# audinate

# Dante Domain Manager
# Quick Start Guide

**v2.10**

**21st July 2021**

**For Dante Domain Manager v1.2.0 and up**

# Copyright

© 2021 Audinate Pty Ltd All Rights Reserved.

Audinate®, the Audinate logo and Dante are trademarks of Audinate Pty Ltd.

All other trademarks are the property of their respective owners.

Audinate products are protected by one or more of US Patents 7747725, 8005939, 7978696, 8171152 and other patents pending or issued. See www.audinate.com/patents.

# 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

1200 NW Naito Parkway

Suite 630

Portland, OR 97209

USA

Tel: +1 503 224 2998

## European Office

Audinate Ltd

Suite 104

Werks Central

15-17 Middle St

Brighton, BN1 1AL

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

# 1. Network Configuration

Dante Domain Manager (DDM) supports automatic device discovery using DNS or mDNS, and also manual device enrollment via IP address.

DNS and DHCP addressing is recommended for multi-subnet systems.

mDNS and link-local addressing is recommended for single-subnet systems.

Device enrollment via IP address can be used for multi-subnet systems that require static addressing (for example, to support third-party network control software).

> **Note**: When using static addressing, the devices *and* the DDM server must be assigned static addresses, either locally (where DHCP is not used) or via static address mapping in DHCP.

## 1.1. Multi-subnet systems

If your network spans multiple IP subnets, you can use a DNS server to resolve the DDM server address for your Dante devices and controllers, and a DHCP server to automatically configure your Dante devices.

Static addressing and manual device enrollment via IP address can also be used, but it is not practical for networks with large device counts.

