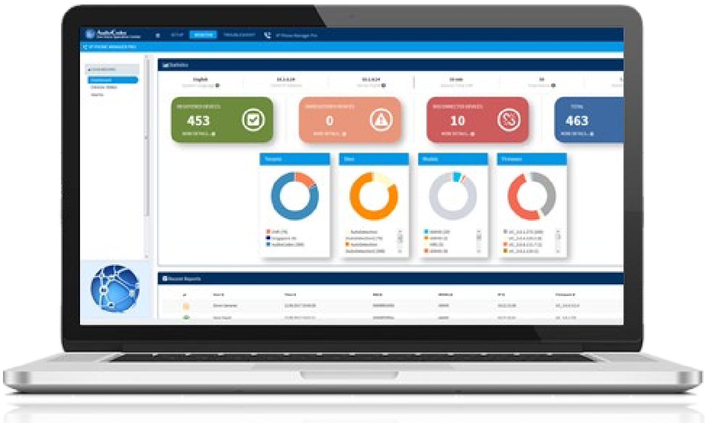
Installation and Configuration Guide

*AudioCodes One Voce Operations Center (OVOC)*

# Device Manager Agent

Version 7.6



# Table of Contents

# List of Figures

## Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: March-24-2019

## WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

## Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

## Stay in the Loop with AudioCodes

## Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://online.audiocodes.com/documentation-feedback.

## Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

## Related Documentation

| Manual Name |
|---|
| Device Manager Pro Administrator's Manual |
| Device Manager Express Administrator's Manual |

## Document Revision Record

| LTRT | Description |
|---|---|
| 91200 | Initial document release |

# 1 Introduction

## 1.1 About this Guide

This guide shows how to install and configure the Device Manager Agent software application in order to manage devices located behind a NAT | Firewall from the OVOC.

## 1.2 About the Agent

The Device Manager Agent is software that can run on a Windows machine, downloadable from AudioCodes website. The Agent is installed on a specific host by the network administrator using an msi file. The host machine must use one of the following operating systems:

- Windows 10
- Windows server 2012
- Windows server 2016

The Agent is configured with the OVOC's FQDN or IP address. The Agent is also configured with the OVOC tenants related to it. The Agent is configured with a key, used to authenticate the Agent in the OVOC. After the Agent is configured and running, it sends a message to the OVOC at < 60 second intervals to check if there are actions for the devices under it. If there are, the Agent fetches an action list from the OVOC and performs the actions one by one on each device. The action list is:

- Check status
- Update firmware
- Reset phone
- Update configuration
- Send message

The Agent is stateless, i.e., it does not know if the action was successful or not.

## 1.3 Benefits

The Device Manager Agent enables network administrators using the OVOC to manage devices located behind a NAT | Firewall in a local enterprise network, from a global cloud network.

The Agent application allows the OVOC to send actions directly to devices.

Deployed on an enterprise's premises, the Agent opens a communications channel with the OVOC located in the global cloud network. The OVOC is then able to send commands to devices in the local network.

The OVOC consequently allows

- Internet Telephony Service Providers (ITSPs) to remotely manage devices in enterprise customer networks, through cloud services
- Software as a Service (SaaS) by a centralized hosting business
- Enterprise network administrators to manage devices located within their own network

