# Dante Domain Manager Deployment Guide for AWS

Document version: 1.1

Document date: 5th September 2024

Document name: AUD-MAN-DDM-AWS-Deployment

Dante®

# Copyright



# Legal Notice and Disclaimer

Audinate retains ownership of all intellectual property in this document.

The information and materials presented in this document are provided as an information source only. While effort has been made to ensure the accuracy and completeness of the information, no guarantee is given nor responsibility taken by Audinate for errors or omissions in the data.

Audinate is not liable for any loss or damage that may be suffered or incurred in any way as a result of acting on information in this document. The information is provided solely on the basis that readers will be responsible for making their own assessment, and are advised to verify all relevant representation, statements and information with their own professional advisers.

# Software Licensing Notice

Audinate distributes products which are covered by Audinate license agreements and third-party license agreements.

For further information and to access copies of each of these licenses, please visit our website: www.audinate.com/software-licensing-notice

# Contacts


## Audinate Pty Ltd

Level 7/64 Kippax Street

Surry Hills NSW 2010

AUSTRALIA

Tel. +61 2 8090 1000

info@audinate.com

www.audinate.com

## Audinate Inc

4380 S Macadam Avenue

Suite 255

Portland, OR 97239

USA

Tel: +1 503 224 2998

## European Office

Audinate Ltd

Future Business Centre

Kings Hedges Rd

Cambridge CB4 2HY

United Kingdom

Tel. +44 (0) 1273 921695

## Asia Pacific Office

Audinate Limited

Suite 1106-08, 11/F Tai Yau Building

No 181 Johnston Road

Wanchai, Hong Kong

澳迪耐特有限公司

香港灣仔莊士敦道181號

大有大廈11樓1106-8室

Tel. +(852)-3588 0030

+(852)-3588 0031

Fax. +(852)-2975 8042

# Contents

# Revision History

| Version | Date | Notes |
|---|---|---|
| 1.0 | 16th August 2024 | Initial version |
| 1.1 | 5th September 2024 | Updates following internal review |

# 1. Dante Domain Manager Overview

Dante Domain Manager (DDM) makes media networking more secure, more scalable and more manageable than ever before. With DDM, integrators can define specific AV device groupings, by room, building and site, allowing for the creation of independent Dante Domains, and enabling a single Dante Domain to encompass multiple network subnets.

DDM provides robust security for IT departments and AV managers, including user authentication and encrypted control.

System managers gain complete visibility and accountability with a suite of dashboards, audit trails, and system alerts.

DDM is available as a virtual appliance for various hypervisors and is now supported for hosting on AWS. It has an intuitive and highly responsive web interface for desktop and tablet browsers.

## 1.1. Features

Key features of DDM include:

- Security:
  - All communication between devices and controllers is encrypted
  - The DDM provides authentication and access controls for users and controllers
- Multiple Subnets: Dante name-based routing functions across subnets
- Monitoring: All system events are logged and can be reviewed by administrators
- Auditing: All user actions are logged and can be reviewed by administrators
- Multimedia support: Audio, video, and ancillary video (control data) channels are supported
- Support for Dante Managed API
  - Provides a way to programmatically interact with your Dante devices when enrolled in Dante Domain Manager

## 1.2. Benefits and limitations of hosting Dante Domain Manager in the cloud

### Benefits

- No on-premises server infrastructure is required when hosting DDM in the cloud.
- Depending on configuration, devices connected to a cloud hosted DDM may be remotely manageable in Dante Controller.
- Depending on configuration, devices connected to a cloud hosted DDM may be remotely manageable via the Dante Managed API.
- Depending on the configuration, it may be possible to combine management of multiple sites into a single DDM instance.

### Limitations

- **IMPORTANT:** 'HA' High Availability mode is not currently supported on cloud hosted DDM.

## 1.3. Deployment Overview

Dante Domain Manager can be deployed on an Amazon EC2 instance owned and managed directly by the user on their AWS account. This guide assumes that the user has a basic understanding of setting up, launching, and using Amazon EC2 Linux instances. Detailed documentation for AWS can be referenced at docs.aws.amazon.com.

