# MXE5 Security Precautions

At Dynacord, we understand the critical importance of cybersecurity in today's digital landscape. We recognize that securing a network, its devices, and the services it supports requires active participation from the entire supply chain and end-user organizations. Therefore, we are committed to providing our customers with the necessary resources and information to create a secure and resilient environment.

The MXE5 is a digital audio matrix that is designed for use in professional audio applications. It has a wide range of features, including many input and output channels and various mixing modes. Furthermore, it can act as a central place to aggregate and distribute control data in the network. Depending on the use case, you might want to implement just a subset or more than the given security measures. The first chapters of this guide elaborate on the various security controls that you should consider. In the second step, some best practices are mentioned.

# 1 Generic Security Controls

## *1.1 Physical Security*

The first step in ensuring the security of the Dynacord MXE5 is to ensure that it is physically secure. This also holds for other equipment being used in the system which is attached to the Dynacord MXE5. This means that devices should be kept in a secure location, and access to the device should be restricted to authorized personnel as much as possible. Consider using locks or other physical security measures to prevent unauthorized access to the device.

## *1.2 Network Security*

The Dynacord MXE5 is designed to be connected to a network, which means that it is vulnerable to various network-based attacks.

Security should be built up in layers. In security sensitive applications, network security is crucial: its main goal is to prevent unauthorized access to the environment. Only when unauthorized access has been gained through the network security layers, the security of the MXE5 and system itself (including hardening of the operating system, system authentication, and encryption) become important. This section describes several methods to harden the network and provide logical intrusion detection.

### 1.2.1 VLANs

Virtual Local Area Networks (VLAN) increase network security by isolating network traffic and limiting access to specific areas of the network by

- Segmenting the network: VLANs segment the network into smaller, more manageable subnets, which can help to reduce the impact of attacks and limit the spread of malicious traffic (e.g., DOS attacks).

- Controlling access: VLANs control access to network resources by limiting which users or devices can access certain VLANs. For example, a VLAN can be created specifically for servers, and only authorized users or devices can be allowed to access that VLAN.
- Enhance monitoring: By segmenting the network using VLANs, network administrators can more easily monitor network traffic and detect any unauthorized access or suspicious activity.

### 1.2.2 ACLs

An Access Control List (ACL) acts as a simplified firewall and allows system administrators to set rules for limiting the communication between network endpoints. Access control lists can be configured on most managed network equipment. It is recommended to check the product datasheet for the exact specifications.

An example rule: “192.168.0.3 can communicate to 192.168.0.254 using port 3260”. Communication on all other ports is prohibited.

Most access lists end with a "deny all other traffic" statement to provide a very good first layer of defense against unauthorized network access by restricting the communication in the network.

### 1.2.3 MAC ACLs

A MAC Access Control List (MAC ACL) can be used in conjunction with VLANs to provide an additional layer of security to the network. MAC ACLs allows network administrators to control which devices are allowed or denied access to the network based on their MAC address.

When using VLANs, MAC ACLs can be applied to specific VLANs to further restrict access to the resources within that VLAN. For example, if a particular VLAN is dedicated to sensitive data, a MAC ACL can be created to only allow devices with authorized MAC addresses to access that VLAN.

MAC ACLs can be configured on most managed network equipment and are applied to a specific port or VLAN. When a device attempts to access the network through that port or VLAN, the switch or router checks the device's MAC address against the MAC ACL to determine if it is allowed or denied access.

### 1.2.4 Firewalls

A firewall has a similar function as an access control list: it restricts network traffic between network endpoints. On top of what an access control list can do, a firewall typically also performs "packet inspection". This allows a firewall to look at the content of the network traffic, verify if the right protocol is used, and if the traffic is matching the protocol specifications. As a result, it is not only able to check if, for example, traffic on port 3260 between the device and other devices is allowed, but it is also able to check if the traffic matches the specification of the used protocol. Firewalls can be deployed as software only packages or combined hardware and software appliances. Well-known vendors include Cisco, Juniper Networks and Checkpoint.

### 1.2.5 IDS/IPS

Intrusion Detection and Prevention systems (IDS/IPS) go one step further compared to firewalls. These systems act as a "virus scanner" on the network. They can detect and block known, and unknown attack methods based on the signature and behavior of a specific attack. These

systems can perform deep analysis of network traffic. Well known vendors include McAfee, Cisco, Trend Micro and Fire Eye.

## *1.3 Software Security*

The firmware running on the Dynacord MXE5 should be kept up to date with the most recently provided Dynacord firmware. Please take the according release notes into account.

# 2 Best Practices

## *2.1 Generic Best Practices*

### 2.1.1 Principle of Least Privilege

The Principle of Least Privilege (PoLP) in this context means giving a user or a device only those privileges which are essential to perform its intended purpose. For example, adding the common ACL rule “deny all other traffic” as a last statement implements this principle. Apply this principle to all applicable security controls to gain maximum system security and stability.

### 2.1.2 Limit internet access

Do not connect the system to the internet or open ports to the internet. The systems are designed to being used in local networks without being exposed to the internet. If remote support is required for your setup, please integrate appropriate security measures according to your security needs.

### 2.1.3 Decommissioning

When you sell or decommission the device, make sure to factory reset the device to clear all confidential data including configuration and passwords of third-party APIs.

