# Table of Contents

## At-a-Glance Security

- A Single, Unified Solution for All Systems ................................................................. 4
- Convenient User Loading and Management ............................................................... 4
- Multiple Viewing Options .......................................................................................... 4
- Automation Rules ....................................................................................................... 5
- Alarm Graphics ......................................................................................................... 5
- Highly Customizable .................................................................................................. 5

## System Features

- .................................................................................................................................. 6

## Access Control Application

- Access Areas ............................................................................................................ 8
- Panel Profiles ............................................................................................................. 9

## Networking Basics

- What is a network? ..................................................................................................... 11
- Network Types ......................................................................................................... 11
- Communication Devices ............................................................................................ 11
- Cabling Types .......................................................................................................... 11
- Protocols ................................................................................................................... 12
- Firewalls .................................................................................................................... 12
- Ports .......................................................................................................................... 12

## Web Client Data Flow

- .................................................................................................................................. 13

## Admin Workstation Data Flow

- .................................................................................................................................. 14

## Server Architecture

- .................................................................................................................................. 15

## Entré and Database Dependencies

- Entré Application Service ........................................................................................... 16
- Entré Standard Client ................................................................................................. 16
- Entré Web Client ....................................................................................................... 16
- Entré hibernate.properties File ............................................................................... 16
- What is a Database? ................................................................................................... 17
- How is a Database Organized? ................................................................................ 17
- Database Authentication Methods ........................................................................... 18
MONITORING AND MAINTAINING THE DATABASE
- Maintenance Best Practices
- Rebuild/Reorganize Indexes
- Update Statistics
- Check for Free Space
- Check Disk Drive Contention
- Check Database Integrity
- Manually Look for Indexes
- Parallelism
- Monitoring Best Practices

FIREWALL AND DATABASE CONFIGURATION
- Using the Entré Log Files
- Using the ODBC Data Source Administrator Utility
- Opening Firewall Ports for SQL

INSTALLING ENTRÉ
- Follow the Installer Prompts

CONFIGURING APACHE TOMCAT SOFTWARE

STARTING ENTRÉ

CONFIGURING AND PROGRAMMING SYSTEMS
- Configuring the Panel for Remote Arming and Multiple Area Schedules
- Configuring the Panel for Real-Time Statuses

ADDING THE PANEL IN ENTRÉ
- Creating an XR550 Panel
- Using the New Panel Wizard

LICENSING THE SOFTWARE

CONFIGURING ENTRÉ FOR THE USER
- User Code Profiles
- Personnel Records, Badges, and User Codes
- Sending Personnel Records, User Codes, and Profiles to the Panel
- Calendars and Holidays
- Area, Door, Output, and Time Schedules
Sending Schedules and Holidays to the Panel

NETWORK AND DBMS TROUBLESHOOTING
- IPCONFIG
- Ping
- NSLOOKUP
- TCPING

USING WIRESHARK
A Single, Unified Solution for All Systems

Entré allows you to combine management and control of all related access and security systems under a single software application. Entré is database and hardware independent, so you can bring various systems and multiple panels together, giving a consolidated view of the system. As a single, unified system, there’s one badge, one face, or one fingerprint - worldwide.

The easy-to-use interface makes for simple system configuration and user permission management. Entré gives you control over all security management activities and functions from a single, high-functioning platform. As a network application, it allows you to manage multiple spread-out facilities from your private network.

Convenient User Loading and Management

There’s no need to reload system user information that already exists in another database. You can import existing data into Entré via standard comma-separated value (CSV) format files. In addition to the standard data fields, you can create up to 20 fully-customizable data fields to meet your unique needs.

To facilitate user management, you can assign each user to one or more profiles on multiple systems. You can greatly simplify processing new users by defining specific rights and access permissions for each profile.

Multiple Viewing Options

Entré offers the at-a-glance simplicity of a graphics-based interface. Instead of viewing system status information and messages as text and tables, you can see an actual picture of the system.

From the graphic display of your facility, you can drill down to any zone, area, or room. Each system component is represented as an icon on the screen. This allows you to point and select any device to control and change its operating parameters, check its status, or process an alert or alarm.
Entré scales from 1 to 500 systems to meet your needs for managing a single building to a large enterprise with many users.

**Automation Rules**
Advanced users have the power to create automated system actions and define automatic responses to any system alarm or event. These responses include generating a report, generating an alert e-mail, or sending commands to selected devices. You can also create scheduled system actions to run once at a specified time and date, or scheduled events that repeat at your defined time and date intervals. System automation enables you to configure unattended activities, freeing system managers from many routine responsibilities.

**Alarm Graphics**
The graphical representation of events and alarms gives you at-a-glance feedback on a system’s status. System maps are linked from level to level, allowing you to transition from a macro view to a specific room or area. You can view alarm status at every level of zoom. User-defined layers representing different alarm types allow you to customize the graphical interface to meet your needs. Select the alarm display icon to acknowledge an alarm or request additional information.

**Highly Customizable**
Take advantage of Entré’s extensive customization capabilities to create a system that matches your exact needs. Define what events are considered “alarms” and what response is required from the system operator.
SYSTEM FEATURES

- Remote panel programming—upload or download your DMP XR Series panels from this single interface, making the management of larger enterprises seamless. Allows bulk programming changes with ease
- Full audit trail, user activity, and event history
- Video integration for Live Image Capture of Access Control or other events
- Write custom SQL database reports or use a variety of standard ones—automate to send these out via e-mail daily, weekly, or triggered by events
- Powerful automation features allow you to customize notifications for almost any requirement or application
- Badge design and printing directly from the application
- Alarm monitoring for proprietary or campus environments allows you to be notified of alarm situations from one seamless interface
- Multi-language: English and Spanish
BURGLARY DETECTION AND ACCESS CONTROL BASICS

The following few sections briefly outline how DMP panels process burglary detection and access control. Having a basic understanding of the mechanics of area logic will enable you to better plan and deploy the system and understand how it works.

**Generally speaking, all burglary detection and access control panels are area systems.** Instead of arming individual zones, you arm the perimeter, or the perimeter and interior areas. The zones are assigned to the interior or perimeter areas. Most panels operate in an All/Perimeter fashion and have built-in rules and templates in their areas that dictate how the zones and areas behave and how the system must be armed and disarmed.

