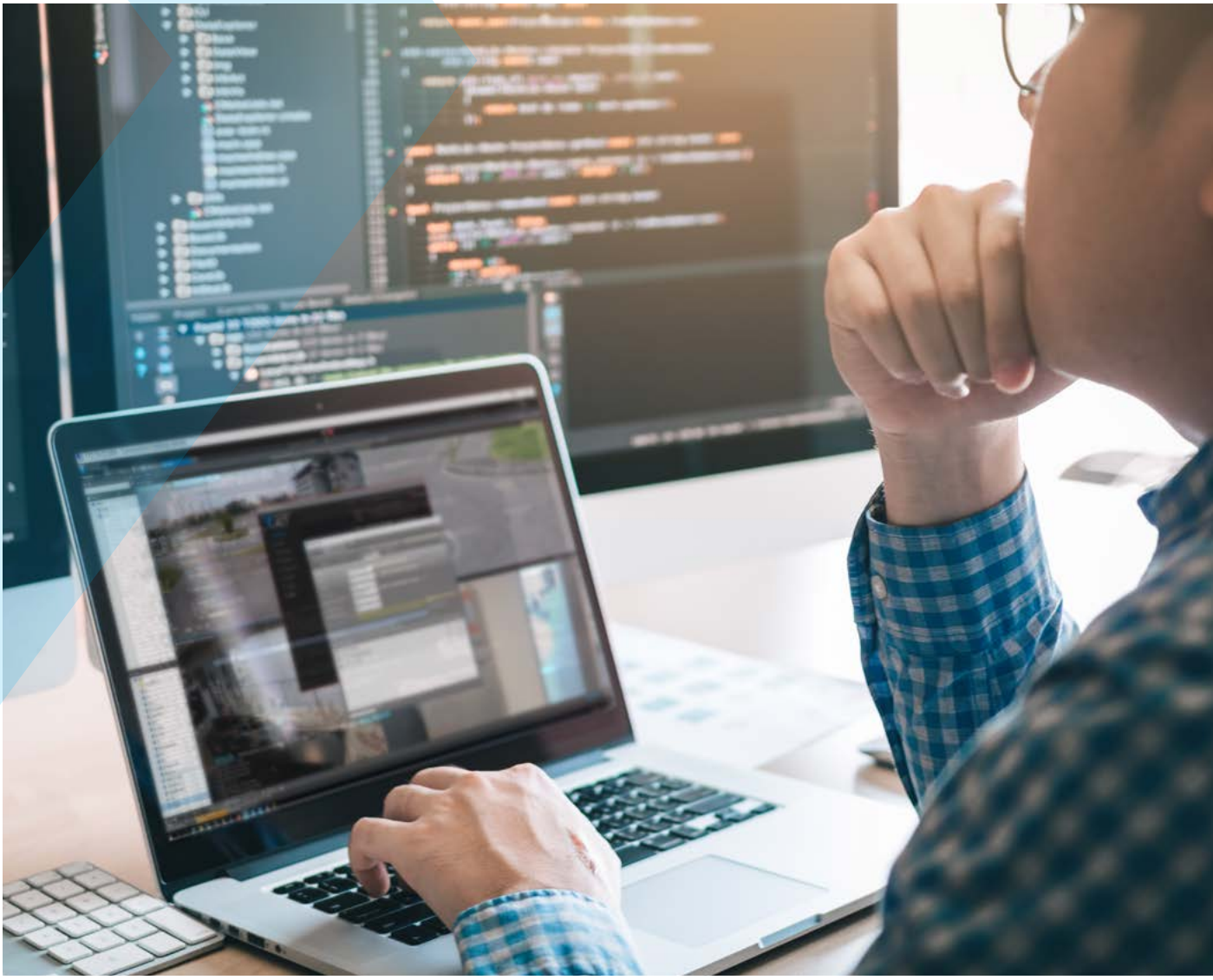


TECH TIP

Connecting Geographic-Wide IP Video Surveillance Installations

MARCH networks

Introduction

Deploying an IP video surveillance system across multiple distributed locations can be challenging. Without an adequate system design, performance can degrade, small tasks can become time-consuming and the cost to manage the system can escalate.