## 1.4. Dante Domain Manager AWS Architecture

Network configuration is ultimately up to the user. There are two basic options for connecting on-premise Danter devices with AWS hosted DDM:

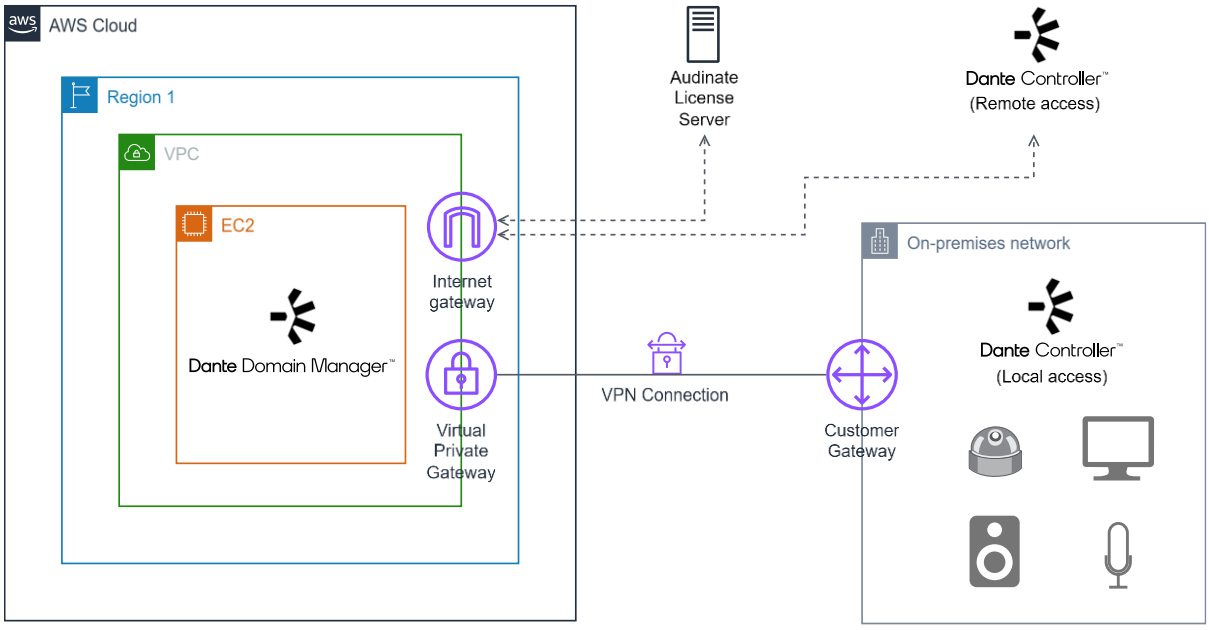
1. AWS Site-to-Site VPN between your on-premise Dante network and the DDM instance in AWS
2. Device connection over the Internet, using UDP over port 8000

Each of these options is covered below.

Please note, in each case Dante Domain Manager periodically needs to contact the Audinate License Server – at the minimum after initial installation then after renewal of the Term license – plus some additional optional services. See the 'detailed deployment guide' below for required address and port and access.

# Example Architecture for Dante Domain Manager over VPN

**1. Example architecture for Dante Domain Manager in AWS over VPN**




Dante Domain Manager is running in its own Amazon EC2 instance in a VPC.

Note that 'HA' High Availability mode is not currently supported on cloud hosted DDM; only a single instance of DDM is possible.

Dante devices are connected to the on-premises network.