DMP uses area logic too, but we allow you to establish how many areas you would like to use, what they are named, and how they are to behave. We allow any area to be armed or disarmed independently of any other area, if desired. When the area is armed or disarmed, the zones associated with it are armed or disarmed.

An area can be a single room that contains a motion detector. An area can also be the entire perimeter of a distribution center, with other areas assigned to interior detection duties.

**Control panels determine how a location reacts to people attempting to enter physical areas.** A burglary or access system is planned around that concept. Its purpose is to notify an interested party of a physical breach of an area through means of attached detection devices and a communicator. It is also designed to control access to an area by electronically locking and unlocking doors.

XR550 Series panels are able to perform either or both of these duties from a single main control panel. Consequently, burglary detection and access control can be either integrated to interact with each other, or separated to work independently of each other.

**XR550 Series panels also detect and report life safety (fire and emergency) and supervisory (flood and temperature) zones.** They are termed “24-hour” zones and are not assigned to an area because they are always armed. However, 24-hour zones do report to the central station with individual area information. This is useful for very large or multi-tenant systems.
XR550 Series panels achieve burglary detection and access control through a common rule: areas. Access areas are created in the same place in panel programming as burglary areas. What is assigned to an area designates it as burglary or access. The inherent flexibility of using area logic means that you can combine burglary and access or separate them.

**Access Areas**

Access areas are named areas in panel programming that are used as placeholders for assigning access permissions to a device to restrict access to a specific door. Although they do not have any zones associated with them, access areas can be armed and disarmed.

Access can be restricted by associating door devices with burglary or access areas. If an area number is listed in the Access Area field of a device (Device Setup in the Programmer Menu), then it can be used to gain access to a device number or door as long as that area is not armed, thus allowing you to restrict access by the armed state of the system.

This allows managers to restrict access by arming certain areas of the system manually at the close of business and allowing door access to the building only when a manager has arrived to disarm the burglary system each day. This arming and disarming can also be done via automatic panel arming or disarming schedules. This feature allows you the flexibility to assign area arming schedules to burglary or access areas and automatically arm or disarm those areas at certain times. These area schedules are also called time schedules and work with the user code profile time selections to restrict access to defined time periods.

**Note:** If you leave the Access Area field of Device Setup blank, anyone with a valid user code or access fob or card in the system can gain access to that specific door regardless of time or profile. This setting is programmed with Remote Link software, or from a keypad, and is not adjustable by the end user from Entré.
Panel Profiles

The ability to disarm a burglary or access area can also be assigned to a user code profile giving a manager the ability to disarm the system on a card swipe. XR550 Series panels support up to 99 profiles. Each profile can support a combination of up to 8 schedules. Creating time schedules and assigning them in user code profiles allows managers to restrict access to an area. They do this by assigning a schedule to the burglary or access area which validates against the check boxes in the profile and only grants access during the specific time listed in the user code profile. When the card is swiped at the reader device, the profile is queried. If a schedule is selected, the panel validates the profile number against the profile’s time schedule and access is granted if the profile number is within the schedule time period.

Pro Tip

When programming an access control system, the most important programming information is usually contained in the profile, Area Information, and the Device Setup access areas.
USER PROFILE AND PERMISSIONS BASICS

Any person allowed to interact with a system needs a specific set of permissions that defines what tasks that user can perform and what areas he or she is allowed to access. When adding a user to the system, a user profile is required. Without a user profile, the user has no authority to do anything with the system.

XR550 Series panels offer 99 fully-customizable profiles. These profiles provide granular control over a user’s permissions. The method of establishing user interaction exists in two separate programming fields: user codes and user profiles.

The user codes section is for creating individual users and their codes. The user profiles section is for creating sets of permissions for single users or groups of users. Requisites for user code programming are user number, user code, and profile assignment.

For burglary systems, a user profile includes which areas a user can arm and disarm, the ability to silence alarms, the ability to see what areas are armed, whether or not the user can access user programming items from a keypad, and whether or not the user’s code is temporary or permanent.

For access control systems, a user’s profile includes which areas a user can access, what times the user’s access works, whether or not the user can access user programming items from a keypad, and whether or not the user’s code is temporary or permanent.

Since the XR550 Series combines burglary and access into one control panel, profiles may be used for both burglary and access applications.

When a user code is entered at a keypad on a burglary system, the panel checks to make sure the code is valid. Then, the panel checks the user code against the permissions defined in the user profile. The panel will carry out the action only if it is allowed in the user’s profile.

When a user code or credential is entered at an input device on an access control system, the panel checks the code and then checks its permissions. If the code or credential is valid, and attempting to access an area that is allowed in the user profile, the door is unlocked by the panel.
What is a Network?
A computer network is a group of interconnected computers. Networks may be classified according to a wide variety of characteristics.

Network Types
- **LAN (Local Area Network)** - This is a network covering a small geographic area like a home, office, or building. Current LANs are most likely to be based on wired or wireless Ethernet technology.
- **WAN (Wide Area Network)** - A WAN is a data communications network that covers a relatively broad geographic area (e.g. one city to another or one country to another). It often uses transmission facilities provided by common Internet service providers. WAN technologies generally function at the lower three layers of the OSI Reference Model: the physical layer, the data link layer, and the network layer.

Communication Devices
- **NIC (Network Interface Card)** - An installed or integrated piece of hardware that allows the computer to connect to a network.
- **Modem** - A gateway device which allows connection to a WAN. A modem typically has an internal IP address for the LAN and an external IP address so it can be identified on the WAN.
- **Switch/Router** - Switches or routers are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path or recipient. These devices can be used as LAN gateways, as they can process traffic to and from a WAN. They have an IP or gateway address.
- **Hub** - Like most switches and routers, a hub contains multiple physical connection ports. Unlike a switch or router, when a packet arrives at one port, it is copied to all of the hub’s ports for transmission. When the packets are copied, the destination address in the frame does not change to a broadcast address: it simply copies the data to all of the nodes connected to the hub. Hubs are not gateway devices because they do not have an IP or gateway address.