March Networks® adopts a centralized architecture when managing multiple sites and March Networks Command™ Enterprise Software (CES) is the core of the solution. Once a network video recorder (NVR) is registered to CES, all video surveillance-related resources get stored inside a common database: CES is the entity granting authenticated user access to such resources.

Here is a simplified diagram showing the data path for a user starting a video-related investigation on video captured from an on-premises NVR.

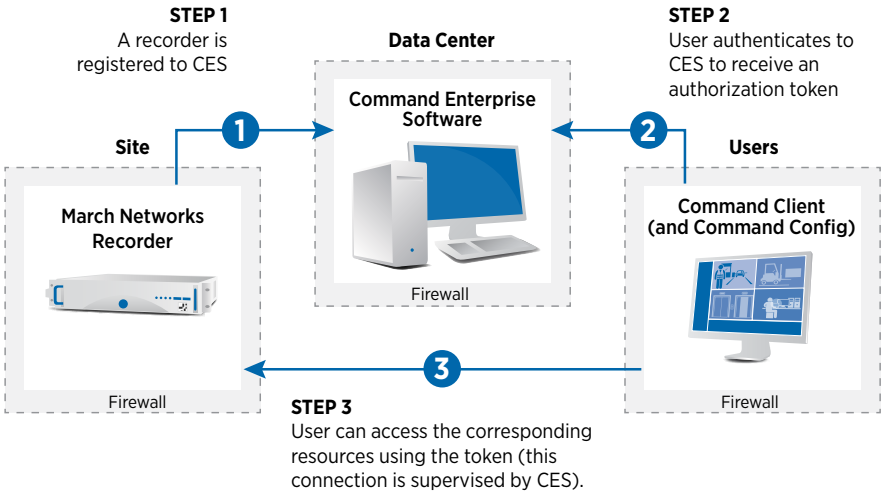


Figure 1: Command Enterprise Software is the core of the March Networks solution. CES provides access tokens to authenticated users.

Creating a successful and efficient geographic-wide video surveillance installation requires proper network design and configuration to ensure any user can easily access the required resources with minimal latency.

Network Topologies

It's possible to connect all the components of the video surveillance system in different ways, but each system design has a different impact on performance. Some designs are also more complex to configure. Let's take a look at the various options:

Option 1: Port forwarding

The following figure illustrates the required ports to be opened by an IT department in order to have a successful communication between device components.

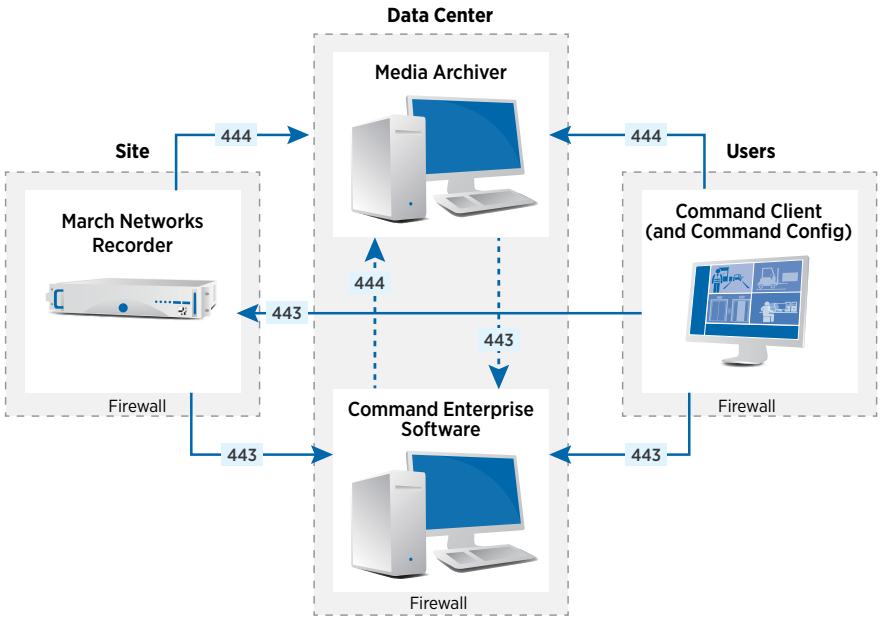


Figure 2: Network port details for each module composing the solution. Applies to Command Solution 2.7 or higher. March Networks Media Archiver, being part of any March Networks CES installation, has been included in the diagram to offer a more exhaustive overview.

