AVIGILON™

Avigilon HDVA3X IPMI Kit Installation and Operations Guide

VMA-AS3X-IPMI

For

VMA-AS3X-24P	VMA-AS3X-16P
VMA-AS3X-8P	

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

20230601

Table of Contents

Introduction

Avigilon provides an optional Intelligent Platform Management Interface (IPMI) Module Kit for the HD Video Appliance 3X (HDVA3X). This kit provides you with enhanced remote control for the HDVA3X appliance, to more easily control and monitor HDVA3X appliances from a central location.

Part Number	Description
VMA-AS3X-IPMI	HDVA3X IPMI Module Accessory Kit

Important: The IPMI module is only compatible with the HDVA3X model video appliance. Earlier HDVA appliances do not support this accessory. A full list of the supported appliances is available below.

Supported HD Video Appliances

VMA-AS3X-24P24	VMA-AS3X-16P12	VMA-AS3X-8P8
VMA-AS3X-24P18	VMA-AS3X-16P09	VMA-AS3X-8P4
VMA-AS3X-24P12	VMA-AS3X-16P06	VMA-AS3X-8P2

Confirm Package Contents

Confirm that the kit you are installing contains the following components:

- 1 × IPMI module
- 3 × screws
- 3 × standoffs

Required Tools

The following tools are not included in the kit package, but are needed to complete the installation:

- HDVA3X appliance (8/16/24 port)
- Monitor
- Keyboard and mouse
- Phillips #2 screwdriver

Important: It is recommended that you always use an antistatic mat and antistatic strap while working on components inside the system.

Before You Begin

Important: The IPMI module is only compatible with the HDVA3X model video appliance. Earlier HDVA appliances do not support this accessory. Before starting the installation you will confirm that you have the correct model of HDVA for the IPMI module, and find the serial number that will be needed later in the process.

1. Confirm that the HD Video Appliance is an HDVA3X (model number VMA-AS3X). Confirm by checking the label on the bottom of the appliance.
2. When checking the label for the model number, note down the serial number listed in the top left section of the label. This serial number will be needed to enter BIOS later.

In cases where the label is missing or unreadable

1. Boot up the appliance and login.
2. Open the command line interface.

   Press the **Windows key** + **R** and the enter **cmd** in the Run dialog that opens.
3. Enter the following command to retrieve the model number information:

```
wmic COMPUTERSYSTEM get SystemSKUNumber
```

4. Enter the following command to retrieve the serial number information:

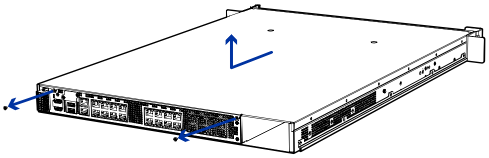
```
wmic BIOS get SerialNumber
```

Installing the IPMI Module

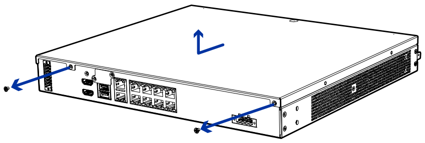
The following steps will install the IPMI module in your HDVA3X appliance.

Important: It is recommended that you always use an antistatic mat and antistatic strap while working on components inside the system.

1. If turned on, power down the HDVA3X appliance.
2. Disconnect the power cord.
3. Use a Phillips #2 screwdriver to remove the two M2 screws on the back of the unit that secure the lid in place.

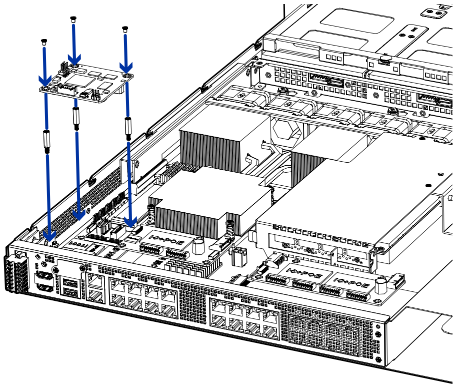


VMA-AS3X-24P/16P

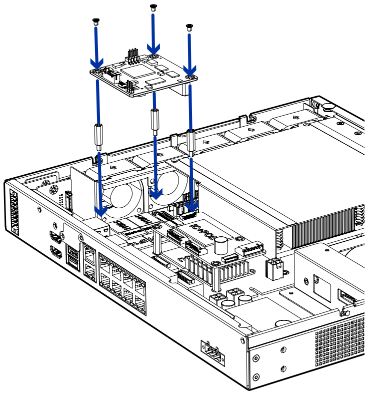


VMA-AS3X-8P

4. Remove the lid by sliding it towards the back of the unit and then lifting the side of the lid with the screw holes up.
5. Install the IPMI module board to the location shown below.

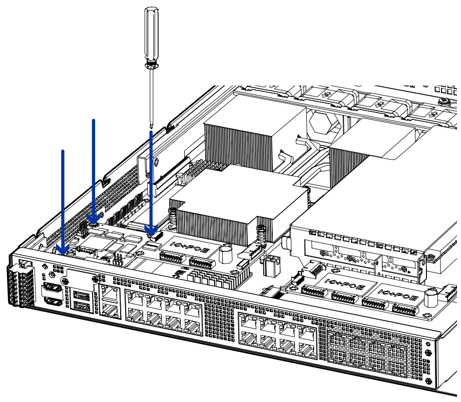


VMA-AS3X-24P/16P

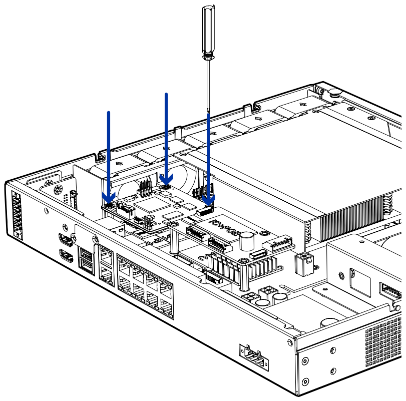


VMA-AS3X-8P

6. Secure the IPMI module board to the appliance with the three standoffs and M3 screws provided.

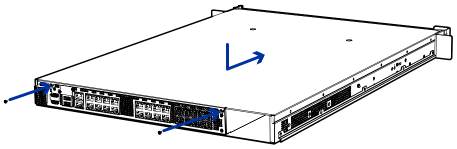


VMA-AS3X-24P/16P

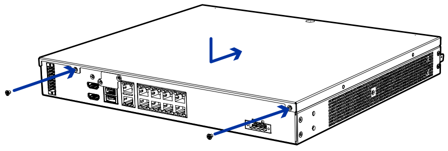


VMA-AS3X-8P

7. Replace the lid back onto the unit and secure it in place with the two M2 screws.

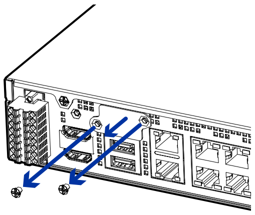


VMA-AS3X-24P/16P

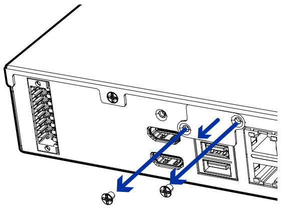


VMA-AS3X-8P

8. By default, the IPMI Web interface IP address is set to 192.168.1.2.
    - If you want to set the IPMI to DHCP, see *Configuring DHCP* on the next page.
    - If you want to continue using the default IP address, see *Accessing the IPMI Web Interface the First Time* on page 13
9. Remove the two M2 Phillips screws that are securing the cover for the IPMI module Ethernet port to connect the Ethernet cable.



VMA-AS3X-24P/16P

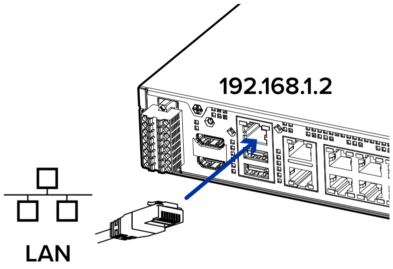


VMA-AS3X-8P

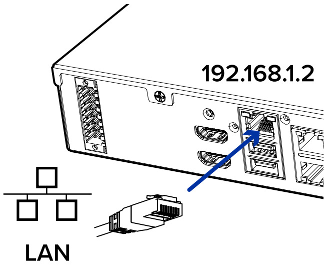
Configuring DHCP

Note: The IPMI module is set to use the 192.168.1.2 static IP address by default. Use the process below to switch to DHCP instead of the default static IP address. If you want to continue using the default static IP address, proceed to *Accessing the IPMI Web Interface the First Time* on the next page.

1. Use a Cat5e Ethernet cable to connect the IPMI module Ethernet port to a DHCP server.



VMA-AS3X-24P/16P



VMA-AS3X-8P

2. Power on the HDVA3X appliance and press the **Delete** key when prompted on the black Avigilon splash screen next to the BIOS option. You will be prompted to enter a password.
3. Enter the unit's serial number as noted earlier in the process. For more information, see *Before You Begin* on page 8.
4. Navigate to the **Server Mgmt** page using the arrow keys on the keyboard.
5. Select **BMC network configuration** and press **Enter**.
6. On the BMC network configuration page, scroll down to **Configuration Address source** and change the option to **DynamicBmcDhcp**.
7. Navigate to the **Save & Exit** tab and select **Save Changes and Reset** by using the arrow keys on the keyboard, and press **Enter**.
8. Check the assigned DHCP address via BIOS for the IP address, by navigating to the **Server Mgmt** tab, go to the **BMC network configuration** option and check the IP address on the right of the Station IP Address line under **Lan Channel 1**.