## 1.4 Security

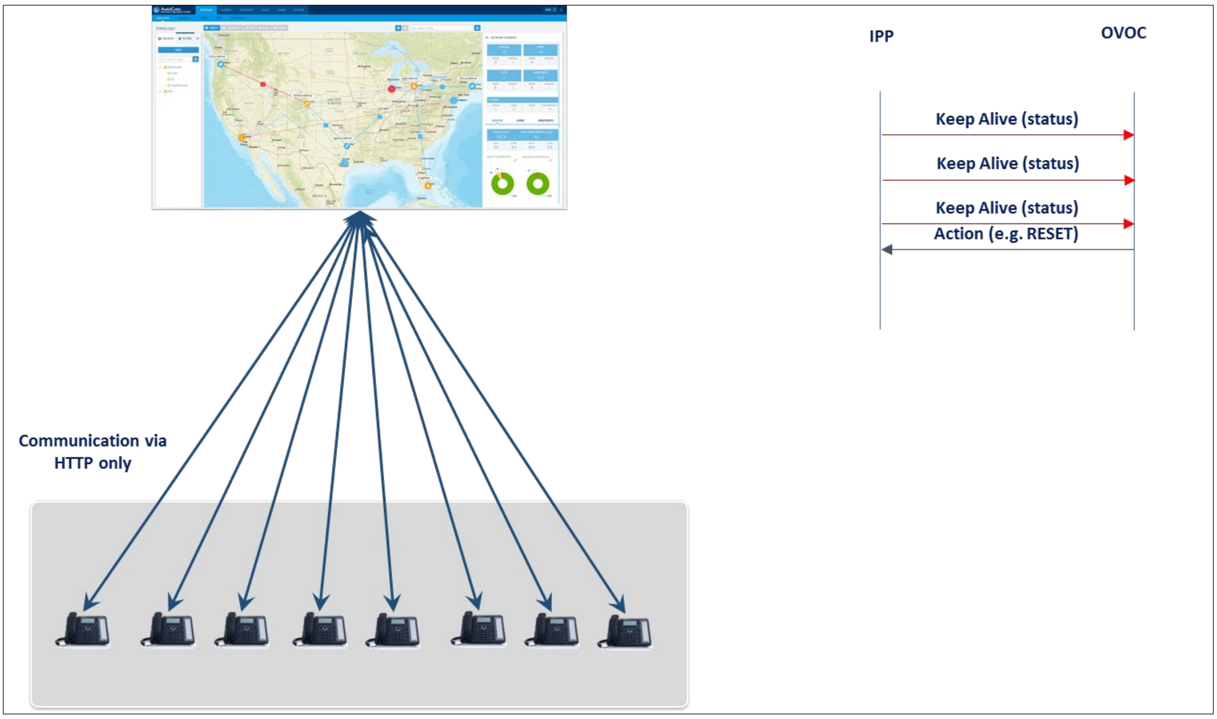
The connection between the OVOC and the Agent is secured using HTTPS over port 443. The Agent can operate with the devices using HTTPS as well.

### 1.4.1 Managing Devices within the Same Network as OVOC

The OVOC allows enterprise network administrators to manage devices located within their own network, viz., the on-premises solution.

- Devices send a keep-alive message to the OVOC once every hour
- The keep-alive timeout can be reduced per the number of the devices in the network
- Actions are sent interactively from the OVOC to the devices

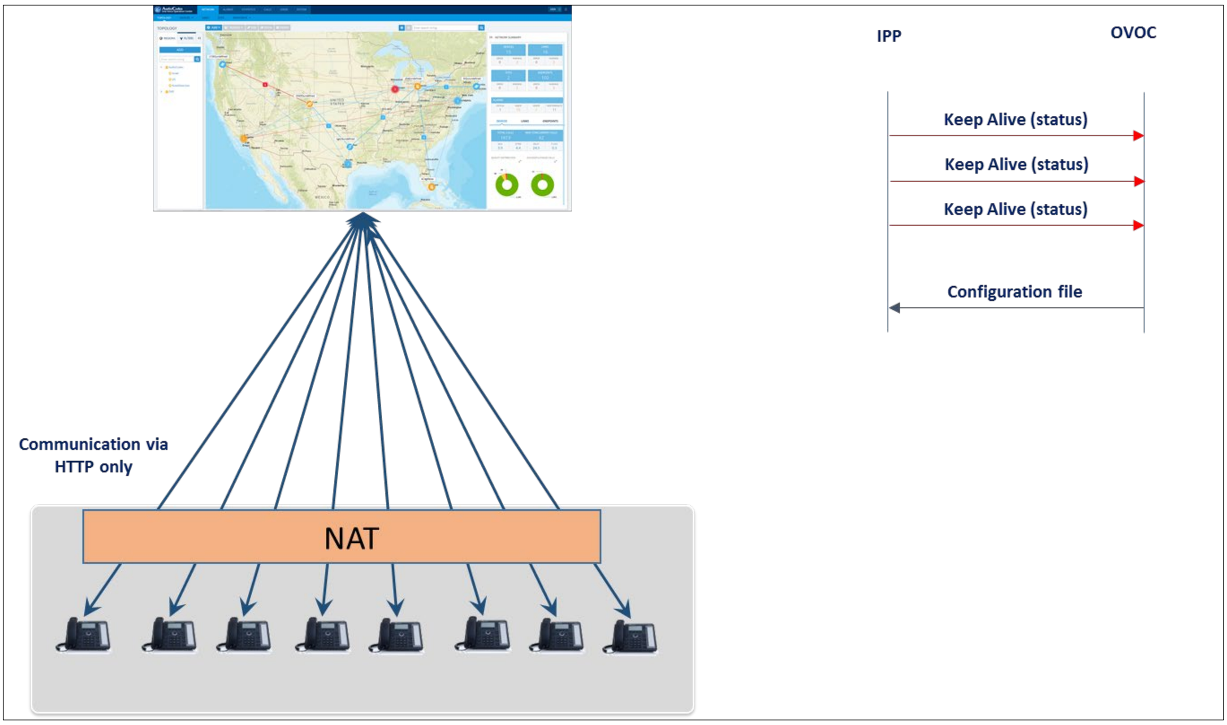
**Figure 1-1: Managing Devices within the Same Network as OVOC**



