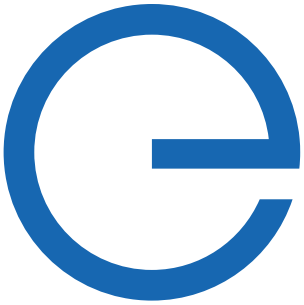


ENTRÉ

SERVER MAINTENANCE GUIDE

A Maintenance Guide for IT Teams and Administrators

TABLE OF CONTENTS

SERVER MAINTENANCE

Below is an overview of recommended Entré 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 link below.

Microsoft Maintenance Plans
https://docs.microsoft.com/en-us/sql/relational-databases/maintenance-plans/maintenance-plans?view=sql-server-ver15

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

MS 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 MS 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 to as close to 10% as possible. Also, ensure there is enough actual drive space to accommodate that growth.

Check Disk Drive Contention

WEEKLY

Ensure that there is not too much 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.

Database Integrity Check

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 SQL's built-in functionality to find what tables need additional indexes.

Parallelism

MONTHLY

When you run a SQL query it will try to spread that query across all four 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. To see this, look at the weight states for threads on the 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.

ADMINISTRATOR TASKS

Starting Entré

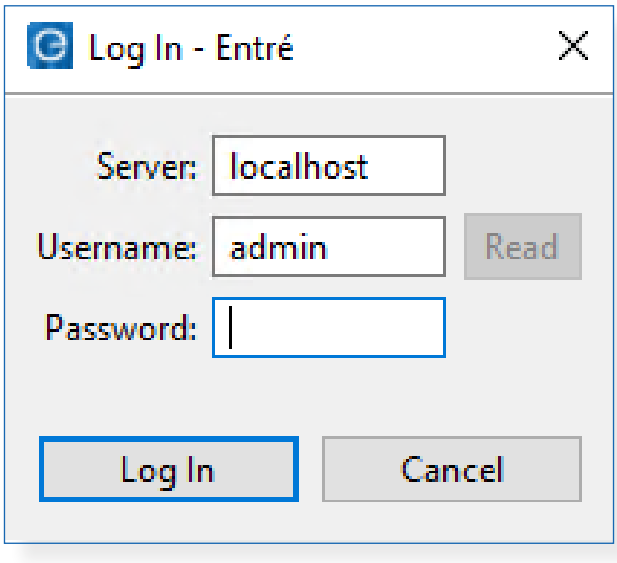
Upon starting, Entré will open a splash page displaying the start-up progress. Enter the IP address or host name of the server machine and log in with a valid username and password.

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.

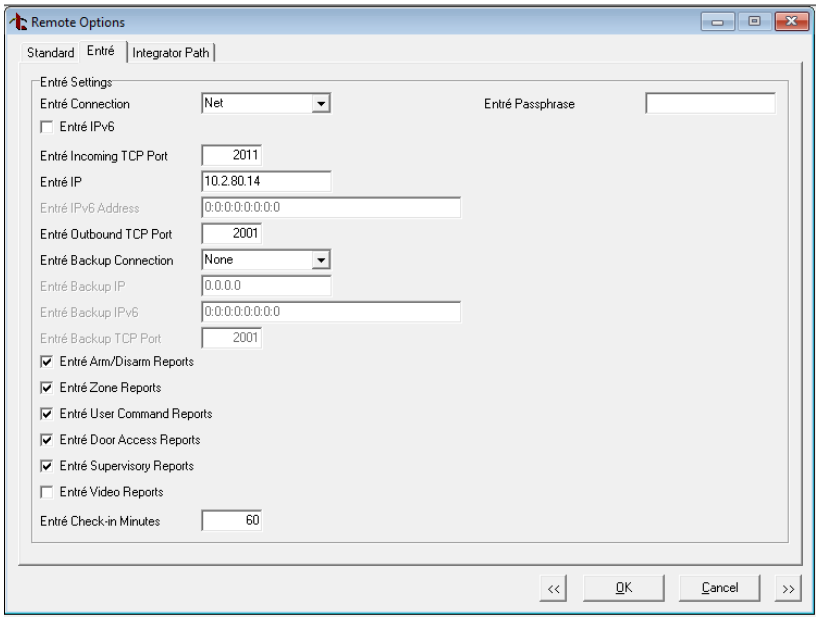
If problems continue, contact your system administrator. If you are the system administrator and cannot resolve the issue, contact your Entré distributor or system installer.



