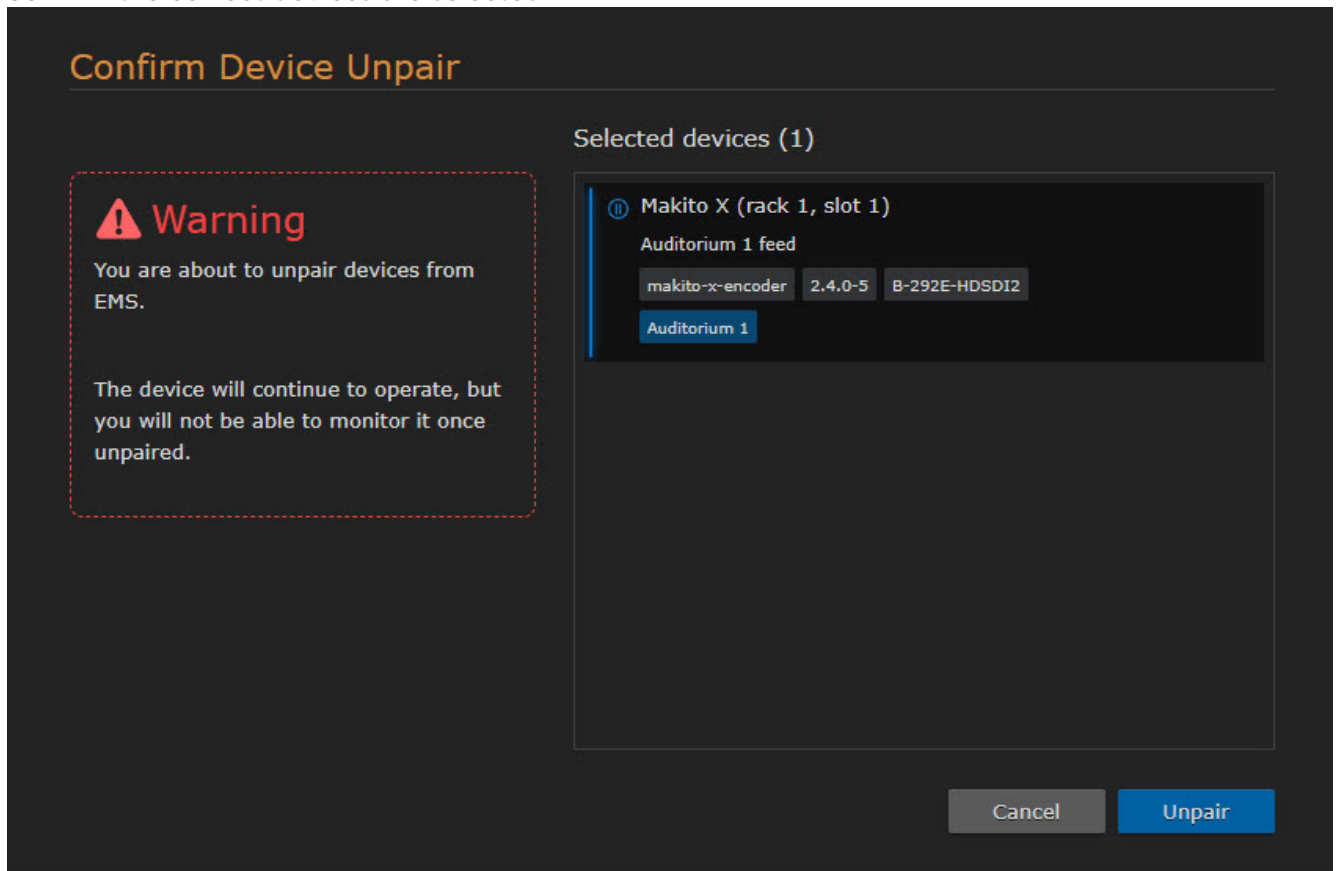
4. Click **Reboot**.

The device's status will change to Offline until it is finished rebooting.

To stop managing a device through EMS, it must be unpaired. To unpair a previously paired device from EMS:

1. Select the device(s) you wish to unpair.
2. Click the **Actions** drop-down menu and select **Unpair**.

3. Confirm the correct devices are selected.



4. Click **Unpair**.

The device(s) will be removed from the device list.

Managing System Settings

Note

The intended audience for this content is system integrators and users with administrative privileges.

Topics Discussed

- [Managing Certificates](#)
 - [Generating a Certificate Signing Request \(CSR\)](#)
 - [Importing and Activating a Certificate \(CRT\)](#)
 - [Generating a Private Key](#)
 - [Importing a Private Key](#)
 - [Certificate Settings](#)
- [Managing Licenses](#)
- [Configuring Network Settings](#)
 - [Network Settings](#)
- [Managing Security](#)
 - [Security Settings](#)
- [Installing System Updates](#)

Managing Certificates

From the Certificates pane, you can generate an SSL private key and certificate signing request (CSR). You can then import the signed certificate and trust chain returned by the Certification Authority (CA).

The Certificates pane lists the Identity Certificates available on Haivision EMS. An Identity Certificate identifies the device during the authentication process when trying to establish a TLS connection in HTTPS session startup. Its Common Name or Alternate Subject Names must match its IP address and/or its FQDN (Fully Qualified Domain Name) if DNS is used.

The default certificate is localhost.crt (self-signed).

Topics Discussed

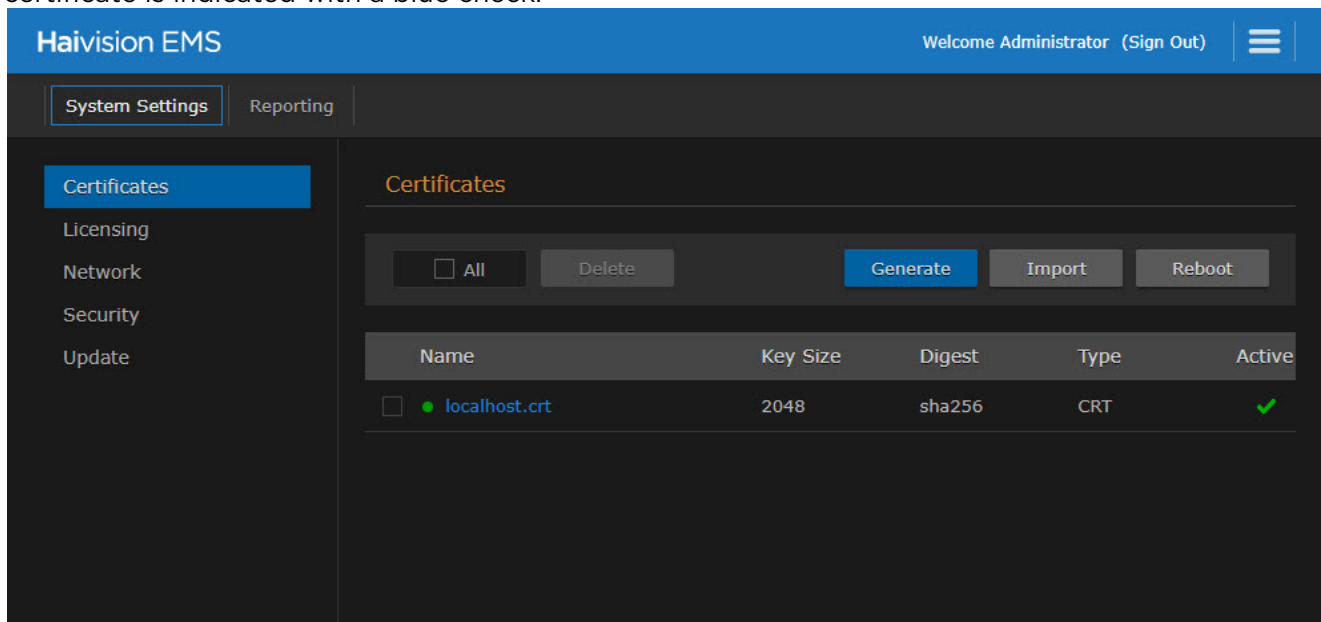
- [Generating a Certificate Signing Request \(CSR\)](#)
- [Importing and Activating a Certificate \(CRT\)](#)
- [Generating a Private Key](#)
- [Importing a Private Key](#)
- [Certificate Settings](#)

Generating a Certificate Signing Request (CSR)

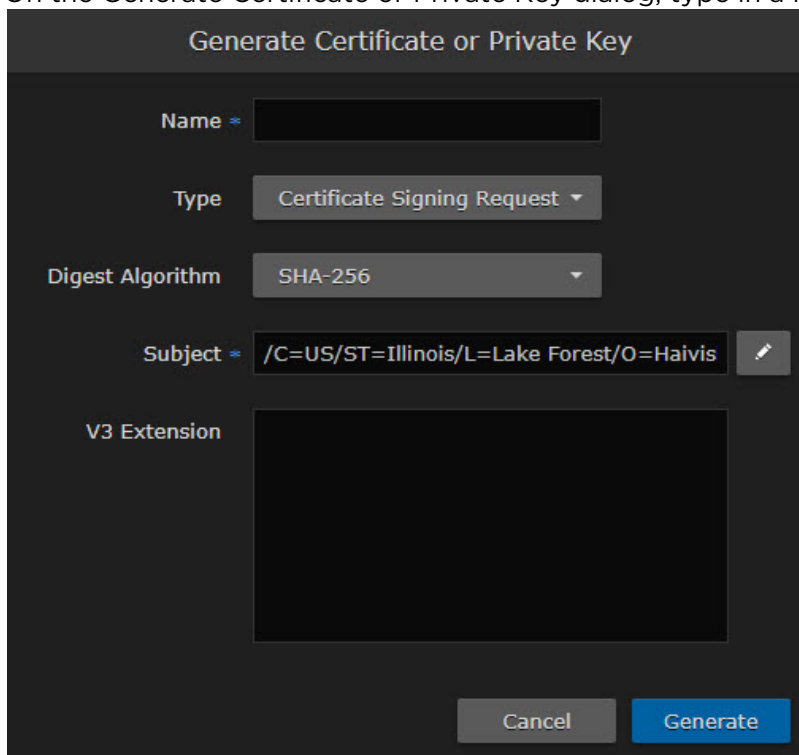
To generate a Certificate Signing Request (CSR):

1. On the Administration screen, click **System Settings** on the toolbar and then click **Certificates** on the sidebar.