### 1.4.2 Managing Devices behind a NAT

- Devices send a keep-alive message to the OVOC once every hour
- The keep-alive timeout can be reduced per the number of the devices in the network
- The OVOC can’t send actions to devices; devices send a configuration file (which can include actions) downloaded from the OVOC once a day (configurable).

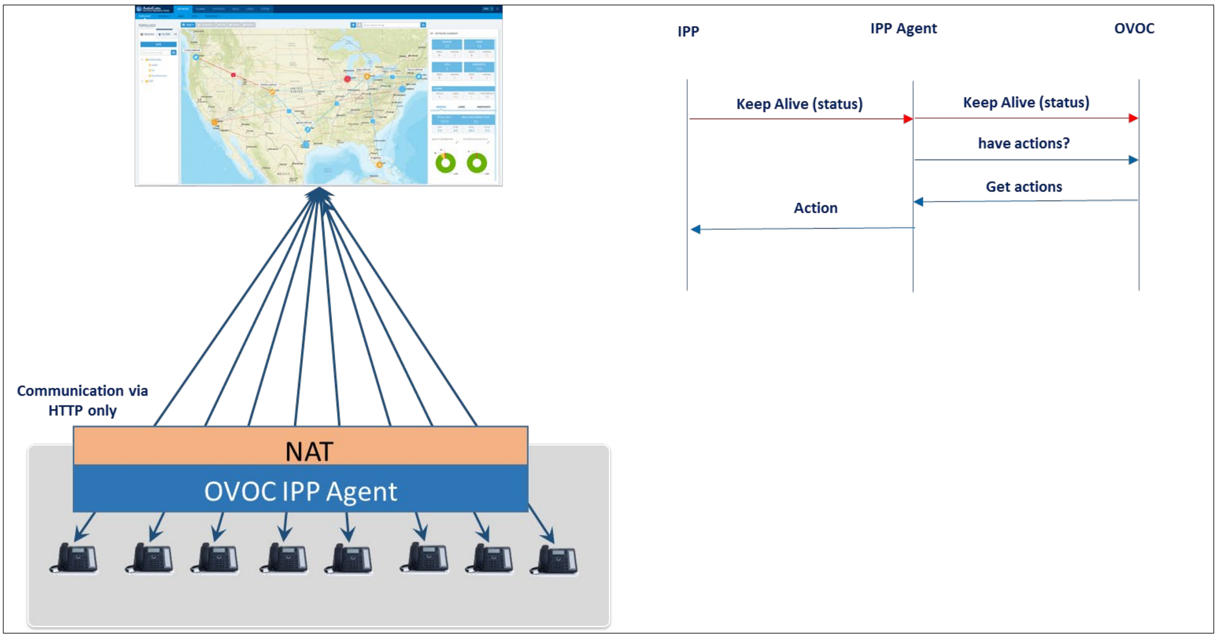
**Figure 1-2: Managing Devices behind a NAT**



### 1.4.3 Sending Actions from OVOC to Devices behind a NAT, via Agent

- Devices send a keep-alive message to the OVOC once every hour
- The keep-alive timeout can be reduced per the number of the devices in the network
- Actions are sent interactively from the OVOC to the devices, communicating via a NAT pinhole created by the Agent. The Agent checks for new actions for devices related to it, in the OVOC. If actions are present, the Agent performs them on the devices.