   Note: If you are connected to a DHCP server an IP address will be automatically assigned.

Accessing the IPMI Web Interface the First Time

To access the IPMI web interface, you will need a computer on the same network as the IPMI module and you will need to know the IP address of the IPMI module. The default static IP address is 192.168.1.2. If you switched the IPMI module to use DHCP to assign IP addresses, contact your network administrator or otherwise discover the assigned IP address of the IPMI module.

1. Open a web browser on a computer on the same network as the IPMI module.
2. Enter `https://` and the IP address of the IPMI module in the browser's address bar and press Enter.

   The default static IP address is 192.168.1.2.
3. Use the default login credentials below to login to the IPMI web interface.
   - Username: admin
   - Password: admin

Note: To use the forgot my password option on the login screen, you must add an email address to the user account for the one time password email to be sent to and configure the SMTP settings for sending the email. For more information, see *Setting Up Email Password Recovery* on page 53.

Overview

The IPMI functionality of the HD Video Appliance is intended to comply with IPMI 2.0.

Functional Description

The IPMI module will provide the following functions on the HD Video Appliance platform. These functions cover the management of the platform, sensor monitoring, event logs, power/reset control, I2C access to internal non-intelligent devices, and firmware upgrades of the IPMI module.

Power and Reset Control

All power and reset control can be completed by issuing corresponding IPMI commands. The IPMI module supports cold and warm resets. Resetting the IPMI module will not affect the system's operation.

- Cold Reset: This command will cause the default settings to be restored. A SelfTest will also run as part of this reset.
- Warm Reset: This command will reset the communication interface and the current settings will be left as they are.

Firmware Upgrade

The IPMI module supports HPM.1 specification upgrading with rollback capability through either the LAN or the KCS interface.

Cooling Management

The smart fan of the HD Video Appliance is controlled by BIOS instead of the IPMI module.

KVM (Kernel Virtual Machine) Control

The KVM control is HTML5-based. This web-based user interface allows you to easily monitor the HD Video Appliance hardware information, including temperatures, fan rotations, voltages, and power. This application also lets you instantly power on/off or reset the HD Video Appliance.

Messaging Interface

The messaging interfaces comply with IPMI v2.0. You can learn more about IPMI messaging interfaces in general in the *IPMI v2.0 Specification, Chapter 6 IPMI Messaging Interfaces, Chapter 9 Keyboard Controller Style (KCS) Interface, and Chapter 13 IPMI LAN Interface*.

To meet the IPMI v2.0 specification, two channels are provided:

- **KCS Channel**: For communicating with the system payload (x86 motherboard).
- **LAN Channel**: Using the side-band interface NC-SI of the HD Video Appliance network interface card. For the LAN port location, see *Configuring DHCP* on page 12.

Using the IPMI Web Interface

The IPMI web-based user interface allows you to easily monitor the remote server's hardware information such as temperatures, fan rotations, voltages and power. You can also remotely power on/off or reset the HD Video Appliance.

Browser Setting Requirements

To properly use the IPMI web interface, use the following browser settings:

Allow File Downloads From This Site

For Internet Explorer: Navigate to **Tools** > **Internet Options** > **Security** tab. Based on your device setup, select from Internet, Local intranet, trusted sites and restricted sites. Click **Custom level**. In the Security Settings - Zone dialog box, find the Download options under settings and enable the **File download** option. Click **Ok** on all of the dialog boxes to save the changes.

For all other browsers: Accept the file download option when prompted.

Enable Java Script for This Site

If not already enabled, go to your browser's settings to enable java script for this site.

Enable Cookies for This Site

If not already enabled, change your browser's settings to allow cookies for this site.

Avoid Using the Following Browser Functions

Once you have logged in to the IPMI web interface, avoid using the following browser functions:

- Refresh button
- Refresh menu
- Back and Forward buttons
- F5 on the keyboard
- Backspace on the keyboard

Dashboard

Click **Dashboard** to view the overall information and status of the HD Video Appliance.

From this page you can view a quick overview of system events, logs and sensor monitoring.

Sensor Readings

Click **Sensor** to view sensor related information on the **Sensor Readings** page.

From this page you can click on any sensor to view more information about that particular sensor, including thresholds and a graphical representation of all associated events.

The Sensor Readings page provides live readings of all of the available sensors, including details like the Sensor Name, Status, Current Reading, and Behavior. You can also choose the types of sensors that you want to display in the list.

Logs & Reports

Expand **Logs & Reports** on the side menu to access the following pages:

- IPMI Event Log
- System Log
- Audit Log

IPMI Event Log

This page lists the event logs from the different sensors on this device. Double-click on a log to see its details.

You can sort the list by clicking on any of the column headers. You can filter the list by date, event type, or sensor type.

You can click **Clear Event Logs** to delete the event logs.

System Log

This page lists the system events that have occurred on the device.

Note: Logs must be configured under **Settings** > **Log Settings** in order to display event entries. For more information, see *Log Settings* on page 21.

You can filter the list by date and event category.

Audit Log

This page lists any system events that have occurred on the device that have been configured as audit logs.

Note: Logs must be configured under **Settings** > **Log Settings** > **Advanced Log Settings** in order to display event entries. For more information, see *Log Settings* on page 21.

IPMI Settings

From the Settings page you can access various configuration settings for the IPMI module. See the sections below for more information on the different settings pages available.

Captured BSOD

This page captures a screenshot of the blue screen and error messages that displays in the event of the system crashing. If the system crashed since the last reboot and you want to find more details about the crash, you can check this settings page for a screenshot of the blue screen message that was displayed just before the crash.

Note: KVM service should be enabled to display the BSOD screen capture. KVM service can be configured from **Settings** > **Services** > **KVM**.

Date & Time Settings

This page is used to set the date and time of the IPMI module. You can set the date and time manually or automatically using an NTP service. See below for more details.

Select the Time Zone

Use the **Select Time Zone** drop-down list or the map to select the time zone for your location. This will then display the exact local time for that time zone.

Automatically Set the Date & Time with an NTP Server

Select your time zone and then check the **Automatic NTP Date & Time** checkbox to enable the IPMI module date and time to be set by an NTP server.

Enter the NTP server hostname that should be used to automatically set the date and time in the **Primary NTP Server** field. In the **Secondary NTP Server** field, enter the NTP server hostname for the server that will be used if the primary server cannot be reached. The secondary NTP server is optional. Click **Save** to save these settings for your IPMI date and time.

Manually Set the Date & Time

If you select to manually set the date and time, the map will be disabled for selecting the time zone. Use the **Select Time Zone** drop-down list to select the time zone.

External User Services

From the External User Services page you can access various configuration settings for external user services such as connecting to an LDAP directory or using the RADIUS (Remote Authentication Dial-in User Service) protocol for dial-in users. See the sections below for more information on the external users services available.

LDAP / E-Directory Settings

From the Lightweight Directory Access Protocol (LDAP) / E-Directory Settings page you need an LDAP or E-directory server on your network to authenticate IPMI users. This is done by passing login requests to your LDAP server and helps to keep authentication centralized and avoid the need to create and update users in multiple locations.

> **Important:** The LDAP feature will not work with any version of Windows Server implementations of LDAP/AD. If possible, please use an implementation of LDAP/AD other than Windows Server.

Setting Up LDAP / E-Directory Authentication

1. Navigate to **Settings** > **External User Settings** > **LDAP/E-Directory Settings** > **General Settings**.
2. Check the **Enable LDAP/E-Directory Authentication** box to enable this option.
3. Select the **Encryption Type** to use when communicating with the LDAP server. If SSL is selected, make sure to use the correct port number.
4. Select **IP Address** as the **Common Name Type**.
5. Enter the IP address of the LDAP server in the **Server Address** field. The IPMI module supports both IPv4 and IPv6 address formats.
6. If you are using the StartTLS encryption type with FQDN, enter the FQDN address.
7. Enter the LDAP port number in the **Port** field.

   The default port is 389. For SSL connections the default port is 636. The port value ranges from 1 to 65535.
8. Enter the **Bind DN** that is used during the binding operation. This authenticates the client to the server.

   The Bind DN is a string of 4-64 alpha-numeric characters and it must start with an alphabetic character. Special characters such as `. , - _` = are allowed in positions other than the starting character.
9. Enter the **Password**.

   The password must be between 1-48 characters. White space is not supported.
10. Enter the **Search Base**. The search base defines which part of the external directory tree to be searched on the LDAP server. The search base may be something equivalent to the organization or group in the external directory.

    The Search Base is a string of 4-64 alpha-numeric characters and it must start with an alphabetic character. Special characters such as `. , - _` = are allowed in positions other than the starting character.
11. Use the **Attribute of User Login** drop-down menu to select the attribute that should be used by the LDAP/E-directory server to identify the user. The cn and uid attributes are supported by the IPMI module.
12. Click **Save** to save the settings.

Adding a New Role Group

1. Navigate to **Settings** > **External User Settings** > **LDAP/E-Directory Settings** > **Role Groups**.
2. Select a blank row and click **Add Role Group**. Alternatively you can double-click the blank row.
3. Enter a **Group Name** to identify the role group.

   The role group name is a string of up to 255 alpha-numeric characters. Special characters – and _ are supported.
4. Enter the **Group Domain** where the role group is located.

   The domain name is a string of 4-64 alpha-numeric characters and it must start with an alphabetic character. Special characters such as . , – _ = are allowed in positions other than the starting character.
5. Enter the privilege level of the group in the **Group Privilege** field. The options are: User, Administrator, Operator, or None.
6. Select the groups access for KVM and VMedia.
7. Click **Save** to save the new role group and return to the role group list.

RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite that includes servers, clients, development libraries and numerous additional RADIUS-related utilities. The RADIUS settings page is used to configure RADIUS authentication.

Configuring RADIUS Authentication

1. Navigate to **Settings** > **External User Settings** > **RADIUS Settings** > **General RADIUS Settings**.
2. Select the checkbox to **Enable RADIUS Authentication**.
3. Enter the IP address of the RADIUS server in the **Server Address** field. IPv4, IPv6, and FQDN formats are supported.
4. Enter the RADIUS port number in the **Port** field.

   The default port is 1812. The port value can range from 1 to 65535.
5. Enter the RADIUS server's authentication secret in the **Secret** field.

   The secret must be between 4-31 characters long. White space is not supported.
6. Click **Save** to save the settings.
7. Navigate to **Settings** > **External User Settings** > **RADIUS Settings** > **Advanced RADIUS Settings**.
8. For authorization purposes, configure the RADIUS user with Vendor Specific Attributes from the RADIUS server. If you change the vendor specific values on the RADIUS server, you should also update those values on this page.
   - Example 1 — testadmin:

     Auth-Type= PAP

     Cleartext-Password="admin"

     Auth-Type=PAP

     Vendor-Specific="H=4"
   - Example 2 — testoperator:

Auth-Type= PAP

Cleartext-Password="operator"

Auth-Type=PAP

Vendor-Specific="H=3"

9. Click **Save** to save your settings.

KVM Mouse Settings

The IPMI module has three options for handling mouse emulation from the local window to the remote screen on the KVM Mouse Setting page. Choose the mouse setting based on the operating system of the device you are remotely connecting to. For an HD Video Appliance, choose **Absolute Positioning (Windows)** and save the setting.

Only users with Administrator privileges can configure this option.

Log Settings

SEL Log Settings Policy

Navigate to **Settings** > **Log Settings** > **SEL Log Settings Policy**. On this page you can set the storage policy for the event logs. Select to enable either the **Linear Storage Policy** or the **Circular Storage Policy** and save the setting.

Circular logging generally performs better and is able to reuse logs and log storage. Linear logging offers more redundancy but would require more administration.

Advanced Log Settings

Use the Advanced Log Settings page to configure the log settings for the event log.

1. Navigate to **Settings** > **Log Settings** > **Advanced Log Settings**.
2. You can enable or disable system logs with the **System Log** checkbox.
3. Choose if the logs should be saved locally or remotely by select the **Local Log** and **Remote Log** checkboxes. One or both of the options can be selected, as required.

   Local files will be stored at `/var/log/`.
4. If the selected log type is Local:
   a. You can specify the maximum size of the local log files in bytes in the **File Size** field. Enter a value from 3 to 65535 bytes. When log files reach the maximum size, they will be backed up based on the Rotate Count setting.
   b. You can back up the log information in backup files when the logs reach their maximum file size, or have the old log information automatically cleared. The **Rotate Count** field supports the values **0** or **1**. Enter **0** if you want the logs to be cleared. Enter **1** if you want the logs to be backed up.
5. If the selected log type is Remote:

   a. Select the type of port used by the remote log server. Select either **UDP** or **TCP** in the **Port Type** field.
   b. Enter the server address in the **Remote Log Server** field. IPv4 and FQDN formats are supported. The maximum allowed size is 64 bytes.
   c. Enter the server port number in the **Remote Server Port** field.
6. Select the enable or disable Audit logs with the **Enable Audit Log** checkbox.
7. **Save** your settings.

Configuring the Remote Server to Enable Syslogging

Note: The following example uses FC13 as the remote machine to log syslog.

On the FC machine, enter the following lines for UDP in `/etc/rsyslog.conf`:

- `MODLOAD imudp`
- `UDPSERVER 514`

Media Redirection Settings

Use this page to configure the media redirection settings for the remote sessions.

1. Navigate to **Settings** > **Media Redirection Settings** > **Remote Session**.
2. Use the **KVM Single Port Application** checkbox to enable or disable single port support. When this setting is changed, any open KVM or VMedia sessions will be restarted.
   - When **KVM Single Port Application** is enabled: KVM sessions will not use their dedicated port. Both Web and KVM sessions will use be established using the Web port.
   - When **KVM Single Port Application** is disabled: KVM sessions and Web sessions will be established using their own respective dedicated ports.
3. Choose the **Keyboard Language** from the list of supported languages.
4. Enter the number of allowed attempts for retrying the redirection sessions in the **Retry Count** field.
5. Enter the time given for each retry attempt, in seconds, in the **Retry Time Interval (Seconds)** field.
6. Enable the **Automatically OFF Server Monitor When KVM Launches** checkbox to automatically lock the local monitor when a remote session is launched.
7. Click **Save** to save the settings.

Network Settings

Network IP Settings

Use this page to configure the network settings for the IPMI module.

1. Navigate to **Settings** > **Network Settings** > **Network IP Settings**.
2. Configure the network settings as either LAN or VLAN:
    - **LAN**:
        a. Check the **Enable LAN** checkbox.
        b. Select the **LAN Interface** to be configured from the drop-down list.
        c. Check the **Enable IPv4** checkbox to enable IPv4 settings on the LAN interface.
            - To have the IPv4 network settings dynamically configured using DHCP, check the **Enable IPv4 DHCP** checkbox.
            - If you don't use IPv4 DHCP, manually enter the **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway** in their respective fields.
        d. Check the **Enable IPv6** checkbox to enable IPv6 settings on the LAN interface.
            - To have the IPv6 network settings dynamically configured using DHCP, check the **Enable IPv6 DHCP** checkbox.
            - If you don't use IPv6 DHCP, manually enter the **IPv6 Address**, **Subnet Prefix Length**, and **IPv6 Index** in their respective fields.
        e. Click **Save** to save the settings.
    - **VLAN**:
        a. Check the **Enable VLAN** checkbox.
        b. Enter the **VLAN ID**. This value ranges from 2 to 4094 and is used to identify the VLAN configuration.
        c. Enter the **VLAN Priority**. This value ranges from 0 to 7, with 7 being the highest priority.
        d. Click **Save** to save the settings.

Network Link Configuration

This page is used to configure the network links for the available network interfaces.

1. Navigate to **Settings** > **Network Settings** > **Network Link Configuration**.
2. Select the **LAN Interface** to be configured from the drop-down list.
3. Select to enable or disable **Auto Negotiation**. When enabled, this option allows the IPMI module to perform automatic configuration of speed and duplex to achieve the best possible link.

    If Auto Negotiation is disabled, you will need to manually enter the **Link Speed** and **Duplex Mode** settings. Duplex mode can be either **Half Duplex** or **Full Duplex**. The Link Speed can be either 10 or 100. 1000 Mbps link speed only applies when Auto Negotiation is enabled.
4. Click **Save** to save the settings.

DNS Configuration

The Domain Name System (DNS) is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates assigned domain names to each device or service using DNS so that they will have a more meaningful name for users to recognize instead of their numerical identifiers. Use the DNS Configuration page to manage the DNS settings of your device.

1. Navigate to **Settings** > **Network Settings** > **DNS Configuration**.
2. Check the **DNS Enabled** checkbox.
3. Select the **Host Name Setting** option of **Automatic** or **Manual**. If Automatic is selected, the **Host Name** field will be read only and automatically filled. If Manual is selected, enter a **Host Name** in the field.
4. Check the **Register BMC** checkbox if you want to register the selected BMC Interface.

   If BMC registration is enabled, select the **Registration Method** you want to use:

   - **Nsupdate**: Register with the DNS server using the nsupdate application.
   - **DHCP Client FQDN**: Register with the DNS server using DHCP option 81.
   - **Hostname**: Register with the DNS server using DHCP option 12.

     Note: The Hostname registration method should only be selected if DHCP Client FQDN is not supported.

5. Select the **Domain Setting** option of **Automatic** or **Manual**.

   If Automatic is selected, the **Domain Name** field will be automatically filled and hidden The Domain Interface field will display instead.

   If Manual is selected, enter a **Domain Name** in the specified field.

6. Select the **Domain Name Server Setting** option of **Automatic** or **Manual**.

   If Automatic is selected, the manual entry fields will be hidden and the **DNS Interface** field will display instead. Select the DNS interface to use from the drop-down list.

   If Manual is selected, enter a **DNS Server Address** in the specified field.

7. Select the **IP Priority** option of **IPv4** or **IPv6**. This field is not applicable for manual configuration.

   If the IP Priority is IPv4, the device will have two IPv4 DNS servers and one IPv6 DNS server. If IPv6 is selected, the device will have two IPv6 DNS servers and one IPv4 DNS server.

8. Click **Save** to save the settings.

Platform Event Filters

The Platform Event Filters (PEF) are a mechanism to configure the IPMI module to take specific actions on event messages that it receives or has internally generated. The possible actions include operations such as powering off the system, resetting the system, and triggering an alert.

PEF Management is used to configure the following settings:

- Event Filters
- Alert Policies
- LAN Destinations

Event Filters

It is recommended to use platform event filtering to provide up to 40 entries in the event filter table. A subset of these entries should be used for pre-configured and common system failure events such as over-heating, power system failure, fan failure, and so on. The remaining entries can be made available for System Management Software configured events.

> **Note:** Individual entries can be tagged as reserved for system use. So the ratio of pre-configured entries and run-time configurable entries can be re-allocated as needed.

