Dante Domain Manager

User Guide

DDM version: 1.1.1 and up

Document version: 1.1

Published: Thursday, February 11, 2021

Copyright

Audinate products are protected by one or more of US Patents 7747725, 8005939, 7978696, 8171152, European Patent 2255541, Chinese Patent ZL200780026677.0, 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

Contents

About Audinate

Audinate® was founded with a vision to revolutionize professional and commercial audio for the 21st century. Audinate’s award winning Dante® audio over IP networking solution is the worldwide leader and used extensively in the professional live sound, commercial installation, broadcast, public address, and recording industries.

About Dante

Dante is the de facto standard digital media networking solution, using standard IP infrastructure to network devices, and making interoperability easy and reliable. It distributes uncompressed, multi-channel digital media via standard Ethernet networks, with near-zero latency and perfect synchronization.

It's the most economical, versatile, and easy-to-use media networking solution, and is scalable from simple installations to large-capacity networks running thousands of channels. Dante can replace multiple analog or multicore cables with a single affordable Ethernet cable to transmit high-quality multi-channel media safely and reliably. With Dante software, the network can be easily expanded and reconfigured with just a few mouse clicks. Dante technology powers products available from hundreds of partners around the world.

For more information, please visit the Audinate website at www.audinate.com.

Overview

Dante Domain Manager makes audio networking more secure, more scalable and more manageable than ever before. With Dante Domain Manager, 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.

Dante Domain Manager 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.

Dante Domain Manager is available as a virtual appliance for various hypervisors. It has an intuitive and highly responsive web interface for desktop and tablet browsers.

Features

Key features of the Dante Domain Manager 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

About Dante Domains

Dante Domain Manager can support multiple domains. A Dante domain is a logical group of Dante devices. Domains can span IP subnets.

Dante devices within a domain support audio routing within and across subnets to other devices in the same domain. Dante label-based routing can be used. All devices with a domain are synchronized to the same clock. Each Dante Domain is an independent clock domain - this means changes in clocking in a given Dante Domain does not affect clocking in other domains.

Multiple Dante domains can co-exist within a network, but devices in one domain do not interact with devices in a different domain (even when they are controlled by a single DDM).

Domains are created, managed and deleted using the DDM user interface, by a user with administrator privileges (see Enrolling Devices in Domains). Once a domain has been created, you can add (enroll) and remove Dante devices, add and remove domain users, and tightly control the permissions for each user in the domain. A single DDM can administer multiple domains.

Dante devices store information locally about the domain into which they have been enrolled - so when they are power-cycled, they remember their domain and automatically reconnect to the DDM server.

Dante devices can only enroll in one domain at a time. Users however can be given access permissions for multiple domains. The top-level DDM administrator has visibility and control over all configured domains in the DDM instance. 'Domain Administrator' users, who manage individual domains, can also be created.

Security

DDM features a user administration layer that supports the creation and authentication of DDM users, and allows those users to be added to and removed from domains.

When a DDM user has been added to a domain, they are able to view and (optionally) control the Dante devices that are enrolled in that domain. An unidentified network user - for example, someone who is running Dante Controller on the same Dante network, but has not been added to DDM as a user - is not able to view or control any Dante devices that are enrolled in a Dante domain.

DDM users must log into Dante Controller using their DDM credentials before they can access and control Dante devices in a configured domain. For users that have permissions for multiple domains, Dante Controller allows the selection of individual domains for viewing. Only one domain can be viewed at a time.

Users that have not logged in can only access devices that are not enrolled in a configured DDM domain. Those devices are referred to as being in the ‘unmanaged’ domain. Logged-in DDM users can also access those devices, by selecting the unmanaged domain in Dante Controller.

Users can be assigned different roles for different domains. The site administrator has full control over all domains and users on the DDM instance.

DDM supports HTTPS for the connection between the DDM user interface and the server.

Network Monitoring

DDM 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 and for detailed event auditing.

Information available includes domain statistics, clocking alerts, security alerts, and device firmware notifications.

All users are able to customize their DDM dashboard.

DDM also supports SNMPv2c for integration with a network monitoring system.

Discovery

For networks that span subnets, DNS can be used to enable Dante devices to discover the DDM server automatically, or you can manually provide DDM with IP addresses for your Dante devices.

For networks that reside on only one subnet, Dante devices can use mDNS for automatic server discovery.

System Requirements

DDM is provided as an ISO for installation on virtualization platforms or bare-metal Linux machines.

The licensing model for DDM includes three editions: Silver, Gold, and Platinum.

Each edition supports a different number of devices and domains - bare-metal machines and hypervisors must provide sufficient system resources based on the product edition.

- For the Silver and Gold editions, DDM requires a CPU with a minimum of 2 cores, and 4GB of RAM.
- For the Platinum edition, DDM requires a CPU with a minimum of 2 cores, and 8GB of RAM. For systems that include more than 200 devices, 16GB of RAM is recommended.

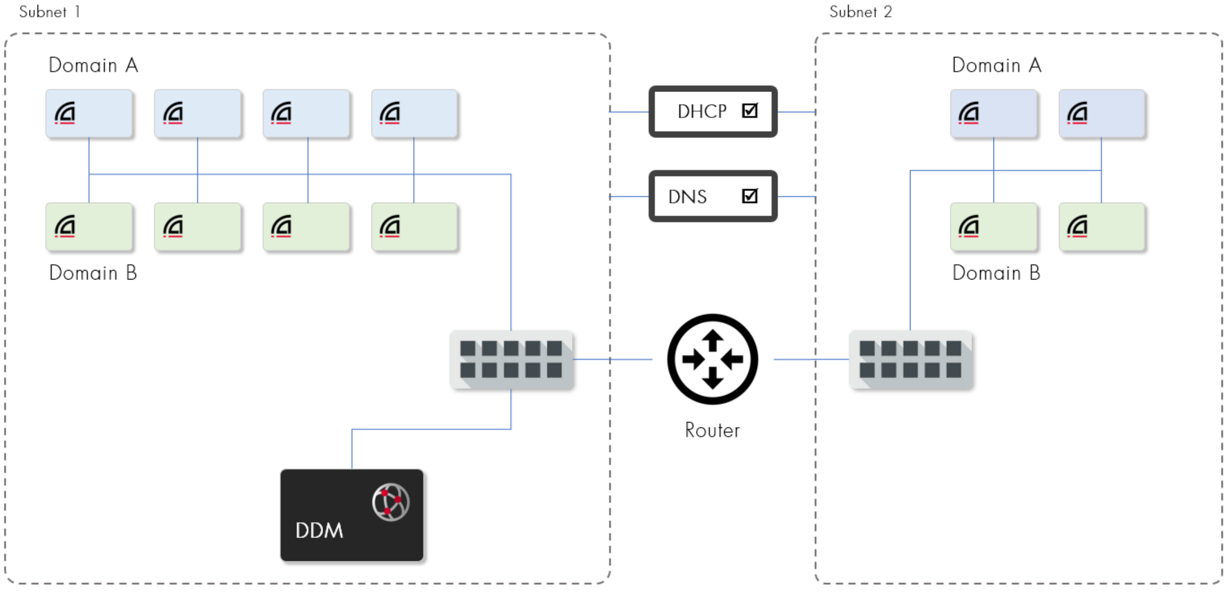
The physical host machine on which a hypervisor is installed must also meet the above specifications (with additional capacity for any other applications).

Device Administration

Bootstrapping Dante Devices and Controllers

Multiple Subnets

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.



DISCOVERY OPTIONS FOR MULTI-SUBNET SYSTEMS

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

Setting up DHCP

A DHCP server provides IP addresses and other bootstrap information for devices in a network. Many routers and switches come with DHCP functionality built in. Refer to the manual for your router, switch or DHCP server for configuration details.

Specify the DNS domain name for the DDM as the first entry in the domain-search option. This is because Dante devices will only use the first entry in this list for locating not fully qualified domain names. The DHCP option for domain-search is as follows:

```
* option domain-search
"domain.name",
"other.domain.name.1",
"other.domain.name2";
```

Here is an example domain-search for a DDM in the engineering department:

```
* option domain-search
```

```
    "eng.example.com",
    "sales.example.com",
    "hr.example.com";
```

Setting up DNS

Devices and controllers use DNS-SD (DNS service discovery) to find the DDM. Each DNS-SD entry consists of an SRV record describing how to connect to the DDM and a TXT record with additional information (empty in this case).

Note that DNS domain names and Dante domain names are different, and need not be related. Names of Dante domains are not added to the DNS.

Customizable Fields

The following fields are customizable to your environment.

- Domain: Replace the string `my.domain.example.com` with your local domain
- DDM: Replace the string `my_ddm.my.domain.example.com` with the name of the device hosting your DDM
- TTL: The system default TTL is usually satisfactory

Required Fields

All other fields must be as specified below,

Controller Record

Record Name

Instance	Service	Domain
`default.`	`_dante-ddm-c._tcp`	`my.domain.example.com`

- `default._dante-ddm-c._tcp.my.domain.example.com`

SRV Record

- Weight, priority: 0
- Port: NNNN
- Target: `my_ddm.my.domain.example.com`

TXT Record

- Empty

Device Record

Record Name

Instance	Service	Domain
`default.`	`_dante-ddm-d._udp`	`my.domain.example.com`

- `default._dante-ddm-d._udp.my.domain.example.com`

SRV Record

- Weight, priority: 0
- Port: NNNN
- Target: `my_ddm.my.domain.example.com`

TXT Record

- Empty

DNS SRV Record Examples

The following example is for Dante **controllers**, using the domain name eng.example.com:

- `default._dante-ddm-c._tcp.eng.example.com. 3600 IN SRV 0 0 8443 ddm.eng.example.com`
- `default._dante-ddm-c._tcp.eng.example.com. 3600 IN TXT ""`

The following example is for Dante **devices**, using the domain name eng.example.com:

- `default._dante-ddm-d._udp.eng.example.com. 3600 IN SRV 0 0 8000 ddm.eng.example.com`
- `default._dante-ddm-d._udp.eng.example.com. 3600 IN TXT ""`

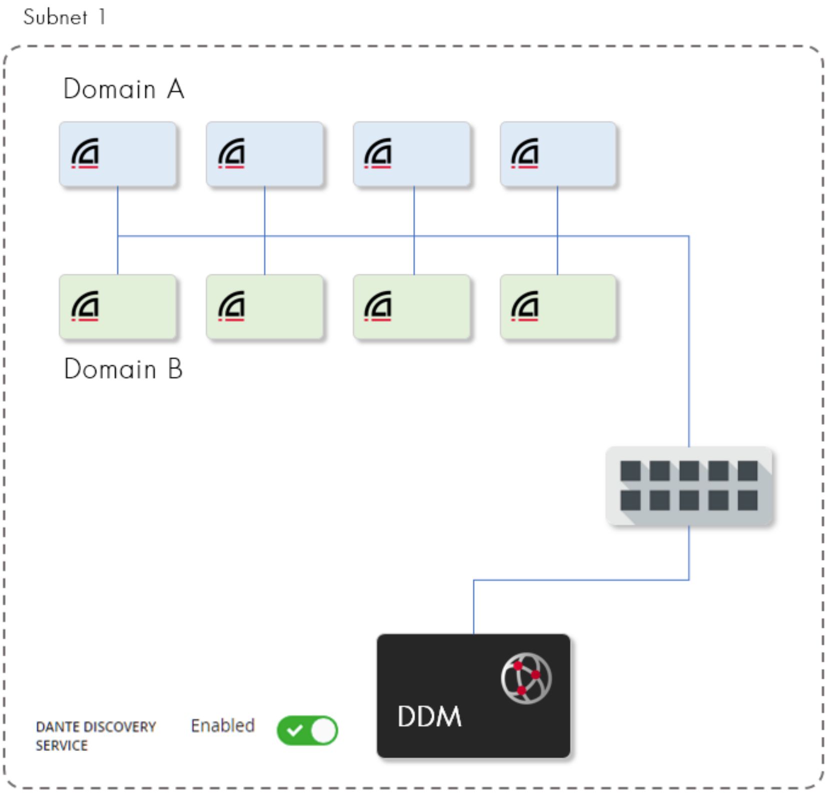
The domain name in the SRV and TXT headers must match the search domain provided to clients by DHCP. Clients are not required to be in the same DNS domain as the DDM, but each DNS domain provided to clients must have DNS-SD records that point to the DDM.

In addition to adding the DDM domain name to DNS, you should obtain a domain validation certificate for the hostname of your DDM. This certificate verifies the identity of your DDM to a web browser accessing the DDM administrative interface as well as Dante controllers connecting to the DDM.

- Adding SRV Records in Windows Server

Single Subnet with mDNS

For networks that reside on a single subnet, mDNS-based discovery can be used to bootstrap devices and controllers. The mDNS discovery feature (Dante Discovery Service) is on by default, and does not need to be activated or configured. All discovered devices will be displayed in the ‘Unmanaged Devices’ domain in the Devices page.



DISCOVERY OPTIONS FOR SINGLE-SUBNET SYSTEMS

- Link-local addressing + Dante Discovery Service (mDNS) (recommended)
- Static addressing + manual enrollment
- DHCP is convenient, but not required

For networks that include multiple DDM instances on the same IP subnet, you can disable the Dante Discovery Service in the Network & Security Settings.

Using Static IP Addresses

Networks that span multiple subnets but do not include a DHCP or DNS server can use static IP addresses. The Linux host running the DDM can be directly configured with a static IP address. Dante devices can be configured with static IP addresses using a Dante Controller on the same subnet as the device.

Routers will also need to be configured with appropriate IP addresses on each subnet.

To enroll devices, enter a list of IP addresses for the Dante devices you wish to enroll into the DDM manual configuration screen. The DDM will push static enrollment and discovery information to each device.

You can either enter individual IP addresses manually, or upload a CSV file containing a list of IP addresses and target domains.

Enrolling Devices in Domains

Devices can be enrolled in only one domain at a time.

When a device is enrolled in a domain, it can be viewed and configured in Dante Controller only by DDM users that are members of the domain, and it can support label-based routing across subnets.

The device's domain credentials are stored locally on the device (as well as in the DDM database) and it will automatically rejoin its domain if it is rebooted.

Note: Sample rate pull-up/down is not supported for enrolled devices - this setting will be automatically cleared when a device is enrolled.

Note: When enrolling an unmanaged device with AES67 enabled into a 'default' (non-AES67) domain, AES67 mode will be automatically disabled for the device. See AES67 and SMPTE Domains for more information.

Enrolling Discovered (Unmanaged) Devices

DDM places all automatically-discovered devices that support DDM in the 'Unmanaged' pseudo-domain.

To view Unmanaged devices, go to **Devices** in the main menu and expand the Unmanaged domain.

To enroll unmanaged devices:

1. Click the device name(s) for the device(s) you want to enroll. Use Ctrl + click or Shift + click to select multiple devices.
2. If only one device is selected, click the **Enroll** button in the 'Domain Enrollment' section of the Device Details panel. If multiple devices are selected, click **Enroll Devices** in the right-hand panel.
3. In the 'Enroll Devices' panel, select the target domain.
4. Click **Enroll**.

You can also drag and drop devices into domains (including into the Unmanaged domain, which unenrolls the devices).

Note: For networks with very large numbers of devices, you can improve user interface performance by disabling the automatic collapsing of domain nodes when using drag & drop to enroll devices. See Personalization Settings for more information.

Enrolling Undiscovered Devices

Networks that span multiple subnets but do not use a DNS can directly enroll devices by IP address.

Enrollment does not assign IP addresses to devices. This must be done using static IP address assignment or DHCP.

To enroll devices that have not been discovered by DDM:

1. Go to **Devices** in the main menu.
2. Click **Enroll Devices**.

3. Click **Enroll By IP Address**.
4. To enter IP addresses manually:
    a. Optionally change the domain into which you want to enroll the devices.
    b. Select the 'Enter manually' radio button.
    c. Paste / type in the relevant IP addresses (one per line).
    d. Click **Enroll**.
5. To upload a CSV file of IP addresses:
    a. Prepare a CVS file containing only a comma-separated list of IP addresses.
    b. Optionally change the domain into which you want to enroll the devices.
    c. Select the 'Import from CSV file' radio button.
    d. Drag and drop the CSV file into the drop zone, or click **browse** and navigate to the CVS file.
    e. Click **Enroll**.