The Certificates pane opens, listing any certificate signing requests generated on EMS. The active certificate is indicated with a blue check.



2. Click **Generate**.
3. On the Generate Certificate or Private Key dialog, type in a name for the certificate.



4. Make sure the Type is Certificate Signing Request and fill in the remaining fields. See [Certificate Settings](#).
5. For the subject, type in information about the device that the Identity Certificate represents. For more information, see the "Subject" entry in [Certificate Settings](#).
6. Click **Generate**.

Note

The generated CSR file needs to be sent to a Certification Authority to be signed. The CSR content can be viewed by clicking on the CSR name in the list; its content will be displayed in a new window where it can be copied. You can import the signed certificate back later by clicking the Import button.

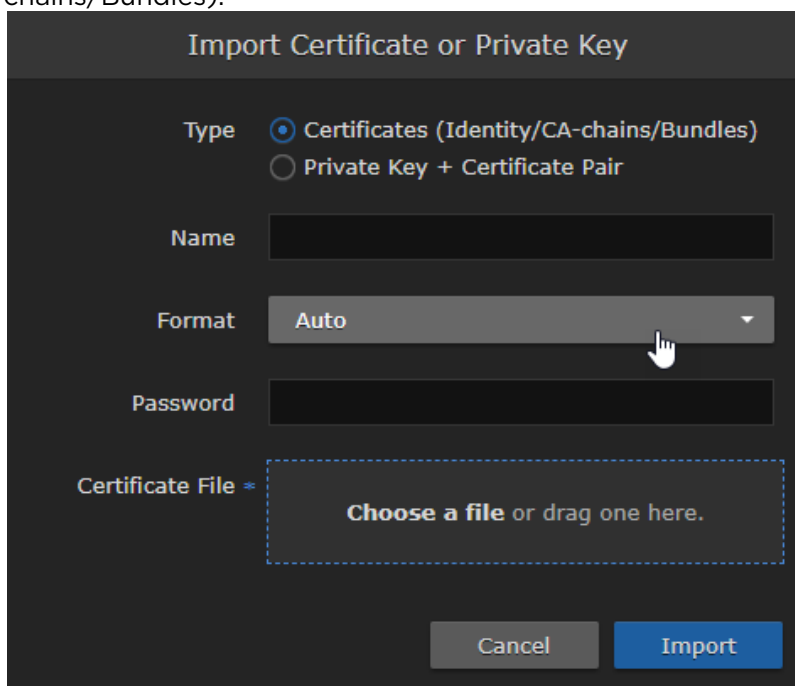
Tip

Keep in mind that there is a difference between importing a new certificate (that was generated externally) and importing a newly signed certificate whose request was previously generated on EMS and exported for signing.

Importing and Activating a Certificate (CRT)

To import and activate a Certificate (CRT):

1. On the Certificates pane, click **Import**.
2. On the Generate Certificate or Private Key dialog, keep the default Type: Certificates (Identity/CA-chains/Bundles).

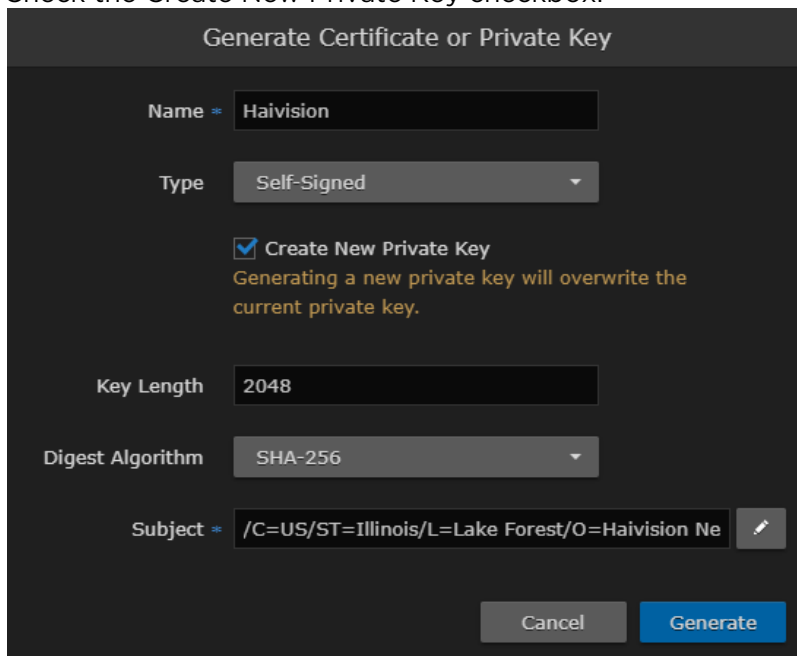


3. Type in the certificate name and fill in the remaining fields. See [Certificate Settings](#).
4. If your certificate is encrypted, type in the password.
5. Drag a CA-signed certificate (CRT) to the drop area or click **Choose a file** to choose and select the certificate (returned from the certificate request generated in the previous section).
6. Click **Import**. On the Certificates pane, the newly imported certificate will be added to the list and should have a green status LED. Click in the Active column to activate the certificate.
7. Click **Reboot** if you have changed the active certificate.

Generating a Private Key

To generate a Private Key:

1. On the Certificates pane, click **Generate**.
2. On the Generate Certificate or Private Key dialog, type in a name for the certificate.
3. For the Type, select **Self-Signed**.
4. Check the Create New Private Key checkbox.



Generate Certificate or Private Key

Name * Haivision

Type Self-Signed

Create New Private Key
Generating a new private key will overwrite the current private key.

Key Length 2048

Digest Algorithm SHA-256

Subject * /C=US/ST=Illinois/L=Lake Forest/O=Haivision Ne

Cancel Generate

5. Fill in the remaining fields. See [Certificate Settings](#).
6. Click **Generate**.

⚠ Caution

Clicking Generate overwrites the current private key and renders unusable any certificates based on that key.

The new certificate is added to the Certificates list, and becomes the active certificate.

7. Click **Reboot**.

Importing a Private Key

To import a Private Key:

1. On the Certificates pane, click **Import**.

- On the Import Certificate or Private Key dialog, for the Type, select **Private Key + Certificate Pair**.

- Type in the password for the private key.
- To update your security certificate, Drag the new SSL Certificate and SSL Certificate (Private) Key, and optionally an SSL Intermediate Certificate Bundle file to the drop area or click **Choose a file**.
- Click **Import**. On the Certificates pane, the newly imported files will be added to the list.
- Click **Reboot**.

Certificate Settings


Note

Please contact your Network Administrator if you are unsure what to put in any of these fields or if you are unsure whether the setting is required on your network.

[Generate Certificate or Private Key](#) **Import Certificate**

Generate Certificate or Private Key

Setting	Description
Name	Type in a unique name under which the certificate will be stored in EMS as well as listed on the Certificate pane

Setting	Description
Type	<p>Select the Signature Type:</p> <ul style="list-style-type: none"> • Self-signed: The certificate will be generated and signed by the system, and the name will be added to the list of Identity Certificates. • Certificate Signing Request: A request will be generated, and its name will be added to the list of Identity Certificates. The request will be located in your home directory (accessible through the CLI), or you may export it by clicking on the View button and copying the content into a new file in a text editor. In its generated form, this certificate is still a request and cannot be used as an Identity Certificate before it is signed by a CA, and imported back.
Digest Algorithm	<p>Select the digest algorithm (Secure Hash Algorithm):</p> <ul style="list-style-type: none"> • SHA-256 • SHA-384 • SHA-512
Subject	<p>The Subject identifies the device being secured, in this case, EMS. Type in the subject in the form: "/C=.../ST=.../L=.../O=.../OU=.../CN=..." where the most common attributes are:</p> <ul style="list-style-type: none"> • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p> Tip</p> <p>For successful authentication, the Common Name in the certificate should be the IP address (by default) or domain name of the device.</p> </div>
V3 Extension	<p>V3 extensions allow more configuration options to be inserted in the Code Signing Request, such as alternative subject names and usage restrictions to certificates.</p> <p>To add one or more Subject Alternative Names, enter the same information that would go in the extensions section of an OpenSSL configuration file. For example:</p> <pre style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> [req] req_extensions = v3_req [v3_req] # Extensions to add to a certificate request subjectAltName = @alt_names [alt_names] DNS.1 = server1.example.com DNS.2 = mail.example.com DNS.3 = www.example.com DNS.4 = www.sub.example.com DNS.5 = mx.example.com DNS.6 = support.example.com </pre>

[Generate Certificate or Private Key](#)
[Import Certificate](#)

Import Certificate

Setting	Description
Type	Select the certificate Type: <ul style="list-style-type: none"> • Certificates: (Identify/CA-chains/Bundles) • Private Key + Certificate Pair
Name	Name of the certificate.
Format	Select the file format for the Certificate (the formats differ in the way the file is encrypted): <ul style="list-style-type: none"> • Auto: detected from the file extension • der: Distinguish Encoding Rules • pkcs #7 • pkcs #12
Password	If the imported certificate contains a password protected private key, type its password in this field. Leave this field empty if the file is not password-protected.
Certificate File	Drag a certificate file to the drop area or click Choose a file to choose a file to upload.