1. Navigate to **Settings** > **Platform Event Filters** > **Event Filters**. This page contains 40 pre-configured events with PEF IDs.
2. Click the Delete icon (**x**) in the top-right corner of a pre-configured entry to delete that entry.
3. To add a new event filter:
   a. Select an event filter section to open the Event Filter entry page. If you select a pre-configured event filter, that event filter will be deleted after adding the new one.
   b. Select the **Enable this filter** checkbox to enable this event filter.
   c. Pick a severity level from the **Event severity to trigger** drop-down list.
   d. **Alert** is checked by default in the **Event Filter Action** field. This enables PEF alert actions.
   e. If necessary, select a **Power Action** from the drop-down list. The options are to power down, power reset, or power cycle the device.
   f. Choose a configured **Alert Policy Group Number** from the drop-down list. Alert policies should be configured separately. For more information, see *Alert Policies* on the next page.
   g. Enable the **Raw Data** option to fill the Generator ID with raw data. Enter the raw data value for ID1 or ID2 in the **Generator ID 1** and **Generator ID 2** fields. Hexidecimal values should use the `0x` prefix.
   h. In the **Generator Type** section, select **Slave** if the event is generated by the connected device, or select **Software** if the event is generated from the system software.
   i. In the **Slave Address/Software ID** field, enter the corresponding device address if Slave was selected, or the software ID if Software was selected.
   j. In the **Channel Number** field, enter the channel that the event message is received over. Enter **0** if the event message is received through the system interface or is internally generated.
   k. Enter the corresponding **IPMB Device LUN** if the event is generated by the Intelligent Platform Management Bus (IPMB).
   l. Select the type of sensor that will trigger the event filter action from the **Sensor Type** drop-down list.
   m. Select the specific sensor that will trigger the event filter action from the **Sensor Name** drop-down list.
   n. In the **Event Options** drop-down list, select either **All Events** or **Sensor Specific Events**.
   o. Enter the event or reading value that triggers the event in the **Event Trigger** field. This value ranges from 1 to 255.
   p. Use the Event Data AND Mask field and Event Data Compare fields to specify either wildcard or compared bits of data. The following instructions are for event data #1, but this can be

configured for up to 3 sets of data.

   i. Enter a value from 0 to 255 in the **Event Data 1 AND Mask** field to indicate a wildcard or compared bit.
   ii. The **Event Data 1 Compare 1** and **Event Data 1 Compare 2** fields are used to indicate whether each bit position's comparison is exact or not.
   iii. If necessary, configure the event data 2 and event data 3 fields.

   q. Click **Save** to save the filter and return to the event filter list.

4. Click Delete to delete the existing filter.

Alert Policies

The Alert Policies page is used to configure the PEF configuration for alerts. You can add, modify, or delete entries on this page.

Adding an Alert Policy

1. Navigate to **Settings** > **Platform Event Filters** > **Alert Policies**. This page contains the Alert Policies that can be configured.
2. Select the Alert Policy Group Number that needs to be configured. This should be a policy number that corresponds with the policy you want to use with an event filter. Click on the empty slot to open the Alert Policies configuration page.
3. Select a **Policy Group Number** from the drop-down list. Make sure to select the policy number that corresponds with the policy you want to use with an event filter.
4. Check the **Enable this alert** checkbox.
5. Select a **Policy Action** from the drop-down list.
6. Choose an available **LAN Channel** from the drop-down list.
7. Use the **Destination Selector** to choose one of your configured LAN Destinations. LAN Destinations should be configured separately. For more information, see *LAN Destinations* on the next page.
8. If the alert policy entry is event specific, check the **Event Specific Alert String** checkbox.
9. Select any one value that is used to look up the alert string to send for this policy entry in the **Alert String Key** field.

   > **Note:** The option for event specific alert strings can be enabled here but the alert strings themselves must be configured using IPMI commands. In this case the command `Set PEF Config Parameter "Alert String"` should be used. For more information on using IPMI commands, see *IPMI Commands* on page 1.

10. Click **Save** to save the alert policy.

Deleting an Alert Policy

To delete a configured alert policy, click on the policy to open the settings and then click **Delete**.

LAN Destinations

The LAN Destinations page is used to configure the LAN destinations for PEF configuration. You can add, modify, or delete entries on this page.

Adding a LAN Destination

1. Navigate to **Settings** > **Platform Event Filters** > **LAN Destinations**. This page contains the LAN destinations that can be configured.
2. Select the LAN destination slot that needs to be configured. This should be a destination number that corresponds with the alert policy you want to use it with. Click on the empty slot to open the LAN Destination Configuration page.
3. Select **SNMP Trap** or **E-Mail** as the **Destination Type**.
   - E-Mail:
     a. Enter the email address that will receive the alerts in the **SNMP Destination Address** field.
     b. Select a **BMC Username** from the list of users. This user should be configured under User Management.
     c. Enter text to use in the email alert subject line in the **Email Subject** field.
     d. Enter text to use in the body of the email alert in the **Email Message** field.
   - SNMP Trap:
     a. Enter the IP address that will receive the SNMP trap notification in the **SNMP Destination Address** field. Both IPv4 and IPv6 address formats are supported.
     b. (Optional) After saving you can click the message icon (✉) to send a sample alert to the configured destination.
4. Click **Save** to save the LAN destination.

Deleting a LAN Destination

To delete a configured LAN destination, click on the destination to open the settings and then click **Delete**.

Services Settings

The Services page displays basic information about the services running on the IPMI module. Only Administrator users can modify the services.

Viewing Service Details

On the Services page you can view many details of the services running on the IPMI module. Navigate to **Settings** > **Services**. The Services list provides the following details:

Field	Description
Service	Name of the service.
Status	The current status of the service.

Field	Description
Interfaces	The interface in which the service is running.
Non-secure Port	The non-secure port number for the service. This field can be edited. Default ports: • Web: 80 • KVM: 7578 • CD Media: 5120
Secure Port	The secure port number for the service. This field can be edited. Default ports: • Web: 443 • KVM: 7582 • CD Media: 5124 • SSH: 22
Timeout	The session timeout value, in seconds, for the service. This field can be edited for Web, SSH, and Telnet services.
Maximum Sessions	The maximum number of allowed sessions for the service.

Note:

- The Service, Status, Interfaces, and Maximum Sessions fields are read-only.
- The SSH service does not support non-secure ports.
- If the Single port feature is enabled, KVM, CD Media, and HD Media ports cannot be edited.
- For the security of your system, the non-secure port feature and port 80 are disabled by default. Non-secure ports can be enabled by using the `ALLOW_NON_SECURE_COMMUNICATION` command.
- If KVM is launched, the web timeout will not take effect.

Viewing Active Sessions

If an IPMI module service currently has an active session, you can view the details of that session:

1. Navigate to **Settings** > **Services**.
2. Click the View icon (≡) for a service with an active session to view the details of that session.
3. The following session details are displayed:

Field	Description
Session Type	Displays the type of active session.
User ID and User Name	Displays the user name and ID of the current user.
Client IP	Displays the IP addresses that are connected to the active session.
Privilege	Displays the privilege level of the current user.

4. If necessary, you can click the Terminate icon (⊗) to end that session.

Modifying an Existing Service

1. Navigate to **Settings** > **Services**.
2. Click the Edit icon (✎) for a service to modify that service. The Service Configuration screen will open.

   Note: The Service Name and Maximum Session fields cannot be modified.

3. Check the **Active** checkbox to enable the current service.

   Note: The interfaces, ports, and timeout fields cannot be edited unless the service is **Active**.

4. Select one of the available interfaces from the **Interface Name** drop-down list.
5. Enter the non-secure port number in the **Non-secure Port** field.
6. Enter the secure port number in the **Secure Port** field.
7. Enter the timeout value, in seconds, in the **Timeout** field.

   Tip:
   - The Web service timeout can range from 300 to 1800 seconds.
   - The KVM service timeout can range from 300 to 1800 seconds.
   - The SSH service timeout can range from 60 to 1800 seconds.

8. Click **Save** to save your changes or click **Cancel** to exit without saving.

SMTP Settings

Simple Mail Transfer Protocol (SMTP) is an Internet standard for email transmission across IP networks. Use the SMTP Settings page to configure the SMTP settings for the IPMI module.

1. Navigate to **Settings** > **SMTP Settings**.
2. Select a **LAN Interface** from the drop-down list.
3. Enter the sender's email address in the **Sender Email ID** field.
4. Check the **Primary SMTP Support** checkbox to enable SMTP support for the IPMI module.
5. Enter the machine name of the SMTP server in the **Primary Server Name** field. Up to 15 alpha-numeric characters can be used. Spaces and special characters are not supported.
6. Enter the IP address of the SMTP server in the **Primary Server IP** field. This is a mandatory field.
7. Enter the port number for connecting to the SMTP server in the **Primary SMTP Port** field. The default port is 25.
8. Enter the secure port number for connecting to the SMTP server in the **Primary Secure SMTP Port** field. The default port is 465.
9. Check the **Primary SMTP Authentication** checkbox to enable SMTP authentication.

   CRAM-MD5, LOGIN, and PLAIN authentication types are supported. If the SMTP server does not support these authentication types, you will get an error message.
10. Enter the user credentials in the **Primary User name** and **Primary Password** fields.
11. Enable the **Primary SMTP SSLTLS Enable** checkbox to send data through the secure port.