Unenrolling Devices

To unenroll devices that are already in a domain:

1. Go to **Devices** in the main menu.
2. Expand the relevant domain.
3. Click the device name(s) for the device(s) you want to unenroll.
4. Click **Unenroll** in the Domain Enrollment panel.

You can also:

- Drag and drop enrolled devices into the Unmanaged domain to unenroll them
- Unenroll devices from the Domains page

Resetting Devices Using Dante Controller

If you have removed a device from the network without first unenrolling it, you need to clear its domain credentials before it can be deployed elsewhere. This can be done using Dante Controller. The device must first be isolated from the Dante network, either physically or by using a VLAN.

1. Isolate the device from the rest of the Dante network.
2. Disconnect and reconnect the device.
3. Wait for at least 2 minutes.
4. Open the Device View for the device.
5. From the Device menu, select **Clear Domain Credentials**.

How to Isolate a Device from the Rest of the Dante Network

There are 3 ways to isolate a device from the rest of the network.

Option 1: Remove all other Dante devices from the Dante network

You can isolate a device by physically disconnecting all other Dante devices from the network switch, or by completely powering down all other devices, leaving on the network only the affected device and the computer running Dante Controller.

Option 2: Connect your Dante Controller computer directly to the device

Physically remove the device from the main Dante network switch, and either connect it directly to your Dante Controller computer (using a normal Ethernet cable), or connect the device and your computer to a separate network switch (to which there are no other Dante devices connected).

Option 3: Use a VLAN

Set up a Virtual Local Area Network on which there are only the locked device, and the Dante Controller computer.

Clear Configuration

When you enroll or unenroll a device, you can choose to also clear the configuration on the device.

This will reset the following configuration settings to the device defaults:

- Device Name
- Channel labels
- Latency
- Sample rate
- Encoding
- Subscriptions

Note: Clear Config is not supported for legacy devices.

Device Enrollment Status

The Device Enrollment Status page is displayed when two or more devices are enrolled or unenrolled, or if there is a condition preventing the operation for any devices.

The page displays the enrollment status for the devices and any conditions preventing the operation.

Cannot Enroll

If an attempt was made to enroll any devices that cannot be enrolled (for example because they are locked, or on a legacy firmware version), a 'Cannot Enroll' menu item is displayed at the bottom of the device list on the Devices page.

The Cannot Enroll page displays all relevant device names, plus the reason that they cannot be enrolled.

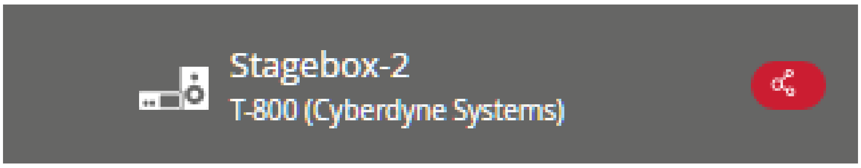
Devices that cannot be enrolled remain in the Unmanaged domain, and can exchange audio with other unmanaged devices as per normal Dante operation.

Forgetting Devices

Once a device has been enrolled in a domain, DDM will continue to list it as an enrolled device until it is unenrolled, even if the device is offline or otherwise unreachable.

This may result in a device presenting as an enrolled device when it shouldn't be - for example, if the device was physically removed from the network without first being unenrolled from the domain.

Offline / unreachable devices are indicated by a red connectivity icon next to the device name:



In cases where a device is presenting as an offline enrolled device but it has actually been removed from the network, you can 'forget' the device, which removes it from the enrolled devices list.

To forget a device:

1. Open the Device Details for the device.
2. In the Domain Enrollment section, click 'Forget'.

In order for the device to be discoverable in another DDM network, you must first clear its domain credentials using Dante Controller (see Resetting Devices Using Dante Controller above).

User Administration

About User Roles

User roles determine the privileges that the user has for the domain(s) of which they are a member. Users can be assigned one of four roles, with varying levels of permissions: Site Administrator, Domain Administrator, Operator, or Guest.

To view the privileges carried by each user role, go to **Roles** in the main menu and select a role.

Site Administrator

Site administrators can create and manage domains and assign roles to users. Only Site Administrators can change DDM configuration.

The Site Administrator role applies across all domains managed by a DDM. Other roles are assigned to users (by a Site Administrator) on a per-domain basis. Users can have different roles for each domain.

Domain Administrator

Domain administrators can administer devices within a domain, including enrolling and upgrading devices, and routing audio within the domain.

Operator

Operators can use Dante Controller to configure audio routing on devices within a domain. They can also view domain configuration in DDM.

Guest

Guests can use Dante Controller to view audio routing on devices within a domain, but not change it. They can also view domain configuration in DDM.

Roles and Domains

Domain Roles

The Site Administrator can specifically assign a user a particular role within a domain. The role can be Domain Administrator, User, Guest, or None. A user with a role of None for a domain cannot even view that domain in Dante Controller or DDM.

Default Roles

Each user has a default role. This role applies in all domains for which that user's role has not been explicitly specified.

For example, a user with a default role of Domain Administrator becomes a Domain Administrator in all domains. The Site Administrator could then set that user's role to Guest for one specific domain. If a new domain is created, the user would automatically have Domain Administrator permissions for the new domain.

Note: A Site Administrator may also assign the Site Administrator role to a user account in addition to the other roles. Domain-specific privileges are not applicable to user accounts with a default role of Site Administrator.

New users are created with a default role of None unless otherwise specified.

Adding Users

Use the Users page to create new users.

Note: Only site administrators can add new users.

Once a user has been added, you can assign the user a role in one or many domains.

Users require a username and a password, and can optionally be associated with an email address for password reset notifications. They can also be assigned a default role.

To add a new user:

1. Go to **Users** in the main menu.
2. Click **Add User**.
3. Enter the display name, username and password. The display name is the name that is displayed in DDM, the username is the string they will use to log in to DDM and Dante Controller. If no display name is provided, their username will be displayed instead.
4. Provide an email address (optional).
5. Assign a default role (optional).
6. Add a Domain Role (optional):
   1. Select the domain for which you want modify the user's role.
   2. Select the domain role for the user.
   3. Click **Add Domain Role** to make more domain assignments.
7. Click **Add**.

Deactivating Users

Use the Users page to deactivate existing users.

Inactive users are unable to log in to the Dante Domain Manager web interface, or connect to a domain via Dante Controller.

Note: Only site administrators can deactivate users.

To deactivate a user:

1. Go to **Users** in the main menu.
2. Click **Deactivate User**.

To reactivate a deactivated user, open the User Details for the user and click **Reactivate User**.

Changing Domain Roles for a User

You can modify a user’s role within a domain when you create the user, or after creating the user.

See Adding Users for information about assigning domain roles to users when the users are created.

To assign domain roles to a user after the user has been created:

1. Go to **Users** in the main menu.
2. Select the user.
3. Click **Edit**.
4. Click Add Domain Role.
5. Select the target domain.
6. Select the domain role for the user.
7. Optionally click **Add Domain Role** again to make further domain assignments.
8. Click **Add**.

Domain Administration

Creating Domains

Use the Domains page to create new domains.

Note: Only site administrators can create domains.

To add a new domain:

1. Go to **Domains** in the main menu.
2. Click **Add Domain**.
3. Enter a name for the domain, and click **OK**.

Once a domain has been added, you can:

- Enroll devices in the domain
- Change domain roles for users

The number of domains your DDM installation can support is determined by your DDM license type.

Managing Domains

To manage domains, go to **Domains** in the main menu.

On the Domains page you can:

- Add new domains
- Delete domains
  When a domain is deleted, all devices that were enrolled in the domain become unenrolled, and revert back to the unmanaged domain.
- Enroll devices in domains
- Unenroll devices from domains
- Configure clocking settings for domains
- Search for domains by name

Note: Only site administrators can add and delete domains.

Viewing Domains in Dante Controller

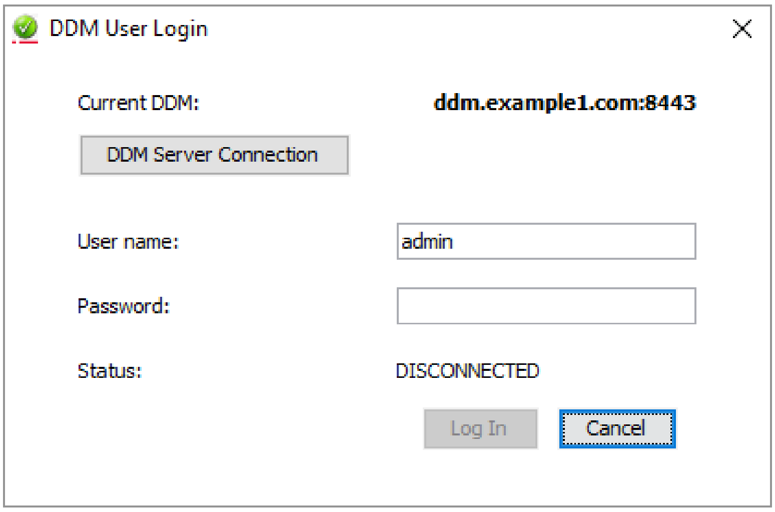
To view enrolled devices in Dante Controller, the user must connect to the DDM server using their configured DDM credentials, and then select the appropriate domain for viewing.

Connecting to a DDM Server

To connect to a DDM server:

1. In the Dante Controller toolbar, click the **Domains** button:

   The DDM User Login dialog is displayed.



DDM User Login

Current DDM: **ddm.example1.com:8443**

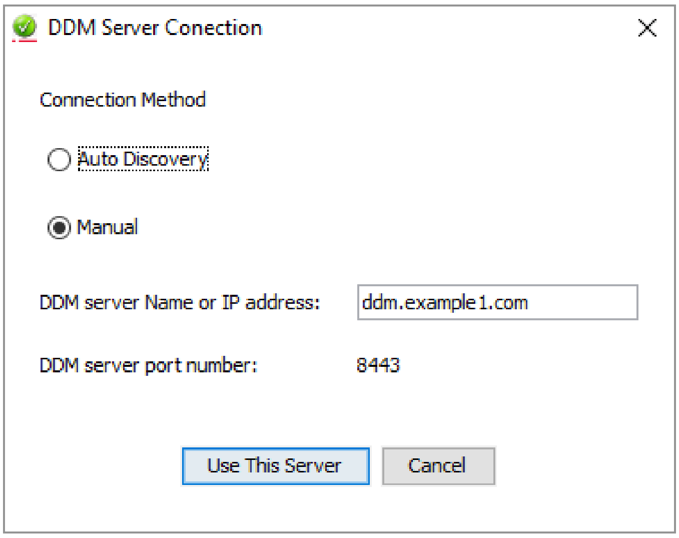
User name: admin

Password:

Status: DISCONNECTED

2. Click **DDM Server Connection**.

   The DDM Server Connection dialog is displayed:



DDM Server Conection

Connection Method

○ Auto Discovery

● Manual

DDM server Name or IP address: ddm.example1.com

DDM server port number: 8443

3. In the DDM Server Connection dialog, either:
   - Select 'Auto Discovery' to search for a DDM server automatically*, or:

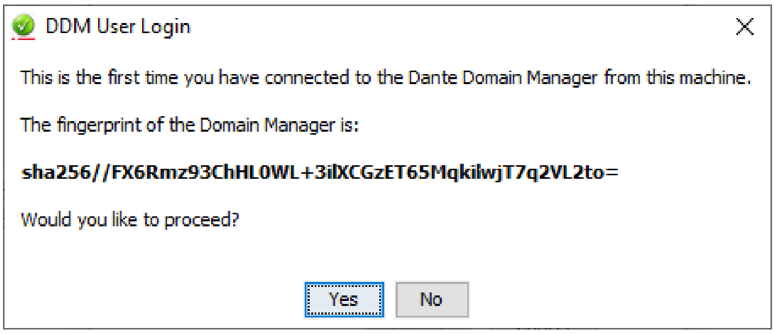
   a. Select 'Manual' to provide a specific IP address or FQDN (requires DNS) and port number.

   b. Enter the DDM server IP address or FQDN.
4. Click **Use This Server**.
5. In the DDM User Login dialog, enter your username and password.
6. Click **Log In**.

* Auto Discovery requires DNS if Dante Controller and the DDM server are in different IP subnets.

First-time Connections

The first time an installation of Dante Controller connects to a DDM server, a pop-up dialog is displayed:


DDM User Login

This is the first time you have connected to the Dante Domain Manager from this machine.

The fingerprint of the Domain Manager is:

sha256//FX6Rmz93ChHL0WL+3ilXCGzET65MqkilwjT7q2VL2to=

Would you like to proceed?

Click **Yes** to connect to the DDM server, or **No** to cancel the connection.

This security mechanism enables you to verify that the DDM server at the specified server name / IP address is the server to which you actually intended to connect.

If the underlying DDM server at a previously used server name / IP address changes, you will see a warning pop-up, so you can cancel the connection if required.

The fingerprint is a unique ID for the DDM server, and is saved locally to your computer.

You can view known fingerprints in the ddm_hosts file at:

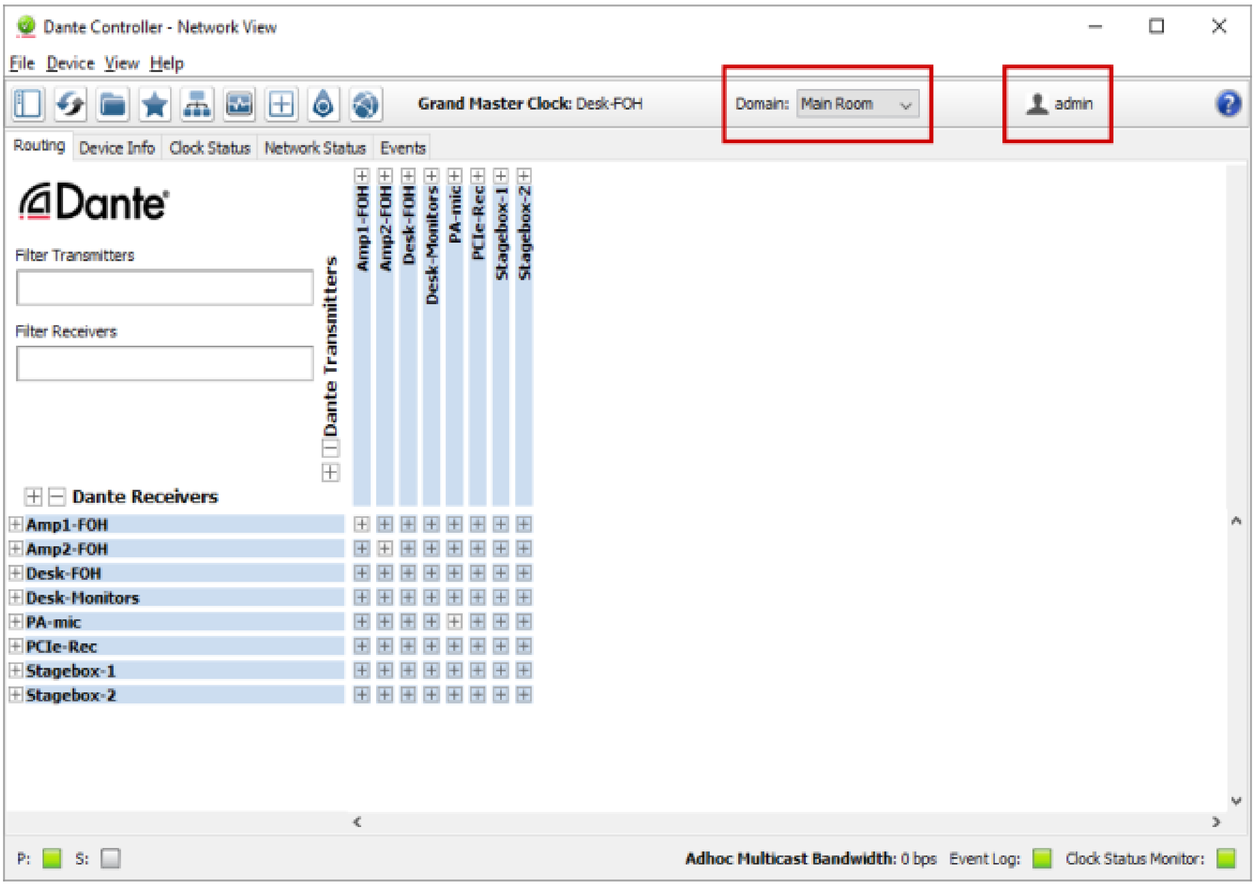
- Windows: C:\Users\<user name>\AppData\Local\Dante Controller
- macOS: ~/Library/Application Support/Dante Controller

You can also view the fingerprint for a DDM server instance in the Network & Security settings of the DDM user interface.