Managing Licenses

This section provides instructions to update your EMS license from the web interface.

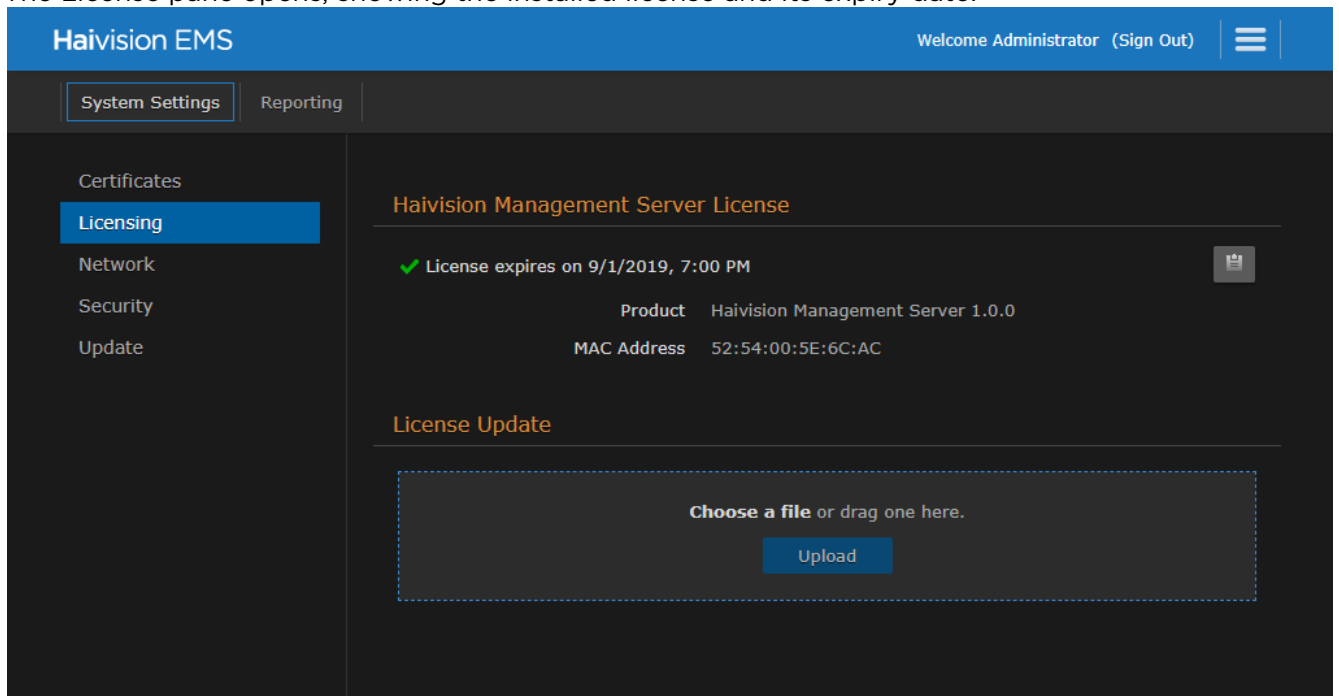
Note


Any update (other than a maintenance release such as v1.x.x) requires a new license.

To update your license:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Licensing** on the sidebar.

The License pane opens, showing the installed license and its expiry date.



2. Click  to copy the current product details (product name, version, and MAC address) to the clipboard.
3. Contact Haivision Technical Support with this information to request the license file.
4. Once you have the license file, drag it into the License Update drag area or click **Choose a file**.
5. Click **Upload** to upload the license to EMS.

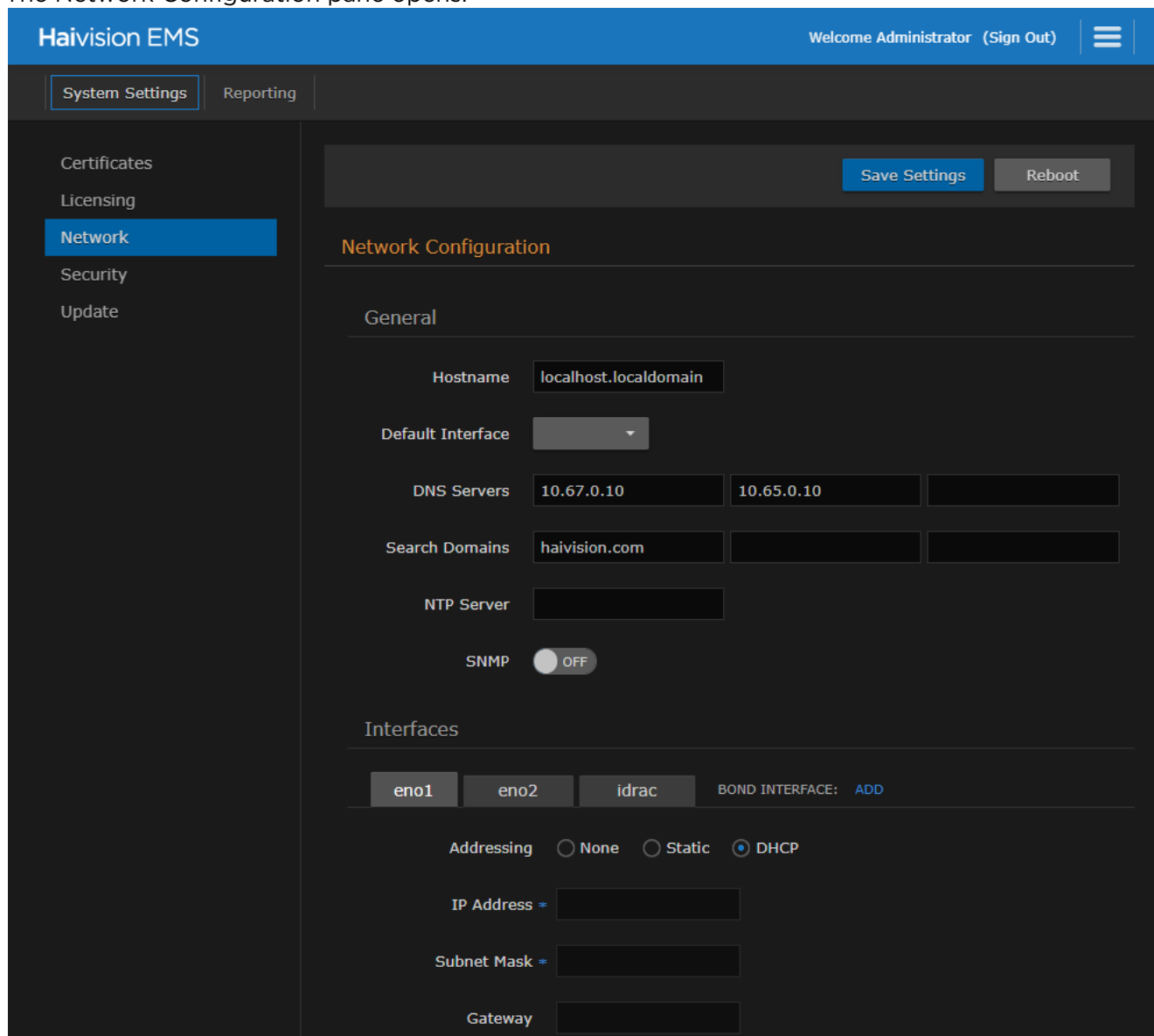
Configuring Network Settings

When setting up EMS, you will need to configure network settings. This includes general settings such as specifying the server hostname, IP address, subnet mask, and DNS server(s), as well as advanced optional settings such as setting up multiple network interfaces, NIC bonding, link negotiation settings, and static routes.

To configure the network settings:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Network** on the sidebar.

The Network Configuration pane opens.



2. Fill in the General section. For details, see [Network Settings](#).
3. To enable SNMP alerts, toggle the SNMP button to **On**.
4. Under Interfaces, select the first interface, if not already selected (eno1 in the above example).
- 5.

Note

When DHCP is enabled, EMS will get an IP Address from a DHCP server on the network to which it is connected. When it is disabled, you must manually enter the appliance's IP Address and Netmask.

- Fill in the required fields. For details, see [Network Settings](#).

Interfaces

eno1

eno2

idrac

BOND INTERFACE: [ADD](#)

Addressing None Static DHCP

IP Address *

Subnet Mask *

Gateway

MTU

MAC Address

Link Auto Manual

Static Routes

All

Actions ▼

+

Destination	Subnet Mask	Gateway	Interface

- To configure multiple network interfaces, select the next interface (e.g., eno2) and repeat the configuration.
- To add a bond interface, click **Add** and fill in the fields, including the Bonding Mode.