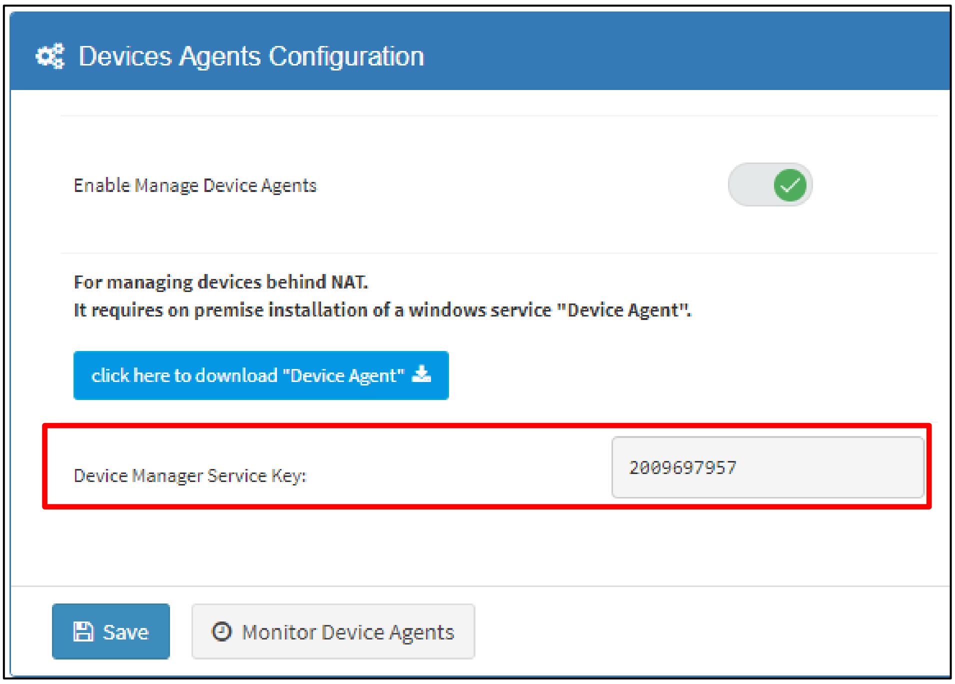
**Figure 1-3: Sending Actions from OVOC to Devices behind a NAT, Using Manager Agent**



The OVOC determines per tenant if devices are behind a NAT and if an Agent is installed.

The Device Manager has its own unique key to ensure that only authenticated Agents can access the application. The key is displayed in the 'Devices Agents Configuration' page of the Device Manager.

**Figure 1-4: Device Manager Key**



Devices Agents Configuration

Enable Manage Device Agents ✓

For managing devices behind NAT.
It requires on premise installation of a windows service "Device Agent".

Device Manager Service Key: 2009697957

The network administrator must configure this key on the Agent, using the Agent's Web Interface (see under Section 2.3 for detailed information). This must be done for Agent authentication purposes.

Each tenant operating with an Agent aggregates the actions of all devices under it. An Agent can handle more than one tenant.

When a network administrator performs an action in the OVOC on a specific device or list of devices, a message pops up indicating that the action was sent to the device and the status of the device will be updated in a few minutes.

Actions are stateless; after the Agent receives the list of actions, it's deleted from the OVOC.

Actions are not reliable; the network administrator can only determine if an action was performed by viewing the device status and device alarms.

This page is intentionally left blank.

# 2 Setting up Device Manager Agents

Before installing and configuring the Device Manager Agent, the Device Manager must be enabled to support Agents as shown in the next section.

