eMERGE
Browser Managed Security Platform

FAQ's for the Network Administrator

What you need to know about the eMerge browser managed security platform

eMerge is a Network Appliance. What exactly does that mean?

Basically, a network or computer appliance is an embedded system that is based on a dedicated hardware platform and designed to perform a specific range of functions. Hardware and software are pre-configured and installed by the manufacturer and can be easily operated to provide a range of functions – in this case all targeting physical security and fast access over a network to the system's controls and capabilities.

eMerge is a configurable, integrated security management and access control system that can be managed from anywhere there is a network connection and access to a standard Internet browser. It is based on the industry-standard Linux operating system and requires no server or client software to be installed because it is a browser based and managed platform. This ensures there are no software compatibility issues with existing network equipment and computers. Additionally, since eMerge has been designed as a native IP device, there are no new gateways, communication wiring or plug-in hardware adapters to install.

The eMerge system runs on an ODBC compliant object-relational PostgreSQL database with an API designed to have much lower maintenance and tuning requirements than proprietary databases. The database has outstanding scalability and performance. Its SQL implementation strongly conforms to the ANSI-SQL 92/99 standards.

Since eMerge works over a network infrastructure, there are some technical considerations and requirements necessary to allow the security appliance to function seamlessly and reliably across your network and as a part of your total security system.

What are some of the topology issues to keep in mind when deploying and using the eMerge appliance?

The eMerge physical security appliance is all about simplicity and worry-free reliability across your network, so factors to consider in installing the system include wiring and bandwidth requirements, the architecture of your current wired and wireless network, site distances and the number of security resources linked to the appliance.

In the most common setup, and the one that will fit most small organizations, eMerge will share the same local area networking (LAN) resources as the users on the network. This means, the appliance will plug into the network much like a server, network router, or wireless access point and provide physical security services through the corporate LAN. A more secure configuration would have the emerge appliance connected to a separate security LAN and then linked to the corporate LAN through a dedicated router. This setup not only increases the level of security by channeling eMerge functions through a dedicated pipeline, but alleviates any bandwidth issues that may occur in high-traffic or media-rich applications.

eMERGE
Browser Managed Security Platform

FAQ's for the Network Administrator

What should I be aware of when using an eMerge Network Expansion Node as part of an eMerge security solution?

eMerge Network Expansion Nodes allow your eMerge security solution to be deployed in the most cost effective manner by making best use of your existing network infrastructure. Additionally, Expansion Nodes allow your system to scale modularly as your security requirements change.

Communication between the eMerge physical security appliance (Network Controller) and its Expansion Nodes can be accomplished securely across the local area network (LAN), wide area network (WAN), or even across the public Internet.

Each message between the eMerge appliance and eMerge Expansion Nodes is encrypted and then authenticated using a unique 160-bit message digest (SHA-1) to ensure security.

In some cases, it may be more cost-effective and desirable to link a series of eMerge Network Expansion Nodes to the eMerge appliance by placing an eMerge Network Node at one end or floor of a site and wire all local system resources to this node. Typically, this configuration is more desirable when extending the security environment across large distances in a building or throughout multiple floors. Important points to keep in mind with this type of layout include:

- Reader wiring that exceeds 500 feet (152 meters) will require an additional node to reduce the wire lengths to less than the maximum allowed by reader standards;
- Input or output wiring that exceeds 2000 feet (610 meters) will require additional nodes to reduce the wire lengths and distance between devices;
- The need for dispersed system resources - for example, at both ends of a large building - may require the addition of more eMerge Network Nodes.

How do eMerge Nodes and the Network Controller use the network?

When an Expansion Node boots, it initially selects for itself a temporary random IP address in the zeroconf address space. The Node then multicasts for a Network Controller at a specific UDP port (7262), and presents a Unique Identifier (UID) to distinguish the Node. A Network Controller then responds to this multicast through the same UDP port 7262, providing its own IP address and presents a unique addressing method for the Node.

There are three IP addressing methods available:

a. An existing DHCP server on the network can assign IP addresses;
b. A static IP address can be assigned using nnconfig.exe (This application is on the CD provided with the Network Controller);
c. The Network Controller can provide IP addresses to Nodes, but only to specific address ranges.

Once a proper IP address for the Node is selected, further communications between the Node and the Network Controller occur directly between their respective IP addresses using TCP port 7262. The Network Controller may also require:

- TCP Port 23 for Telnet server access. This can be used for remote support. The Telnet server is disabled by default.
- TCP Port 3000 open for communication from video management system inputs
- TCP Port 3306 open for PostgreSQL report usage

eMERGE
Browser Managed Security Platform

FAQ's for the Network Administrator

eMerge Security Network Information Requirement Checklist

- ✓ DNS (Domain Name Server) IP address (es)
- ✓ Gateway IP address, if any
- ✓ Subnet mask and IP addresses for the eMerge Controller and Nodes
- ✓ E-mail relay server address or name
- ✓ E-mail address name for the eMerge and setup on the e-mail server to accept mail for the eNC relay
- ✓ Domain account name and password for a server providing network attached storage (NAS) *Optional
- ✓ NAS server name in Universal Naming Convention (UNC) format: \\domain name\\machine name\\share name
- ✓ NTP (Network Time Protocol) server name (s) if the network has no Internet access (Pool.ntp.org is specified by default).