✔ **Tip**

Bond interfaces provide a method for aggregating multiple network interfaces into a single logical bonded interface. The goal is to increase throughput and to ensure redundancy in case one of the links should fail. See "Bond Interface" in [Network Settings](#).

- To add one or more static routes, click **+Route** under Static Routes and fill in the fields.
- Click **Save Settings**.
- Click **Reboot** to restart the EMS server.

Topics Discussed

- Network Settings

Network Settings

Note

Please contact your Network Administrator if you are unsure what to put in any of these fields or if you are unsure whether the setting is required on your network.

General Interfaces Static Routes

General

Setting	Description
Hostname	The hostname to be assigned to EMS. This is a FQDN (Fully Qualified Domain Name); for example, myserver.mycompany.com .
Default Interface	<p>Note</p> <p>Network Interface names for Ethernet interfaces may vary, such as eth0/eth1/... or em1/em2/.... "None" indicates that the default interface is not set.</p>
DNS Servers	(Optional) The IPv4 address(es) of the Domain Name Server(s) to use.
Search Domains	(Optional) The search strings to use when attempting to resolve domain names.
NTP Server	(Optional) If Network Time Protocol (NTP) is enabled, enter the IP address of the NTP server.
SNMP	To enable SNMP (Simple Network Management Protocol) alerts for out-of-band monitoring, toggle this button to On . This tells EMS to start the SNMP server, in order to query for OS information, such as CPU usage. SNMP alerts are typically used by IT administrators to monitor system health.
Read-Only Community	(SNMP must be enabled) Type in the SNMP community string associated with the SNMP Trap Server. This is the string to use when sending a trap to an SNMP Trap server. For example: "Haivision EMS"
SNMP Trap Servers	(SNMP must be enabled) The SNMP server to send SNMP Traps to. This is an IPv4 or FQDN of an SNMP Trap server listening for traps via SNMP. For example: SNMP1.mycompany.com

General Interfaces Static Routes

Interfaces

Setting	Description
eno1 eno2 idrac	<p>Note</p> <p>Network Interface names for Ethernet interfaces may vary, such as eth0/eth1/..., pNp1/pNp2/..., or em1/em2/....</p>
Bond Interface	Bonding enables an administrator to use more than one physical network port as a single connection. This can be used to increase performance or redundancy of a server. See the Bonding Mode entry in this table.
Addressing	Choose whether the interface will use a static or dynamic IP address:
IP Address	<p>Note</p> <p>If DHCP is disabled, you may enter an IP address in dotted-decimal format (xxx.xxx.xxx.xxx).</p>
Subnet Mask	<p>Note</p> <p>If DHCP is disabled, you may enter a Network Mask in dotted-decimal format (e.g., 255.255.0.0).</p>
Gateway	<p>Note</p> <p>If DHCP is disabled, you may enter a gateway address in dotted-decimal format.</p>
MTU	(Maximum Transmission Unit) Specifies the maximum allowed size of IP packets for the outgoing data stream. 228..1500
MAC Address	(Read-only) The Media Access Control address assigned to the interface. This is the physical address of the network interface and cannot be changed.
Link	Select the link negotiation settings for the interface, either Auto or Manual. If you select Manual, you can select the Speed (10, 100 or 1000) and Duplex setting (Full or Half).

Setting	Description
Bonding Mode	<p>(Bond Interface only) Modes for the Linux bonding driver determine the way in which traffic sent out of the bonded interface is actually dispersed over the real interfaces. Modes 0, 1, and 2 are by far the most commonly used among them.</p> <ul style="list-style-type: none"> • Round Robin Sequential: Transmits packets in first available network interface (NIC) slave through the last. This mode provides load balancing and fault tolerance. • Active Backup: Only one NIC slave in the bond is active at a time. A different slave becomes active only when the active slave fails. This mode provides fault tolerance • XOR Sequential: Transmits based on XOR formula. (Source MAC address is XOR'd with destination MAC address). This mode selects the same NIC slave for each destination MAC address and provides load balancing and fault tolerance. • Broadcast - Fault Tolerance: Transmits network packets on all slave interfaces. This mode is least used (only for specific purpose) and provides only fault tolerance. • IEEE 802.3ad Dynamic Link Aggregation: Creates aggregation groups that share the same speed and duplex settings. Utilizes all slave network interfaces in the active aggregator group according to the 802.3ad specification. This mode is similar to the XOR mode above and supports the same balancing policies. The link is set up dynamically between two LACP-supporting peers. • (Adaptive) Transmit Load Balancing (TLB): The outgoing traffic is distributed according to the current load and queue on each slave interface. Incoming traffic is received by one currently designated slave network interface. If this receiving slave fails, another slave takes over the MAC address of the failed receiving slave. • (Adaptive) Active Load Balancing (ALB): This includes balance-tlb + receive load balancing (rlb) for IPV4 traffic. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the server on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different clients use different hardware addresses for the server.
Slave Interfaces	(Bond Interface only) Check this checkbox to select the slave interface(s) to allow the bond interface be the master.

General Interfaces Static Routes

Static Routes

Setting	Description
+Route	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Note</p> <p>A static route cannot be created with a Subnet Mask of either 0.0.0.0 or 255.255.255.255.</p> </div>

Managing Security

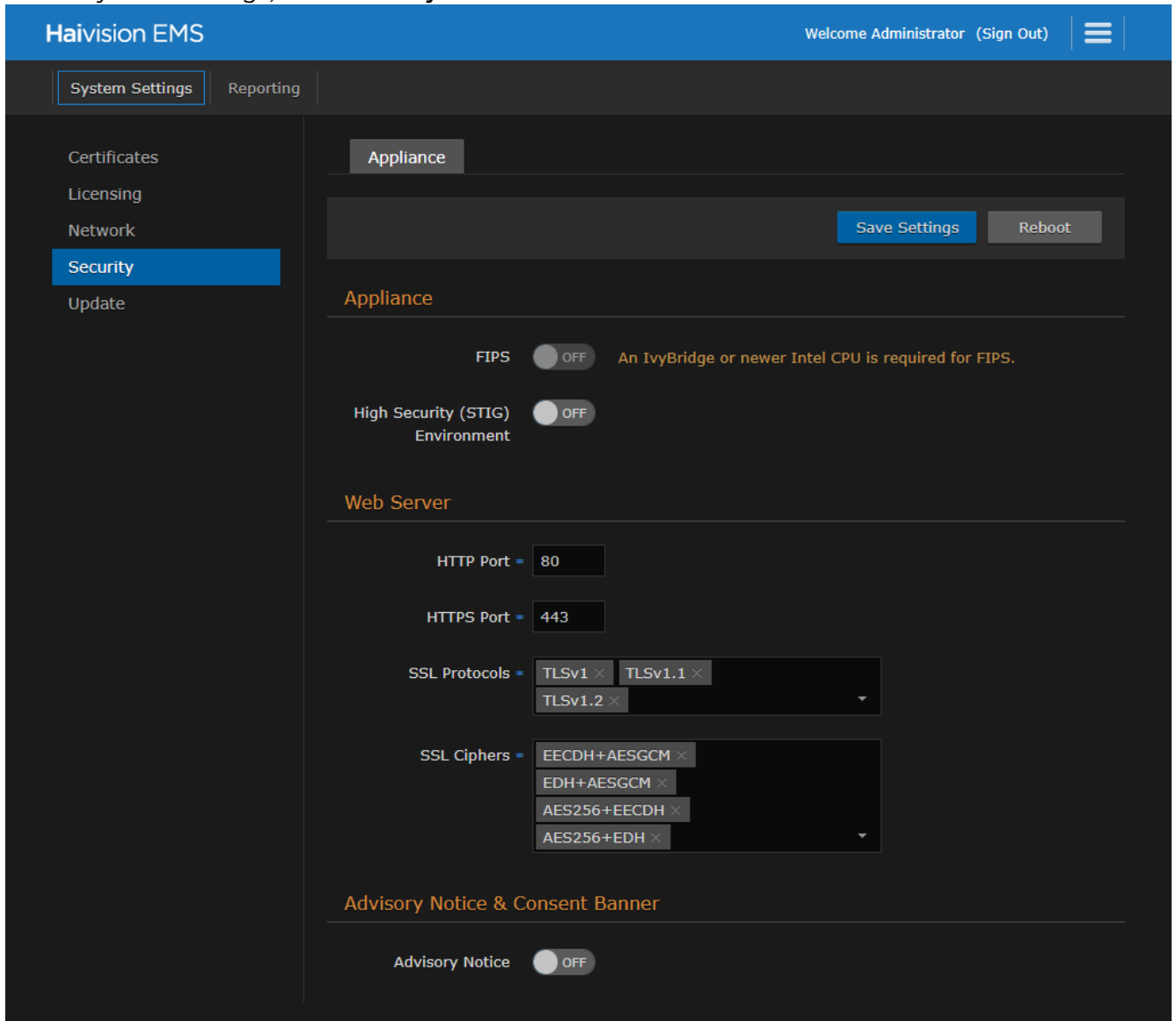
From the Security pane, you may (optionally) configure system security hardening settings and a security banner:

- FIPS compliance
- High Security (STIG) Environment hardening settings

- Web Server security and policy settings
- Advisory Notice & Consent Banner

To configure appliance security:

1. Under System Settings, click **Security**.

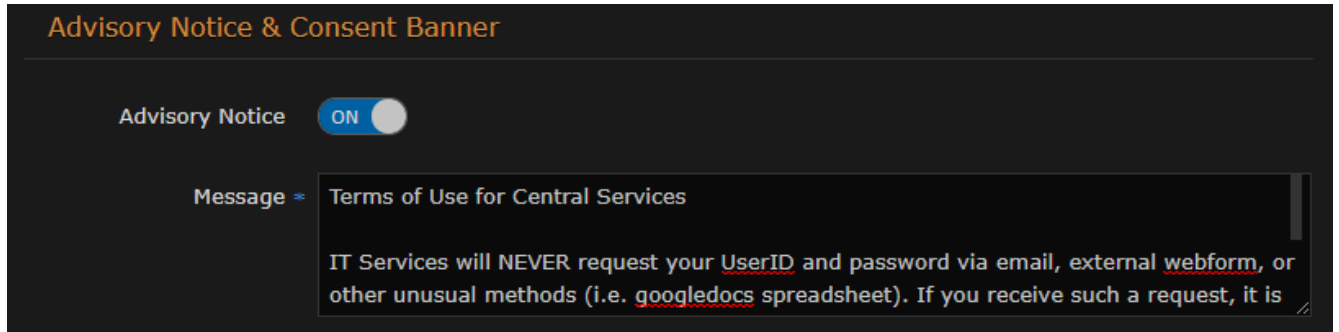


2. To configure FIPS compliance, under Appliance, toggle the **FIPS** button to **On**. See the Appliance entry in [Security Settings](#).
3. To enable security hardening features for high-security environments, toggle the High Security (STIG) Environment button to **On**.

4. **! Important**

Changes to port numbers take effect immediately. Changing port numbers will affect ongoing operations using the service at that port.

- To configure a banner, type or copy in the desired banner text. Toggle the **Advisory Notice** button to **On**.



- Click **Save Settings** to save the connection.
- Click **Reboot** to restart the EMS server.

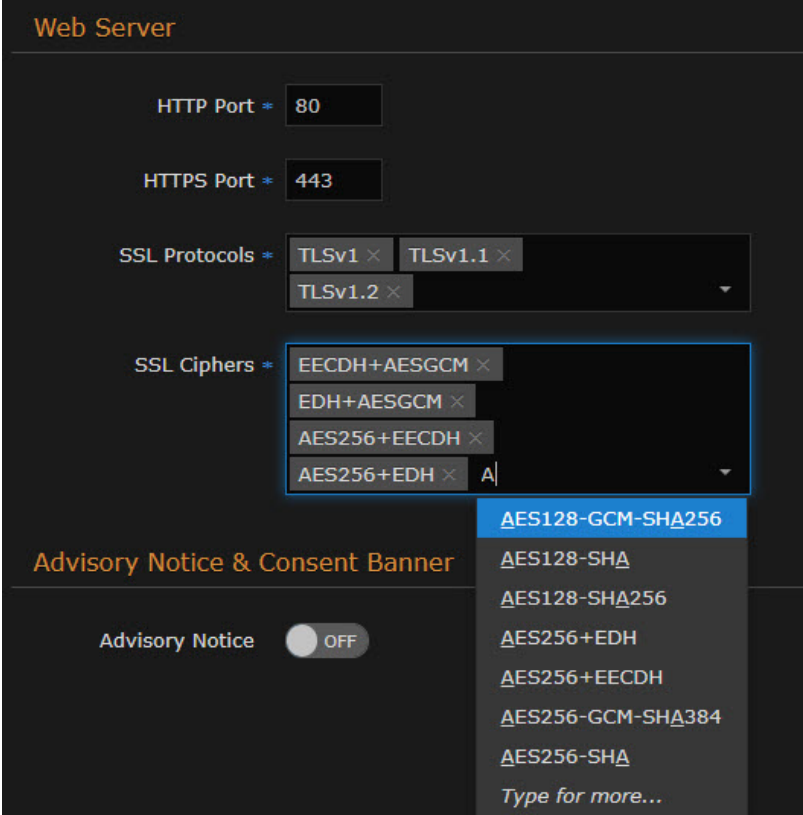
Note
All settings except for Web Server require a reboot.

Security Settings

Note
Please contact your Network Administrator if you are unsure what to put in any of these fields or if you are unsure whether the setting is required on your network.

Setting	Description
Appliance	
FIPS	<p>To enable FIPS cryptographic compliance on your system, toggle the FIPS button to On. Enabling FIPS cryptographic compliance applies cryptographic modules accredited under the U.S. Federal Information Processing Standard (FIPS) Publication 140- 2.</p> <p>Note To use FIPS mode, the CPU must be an IvyBridge or newer Intel CPU with the RDRAND instruction.</p>

<p>High Security (STIG) Environment</p>	<p>To enable security hardening features for high-security environments, toggle this button to On. This setting includes:</p> <ul style="list-style-type: none"> • Session timeouts/locks for all interfaces. • Stronger password requirements • Lock/disable accounts due to multiple authentication failures or expired passwords. • Disabling unnecessary services. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>This complies with National Institute of Standards and Technology (NIST) Special Publication 800-53 (see https://nvd.nist.gov/800-53/ Rev 4).</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Important</p> <p>Only security professionals who understand the cipher support and requirements within their organization should change this setting. Some of these settings are not supported by Haivision Play Set-Top Box or by Google Chrome. The default list has been verified for broad acceptance, and should typically only be adjusted to mitigate new and critical vulnerabilities that may occur.</p> </div>
<p>Lock Session After</p>	<p>(High Security (STIG) Environment must be enabled) Type in the time period (in minutes) allowed for inactivity before an EMS session is locked (on all interfaces, console, ssh, and Web).</p>
<p>Web Server</p>	
<p>HTTP Port HTTPS Port</p>	<p>To configure the Web port for EMS:</p> <ul style="list-style-type: none"> • HTTP Port number (Default = 80) • HTTPS Port number (Default = 443)
<p>SSL Protocols</p>	<p>To specify which TLS (Transport Layer Security) versions are accepted, select from the drop-down list: TLS v1, TLS v1.2, TLS v1.2.</p>

<p>SSL Ciphers</p>	<p>To specify which SSL Ciphers are accepted, select from the drop-down list or type in another cipher name:</p>  <p>The screenshot shows the 'Web Server' configuration page. It includes fields for 'HTTP Port' (80) and 'HTTPS Port' (443). Under 'SSL Protocols', 'TLSv1', 'TLSv1.1', and 'TLSv1.2' are selected. The 'SSL Ciphers' dropdown is open, showing a list of ciphers: ECDH+AESGCM, EDH+AESGCM, AES256+EECDH, AES256+EDH, AES128-GCM-SHA256, AES128-SHA, AES128-SHA256, AES256+EDH, AES256+EECDH, AES256-GCM-SHA384, and AES256-SHA. The 'Advisory Notice & Consent Banner' section is visible below, with the 'Advisory Notice' toggle set to 'OFF'.</p>
<p>Advisory Notice & Consent Banner</p>	
<p>Advisory Notice</p>	<p>When enabled, the banner will appear when users sign in (console, SSH and Web interface) and remain on the screen until the administrator acknowledges the usage conditions and takes explicit actions for further access. The banner is typically an advisory/warning notice to be displayed before the Sign-in page. To enable the banner (as shown in the text box), toggle the Advisory Notice button to On. Type or copy the banner text into the text box.</p>

Installing System Updates

When you first receive the Haivision EMS appliance, the necessary software is pre-installed on it. System updates are issued through the [Haivision Support Portal](#).

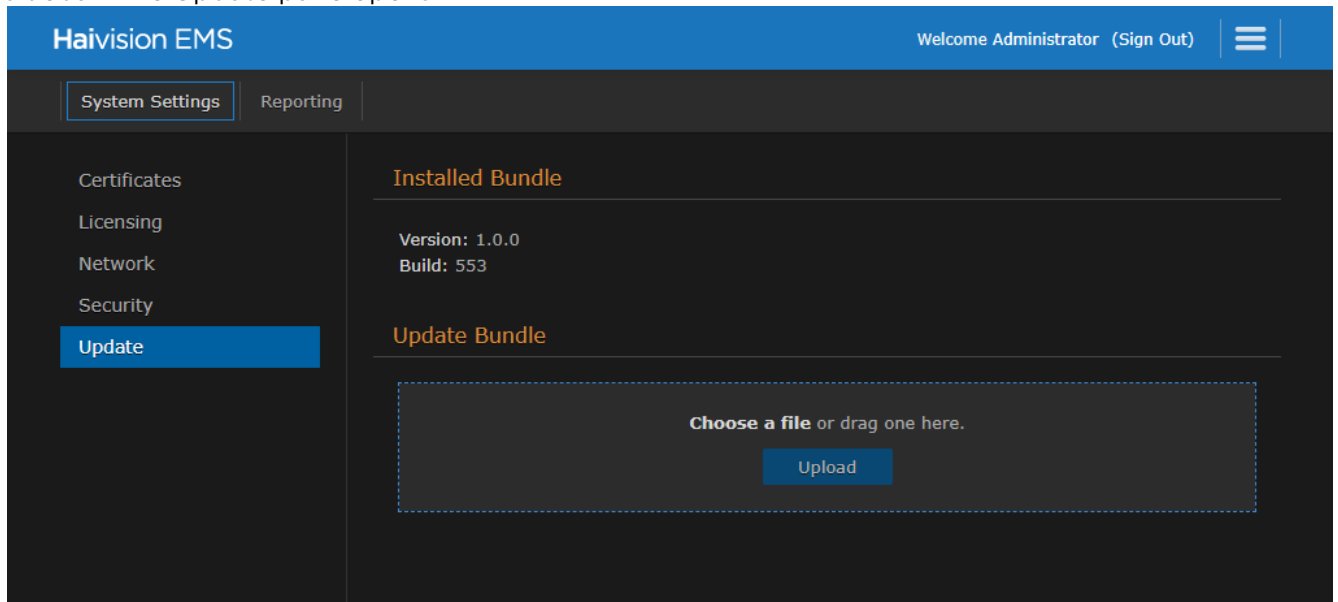
Note

For major releases, you need to apply a valid license key before or after the update (see [Managing Licenses](#)). Please contact Haivision Technical Support to obtain a valid license key. Only customers under a maintenance agreement can obtain an update package. If you install an update without a valid license key, EMS will not function. You cannot installed system updates from a mobile device.