Viewing a Domain

To select a domain for viewing, select the required domain from the Domain drop-down menu in the Dante Controller main toolbar.

The domains and devices you are able to view and configure are determined by your DDM user account privileges.



The currently logged in user is displayed next to the Domain drop-down menu.

Note: When connected to the <unmanaged> domain, Dante Controller will only display devices in the local subnet.

Settings

Updates and System Information Settings

The Updates and System Information page allows you to:

- Check online for updates to the DDM software
- Update your DDM installation, if an update is available
- Roll back to a previous DDM version
- Save the current system configuration
- Save system logs

System Configuration

Saves the current system configuration to your device, which can be used to restore a new DDM installation to the saved state.

When you save a system configuration, the following information is saved:

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

Note: Saved system configurations can only be restored during the DDM installation process - you cannot restore a saved configuration once DDM has been fully installed.

Important: If prior to restoring a previously-saved system configuration you make domain changes in a fresh DDM installation, you may not be able to successfully restore the saved configuration. This is because domain credentials are saved locally on Dante devices - if a device has credentials for a new domain which doesn't exist in the restored configuration, it will not be able to reconnect to the old domain.

About System Configuration File Formats

DDM supports system configuration files with extensions .tgz or .tar.gz.

System configuration files are saved by default as .tgz files.

However, if you are using Safari on Mac, your browser may automatically extract the downloaded file to a .tar file, which cannot be uploaded to restore a DDM configuration.

To prevent this from happening, you can disable the 'Open “safe” files after downloading' option in Safari (choose Safari > Preferences, then click General).

- More information: https://support.apple.com/en-au/guide/safari/ibrw1072/mac
- If you have already downloaded a system configuration file and it has been extracted by your browser to a .tar file, you can re-zip it to a .tar.gz file using the 'gzip' command in Terminal.

More information: https://www.gnu.org/software/gzip/manual/gzip.html

System Logs

Saves the DDM system logs to your device. You may be asked by Audinate technical support to provide system logs for troubleshooting.

Network & Security Settings

Security

Upload TLS Certificate

Uploads the files required to implement HTTPS for the connection from the user interface to the DDM server.

The file must be a zip file containing:

1. A private key - [yourdomain].key
2. A domain certificate - [yourdomain].crt
3. One or more intermediate certificates - intermediate.crt

Note: The web proxy used by the Dante Domain Manager is Nginx. Some certificate authorities may provide a single composite certificate containing both the domain certificate and intermediate certificates suitable for Nginx. If that is the case, you should use the composite certificate instead of individual certificates.

Controller Fingerprint

The Controller Fingerprint is a unique ID for the DDM instance that is presented to Dante Controller users when they first connect to DDM.

Dante Controller users can confirm that they are connected to the intended DDM instance by manually verifying that the fingerprint strings displayed in Dante Controller and DDM are identical.

Network

Dante Interface

If you have multiple physical network interfaces connected to different Dante networks, you can use the Dante Interface menu to switch between them.

FQDN

Provide a fully qualified domain name for the DDM instance. The FQDN must be valid for the network in which DDM resides. Click **Suggest** to auto-populate the FQDN, based on the current DNS configuration if applicable.

Note: It may be necessary to change the FQDN if the DDM instance is moved to another network.

Advertise DDM for Discovery Using mDNS

For networks that reside on a single IP subnet and do not include a DNS server, this feature enables automatic discovery of DDM by Dante devices (using mDNS). If you have multiple DDM instances running on the same IP subnet, you should disable the service, and use manual (IP address) device enrollment.

Run Diagnostics

The Diagnostics function performs a set of high-level tests to establish the status of some basic network configuration parameters relevant to the DDM server.

Note: Requires the site administrator role.

Legacy Devices

Enables legacy (pre-v4.0 firmware) products to exchange audio with enrolled devices on the same IP subnet.

- See Legacy Devices for more information.

Note: Legacy Interop must also be enabled at domain level in the Domain Details page.

Browser Login Expiry

Specify the time after which idle users will be automatically logged out of the DDM web interface, and will have to log in again.

Supported values are weeks (w), days (d), hours (h), and minutes (m), for example: 3w 4d 12h 30m

Network Diagnostic Results

The Network Diagnostic Results panel displays the following information:

Basic Configuration

- **IP address**

  The IP address of the DDM server
- **Subnet mask**

  The subnet mask for the DDM server
- **Address acquired by**

  The method by which the DDM server acquired its IP address
- **Search path(s)**

  All search paths configured for the DDM server

Test Results

The DDM can reach the default gateway

The default gateway is typically configured as part of static IP address settings (in the appliance menu), or provided by DHCP.

- **Success**

  The DDM was able to ping the default gateway

- **Fail**

  A default gateway is configured, but the DDM was unable to ping it
- **Not configured***

  No default gateway is configured

The DDM can reach the DNS server

- **Success**

  The DDM was able to ping the DNS server
- **Fail**

  A DNS server is configured, but the DDM was unable to ping it
- **Not configured***

  No DNS server is configured

The DDM can access the internet

- **Success**

  The DDM was able to ping google.com
- **Fail**

  A DNS server is configured, but the DDM was unable to ping google.com
- **Cannot test***

  No DNS server is configured

DDM discovery records exist in the DNS server

- **Success**

  The DDM was able to successfully resolve DNS records for both devices and controllers to the correct IP address and port for this DDM
- **Fail**

  A DNS server is configured, but the DDM was unable to resolve either device or controller records to the correct IP address and port for this DDM
- **Partial**
  - 'A record exists for discovery by devices'
    - Pass: The DDM was able to resolve the device DNS record
    - Fail: The DDM was unable to resolve the device DNS record
  - 'The discovery record for devices resolves to this DDM'
    - Pass: The device DNS record resolves to the correct IP address and port for this DDM
    - Fail: The device DNS record does not resolve to the correct IP address and port for this DDM
  - 'A record exists for discovery by controllers'
    - Pass: The DDM was able to resolve the controller DNS record
    - Fail: The DDM was unable to resolve the controller DNS record
  - 'The discovery record for controllers resolves to this DDM'
    - Pass: The controller DNS record resolves to the correct IP address and port for this DDM

  - Fail: The controller DNS record does not resolve to the correct IP address and port for this DDM

- **Cannot test***

  No DNS server is configured

** This is the expected result for Link-local networks.*

License Management Settings

The License Management page displays your current DDM license details and feature expiry, and allows you to activate and deactivate DDM licenses.

Click **Refresh** to update your license status from the Audinate license server.

It also displays information about your current DDM version.

Personalization Settings

Unenroll Confirmation

When enabled, unenroll actions will require a confirmation step. Use this setting to reduce the likelihood of accidental unenrollment.

Collapse on Dragging

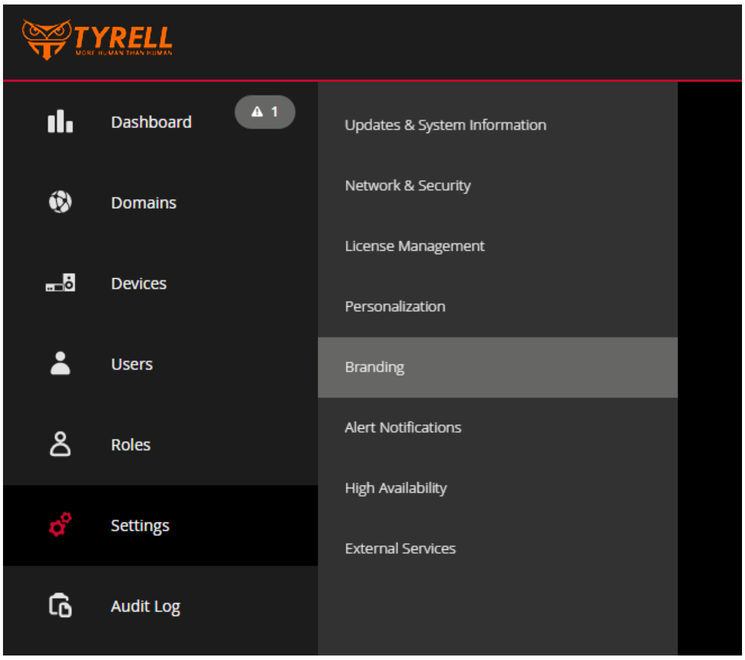
When enabled, domain nodes will automatically collapse when using drag & drop to enroll devices. Disable this feature to improve user interface performance for networks with very large numbers of devices.

Branding Settings

To enable the Branding settings, select 'Branding Mode' from the Administration menu in the VM.

Customize Logo

Use the Customize Logo panel to provide a custom logo to be displayed in place of the Dante Domain Manager logo at the top left of the DDM web interface.

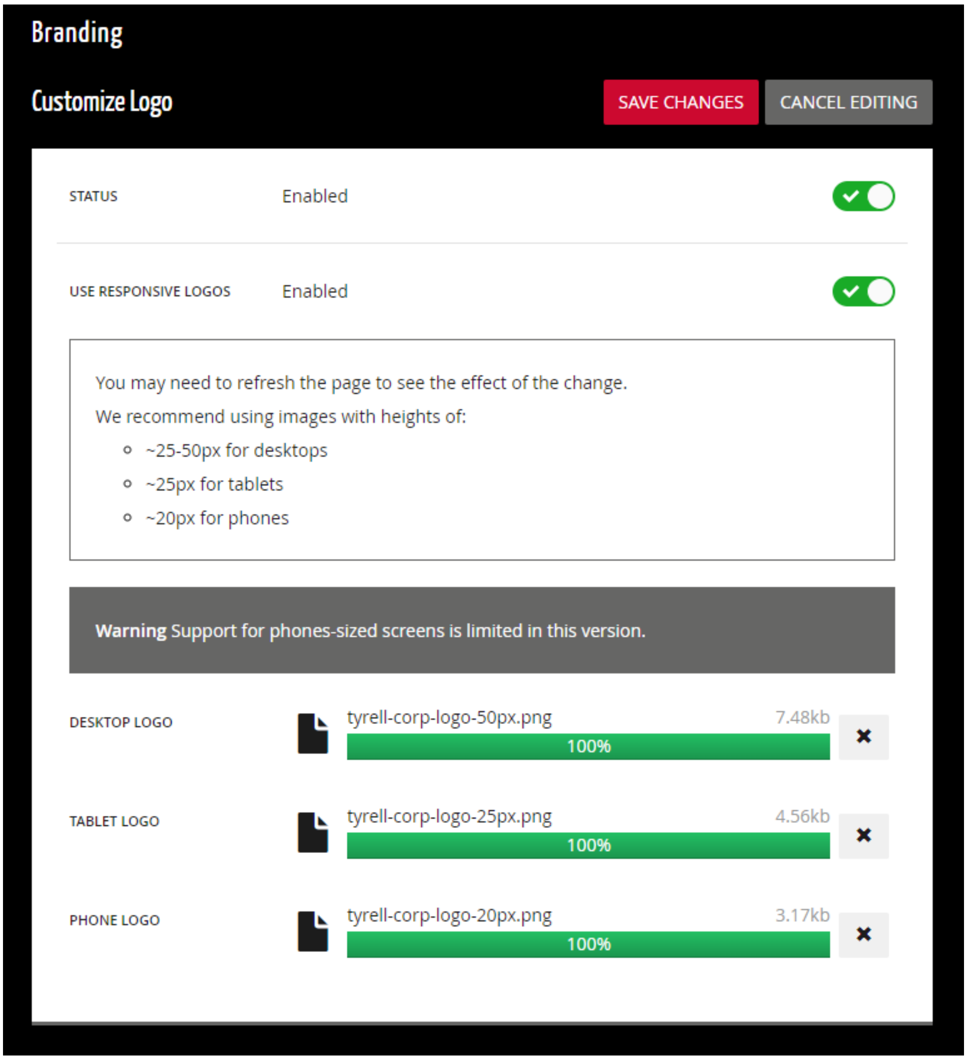


Status

Set the 'Status' to **Enable** to display the custom logo in DDM.

Use Responsive Logos

Enable 'Use Responsive Logos' to provide different size logos for desktop, tablet and mobile phone display.



Branding

Customize Logo

STATUS Enabled

USE RESPONSIVE LOGOS Enabled

You may need to refresh the page to see the effect of the change.

We recommend using images with heights of:

- ~25-50px for desktops
- ~25px for tablets
- ~20px for phones

Warning Support for phones-sized screens is limited in this version.

DESKTOP LOGO tyrell-corp-logo-50px.png 7.48kb 100%

TABLET LOGO tyrell-corp-logo-25px.png 4.56kb 100%

PHONE LOGO tyrell-corp-logo-20px.png 3.17kb 100%

When you have selected your logo(s), click **Save Changes** and refresh the DDM UI to see the changes.

When you are happy with the changes, use the Administration menu in the VM to hide the Branding settings.

To restore the Dante Domain Manager logo, set 'Status' to **Disabled** in the Branding settings.

Alert Notification Settings

Email Notifications

Use this panel to enable and configure Email alert notifications.

Note: Requires that Email is configured and enabled in the External Services settings.

Status

Click the toggle switch to enable / disable Email alert notifications.

Email Address

Provide the email address to which alerts will be sent.

Alert Categories

Use the alert categories tabs to select / deselect the alerts that will be sent to the configured Email address.

High Availability Settings

About High Availability

High Availability is a redundancy feature included with the Dante Domain Manager (DDM) Platinum license. This feature enables a secondary or backup server (the 'HA Only node') to take over if the primary server (the 'Standalone node') goes down or goes offline.

In normal operation, the Standalone node's state is 'active', and the HA Only node's state is 'auxiliary'.

All configuration data on the active server is dynamically replicated to the auxiliary server. If the auxiliary server detects that the active server is offline, it will take over as the active DDM server and all Dante clients (devices and controllers) will connect to it.

High Availability (HA) allows a DDM system to continue normal operation in the case of a server failure. In a DDM system with or without HA, audio is never disrupted if a server goes down. The benefit of HA is that control connections - i.e. being able to log into Dante Controller and make changes to devices and routes - will resume after a brief disruption, rather than when the server is restored. High Availability requires additional server and network resources.

Users logged into a DDM server in Dante Controller will have to log in again in the event of an active server failure. Device configuration via embedded controllers and Host CPU interfaces may not be possible while the system is in the process of failing over.

Note: Dante Domain Manger High Availability is not related to Dante device redundancy and setting up a Dante redundant (secondary) network.

How Does it Work?

The DDM high availability implementation requires 3 servers: the Standalone node, the HA Only node, and the arbiter.

The arbiter serves as a tiebreaker in the event the network becomes partitioned - in which case the server which is still in communication with the arbiter takes over as the active server.

If at any point there are not at least two servers visible to each other, the system will switch to 'read-only' mode: existing audio subscriptions will be maintained, but configuration changes via the DDM user interface and Dante Controller will be disabled.

High Availability utilizes a virtual IP address. Devices and controllers connect to this virtual address instead of the physical address of the individual servers. The virtual IP address is configured as an additional address on the network interface of the currently active server. In the event the active server becomes disconnected, it gives up this address. The auxiliary server then takes over the virtual address and configures it on its own network interface.

Server Requirements

The Standalone and HA Only nodes should ideally be specified identically, in line with the standard DDM system requirements. If the servers cannot be specified identically, you may encounter performance degradation in the event of a failover.

Standalone and HA Only Server Minimum Requirements:

- A CPU with a minimum of 2 cores (for VMs spec 2 CPUs)
- 8GB of RAM.
  - For systems that include more than 200 devices, 16GB of RAM is recommended.
- At least 20 GB hard drive space

The arbiter server must be reliable, but does not replicate the DDM database, and therefore does not need to match the performance of the Standalone and HA Only nodes.