### 2.1.4 Port security

It is recommended to disable unused ports of network switches to avoid the possibility that equipment is connected that may compromise the system.

### 2.1.5 Wall panels

Wall panels are usually accessible by unauthorized people, and it is easy to gain access to that specific network port.

Therefore, when using wall panels, we highly recommend using MAC-based VLAN assignment, which assigns the panel to a different VLAN depending on its MAC. Ideally combine this with a port security scheme like shutdown: when an unauthorized device attempts to connect to the port, the switch should automatically disable the port, effectively preventing any traffic from passing through it. Furthermore, restrict the allowed MAC addresses on that port only to the wall panel and to one single MAC address. This avoids attacks where a network hub is used to bypass that mechanism.

Finally, consider filtering out Dante traffic on that port, as Dante is inherently unsecure and not required by wall panels.

Also, use the PIN feature of the wall panels to control access to elevated actions and systems.

## *2.2 MXE specific Best Practices*

### 2.2.1 Lock Dante Ports

Unsecure Dante or AES67 audio connections are used both as inputs and as outputs. These Dante and AES67 connections are not authenticated and not encrypted. They form a security risk, as no precautions are taken against malicious or accidental attacks through their network interfaces.

Only Dante devices that support Device Lock should be used. Device Lock allows you to lock and unlock supported Dante devices through a 4-digit PIN (Personal Identification Number).

Make sure that the devices are locked when in normal operation. The Dante Controller is needed to set the PIN and set up the connections. Alternatively, use the Dante Domain Manager.

### 2.2.2 Disable HTTP API

The MXE5 comes with a built-in HTTP / HTTPs API. This can be activated / deactivated using the front panel display. If you do not use the HTTP API in your application, it is best practice to have it deactivated.

### 2.2.3 MXE5 in general

If the setup in which the MXE5 participates in has security needs, please be aware that the wall panels and MXE5 do not take any special precautions against malicious attacks. Therefore, consider implementing network security as described in the following chapter. Note: In general, we consider systems security relevant, where a lot of people are addressed.

### 2.2.4 MXE5 in combination with PROMATRIX systems

When using the MXE5 as interface between PROMATRIX systems you must consider the security precautions of all systems. The PROMATRIX 9000 precaution guide can be downloaded from the official documents page of the PROMATRIX 9000 controller.

Be aware that PROMATRIX 8000 / 6000 and MXE5 offer maximum compatibility with all networked audio devices to allow for fast and easy setup and maintenance on the network. This means that these devices do not take any special precautions against malicious or accidental attacks via their network interfaces.

It is strongly recommended to use it in a safe and isolated network, meaning that no untrusted and unknown parties and hardware components can get access to the network. Furthermore, all parties of the network should not be connected to the internet or bridged to other networks.

An isolated network in this context is defined as a network that is neither logically nor physically accessible to untrusted parties. In this specific case an isolated network is given if:

- Access to all network ports and devices are physically restricted
- And for those ports and devices which are accessible to untrusted parties, there is a logical access restriction to the network / device

Devices at the network's physical edge are susceptible to attacks. Especially wall panels or call stations are mostly installed in places that are accessible to the public. As these devices must be connected to the same network to work properly, this also increases the risk of unwanted access to the network: people could try to disconnect the device and connect their own equipment to try to gain access to the network. Therefore, when using the MXE5 in a life safety critical system, it is highly suggested to take specific security controls into account to keep the network isolated:

- Physically secure the wall panels by mounting them e.g., with RESISTORX screws
- For the ports of the switch used for wall panels, use port security and ACLs:
    - Only allow the MAC address of the wall panel on the port of the switch
    - If another MAC address appears, turn off the port
    - To address MAC spoofing, consider using a TCL script which automatically turns off ports which are marked as temporarily unused. This is the case when an attacker wants to spoof the MAC address. Reactivating the port should be done manually on a PC residing in a physically secured place. This ensures that an attacker does not get automatic access to the network after spoofing the MAC.
- Use firmware version >= 1.2.6 for the TPC-1 as it disables the USB port
- Use separate VLANS for touch and wall panels or other IP-based control devices which are physically accessible in public areas.

Additional layers of security (next to keeping the system isolated) should also be considered:

- Use a firewall
- Introduce intrusion prevention systems
- Enable DHCP snooping

It is also recommended As Dante is inherently insecure, make sure to filter all Dante (control / audio) traffic on ports used for the wall panels in both directions. Furthermore, restrict traffic to and from various devices:

| Origin | Destination | Destination Port | Protocol |
|---|---|---|---|
| WPN-1 | MXE5 | 27999 | TCP / WebSocket (Proprietary) |
| TPC-1 | MXE5 | 55555 / 55556 | TCP / OCA |
| TPC-1 / WPN-1 / MXE5 | TPC-1 / WPN-1 / MXE5 | 5353 | UDP / MDNS (Multicast) |

| | | | |
|---|---|---|---|
| MXE5 | PROMATRIX 6000 / 8000 | 6271 | DCP / TCP |
| MXE5 | PROMATRIX 9000 | 9403 | OpenInterface / TCP |
| | | | |
| | | | |

# 3 Document History

| Version | Date | Description / Changes |
|---|---|---|
| V1.0 | June 2023 | Initial Release for MXE5 Firmware 1.4 |