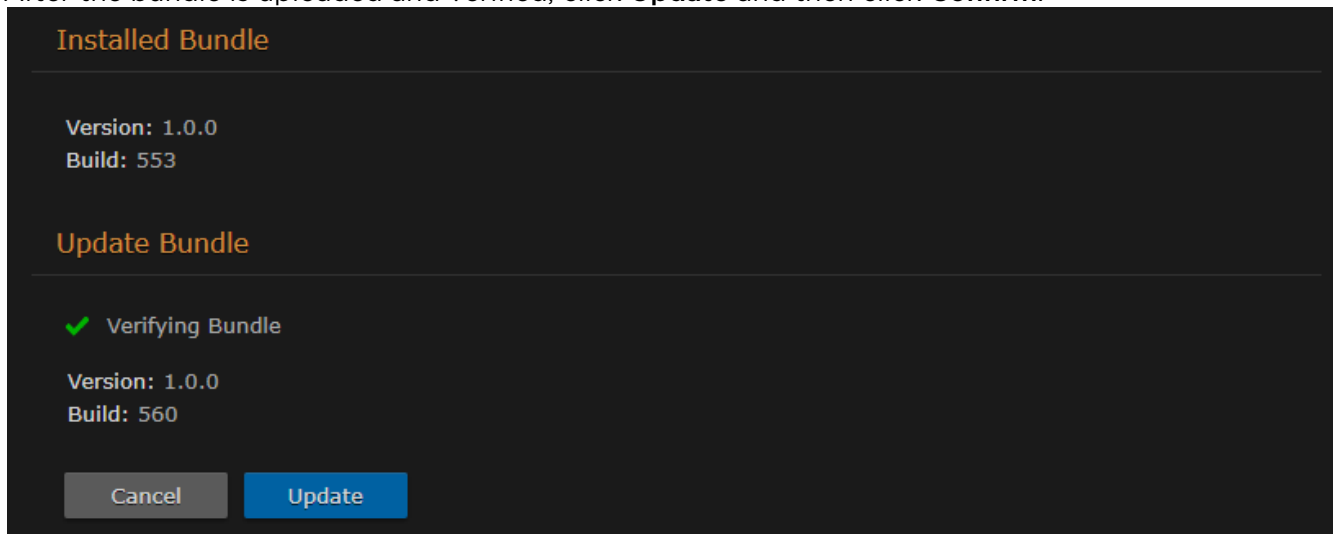
The system update is entitled `ems-xxxxx_rxxxxx_release.hai` , which when loaded replaces the application on your EMS.

To install a system update:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Update** on the sidebar. The Update pane opens:



2. Drag an update bundle to the drop area or click **Choose a file** to select a bundle to load.
3. After you select the bundle, a confirmation appears showing the filename. Click **Upload** to continue. The progress bar shows the progress of the upload.
4. After the bundle is uploaded and verified, click **Update** and then click **Confirm**.



5. Wait until the update is complete and the appliance restarts.
6. After the appliance restarts, the browser displays the EMS Sign-in screen (depending on your Web browser and settings). If not, reload your browser.
7. Sign in and ensure the system is functional.


Reporting

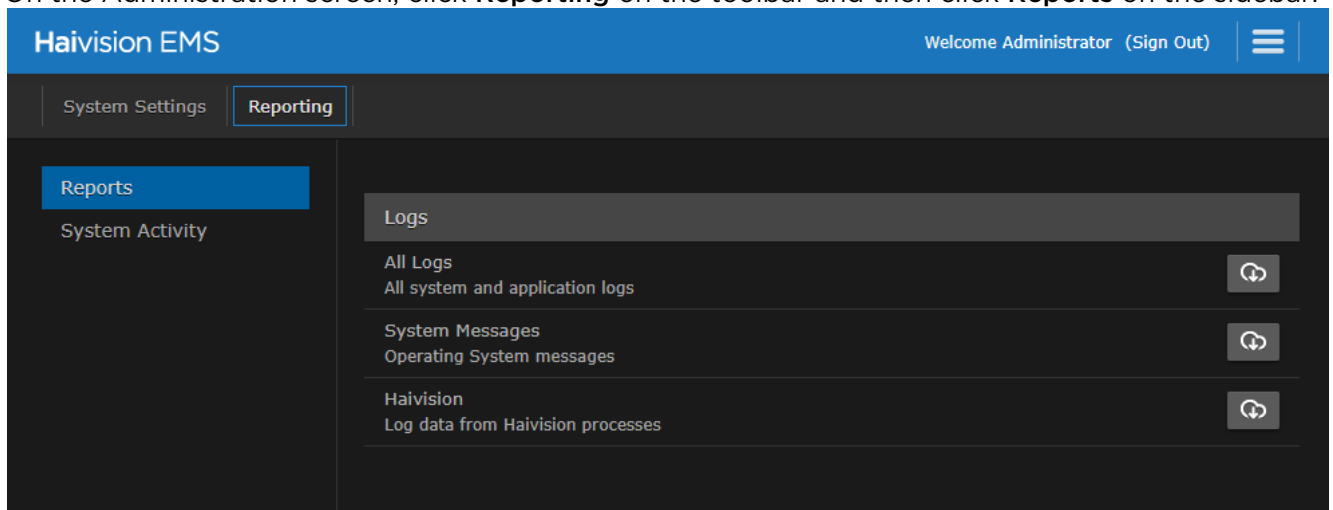
The Administration Reporting screen includes two panes: Reports and System Activity.

The Reports pane lists system logs that you can download in CSV file format. For the list of available logs, see [System Logs](#).

Viewing Reports

To view the reports:

1. To navigate the Administration screen, click the  icon on the banner and select **Administration** from the navigation drop-down menu.
2. On the Administration screen, click **Reporting** on the toolbar and then click **Reports** on the sidebar.



3. To download an activity report or log to your local system, click the  icon.

Topics Discussed

- [System Logs](#)
- [Viewing System Activity](#)

System Logs

The following table lists the available reports and logs:

Log Item	Description
All Logs	All system and application logs.
System Messages	A log of messages generated by the operating system.

Log Item	Description
Haivision	Log data from Haivision processes.

