Dante®

Securing Dante networks for use with SaaS tools and Dante Director

Moving your traditional AV networks from analog to AV-over-IP is a step that many have been making over the past few decades. The benefits of this shift are widespread and include increased flexibility of signal routing, easy interoperable use of technology from multiple manufacturers, and a significant decrease in the amount of cabling required to complete any task. All of this is enabled by Dante technology built into thousands of devices from hundreds of manufacturers.

Because all these devices are now completely networked, the risks that we once only considered relevant to our computers and other endpoints, are now also applicable to our AV devices. We, as IT and AV professionals, worry about potential hacking, unauthorized access, and even potential negative consequences of well-intended users.

The current approach to AV-over-IP security has been to sequester AV devices on an isolated, separate network that has no access to anything outside the AV network. In many cases, this even means "air-gapping" the network, preventing access to any corporate network or even the internet.

In this paper, we will cover how Dante networks can be made more secure by opening access to the internet for use with emerging tools like Dante Director that provide new benefits for network visibility and security.

Problems with air-gapped networks

An air-gapped network is any network that operates independently, without any access to external networks including the internet. This has been the preferred method of securing AV networks as it limits most access by design.

Creating a completely isolated network (air-gapped) might seem like an easy fix at first, but it actually hinders the development of your AV system. In many cases, it also ignores existing problems that could cause instability and other network issues down the line.

The first issue with an air-gapped network is that most aren't truly 100% separated from the internet. Due to the digital nature of the devices, it is necessary for most devices to receive periodic updates for firmware and software enabling them to function well and maintain optimal security. This can be to fix any software bugs, increase stability, and even maintain current licensing. To serve these needs, most admins will plug into the physical AV network and connect to the internet using the separate WIFI connection – thus breaking the true nature of an air-gaped network.

> While preference to air-gap media traffic, control and configuration signals are often required to bridge the gap to allow mixed-use and control surfaces access to the devices.

Secondly, any AV-over-IP network relies upon the same ethernet and switch types of any other network. If any of these switches, cables or network connections are in open areas where anyone in the vicinity can plug into, the air-gapped network loses its security. Also, depending upon the type of install-location, some networks are at a much higher risk. Take for example universities, music schools, technical colleges, houses of worship and performing arts venues. These institutions have a vested interest in educating students and engaging volunteers to manage AV-over-IP networks. It's a benefit, but also a significant source of potential risk. All it takes is one curious student, or well-intended volunteer to make changes that negatively affect the entire AV network. And in the worst possible cases, the leaking of confidential information can occur over misrouted AV signals.

An additional challenge is that while there is a preference to air-gap media traffic, control and configuration signals are often required to bridge the gap to allow mixed-use and control surfaces access to the devices. VLANs can help here but are more complex to setup and do not offer the level of isolation assumed from a truly air-gapped system.

Finally, when a network is completely isolated, it severs any possibility of observation, monitoring, and management by administrators. The ability to monitor device performance is prohibited, and makes remote diagnosis and repair impossible. Isolation also prevents audit trails from being created which can lead to non-compliance in some regions.

Securing a Dante network and giving access to the internet

Opening your network to the internet is a necessary step to enable advanced management tools like Dante Director. When done properly, it can be more secure than running a local, unmanaged Dante network.

If you have already opened your network to the internet, either by using a network that is converged with the rest of your internet traffic, or directly opening the Dante network itself to the internet, you will also want to take these additional setups to make your network secure from tampering and signal eavesdropping.

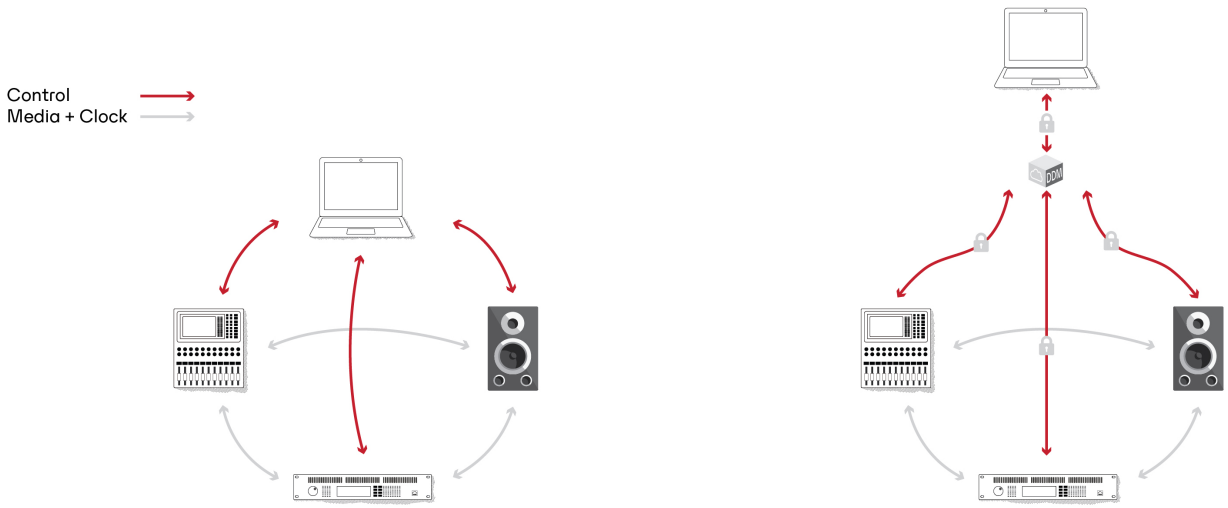
To secure a Dante network:

1. Manage your Dante network by enrolling your devices into a Dante network manager such as Dante Director
2. Open select ports in your firewall and/or switches
3. Restrict traffic to/from known sources
4. Create user accounts and give access to trusted users and admins

Managing your Dante network

There are two types of Dante networks – unmanaged and managed.

The default configuration of Dante networks is unmanaged. In this state, devices send media (audio/video/clock) and signal data between each other. The control data (signal routing and subscriptions, sample rate settings, etc.) can be configured by anyone using Dante Controller.



Unmanaged

Managed

In a managed state, all control data is routed through a separate management application, Dante Director or Dante Domain Manager. When Dante devices are registered with a management application, additional layers of security are added as all control communication for devices is secured and encrypted by the management application. Users are granted access by the Director administrator and are required to authenticate to gain access, and media communication continues to flow between devices as defined in the management application.

Managing a Dante network prevents any inadvertent or malicious changes. All user actions and changes to the Dante network are logged by Dante Director, ensuring full ability to trace any network changes back to specific users and the time of any change.

Additionally, only specific URLs and ports are required to be opened in any firewall that provides access to your Dante network. The traffic to that port can also be restricted to a scope and range. This ensures that only valid, control signals are entering and exiting your network as required.

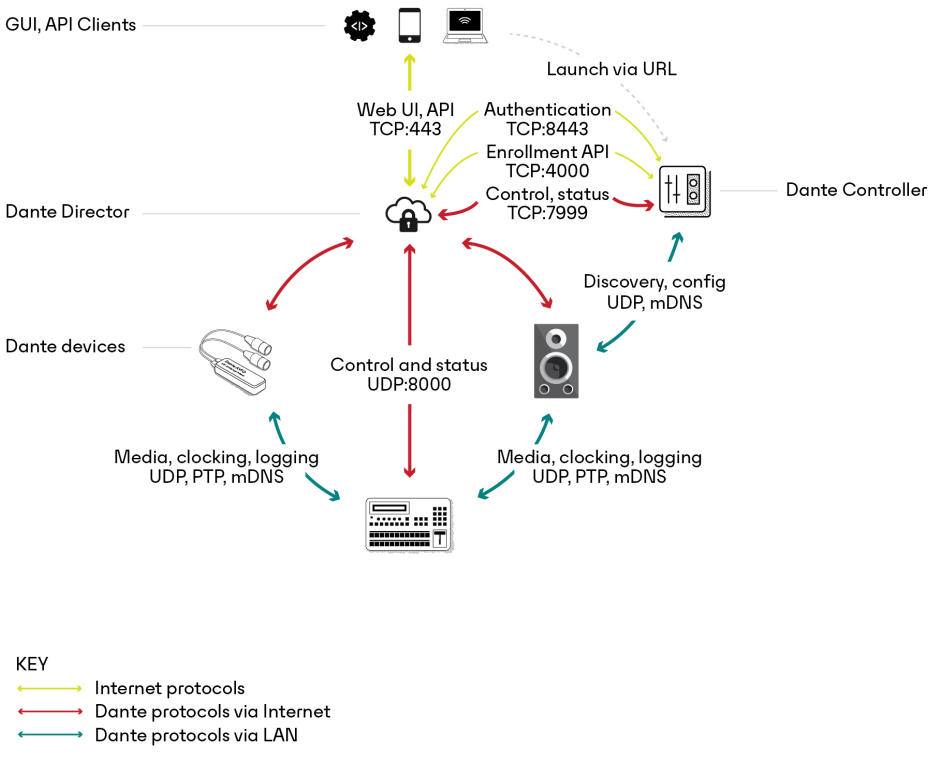
Managing your network with Dante Director

For the initial setup of Dante Director, when enrolling devices your computer with Dante Controller running will need to be connected to the same local network subnet as your Dante devices. It is possible to use another network – corporate WIFI, cellular, etc. – to give your computer access to is enroll devices in Director, if you want to restrict access to your device network. This direct access is only required for the computer, and only required during device enrollment. All access post-setup can be done via the internet.