This approach will require each recorder to have local port 443 translated to a published address using the Network tab settings in March Networks Command Client. This setting is available once you are locally connected to the recorder with Command Client.

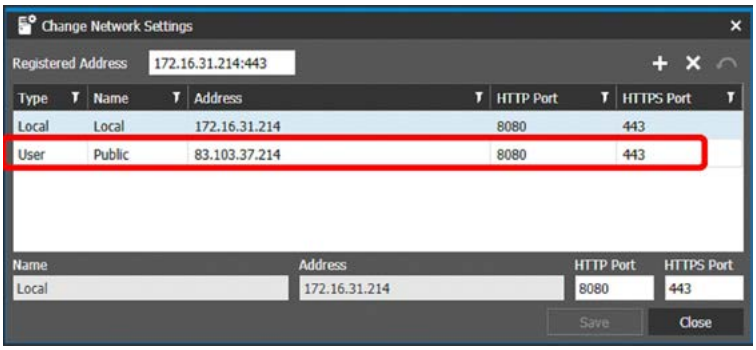


Figure 3: Adding the published address to each recorder using the "Change Network Settings" feature. From Command Client version 2.7 the HTTP port is optional. In this example, we use the original 443 value but it can be changed to match network requirements.

The next step is to open CES Management Console, navigate to the Network tab and add the public address(es) of the CES server:

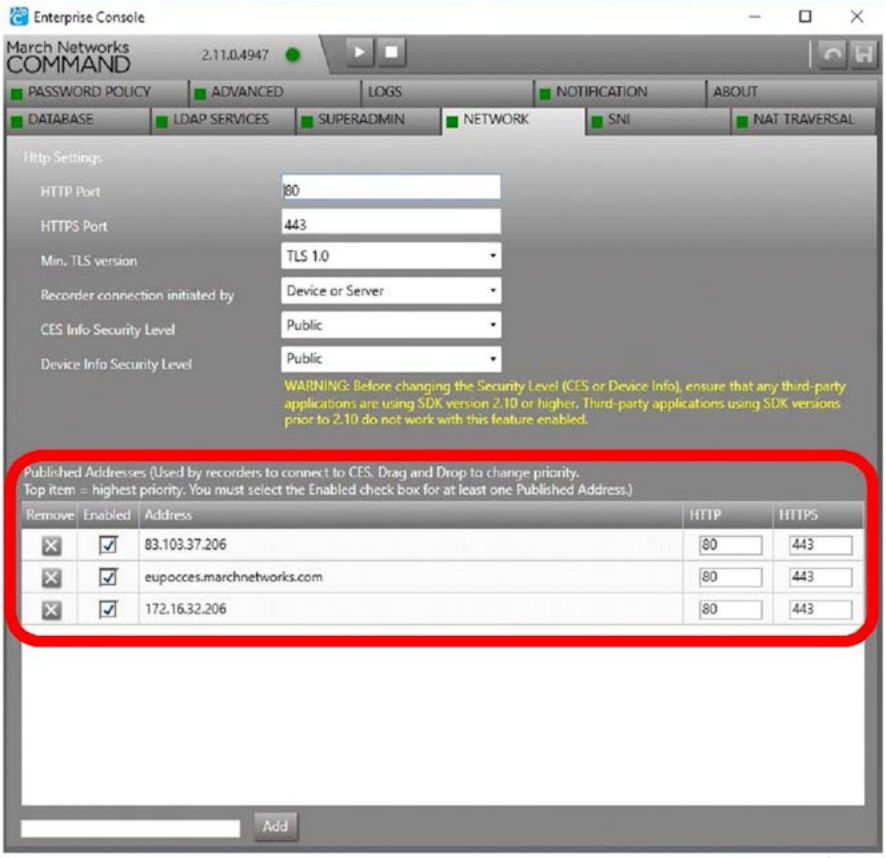


Figure 4: CES Management Console. Here it's necessary to add the public address for the CES server, specifying the priority. Those values are passed to each recorder during the registration process or when CES/NVR reboots (ensure "Recorder connection initiated by" is set to "Device or Server").