Subnet 1
Domain A
Domain B
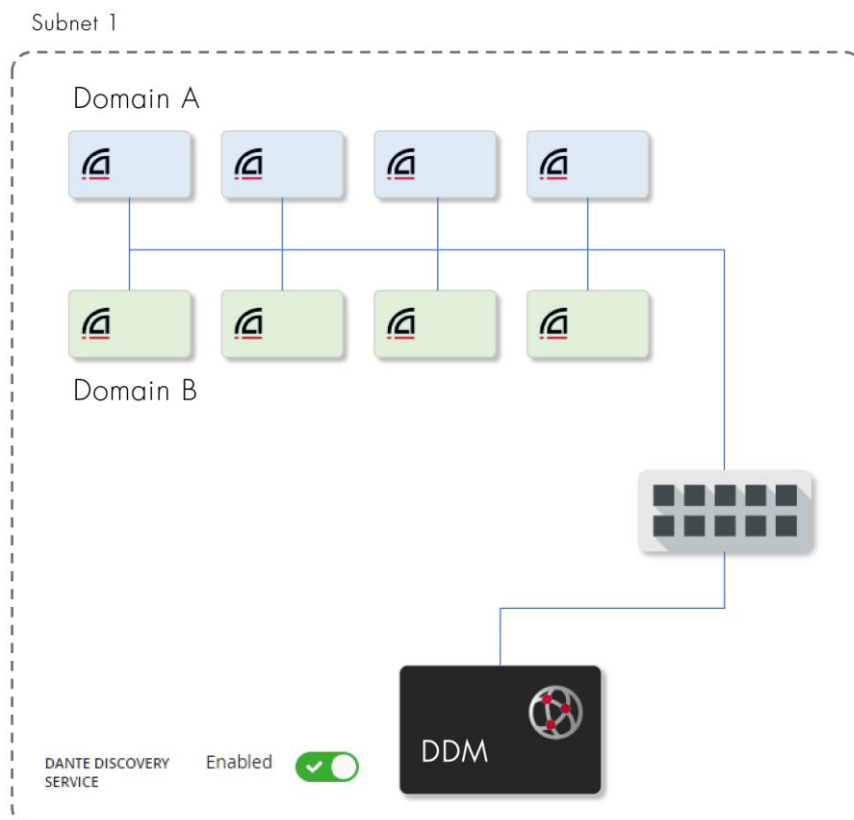
DHCP ☑
DNS ☑

Router

Subnet 2
Domain A
Domain B

DDM
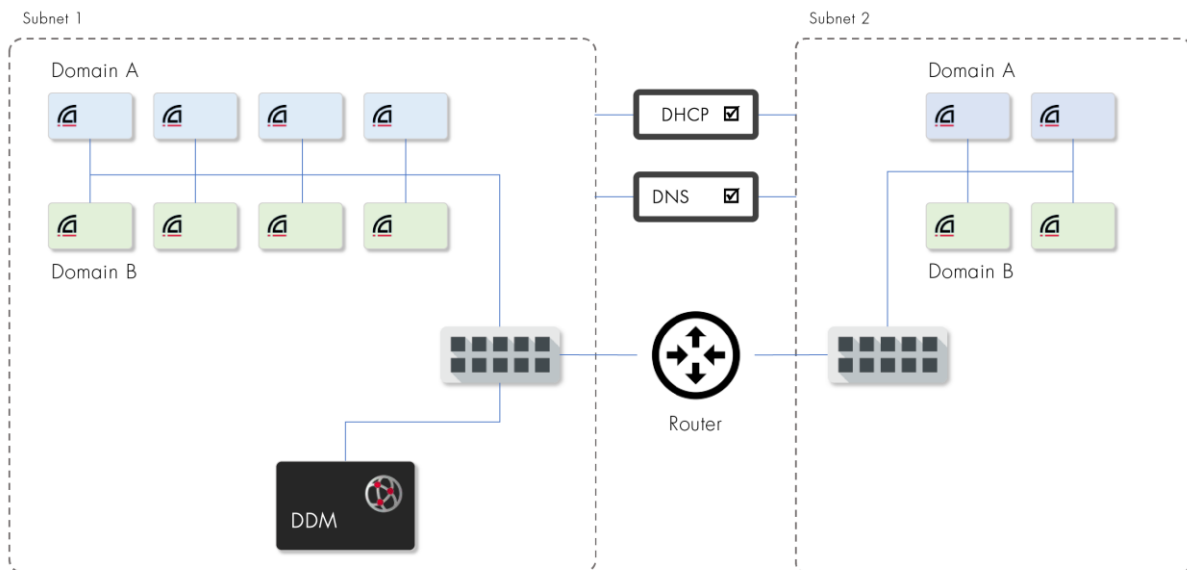
DISCOVERY OPTIONS FOR MULTI-SUBNET SYSTEMS

- DHCP + DNS (recommended)
- Static addressing + manual enrollment
  (not suitable for large device counts)

Refer to the DDM user guide for more information about bootstrapping Dante devices and controllers, including DNS and DHCP setup.

## 1.2. Single-subnet systems

For networks that reside on a single subnet, link-local addressing and mDNS-based discovery is recommended. The mDNS discovery feature (Dante Discovery Service) is on by default, and does not need to be activated or configured.



# 2. Installing DDM

## 2.1. Overview

DDM is packaged as an ISO file, which includes a streamlined Linux distribution which has been pre-configured for the DDM application.

To install DDM you can create a bootable USB drive (for installing DDM on a bare-metal machine, for example) or import the ISO directly into a virtualization platform such as Oracle VirtualBox® or VMWare ESXi®. You can also burn the ISO image to a DVD.

## 2.2. System Requirements for the Physical Host Machine

The licensing model for DDM includes three editions: Silver, Gold, and Platinum. Each edition supports a different number of devices and domains.

- For the Silver and Gold editions, the host machine requires a minimum of 2 CPUs, 20GB of disk space and 4GB of RAM.
- For the Platinum edition, the host machine requires a minimum of 2 CPUs, 20GB of disk space and 8GB of RAM.
- For systems that include more than 200 devices, 16GB of RAM is recommended.

## 2.3. Creating a Bootable USB Drive

### 2.3.1. In Windows

There are various applications available for creating bootable USB drives in Windows.

Rufus (https://rufus.ie/) is a popular (free and open-source) application, but there are other alternatives that may be more suitable for your own environment.

> **Note**: Do not change the volume label.
>
> When prompted, after clicking 'START', select 'DD Image mode' (not 'ISO Image mode') for writing.

### 2.3.2. In Linux

The industry-recommended method for creating a bootable USB drive in Linux is by using dd. The following instructions are adapted from the Centos instructions.

- Assuming your USB stick is seen as /dev/sdb:

  ```
  dd if=[filename].iso of=/dev/sdb
  ```

- You must write to the entire device, and not a partition on it (so, /dev/sdb not /dev/sdb1).

- When asked for the media to install from, select 'Hard disk' and then the device corresponding to the USB key.

- Make sure you select as destination the device corresponding to the USB key (/dev/sdb in the above example) and not a partition (such as /dev/sdb1).

### 2.3.3. Booting from USB

Once you have created a bootable USB drive, you must instruct the target computer BIOS to boot from the USB drive.

Computer manufacturers use many different BIOS implementations – refer to the instructions for your particular computer to find out how to configure the BIOS.

### 2.3.4. Importing the ISO Directly into a Virtualization Platform

ISO files are supported by all major virtualization platforms. Refer to the user guide for your particular platform to find out how to import an ISO file.