Configuring and Programming Systems

Warning: For systems to work with Entré successfully, you must 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.



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

Enter the primary Entré IP address for the Entré App server. This is 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

Enter a secondary IP address for the Entré app server. This is used in case the connection to the primary IP fails. This may be left blank. In most cases, this is not used.

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 AES-128 Encryption between the panel and Entré, 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.

Configure 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.

Configure the Panel for Real-Time Status

Entré will display real-time status 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.

Only enable real-time status on key devices, zones, or outputs that you must see continual status updates on. Enabling real-time status will add a significant amount of events for the server to process for each door or zone.

Note: Do not enable real-time status for devices, zones, or outputs that will have an excessive amount of activity that will not contribute to your security posture. For example, a PIR in a lobby would have too much activity to enable real-time status for this device.

- Door Status - turn on Door Real-Time Status for each access device in the Device Setup section of the Programmer Menu
- Zone Status - turn on Zone Real-Time Status for each zone in the Zone Information section of the Programmer Menu
- Output Status - turn Output Real-Time Status on for each output in the Output Information section of the Programmer Menu

Add a Panel in Entré

For information about adding and managing a panel, refer to the appropriate sections in LT-2495 Entré Operator's Guide.

Swap a Panel in Entré

For information about swapping a panel, refer to the appropriate section in LT-2495 Entré Operator's Guide.

Delete a Panel in Entré

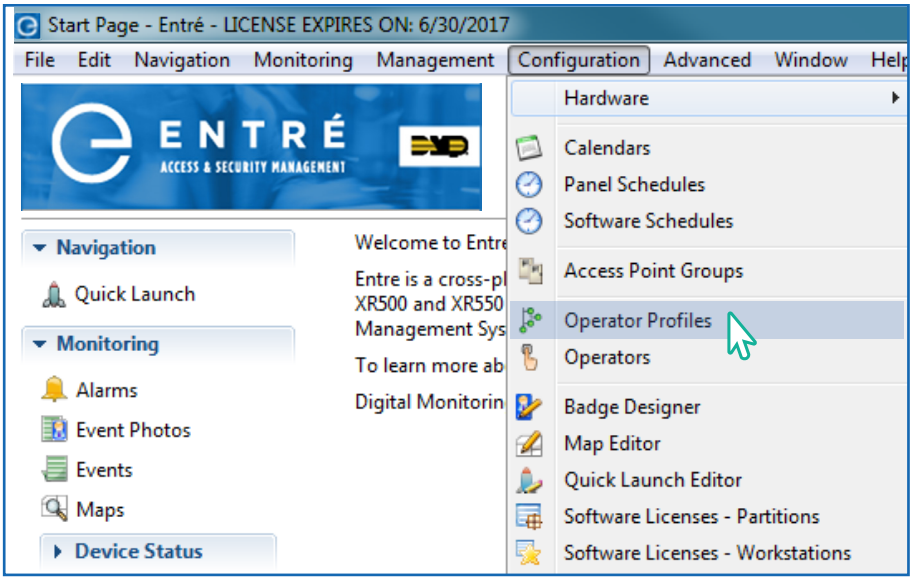
For information about deleting a panel, refer to the appropriate section in LT-2495 Entré Operator's Guide.

Configure Entré for the Operator

In order to create a new operator login, use an existing profile or create a new profile. Profiles determine an operator's access to the Entré application.