    If this option is enabled, the non-secure port and STARTTLS options will be hidden.
12. Enable the **Primary SMTP STARTTLS Enable** checkbox configure secure communication if you are not using the SSLTLS option. Upload the required certificate files:
    a. **Upload SMTP CA Certificate File**: upload the file that contains the certificate of the trusted CA certs. The CACERT key file should be of pem type.
    b. **Upload SMTP Certificate File**: upload the client certificate file. The CERT key file should be of pem type.
    c. **Upload SMTP Private Key**: upload the client private key file. The SMTP key file should be of pem type.
13. Check the **Secondary SMTP Support** checkbox to enable configuration of a backup SMTP service that can be used if the primary server is having difficulty. The secondary SMTP server field requirements are the same as the primary fields. Enter the details of the secondary SMTP server in these fields.
14. Click **Save** to save the settings.

SSL Settings

The Secure Socket Layer (SSL) protocol ensures secure transactions between web servers and browsers. This protocol uses a third party, a Certification Authority (CA), to identify one end or both ends of the transaction. Upload the CA-signed certificates and configure the SSL settings so the device can be accessed in a secured mode. There are three options for setting your SSL certificates:

- Use a CA-signed certificate that you already possess. For more information, see *Using a CA-Signed SSL Certificate* below.
- Generate a certificate signing request (CSR) to send to a CA for signing. For more information, see *Using the Certificate Signing Request Workflow* below.
- Use a self-signed certificate. For more information, see *Using a Self-Signed Certificate* on the next page.

Using a CA-Signed SSL Certificate

Use this procedure if you already have a signed certificate and private key that you want to use.

1. Navigate to **Settings** > **SSL Settings**.
2. Click the **Upload SSL Certificate** tab.
   a. Click the **Browse** buttons. Find and select your signed certificate and private key files.
   b. Click **Upload**.
3. Click the **Generate SSL Certificate** tab. Fill in the required information to generate the certificate:
   a. **Common Name**: enter a common name for the certificate.
   b. **Organization**: enter the organization name for which the certificate will be generated.
   c. **Organization Unit**: enter the organization unit name for which the certificate will be generated.
   d. **City or Locality**: enter the location of the organization.
   e. **State or Province**: enter the state or province the organization is located in.
   f. **Country**: enter the country the organization is located in.
   g. **Email Address**: enter the email address of the organization.
   h. **Valid For**: enter the number of days the certificate will be valid for. This value can range from 1 to 3650 days.
   i. **Key Length**: enter the key length bit value for the certificate.
   j. Click **Save** to generate the certificate.
4. Click the **View SSL Certificate** tab to view the uploaded certificate in a user-readable format.

> **Note:** After the file is uploaded successfully, the HTTPS service will be restarted to use the newly uploaded certificate. You can now access your IPMI module securely using the following IP address format in your browser:
> `https://<IPMI module IP address>`

Using the Certificate Signing Request Workflow

Use this procedure to generate a certificate signing request (CSR) to get signed by a certification authority (CA).

1. Navigate to **Settings** > **SSL Settings**.
2. Click the **Generate SSL Certificate** tab. Fill in the required information to generate the certificate:
    a. **Common Name**: enter a common name for the certificate.
    b. **Organization**: enter the organization name for which the certificate will be generated.
    c. **Organization Unit**: enter the organization unit name for which the certificate will be generated.
    d. **City or Locality**: enter the location of the organization.
    e. **State or Province**: enter the state or province the organization is located in.
    f. **Country**: enter the country the organization is located in.
    g. **Email Address**: enter the email address of the organization.
    h. **Valid For**: enter the number of days the certificate will be valid for. This value can range from 1 to 3650 days.
    i. **Key Length**: enter the key length bit value for the certificate.
    j. **Type**: select **CSR** to generate a CSR file that can be sent to a third-party certification authority (CA) to be signed. It also installs the corresponding private key in the system.
    k. Click **Save** to generate the certificate.
3. Click the **Download SSL CSR** tab. Click **Download** to download the CSR file that you generated in the previous steps. Send this file to a third-party CA for verification and signing.
4. Once you get the signed CSR file back from the third-party CA, click the **Upload SSL Certificate Without Privatekey** tab.

    Tip: The Private Key was already created when you generated the CSR file.

5. Click the **Browse** button. Find and select your signed CSR file.
6. Click **Upload**.

    Note: After the file is uploaded successfully, the HTTPS service will be restarted to use the newly uploaded certificate. You can now access your IPMI module securely using the following IP address format in your browser:
    `https://<IPMI module IP address>`

Using a Self-Signed Certificate

Use this procedure to generate a self-signed certificate and private key.

Important: Self-signed certificates pose a higher security risk than CA-signed certificates. If system security is a concern, it is recommended to use one of the CA-signed certificate options above.

1. Navigate to **Settings** > **SSL Settings**.
2. Click the **Generate SSL Certificate** tab. Fill in the required information to generate the certificate:
    a. **Common Name**: enter a common name for the certificate.
    b. **Organization**: enter the organization name for which the certificate will be generated.
    c. **Organization Unit**: enter the organization unit name for which the certificate will be generated.
    d. **City or Locality**: enter the location of the organization.
    e. **State or Province**: enter the state or province the organization is located in.
    f. **Country**: enter the country the organization is located in.
    g. **Email Address**: enter the email address of the organization.
    h. **Valid For**: enter the number of days the certificate will be valid for. This value can range from 1 to 3650 days.
    i. **Key Length**: enter the key length bit value for the certificate.
    j. **Type**: select **Self-Signed Certificate** to create a self-signed certificate and the corresponding private key in the system.
    k. Click **Save** to generate and install the self-signed certificate and private key.

> **Note:** After the file is uploaded successfully, the HTTPS service will be restarted to use the newly uploaded certificate. You can now access your IPMI module securely using the following IP address format in your browser:
> `https://<IPMI module IP address>`

System Firewall Settings

The System Firewall page allows you to configure the IPMI module firewall settings. Firewall rules can be set for specific IP addresses, a range of IP addresses, or port numbers. You must be at least an Operator to view this page. Only Administrators can delete a firewall.

General Firewall Settings

In the General Firewall Settings page you can add new firewall settings or update existing firewall settings.

Adding Firewall Settings

1. Navigate to **Settings** > **Firewall** > **General Firewall Settings** > **Add Firewall Settings**.
2. Select **Block All** to block all the incoming IPs and Ports.
3. Select **Flush All** to flush all of the system firewall rules.
4. Select **Timeout** to enable or disable firewall rules with timeout.
5. Enter the **Start Time** as the time when the respective firewall rule takes effect.

6. Enter the **End Time** as the time when the respective firewall rule ends.

   > **Note:** The time should be in the `dd-mm-yy:hh-mm` format.

7. Click **Save** to save the settings.

Updating Existing Firewall Settings

This page will be blank if no firewall settings have previously been added. For more information, see *Adding Firewall Settings* on the previous page.

1. Navigate to **Settings** > **Firewall** > **General Firewall Settings** > **Existing Firewall Settings**. The existing firewall settings will be displayed.
   - **Block All**: Displays the blocked incoming IPs and Ports.
   - **Flush All**: Use to flush all of the system's firewall rules. This field is read-only.
   - Select **Timeout** to enable or disable firewall rules with timeout.
   - When **Timeout** is enabled, the respective firewall rule's **Start Date&Time** and **End Date&Time** will be displayed.
2. Click **Delete** to delete the system firewall rules.

IP Address Firewall Rules

In the IP Address Firewall Rules page, you can add a new IP rule or view the existing rules.

Adding an IP Rule

1. Navigate to **Settings** > **Firewall** > **IP Address Firewall Rules** > **Add New IP Rule**. The Add IP Rule page opens.
2. Enter an IP address in the **IP Single (or) IP Range Start** field.

   > **Note:**
   > - If the rule is for a single IP address, enter that address in this field. If the rule is for a range of IP addresses, enter the first address in that range here. You will then enter the last IP address in the range in the **IP Range End** field.
   > - Only the IPv4 address format is supported.

3. If you are creating a rule for a range of IP addresses, enter the last address of the range in the **IP Range End** field.
4. Select the **Enable Timeout** checkbox to enable this rule with timeout settings. If you have enabled timeout, configure the following settings:

   > **Note:** Use the `YYYY/MM/DD` date format and `hh-mm` time format.

   a. Enter the date the rule will take effect in the **Start Date** field.
   b. Enter the date the rule will end in the **End Date** field.
   c. Enter the time the rule will take effect in the **Start Time** field.
   d. Enter the time the rule will end in the **End Time** field.
5. In the **Rule** drop-down list, select to **Allow** or **Block** the IP address.
6. Click **Save** to save the settings.

Viewing Existing IP Rules

1. Navigate to **Settings** > **Firewall** > **IP Address Firewall Rules** > **Existing IP Rules**. A blank page will open if you have not previously added any IP rules. If any rule had been added, it will be listed on the Existing IP Rules page.
2. Click the **IP Adresses** tab. The existing IP rule settings will be displayed.
   - **IP Single (or) Range Start**: Displays the configured IP address or range of IP addresses.
   - **IP Range End**: Displays the configured IP address or range of IP addresses.
   - **Enable Timeout**: Enables or disables timeout for this IP rule.
   - **Start Date&Time**: Displays the start date and time for the respective firewall IP rule.
   - **End Date&Time**: Displays the end date and time for the respective firewall IP rule.
   - **Rule**: Indicates the current setting for the listed IP address or range of IP addresses. This can be set as either `Allow` or `Block`.
3. Click **Delete** to delete this IP rule.

Port Firewall Rules

In the Port Firewall Rules page, you can add a new port rule or view the existing rules.

Adding a Port Rule

1. Navigate to **Settings** > **Firewall** > **Ports Firewall Rules** > **Add Port Rule**. The Add Port Rule page opens.
2. Enter a port number in the **Port Single (or) Port Range Start** field.

