VIEVU Docking Station SNMP Guide

INTRODUCTION

VIEVU Solution is the next generation, fully-hosted, cloud evidence management system. This guide describes how to operate the VIEVU Solution. Additional support material is available at www.vievu.com/support**.**

CONTACT US

If you need assistance or have any questions, contact us by phone at 888-285-4548 or email **support@vievu.com**.

TABLE OF CONTENTS

SNMP SERVICE SETUP

Setup describes configuration of the SNMP service.

SNMP Configuration

The following sections provide SNMP configuration information for both the Agent side and the Manager side.

Agent Side

➔ To configure SNMP from the Agent side:

1. Click the **SNMP** toggle to **enabled**.
2. In the **Manager Host** field, specify the **IP/Hostname** where traps will be sent.
3. In **Manager Community String**, input a string to be sent to the SNMP Manager with each trap. By default, this is set to **public**.
4. The **Agent Community String** must be sent to receive Docking Station SNMP variables. By default, this is set to **public**.

Manager Side

To receive the MDN traps, it is necessary to configure your server application to process traps with the **Community String** specified in the **Manager Community String** field. You can set up trap processing rules for your server application either now or later.

Note: VIEVU Docking Station sends traps on UDP Port 162 and supports SNMP v2c only

To have access to MDN variables, you will need to configure your client to use the Community String specified in the **Agent Community String** field.

You can configure your server application or client application to use the MIB file, provided at the end of this guide, to use human-readable names instead of Object Identifiers (OIDs).

SSL Certificate Support

Secure Sockets Layer and, more recently, Transport Layer Security are both frequently referred to as “SSL.” These are cryptographic protocols for providing communications security over a computer network.

To ensure secure HTTPS connections, this release of software allows you to upload SSL certificates on the Docking Station **Configuration** page.

➔ To set up secure HTTPS connections:

1. In the SSL field at the lower-right side of the Docking Station Configuration page, click the **HTTPS** button, shown in Figure 1.