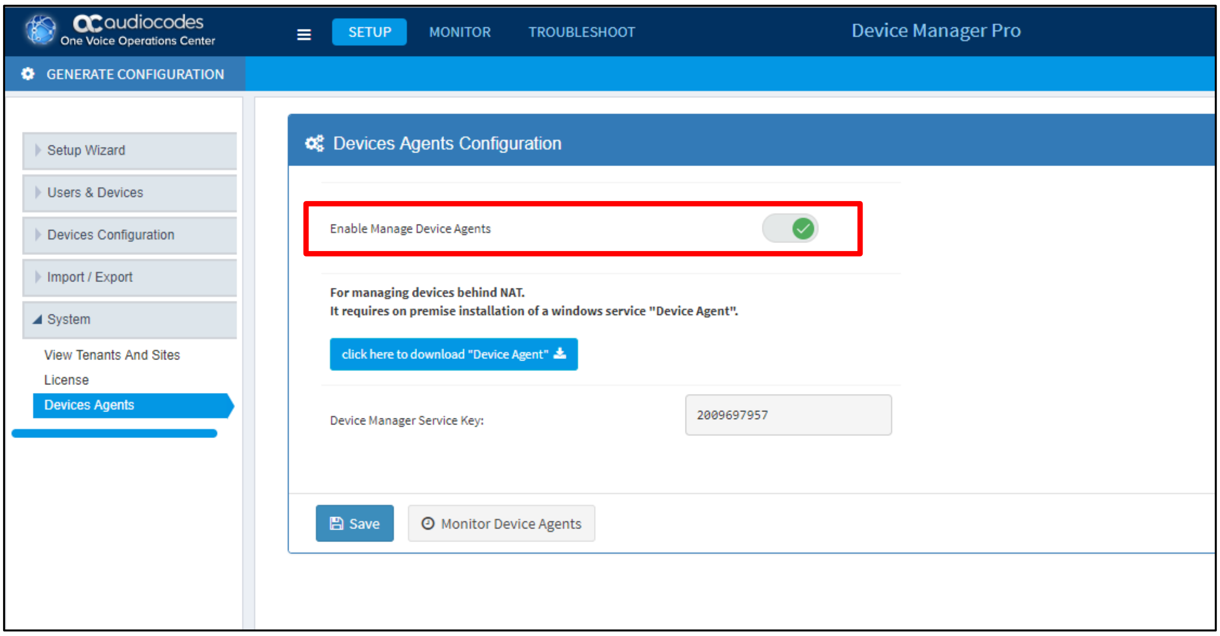
## 2.1 Enabling Device Manager to Support Agents

The network administrator can enable support for the Agent in the Device Manager.

➢ **To enable support for the Agent:**

1. In the Device Manager, open the Devices Agents Configuration page (**Setup** > **System** > **Device Agents**).
2. Drag the **Enable Manager Device Agents** slider to the 'on' position.

**Figure 2-1: Enabling Manager Device to Support Agents**



Enable Manage Device Agents ✓

For managing devices behind NAT.
It requires on premise installation of a windows service "Device Agent".

Device Manager Service Key: 2009697957

3. Click **Save**; the Device Manager now supports Agents.
4. Make sure that the icon ⚙ is displayed in the uppermost right corner of the Device Manager GUI.
5. If it isn't displayed, log out and log in again.

## 2.2 Installing a Device Agent

Before installing the Device Manager Agent software application, make sure you have a clean Windows server

- with at least two cores for every 300 devices
- inside the NAT network (mandatory)
- able to reach all devices (mandatory)

➢ **To download the installation:**

1. Click click here to download "Device Agent"
2. Go to your Windows server and install it.

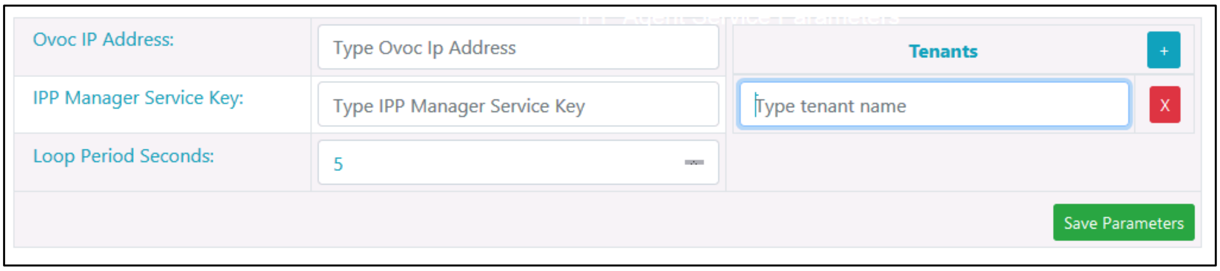
## 2.3 Configuring a Device Agent

After installing the Device Manager Agent software application on the desktop, view the following icon displayed:

➢ **To configure a Device Agent:**

1. Click the icon shown above which is displayed after installing the Device Manager Agent software application on the desktop; the Agent's Web Interface page opens.