Cabling Types
- **Patch Cable** - A standard network cable designed to connect devices to each other through a hub or gateway device.
- **Crossover Cable** - A network cable that is pinned in such a way that a gateway device is generally not necessary – typically used for directly connecting two nodes to each other.
Protocols

- **TCP/IP (Transmission Control Protocol/Internet Protocol)** - A technology that allows network traffic to be sent to a specific device or address via communication devices, with built-in error protection. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255. For example, 1.160.10.240 could be an IP address.

- **Subnet Mask** - A 32-bit number that masks an IP address and divides the IP address into a network address and host address. A subnet mask is made by setting network bits to all “1”s and setting host bits to all “0”s. Within a given network, two host addresses are reserved for special purposes. The “0” address is assigned to a network address and “255” is assigned to a broadcast address. They cannot be assigned to a host.

- **UDP (User Datagram Protocol)** - A technology that broadcasts network traffic to all devices on the network under the assumption that the device in which the message was intended is connected without error protection.

Firewalls

- **Software Firewall** - A software firewall is installed on a PC and is designed to prevent unauthorized access. It prevents Internet traffic from entering or exiting that machine without the authorization of the administrator.

- **Hardware Firewall** - A hardware firewall is usually installed at the server or network level. It polices all incoming and outgoing traffic on a network by limiting access to ports or various PCs.

Ports

- **2001** - The port the panel uses to receive programming from Entré.
- **2011** - The port Entré uses to send programming to the panel.
- **1433** - The Microsoft SQL database port.
- **443** - The Web Server port for SSL configuration.
- **8080** - The Web Server port for incoming and outgoing information.
- **1236 & 1237** - The client ports.
- **9090 & 9091** - De-bugging ports for the app server. These ports can only be accessed locally.
The Entré Client Web Server reads data from the Microsoft SQL Database/App Server.

When a change is made, the Entré Client Web Server changes the data.

A notification of the change is sent to the Entré App Server.

The Entré App Server notifies all Entré Clients and Entré Client Web Servers of the change.

The Entré App Server pulls the change from the Microsoft SQL Database/App Server and builds an audit record.

The Entré App Server sends the change to the Panels.
The Admin Workstation reads data from the Microsoft SQL Database/App Server.

When a change is made, the Admin Workstation changes the data.

A notification of the change is sent to the Entré App Server.

The Entré App Server notifies all workstations of the change.

The Entré App Server pulls the change from the Microsoft SQL Database/App Server and builds an audit record.

The Entré App Server sends the change to the panels.
**SERVER ARCHITECTURE**

**Microsoft SQL Database Server**
* Dell 630 - Approximately $11,000*

- **Processors** - 2 (6-cores each)
  - All but 2 cores should be allocated to SQL.
- **Hard Drive**
  - The operating system, primary file system drive, SQL data drive, and log drives are all located on physical 15K RPM SAS drives.
  - **TempDB Drives** - 2 (146 GB, RAID 0)
  - **Data Drives** - 4 (300 GB, RAID 10)
  - **Log Drives** - 2 (300 GB, RAID 1)
- **RAM** - 128 GB RAM (120 GB dedicated to Microsoft SQL)

**Supported Versions**
- Apache Tomcat - 8.5
- Java - 8
- Windows Work Station - 10

* Cost based on standard pricing from dell.com.

**Entré App Server**
* Dell 430 - Approximately $6,000*

- **Processors** - 2 (6-cores each)
- **Hard Drives** - 2 (146 GB, RAID 1)
- **RAM** - 64 GB RAM (50 GB dedicated to Java)

**Apache Tomcat Web Client Server**
(per 100 users)
* Dell 430 - Approximately $5,000*

- **Processors** - 1 (8-cores each)
- **Hard Drives** - 2 (146 GB, RAID 1)
- **RAM** - 96 GB RAM

**Note:** For redundant sites, use Microsoft high-availability services.

**Full Client Specifications**
- Core i7 Series Processor or equivalent
- 32 GB RAM (16 Minimum)
- 250 GB HDD

**Requirements:** All servers require a Gigabit Ethernet Adapter or better.

---

**Call DMP Inside Sales at 1-877-757-4367 for information on Entré NOC pricing and availability.**

---

**PANELS: 500 or less**
**EVENTS: 50,000 or less per day**
**USER CHANGES: 500 or less per day**
**ENTRÉ AND DATABASE DEPENDENCIES**

**Entré Application Service**
The Entré application service is a program that runs in the background at the operating system level and listens for events coming from control panels. It classifies the events and then stores them in the SQL database. Each time the application service starts it uses a file named *hibernate.properties* as a road map to locate and connect to the SQL database along with the help of the SQL Browser Service. The application service automatically starts each time the operating system is restarted.

**Entré Standard Client**
The Entré standard client is a program or graphical user interface (GUI) written in Java that makes a simultaneous TCP connection to the Entré Application Service and the SQL database. The client requests and displays, in a graphical format, the data that is parsed by the service and stored in the database. Through the client GUI, the operator can make changes to personnel records, user codes, schedules, holidays, and other information stored in the SQL database. The operator can then run reports against the database that can be displayed in the software GUI or saved in various output formats.

You can install the standard client on as many machines as you wish, but you can only maintain the number of simultaneous connections listed in the permanent license.

**Entré Web Client**
The Entré web client is an Apache Tomcat-based browser version of the Entré Standard Client. Apache Tomcat Web Server software must be installed and configured as part of the Entré installation and licensed on a per client basis before it will function. The closely integrated DVR video, graphic maps, and badging module do not function from the Entré Web Client.

**Entré hibernate.properties File**
The *hibernate.properties* file is located in the Entré installation directory and is used each time the Entré Application Service starts. There are three lines in that file that you should be familiar with and use during troubleshooting.

- **Line 6** - The SQL user name. The name should be “SA” or a login name supplied by the SQL database administrator with equivalent system administrator permissions for the database. Entré requires read and write permissions in order to connect to the database and create the default system tables and write events to the database when the service is running.
• **Line 7** - The password for the SQL instance. There is a minimum character limit of six characters. At least one numeric character is required for the password to be valid.

