



White Paper

Spotlight on Disaster Recovery:

How Entré Standards Ensure High Availability When Disaster Happens

Identified in this white paper are the different approaches to having Disaster Recovery available with Entré. This information is written for the technical teams who are responsible for architecting, building and implementing Entré as a solution in their environments. Understanding how this system works can be the difference of having three or four server environments compared to one or two — and potentially saving hundreds or thousands of dollars in server licensing.

Standard Backup/Disaster Recovery

There are many different approaches to having Disaster Recovery available with Entré. The costs and benefits need to be weighed carefully to determine which options work best in your environment.

Traditionally, Disaster Recovery for Entré has consisted of having a recent backup of the database and the ability to reinstall the application on a new machine if necessary to recover from a complete server failure. It's important to understand that access control and panel functionality are not impacted in the event of an Entré server failure. The panels continue to perform access control as normal, and events are buffered in panel memory (up to 10,000) until communication is restored with the Entré server. This means no events are lost, and no customers are denied access to their buildings because of a program failure. The only functionality impacted is the ability to create and send new "badges" to the security panels by Entré operators who are unable to log into the application.

In the event of an Entré server failure, the panels continue to perform access control as normal — no events are lost, and no customers are denied access to their buildings due to a program failure.

It's also important to understand that in most cases, Entré is not the sole monitoring station for events. Most DMP alarm panels using Entré also still use traditional central station monitoring with communication paths programmed to send all alarms, troubles, panic signals, etc. Even in the case of Entré service outages, the primary means of alarm monitoring for emergency response (such as fire) is still operating normally as long as the panel's means for communication still exist and are working.

In the event of a software failure, DMP alarm and access panels continue to work unaffected. Once customers using Entré understand that, they typically do not deem High Availability as a necessary cost for their particular needs. It's up to the customer, dealer and the IT stakeholders who are involved to determine what is an acceptable MTTR or "downtime." In the world of Virtual Machines, even a complete server failure does not take long to repair thanks to snapshots, and even in a worst-case scenario, spinning up an entirely new machine can take minutes.

High Availability

Some customers do have a need because of their specific use cases for as little downtime as possible. For these customers, operators may need to add new personnel badges for immediate access to secured sites, have time sensitive reporting purposes or might use Entré as the sole non-UL specific monitoring service for alarms at a private monitoring center specific to the customer.

SQL

The SQL database is where all of Entré's most important data is held. The application server can be quickly reinstalled on an entirely new machine and pointed to an existing SQL database. Once a license is applied, it will operate exactly as it did on the other machine.

Presently, Entré has no compatibility with a SQL High Availability listener. If a database connection were to fail, you would need to restart the service once the database is available again or point it to a new database manually.

Application Server

There is currently only one compatible configuration for an application server Disaster Recovery setup. That is Active/Passive.

Active/Passive

In this build, there is a primary Entré server actively talking to both the SQL database and alarm panels. The backup Entré server has been installed, configured to point to the Entré SQL database and has been properly licensed to run on the specific server it's on once the service is started. For all intents and purposes, it is a duplicate of the primary, which is ready to be turned on when needed, but most importantly, the service stays OFF while not in use.

In the event of a primary application server failure, the Entré application service would need to be started on the backup (DR) server. This could be done manually by a designated manager or automatically by a script/task, which enables this service once the primary server is no longer accessible or the primary service has been determined to be stopped. It's important that two separate Entré services are not running against the same database at the same time as data corruption could occur.