Arbiter Server Minimum Requirements:

- A CPU with a minimum of 2 cores (for VMs spec 2 CPUs)
- 4GB of RAM
- At least 20 GB hard drive space

IP Addresses and Hostnames

Each server must be specified with a unique IP address and hostname. All server IP addresses must be in the same IP subnet. Unique hostnames, if required, must be set before enabling HA Mode.

Additionally, a virtual IP address will be required for the cluster. The virtual IP address must be in the same subnet as the DDM servers, currently unused, and not allocated (or enabled for allocation) by DHCP.

A DNS ‘A’ record can be configured as an alias for the Virtual IP address. If present, the ‘A’ record should eventually match the FQDN for the DDM installation, but can be configured to match after forming the cluster in the DDM ‘Network & Security’ settings page.

Network Time

To ensure accurate replication in the event of server clock drift, you can optionally provide the DDM server with access to an NTP server. NTP servers can be specified for the DDM server using the Administration Menu. If your network is not connected to the Internet, specifying an alternative NTP server is a requirement.

Device Discovery

Unicast DNS is strongly recommended for discovery in HA mode.

Dante Discovery Service (mDNS) is not supported in HA mode, and will be deactivated automatically when HA is enabled.

For unicast DNS, SRV records allow devices/controllers to discover the DDM Server Cluster. The SRV records in your DNS server should point to the cluster’s virtual IP address, or FQDN (if you are using a hostname for the virtual IP address).

Note: If you have previously enrolled devices into a different DDM server or a DDM server in Standalone mode, they may experience discovery issues. See 'Transitioning to HA mode from Standalone Mode'.

It is not recommended to use manual device enrollment by IP address with HA mode - but if it is unavoidable, the following should be considered:

- **The HA Cluster must be configured before enrolling any devices into a domain**. When you manually enroll a device by IP address into a domain, the DDM server sends a static reference to the device, based on the currently configured FQDN for the DDM. The static reference is the DDM server's IP address. If the devices are referencing the IP address of the standalone node (active) server rather than the Virtual IP address of the cluster when the server fails over to the HA Only node (auxiliary) server, all devices will be shown as offline and will not appear in Dante Controller.

Note: Additional precaution should be taken when manually enrolling devices by IP address with Dante firmware versions 4.0-4.2 as when a device is manually enrolled by IP, discovery will be permanently disabled in the device until the device has been reset and domain credentials cleared. This results in devices becoming undiscoverable if you wish to use DNS for discovery in the future. (This issue should be resolved in future Dante device firmware versions)

Licensing

Only one DDM License (Platinum) and product key are required to license (activate) the HA Cluster.

When configuring and activating the severs, you will need to enter the product key on the Standalone node and the HA Only node. Internet access is required to activate these servers. The Arbiter server does not need to be licensed.

Prior to installation and activating, it must be decided which server will be the Standalone node (typically the preferred active server). The other becomes the HA Only Node and inherits its license state dynamically from the Standalone node.

Important: If you experienced a failover to the HA Only node, it is important to make sure the Standalone node becomes the active server again when it is restored. If the HA Only node remains the active server for more than 30 days continuously, the license on the HA Only node will become deactivated. To avoid license deactivation when the Standalone node is restored, change it to the active Server. If the Standalone node is unrecoverable, you can make the HA Only node a Standalone node.

Setting Up and Configuring HA

Important: The HA Cluster should be set up and configured before enrolling devices into domains.

Installing and Activation

1. Begin by installing the DDM ISO file onto 3 virtual machines or bare metal servers.
2. Boot up your preferred active server, open the DDM web interface for this server and follow the prompts to install DDM as a 'Fresh Installation.' In the context of HA, this is the Standalone node. An Internet connection is required for activating the Standalone and HA Only nodes.
3. Configure a TLS certificate, if required (note that the TLS certificate will be shared by all nodes). The TLS certificate should contain the subject name for the FQDN for the virtual IP address.
4. Boot up your preferred auxiliary (backup) server.
5. Open the DDM web interface for this server.

6. On the ‘Installation & Configuration’ page, choose ‘High Availability Redundant Node’ and click **Next**.
7. Follow the prompts to complete the installation, using the same product key you used for the Standalone node. In the context of HA, this is an HA Only node.
8. Start the DDM appliance on your preferred arbiter server.
9. Open the DDM web interface for this server.
10. On the ‘Installation & Configuration’ page, choose ‘High Availability Arbiter’ and click **Next**.
11. Follow the prompts to complete the installation. You do not need a product key to install an arbiter node. This server becomes the Arbiter node.

Enabling HA Mode

1. On your Standalone node, navigate to Settings > High Availability.
2. In the ‘Node Status’ section, copy the Security Key.
3. In a new browser tab, navigate to the URL or IP address of the HA Only Node.
4. In the ‘Node Status’ section, click **Edit** and paste in the security key.
5. Repeat the two steps above for the Arbiter node.
6. Return to the browser tab for the Standalone node, and click the toggle switch to enable HA mode.
7. In the Cluster Settings, enter a virtual hostname or IP address. The virtual hostname and IP address of the cluster must be unique on the network, and in the same subnet as the DDM servers.
8. In the ‘Node 1’ field, enter the hostname or IP address of the Standalone node.
9. In the ‘Node 2’ field, enter the hostname or IP address of the HA Only node.
10. In the ‘Arbiter’ field, enter the hostname or IP address of the Arbiter node.
11. Click **Save Changes** to enable the cluster.

Note: While the cluster is active, you cannot use the DDM UI on the auxiliary and arbiter servers.

Changing the Active Server

To change the active server to auxiliary and the auxiliary server to active, in the High Availability settings for the cluster or active server, click **Change Active**.

Making the HA Only Node a Standalone Node / Active Server

If the original Standalone node goes offline and is unrecoverable and the HA Only node is now the active server, you can upgrade the HA Only node to a Standalone node.

To make an HA Only node Standalone, in the DDM UI navigate to Settings > High Availability and click **Make Standalone**.

The license for the new Standalone mode must then be deactivated and reactivated as a standalone license (requires Internet access). It is likely you will need to contact Audinate Support to reset the license, so you can activate the HA Only node as Standalone. Therefore, it is advisable to wait until you’ve been in contact with Audinate support to reset your license before transitioning to a Standalone Node (you can keep the HA Only node as the Active server in HA Mode for 30 days before the license becomes deactivated.)

Transitioning To / From HA

Disbanding the HA Cluster

To disband the HA cluster, on the active server, go to Settings > High Availability and click **Disband**.

Transitioning from HA Mode to Standalone Mode

Because devices remember the IP address or hostname of the DDM server, the best way to avoid device discovery issues when transitioning from a system set up in HA Mode to Standalone mode is to give the Standalone node the IP address and hostname of the former cluster.

Transitioning to HA Mode from Standalone Mode

The best way to avoid device discovery issues when transitioning from a system already setup in Standalone mode to HA mode is to give the Standalone node a new IP address and hostname, and give the cluster the former Standalone node's IP address/hostname.

Resolving Issues with Device Discovery

If a device that has previously been enrolled in a domain is not discovering the DDM, you can reset the device and clear the domain credentials using Dante Controller.

1. Isolate the device from the rest of the Dante network and the DDM server.
2. Disconnect and reconnect the device.
3. When the device appears in Dante Controller, double-click it to open the Device View for the device.
4. From the Device menu, select **Clear Domain Credentials**.
5. In the popup window, click the **Clear Config** button.

Updating DDM in HA Mode

It is advisable to make a backup of the DDM system configuration before updating.

To update DDM in HA mode:

1. Disband the HA cluster.
2. Update each server independently.
3. Recreate the cluster.

Note: While the cluster is disbanded, devices will present as offline (because the virtual IP address/hostname is temporarily not attached to any network interface).

External Services Settings

Email

Use this panel to enable and configure Email integration. Asterisks indicate required fields.

Status

Click the toggle switch to enable / disable Email integration.

Sender Address

Enter a sender address for emails sent from DDM.

Server Details

Hostname	Enter the hostname or IP address for your Email server.
Port	Enter the port used to connect with your Email server to send outgoing mail. The default port for SMTP / StartTLS is 25, and the default port for SMTPS is 465.
Encryption	If your Email server is configured to use an encrypted connection, select the appropriate encryption protocol here to enable encrypted communication between DDM and the Email server (supported protocols are SMTPS and StartTLS).

Credentials

These fields are not required if the Email server does not use username / password authentication.

Username	Enter the username for the email account that will be used by DDM for sending email.
Password	Enter the password for the email account that will be used by DDM for sending email.

LDAP

Use this panel to enable and configure LDAP integration.

LDAP integration adds the users specified in the LDAP settings to the DDM user pool. LDAP users are able to log in to the DDM user interface and Dante Controller using their credentials from the directory server.

Status

Click the toggle switch to enable / disable LDAP integration.

Server Details

Hostname	Enter the hostname or IP address for your directory server.
Port	Enter the port used to connect and authenticate with your LDAP server. The default port for LDAP / StartTLS is 389, and the default port for LDAPS is 636.
Encryption	If your LDAP server is configured to use an encrypted connection, select the appropriate encryption protocol here to enable encrypted communication between DDM and the LDAP server (supported protocols are LDAPS and StartTLS).

Credentials

Dante Domain Manager requires the ability to read all relevant user records in the LDAP database. You must create an LDAP account with sufficient permissions to search the LDAP database for any user objects and attributes that you access in this panel or the LDAP Groups panel. Write access is not required.

Read-only Bind	Enter the full bind string for the administrator user.

Password	Enter the password for the administrator user.
Test Connection	Click to test the server connection. If successful, a green check mark is displayed.

Directory Entry Attributes

Search Root	Enter the full search root for the users that you wish to add to the DDM user pool.
Login Name Attribute	Enter the LDAP attribute that users will use to log in to DDM and Dante Controller (must be unique).
Email Attribute	Enter the LDAP attribute that DDM will use for email notifications.
Name Attribute	Enter the LDAP attribute that DDM will use for displayed names.

Example

- Search root: `ou=users,dc=example,dc=com`
- Login name attribute: `userId`
- Email attribute: `mail`
- Display name attribute: `cn`

When user BJones tries to log in, the Dante Domain Manager will search the LDAP subtree from `users,example,com` for a node with `userId=BJones`. Bruce's e-mail will be extracted from the LDAP attribute `mail` and his display name from the LDAP attribute `cn`.

LDAP Groups

Click to define LDAP groups and assign privileges for each group.

LDAP Groups

Use the LDAP Groups panel to define groups of LDAP users for the assignment of DDM privileges.

Note: Groups defined here are defined only on the DDM server. No changes are sent to the LDAP server.

Group Details

Name	Enter a name for the group.
LDAP Query	Enter a query that returns the LDAP nodes belonging to users in the group.
Test Query	Llist the users who match the current query.

Example

We want to create a group that gives members of the "tech team" domain administrator access. As it happens, the tech team can be identified in our LDAP database by the attribute `team=tech` on all members of the tech team.

- Name: Tech team
- LDAP Query: `(team=tech)`
- Privileges:
  - Default: domain administrator

`memberOf` queries will also work, but the syntax is a lot more verbose than simply having an attribute on the LDAP node.

Further example:

At some point, we add some casuals to the tech team. We don't want casuals having domain administrator access, except in the "Demo Room".

First, we modify the "Tech Team" group:

- LDAP Query: `(&(team=tech)(!(role=casual)))`

Then we create a new group:

- Name: Tech team casuals
- LDAP Query: `(&(team=tech)(role=casual))`
- Privileges:
  - Default: operator
  - Domain "Demo Room": administrator
  - Domain "Private Studio": none

Note: A user can be a member of more than one group; their privileges add together between groups. Domain-specific privileges override default privileges for a particular group, but will not remove default permissions granted by a different group.

Note: The results from "Test Query" might include entries that say Missing. In this case, the query is matching nodes that do not contain one or more of the user attributes configured above. Consider adding additional conditions to the query to remove those cases.

Example:

Query `(!(role=manager))` will return all nodes that do not have a role attribute that equals manager, which might include some unwanted nodes.

Query `(&(userId=*)(!(role=manager)))` only considers nodes that have a `userId` (and are not managers).

Privileges

Select the default role for the group.

Domain-specific Privileges

Optionally add one or more domain roles for the group.

■ See About User Roles for more information about default and domain roles.

SNMP

Use the SNMP panel to enable integration with an SNMP server.

When enabled, DDM becomes a read-only SNMP agent. Status information available in the DDM MIB includes core DDM functionality, licensing, external services, domains and devices.

The DDM supports two notifications (traps) to indicate that data has changed. One notification covers external services and core DDM functionality. The other covers health and connectivity of domains and devices. Upon notification, the MIB can be polled by the external SNMP management system to identify the specifics of the change. This could trigger alarms or other actions.

Refer to the MIB for details.

DDM supports SNMPv2c.

Status

Click the toggle switch to enable / disable SNMP integration.

Community Password

Provide the community password for your SNMP server.

System Contact

Provide contact details (for example, an email address) for your SNMP system administrator.

System Location

Provide information about the physical location of the SNMP server (for example, 'Rack 2 in server room B').

Add Endpoint

Adds a notification endpoint (for example, an NMS). DDM will send traps to all endpoints configured here.

Hostname	Enter the hostname or IP address for the SNMP endpoint.
Port	Enter the port number used by the SNMP endpoint for incoming traps (typically 162).

Clocking Settings

In order to enable synchronous clocking across domains that span multiple subnets, devices must be assigned as unicast clocks for each subnet in the domain. This can be done automatically, or manually.

Unicast clocks distribute clocking between subnets via unicast PTP. They can act as a unicast master or a unicast slave, depending on their proximity to the grand master clock. For example, a unicast clock in the same subnet as the grand master clock for the domain has the role of unicast master, transmitting PTP to a unicast slave in another subnet - which then distributes multicast PTP for the other devices in its subnet.

- See also: Synchronous Clocking

A unicast clock will often (but not always) also act as the multicast clock master for its own subnet.

If all PTP unicast clocks for a domain are removed from the network, powered down, or unenrolled from the domain, the subnet will lose its clock connection to other subnets, and audio between subnets may begin to glitch until a new unicast clock is assigned. The DDM dashboard will provide a notification in this event.

Note: Clocking configuration is only required for domains that span two or more subnets.

Note: Legacy Ultimo devices cannot function as unicast clocks, but Ultimo X devices can. To determine if a device is legacy Ultimo or Ultimo X: In Dante Controller, open the Device View > Status tab for the device, and check the Model type in the Dante Information panel. Legacy Ultimo devices are listed as 'Ultimo' or 'Ultimo4', and Ultimo X devices are listed as 'UltimoX' or 'UltimoX4'.

Auto-configure

The Auto-configure function assigns one device in each subnet to act as the active unicast clock, and also where possible a secondary unicast clock to act as backup if the active unicast clock is disconnected, powered off or unenrolled.

Auto-configure is applied at the point of configuration. The DDM will not independently reconfigure unicast PTP in the event of a device failure.

To configure clocking for a domain automatically:

1. In the Domains menu, select the domain.
2. In the Settings section of the Domain Details panel, click **Auto-Configure**.

To see or change which devices have been assigned as unicast clocks, click Advanced Settings.

Advanced Settings

Use the Advanced Settings page to set the clocking mode for the domain, and manually configure domain clocking.

Clocking Mode

Three domain clocking modes are supported:

- Default

  In default mode, the domain uses the standard Dante PTP clocking solution as described above.

- AES67

  In AES67 mode, the domain is configured for AES67 clocking, enabling audio interoperability between Dante devices and non-Dante AES67 devices.

- SMPTE

  In SMPTE mode, the domain is configured for SMPTE ST 2110-30 clocking, enabling audio interoperability between Dante devices and non-Dante SMPTE devices.

🟥 See AES67 and SMPTE Domains for more information.

PTP Configuration

Set the PTP Configuration to 'Custom' to enable PTP V2 clocking, specify the PTP V2 domain number, and specify the default PTP V2 priorities for all supporting devices in the domain (or shared audio group).

This feature enables you to configure the domain so that a non-Dante clocking device (for example, a GPS-enabled device) can win the clock election, and thus become grand master clock for the domain.

PTP V2 priorities can also be specified at device level via the 'Customize Clocking' feature. Device-level priorities override domain-level priorities.

Note: Custom PTP configuration is supported by devices at v4.2 firmware or above.

Note: With Custom PTP Configuration enabled, the Dante Controller 'Preferred Master' setting is unavailable for devices enrolled in the domain.