• **Line 8** - The path to the SQL database. You may notice this line specifies the computer name or IP address, the name of the database, the port used to communicate to the SQL server, and the instance name that the database resides in.

**What is a Database?**

A database is a collection of information organized to provide efficient retrieval. There are physical and electronic databases. The collected information could be in any number of formats (electronic, printed, graphic, audio, statistical, combinations).

A database could be as simple as an alphabetical arrangement of names in an address book or as complex as a database that provides information in a combination of formats.

**How is a Database Organized?**

Understanding how a database is organized can help you retrieve information more efficiently. Information about each item in a database is called a **record**.

Elements of an individual record are called **fields**. Fields can be used as points of access when searching a database.

Try visualizing a record in an electronic database as being part of a table. Each column in the table represents the fields and each row represents the individual record. The table below represents what an electronic database of students in a class might look like:

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Class</th>
<th>Hometown</th>
<th>Birth Month</th>
<th>Gender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smith</td>
<td>John</td>
<td>Freshman</td>
<td>Macon</td>
<td>August</td>
<td>Male</td>
</tr>
<tr>
<td>Turner</td>
<td>Evelyn</td>
<td>Freshman</td>
<td>Brunswick</td>
<td>April</td>
<td>Female</td>
</tr>
<tr>
<td>Arndale</td>
<td>Carrie</td>
<td>Sophomore</td>
<td>Atlanta</td>
<td>September</td>
<td>Female</td>
</tr>
<tr>
<td>Zwemke</td>
<td>Jason</td>
<td>Freshman</td>
<td>Cartersville</td>
<td>May</td>
<td>Male</td>
</tr>
<tr>
<td>Lane</td>
<td>Penny</td>
<td>Sophomore</td>
<td>Decatur</td>
<td>September</td>
<td>Female</td>
</tr>
</tbody>
</table>
**Database Authentication Methods**

What is the difference between Windows authentication and SQL authentication? With Windows authentication, the SQL server service already knows that someone is logged in to the operating system with the correct credentials, and it uses these credentials to allow the user into its databases. This works as long as the client resides on the same computer as the SQL server, or as long as the connecting client matches the Windows credentials of the server. Windows authentication is often used as a more convenient way to log in to a SQL server instance without typing a user name and a password. However, when more users are involved, or remote connections are being established with the SQL server, SQL authentication should be used. SQL authentication should always be used with Entré.

Entré Client connections use a remote TCP connection. This means that any end user-supplied SQL server must be configured to allow remote TCP connections. The login name provided to Entré must possess database owner-level access so that the Entré Application Service can read to and write from the VXDB database that is created when the software is installed.

**Server Instances**

A SQL Server instance is a complete SQL server. You can install many instances on a machine, but you can have only one default instance. A SQL Server instance has its own copy of the server files, databases, and security credentials.

Entré can be installed using either the default instance, or you can specify an instance during the installation. This instance name and a SQL login with server administrator permissions are used to create the TCP link to the SQL database in which the default VXDB Entré Database is created.

**Management Tools for SQL**

If there is already an Enterprise-level SQL Server, then the site database administrator will have access to the SQL Database Management Studio. If you don’t know which level of SQL you need to get, consult your Microsoft certified provider or visit the link below.

Maintenance Best Practices

Below is an overview of recommended Microsoft SQL database maintenance best practices and how frequently they should be performed. For any additional information on these practices or how to perform them, refer to the Microsoft links below.

Microsoft Maintenance Tasks

  x?f=255&MSPPError=-2147217396

How to Set Up Maintenance Tasks Using Maintenance Plan Wizard

- Docs.Microsoft.com/en-us/sql/relational-databases/
  maintenance-plans/use-the-maintenance-plan-wizard

Rebuild/Reorganize Indexes

Daily/ Weekly

As data is added, indexes become inaccurate because data is added to the end instead of in order. It is a maintenance best practice to reorganize daily and rebuild weekly. Reorganizing is faster and puts less overhead on the system. Rebuilding takes more system resources and automatically updates statistics.

Update Statistics

Nightly

Microsoft SQL tries to optimize its performance by making the most used data the most readily available. “Statistics” is defined as which data is used and how often. Updating statistics allows Microsoft SQL to come up with query plans to find data the fastest. Those statistics can be set to auto update or run nightly. You will want to update statistics manually after performing a database reorganization.
Check for Free Space

Weekly
If auto grow is turned on, then you need to ensure that it is set as close to 10% as possible. Also, ensure there is enough actual drive space to accommodate that growth.

Check Disk Drive Contention

Weekly
Check disk drive contention weekly. Ideally, data files and log files are on different physical disks. You can use Windows Performance Monitor to monitor the disks and ensure that the read and write cue lengths are always less than 1. If the cue length is longer than 1, the disk is receiving more requests for data than it can process. This will slow down performance significantly.

Check Database Integrity

Weekly
Use the DBCC Check to verify the health of the database in general. Also, run the DBCC check table and check ALLOC and the DBCC check catalog. These commands verify that the database is not corrupt.

Manually Look for Indexes

Monthly
Which indexes a database needs depends on how you use Entré. Over time, you may find that you can add indexes to improve performance. You can use Microsoft SQL's built-in functionality to find what tables need additional indexes.

Parallelism

Monthly
When you run a Microsoft SQL query, it will try to spread that query across all processor cores. This can aid performance to an extent, but occasionally those processors can not handle anything else while this is happening. If one query is tying up the processor for too long, that core can not process anything else while it is happening. Look at the weight states for threads on the Microsoft SQL server and you will see CX packets. A CX packet is the state of the thread when there is not a core available to process the thread.
Monitoring Best Practices

Microsoft provides helpful resources for monitoring your Microsoft SQL database. Visit the links below to learn more about monitoring best practices.

Performance Monitoring and Tuning Tools

Activity Monitor

Log File Viewer

General Database Engine Tutorials
FIREWALL AND DATABASE CONFIGURATION

Entré uses network ports for communications between Entré Client Software, the Entré Application Server, and the SQL database. Therefore, certain ports must be open bidirectionally in the operating system and network firewalls. Each standard client machine will need to access both the SQL Server and the Entré Server on the host machine. See the Web Client and Admin Workstation Data Flow sections of this document for more information on which ports should be used.