In this way, each recorder will keep the full list of CES addresses and will try connecting to CES starting from the one with higher priority. It's possible to check the address list has been successfully passed to each NVR, as displayed in the following picture.

```
system.ready: true
system.ready.connected: true
system.ready.details: true
system.ready.registrationDetails: true
system.ready.ssl: true
system.ready.gateway.mobile: true
system.details.id: 344
system.details.manufacturer: 1
system.details.family: 257
system.details.model: 8
system.details.serial: AR1336P196
system.details.version: 5.19.0.0132
system.details.stationId: NVR-344
system.details.patchList: FPGA:23:2.3,EvidenceReviewerCD:
   050709.0126:5.7.9.0126
system.interface.1: Public
system.interface.1.address: 83.103.37.214
system.interface.1.httpPort: 8080
system.interface.1.httpsPort: 443
system.registration.enabled: true
system.registration.currentEndpoint: https://83.103.37.203:443
system.registration.endpoints: https://83.103.37.203:443,
   https://172.16.32.203:443, https://ces.marchnetworks.com:443,
   http://83.103.37.203:80, http://172.16.32.203:80,
   http://ces.marchnetworks.com:80
system.registration.server: 83.103.37.203:80
system.registration.addresses: 83.103.37.203:80, 172.16.32.203:80,
   ces.marchnetworks.com:80
system.registration.deviceId: 344
system.interface.httpPort: 8080
system.interface.httpsPort: 443
system.interface.streamPort: 8080
system.interface.secureStreamPort: 443
system.interface.version: 100.0.0.1385
system.interface.build: 2.11.0.1385
system.interface.api.version: 100.0.2.1385
system.productname:
agentmediaport: 8080
system.interface.wdport1: 80
system.interface.wdport2: 2804
_hash: nD52gzeBimUwJ+tV1CZGGUHu9Go=
```

Figure 5: If "Device info Security Level" is set to Public in CES Management Console, it's possible to query each recorder using http://NVR_IP/info to collect useful details about NVR status, including the full list of CES addresses.

To complete the configuration, it will be necessary to implement NAT port forwarding rules for each recorder and CES Server.

Table 1: Assuming two separate public IP are available, it's possible to map LAN port 443 to WAN port 443 for both CES and recorder. In case this is not possible, those values can be adjusted simply editing the highlighted networks panels.

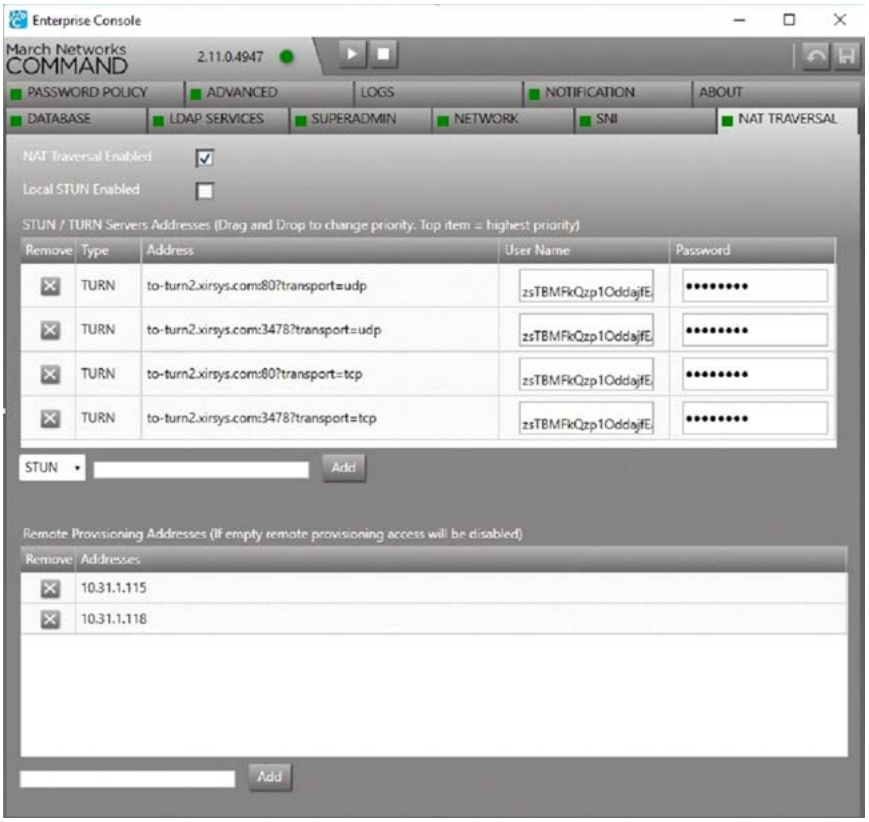
Device	LAN IP	LAN Port	WAN IP	WAN Port
CES	172.16.32.206	443	83.103.37.206	443
NVR	172.16.31.214	443	83.103.37.214	443