Note: The PTP V2 domain number cannot be specified for AES67 domains.

Domain Clocking

Manual clocking configuration allows you to selectively nominate unicast clocks for the domain. Suitable devices are those that are unlikely to be removed from the network or powered down. Where possible you should nominate two devices.

Note: As a rule of thumb, the more powerful Dante platforms provide slightly better clocks - for example, a Brooklyn II based device should be preferred over an Ultimo based device.

To configure clocking for a domain manually:

1. In the Domains page, select the relevant domain.
2. In the Domain Details panel, click **Advanced Settings**.
3. For each subnet, enable one or two devices to act as unicast clocks.

Note: It is common for devices to share the roles of subnet master and unicast clocking (boundary clock). See Synchronous Clocking for more information.

Assign Zone

Enables subnets in a domain to be independently clocked by an external clock source (for example, GPS).

- See About Zones for more information.

Note: The Assign Zone button is displayed when two or more devices in a domain reside in different subnets.

Customize Clocking

Click **Customize** to enable PTP Preferred Master and PTP sync External for the device, and to toggle PTP v1 delay requests between unicast and multicast. See the Dante Controller user guide for more information about these device features.

For SMPTE domains, you can also use Customize Clocking to specify the PTP V2 priorities and the RTP prefix for RTP-enabled devices.

For domains with a Custom PTP configuration, you can use Customize Clocking to specify the PTP V2 priorities for devices.

Shared Audio

Clocking settings can cover multiple domains if you have configured audio sharing between domains.

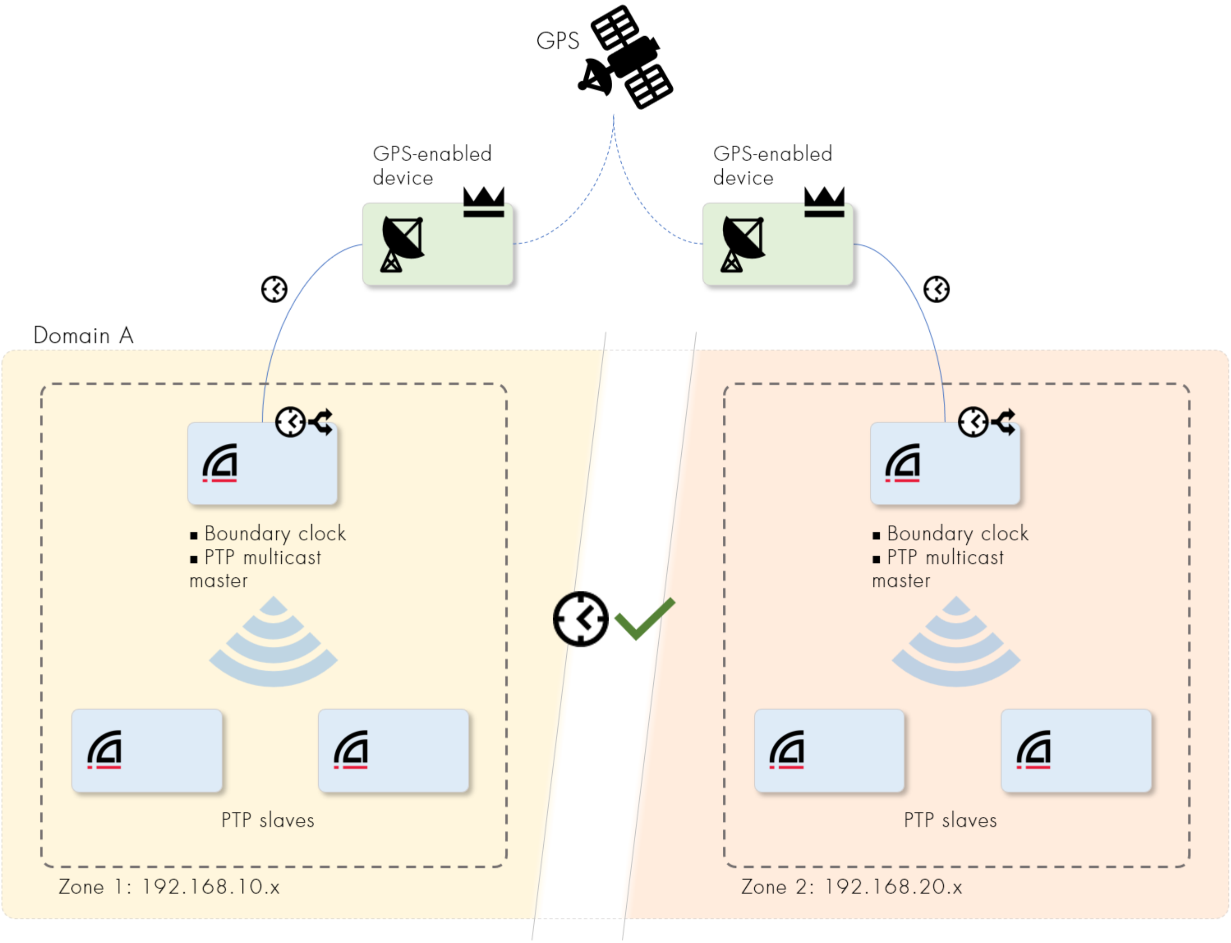
About Zones

Assign Zone creates a logical 'zone' for all devices in the selected subnet, and another zone for the remaining devices.

Standard multi-subnet domains require at least one unicast clocking device in each subnet, to distribute the network clock between the subnets. Zoned domains, however, do not have the same requirement - unicast clocking between the zones is not mandated.

This enables the zones to be clocked independently by a shared non-local clock source - for example, GPS - which in turn enables audio in geographically-separated zones to be fully synchronized.

In the example below, one device in each zone is acting as a boundary clock, taking their clock from a GPS-enabled device, and the rest of the devices in each zone are synchronized to the local boundary clock.



System Monitoring

Dashboard

To view the dashboard, select Dashboard from the main menu.

The dashboard is comprised of a set of widgets showing alerts and various types of system information, and is updated dynamically.

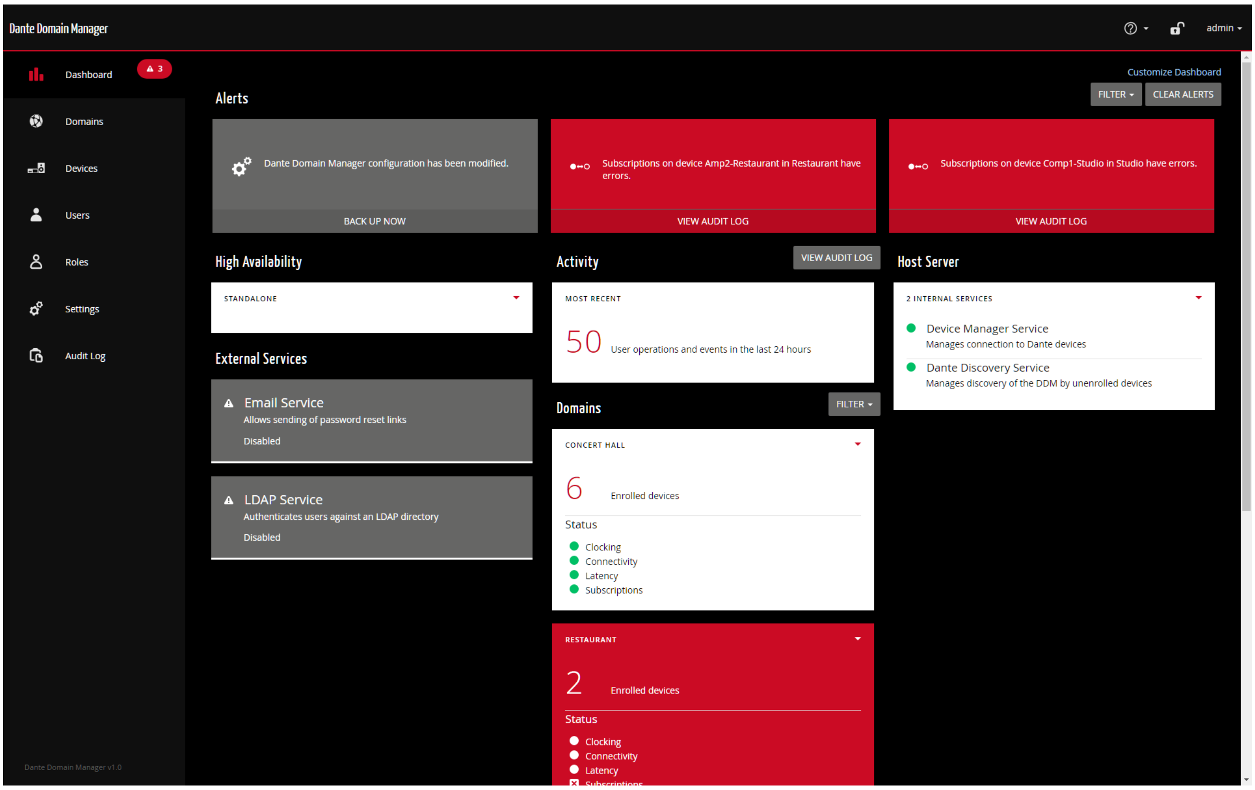
To filter the dashboard to show only information for specific domains or alert categories, click **Filter**.

To add, remove or move widgets, click **Customize Dashboard**. Editing your dashboard view does not affect any other users' dashboards.

In Customize mode:

- To remove a widget, click **Remove** at the top right of the widget
- To move a widget, drag & drop the widget into the target panel
- To add a widget, click **Add Widget** in the target panel
- To rename a widget, click anywhere in the widget name, or hover over the widget name and click the pencil icon

Note: For device-related information, refer to Dante Controller.



Dante Domain Manager configuration has been modified.

Subscriptions on device Amp2-Restaurant in Restaurant have errors.

Subscriptions on device Comp1-Studio in Studio have errors.

50 User operations and events in the last 24 hours

● Device Manager Service
Manages connection to Dante devices

● Dante Discovery Service
Manages discovery of the DDM by unenrolled devices

Email Service
Allows sending of password reset links
Disabled

LDAP Service
Authenticates users against an LDAP directory
Disabled

6 Enrolled devices

Status
● Clocking
● Connectivity
● Latency
● Subscriptions

2 Enrolled devices

Status
○ Clocking
○ Connectivity
○ Latency
☒ Subscriptions

Figure 1 - The DDM Dashboard

Alerts

The alerts section of the Dashboard displays system, device and user-related alerts.

The text in the alert card provides details about the nature of the alert. Click the live area at the bottom of the alert card to address the alert, or to view further information about the alert type.

Alert categories are identified by icons:

Icon	Category	Description	Alert Type Resolutions
🕒	Clocking	Clocking alerts indicate issues such as loss of clock sync for a device, or the presence of a multi-subnet domain for which subnet clocking has not yet been configured.	■ 'A unicast capable device is available but not enabled for [subnet] in [domain]': This indicates that a multi-subnet domain has not been configured for multi-subnet clocking. See Clocking Settings for more information. ■ 'No unicast clocking capable devices are available for [subnet] in [domain]': This indicates that multi-subnet clocking cannot be implemented for the domain because there are no devices in the domain capable of unicast clocking. ■ 'A secondary unicast clocking device is recommended for [subnet] in [domain]': This indicates that there is only one device in the domain configured as a unicast clock, and a second should be added to the domain to maintain clocking if the primary device goes offline. ■ 'A secondary unicast clocking device is available but not enabled for [subnet] in [domain]': This indicates that only one device in the domain has been configured as a unicast clock, but there is another device present in the domain which should also be configured as a unicast clock. ■ 'A superior unicast clock device is available for [subnet] in [domain]': This indicates that the device most suitable for unicast clocking in the domain is not currently configured as a unicast clock. ■ 'An excessive number of unicast devices are enabled for [subnet] in [domain]': This indicates that there are too many devices in the domain configured as unicast clocks - only two are required for each multi-subnet domain. ■ 'Clock out of sync - [device] in [domain]': This indicates that a device has lost clock sync. This could be because a slave clock is unable to maintain sync with its clock master, or because the device is in a different clock domain from the master clock. Refer to the Dante Controller user guide for more information about device clocks. ■ 'Clock drift - [device] in [domain]': This indicates that a device clock is drifting and may be at risk of losing sync.

Icon	Category	Description	Alert Type Resolutions
🔗	Connectivity	Connectivity alerts indicate device connectivity issues, such as an enrolled device going offline.	▪ 'Device offline - [device] in [domain]': This indicates that an enrolled device is offline (has been powered down, or physically / logically disconnected from the network). Power up or reconnect the device to resolve the alert.
▮▮▸	Latency	A latency alert indicates that a device's latency setting is too low for the network configuration, resulting in dropped audio packets.	▪ 'Latency too high - [device] in [domain]': This indicates that a device's latency setting is too low for the network configuration and audio packets are being dropped. Use Dante Controller to increase the device's latency setting.
●↔○	Subscriptions	Subscription alerts indicate issues such as unresolved subscriptions between devices, or the loss of audio flow between subscribed devices.	▪ 'Subscriptions have errors - [device] in [domain]': This indicates that one or more audio subscriptions for the device are unresolved. This could be because the receiver and transmitter are using different sample rates, or because the transmitter is offline. It can also indicate loss of audio flows between subscribed devices.

Icon	Category	Description	Alert Type Resolutions
⚙	System	System alerts indicate issues such as an expired TLS certificate or DDM license.	■ 'Dante Domain Manager configuration has been modified': This indicates that configuration changes (for example, device enrollments) have been made, and the configuration can be backed up if required. ■ 'Dante Domain Manager software update failed to install': This may be a problem with the target computer or the update file. Contact your technical support representative for more information. ■ 'Dante Domain Manager software update available': Go to Settings > Updates and System Information Settings to download and install the update. ■ 'External service unavailable': An integrated service (for example, email or LDAP) is unavailable and must be restarted or reconfigured. ■ 'Internal service unavailable': The DDM manager service or the Dante Discovery service has stopped. Restart DDM to resolve this issue. ■ '[Certificate] has expired / will expire on ... ': Your TLS certificate has expired or will soon expire. Upload a valid certificate to resolve this issue. ■ 'Dante Domain Manager license has expired / will expire on ... ': Contact your sales / support representative for more information.

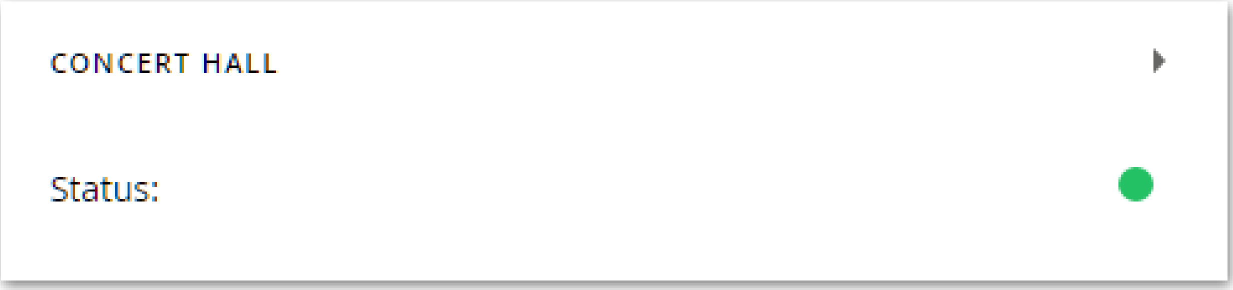
To dismiss alerts, click the **x** icon in the top-right corner of the alert, or click **Clear Alerts**.

Note: Some alerts are 'sticky' and cannot be dismissed - they will disappear when the underlying issue has been resolved.

Domain Cards

The cards in the Domains section of the Dashboard display the status of all domains, including the number of enrolled devices and the status of various domain attributes.