Some installations may require other system ports to be opened, but the ports shown in the data flows are the required ports for most common installations.

Configuring the operating system to allow the installer to operate might be required before starting the installation. Entré software does not make any changes to the system registry, but the installer must have full local administrator read and write permissions to complete the installation.

The Entré installer does not set or override firewall permissions, or override domain policies. Software installations that error out, or fail to create log files during the installation, are commonly seen on machines that are part of a domain with a policy restricting the installation of software. Simply right-clicking on the Entré installer and running it as “Administrator” by entering the local administrator password will usually resolve this issue.

The Entré Application Service uses the information specified during the installation process to connect to the database and add the required tables.

When installing Entré and interfacing it with an existing SQL database, you need to contact the site IT staff to verify that the operating system is configured properly for SQL. DMP Tech Support is not allowed to make changes to domain policy or firewall configurations. It is the responsibility of the dealer technician to ensure that the site PC is configured properly before installing Entré.
Using the Entré Log Files

Entré’s log files are located in the DMP\Entré\log\ directory. The four log files that are part of the Entré system are shown in Figure 1 and described below.

- **vx.adminapp.log** - Logs the operation of the installation process.
- **vx.gui.log** - Details the operations of the Java based standard client or Apache Tomcat based web client software connection to the service.
- **vx.wrapper.log** - Logs the actual Entré Application Service connection with the operating system.
- **vx.appserver.log** - Details the running operations of the Entré Application Service. This is the most useful log to certified installation technicians.

These are two examples of errors seen in **vx.appserver.log** log files. These two errors are an indication that the TCP/IP ports that the operating system uses to communicate with the SQL server are not open so Java is not able to talk to the database.

- **[2010-03-15 15:11:22,046] WARN** - SQL Error: 0, SQLState: HY000
- **[2010-03-15 15:11:22,046] ERROR** - Unable to get information from SQL Server:164.51.192.16.

**Note:** If you do not see a **vx.appserver.log** then you know the operating system did not allow the service to be installed. Therefore, there is no service in place to make error logs.

Windows operating systems with a default configuration do not allow Microsoft SQL Server to communicate internally without making several port adjustments.
Using the ODBC Data Source Administrator Utility

You can check to see if the required ports are open for SQL to communicate with the operating system by using the Open Database Connectivity (ODBC) Data Source Administrator Utility. It is included as one of the basic windows system tools. Obtain the services of an IT professional for these advanced diagnostic procedures.

1. Select Run from the Start menu and run the command odbcad32.
2. Select Add and you will be presented with a list of drivers to choose from.
3. Scroll to the bottom and select SQL Server from the list. Select Finish.
4. Enter a Name and Description and then open the Sever drop-down list and your computer will query the network for a list of existing SQL servers.

   Note: It is important to let the tool query the network for the list of existing servers. If this list does not appear, you need to verify that the SQL Browser Service is running and set to automatically start when the SQL service starts. The SQL Browser Service is what Entré relies on to resolve the localhost machine name to the system-assigned IP address.

5. Select the computer’s machine name from the list and then select Next.
6. Select With SQL Server authentication using a login ID and password entered by the end user.
7. Enter the login name and password that you entered in during the Entré installer and then select Next.
8. The next screens can be left at their defaults. If you have made it this far then your login and password are correct for the SQL instance that you selected and you can continue on with your connection test to see if the required internal ports are open.
9. Select the Finish and you will be presented with a summary of the data source connection information.
10. Select Test Data Source and a series of connection tests will be ran on the ports of your computer for the SQL instance.

   Note: If the test is not successful, you will need to have an IT technician or SQL Database Administrator (DBA) verify that the SQL server is properly configured for remote connections via TCP/IP and the proper ports are open for the operating system being used.
Opening Firewall Ports for SQL

The Configuring the Windows Firewall to Allow SQL Server Access Books Online entry contains the information to open the required ports in Windows Firewall for each one of the SQL Server services. There’s also a much easier way to open the required Windows Firewall ports for SQL Server in the following Knowledge Base Article (KB968872).

The link below will take you to a tool that Microsoft has supplied to assist you in configuring the Windows Server operating system to allow SQL to communicate internally.

INSTALLING ENTRÉ

Before beginning installation, please make sure you have completed the Pre-Installation Checklist found in LT-1660. Follow the steps below to open the software and run the installer.

Open the Software

If you are using an install CD, insert it now. Otherwise, contact your DMP representative or DMP Technical Support for access to the Entré software.

Follow the Installer Prompts

1. If you are using an install CD, the following screen displays automatically. If the screen does not automatically display, open the Entré installer file. Select Install to begin the installation.
2 When the welcome screen displays, select Next.

3 Enter your User Name and Organization. Often, this information is auto-filled based on your computer’s existing information. Select Next.
If you are installing Entre for the first time, select **New**. If you are upgrading an existing version of Entre, select **Upgrade**. Select **Next**.

Choose a **Setup Type**.

Selecting **Custom** allows you to customize program features and where they are installed. Use this option if you would like to install a client workstation by itself.

Selecting **Complete** installs all available Entre features to the specified directory. Select **Next**.
If you chose the **Custom** installation option, the screen below displays. If you chose **Complete**, skip to the next step.

Open the **Core Files** drop-down menu and select **This feature will be installed on local hard drive.** The **Core Files** feature is required for all installations.

Open the **Entré Client** drop-down menu. If you are installing a client workstation, select **This feature will be installed on local hard drive.** If you are not installing a client work station, select **This feature will not be available.**

Open the **Entré Server** drop-down menu. If you are installing a server, select **This feature will be installed on local hard drive.** If you are not installing a server, select **This feature will not be available.** Select **Next.**

Review the **Entré Prerequisites Checklist** to make sure that all of the items have been completed. Once the requirements have been verified, check the **I have completed the checklist requirements** box and then select **Next.**
If you are installing the Entré Server feature, you will see the following screen.