To enroll Dante devices into Dante Director:

1. Connect all Dante devices into the AV switches
2. Plug computer with Dante Controller into the same subnet as your Dante devices
3. Ensure that your computer has access to Dante Director on ports 8443, 4000 and 7999
4. Enroll devices into Dante Director
5. Ensure Port 8000 is open in the firewall that connects your Dante network to the internet
6. It is now safe to unplug your computer from the subnet and manage your Dante network using Dante Director from any internet connection.

Scenario: Device Enrollment with Dante Controller



Opening ports in your firewall

When opening an air-gapped AV network to the internet, ensuring your approach meets the security needs of your organization is imperative.

Whether you use a hardware or software firewall, or do port filtering at the network switch level, understanding the ports necessary is the first step. Most SaaS applications, including Dante Director, will include the necessary information in their product documentation, wiring diagrams and other support repositariesrepositories.

The following is a list of ports used by Dante Director and associated applications. These ports can also be found in the diagrams included in this document.

The only port that is absolutely required for Dante Director after devices have been enrolled is Port 8000. If you intend to add new devices using Dante Controller, and access the other resourcesresources, you need to open the additional ports listed below.

Ports and URLs used be Dante Director GUI and API		
Address	Port	Usage
director.dante.cloud	TCP 443	Web user interface
api.director.dante.cloud	TCP 443	External GraphQL API clients
Ports and URLs used by devices enrolled in Dante Director		
device.director.dante.cloud IP: 15.197.156.165 or 3.33.153.19	UDP 8000	Device communications with Dante Director
Ports and URLs used by Dante Controller when used with Dante Director		
device.director.dante.cloud	TCP 8443	Dante Controller authentication to Dante Director
device.director.dante.cloud	TCP 7999	Dante Controller communications with Dante Director
api.director.dante.cloud	TCP 4000	Dante Controller API access to Dante Director
Ports and URLs for other resources		
www.audinate.com	TCP 443	FAQs
my.audinate.com	TCP 443	Dante Controller download
dev.audinate.com	TCP 443	User guide
audinate.onfastspring.com	TCP 443	Account subscriptions

Device security and control data

Dante is designed with security at its core. The latest Dante hardware devices are built with secure bootup and secure firmware updates from Dante Updater. Control data that is transferred between Dante devices, and to Dante Director is encrypted in transit. This ensures that control data cannot be intercepted, spoofed, or manipulated in transit, guaranteeing the integrity of the network configuration and preventing the redirection of media to or from unintended endpoints.

Restricting traffic based on source

By only opening specific ports in your firewall, you are already restricting access down to only specific areas that can be closely monitored. To add an additional layer of security, you may want to restrict traffic to only known sources.

For example, if you are using Dante Director, after you have enrolled all your devices, you can restrict traffic for port 8000 to only allow only Dante Director to communicate with your Dante network.

To restrict traffic to Dante Director only, set https://director.dante.cloud/ as the source for all traffic on port 8000.

Keep in mind, if you need to enroll additional devices while plugged into your Dante network, you will need to have additional ports open for Dante Controller outbound communication to Dante Director. All remote access for Dante Director and Dante controller comes in on port 8000, but outbound communication while plugged in to the network needs additional ports listed in the chart above.

Enabling user access controls

Dante Director enables the restriction of access for management of the AV network to only approved users. This is done via the creation of user accounts on within Dante Director and then granting restricted access only to necessary sites.

What might seem like a small change provides quite a large benefit. Traditionally AV network signal routing, monitoring and control has been provided through an application such as Dante Controller. As this is a free application, anyone can download it and use it to modify Dante networks. The plug-and-play nature of Dante Controller provides ease of use for many new AV-over-IP users, however, the unrestricted access can quickly become a potential security nightmare for growing systems.

By enabling user access controls, tools like Dante Controller now require login to access or modify any signal routing. Any networks and devices the user doesn't have access to are now unavailable and remain in their current state until an authorized user logs in to make changes.

Users are restricted and only allowed to manage specific sites granted by the administrator. This way, team members can be assigned specific areas of management, preventing unintentional changes to your network.