For more information about installing DDM in a hypervisor, see the Technical Documentation page at audinate.com.

#### 2.3.4.1. System Requirements for Hypervisors

Hypervisors must be configured to provide sufficient system resources for the virtual appliance based on the host machine RAM and disk space requirements listed in section 2.2.

# 3. Administration Menu

The startup script displays a dialog showing the Dante interface and the IP address for the VM, plus an administration menu.

## 3.1. Network Diagnostics

The Network Diagnostics function performs a set of high-level tests to establish the status of some basic network configuration parameters relevant to the DDM server. Refer to the Network Diagnostics Results page in the DDM user guide for more information.

The license server is at https://software-license-ddm.audinate.com on port 443.

## 3.2. Set Hostname

Use this option if you specifically need to change the hostname (for example, if you are running two DDM servers on the same subnet).

## 3.3. Configure Interfaces

This feature allows you to specify the network interface that DDM will use to connect to the network.

## 3.4. Set NTP Servers

This feature allows you to specify up to four NTP (Network Time Protocol) servers.

By default, the virtual machine on which DDM is installed will derive its time from a public NTP server on the Internet, unless one or more alternative NTP servers are specified here.

**Note**: If your DDM system is configured to use HA and your network is not connected to the Internet, specifying an alternative NTP server is a requirement to ensure accurate database replication.

## 3.5. Set Update Key

Use this function only if instructed to by Audinate technical support.

## 3.6. Fix LMX Time Gone Backwards

Use this function only if instructed to by Audinate technical support.

## 3.7. Configure Logging

Use this feature to set the logging level for the service, web app and device manager, or to set a global logging level. The default logging level for all components is 'notice'.

For the device manager you can also set per-scope logging levels.

## 3.8. Configure Web Proxy

Use this feature to enable DDM to connect to the Internet via an existing NTLM, Kerberos or basic proxy on your web server. Configuration options vary between proxy types.

## 3.9. Branding Mode

Use this option to enable and disable the Branding Settings main menu option in the DDM user interface. See the user guide for more information about configuring the Branding Settings.

## 3.10. Additional Packages

Allows you to install selected Linux packages.

## 3.11. Download Crash Logs

Use this option to download crash logs (if requested by Audinate technical support) in cases where the DDM user interface is unusable.

## 3.12. Exit HA Cluster

Use this function to immediately reset the DDM configuration to 'standalone', for cases where none of the DDM servers are easily accessible.

## 3.13. Performance Logging

Use this feature to temporarily enable performance logging. The logs will be made available for download at port 8080 once logging has been stopped.

## 3.14. Shutdown/Reboot

Use this option to shut down or reboot the DDM instance.

## 3.15. Quit

Closes the administration menu and returns you to the VM main console.

# 4. Licensing and Setup

1. Open up a web browser on a device connected to the virtual machine and navigate to http://<Virtual Machine IP address>

2. The initial screen presents the End User License Agreement (EULA).
   Read the EULA and click "I Accept" to proceed.

3. The following screen allows you to upload and use your own TLS certificate to secure the Dante Domain Manager. This configuration can be skipped for now and accessed later under Settings. If you want to use a TLS Certificate, refer to the DDM User Guide for more information.

4. The next screen allows you to select between starting with a fresh installation, or restoring your configuration from a backup of an existing system. Choose the 'Fresh Installation' option (unless you have a saved configuration that you want to restore).

5. Step 1 of the wizard asks if you are installing as a third party (for example, a system integrator) or an end customer. This information is only required for EULA notification purposes.

6. Step 2 allows you to set the administrator user's password. Enter and confirm the password, generate and record the recovery code, and click S*ubmit* to proceed to the next step.

7. Step 3 prompts you to enter your Dante Domain Manager product key to license the product. Enter your product key and click *Activate* to proceed.
   **Note**: This step requires the DDM to have an active internet connection.

8. Step 4 prompts you for a fully qualified domain name (FQDN) for the DDM server. The field is pre-populated with a suitable FQDN based on your network configuration, but you can edit this if required.

9. Step 5 allows you to create your first Dante Domain. Enter the name of the Domain and click S*ubmit* to complete the wizard. You can easily delete this domain and add new domains later.

You are now ready to begin enrolling devices in your newly created domain.

## 4.1. Viewing Domains in Dante Controller

After enrolling devices, launch Dante Controller and click on the Domains icon on the far right of the toolbar.

Enter the host details and login details for your Dante Domain Manager in the domain connection dialog, and click *Connect* to view and configure the domain-connected devices. Use the drop-down menu to select different domains.