**Figure 2-2: Agent's Web Interface**



IPP Agent Service Parameters

| | | | |
|---|---|---|---|
| Ovoc IP Address: | Type Ovoc Ip Address | Tenants | + |
| IPP Manager Service Key: | Type IPP Manager Service Key | Type tenant name | X |
| Loop Period Seconds: | 5 | | |
| | | | Save Parameters |

2. Enter the OVOC's IP Address/FQDN.
3. In the 'Manager Service Key' field, enter the key. Obtain it from its field displayed in the 'Devices Agents Configuration' page in the Device Manager (**Setup** > **System** > **Device Agents**) (see Figure 1-4).
4. Enter a tenant name (you can set more than one tenant using the **+** icon)
5. Click **Save Parameters**.

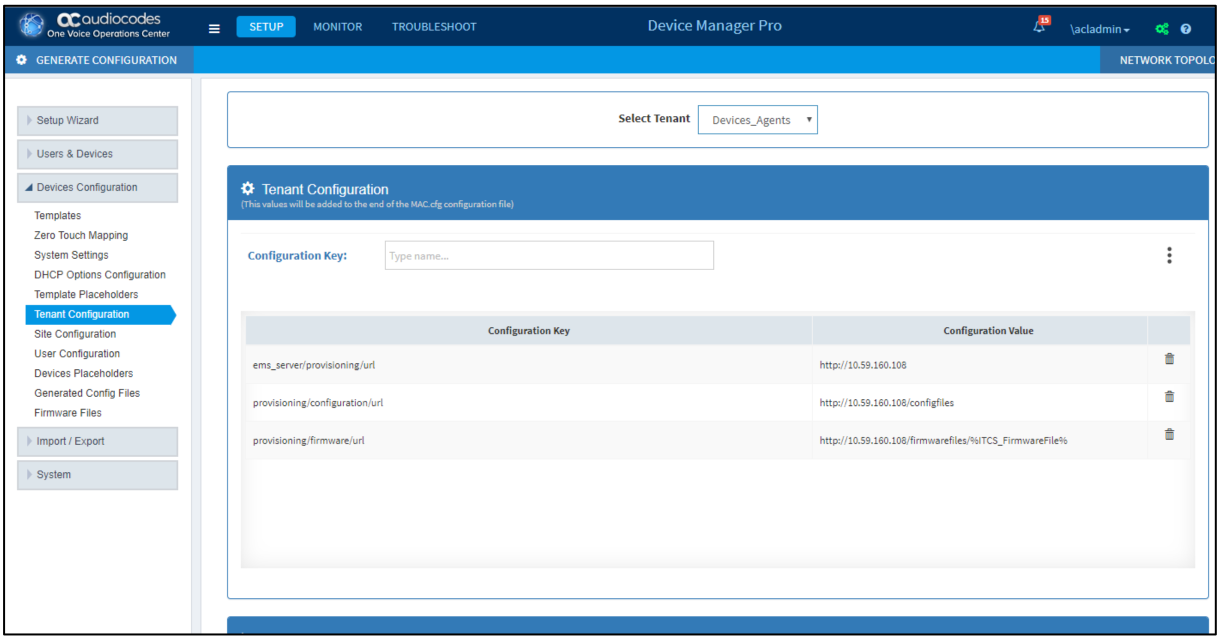
## 2.4 Configuring a Tenant

Devices can send all their traffic directly to the OVOC or through an Agent. For devices to send their traffic through an Agent (recommended), you need to perform configuration at the tenant level. The tenants are the same tenants you configure in the Agent.

### ➢ To configure a tenant:

- In the Device Manager, open the Tenant Configuration page (**Setup** > **Devices Configuration** > **Tenant Configuration**).