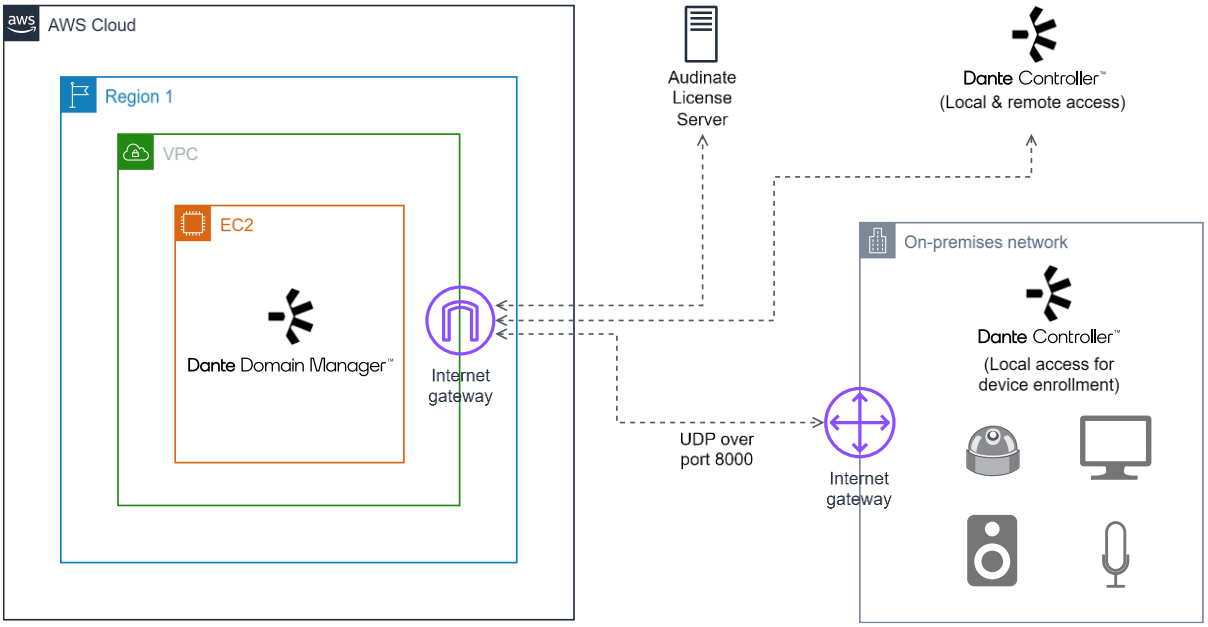
There is a Site-to-Site VPN connection between the on-premises network and the AWS VPC, creating effectively one LAN with routable IP addresses for the DDM server and the Dante devices. See https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html for more information.

Dante devices can be discovered by DDM using DNS and DHCP; enrolled by IP address or enrolled using Dante Controller in local access mode (connected to the same LAN subnet as the devices at the time of enrolling). See the DDM user guide for more information about device discovery and enrolment.

Once devices are enrolled in Dante Domain Manager, their configuration may be accessed by Dante Controller in remote access mode, running anywhere and connected to DDM via the Internet Gateway. Dante Controller connects to the Dante Domain Manager via its own secure protocol. See the 'detailed deployment guide' below for required inbound port access.

# Example Architecture for Dante Domain Manager over Port 8000

**2. Example architecture for Dante Domain Manager in AWS over port 8000**




Dante Domain Manager is running in its own Amazon EC2 instance in a VPC.

Note that 'HA' High Availability mode is not currently supported on cloud hosted DDM; only a single instance of DDM is possible.

Dante devices are connected to the on-premises network, with a gateway allowing selected Internet traffic to / from the Dante devices. NAT translation is supported by this model.

UDP over Port 8000 ingress & egress must be allowed by firewall rules. This is used for direct device connection to DDM hosted AWS. All communications over this port are initiated by the local device.

Dante devices can only be enrolled using Dante Controller in local access mode (connected to the same LAN subnet as the devices at the time of enrolling) in this model. Devices can be configured with either a fixed IP address for your DDM server, or a Fully Qualified Domain Name (FQDN) resolving to that address. If an FQDN is used, it is recommended to also maintain a fixed IP address for best compatibility as some versions of Dante devices are unable to store an FQDN for the DDM server and will revert to storing the IP address.

Once devices are enrolled in Dante Domain Manager, their configuration may be accessed by Dante Controller in remote access mode, running anywhere and connected to DDM via the Internet Gateway. Dante Controller connects to the Dante Domain Manager via its own secure protocol. See the 'detailed deployment guide' below for required inbound port access.

# 1.5. Deployment Considerations

## Quotas

There is nothing fundamental in Dante Domain Manager that would require an increase of AWS limits. Only control and monitoring traffic is sent between devices, controllers and DDM. No media is routed outside the local network in the usage scenario described in this document.

## AWS Regions / Data Centers

Dante Domain Manager can be installed on any AWS data center/region that provides the required Amazon EC2 instance types. We recommend that you choose a region closest to you for faster service and lower latency.