This approach offers the best performance in terms of video latency and system responsiveness. No additional resources are required to connect the various components of the system. The main disadvantage is the requirement to create a specific NAT rule for any device and this can be problematic when handling hundreds or thousands of recorders. There are situations where this approach is impossible to implement, so, for such scenarios, it's necessary to explore alternatives.

Option 2: NAT Traversal using STUN/TURN service

Introducing a STUN or TURN server removes the necessity to create port forwarding rules for each recorder. This greatly simplifies the network's configuration, but introduces an additional element in the architecture, which causes a significant degradation in terms of system performance and latency. STUN or TURN services need to be configured inside March Networks Command's Enterprise Management console:

Figure 6: Command Enterprise Version 2.7 or higher has the NAT TRAVERSAL tab to configure STUN or TURN services. Here it's possible to enable local STUN services or third-party STUN/TURN services.



The way STUN and TURN services operate is quite different:

STUN service acts as an operator that bridges connections between devices, establishing peer-to-peer bi-directional communication. STUN protocol relies on UDP packets to establish the connection so this has to be considered when discussing the solution with IT, to ensure no rule is in place preventing this kind of protocol to propagate inside the network. STUN resources are usually free of charge and CES itself offers an embedded STUN service which can be enabled inside the Enterprise Management Console (UDP traffic is routed by default on port 3478). In addition, it's possible to use Google STUN services, further reducing the rules to put in place.

TURN service acts as a "Relay" between the Command Client and recorders. This type of service is offered by several third-party companies for a monthly fee and requires custom ports to be opened, depending on the selected operator.
The following diagram offers an overview of the network resources to be considered when introducing STUN/TURN services:

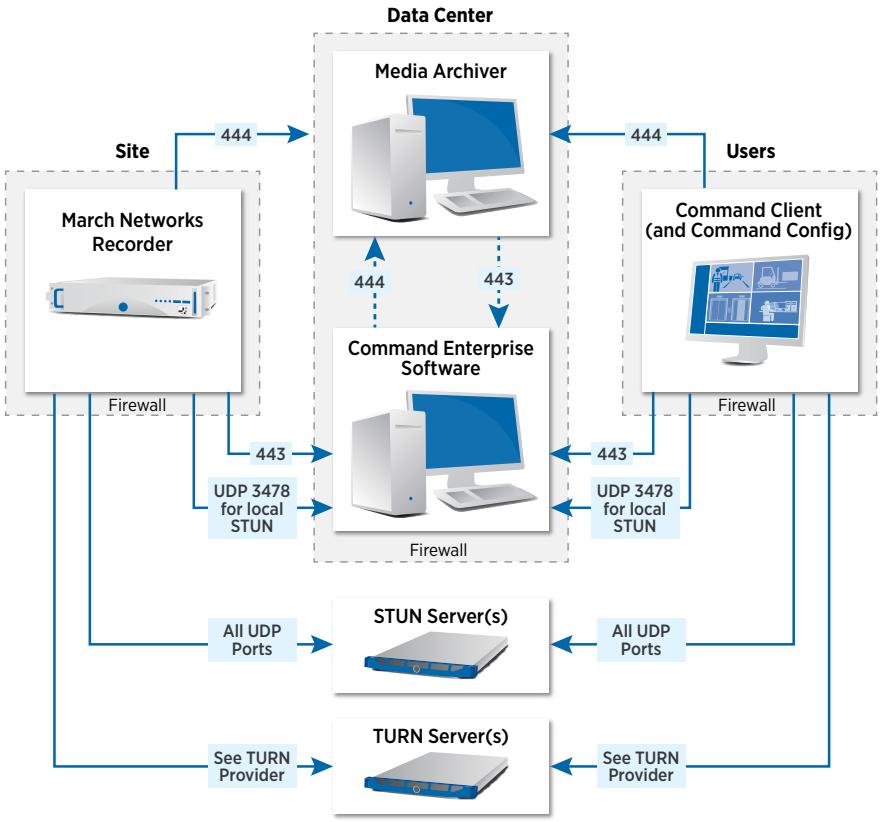


Figure 7: Network architecture when introducing STUN or TURN services. The CES server still need to be published/accessible from the client PC but no direct connection between Client and recorder is necessary. All video-related traffic is handled by the STUN/TURN server.

A couple of summary notes:

1. If you enable NAT Traversal but leave the "port forwarding rules" in place on the firewall for the recorder, the Client will continue to use the "direct connection" method. The Client will only fall back to a NAT Traversal connection, when unable to reach the recorder over the direct connection.

2. Bandwidth requirements may be huge when transferring video content, especially when multiple cameras are investigated in parallel. This can quickly saturate available resources, so this approach is not recommended for control rooms requiring 24/7 video availability. Port forwarding is still the best option for this kind of application. However, assuming the user has only sporadic video requests, the NAT traversal approach can potentially offer more protection against cyber-attacks since no permanent port needs to be opened for any of the recorders.

Option 3: Creating VPN tunneling between the NVR, CES and Clients

Creating a VPN to connect all video surveillance resources would remove the necessity to publish addresses or adopt STUN/TURN servers. This option is at the discretion of the end user's IT department to implement, and for this reason is not covered in this document. This solution represents a valid alternative for transit installations where LTE or Wi-Fi is used to connect mobile equipment with central servers since the encryption layer introduced by VPN increases the security against cyber-attacks.

In terms of performance, VPN architecture should offer adequate performance, but it is slightly degraded compared to port forwarding due to the additional layer introduced by VPN protocols.

Conclusions

Different methods have been presented to implement connectivity for a geographic-wide video surveillance installation. When possible, standard port forwarding offers the best performance and reduced latency, so this should be the way to go, unless your IT department can't implement port forwarding rules. In this scenario, NAT Traversal or VPN can offer alternate ways to establish connectivity between the device components, but this has some drawbacks to consider, both in terms of reduced performance (STUN/TURN), cost (TURN/VPN) and complexity (VPN).

Company Overview

March Networks® helps organizations transform video into business intelligence through the integration of surveillance video, analytics, and data from business systems and IoT devices. Companies worldwide use our software solutions to improve efficiency and compliance, reduce losses and risk, enhance customer service and compete more successfully. With deep roots in video security and networking, March Networks is also recognized as the leader in scalable, enterprise-class video management and hosted services. We are proud to work with many of the world's largest financial institutions, retail brands, cannabis operators and transit authorities, and deliver our software and systems through an extensive distribution and partner network in more than 70 countries. Founded in 2000, March Networks is headquartered in Ottawa, Ontario, Canada. For more information, please visit **www.marchnetworks.com**.

Please contact March Networks' sales engineering team for further details. They will work together with you to identify the best option for your specific business requirements.

Customer Support and Assistance

North America, South America, & Australia

Direct: 1.613.591.1441

Toll Free (US & Canada): 1.800.472. 0116

E-mail: techsupport@marchnetworks.com

EMEA

Direct: +39 0362 17935 ext. 3 (CET)

E-mail: emeatechsupport@marchnetworks.com

Middle East & Africa

Direct: +00 971(0)52 818 8483

Email: supportmea@marchnetworks.com