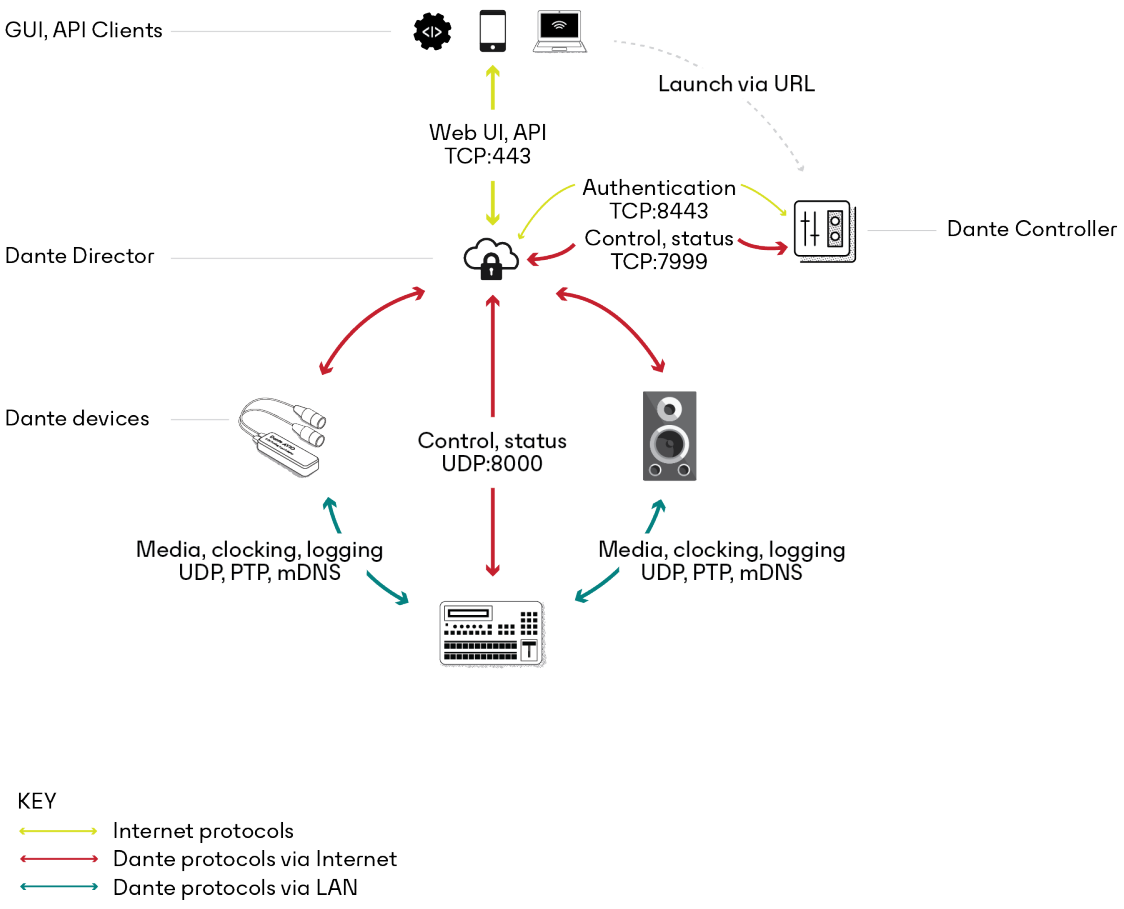
Dante Director enables the restriction of access for management of the AV network to only approved users.

Managing Dante networks with Dante Director after device enrollment

After you have enrolled devices in a Dante network into Dante Director, there is only one port required for devices to access the internet, Port 8000. All the traffic to control the network using Dante Director will be routed through this port. This includes any management using Dante Controller on the remote computer. The remote computer will need access to a few additional ports to access Dante Director itself, but this is all passed through port 8000 by Director to the devices.

As mentioned previously, if you need to plug-in directly into your local subnets, there will be additional ports required for outbound communication by Dante Controller and other applications. Of course, this all depends upon your security posture, and can be managed at the firewall or switch level.

Standard use of Dante Director paired with Dante Controller



Advantages of working with SaaS products

Software as a service (SaaS) products like Dante Director are the next evolution that is coming to the AV industry. Working with SaaS products gives you many benefits over more traditional models of software deployment.

Some of these benefits include:

- The fast setup and configuration of a service without the need to spin up your own servers, containers or hypervisors before utilizing the application.
- Regular feature improvements that can be introduced and adopted more quickly than waiting for a traditional software release cycle.
- Frequent quality control updates to cloud-applications.
- A shared responsibility model for software security and compliance, where the software vendor is responsible for the security of the application, leaving you to only address local concerns.
- An escape from costly, regular hardware refresh cycles and ongoing maintenance for hardware that may not directly support your project's end goals.

Conclusion

Dante Director and other SaaS tools can provide many benefits to the management, monitoring and upkeep of your AV networks. With some planning, your network can be even more secure and manageable than ever before. For further information, please refer to these online resources.

- Dante Director FAQs – quick answers to common questions
- Dante Professional Services – need some extra help? Contract with Audinate for custom training and expert advice.
- Dante Managed API – extend your Dante network with custom integrations
- Dante Director Support – contact us and submit a support request

READY TO REMOTELY MANAGE YOUR DANTE NETWORK?
TRY DANTE DIRECTOR FREE FOR 30 DAYS >