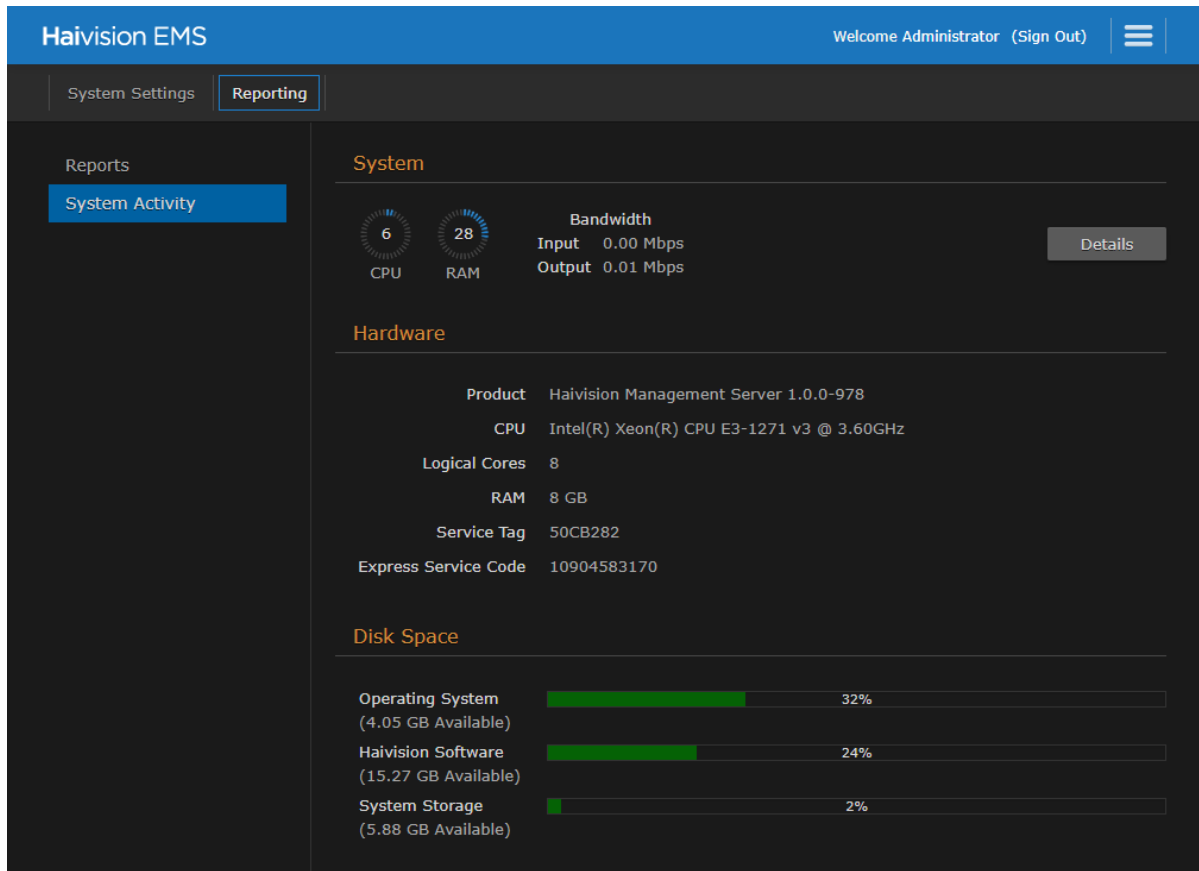
Viewing System Activity

The System Activity pane summarizes:

- Real-time system status information, such as CPU and memory usage, and I/O bandwidth rates, with the option to view graphical details.
- Hardware details, including whether EMS is running on a VM or a Haivision appliance.
- The available space for the operating system, Haivision software, and system storage (in GBs available, as well as percent used).

To view the System Activity:

1. On the Administration screen, click **Reporting** on the toolbar and then click **System Activity** on the sidebar.



Tip

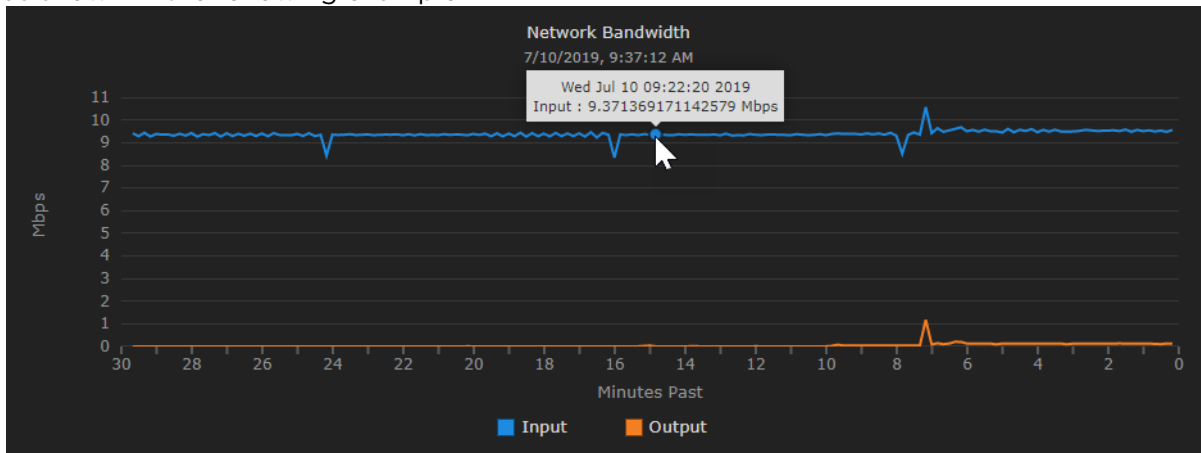
The color of the bars in the Disk Space graph change to orange when the space used on disk reaches 75%, and then to red when it reaches 90%.

2. To view the Network Bandwidth, CPU, and Memory graphs, click **Details**. The X-axis units are days, hours, or minutes past (corresponding to the selected Time Scale). The Y-axis units are as follows:
 - Network (Bandwidth) Usage (megabits per second).
 - CPU (Load) Usage (percentage).

- Memory Usage (percentage used).



3. You can adjust the Refresh Rate (from 1 second to 30 minutes) and the Time Scale (from 5 minutes to 30 days past) for the graphs.
4. To fine-tune the Bandwidth usage graph, select the data to include: Input and/or Output (playback).
5. To display an exact reading for the time and usage, you can mouse over the any of the graph lines, as shown in the following example.



Warranties

1-Year Limited Hardware Warranty

Haivision warrants its hardware products against defects in materials and workmanship under normal use for a period of ONE (1) YEAR from the date of equipment shipment ("Warranty Period"). If a hardware defect arises and a valid claim is received within the Warranty Period, at its option and to the extent permitted by law, Haivision will either (1) repair the hardware defect at no charge, or (2) exchange the product with a product that is new or equivalent to new in performance and reliability and is at least functionally equivalent to the original product. A replacement product or part assumes the remaining warranty of the original product or ninety (90) days from the date of replacement or repair, whichever is longer. When a product or part is exchanged, any replacement item becomes your property and the replaced item becomes Haivision's property.

EXCLUSIONS AND LIMITATIONS

This Limited Warranty applies only to hardware products manufactured by or for Haivision that can be identified by the "Haivision" trademark, trade name, or logo affixed to them. The Limited Warranty does not apply to any non-Haivision hardware products or any software, even if packaged or sold with Haivision hardware. Manufacturers, suppliers, or publishers, other than Haivision, may provide their own warranties to the end user purchaser, but Haivision, in so far as permitted by law, provides their products "as is".

Haivision does not warrant that the operation of the product will be uninterrupted or error-free. Haivision does not guarantee that any error or other non-conformance can or will be corrected or that the product will operate in all environments and with all systems and equipment. Haivision is not responsible for damage arising from failure to follow instructions relating to the product's use.

This warranty does not apply:

- (a) to cosmetic damage, including but not limited to scratches, dents and broken plastic on ports;
- (b) to damage caused by accident, abuse, misuse, flood, fire, earthquake or other external causes;
- (c) to damage caused by operating the product outside the permitted or intended uses described by Haivision;
- (d) to a product or part that has been modified to alter functionality or capability without the written permission of Haivision; or
- (e) if any Haivision serial number has been removed or defaced.

TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND REMEDIES PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS OR IMPLIED. AS PERMITTED BY APPLICABLE LAW, HAIVISION SPECIFICALLY DISCLAIMS ANY AND ALL STATUTORY OR IMPLIED WARRANTIES,

INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS. IF HAIVISION CANNOT LAWFULLY DISCLAIM STATUTORY OR IMPLIED WARRANTIES THEN TO THE EXTENT PERMITTED BY LAW, ALL SUCH WARRANTIES SHALL BE LIMITED IN DURATION TO THE DURATION OF THIS EXPRESS WARRANTY AND TO REPAIR OR REPLACEMENT SERVICE AS DETERMINED BY HAIVISION IN ITS SOLE DISCRETION. No Haivision reseller, agent, or employee is authorized to make any modification, extension, or addition to this warranty. If any term is held to be illegal or unenforceable, the legality or enforceability of the remaining terms shall not be affected or impaired.

EXCEPT AS PROVIDED IN THIS WARRANTY AND TO THE EXTENT PERMITTED BY LAW, HAIVISION IS NOT RESPONSIBLE FOR DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO LOSS OF USE; LOSS OF REVENUE; LOSS OF ACTUAL OR ANTICIPATED PROFITS (INCLUDING LOSS OF PROFITS ON CONTRACTS); LOSS OF THE USE OF MONEY; LOSS OF ANTICIPATED SAVINGS; LOSS OF BUSINESS; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION; LOSS OF, DAMAGE TO OR CORRUPTION OF DATA; OR ANY INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE HOWSOEVER CAUSED INCLUDING THE REPLACEMENT OF EQUIPMENT AND PROPERTY, ANY COSTS OF RECOVERING, PROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED OR USED WITH HAIVISION PRODUCTS AND ANY FAILURE TO MAINTAIN THE CONFIDENTIALITY OF DATA STORED ON THE PRODUCT. THE FOREGOING LIMITATION SHALL NOT APPLY TO DEATH OR PERSONAL INJURY CLAIMS, OR ANY STATUTORY LIABILITY FOR INTENTIONAL AND GROSS NEGLIGENT ACTS AND/OR OMISSIONS.

OBTAINING WARRANTY SERVICE

Before requesting warranty service, please refer to the documentation accompanying this hardware product and the Haivision Support Portal <https://support.haivision.com>. If the product is still not functioning properly after making use of these resources, please contact Haivision or Authorized Reseller using the information provided in the documentation. When calling, Haivision or Authorized Reseller will help determine whether your product requires service and, if it does, will inform you how Haivision will provide it. You must assist in diagnosing issues with your product and follow Haivision's warranty processes.

Haivision may provide warranty service by providing a return material authorization ("RMA") to allow you to return the product in accordance with instructions provided by Haivision or Authorized Reseller. You are fully responsible for delivering the product to Haivision as instructed, and Haivision is responsible for returning the product if it is found to be defective. Your product or a replacement product will be returned to you configured as your product was when originally purchased, subject to applicable updates. Returned products which are found by Haivision to be not defective, out-of-warranty or otherwise ineligible for warranty service will be shipped back to you at your expense. All replaced products and parts, whether under warranty or not, become the property of Haivision. Haivision may require a completed pre-authorized form as security for the retail price of the replacement product. If you fail to return the replaced product as instructed, Haivision will invoice for the pre-authorized amount.