   > **Note:**
   > - If the rule is for a single port, enter that port number in this field. If the rule is for a range of ports, enter the first port in that range here. You will then enter the last port in the range in the **Port Range End** field.
   > - Port values can range from 1 to 65535.

3. If you are creating a rule for a range of ports, enter the last port of the range in the **Port Range End** field.
4. Select the protocol of the port(s) for this rule from the **Protocol** drop-down list.You can select from **TCP**, **UDP**, or **Both**.

5. Select the network type of the port(s) for this rule from the **Network Type** drop-down list.You can select from **IPv4**, **IPv6**, or **Both**.
6. Select the **Enable Timeout** checkbox to enable this rule with timeout settings. If you have enabled timeout, configure the following settings:

   > **Note:** Use the `YYYY/MM/DD` date format and `hh–mm` time format.

   a. Enter the date the rule will take effect in the **Start Date** field.
   b. Enter the date the rule will end in the **End Date** field.
   c. Enter the time the rule will take effect in the **Start Time** field.
   d. Enter the time the rule will end in the **End Time** field.
7. In the **Rule** drop-down list, select to **Allow** or **Block** the port(s).
8. Click **Save** to save the settings.

Viewing Existing Port Rules

1. Navigate to **Settings** > **Firewall** > **Port Firewall Rules** > **Existing Port Rules**. A blank page will open if you have not previously added any port rules. If any rule had been added, it will be listed on the Existing Port Rules page.
2. Click an existing port rule. The port rule settings will be displayed.
   - **Port Single (or) Range Start**: Displays the configured port or range of ports.
   - **Port Range End**: Displays the configured port or range of ports.
   - **Protocol**: Displays the specified protocols for the port or range of ports.
   - **Network Type**: Display the specified network type for the configured port or range of ports.
   - **Enable Timeout**: Enables or disables timeout for this port rule.
   - **Start Date&Time**: Displays the start date and time for the respective firewall port rule.
   - **End Date&Time**: Displays the end date and time for the respective firewall port rule.
   - **Rule**: Indicates the current setting for the listed port or range of ports. This can be set as either `Allow` or `Block`.
3. Click **Delete** to delete this IP rule.

User Management

The User Management page allows you to view the current list of user slots for the server. You can add a new user, modify, or delete an existing user.

Navigate to **Settings** > **User Management**. The user list is displayed with a maximum of 10 users. The following information and options are available on the User Management page:

- User icon:
  - You can click on a free user icon to add a new user. Free slots are shown as disabled. For more information, see *Adding a New User* below.
  - You can click on an active user's icon to modify that user's settings. For more information, see *Modifying an Existing User* on page 39.
- Delete icon: Click to delete a user from the list.
- Channel: Choose an available channel from the list.
- User ID: Displays the ID number of the user.
- User Name: Displays the name of the user.
- User Access: Displays the access privilege level of the user.
- Network Access: Displays the network access privilege level of the user.
- SNMP Status: Displays if the SNMP status of the user is enabled or disabled.
- E-Mail ID: Displays the email address of the user.

Adding a New User

1. Click on a free section on the *User Management* page to open the Add User screen.
2. Enter the name of the user in the **User Name** field.

   The user name is a case sensitive string of 1 to 16 alpha-numeric characters. It must start with an alphabetic character. Special characters – _@ are supported.
3. Select the size of the new password with the Password Size drop-down menu. For a 20 byte password, the LAN session will not be established.
4. Enter your new password in the **Password** and **Confirm Password** fields.

   > **Tip:**
   > - The password should be a combination of alphanumeric characters, symbols, and uppercase characters.
   > - Spaces are not supported. For a list of all unsupported password characters, see *Unsupported Password Characters* on the next page.
   > - The password should be a string if you are setting the password using the *ipmitool user set password* command.
5. Enable or disable the **Enable User Access** checkbox. Enabling user access will assign the IPMI messaging privilege to the user.
6. Assign a privilege level to the user with the **Privilege** drop-down menu. The user can be an *Administrator*, *Operator*, *User*, *OEM*, or *None*.
7. Enter the user's email in the **Email ID** field. If the user forgets their password, the new password will be sent to this email address.

Note: For new password emails to be sent, the SMTP server must be configured to send emails. For more information, see *SMTP Settings* on page 30.

8. Select the format of the emails with the **Email Format** drop-down menu. There are two options:
   - **AMI-Format**: The subject line for this format will be `Alert from (your host name)`. The content will show sensor information such as sensor type and description.
   - **Fixed-Subject Format**: Select this format if you want to manually define a specific subject and message content for the emails. You must set the subject and message fields if this option is selected.
9. In the **Upload SSH Key** field, click **Browse**. Find and select your SSH key file. The SSH key should be a *pub* type.
10. Click **Save** to save the new user and return to the user list.

Unsupported Password Characters

Hex	Character
00	NUL '\0'
01	SOH (start of heading)
02	STX (start of text)
03	ETX (end of text)
04	EOT (end of transmission)
05	ENQ (enquiry)
06	ACK (acknowledge)
07	BEL '\a' (bell)
08	BS '\b' (backspace)
09	HT '\t' (horizontal tab)
0A	LF '\n' (new line)
0B	VT '\v' (vertical tab)
0C	FF '\f' (form feed)
0D	CR '\r' (carriage net)
0E	SO (shift out)
0F	SI (shift in)
10	DLE (data link escape)

Hex	Character
11	DC1 (device control 1)
12	DC2 (device control 2)
13	DC3 (device control 3)
14	DC4 (device control 4)
15	NAK (negative ack.)
16	SYN (synchronous idle)
17	ETB (end of trans. blk)
18	CAN (cancel)
19	EM (end of medium)
1A	SUB (substitute)
1B	ESC (escape)
1C	FS (file separator)
1D	GS (group separator)
1E	RS (record separator)
1F	US (unit separator)
20	SPACE
7F	DEL

Modifying an Existing User

1. Click on an active user tab on the *User Management* page to open the User's screen.
2. Click **Delete** if you want to delete the user.
3. Enter the name of the user in the **User Name** field.

   The user name is a case sensitive string of 1 to 16 alpha-numeric characters. It must start with an alphabetic character. Special characters –_@ are supported.
4. Select the **Change Password** checkbox if you want to modify the password or password settings.
5. Select the size of the new password with the Password Size drop-down menu. For a 20 byte password, the LAN session will not be established.
6. Enter your new password in the **Password** and **Confirm Password** fields.

Tip:

- The password should be a combination of alphanumeric characters, symbols, and uppercase characters.
- Spaces are not supported. For a list of all unsupported password characters, see *Unsupported Password Characters* on page 38.
- The password should be a string if you are setting the password using the *ipmitool user set password* command.

7. Enable or disable the **Enable User Access** checkbox. Enabling user access will assign the IPMI messaging privilege to the user.
8. Assign a privilege level to the user with the **Privilege** drop-down menu. The user can be an *Administrator*, *Operator*, *User*, *OEM*, or *None*.
9. Enter the user's email in the **Email ID** field. If the user forgets their password, the new password will be sent to this email address.

   Note: For new password emails to be sent, the SMTP server must be configured to send emails. For more information, see *SMTP Settings* on page 30.

10. Select the format of the emails with the **Email Format** drop-down menu. There are two options:
    - **AMI-Format**: The subject line for this format will be `Alert from (your host name)`. The content will show sensor information such as sensor type and description.
    - **Fixed-Subject Format**: Select this format if you want to manually define a specific subject and message content for the emails. You must set the subject and message fields if this option is selected.
11. In the **Upload SSH Key** field, click **Browse**. Find and select your SSH key file. The SSH key should be a *pub* type.
12. Click **Save** to save the settings and return to the user list.

Reserved Users

There are certain reserved users which cannot be added as IPMI users. The following users are reserved users:

- sysadmin
- daemon
- sshd
- ntp
- root

Remote Control

Click **Remote Control** on the side navigational panel to take remote control of the HD Video Appliance. This page allows you to remotely control the HD Video Appliance operating system as if you were directly connected to the appliance.

1. Click **Launch KVM** to start the remote control session with the HD Video Appliance.
2. You will need to reboot the Appliance after the KVM window popped up to have the remote screen shown up.
3. Once the reboot is complete, change windows display settings to duplicate.
4. Click **Stop KVM** when you are finished with the remote control session.

Note: This operation only needs to be done once.

Supported Browsers

KVM remote control is supported on the following browsers:

- Chrome (latest version)
- Internet Explorer 11 and above
- Firefox (limited support)

Tip: It is recommended to use Chrome or IE for the H5Viewer. Firefox has its own memory limitations.