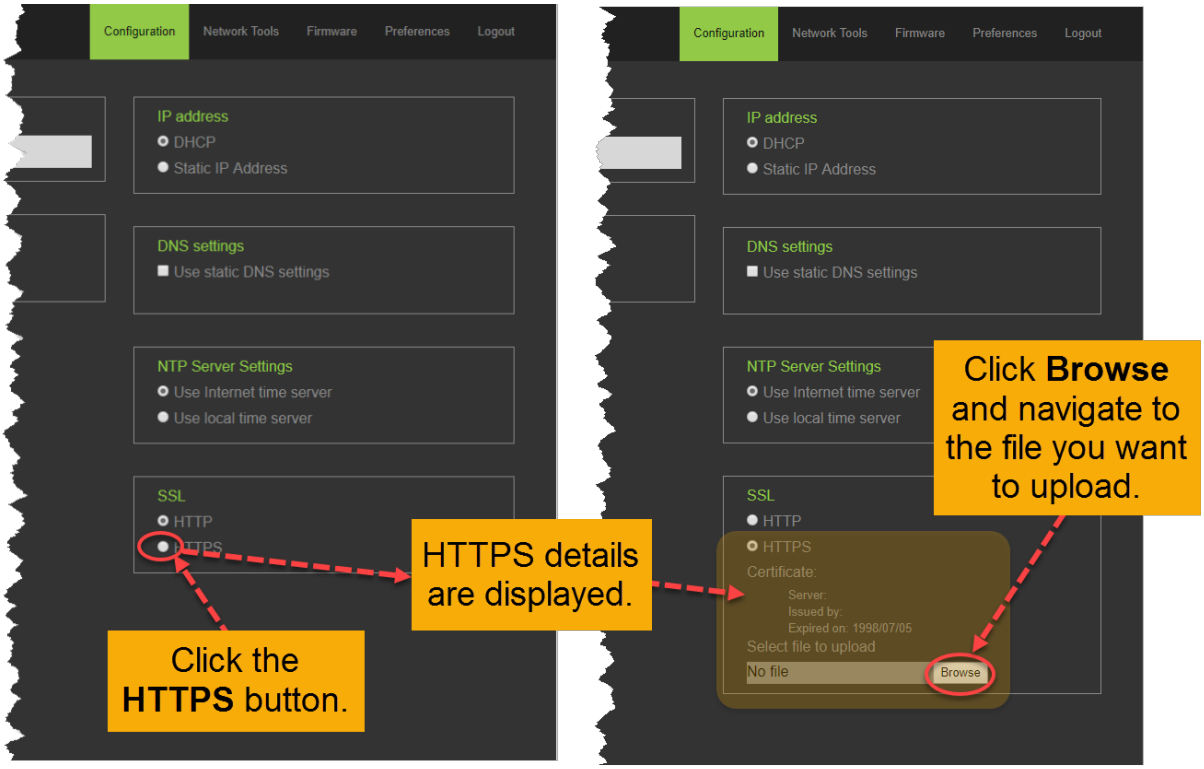

Figure 1

2. Click the **Browse** button and select the SSL certificate file to upload.

Variables

The Docking Station SNMP agent provides the following table which contains status information for each Cradle (USB Connection port) used to communicate with camera.

NAME	OID	TYPE	DESCRIPTION
usbPortTable	1.3.6.1.4.1.99999.1.1	Table	A table containing information on current state of MDN's USB ports.
usbPortEntry	1.3.6.1.4.1.99999.1.1.1	Row	An entry containing a USB port and its status.
upIndex	1.3.6.1.4.1.99999.1.1.1.1	Integer	Unique index
upDeviceName	1.3.6.1.4.1.99999.1.1.1.2	String	Defines device name, e.g. /dev/ttyUSB0
upCameraSerial	1.3.6.1.4.1.99999.1.1.1.3	String	The Camera Serial Number connected to the port.
upPutInQueue	1.3.6.1.4.1.99999.1.1.1.4	String	UTC date/time when camera was put in queue to upload.

upTakenFromQueue	1.3.6.1.4.1.99999.1.1.1.5	String	UTC date/time when camera was processed last.
upErrorAttempts	1.3.6.1.4.1.99999.1.1.1.6	Integer	Number of attempts which ended with an error, and camera was rescheduled for processing.
upStateFlag	1.3.6.1.4.1.99999.1.1.1.100	Integer	An Error flag to indicate trouble with a port. It goes to 2 or 3 if there is an error and 0 if no error.
upAttentionReason	1.3.6.1.4.1.99999.1.1.1.101	String	Short description of the reson why attention is required, e.g. commit failed, api logon failed

Traps

The Docking Station SNMP agent will send two traps:

- **Camera requires attention** (OID: 1.3.6.1.4.1.99999.1.2.1) - this trap is sent whenever MDN requires user attention to solve problem. This trap is accompanied with the following information:
  - Camera serial number (OID: 1.3.6.1.4.1.99999.1.2.1.1)
  - Attention reason (1.3.6.1.4.1.99999.1.2.1.2) – describes why camera requires attention. The following reasons can be sent to SNMP manager:
  - **Unable to log on to the API** – this message appears in the following cases: MDN is not configured or there is no network connection to the VERIPATROL or VIEVU Solution server.
  - **Camera is not assigned** – this message appears when the camera has not yet been assigned.
  - **Unable to remove video file from camera** – MDN was not able to remove video from camera. Please contact VIEVU Support for assistance.
  - **Camera storage is corrupted** – MDN detects file-system inconsistency which cannot be corrected. Please contact VIEVU Support for assistance.
  - **Unable to upload video to server** – this message appears when video cannot be uploaded to the server, e.g. connectivity issue.
  - **Unable to commit video file** – this message appears when the video has been uploaded to target server but can't be committed for any reason, e.g. network connectivity problem, server related issue.
  - **Video metadata is corrupted** – this message appears when MDN detects corruption of video file metadata. Metadata can be re-entered manually.
- **Too many upload tries** (OID: 1.3.6.1.4.1.99999.1.2.2) – this trap is sent if video cannot be uploaded to the target server after 10 attempts. In most cases this is related to connectivity problems.