**Figure 2-3: Tenant Configuration**



Select Tenant: Devices_Agents

Tenant Configuration
(This values will be added to the end of the MAC.cfg configuration file)

Configuration Key: Type name...

| Configuration Key | Configuration Value |
|---|---|
| ems_server/provisioning/url | http://10.59.160.108 |
| provisioning/configuration/url | http://10.59.160.108/configfiles |
| provisioning/firmware/url | http://10.59.160.108/firmwarefiles/%ITCS_FirmwareFile% |

### ➢ To configure keep-alive traffic to be sent via the Agent:

```
ems_server/provisioning/url http://AGENT_IP
```

### ➢ To configure configuration files traffic to be sent via the Agent:

```
provisioning/configuration/url http://AGENT_IP/configfiles
```

### ➢ To configure firmware files traffic to be sent via the Agent:

```
provisioning/firmware/url http://AGENT_IP/firmwarefiles/%ITCS_FirmwareFile%
```

This page is intentionally left blank.

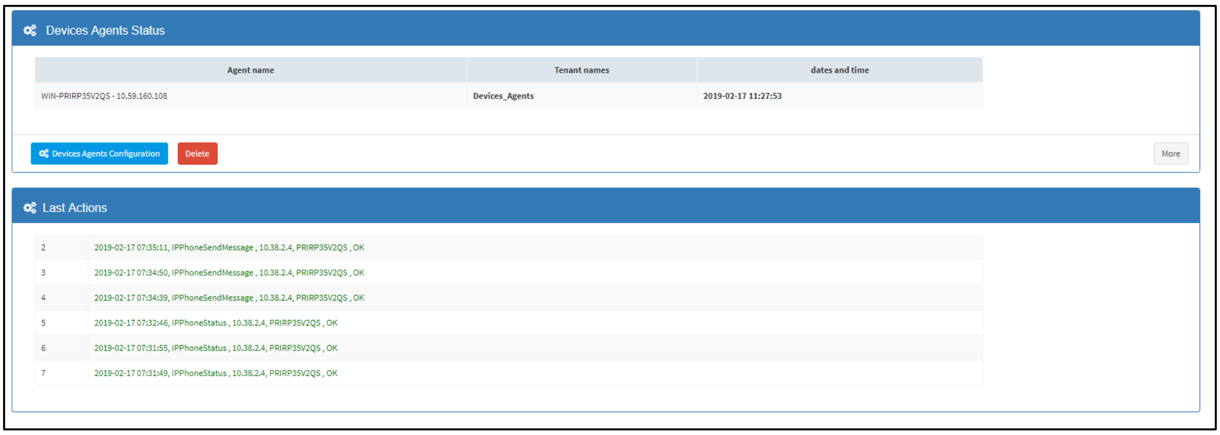
# 3 Monitoring Device Manager Agents

The Device Manager allows network administrators to view a list of Device Manager Agents registered to the deployment as well as view the last action each Agent performed for its devices.

### ➢ To monitor Agents:

1. In the Device Agents Configuration page, click the Monitor Device Agents button or the icon displayed in the uppermost right corner.

**Figure 3-1: Monitoring Device Manager Agents**



Devices Agents Status

| Agent name | Tenant names | dates and time |
|---|---|---|
| WIN-PRIRP35V2QS - 10.59.160.108 | Devices_Agents | 2019-02-17 11:27:53 |

Last Actions

| | |
|---|---|
| 2 | 2019-02-17 07:35:11, IPPhoneSendMessage , 10.38.2.4, PRIRP35V2QS , OK |
| 3 | 2019-02-17 07:34:50, IPPhoneSendMessage , 10.38.2.4, PRIRP35V2QS , OK |
| 4 | 2019-02-17 07:34:39, IPPhoneSendMessage , 10.38.2.4, PRIRP35V2QS , OK |
| 5 | 2019-02-17 07:32:46, IPPhoneStatus , 10.38.2.4, PRIRP35V2QS , OK |
| 6 | 2019-02-17 07:31:55, IPPhoneStatus , 10.38.2.4, PRIRP35V2QS , OK |
| 7 | 2019-02-17 07:31:49, IPPhoneStatus , 10.38.2.4, PRIRP35V2QS , OK |

2. View in the Devices Agents Status page that opens (shown in the preceding figure):
   - the names of the Agents registered in the deployment
   - the names of the Tenants under which Agents are registered
   - the date and time each Agent was registered
   - the last action each Agent performed for its devices

**International Headquarters**
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

**AudioCodes Inc.**
200 Cottontail Lane,
Suite A101E, Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

**Contact us:** https://www.audiocodes.com/corporate/offices-worldwide
**Website:** www.audiocodes.com