Using the Remote Control Interface

Click **Remote Control** on the side navigational panel and click **Launch KVM** to start the remote control session. Detailed descriptions of the different menus and options available in the remote control session are given below:

- **Start KVM**: Starts the H5Viewer video redirection.
- **Stop KVM**: Stops the H5Viewer video redirection.
- **Video Record**: This menu contains the following sub-menu options:
    - **Record Video**: Starts recording a video of the screen.
    - **Stop Recording**: Stops the video recording.
    - **Record Settings**: Used to set the Video Recording Duration.
- **Send Keys**: This option is used to key items. This menu contains the following sub-menu options:

    - **Hold Down**: This menu contains the following sub-menu options:
        - **Right Ctrl Key**: This menu option can be used to act as the right-side `CTRL` key when in Console Redirection.
        - **Right Alt Key**: This menu option can be used to act as the right-side `ALT` key when in Console Redirection.
        - **Right Windows Key**: This menu option can be used to act as the right-side `WIN` key when in Console Redirection.
        - **Left Ctrl Key**: This menu option can be used to act as the left-side `CTRL` key when in Console Redirection.
        - **Left Alt Key**: This menu option can be used to act as the left-side `ALT` key when in Console Redirection.
        - **Left Windows Key**: This menu option can be used to act as the left-side `WIN` key when in Console Redirection.
    - **Press and Release**: This menu contains the following sub-menu options:
        - **Ctrl+Alt+Del**: This menu option can be used to act as if you pressed the `CTRL`, `ALT`, and `DEL` keys simultaneously on the server when in Console Redirection.
        - **Left Windows Key**: This menu option can be used to act as the left-side `WIN` key when in Console Redirection. You can also decide how the key should be pressed: *Hold Down* or *Press and Release*.
        - **Right Windows Key**: This menu option can be used to act as the right-side `WIN` key when in Console Redirection. You can also decide how the key should be pressed: *Hold Down* or *Press and Release*.
        - **Context Menu Key**: This menu option can be used to act as the context menu key when in Console Redirection.
        - **Print Screen Key**: This menu option can be used to act as the print screen key when in Console Redirection.
- **Hot Keys**: This menu is used to add user-configurable shortcut keys that can then be used on the host machine. The configured key events are saved in the IPMI module. This menu contains the following sub-menu options:
    - **Add Hot Keys**: Use this menu to add hot key macros. Click **Add** to add macros.
- **Settings**:
    - **Keyboard Layout**: Provides a list of host physical keyboard languages supported by the H5Viewer.
- **Video**: This menu contains the following sub-menu options:
    - **Pause Video**: Pauses Console Redirection.
    - **Resume Video**: Used to unpause Console Redirection.
    - **Refresh Video**: Updates the display shown in Console Redirection.
    - **Display on**: If you disable this option, the display will be shown on the screen in Console Redirection.
    - **Display off**: If you enable this option, the server display will be blank but you can view the

screen in Console Redirection. If you disable this option, the display will be back on the server screen.

    - **Capture Screen**: Use this option to take a screenshot of the host screen and save it in the client system.
- **Mouse**: This menu contains the following sub-menu options:
    - **Show Client Cursor**: This option can be used to show or hide the local mouse cursor on the remote client system.

      > **Note:** The client cursor is always enabled by default.

    - **Mouse Mode**: This option configures mouse emulation from the local window to the remote screen using either of the two methods. Only administrators can configure this option.
        - **Absolute mouse mode**: The absolute position of the local mouse is sent to the server if this option is selected.
        - **Relative mouse mode**: The calculated relative mouse position displacement of the local mouse is sent to the server if this option is selected.
        - **Other mouse mode**: This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific to SUSE Linux installations.
- **Options**: The **Bandwidth Usage** option allows you to adjust the bandwidth. You can select from one of the following options:
    - **Block Privilege Request**: Enables or disables the access privilege of the user.
    - **Keyboard/Mouse Encryption**: Allows you to encrypt keyboard inputs and mouse movements sent between the connections.
- **Power**: Use the power options to perform any power cycle operations. Click on an option to perform that operation:
    - **Power Reset**: Reboots the system without powering off (warm boot).
    - **Power Cycle**: Will first power off and then reboot the system (cold boot).
    - **Power On**: Powers on the system.
    - **Immediate Shutdown**: Powers off the system.
- **Active Users**: Click this option to display a list of the current active users and their system IP addresses. Active KVM sessions can be terminated from a full-privilege KVM session when there are multiple active KVM sessions.

  > **Note:** The native resolution for KVM is 1024x768, local display resolution will be downgraded to this resolution while KVM is active.

Power Control

The Power Control page allows you to view and control the power of your server. To perform a power function, select that option from the list and click **Perform Action**. The various options on the Power Control page are described below:

- **Power Off**: Immediately power off the server.
- **Power On**: Power on the server.
- **Power Cycle**: This option will first power off, and then reboot the system (cold boot).
- **Hard Reset**: This option will reboot the system without powering off (warm boot).
- **ACPI Shutdown**: Initiates the operating system shutdown prior to the shutdown.

Note: When executing a power function, you will be asked to confirm your choice. After confirming your choice, you will be informed about the status of the action after a few minutes.

ACPI Shutdown Windows Settings

To use the ACPI shutdown on a Windows OS, you need to set the power button actions in the Windows Settings:

1. Open your Windows System Settings and select **Power & Sleep**.
2. Click **Additional power settings** under Related settings.
3. Click **Choose what the power buttons do**.
4. Select **Shut down** from the **When I press the power button** drop-down list.
5. Save the settings.

Maintenance Options

The Maintenance group of pages allows you to perform maintenance tasks on the device. See the following sections for more detailed information.

Backup Configuration

This page allows you to set up the specific configurations to be backed up.

1. Navigate to **Maintenance** > **Backup Configuration** to set up the backup. You can select which configurations to back up from the following options:
   - **Check All**: Selects all of the configurations.
   - **KVM**: Select to backup the KVM configuration settings.
   - **Network & Services**: Select to backup the network and services settings. Selecting to backup Network & Services will also automatically select to backup IPMI.
   - **IPMI**: Select to backup the IPMI module settings.
   - **NTP**: Select to backup the NTP settings.
   - **Authentication**: Select to backup the user and authentication settings.
   - **SYSLOG**: Select to backup the SYSLOG settings.
2. Click **Download** to save the backup file to the client system.
3. When prompted, click **OK** to perform the backup.

Dual Firmware Update

The Dual Firmware Update wizard takes you through the steps of the dual image based firmware upgrade.

1. Navigate to **Maintenance** > **Dual Firmware Update**.
2. Select the image that you want to update in the **Image to be Updated** drop-down list. Options are: **Inactive Image**, **Image 1**, **Image 2**, or **Both Images**.
3. (Optional) Select the **Reboot the device after update** checkbox to have the device automatically reboot when the update is completed.
4. Click **Preserve all Configuration** to preserve your configuration settings during the update. In necessary, click **Edit Preserve Configuration** to modify which settings will be preserved.
5. Click **Browse** to find and select the dual firmware image you want to update to. The update process will go through the following steps:

a. Closes all active client requests.

b. Prepares the device for the firmware upgrade.

c. Uploads the firmware image.

> **Note:** A file upload pop-up window will open for http/https uploads. For tftp files, the file is automatically uploaded and will display the status of the upload. You can set the IPMI module to use either web upload or tftp on the Firmware Image Location page. For more information, see *Firmware Image Location* on the next page.

d. Browse and select the dual firmware image file and click **Upload**.

e. Click **Start firmware update** to start the process. A warning message will open.

f. Click **OK** to proceed with the update.

6. (Optional) In the Section Based Firmware Update area, you can configure the firmware image for section-based flashing. Select the required sections and click **Proceed** to update the firmware. If flashing is required for all images, select the **Full Flash** option.
7. (Optional) If you selected the Version Compare Flash option, the current and uploaded module versions, FMH location, and size will be compared. If the modules differ in size and/or location, you can proceed with a forced firmware upgrade. If all of the module versions are the same, restart the IPMI module by saying all of the module versions are similar. If only a few module versions are different, those modules will be flashed.

   Only the selected sections of the firmware will be updated. Other sections will be skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.

> **Note:** The Dual Firmware Update page will be disabled and you will not be able to perform any other tasks until the firmware upgrade is complete and the device is rebooted. The device will reset if the update is canceled. The device will also reset upon successful completion of the firmware update.

Dual Image Configuration

This page is used to configure the dual image information. Dual image support is helpful to store two firmware images on two 16MBs SPIs, and boot any of the image according to user requests. The running firmware is responsible for setting the Boot Selector and Firmware Upload Selector options.

1. Navigate to **Maintenance** > **Dual Image Configuration**.
2. Dual image information is displayed. Update the various Dual Image Configuration options, as needed:
   - **Firmware Version**: Displays the firmware version of both images.
   - **State**: Displays the current state of both images.
   - **Image to be booted from upon reset**: Select this option to boot a particular image (either 1 or 2) in the next boot up process.

    - **Higher firmware version**: Select this option to boot the image with the higher firmware version in the next boot up process.
    - **Lower firmware version**: Select this option to boot the image with the lower firmware version in the next boot up process.
    - **Most recently updated firmware**: Select this option to boot the image with the most recently updated firmware in the next boot up process.
    - **Least recently updated firmware**: Select this option to boot the image with the least recently updated firmware in the next boot up process.
3. Click **Save** to save your changes.

Firmware Image Location

Use this page to set if the IPMI module will use a TFTP server or web (HTTP/HTTPS) to download the firmware image from.

1. Navigate to **Maintenance** > **Firmware Image Location**.
2. Select the **Image Location Type**:
    - **Web Upload during flash**: Choose to download the firmware images through a web connection. If you select this option, a pop-up window will open during the firmware upgrade process asking for the web upload details.
    - **TFTP Server**: Choose to download the firmware images through a TFTP connection. If you select this option, you will need to complete the following fields:
        - **TFTP Server Address**: Enter the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
        - **TFTP Image Name**: Enter the full source path and filename of the firmware image stored on the TFTP server.
        - **TFTP Retry Count**: Enter the number of times, from 0 to 255, that the image download will be retried if a transfer failure occurs.
3. Click **Save** to save your changes.

Firmware Information

The **Firmware Information** page is used to provide the following details about the currently active image:

- **Active Image ID**: Identifies which of the dual images is currently active.
- **Build Date**: Lists the build date of the currently active image.
- **Build Time**: Lists the build time of the currently active image.
- **Firmware Version**: Lists the firmware version of the currently active image.