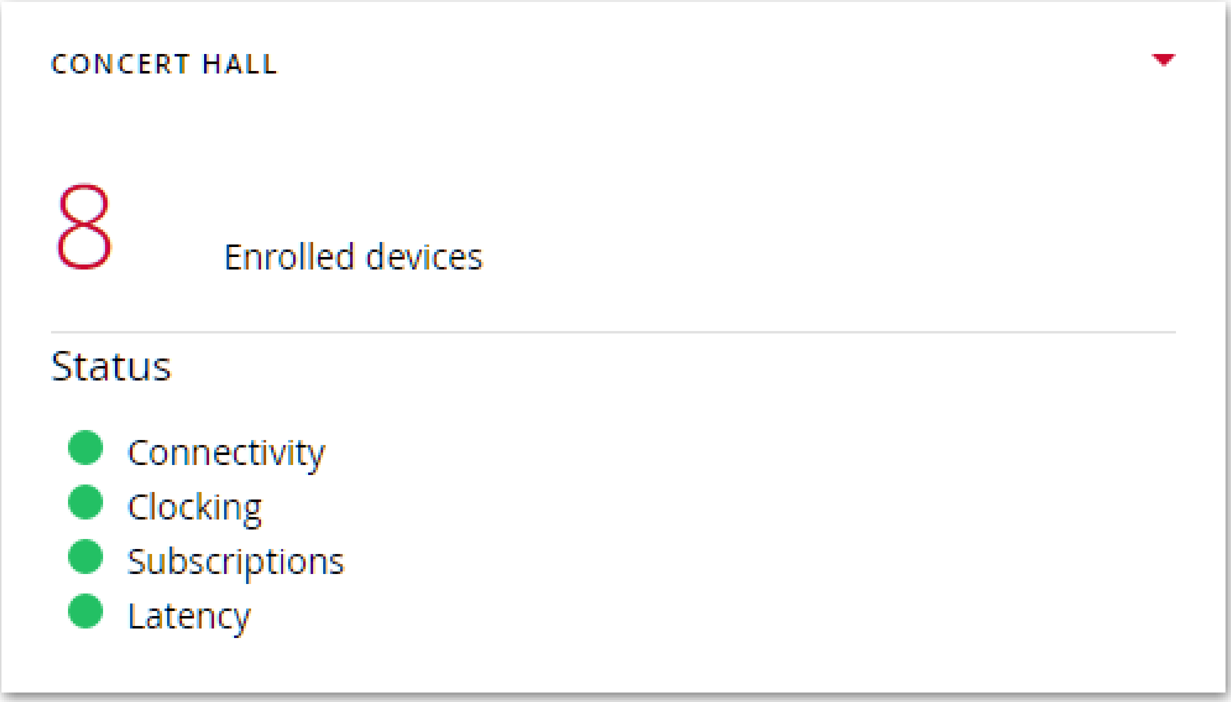
White domain cards with green LED status icons indicate fully-functional domains.



CONCERT HALL

Status: ●

Click the ▸ icon to expand a domain card. The connectivity, clocking, subscriptions and latency status is displayed for each domain.



CONCERT HALL

8 Enrolled devices

Status

● Connectivity

● Clocking

● Subscriptions

● Latency

Red domain cards indicate domains with one or more functional issues. In the collapsed state, icons indicate the functional areas that need attention.

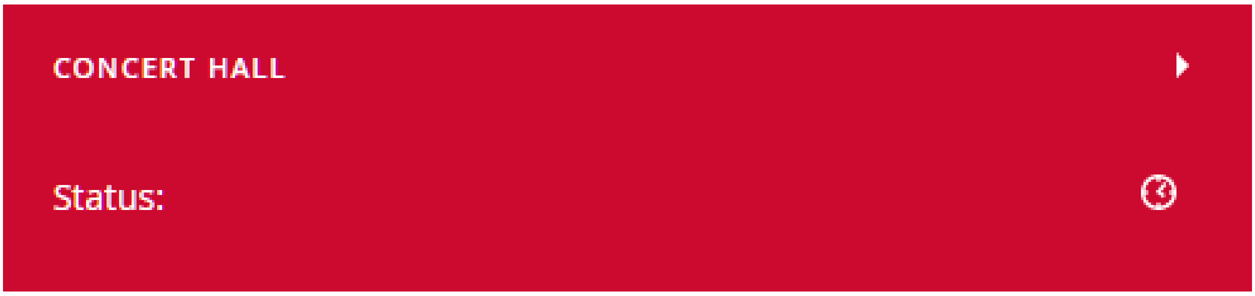
Connectivity issue

Clocking issue

Unresolved subscriptions

Device latency issue	▮▮▸

The domain shown below has a clocking issue.



CONCERT HALL

Status:

- See Alerts for information about resolving domain-related issues.

Using the Domains Filter

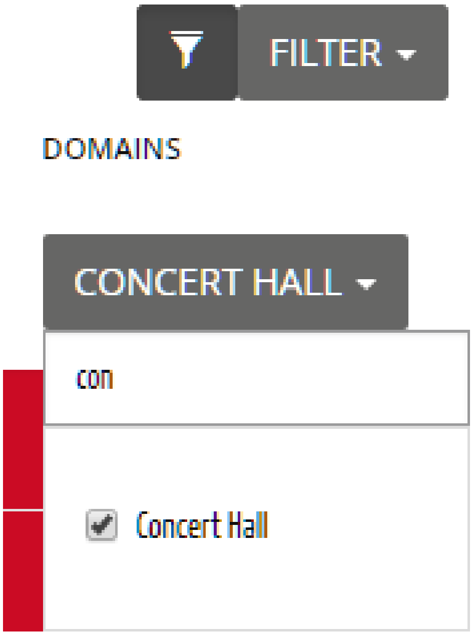
Use the domains filter to display only selected domain cards on the dashboard.

Use the filter button to globally disable and re-enable the domains filter:

To display only selected domain cards on the dashboard:

1. In the Domains panel, click **Filter**.
2. Click **Domains**.
3. Click **All.**
4. Start typing the name of a domain until the relevant checkbox is displayed.
5. Select the displayed checkbox.

You can filter domain card display to one or more domains.



Other Dashboard Cards

High Availability

The High Availability card displays the status of the high availability configuration.

Activity

The Activity card displays the number of recent user operations and events.

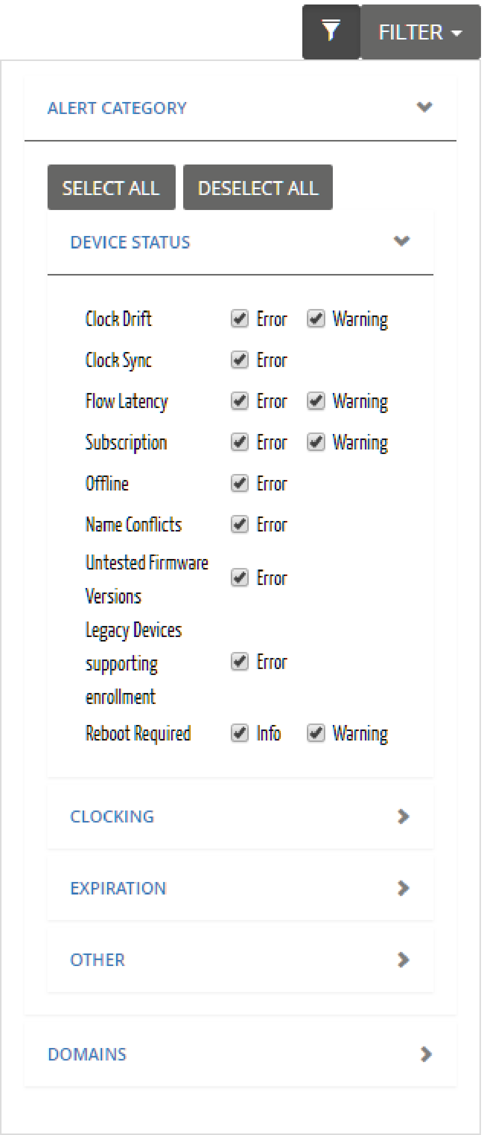
Host Server

The Host Server card displays the status of the internal services. If any internal service has stopped (indicated by a red LED icon), restart the machine.

External Services

The External Services cards display the configuration status of the external services.

Using the Alerts Filter



FILTER

ALERT CATEGORY

SELECT ALL | DESELECT ALL

DEVICE STATUS

Clock Drift	☑ Error	☑ Warning
Clock Sync	☑ Error	
Flow Latency	☑ Error	☑ Warning
Subscription	☑ Error	☑ Warning
Offline	☑ Error	
Name Conflicts	☑ Error	
Untested Firmware Versions	☑ Error	
Legacy Devices supporting enrollment	☑ Error	
Reboot Required	☑ Info	☑ Warning

CLOCKING

EXPIRATION

OTHER

DOMAINS

Use the alerts filter to restrict the display of dashboard alerts to selected categories and/or domains.

Use the filter button to globally disable and re-enable the alerts filter:

Alert Category

To display alerts of selected categories only:

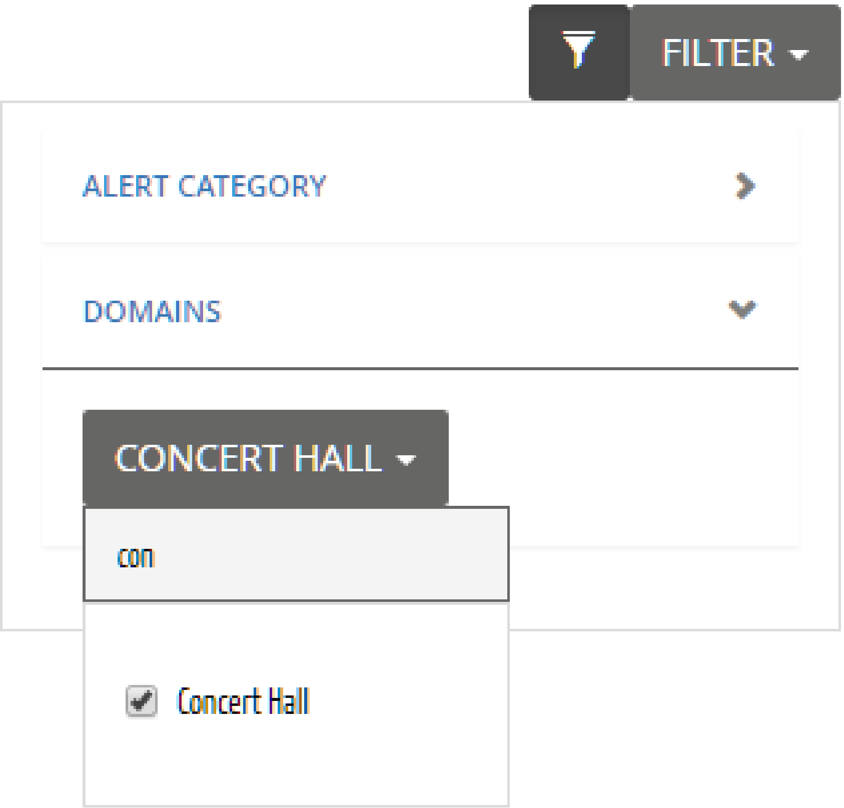
1. In the Alerts panel, click **Filter**.
2. Click **Alert Category**.
3. Click the required category group.
4. Use the checkboxes to enable or disable display for each alert category.

Domains

To display alerts for selected domains only:

1. Click **Filter**.
2. Click **Domains**.
3. Click **All.**
4. Start typing the name of a domain, until the relevant checkbox is displayed.
5. Select the displayed checkbox.

You can filter alert display to one or more domains.



Audit Log

To view the audit log, select **Audit Log** from the main menu or click **View Audit Log** in the dashboard 'Activity' panel.

The audit log displays a timestamped list of user-related events.

Note: For device-related events, please refer to the event log in Dante Controller.

Click **Customize Columns** to enable or disable audit log columns.

Click **Export to CSV** to save all entries to a CSV file.

Click **Clear Log** to permanently delete all entries.

Searching Event Details

To search for text in event details, click the 'Search event details...' field and enter text.

Use the associated check boxes to apply additional parameters.

Filtering the Log Entries

Click **Add Filter** to filter log entries by user, domain, device and event parameters. Filters are additive - the displayed results match all filters.

For example, a domain filter with domain name of 'Concert Hall', plus a user filter with a username of 'John' will filter the log to display only entries related to the Concert Hall domain and the user John.

Displaying More Entries

By default, 25 events are displayed per page. Use the 'Show [x] entries' drop-down menu to change the number of events displayed on each page.

User Interface Reference

Domains

The Domains page lists all domains.

Click a domain name to see the domain details.

Click **Add Domain** to add a new domain.

The Domains page also allows you to:

- Search for domains by domain name
- Delete existing domains

Note: Only site administrators can add and delete domains.

Domain Details

To rename a domain, click anywhere in the domain name, or hover over the domain name and click the pencil icon

Settings

- Click **Advanced Settings** to open the Advanced Settings page.
- 'Clocking Type' indicates the type of clocking in use by the domain. Values are single-subnet (all devices in the domain are on the same IP subnet) and multi-subnet.
- Click **Auto-configure** to automatically configure clocking for the domain.
- 'Grand Master' indicates the device that is currently the grand master clock for the domain.
- 'Allow association with pre v4.0 firmware devices': Use this switch to enable legacy device support for the domain. Legacy Interop must also be enabled globally in the Network & Security settings.

Shared Audio

The Shared Audio panel lists any shared audio group configured for the domain, and allows you to edit the group.

Dante SMPTE/AES67 Sessions

If present, this section lists existing SMPTE or AES67 sessions (Tx multicast flows) that have been created using Dante Controller for Dante devices enrolled in the domain.

Click the session name to view the session descriptor.

External SMPTE/AES67 Sessions

If present, this section lists existing SMPTE or AES67 sessions that have been created using the 'Add Session' function (for non-Dante devices).

Click the session name to view the session descriptor.

Click **Remove** to remove a session.

Devices

The Devices field lists the devices in the domain, their enroll and connectivity states, and which IP subnet they are in.

To add devices to the domain, click **Enroll Devices**.

To remove devices from the domain, click **Unenroll Devices**.

Click a device name to view the device details for the device.

Enroll by IP Address Status

This field displays issues that were encountered during manual device enrollment by IP address - for example, IP addresses that could not be found, and devices that were not successfully enrolled.

Click **Delete** to cancel a pending enrollment.

Devices

The Devices page lists all devices enrolled in or associated with each domain.

Click the ‣ icon to expand a domain and view the enrolled devices.

Click a device name to see the device details.

The Devices page also allows you to:

- Search for devices by domain name
- Enroll devices
- Identify locked devices
- View devices that cannot be enrolled

🟥 See also: Legacy Devices

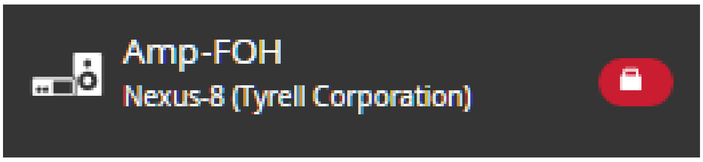
Note: Each Dante 'node' counts as an individual device - for example, a console with 3 Dante interface cards installed will present as 3 devices in DDM.

Unmanaged Domain

The Unmanaged domain includes all devices that have been discovered on the Dante network, but are not enrolled in a specific domain.

Locked Devices

Devices that have been locked in Dante Controller are indicated by a red padlock icon next to the device name:



Amp-FOH

Nexus-8 (Tyrell Corporation)

Enroll and unenroll operations on locked devices will only complete when the device becomes unlocked.

Cannot Enroll

If an attempt was made to enroll any devices that cannot be enrolled, those devices are listed here.

Export CSV

Exports a CSV file listing all discovered devices, with version, interface, domain and status information for each device.

Device Details

Field	Description
Manufacturer	The host device manufacturer
Product Type	The product type
Product Version	The product version
Dante Firmware / Software Version	The firmware or software version for the Dante module on the device
Hardware Version	The hardware version for the Dante module on the device (if applicable)
Last Connected	The date and time the device was last connected to the DDM
Connected Since	The date and time the device was first connected to the DDM
Domain Enrollment	
Domain	The domain in which the device is enrolled
Enrollment Status	The status of any enrollment or unenrollment processes
Network Interface	
Primary IP Address	The IP address of the device’s primary network interface

The following fields are also present for enrolled devices.

Field	Description
Recent Activity	A time-stamped list of device-related events
Domain Enrollment	
Clock sync status	The status of the device's clock synchronization with its master clock
Device Info	
Location	Editable free text field
Description	Editable free text field

Field	Description
Comments	Editable free text field
Embedded Controller Policy These fields are only present when enabled in the module configuration.	
Configuration of This Device	Prevent: A local controller (such as a front panel) can query device settings, but not change them. Allow: A local controller can query and make changes to device settings.
Dante Network Role	Operator: Remote controllers (such as Dante Controller) can query and make changes to device settings. Guest: Remote controllers can only query device settings. None: Remote controllers cannot query or change device settings.