APPLICABLE LAW

This Limited Warranty is governed by and construed under the laws of the Province of Quebec, Canada.

This Limited Hardware Warranty may be subject to Haivision's change at any time without prior notice.

EULA - End User License Agreement

READ BEFORE USING

THE LICENSED SOFTWARE IS PROTECTED BY COPYRIGHT LAWS AND TREATIES. READ THE TERMS OF THE FOLLOWING END USER (SOFTWARE) LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE ACCESSING THE LICENSED SOFTWARE. BY SCANNING THE QR CODE TO REVIEW THIS AGREEMENT AND/OR ACCESSING THE LICENSED SOFTWARE, YOU CONFIRM YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, HAIVISION IS UNWILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO ACCESS THE LICENSED SOFTWARE.

Click the following link to view the Software End-User License Agreement: [Haivision EULA.pdf](#)

If you have questions, please contact legal@haivision.com

SLA - Service Level Agreement

1. Introduction

This Service Level and Support supplement forms a part of and is incorporated into the Service Agreement (the "Agreement") between You and Haivision Network Video Inc. ("Haivision"). Capitalized terms used but not otherwise defined in this supplement shall have the meaning ascribed to them in the Agreement. Haivision may, upon prior written notice to You, amend this supplement to incorporate improvements to the service levels and support commitments at no additional cost to You. This supplement applies only to those products and services set forth below.

2. Definitions

- "Audience Member" means an individual or entity that accesses Your Published Media Objects through a public URL.
- "Access Service" means the service provided by Haivision VCMS that verifies an Audience Member's credentials.
- "Digital Media File" means a computer file containing text, audio, video, or other content.
- "Outage" is a 12-minute period of consecutive failed attempts by all six agents to PING the domain on the Haivision Streaming Media network.
- "Published Media Object" means a Digital Media File with a public URL.
- "Transaction" means the creation of a right for an Audience Member to access a Media Object and the completion of an order logged in the order history service.

3. Service Levels for the Video Content Management System

The service levels in this [Section 3](#) apply only to the hosted version of Haivision VCMS and the Haivision VCMS development kit (collectively, the "Standard Hosted Components" of Haivision Video Cloud Services). Subject to the exceptions noted in [Section 4](#) below, the aforementioned components of Haivision Video Cloud Services will be available for use over the course of each calendar month as follows:

Type of Access	Definition	Availability Level
Write Functions	<ul style="list-style-type: none"> • Access to all functions through the administrative user interface. • Ability to add or modify objects and metadata through the application programming interface (“API”) • Ability of ingest service to check for new or updated files or feeds 	99.999%
Read-Only Functions	<ul style="list-style-type: none"> • Ability to retrieve data through the API • Ability for Audience Members to authenticate through the Access Service • Ability for Audience Members to play Published Media Objects • Ability for Audience Members to play Haivision VCMS-authenticated or entitled Published Media Objects • Ability to complete Transactions 	99.999%

4. Exceptions to Availability for the VCMS

The Standard Hosted Components may not be available for use under the following circumstances, and in such case such periods of unavailability shall not be counted against Haivision Video Cloud for purposes of calculating availability:

- a. Normal Maintenance, Urgent Maintenance and Upgrades as defined in the table below;
- b. Breach of the Agreement by You as defined in the Agreement;
- c. The failure, malfunction, or modification of equipment, applications, or systems not controlled by Haivision Video Cloud;
- d. Any third party, public network, or systems unavailability;
- e. Acts of Force Majeure as defined in the Agreement;
- f. Modification of software made available to You as part of Haivision Video Cloud Services by You or a third party acting on Your behalf; and
- g. Any third party product or service not incorporated into Haivision Video Cloud Services or any third party plug-in.

Haivision Video Cloud shall make commercially reasonable efforts to notify, or work with, applicable third parties to repair or restore Haivision VCMS functionality affected by such exceptions.

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Normal	<ul style="list-style-type: none"> • Preventive maintenance on the software/hardware components of Haivision VCMS • Addition of new features/functions • Repair errors that are not immediately affecting Your use of Haivision VCMS 	No	Yes	10 Hours	6 Hours	10:00p m - 5:00a m	48 Hours
Urgent	<ul style="list-style-type: none"> • Repair errors that are immediately affecting Your use of Haivision VCMS 	No	Yes	30 Minutes	15 Minutes	Any Time	3 Hours

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Upgrades	<ul style="list-style-type: none"> Perform upgrades on software or hardware elements necessary to the long term health or performance of Haivision VCMS, but which, due to their nature, require that certain components of Haivision VCMS to be shut down such that no access is possible 	No	No	1 Hour	1 Hour	12:00am - 4:00am M-F	5 Days

5. Credits for Downtime for the VCMS

Haivision Video Cloud will grant a credit allowance to You if You experience Downtime in any calendar month and you notify Haivision Video Cloud thereof within ten (10) business days after the end of such calendar month. In the case of any discrepancy between the Downtime as experienced by You and the Downtime as measured by Haivision Video Cloud, the Downtime as measured by Haivision Video Cloud shall be used to calculate any credit allowance set forth in this section. Such credit allowance shall be equal to the pro-rated charges of one-half day of Fees for each hour of Downtime or fraction thereof. The term “Downtime” shall mean the number of minutes that Standard Hosted Components are unavailable to You during a given calendar month below the availability levels thresholds in [Section 3](#), but shall not include any unavailability resulting from any of the exceptions noted in [Section 4](#). Within thirty (30) days after the end of any calendar month in which Downtime occurred below the availability levels thresholds in [Section 3](#), Haivision Video Cloud shall provide You with a written report detailing all instances of Downtime during the previous month. Any credit allowances accrued by You may be offset against any and all Fees owed to Haivision Video Cloud pursuant to the Agreement, provided that a maximum of one month of credit may be accrued per month.

6. Support Services for the VCMS

Support for Haivision Video Cloud Services as well as the Application Software (defined as the VCMS application software components that Haivision licenses for use in conjunction with the Video Cloud Services) can be reached at hvc-techsupport@haivision.com and shall be available for all Your support requests. Haivision Video Cloud will provide 24x7 monitoring of the Standard Hosted Components.

Cases will be opened upon receipt of request or identification of issue, and incidents will be routed and addressed according to the following:

Severity Level	Error State Description	Status Response Within	Incident Resolution within
1 - Critical Priority	Renders Haivision VCMS inoperative or causes Haivision VCMS to fail catastrophically.	15 minutes	4 hours
2 - High Priority	Affects the operation of Haivision VCMS and materially degrades Your use of Haivision VCMS.	30 minutes	6 hours
3 - Medium Priority	Affects the operation of Haivision VCMS, but does not materially degrade Your use of Haivision VCMS.	2 hours	12 hours

Severity Level	Error State Description	Status Response Within	Incident Resolution within
4 - Low Priority	Causes only a minor impact on the operation of Haivision VCMS.	1 business day	3 business days

7. Service Levels for Haivision Streaming Media Service

Haivision agrees to provide a level of service demonstrating 99.9% Uptime. The Haivision Streaming Media Service will have no network Outages.

The following methodology will be employed to measure Streaming Media Service availability:

Agents and Polling Frequency

- a. From six (6) geographically and network-diverse locations in major metropolitan areas, Haivision’s Streaming Media will simultaneously poll the domain identified on the Haivision Streaming Media network.
- b. The polling mechanism will perform a PING operation, sending a packet of data and waiting for a reply. Success of the PING operation is defined as a reply being received.
- c. Polling will occur at approximately 6-minute intervals.
- d. Based on the PING operation described in (b) above, the response will be assessed for the purpose of measuring Outages.

If an Outage is identified by this method, the customer will receive (as its sole remedy) a credit equivalent to the fees for the day in which the failure occurred.

Haivision reserves the right to limit Your use of the Haivision Streaming Media network in excess of Your committed usage in the event that Force Majeure events, defined in the Agreement, such as war, natural disaster or terrorist attack, result in extraordinary levels of traffic on the Haivision Streaming Media network.

8. Credits for Outages of Haivision Streaming Media Service

If the Haivision Streaming Media network fails to meet the above service level, You will receive (as your sole remedy) a credit equal to Your or such domain’s committed monthly service fee for the day in which the failure occurs, not to exceed 30 days of fees.

9. No Secondary End User Support

UNDER NO CIRCUMSTANCES MAY YOU PROVIDE CONTACT INFORMATION FOR HAIVISION SERVICES TO CUSTOMERS OR AUDIENCE MEMBERS OR OTHER THIRD PARTIES WITHOUT HAIVISION’S EXPRESS PRIOR WRITTEN CONSENT.

Getting Help

<p>General Support</p>	<p>North America (Toll-Free) 1 (877) 224-5445</p> <p>International 1 (514) 334-5445</p> <p><i>and choose from the following:</i> Sales - 1, Cloud Services - 3, Support - 4</p>
<p>Managed Services</p>	<p>U.S. and International 1 (512) 220-3463</p>
<p>Fax</p>	<p>1 (514) 334-0088</p>
<p>Support Portal</p>	<p>https://support.haivision.com</p>
<p>Product Information</p>	<p>info@haivision.com</p>

