Linear® Managed Access Control

A remote access capability integrated into the E3-Series web server (client) provides secure, authenticated remote access control system management, and Recurring Monthly Revenue (RMR) generation for dealers.

Linear's Remote Management Console (RMC) is designed to provide secure connectivity to E3-Series access control systems that are located behind a NAT router or firewall, or those without a public IP address.

Browser-based user interfaces are state-of-the-art in today's embedded systems. These user interfaces make configuration, control and monitoring of a system from every PC, smart phone or tablet device that can run a web browser possible. Thanks to today's web browsers equipped with JavaScript and Ajax technologies, browser-based user interfaces are powerful, visually attractive and easy to use.

Many browser-based interfaces require only a HTTP(S) connection between the web browser and the associated web server to which a person is connecting, thus they are perfectly fitted for remote access situations. However, for this to work, the web browser interface must be able to create a network connection to the web server. This is typically only possible if the device serving up the browser interface is located on the same network as the device running the web browser. If the networks containing the client and server are linked, or if the device can be directly reached over the internet then the connection is possible.

Unfortunately in real-life situations, this is often not the case. Embedded devices in the field are often connected to private networks behind routers employing network address translation (NAT) or firewalls. This is especially true for consumer electronics devices like set-top-boxes, home automation devices or smart meters, which are usually located behind a NAT broadband router.

Even devices connected to a wireless network such as GSM/GPRS or UMTS most often do not have fixed, public IP addresses and thus are not directly reachable. This means that while these devices can open connections to servers on the internet, it is not possible to access the equipment's web server from outside the network, unless additional measures are taken.

INTERNET-BASED REMOTE ACCESS TO E3-Series systems / RMC Clients

Port forwarding and Virtual Private Networks (VPN) are well-known, established technologies for enabling internet-based remote access to computers and networked equipment behind NAT routers or firewalls. However as detailed in the table below, both technologies have significant drawbacks when being used with browser-based systems.

For this reason, Linear has developed a superior alternative to port forwarding and VPN, referred to as the Remote Management Console method. RMC enables easy and secure remote access to the web server of its E3-Series equipment, even if the device is located in a private or mobile network behind a NAT router or firewall. How this technology works will be explained in the following section.

How Remote Management Console (RMC) Works

RMC is based on an extension of the well-known and proven HTTP protocol that drives the internet. The main difference between standard HTTP connections has to do with whether the client or server is setting up the network connection used for sending HTTP requests and receiving their responses. In traditional HTTP connections, the client (web browser) is responsible for opening a connection to the equipment's web server, over which it then sends the requests.

With RMC, however, it's the E3-Series panel equipment that establishes the HTTP network connection, using its RMC app software. Since the equipment does not know the IP address of its respective clients, and would not even be able to create a direct network connection to each client due to the fact that clients are usually

separated from the E3-Series server by a NAT router or firewall, the E3-Series RMC software app opens a connection to a uniquely-engineered dedicated server called the RMC Server. For this to work, the RMC Server must be accessible over the internet by the E3-Series equipment that contains the web server providing the system's browser-based interface.

Once a connection between the E3-Series panel equipment (with its RMC client app software) and the RMC Server has been established, the RMC Server uses this connection to send ("tunnel") HTTP requests to the panel equipment.

Where do these HTTP requests come from? The RMC Server also contains a normal HTTP server, which accepts requests from web browsers, such as outside-the-network browsers (smart phones, PCs, tablets, etc.). These requests are then simply forwarded to the E3-Series panel equipment, using the tunnel connection between the RMC Server and the RMC client app on the panel equipment.

Setting up the initial tunnel connection between the E3-Series equipment, RMC client app software and the RMC Server is almost always possible as long as the device can access the internet. It will typically even work if the only available internet connection is through a HTTP proxy server. The tunnel connection uses the standard Web Socket protocol, which makes it firewall- and proxy-friendly.

RMC IN PRACTICE

In a typical usage scenario, more than one E3-Series system (or other device Linear plans to embed the RMC software app technology into) will be connected to an RMC Server at any given time. Therefore, when the RMC Server receives an HTTP request from an E3-Series system with the RMC app software installed, it needs to determine which client's (PC/smart phone/tablet) remote browser to which the request must be forwarded.

There are two ways to make this work:
The first one is via the URL sent from the client to the RMC Server (e.g., *http://dev1.RMC.net*). This requires setting up a wildcard DNS record in the network's DNS server which resolves all requests for **.RMC.net* to the RMC Server *www.XX.RMC.net*. The RMC Server can then use the Host header in the HTTP request together with an internal table to associate the request with a specific E3-Series panel/system.