## Technical Prerequisites and Requirements to Complete Deployment Process

| | |
|---|---|
| AWS Instance Type | Requirements for Dante Domain Manager depends on the number of Dante devices in the system. See Detailed installation guide below for more information.<br><br>AWS Instance Type t3.medium is generally sufficient for Dante Domain Manager. |
| Operating System | Rocky 9 Linux |
| GPU | Not required |
| Storage | Amazon EBS volume (General Purpose SSD) for OS and application installation |
| Remote access | DDM web user interface; SSH if required |
| Licensing | DDM license purchased from Audinate (DDM Gold or Platinum) |

### Skills Or Specialised Knowledge Required by The User

It is recommended that as a user of Dante Domain Manager:

- You have at least Dante Certification Level 3
- You are comfortable deploying Linux servers either on the Cloud or on a local Hypervisor
- You are comfortable working with AWS
- Instances have Internet access for licensing DDM

## Security Considerations

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared responsibility model reduces your operational burden because AWS operates, manages, and controls the components including the host operating system, the virtualization layer, and the physical security of the facilities in which the services operate. For more information about AWS security, visit AWS Cloud Security.

It is the responsibility of the customer to ensure the security of communications between Dante Domain Manager and the on-premise network. A Site-to-Site VPN is strongly recommended.

## Root User Privileges Are Not Required

The user deploying Dante Domain Manager on AWS does not require the use of root privileges for deployment or operation. Users should not use root access for any deployment of Dante Domain Manager.

## Least Privileges Principle

Users of the system can only manage Dante device settings, channel mappings and Dante domain configuration via Dante Controller or the Dante Domain Manager web interface and need not access the underlying instances or configuration.

Access for users is additionally limited by authentication into Dante Domain Manager via Dante Controller and into the Dante Domain Manager web interface, with users, roles and access privileges maintained within Dante Domain Manager.

Additionally, Dante Domain Manager (DDM) offers the 'Dante Managed API' to query and control Dante parameters of devices. This API is secured by API keys which are generated inside the DDM web user interface. Each API key is limited by DDM user scope (constrained to devices and actions associated with the user role).

## Security Groups

The Dante Domain Manager instance should be configured using AWS Security Groups to allow the specific protocols, ports and IP address ranges required for operation of Dante Domain Manager and Dante Controller, for management of the instance via SSH and for access to the external licensing server.

Details for configuration of Security Groups are listed in the 'Security' section of the Detailed installation guide below.

It is recommended that a single Security Group is established for the Dante Domain Manager Instance unless the specific application calls for a more complex scheme.

Additional information about Security Groups is available at Control traffic to your AWS resources using security groups - Amazon Virtual Private Cloud.

Additional information on Network Ports used by Dante is available at Which network ports does Dante use? | Audinate | FAQs

# 1.6. Costs

## AWS Resource Costs

AWS costs to consider are:

- EC2 instance costs
- Elastic IP costs (when a public static IP address is required, e.g. for device communications outside of a VPN)

General information for each of these cost considerations is below.

- Customers must license an Amazon EC2 instance in order to deploy Dante Domain Manager (see 'Technical Prerequisites and Requirements to Complete Deployment Process' above for details). Costs associated with each AWS billable service is owned and maintained solely by AWS and is separate from costs associated with licensed Audinate software.

The recommended EC2 instance for Dante Domain Manager is t3.medium. As of February 2023, the cost of running this EC2 with the default settings in the US East (N. Virginia) Region is $30.37/Month ($0.0416/Hour) based on the AWS OnDemand hourly rate.

The design on the network on which Dante Domain Manager is deployed is very much up to the customer's needs. Deployments in a single subnet, single site, multiple site etc. are all possible and solely guided by the workflow requirements of the customer. In more complex deployments additional costs are applicable.

One Elastic IP address is free to use with an EC2 Instance. However, there is a charge of $0.005 per every hour the instance is not running (for example, stopped overnight). For full details, refer to the pricing webpage for each AWS service you will be using, or contact your AWS account manager.

Details of the costs can be estimated using AWS Pricing Calculator.

## Audinate Licensing

Dante Domain Manager is offered as a Bring Your Own License (BYOL) model. The license for Dante Domain Manager is installed and activated on its Amazon EC2 host instance.

Pricing is based on an up-front term model. Pricing depends on the number of devices being managed and options selected.

Cost and payments for the Dante Domain Manager software is managed directly between the customer and Audinate or its authorized agents. Charges and payment options are not supported within the AWS payment process at this time.

# 2. Detailed Installation Guide

## 2.1. Bootstrap Dante Domain Manager (DDM)

Ensure DDM has a sufficient license type to support the desired number of Dante devices being managed.