How do eMerge Network Expansion Nodes connect to the eMerge appliance across subnets or the public Internet?

Connecting eMerge Expansion Nodes across various subnets or even over the Internet is relatively easy, although there are some important points to remember to make the connections as effective and reliable as possible.

Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network. Subnets connect to the central network through a router, hub or gateway, are defined as all devices whose IP addresses have the same prefix. Addresses within a subnet are reachable without going through a router, and thus can be reached by broadcast.

In installations where Expansion Nodes are on a separate subnet or LAN from the Network Controller, you will have to directly supply the Expansion Node with an IP addressing method and the address of the Network Controller that will manage it. This is because the Expansion Node multicast transmissions and Network Controller responses are usually blocked across subnet boundaries.

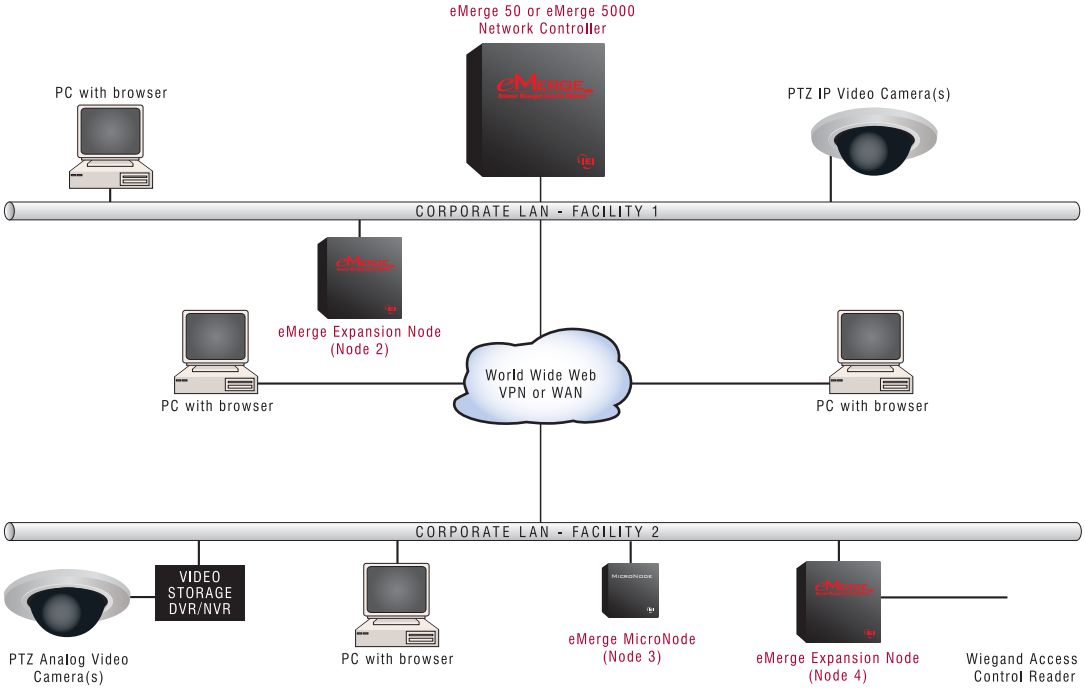
Direct addressing of the Expansion Node can be accomplished by using nnconfig.exe (This application is on the CD provided with the Network Controller). Please keep in mind that when communicating across subnets or networks, you must transmit through a router, and this may mean that a port must be opened to allow communication (refer to Network Port Usage Table on next page).

eMERGE
Browser Managed Security Platform

FAQ's for the Network Administrator

Network Port Usage Table (Versions 1.4 and higher)

TCP Port 80	Must be open to the Network Controller for Browsers to access the Security Application. This can be configured on a different port.
TCP Port 443	Must be open to the Network Controller for Browses to access the Security Application using HTTPS (SSL). This can be configured on a different port.
TCP Port 7262	Must be open to the Network Controller for communications between the Controller and Nodes. Be sure that this port is open through routers and firewalls for any Nodes on different subnets from the Network Controller.
TCP Port 23 (For support only)	Must be open to the Network Controller using a jumper on the Controller module for Telnet access to the Controller.
TCP Port 3000	Must be open to the Network Controller for Video Management System virtual inputs to communicate camera up/down and motion detection messages.
TCP Port 3306, 5432	Must be open to the Network Controller for PostgreSQL report usage.
TCP Port 20, 21	When using active FTP, these ports must be open to the FTP server for FTP backup from the Network Controller. When using passive FTP, port 20 is not required. Ports must also be left open to the network Controller for the FTP server responses. The network administrator must set up these ports.



Linear®
Building On Innovation.

USA & Canada (800) 421-1587 & (800) 392-0123
(760) 438-7000 - Toll Free FAX (800) 468-1340
www.linearcorp.com

Printed in China Lit. Order # 229983 B