Check **Run Database Import Scripts** if you would like to reinstall Entré’s core files and override an existing database.

If you are installing a Microsoft SQL server onto this computer, enter the IP address of this computer in the **Host or IP Address of Database Server** field.
If you are using an existing database server, enter the IP address of that computer.

Check **Custom SQL Server Instance Name** to specify a SQL server instance name. Use this option if you are linking to an existing server that has a named instance.

If you are installing Microsoft SQL server onto this computer, you must specify an administrative password for this database instance. Choose a secure password containing at least one number, one special character, and a combination of upper and lower case characters.

If you are using an existing database server, enter an administrative level **Username** and **Password** so that the installer can create a default database on this server.

Select **Next**.
9 Select **Install**.

10 If you’ve chosen to upgrade an existing instance of Entré, you’ll see the following screen while the database is updating. Please wait until the **InstallShield Wizard Complete** screen displays.
When the installation is complete, the following screen displays. Select **Finish**.
CONFIGURING APACHE TOMCAT SOFTWARE

Follow these steps to configure the Apache Tomcat software. Keep in mind, you must have Apache Tomcat software installed prior to starting this process.

1. Stop the Apache Tomcat Service on the host machine.
2. Paste the dmp.war file into the C:\Program Files\Apache Software Foundation\TomcatX.X\webapps folder (where “X.X” represents the version number).
3. Start the Apache Tomcat Service on the host machine.
4. Open your web browser and use the following URL to access your client:
   http://ipaddress:port/dmp/Entré/start
5. Run Tomcatw.exe to configure the Apache Tomcat Server. The Dvx hostname should be the address of the App Server.
6. Add the settings below as new lines in the Java Options section.
   • -XX:MaxPermSize=256M
   • -XX:+UseG1GC
   • -Xms256M
   • -Xmn64M
   • -Xmx384M
STARTING ENTRÉ

Upon starting, Entré will open a splash page displaying the start-up progress. See Figure 2. Enter the IP address or hostname of the server machine and log in with a valid username and password.

The system administrator username is admin. When Entré is first installed, the factory-default password is pass. Be sure to change the administrator password soon after installation.

If the username and password are valid, Entré displays the start page, or the modules that were open during the operator’s previous session.

If the username and password are not valid, an error is displayed. If the application has not accepted the username and password, repeat the steps above. Make sure the username and password are correct, with the correct case.

If problems continue, contact your system administrator. If you are the system administrator, and cannot resolve the issue, contact your Entré distributor or system installer.

Figure 2: Entré Log In Screen
For systems to work with Entré successfully, you need to change each panel’s Entré settings in Remote Options. To do this, you can use either Remote Link or a keypad connected to the system.

Navigate to the Remote Options section of the Programmer Menu and adjust the information to match the way you plan to set up Entré. This will allow Entré to retrieve panel programming and easily communicate with each system. See Figure 3 for the Remote Options programming fields.

**Entré Connection**

Select **Net** from the Entré Connection drop-down menu to enable a dedicated network connection with Entré.

**Entré Incoming TCP Port**

Enter the number for the **Entré Incoming TCP Port**. This is the port used for programming and control commands with Entré. This port cannot be the same port that is programmed in the Network Programming Port. The default panel incoming TCP Port setting is **2011**.

**Entré IP Address**

Enter the **Entré IP** address where the panel sends network messages, alarms, and events.

**Entré Outbound TCP Port**

Enter the number for the **Entré Outbound TCP Port**. This is the port used to send alarm events and
status messages to Entré. The default port setting is 2001.

**Entré Backup IP Address**

This field is not currently supported.

**Entré Backup TCP Port**

Enter the backup port number for the outbound Entré connection in case the connection to the primary IP fails. This may be left blank. In most cases, this is not used.

**Entré Check-In Minutes**

Select the rate at which check-in messages are sent over the Entré connection to verify that the network path is available. If Entré does not receive a check-in message from the panel by the time programmed into this field, Entré will attempt to re-establish communication with the panel three times before placing the panel in an offline status. Check-in minutes should be enabled for 20-30 minutes.

**Entré Passphrase**

To enable encryption, enter an 8 to 16-character passphrase using alphanumeric characters. If you leave the passphrase blank, the panel still communicates with Entré, but the data is not encrypted. The passphrase is blank by default. The matching encryption key is programmed in Entré by right-clicking on the DMP Driver in the Hardware Tree and entering the encryption key in the Driver sub menu.

If the panel does not have a DMP receiver IP address programmed in primary path 1 of the panel programming, then do the following:

1. Program the panel’s path 1 as a primary network path.
   
   **Note:** This is only necessary if the panel is not communicating to a DMP Receiver such as the SCS-VR or SCS-1R.

2. Place the IP address of the Entré Server machine in the receiver IP address field.

3. Disable all the options on the advanced tab.

This will cause the panel to request the time once per day and Entré will update the panel time based on the current time of the machine running the Entré Application Service and the Hours from GMT setting programmed in the panel System Options menu. Subsequent paths 2-8 can be programmed to communicate with all normal panel supported methods.
Configuring the Panel for Remote Arming and Multiple Area Schedules

In order for any DMP software, including Entré, to be able to disarm the system or areas, Remote Disarm in the Remote Options section of the Programmer Menu must be turned on.

If multiple independent area schedules will be used, then Area Schedules in the Area Information section of the Programmer Menu must be turned on.

Configuring the Panel for Real-Time Statuses

Entré will display real-time statuses for door access devices, zones, and outputs, but only if the panel is told to send them. Enabling real-time door status is not a global option and must be enabled for each device, zone, or output.

To enable real-time door statuses, turn on Door Real-Time Status for each access device in the Device Setup section of the Programmer Menu.

To enable real-time zone statuses, turn on Zone Real-Time Status for each zone in the Zone Information section of the Programmer Menu.

To enable real-time output statuses, turn Output Real-Time Status on for each output in the Output Information section of the Programmer Menu.

Pro Tip

Use caution when turning on real-time status for heavily used zones, doors, and outputs. On very active devices there may be a significant increase to network traffic and database storage.
**ADDING THE PANEL IN ENTRÉ**

**Creating an XR550 Panel**

1. Open the **Hardware Tree** by selecting it on the Start Page or from the Module menu.

2. Right-click the **DMP Driver** device in the Hardware Tree and select **New Panel**. This will open the **New Panel** window.