HPM Firmware Update

This wizard takes you through the process for HPM-based firmware updates.

Note: All configuration items will be set as preserved/overwrite by default during the restore configuration operation.

1. Navigate to **Maintenance** > **HPM Firmware Update**.
2. Click **Browse**. Find and select the firmware image to be flashed in HPM format.
3. Click **Start firmware update** to upgrade the current device firmware.
4. The device will start preparing for the firmware upgrade.
5. The firmware image file will be uploaded.
6. If flashing is required for all components, select the **Update All** option. Alternatively, you can select the specific components that need to be flashed.
7. Click **Proceed** to start the firmware update.

Note: The update resets the webUI IP address back to its default value. You will need to re-configure the IP address again after this action.

Note: You will not be able to perform any other tasks until the firmware upgrade is complete and the device is rebooted. During the update process, widgets, other web pages, and services will not work. All of the open widgets will be closed. The device will reset if the update is canceled. The device will also reset upon successful completion of the firmware update.

Preserve Configuration

This page allows the user to configure the configuration items that should be preserved when the Restore Factory defaults command is used. The configuration items selected here will not be overwritten with default settings whenever factory default settings are restored.

Tip: You can navigate to the **Firmware Update** or **Restore Factory Defaults** pages directly from this page by clicking their links.

1. Navigate to **Maintenance** > **Preserve Configuration**.
2. Select the checkboxes for the configuration options that you want to have preserved if restore factory defaults is used. Optionally, you can select **Check All** to preserve all of the configuration items on the list.
3. Click **Save** to save your changes.

Restore Factory Defaults

This page allows you to restore the factory default settings of the device firmware.

Important: After entering the restore factory defaults widget, other web pages and services will be disabled. All open widgets will be closed automatically and the device will reset and reboot within a few minutes.

Note: Rebooting resets the webUI IP address back to its default value. You will need to re-configure the IP address again after this action.

1. Navigate to **Maintenance** > **Restore Factory Defaults**.

   Tip: The Preserve Configuration settings are displayed. You can navigate to the **Preserve Configuration** page directly from this page by clicking the link.

2. Click **Restore Factory Defaults** to start the process.

Restoring Factory Defaults with ipmitool Commands

In cases where you are not able to log into the WebUI, you can still use an ipmitool command to restore factory defaults.

Examples:

```
# ipmitool raw 0x32 0x84 3 (get if IPMI preserve is set)
    00
# ipmitool raw 0x32 0x84 2 (get if SEL preserve is set)
    01
# ipmitool raw 0x32 0x83 3 1 (set IPMI as preserve)
# ipmitool raw 0x32 0x66 (do factory restore)
```

Set Preserve Configuration Status

This command is used to enable the configurations to be preserved in the /conf portion.

NetFn	0x32
Command	0x83

Request Data:

Byte	Data Field
1	Selector 0h = SDR 1h = FRU 2h = SEL 3h = IPMI 4h = Network 5h = NTP 6h = SNMP 7h = SSH 8h = KVM 9h = Authentication 10h = Syslog 11h = CMX 12h = WEB 13h = EXTLOG 14h = REDFISH
2	Status 0h = Disable 1h = Enable

Response Data:

Byte	Data Field
1	Completion Code 80h = Param Not Supported

Get Preserve Configuration Status

This command is used to get the configurations to be preserved in /conf.

NetFn	0x32
Command	0x84

Request Data:

Byte	Data Field
1	Selector 0h = SDR 1h = FRU 2h = SEL 3h = IPMI 4h = Network 5h = NTP 6h = SNMP 7h = SSH 8h = KVM 9h = Authentication 10h = Syslog 11h = CMX 12h = WEB 13h = EXTLOG 14h = REDFISH
2	Status 0h = Disable 1h = Enable

Response Data:

Byte	Data Field
1	Completion Code 80h = Param Not Supported
2	Status 0h = Disabled 1h = Enabled

Note: In case of SNMP, EXTLOG, and REDFISH are disabled in the stack, Set and Get for SNMP, EXTLOG, and REDFISH will fail with error code: `80h - Param Not Supported`.

Restore Default Configuration Command

This command is used to restore the default configuration values.

NetFn	0x32
Command	0x66

Response Data:

Byte	Data Field
1	Completion Code

Password Recovery

There are two password recovery options for the IPMI module. You can configure password recovery emails or use the IPMITool to reset the password.

Setting Up Email Password Recovery

You can configure the IPMI module to send password recovery emails in the event that a user forgets their password. To enable this, you must set up the user's email information and configure the IPMI module SMTP settings.

Password Recovery User Management Settings for Email Receiver

On the User Management Configuration page for each user (Settings > User Management > User Management Configuration), enter the email address to be used for the password recovery email in the **Email ID** field.

Password Recovery SMTP Settings

Go to **Settings** > **SMTP Settings**. The settings entered here will depend on the type of email service used. See the section below that applies to your email provider.

Internal Email Server

Enter the corresponding settings for your email service:

- **Sender Email ID**: email ID that will be sending the password recovery emails.
- **Primary Server IP**: IP address of the primary email server.

Gmail Server

Note: Before you get started, make sure your Gmail sender email account is set up for SMTP. See **this Gmail SMTP setup page** for further details.

Enter the corresponding settings for your Gmail service:

- **Sender Email ID**: Gmail account that will be sending the password recovery emails. Typically this is the admin of the IPMI module.
- **Primary Server Name**: a name to identify this server. This name will be used during SSL handshake.
- **Primary Server IP**: IP address of smtp.gmail.com. You can ping this address to get this information.
- **Primary SMTP port**: 587 (used for STARTTLS).
- **Primary Secure SMTP port**: 465 (used for SSLTLS).

- **Primary Username**: the same as the Sender Email ID.
- **Primary Password**: the two-step authentication APP password. See the **Gmail SMTP setup page** for more details.

For the secured channel option, check whichever of the following options that applies to your setup:

- **Primary SMTP SSLTLS Enable**
- **Primary SMTP STARTTLS Enable**

Both of the above options will have the below fields to fill:

- **Upload SMTP CA Certificate File**: Upload the file that contains the certificate signed by the trusted CA. The CACERT file should be a .pem file (optional).
- **Upload SMTP Certificate File**: Upload the client certificate file. The CERT file should be a .pem file. This field will be automatically filled if you generate or upload the CERT on the SSL Setting page. For more information, see *SSL Settings* on page 30.
- **Upload SMTP Private Key**: Upload the client private key file. The SMTP key file should be a .pem file. This field will be automatically filled if you generate or upload the CERT on the SSL Setting page. For more information, see *SSL Settings* on page 30.

Go to Settings > User Management > User Management Configuration and enter the email address to be used for in the **Email ID** field for both the admin user, typically the sender, and any users that may need to receive the password recovery emails.

Hotmail Server

Enter the corresponding settings for your Hotmail service:

- **Sender Email ID**: Hotmail account that will be sending the password recovery emails. Typically this is the admin of the IPMI module.
- **Primary Server Name**: a name to identify this server. This name will be used during SSL handshake.
- **Primary Server IP**: 40.101.146.98, IP of smtp.office365.com. You can ping this address to verify the IP address.
- **Primary SMTP port**: 587 (used for STARTTLS).
- **Primary Username**: the same as the Sender Email ID.
- **Primary Password**: Hotmail password.

Check the **Primary SMTP SSLTLS Enable** checkbox, which opens the following fields to be filled:

- **Upload SMTP CA Certificate File**: Upload the file that contains the certificate signed by the trusted CA. The CACERT file should be a .pem file (optional).
- **Upload SMTP Certificate File**: Upload the client certificate file. The CERT file should be a .pem file. This field will be automatically filled if you generate or upload the CERT on the SSL Setting page. For more information, see *SSL Settings* on page 30.
- **Upload SMTP Private Key**: Upload the client private key file. The SMTP key file should be a .pem file. This field will be automatically filled if you generate or upload the CERT on the SSL Setting page. For more information, see *SSL Settings* on page 30.

Go to Settings > User Management > User Management Configuration and enter the email address to be used for in the **Email ID** field for both the admin user, typically the sender, and any users that may need to receive the password recovery emails.

Password Recovery with the IPMITool

If a user's password requires recovery and the email option has not been set up, you can use the IPMITool to reset that user's password instead.

1. Download the IPMITool from the support website and load it on to the HD Video Appliance.
2. Open the command line prompt and navigate to the folder where you downloaded the IPMITool.exe file.
3. Enter the following comment to check for the list of active users:

   ```
   .\ipmitool.exe -I wmi user list 'channel_id'
   ```

   The default channel is **1**.
4. Locate and record the **User_ID** and **Channel ID** information for the user that needs their password reset.
5. Enter the following command using the information gathered in the previous step:

   ```
   .\ipmitool.exe -I wmi user set password 'User_id' 'New_password'
   ```

   For **User_id**, enter the user ID that was recorded in the previous step. For **New_password**, enter the password you want the user to be reset to.
6. Communicate the new password specified in the previous step to the user.

Limited Warranty

Avigilon warranty terms for this product are provided at **avigilon.com/warranty**.

For More Information

For additional product documentation and software and firmware upgrades, visit **support.avigilon.com**.

Technical Support

Contact Avigilon Technical Support at **support.avigilon.com/s/contactsupport**.

Product User Guides

For product user guides, visit the Downloads page:

Avigilon Workstations: **avigilon.com/products/video-infrastructure/remote-monitoring**

AI NVR: **https://www.avigilon.com/products/video-infrastructure/ai-nvr#downloads**