Users

The Users page lists all users.

Click a user name to see the user details.

Click **Add User** to add a user.

Select a user and click **Delete User** to delete the user.

Note: Only site administrators can perform user configuration actions (including adding new users), except for password resets.

The Users pages also allows you to:

- Edit existing users
- Deactivate existing users
- Reactivate inactive users
- Add users to domains

LDAP Users

When LDAP is configured, LDAP users are displayed in the Users page.

LDAP users cannot be edited using DDM.

Forget User

Click **Forget User** to remove the user from the LDAP Users list, until they next log in to DDM or Dante Controller.

Note: Forgetting an LDAP user does not affect their DDM privileges.

User Details

Click **Deactivate User** to deactivate the user.

Click **View Audit Log** to see the actions history for that user.

Field	Description
Username	The user's username
Password	Click **Reset Password** to change the user's existing password
Email Address	An email address to which password reset links will be sent
Last Logged In	The date and time the user was last logged into DDM
Last IP address	The last IP address that was recorded for the user
Recent Actions	
A timestamped list of actions performed by the user	
Privileges	
Default Role	The default role assigned to the user
Domain-specific Privileges	
Domain	The domain name(s) for which the user has a specific role
Role	The user's role for the listed domain

Roles

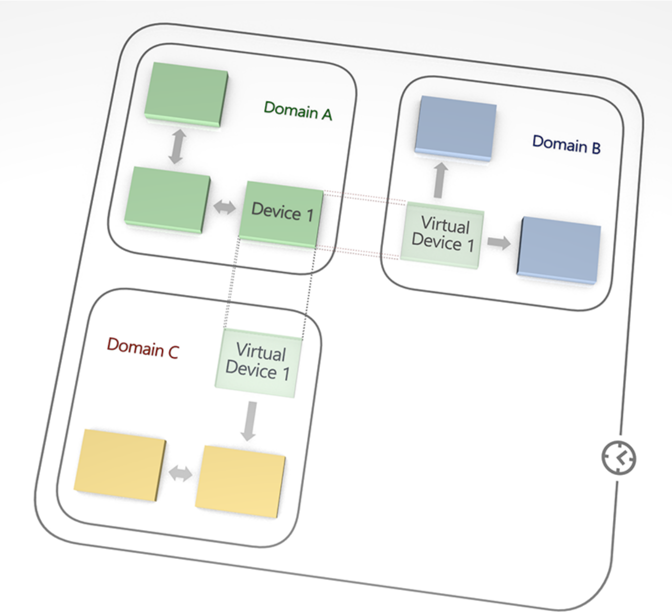
The Roles page lists all user roles.

Click a role name to see the role details.

Role Details

The Role Details page lists the privileges associated with the selected role.

Sharing Audio Between Domains



DDM supports the sharing of audio between domains using the concept of 'virtual' devices.

A virtual device is a 'projection' of a real device, which can appear in multiple domains simultaneously, and can be subscribed to by real devices in those domains. It presents in Dante Controller as an independent transmitter, but is really just a logical entity which acts as a subscription proxy for a real device.

When you subscribe to a virtual device, the audio you receive is from the real device. Virtual devices cannot subscribe to other devices.

You can control the domains in which a virtual device appears, and which channels on the real device are exposed by the virtual device. Virtual devices can be assigned their own individual device names. They do not appear in the device lists in the DDM interface.

How to Share Audio Between Domains

Process Summary

1. Create a shared audio group.
2. Add the required domains to the group.
3. Specify which devices are allowed to share their audio (this creates a virtual device from each real device).
4. Specify which transmit channels on the real devices are exposed in the respective virtual devices.
5. Configure clocking for the shared audio group. Shared audio group clocking overrides domain-level clocking.
6. Use Dante Controller to route audio between the relevant devices.

Create a Shared Audio Group

A shared audio group is a set of domains between which audio can be shared. Shared audio groups use a common clock domain, which replaces domain-level clocking.

To create a shared audio group:

1. Go to the Domain Details page for one of the domains that you want to be part of the group.
2. Click **Edit**.

3. In the Shared Audio section, type a Group Name for the shared audio group.
4. Click **Save Changes** at the top of the page.

Add Domains to the Group

1. Ensure you are still on the Domain Details page for the domain you just added to a group.
2. In the Shared Audio Group section, click **Edit**.
3. On the Edit Shared Audio group page, click **Edit Domains**.
4. Select the checkboxes for the domains that you want to add to the group.
5. Click **OK** and then **OK** again.

Add Devices to the Group

1. Go to the Device Details page for the device that you want to add to the shared audio group (note: It must be enrolled in one of the domains in your group).
2. Click **Edit**.
3. Scroll down to the 'Tx Channel Sharing' section.
4. Change the sharing Scope for the device from :[Domain name] Only (which means no channels are shared) to one of:
   - All domains / selected channels (the selected channels will be shared with all domains in the group)
   - Selected domains & channels (the selected channels will be shared with selected domains in the group)
5. In the Shared Name field, enter a name for the virtual device. This can be the same as the real device name (a virtual device will not appear in the same domain as the real device from which it was created).

ℹ **Note:** Legacy devices cannot share audio between domains.

Specify Shared Channels

1. While still in Edit mode, in the Tx Channel Sharing section, click the hyperlink under Shared Channels (this will say 'none' if there are no channels currently shared).
2. Select the checkbox for each channel that you want to share.
3. Optionally, under 'Destination Name', enter a new name for one or more channels.
4. Click **OK**.
5. Scroll to the top of the page and click **Save Changes**.

Configure Clocking for the Group

Clocking for shared audio groups is identical to domain-level clocking, except that the settings apply to multiple domains instead of just one.

1. Go to the Domain Details page for one of the domains you added to your group.
2. Click **Clocking Settings**. The title at the top of the page indicates how many domains are affected by the settings.

3. Click **Configure Automatically**, and then **OK**; or click Advanced Settings if you want to select your own clocks.

Routing Shared Audio in Dante Controller

Virtual devices appear in Dante Controller as transmit devices in green text, with no receive channels.

You can subscribe to a virtual device in the same way you would a real device.

Redundant Networks

Dante Domain Manager supports redundancy only **within** a subnet.

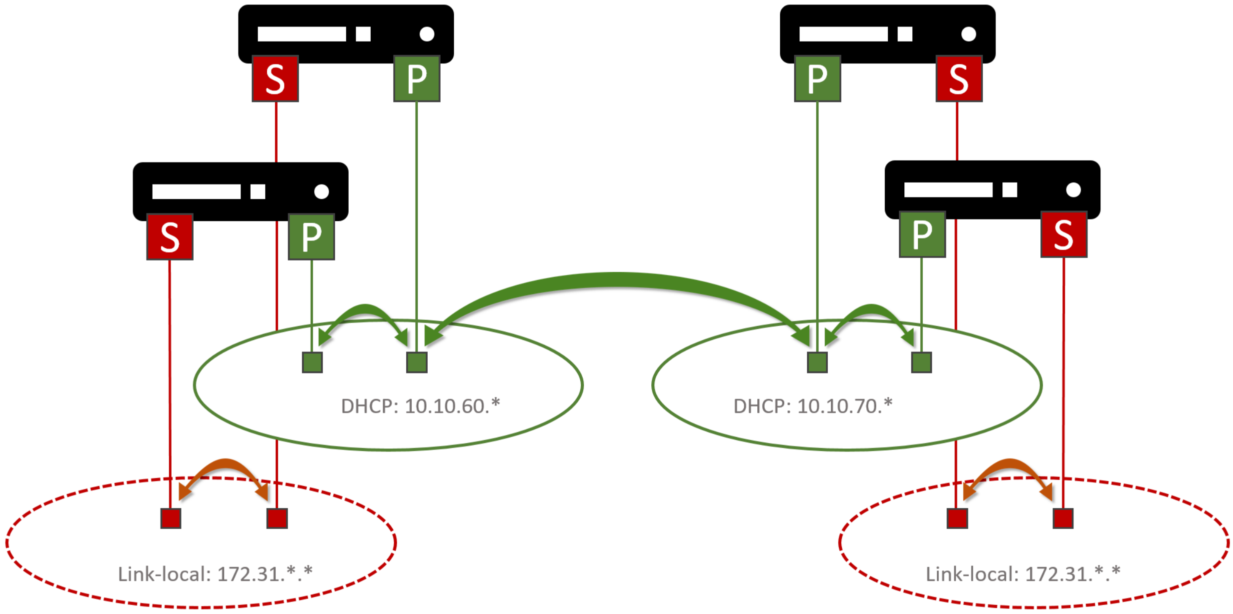
Redundant audio is not supported between devices in different subnets. Dante Domain Manager will filter subscriptions across subnets to disable redundancy on these subscriptions.

Dante Domain Manager assumes that connectivity of secondary subnets mirrors their primary subnets. The following are explicitly not supported for 'correct' redundant operation:

- Devices in different primary subnets sharing a secondary subnet
- Devices in the same primary subnet being in different secondary subnets
- Secondary subnets using DHCP for address allocation (only link local is supported on secondary; all devices disable DHCP on the secondary interface)

In the example of a supported configuration illustrated below, there are two primary subnets (10.10.60.* and 10.10.70.* are used as example address ranges) which are served addresses by DHCP. DDM enables audio routing between these subnets.

The secondary interfaces for the devices in each primary subnet are connected to isolated subnets, using Link-local for address allocation. Audio routing is not supported between these subnets.

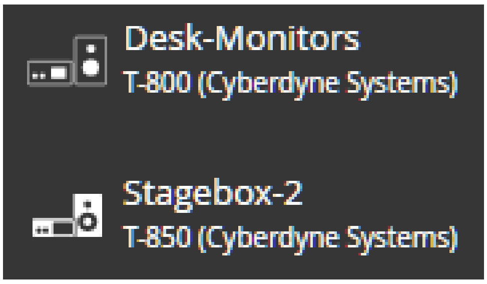


Legacy Devices

Devices with some legacy (pre-v4.0) versions of firmware (shown in the table below) can be 'associated' with domains. This adds them to the relevant clock domain, and allows them to exchange audio with devices enrolled in the same domain, which are also on the same IP subnet (legacy devices do not support audio routing between subnets).

Support for legacy devices can be enabled globally in the Network & Security settings, and at domain level in the Domain Details page.

Legacy devices can be easily identified by their icon in the Devices page. In the image below, the 'Desk-Monitors' device is a legacy device, and the 'Stagebox-2' device is a non-legacy (firmware v4.x or above) device.



Desk-Monitors
T-800 (Cyberdyne Systems)

Stagebox-2
T-850 (Cyberdyne Systems)

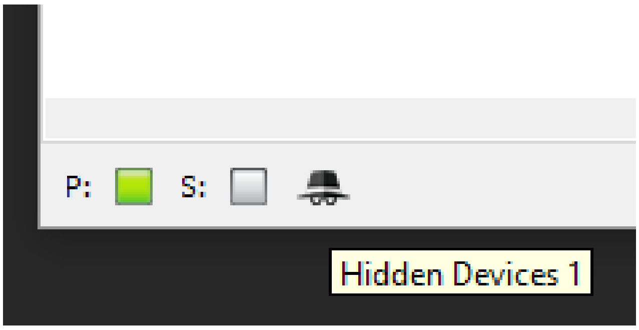
Note: Dante Controller must be connected to the same subnet as a legacy device in order for it to appear in the Dante Controller interface.

Important: When legacy devices are associated with a domain, they are **not** protected from unauthorized access via Dante Controller. Also, when associated, they are placed in a dedicated clock domain and thus can no longer exchange audio with unmanaged devices.

Hidden Legacy Devices

If a legacy device is moved to an unmanaged Dante network without first being de-associated, it will not appear by default in Dante Controller.

Dante Controller notifies you with a spy icon (next to the network status icons at the bottom left of the UI) if you have hidden devices on your network:



To view hidden devices in Dante Controller, select View > 'Show All Unmanaged Devices'.

To clear their domain credentials, open the Device View for the device, and select Device > 'Clear Domain Credentials'.

Legacy Firmware Support

The table below lists the legacy firmware versions that support domain association for each Dante product or platform.

Minimum versions may exhibit errors when associated. Supported versions will provide better performance.

Product / Platform	Minimum	Supported
Brooklyn I	3.7.2	3.7.2
Brooklyn II	3.7.x	3.8.x
Dante-MY16-AUD	3.10.x	3.10.x
Dante-MY16-AUD2	3.10.x	3.10.x
Dante PCIe Cards	3.7.x	3.10.x
Ultimo (ULT-01-002/4)	2.2.x	3.9.x
Ultimo X (UXT-001-002/4)	3.9.x	3.9.x
Dante HC	3.9.x	3.10.x
Yamaha HY144-D	3.9.x	3.10.x

Note: Legacy support for Ultimo / Ultimo X v3.9 was introduced in DDM v1.0.6

Troubleshooting

502 Bad Gateway

You may see this page temporarily at the DDM URL when starting up the DDM server.

It indicates that the web server is running, but the DDM services have not yet started. Wait a few seconds and refresh your browser to open the DDM UI.

Appendix

Synchronous Clocking

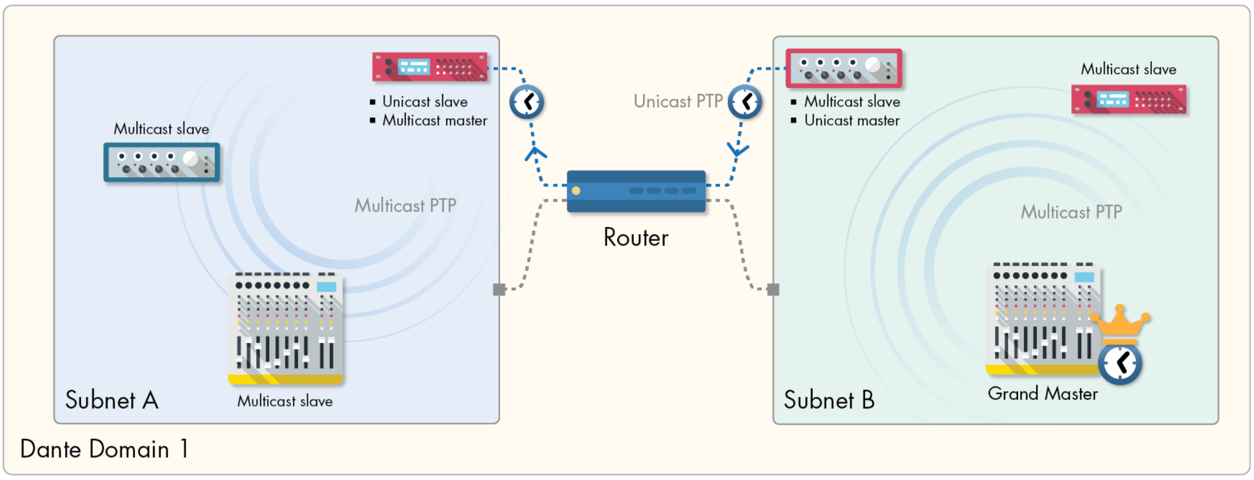
All Dante devices in a given domain lock directly or indirectly to one single Grand Master clock device.

In the case of domains for which all devices reside on the same IP subnet, the standard Dante method of multicast PTP clocking is used. One clock master device is automatically elected or manually specified, which broadcasts the clock signal via multicast PTP, and all other devices slave their own clocks to that master device.

In the case of domains that span subnets, one Grand Master clock device is automatically elected (or manually specified) for the domain, and one boundary clock device will be automatically elected for each subnet (identified as the 'unicast clocking' device in the DDM clocking settings). Usually, the Grand Master will also act as the unicast master for its own subnet.

The Grand Master transmits the PTP clock signal via multicast to the slave devices in its own subnet, as is the case for traditional Dante networks. The elected unicast clock in the Grand Master’s subnet transmits the clock signal via unicast PTP, through the router, to the unicast clock in the adjoining subnet, which in turn transmits multicast PTP to the other devices in that subnet.

The same model applies to any other subnets in the domain. This system enables synchronous Dante networks that span multiple subnets.