3. Name the new panel in the **Name** field.

4. Select the **Communication** tab and enter the IP address configured in the panel in the **Address** field.

5. Enter the port number (2011) used for the Entré connection into the **Port** field.

6. Enter the account number configured in the panel in the **Main Account Number** field.

7. Select **Save and Close**.

To complete the configuration process and bring the panel online, follow these steps:

1. Right-click the panel in the Hardware Tree.

2. Hover over **Panel Control** and select **Start**. The panel status will change from **Unknown** to **Starting** and then to an **Online** state. Once it’s online, the panel is successfully communicating to the server and will be supervised based on the check-in time programmed in the Entré connection.

Next, pull panel hardware configuration from the panel and add it to the Entré database.

1. Right-click the panel in the Hardware Tree.

2. Hover over **Panel Configuration** and select **Download Configuration**. An additional window will open with device types available for selection.

**Note:** This process does not retrieve panel user codes, profiles, holidays, or schedules from the panel. Those items will need to be entered from Entré and sent to the panel after the panel hardware has been added to the database.

From the **Download Configuration** window, selecting an option and selecting **OK** will bring configuration from the panel into the Entré database. During this process the panel status changes from **Online**, to **Get Configuration**, to **Updating Status**, and then back to **Online**.

**Using the New Panel Wizard**

1. Right-click the **DMP Driver** device in the Hardware Tree and select **New Panel Wizard**.

2. Enter all of the information shown in the **DMP Panel Wizard** screen and select **Finish**.
LICENSING THE SOFTWARE

Once you have installed and configured Entré and finalized your add-on modules and client license requirements, it is time to license your software. Any future add-on modules or client license additions will require a new license to be generated. Before you continue, verify that you have accounted for everything. Then, go to the Entré Licensing website listed below:

- DMP.com/License/Entre/

Enter the information requested and submit the license request. DMP Customer Service will validate your request against the order you submitted. Your license will be generated and e-mailed to you.

**Note:** If you request a module on your license that is not on the order submitted through customer service, a customer service representative will attempt to contact you using the phone number listed on the form.

After you receive your new license, you will have to unzip the license, apply the license, update the database, and make sure it works. Follow the instructions that come with the license to ensure that it is installed properly.

1. From the server machine, exit the Entré Client and shut down the Entré Application Service manually within Windows.
2. Rename the default license file named `vx.license.properties` located in the C:\Program Files\DMP\Entré directory to `vx.license.properties.bak`.
3. Unzip and then copy the new license file into that directory.
4. Navigate to the C:\Program Files\DMP\Entré\utilities directory and run the `Entré-plugin-upgrade-sqlserver-windows.bat` file located there.
5. Restart the Entré Application Service and start Entré.
6. Verify that your purchased modules and client licenses are functional.

**Note:** Modules that are licensed on a per-seat basis will have to be assigned to the workstation through the software licenses workstations menu.
User Code Profiles

The panel supports 99 profiles in each panel and can support schedules, if desired. The schedules are enforced by creating time schedules and assigning them to a user code profile. This feature allows managers to restrict access to a building or area. The profile only grants access during the specific time listed in the area schedule. When the card is swiped the profile schedule is checked against the profile’s time schedule and access is granted if the profile schedule is within the time schedule.

Access can also be restricted by associating door devices with burglary or access areas. If the area is listed in the device access area listing then it can be used to gain access to a door as long as that area is not armed. This arming and disarming can also be done through automatic arming and disarming via a time schedule.

The Entré User Codes Profile menu is the central database location for the User Code Profiles for all the panels in the system. Profiles in Entré can be created for each panel individually or can span multiple panels.

Note: If a new panel is added to the system after the initial set up, the technician will need to edit each profile and verify that the new panel’s areas are added to the Access Area and Arm/Disarm Area sections.

The profile menu in Entré is very similar to Remote Link. There are multiple sets of panel areas to select from, which Remote Link does not support. This ability to assign more that one panel to a profile is one of the features that makes Entré so powerful. When a profile is changed and saved, that change is sent to each affected panel.
**Personnel Records, Badges, and User Codes**

The Entré Personnel Records module is the central database location for all personnel records in the system. From this menu, you can add users to the system, assign user codes, as well as access credentials. Personnel records are stored in the database with separate fields for first and last name.

Users can be assigned multiple badges in Entré. A user arming code is a badge; a proximity card used for door access is also a badge. Each badge is assigned a user code profile just like in Remote Link, but in Entré you can assign profiles that span multiple panels. This allows you to update a user by changing their permissions in one place. Changes made to a badge or personnel record are automatically updated in each affected panel when the record is saved.

All personnel and user information entered in Entré is stored in the SQL database, even the picture from the badge.

The only data stored in the panel is the panel user number, first and last name, internal user code, and the profile number (and pin code if the panel has the Card Plus Pin option enabled).

When connecting with Remote Link it is important to not send panel programming to a panel under control of the Entré database. Sending programming to a panel from Remote Link will overwrite the user codes in the panel that were sent from Entré. This may, among other things, cause a user to appear multiple times in the user code list. To correct this, perform a clear and send from Entré to re-sync the panel with the software.

When programming a panel with Remote Link, programming changes will be sent to the panel when you select **Apply** or **OK** on the current screen to save new zones or areas. Perform the **Download Configuration** command in the Entré Hardware Tree after adding new areas, doors, or zones to the system.
Sending Personnel Records, User Codes, and Profiles to the Panel

You can create User Code Profiles and Personnel Records and then assign user codes to badges. For newly added panels, these profiles and records need to be sent to the panel by following this process:

1. Right-click on the panel in the Hardware Tree, hover over Panel Configuration, and then select Download Configuration. See Figure 4.

2. Select Users and Profiles and Clear Users and Profiles and then select OK.

Entré will connect to the panel and the Personnel Records, User Codes, and User Code Profiles will be sent to the panel. This will clear out any existing user codes and profiles in the panel and send them from Entré. From this point forward all user code and profile changes should be made from Entré.