1 Create the Operator Profile.

a. Go to **Configuration** > **Operator Profiles**.



b. Select **Add**.

c. In **Template**, select one of the following:

- **Most Restrictive**: Allows only restricted use of the application. It does not allow access to any modules and does not allow to change passwords.
- **Least Restrictive**: Allows almost unlimited use of the application. It allows access to all the modules and allows the profile to change passwords. This option is recommended for new profiles.
- **Default**: Gives minor use of the application. The profile is allowed to change the password, but it does not have access to any modules.

d. Select **OK**.

e. Enter a profile name and select each module that the profile should have permission to access.

f. Select **Allow access to the application** and select **Save and Close**.

2 Create the user and add the user to the operator profile.

a. Go to **Configuration** > **Operators**.

b. Select **Add**, then complete the following required fields: Username, Password, Confirm password.

c. In **Assigned to**, press **Select** and assign the login to a personnel record.

d. To assign privileges to the login, go to **Profiles**.

e. Select the profile that the login should have access to. A profile can be assigned to more than one location.

f. Press **Save and Close**.

g. To verify changes and operator permissions, log out of Entré, then log in as the new operator.

Refer to LT-2495 Entré Operator's Guide for more information about Entré Personnel and Users.

3 Configure the Data Types tab.

a. Expand the **Data Types** tree.

b. In **Access Level** and select **View**.

c. In **Badge**, select **View**, **Create**, **Modify**, and **Delete**. This will grant the profile full access to the Badges module.

d. In **Event**, select **View**.

e. In **Personnel Record**, select **View**, **Create**, **Modify**, and **Delete**. This will grant the profile full access to the Personnel module.

f. Press **Save and Close**.

4 Create a login for the badge privileges profile.

a. Go to **Configuration** > **Login**.

b. Select **Add**.

c. Name the login *Badge Privileges* and enter a password.

d. In **Profiles**, select **Badge Privileges**.

e. Press **Save and Close**.

f. To test the profile, log out of Entré, then log back in with the new profile.

SINGLE SIGN-ON VS. ACTIVE DIRECTORY

Overview

Entré has the capability to control users' access to systems with single sign-on and Active Directory.

Single Sign-On (SSO) gives users the ability to log in to a system with one username and password that grants access to multiple parts of the system. For example, a user management system at a retail chain's corporate HQ allows employees to sign into a computer, then uses an authentication token to automatically sign them in to their email and programs.

Active Directory (AD) is a centralized user management feature included with Microsoft® operating systems that allows system administrators to manage users on a Windows® domain. For example, a college system administrator uses Active Directory to restrict access to specific network drives by assigning students to a pre-defined student user group.

How Does Single Sign-On Relate to Active Directory?

Active Directory is often used as a source for user credentials, which allows Single Sign-On services to integrate with systems already managing users with Active Directory. These integrations allow SSO to use AD information to control access to non-Windows products like web applications.

How Entré Uses SSO

In Version 8.4.0 and higher, Entré supports using SSO to authenticate users for Entré and panel access.

Full Client

After the Entré full client is installed and a local Windows user is assigned an operator profile, the user is automatically logged in to the full client with their Windows credentials. The user may perform the functions allowed according to the operator profile assigned to them.

Web Client

Use PingFederate® or PingAccess® software from Ping Identity® to interact with Active Directory and create a certificate based on predetermined program access. The Entré application server uses the certificate sent from the Ping Identity server to allow users to log in to the web client without requiring them to re-enter their credentials. The user may perform the functions allowed according to the operator profile assigned to them.