Panel Programming

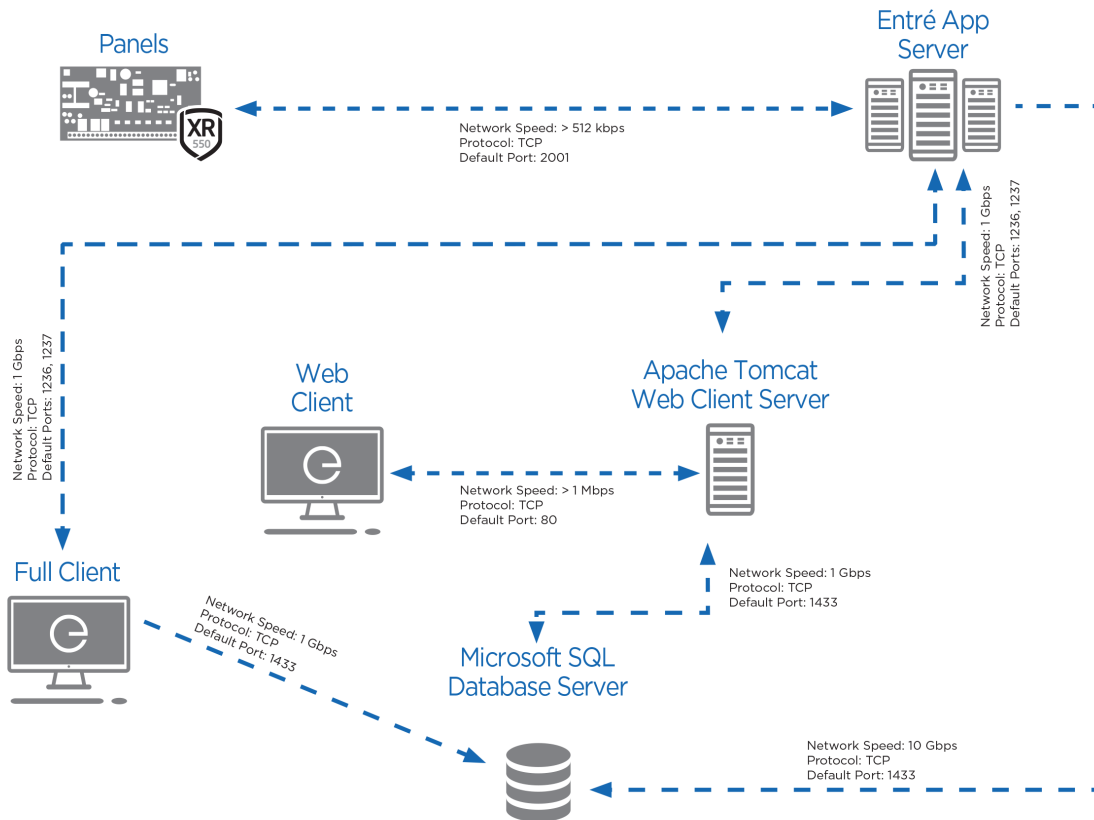
In Remote Options of DMP alarm panel programming, you can program an "Entré Backup Connection." The purpose of programming this field allows the panel to also be involved in the Disaster Recovery setup. In the event the primary Entré server does not respond, the panel will attempt to communicate with the backup Entré server, sending events, receiving panel commands, etc. by using the information programmed. This removes the need to perform network route alteration at a router/switch level in the event of a server failure — the panel will simply try to send events to the other server IP already preprogrammed. However, a completely viable alternative is simply rerouting network traffic to the new "Backup" Appserver to achieve the same result. It's up to the customer to determine which method of signal routing they prefer to use.

A completely viable alternative is simply rerouting network traffic to the new "Backup" Appserver. It's up to the customer to determine which method of signal routing they prefer to use.

Clients

Currently, the Entré full client connects both to the application server as well as the SQL server. In the event that one of these server connections fail, the client would be disconnected. If using a backup Entré application server, you would need to change the IP address or URL entered in the client to point to the correct server the client is attempting to log into in the event of a failover.

NOC Multiple Server Data Flow




Review & Points of Consideration:

Licensing

Entré NOC licensing includes one production license and one additional license that is listed as UAT/DR. A third license is included for DEV environment testing. This DEV license expires every year and should be renewed at the time the annual support fee is paid. There is no server fingerprint associated with this license, allowing you to create and destroy Virtual Machine environments as needed for testing. This DEV license is not valid to be used for DMP Technical Support as it is strictly for testing purposes. Any technical issues that arise on a server using this license during testing should be directed to the DMP Dealer Development Manager and the Software Services department via email for review and assistance.

Network

It's important to have a detailed plan that determines how to handle panel communications in the event of a server failure. Do you program a primary and backup Entré IP? Or do you simply reroute traffic on a load balancer or other device to repoint to the backup server? Both options are valid, but depending on the existing network infrastructure, one may be more difficult than the other.

	866-266-2826	INTRUSION • FIRE • ACCESS • NETWORKS
	DMP.com	2500 North Partnership Boulevard
		Springfield, Missouri 65803-8877