Calendars and Holidays

Creating a calendar is the first step to setting up holidays.

1. Select Calendars from the Configuration menu.

2. Select Add and assign a Name to the calendar. You can have one, or as many as you like, but you can only assign one calendar to each panel.

3. Select Holiday from the side menu and select Add.

4. Enter a Name, Date, and Duration. Then, assign any relevant Categories.

5. Select Save and Close.

Holidays are stored in the calendar and are global to the panel based on the calendar that is selected in the panel menu.

Holidays are exceptions to arming and door schedules and take effect at midnight or hour 00:00 of the day that you assign it. They end on midnight that night or hour 23:59 for the duration (number of days) that you specify.

Assign the calendar and three classes to their respective field (A, B, C) in the Hardware Tree by right-clicking on the panel, selecting Edit, and selecting Calendars.

You can use a different calendar for each panel or use the same calendar for each panel in your database. Changes made to the calendar are sent to the panels when schedules and holidays are sent from the panel configuration download menu in the Hardware Tree.
Area, Door, Output, and Time Schedules

Time schedules for automation rules and event policies are created and stored in the Software Schedules module. Time schedules for areas, outputs, and doors are created and stored in the Panel Schedules module and can be assigned to panel areas for arming and shift schedules, outputs for output relay schedules and to doors for door schedules.

Creating Area, Door, or Output Schedules

1. Select Panel Schedules from the Configuration menu.
2. Select Add and enter a Name and Usage type for the schedule.
3. Enter the Start and Stop times and select Save and Close.

Assigning Area Schedules

1. Right-click the area icon in the Hardware Tree and select Edit.
2. Select Area Schedules and select Add.
3. Enter a schedule number (1-8) and select a time schedule from the Schedule drop-down list.
4. Select Save and Close.

Note: The maximum number of schedules per area is 8.

Assigning Door Schedules

1. Right-click on the keypad or door icon in the Hardware Tree and select Edit.
2. Select Door Schedules from the menu and then select Add.
3. Select the appropriate time schedule from the drop-down list and select Save and Close.

Note: The maximum number of schedules per door access relay is 8.

Assigning Output Schedules

1. Right-click on the output icon in the Hardware Tree and select Edit.
2. Select Output Schedules from the menu and then select Add.
3. Select the appropriate time schedule from the drop-down list and select Save and Close.

Note: The maximum number of schedules you may assign per relay output is 8.
Sending Schedules and Holidays to the Panel

Follow these steps to send schedules and holidays to the panel (or panels). Holidays are sent when you send the schedules to the panel.

1. Right-click on panel, hover over Panel Configuration, and select Download Configuration.
2. Check the Schedules option and select OK.

**Note:** If this is a new installation make sure to check Clear Schedules to clear the current schedules out of the panel. This is very important the first time schedules are sent to make sure that old data is cleared out of the panel.

**Pro Tip**

When you perform a clear and send from Entré, user access may be momentarily effected.
**IPCONFIG**
This Windows utility provides diagnostic information related to TCP/IP network configuration. Ipconfig also accepts various Dynamic Host Configuration Protocol (DHCP) commands, allowing a system to update or release its TCP/IP network configuration.

To run the *ipconfig.exe* utility, at a command prompt, type `ipconfig`, and then add any appropriate options.

- `ipconfig` (with no parameters specified) will display only the IP address, subnet mask, and default gateway for each adapter that is bound to TCP/IP.
- `ipconfig /all` displays all of the current TCP/IP configuration values, including the IP address, subnet mask, default gateway, and Windows Internet Naming Service (WINS) and DNS configuration.

**Ping**
Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

Ping verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. You can use ping to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might have a name resolution problem.

**NSLOOKUP**
Nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through the PC’s Control Panel. Nslookup.exe can run in two modes: interactive and non-interactive. Non-interactive mode is useful when only a single piece of data needs to be returned.

- The syntax for non-interactive mode is `nslookup [-option] [hostname] [server]`
- To start *Nslookup.exe* in interactive mode, simply type `nslookup [domain name]` into the command prompt. The domain name and addresses will be returned.

Typing “help” or “?” at the command prompt will generate a list of available commands.
Anything typed at the command prompt that is not recognized as a valid command is assumed to be a host name and an attempt is made to resolve it using the default server.

- To interrupt interactive commands, press Ctrl+C.
- To exit interactive mode and return to the command prompt, type exit at the command prompt.

Refer to the Microsoft Support Knowledge Web Page for further information on using this utility.

- Support.Microsoft.com/kb/200525

**TCPING**

TCPING measures the latency of a TCP connection. It connects and then disconnects, measuring the time it takes to get a SYN, SYN+ACK, ACK+FIN and FIN packet across the network. TCPING is a utility that can be downloaded from the Internet and installed on the site PC.

TCPING does a TCP connect to the given IP/port combination. The user can specify a timeout in seconds. This is useful in shell scripts running in firewalled environments. Often SYNs are just being dropped by firewalls, thus connection establishment will be retried several times (for minutes) until a TCP timeout is reached. With TCPING it is possible to check first if the desired port is reachable and then start connection establishment.

**Exit Codes**

- -1: an error occurred
- 0: port is open
- 1: port is closed
- 2: user timeout

**Syntax**

tcping [-q] [-t timeout_sec] [-u timeout_usec] <ip addr> <port>

- -q : quiet mode, do not output anything (except error messages)
- -t : timeout in seconds
- -u : timeout in microseconds
Wireshark can help you verify communication between the panel and Entré. The panel network interface card for an XR550 Series panel is a 100BASE-T full duplex hardware connection. Your network might have to be configured to allow bidirectional communication on the port programmed in either path communications or Remote Options menus. Wireshark can be programmed to filter out unwanted packets and only show the communication between your server PC and the panel by using the following filter:

```
host <space> (ipaddressofpanel) xxx.xxx.xxx.xxx
```

This filter will only show TCP packets between the host PC and the panel IP address in the filter. Figure 5 shows a successful restart command and subsequent connection from Entré to the panel.

![Figure 5: Wireshark Restart Command](Image)