The following information is needed to configure SSO for the Entré web client:

- **Assertion Attribute Mapping**—The attribute in the IdP that is mapped to the Entré Operator's login username from the SAML Response's Attribute Statement
- **Strict**—When checked, this option provides further validation of the SAML Response formatting for high security implementations
- **IdP Entity ID**—The SSO Service Entity ID (URL) used for validation of the SAML Response
- **IdP Redirect URL**— The IdP-initiated SSO URL from the IdP
- **Assertion Consumer Service URL**— The URL for the SAML Response consuming service (Tomcat). The default is **http://[tomcat-web-server:port]/dmp/entre-acs**.
- **SP Entity ID**— The configurable entity ID for Entré, the Service Provider

For more information about Ping Identity SSO software, refer to PingFederate and PingAccess.

How Entré Uses AD

The Entré NOC Active Directory Service allows organizations to deactivate personnel accounts in Entré for inactive users in the Active Directory. When personnel are disabled in the Active Directory, the Entré Active Directory Service queries both the AD and Entré databases, compares the information, then updates the appropriate table for that personnel record in Entré. The status of the associated personnel account and their badges is changed to inactive in Entré.

To configure Active Directory for Entré, refer to the Entré Active Directory and LDAP Guide (LT-2455).

CONFIGURE SINGLE SIGN-ON

You must have Entré 8.4.0 or higher to set up Single Sign On (SSO).

Configure SSO in Ping Identity

1. The SAML Signing Certificate must be obtained from the IdP so the SAML Response can be validated. Name the certificate **SSO.cer** and save it to the Entré App Server running directory. The default location of this directory is **C:\Program FIles\DMP\Entre** and contains the **vx.license.properties**, **hibernate.properties**, etc.
2. In the PingFederate Admin console, select **PingID Connector**. Then select **Assertion Consumer Service URL** (IPv4).
3. Set **Endpoint** to the address or domain name of the machine the Apache Tomcat Server is running on. The default value is **http://[tomcat-address:port]/dmp/entre-acs**.
4. Select **Save**.

Configure SSO in Entré

1. Open the Entré Client and navigate to **Configuration** > **System Configuration** > **Single Sign On**.

2. In **Assertion attribute mapping**, enter the assertion value that is in the SAML 2.0 response. This value is passed into Entré as the Operator (Entré Login) username for SSO.

Note: Enable **Strict** for further validation of the SAML Response value and properties for higher security. Include an **Attribute Statement** in the Assertion.

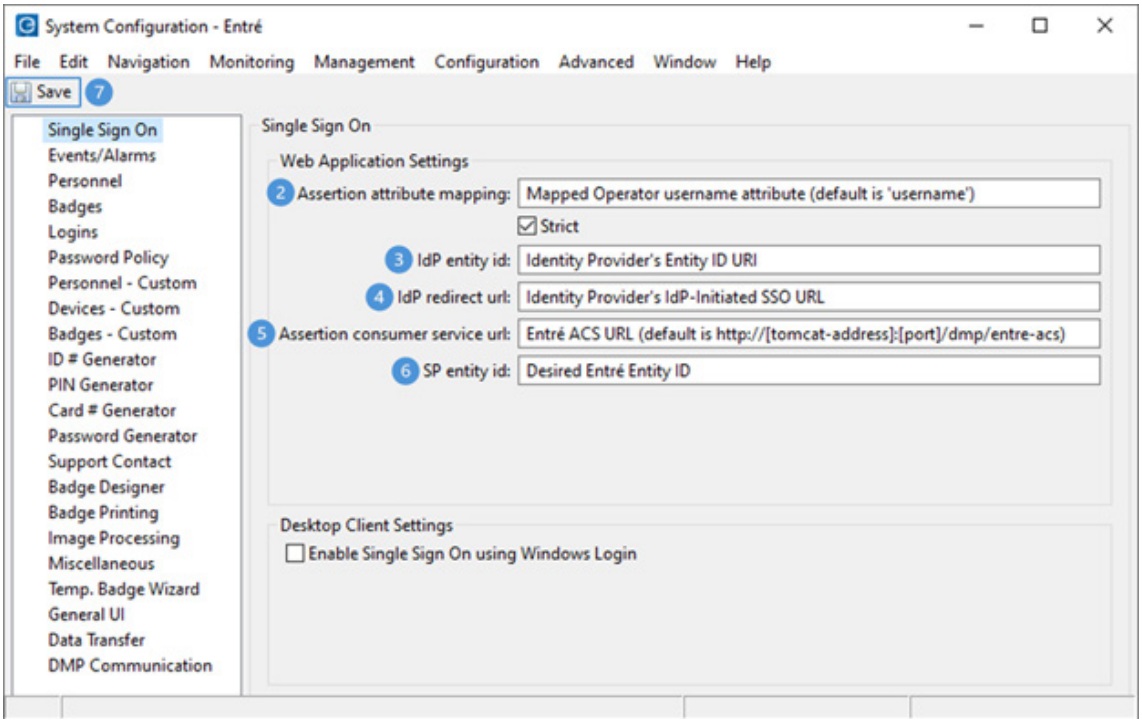
3. In **IdP entity id**, enter the Entré SSO Service Entity ID (URI). This is found in the **PingFederate Identity System** > **Server** > **Protocol Settings** > **Federation Info** > **SAML 2.0 Entity ID**.