Alternately, the RMC Server could place a 'cookie' in the web browser's memory once it has logged into the RMC Server and selected a target E3-Series panel/system. This cookie is then sent with every request from the remote device's web browser to the RMC Server and allows the server to forward the request to the appropriate E3-Series panel/system.

There are multiple options for running the RMC Server for dealers and systems integrators:

1. Linear offers a hosted version of the RMC Server as software-as-a-service, provided for a fee. This turnkey solution allows the dealer/integrator to leverage this technology with minimal investment to establish.
2. Linear offers a licensing option for RMC giving the dealer/integrator the ability to install the software on their own server equipment and thus manage their own RMC Server. RMC can be run on an internet-facing server in a private data center, or it can be run on a virtual server provided by a cloud service provider such as Amazon (EC2) or Rackspace, to mention just two such options.

SECURITY AND PRIVACY GUARANTEED

Since the RMC Server simply forwards HTTP requests, without storing any data passed through it (except for optional caching of images and style sheets in order to improve performance), the RMC service does not introduce any additional data security or privacy risks – even if the RMC Server is operated in a private data center.

Of course, both the connection between the E3-Series' RMC app software and the RMC Server, as well as the connection between the remote client's web browser interface and the RMC Server can and should be encrypted with SSL or TLS. A single RMC Server instance can easily handle thousands of devices, with up to 100 or more simultaneous browser sessions.

A great advantage of this technology is that it is inherently secure by design. Since the E3-Series system equipment does not require any wide open ports to the internet, there is no danger of denial-of-service or similar attacks against the equipment. Requests to the device can only be

sent through the RMC server, and the RMC Server requires proper authentication of the requester before forwarding requests to the system/equipment.

Also, the E3-Series app software must authenticate itself to the RMC server when setting up the tunnel connection. Authentication is done through shared secret password, or challenge-response/CHAP protocols.

WORKS FOR WEB SERVICES AND SSH AS WELL

Linear's RMC system is not designed just to facilitate remote clients wanting to access behind-the-firewall web pages. Virtually every TCP-based protocol can also be used over an RMC tunnel connection, including web services based on SOAP, JSON or REST technologies, and even the SSH protocol, if desired. This makes RMC a great foundation for automated device management applications.

EASY INTEGRATION AND CUSTOMIZATION

The application software app necessary for integrating the RMC capability into an E3-Series system, as well as the software for the RMC Server is owned and supported by Linear exclusively.

Linear's RMC app software is capable of being ported to work on many other devices in the future. In addition, the RMC Server can also be integrated with customer applications via its REST API, and the default web user interface of the RMC Server can be customized to match customer-specific needs and visual style.

The RMC Server software optionally supports LDAP for user authentication, should a customer desire to employ this method of security. All of the RMC software and its corresponding optional support modules have been thoroughly tested in real-world environments, and will continue to be developed to support our dealers' go-to-market strategy.

Linear believes that the RMC software solution is a superior alternative to NAT, port forwarding and Virtual Private Networking (VPN) technology, enabling easy and secure remote access to field-deployed systems. IT managers should also agree, as they can implement remote access and connectivity securely without mangling the existing network infrastructure and policies.

Technology	Advantages	Disadvantages
Remote Management Console **"RMC"**	• Based on proven and proxy/firewall friendly Web Socket protocol • Can be used without changes to the existing network infrastructure • Supports secure, encrypted (SSL/TLS) and authenticated connections • Secure forwarding of most TCP/IP based protocols, not just HTTP • RMC server can be operated in the cloud • High scalability, up to thousands of RMC clients per RMC server instance (Multiple RMC servers can be clustered to increase capacity) • Designed for Linear Commercial Eco system and capabilities uniquely developed for security, support and recurring monthly revenue • Integrated API allows for customization and feature enhancements requested	• RMC Client must be integrated into device, or a gateway; device must be used to integrate legacy devices • Some TCP-based protocols cannot be forwarded (e.g., FTP)
Port Forwarding	• Simple and widely supported by NAT routers • Allows access to any TCP or UDP-based network service provided by RMC Client	• NAT router configuration for port forwarding can be complex, especially if multiple devices must be accessible (every device needs a unique public port number) • Dynamic DNS service is needed if the NAT router does not have a static public IP address • The device is directly exposed to the internet – very high risk and danger of denial-of-service or other attacks
Virtual Private Network	• RMC client is directly integrated into a remote network using a secure tunnel through the internet • Secure, encrypted connection (HTTPS) • Proven, standardized and widely-available technology	• VPNs may be blocked by network provider • Necessary network and VPN server infrastructure is difficult to setup and to maintain, especially if other devices must be integrated • All clients must have access to VPN in order to access the devices • Additional measures must be taken to isolate devices in the VPN from one another and to prevent users from accessing devices they should not access