### Provisioning the Server for DDM

#### System Requirements

| No. of Devices | <100 | 100 - 200 | >200 |
|---|---|---|---|
| CPUs | 2 | | 3 |
| RAM (GB) | 4 | 8 | 16 |
| Hard Disk (GB) | 20 | | 30 |
| Architecture | Intel x86 64-bit | | |

AWS Instance Type t3.medium is sufficient for DDM.

### Security

DDM needs Internet access for activating the license and installing the online upgrades.
IP Ranges below are only given as an example.

Depending on the desired level of security of your DDM image over the internet or an internal link you might need to ensure the following ports are opened either for DDM control or device management:

| Type | IpProtocol | FromPort | ToPort | IpRanges |
|---|---|---|---|---|
| Inbound/Ingress | tcp | 80 | 80 | 0.0.0.0/0 (Web UI) |
| Inbound/Ingress | udp | 8000 | 8000 | 10.0.0.0/8 (Typical - Dante Device communication) |
| Inbound/Ingress | tcp | 8001 | 8001 | 0.0.0.0/0 (Dante Controller communication) |
| Inbound/Ingress | tcp | 8080 | 8080 | 0.0.0.0/0 (Crashlogs download) |
| Inbound/Ingress | tcp | 22 | 22 | 0.0.0.0/0 |
| Inbound/Ingress | tcp | 8443 | 8443 | 0.0.0.0/0 (Dante Controller login) |
| Inbound/Ingress | tcp | 443 | 443 | 0.0.0.0/0 (Web UI TLS) |
| Inbound/Ingress | icmp | -1 | -1 | 0.0.0.0/0 |
| Inbound/Ingress | udp | 8702 | 8702 | 10.0.0.0/8 (Typical - Device Enrolment via IP) |
| Outbound/Egress | -1 | | | 0.0.0.0/0 |

Inbound 0.0.0.0/0 is only needed if you need a public-facing DDM Server. Otherwise, internal VPC range should be enough.

# Installing DDM

⚠ Rocky 9 x86 is the only official Linux version supported by DDM.

Proper DDM installation and behaviour are not guaranteed in any other Linux version.

## DDM Installer script

The DDM Installer script is downloadable from the Dante website. Go to https://www.getdante.com/product-support/dante-domain-manager/ and choose 'Download Dante Domain Manager' to get to the latest download page. You will need to log in with your Audinate account.

*Note, the ISO image is generally not compatible with AWS hosting.*

The DDM Installer script is offered as a direct download from the website, or you can copy the URL to directly download it to your server, for example:

```
curl -O <url>
```

The command to run the script looks like (for example):

```
sudo bash ddm-n.n.n.n_linux_x64.sh -s -b
```

# DDM First Configuration

Once the Instance is up and running you will be able to reach its web interface to finish the DDM setup (either using its public IP or the private one depending on your setup).

- **Installation Type**: Fresh installation.
- **Admin User**: Create a new DDM admin user password.
- **Product Key:** Insert the DDM license we provided you.
  This step requires the DDM instance to have internet access.
- **TLS Certificates**: allows SSL for the web interface.
  You might need to refresh the Web UI after applying them.
- **FQDN**: Use the default value or the private server IP address (or your custom FQDN name if you have your own DNS).

See the Dante Domain Manager user guide for more information about enrolling devices (HTML / PDF).

At this point you should have a running DDM server.

⚠ Under some situations you might need to verify the right network interface has been selected by DDM to reach the Dante Devices.

Go to 'Settings' > 'Network & Security' > 'Network' and double check the "Dante Interface" name matches with the Linux Instance name (you can run ip addr under a remote SSH connection)

# 3. Operations

## 3.1. Troubleshooting

The Dante Domain Manager web interface offers detailed event information through the Audit Log. This information is designed to assist with day-to-day troubleshooting.

There are additional logging options available in Dante Domain Manager - see 'Configure Logging' in the Administration Menu of the web interface. Logging options include performance logging, crash logs and core dumps.

Logging levels can be set for the service, web app and device manager, or at a global level. The default logging level for all components is 'notice'. For the device manager you can also set per-scope logging levels.

Logs and core dumps may be used to provide information back to Audinate Support to assist with root cause analysis.

Refer to the DDM User Guide for more information.

**Dante Controller** provides additional troubleshooting tools in including device status, clock status, clock and latency histograms, device level event logs, channel subscription status and signal presence.