AES67 and SMPTE Domains

Overview

Dante supports multicast audio interoperability between Dante devices and non-Dante AES67 RTP and SMPTE ST 2110-30 audio devices.

AES67 is supported in DDM and non-DDM networks. SMPTE is only supported in DDM networks.

Use Dante Controller to subscribe to and generate AES67 and SMPTE multicast flows.

Not all Dante devices support AES67 and SMPTE - check with your device manufacturer. SMPTE support requires Dante firmware v4.2.x or above.

In DDM

AES67 and SMPTE support is enabled at device level, and also at domain level. Devices and domains cannot be configured for AES67 and SMPTE simultaneously.

Enabling AES67 or SMPTE for a domain does not affect the audio transport used directly between Dante-enabled devices in the domain. Audio transport directly between Dante-enabled devices is always via Dante Audio Transport Protocol, even if the audio originated from an AES67 or SMPTE device.

Enabling Support for AES67 or SMPTE

To enable AES67 or SMPTE mode, open the Domain Details page for the domain and click **Advanced Settings**.

AES67 Mode

AES67 mode enables audio interoperability between Dante devices in the domain and non-Dante AES67 devices.

Note: AES67 must also be enabled at device level, via the Device Details page in DDM. You can also use Dante Controller to specify an address prefix for AES67 multicast transmit flows.

Note: AES67 uses a fixed PTP V2 domain number (0), which means that AES67 can only be enabled for one domain at a time.

SMPTE Mode

SMPTE mode enables audio interoperability between Dante devices in the domain and non-Dante SMPTE devices.

Note: SMPTE must also be enabled at device level, via the Device Details page in DDM.

Note: You can enable SMPTE for multiple domains. Ensure that each domain uses a different PTP V2 domain number.

Clock masters in SMPTE clock domains are decided by the protocol via automatic election. The PTP V2 Priority values can be used to determine if your SMPTE-enabled Dante devices are more likely to be elected as masters or slaves. Refer to the SMPTE standard for more information.

SMPTE Parameters

A variety of parameters can be specified for SMPTE mode.

- **PTP V1 Multicast**

  If all devices in the domain that are configured for unicast clocking are at Dante firmware v4.2 or above, disabling PTP V1 multicast can prevent instability in non-Dante SMPTE devices.

- **PTP V2 Domain Number**

Can be set to any value between 0 and 127.

However, if there are any unicast clocking devices in the domain on Dante firmware v4.0.x or v4.1.x, set this to a value between 0 and 3.

See 'About SMPTE and Unicast Clocking' for more information.

- **PTP V2 Priority 1/2**

  The PTP V2 priorities determine which devices in a SMPTE clock domain will be automatically elected as clock master. The range extends from 0-255, with 0 being highest priority.

- **PTP V2 Sync Interval**

  The time interval between two successive PTP V2 multicast sync packets, expressed as logarithm to the base 2.

- **PTP V2 Announce Interval**

  The Time interval between two successive PTP V2 multicast announce packets, expressed as logarithm to the base 2.

- **PTP V2 Multicast TTL**

  The range over which a PTP V2 multicast packet is propagated in your network.

- **PTP Slave Only**

  Devices in the domain will not be elected as clock master.

- **RTP Transmit Port**

  The transmit port number for RTP packets.

- **System Packet Time**

  The transmit time (transmitter) of the RTP stream expressed as the number of samples of each channel in one packet.

- **Rx Latency**

  The receive latency for SMPTE flows in the domain.

- **RTP Prefix V4**

  The IP address prefix for RTP flows.

Configuring DDM for Interoperability with Non-Dante RTP Devices

Subscribing Dante Devices to RTP Flows from Non-Dante Devices

RTP transmit flows need to be advertised on the network by the transmitting device. These advertisements provide the information required by receivers to subscribe to the flow. The flows can be advertised in a variety of ways.

Dante Controller supports RTP descriptors transmitted via SAP, and containing a range of specific values. Flows that are advertised this way will automatically appear in Dante Controller as a transmit flow.

For non-Dante devices that do not use SAP to transmit RTP descriptors, DDM must be configured to 'proxy' the descriptor via SAP so that Dante devices can subscribe to it.

To generate a SAP/SDP descriptor for these devices:

1. Copy the RTP descriptor for the relevant flow into a text editor.
   - To identify the descriptor, refer to the user manual for your device (or you can use a packet analyzer such as Wireshark to search for SDP descriptors).
2. Ensure that the descriptor complies with the format described in Sample SDP Specification.

3. In the Domain Details for the RTP domain, click **Add Session**.
4. Paste in the SDP descriptor and click **OK**.

Existing sessions will present as RTP transmit flows in the relevant domain in Dante Controller.

To remove an existing session, click the **Remove** button next to the session name.

Subscribing Non-Dante Devices to RTP Flows from Dante Devices

For supporting Dante devices, RTP transmit flows are created in Dante Controller using the Create Multicast Flow dialog.

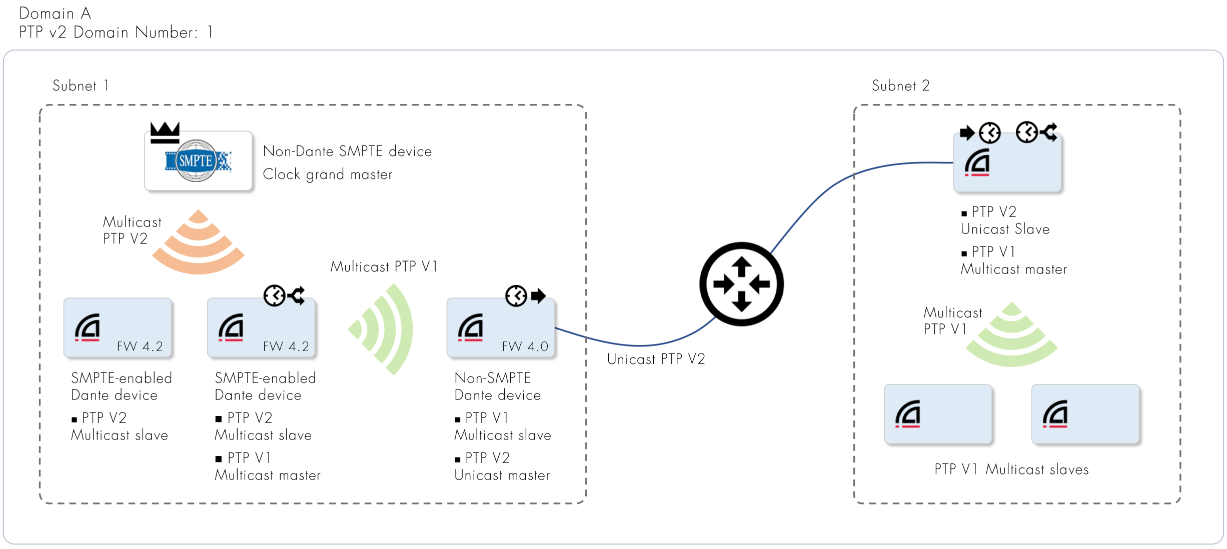
The transmit flow will present automatically in the non-Dante controller software if it supports SAP/SDP parsing. If not, a mechanism is required to parse the SDP descriptor from the Dante device. The configuration of non-Dante devices to receive RTP flows is specific to the device.

About SMPTE and Unicast Clocking

The default PTP V2 domain number for SMPTE is 127. Dante devices at firmware v4.0.x and 4.1.x do not support unicast clocking when the PTP V2 domain number is any value above 3.

If unicast clocking is enabled for any devices in the domain, and SMPTE mode is activated with a PTP V2 domain number above 3, DDM will display a warning pop-up. If you acknowledge the pop-up, unicast clocking will be automatically disabled for all devices in the domain, and the SMPTE settings saved as configured. Alternatively, you can cancel the pop-up, change the domain number to anything between 0 and 3, and save the SMPTE settings without affecting the unicast clocking configuration.

The diagram below illustrates an example of a routed multi-subnet domain with a mix of Dante firmware versions, and all device clocks synchronized to a non-Dante SMPTE device.



Customize Clocking

Click Customize Clocking to specify the PTP V2 priorities for the device. This overrides the PTP V2 priorities for the domain.

Sample SDP Specification

SDP (Session Description Protocol) for SMPTE requires the following fields to be present.

Fields must appear in the order shown below, except that multiple adjacent 'a' fields can be in any order.

The SDP format is defined by RFC4566 (https://tools.ietf.org/html/rfc4566). SMPTE SDP is defined in the ST2110-10-2017 standard.

Note: AES67 descriptors use the same format but do not support redundant flows.

Sample SDP for a Multicast Flow

```
v=0
o=- 123456 123458 IN IP4 10.0.1.2
s=My sample flow
i=4 channels: c1, c2, c3, c4
t=0 0
a=recvonly
m=audio 5004 RTP/AVP 98
c=IN IP4 239.69.11.44/32
a=rtpmap:98 L24/48000/4
a=ptime:1
a=ts-refclk:ptp=IEEE1588-2008:00-11-22-FF-FE-33-44-55:0
a=mediaclk:direct=0
```

Sample SDP for a Redundant Multicast Flow

```
v=0
o=- 345678 345979 IN IP4 10.0.1.2
s=My sample redundant flow
i=2 channels: c6, c7
t=0 0
a=recvonly
a=group:DUP prim sec
m=audio 5004 RTP/AVP 98
c=IN IP4 239.69.22.33/32
a=rtpmap:98 L24/48000/2
a=ptime:1
a=ts-refclk:ptp=IEEE1588-2008:00-11-22-FF-FE-33-44-55:0
a=mediaclk:direct=0
a=mid:prim
m=audio 5004 RTP/AVP 98
c=IN IP4 239.69.22.33/32
a=rtpmap:98 L24/48000/2
a=ptime:1
a=ts-refclk:ptp=IEEE1588-2008:00-11-22-FF-FE-33-44-55:0
a=mediaclk:direct=0
a=mid:prim
m=audio 5004 RTP/AVP 98
c=IN IP4 239.69.44.55/32
```

```
a=rtpmap:98 L24/48000/2
a=ptime:1
a=ts-refclk:ptp=IEEE1588-2008:00-11-22-FF-FE-33-44-55:0
a=mediaclk:direct=0
a=mid:sec
```

Keys and Attributes

Session Level Keys

Key	Name	Example	Notes
`v`	Version	`v=0`	Always zero
`o`	Origin	`o=- 345678 345979 IN IP4 10.0.1.2`	See https://tools.ietf.org/html/rfc4566#section-5.2 for details
`s`	Session name	`s=My sample redundant flow`	Non-empty text string 'naming' flow
`i`	Session information	`i=2 channels: c6, c7`	▪ Human-readable session information ▪ Optional
`c`	Connection information	`c=IN IP4 239.69.22.33/32`	▪ Connection data (destination address) for multicast flow ▪ Must exist either here (non-redundant) or at media level
`t`	Time description	`t=0 0`	▪ Must have at least one entry ▪ Usually "`0 0`" - not time-limited

Session Level Attributes

Attribute	Example	Notes
Receive-only session	`a=recvonly`	Multicast flows are receive only
Media grouping	`a=group:DUP prim sec`	▪ Redundant flows only ▪ Indicates which media descriptions apply to this redundant flow. There must be a suitable media description with a 'mid' attribute matching each name. ▪ If this attribute is missing, the first suitable (audio) media descriptor will be used and any others ignored

Media Level Keys

Key	Name	Example	Notes
`m`	Media name and transport	`m=audio 5004 RTP/AVP 98`	■ The example describes an RTP audio flow, port 5004, using dynamic format 98 ■ SMPTE flows typically use a dynamic format in the range 96-127
`c`	Connection data	`c=IN IP4 239.69.22.33/32`	■ Must be specified at media level for redundant flows ■ May be specified at media or session level for non-redundant flows

Media Level Attributes

Attribute	Example	Notes
RTP payload type mapping	`a=rtpmap:98 L24/48000/2`	■ Defines dynamic format 98 as being 24 bit, 48k, 2 channels ■ Dynamic format ID must match value in media description
RTP packet time	`a=ptime:1`	■ Specifies packet as containing 1ms of data ■ This will vary by number of samples per packet
Reference clock	`a=ts-refclk:ptp=IEEE1588-2008:00-11-22-FF-FE-33-44-55:0`	■ Grand master identifier ■ SMPTE requires that this be specified at the media level, even though redundant flows should have the same value for each flow
Clock mapping	`a=mediaclk:direct=0`	■ Must be specified at media level ■ Always has value `direct=0`
Media identifier	`a=mid:prim`	■ Tags a media description with an identifier ■ These identifiers must match the identifiers used in the session level 'group' attribute. If there is no group attribute then it will be ignored.

Other fields and attributes are ignored by Dante devices.

If there is no `a=group:DUP` attribute then the first valid audio media descriptor is used and any further descriptors are ignored. If there is an `a=group:DUP` attribute then only the specified media descriptors are used, and any others are ignored.

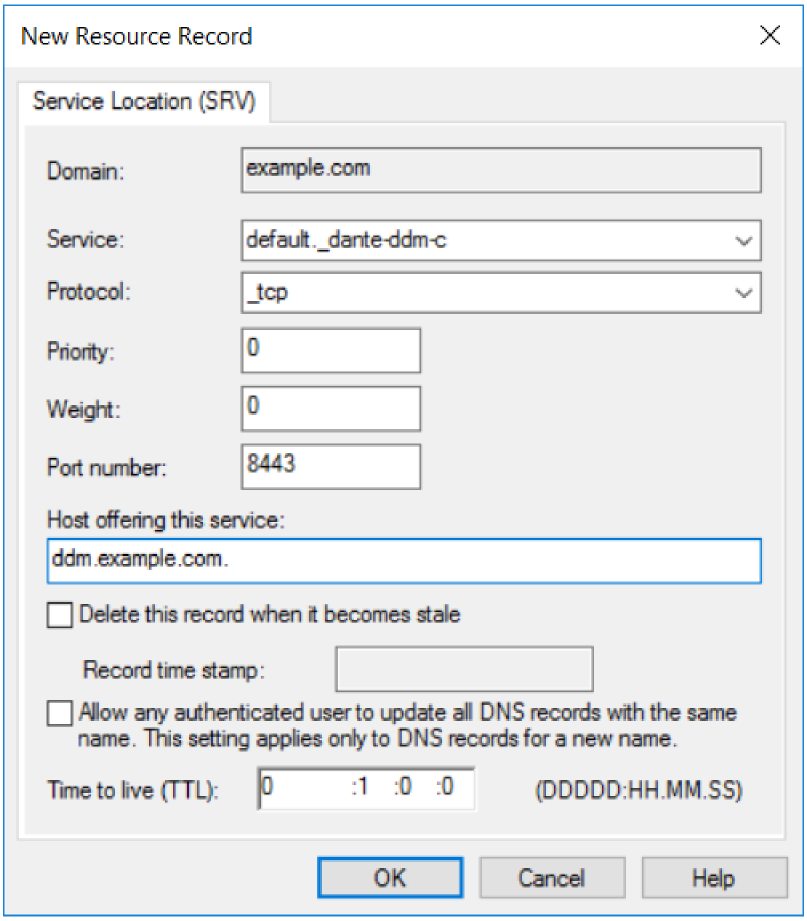
Note: Descriptors that are legal SDP but not well-formed for SMPTE will be silently ignored by Dante Controller and Dante devices.

Windows Server DNS Configuration

An example of how to configure an SRV record at the DNS domain level is shown below.

The instance (`default.`) and service (`_dante-ddm-c._tcp`) are concatenated and entered in the Service field.

When the record has been created, it will reside in a subfolder with the same name as the service, inside the protocol folder - for example, `_tcp\_dante-ddm-c`.



Domain: example.com

Service: default._dante-ddm-c

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 8443

Host offering this service: ddm.example.com.

□ Delete this record when it becomes stale

Record time stamp:

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Installing TLS Certificates on DDM HA Clusters

1. Create a TLS certificate that includes the cluster name, and optionally the DDM node names - for example: ha.yourdomain.com, hanode1.yourdomain.com, hanode2.yourdomain.com (note that the arbiter name is not required). If you need to log directly into an individual node, adding the name for each DDM node will prevent the presentation of security errors in the browser.
2. Install the certificate on the active node during installation.

Note: If the redundant node becomes active, the certificate will automatically propagate to that mode.

Index