Refer to the Dante Controller user guide for more information.

### DDM Discovery and Enrolment

If a Site-to-site VPN is used and DNS discovery is properly configured, Dante devices should automatically discover DDM. Open the DDM web user interface, navigate to the Devices panel, and watch for Dante Devices showing up in the Unmanaged section.

See the DDM User Guide for more information about setting up DHCP and DNS for device discovery.

If that's not the case, other options are available, depending on the architecture you have chosen:

1. Manual enrolment using Dante Controller (works with any architecture):
    a. You must be able to run Dante Controller on a computer that is connected to the same network subnet as the Dante devices you wish to enrol.
    b. Launch Dante Controller from DDM, so that it is authenticated to the DDM. Alternatively you can log into DDM from Dante Controller with the DDM address and DDM user credentials.
    c. Select the '<unmanaged>' domain. You should see unenrolled devices on your local network. Check your network port selection if they don't appear.
    d. Choose 'Devices > Connect devices to DDM / Dante Cloud'
    e. Check the DDM server address and port. If this is not correct, you may need to log out of DDM in Dante Controller, choose 'Devices > Connect devices to DDM / Dante Cloud' again then 'Manually configure server'.
    f. Select your devices to enrol and click 'OK'
    g. In the DDM web UI, the devices should now turn up in the 'Unmanaged' section. Move your devices to the desired Domain.

2. Enrol devices by IP (this option requires a Site-to-site VPN as DDM must be able to find the devices by their IP address)
    a. In the DDM Web UI go to Devices > Enrol Devices > Enrol by IP Address
    b. Add your Device IP or upload a CSV file.
    It will be automatically moved to the Domain.

If the device remains in Pending, there may be a communication issue between itself and the DDM or not all the necessary ports have been authorised: Which network ports does Dante use? | Audinate | FAQs

## Health Check

The Dante Domain Manager web interface features a system dashboard that shows alerts and statistics for various system health and performance metrics. The dashboard can be used for general performance monitoring. Information available includes domain statistics, clocking alerts, security alerts, and device firmware notifications. Additional per device performance metrics on audio latency and clock drift.

All users are able to customize their DDM dashboard.

## Backup & Recovery

Dante Domain Manager is able to create a backup file of its configuration as required. Contents of the backup include:

- Domain names and credentials (domain credentials are shared between domains and devices to establish membership)
- Device enrolment information
- User and role information, including usernames, passwords (encrypted), role names, etc.
- Dashboard alerts

The backup function is available in the Administration menu of the Dante Domain Manager web interface. The backup configuration will be made available for download at port 8080. Note that DDM will go offline while the backup is taken.

Configuration can be restored during the Licensing and Setup process following fresh installation of Dante Domain Manager.

Refer to the Dante Domain Manager user guide for more information.

# 3.2.Routine Maintenance

Available updates to Dante Domain Manager can be viewed and applied from within the Settings menu of the Dante Domain Manager web interface.

Refer to the Dante Domain Manager user guide for more information.

# 3.3.Emergency Maintenance and Support

## Emergency Maintenance

The monitoring of the network on which Dante Domain Manager in deployed is the customer's responsibility, mechanisms such using CloudWatch to monitor the EC2 instance or autoscaling can be used as required.

In the event of an EC2 failure, Dante Domain Manager state can be restored from a backup see the section 'Backup and Recovery' for details. Please note that Dante Domain Manager cannot be run in High Availability mode when hosted on AWS (as of DDM v1.8). This may be supported in a future release.

## Standard Support

Support enquiries may be lodged via a web-based form at https://www.audinate.com/contact/support or via email to support@audinate.com.

Our support teams operate during normal business hours (9am-5pm Monday-Friday, excluding public holidays) in your closest region being USA (Pacific Standard Time), EMEA (Greenwich Mean Time) or Asia-Pacific (Japan/China).

Support issues may be escalated to our engineering team if no solution or workaround is available.

## Enhanced Support Services

We may offer enhanced support services via partners depending on customer needs. Please discuss with your Audinate or partner representative.

## Ongoing Maintenance

From time-to-time we will provide:

- Updates. These may include issue resolutions, security updates and minor enhancements.
- New Releases. These may include new functionality.

Updates can be applied to existing installations of Dante Domain Manager via the in-built online update function.