4. In **IdP Redirect URL**, enter the IdP-Initiated SSO URL found in the identity provider. Entré redirects the URL to the user to begin the authentication process.

Note: Entré does not send a SAML Request to the IdP. Enter the IdP-Initiated SSO URL in this field.

5. In **Assertion consumer service url**, enter Entré's ACS URL. The default is **http://[tomcat-address:port]/dmp/entre-acs**. This is found under **PingFederate SP Connection** > **Protocol Settings** > **Assertion Consumer URL** > **Endpoint** in PingFederate.

6. In **SP entity id**, enter the desired Entré Entity ID. This is used during validation of the SAML Response sent to Entré.



7. Select **Save** and restart the Entré Application Server service.

Add a New Operator

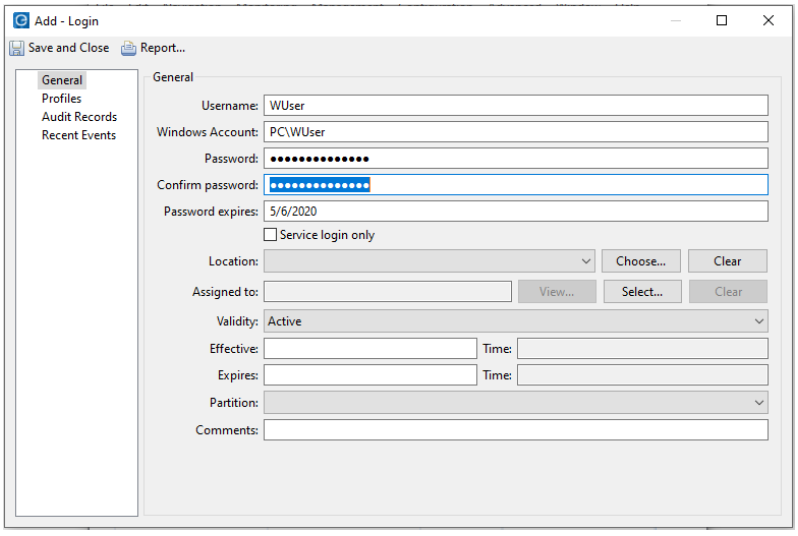
Add a new operator in Entré with any password you want. Entré requires a password to create an operator but authentication will be handled with the identity provider so it won't be used by the web client.

1. Start the Apache Tomcat Service.
2. Enter **http:[tomcat address]:[port]/dmp/entre-sso** in the browser.
3. You will be redirected to the Entré start page.

Set Up the Desktop Client SSO with Windows Login

This feature allows Entré to use the Windows domain user from the machine that is logged in and verifies it against the Entré operator.

1. Open the Entré Client and navigate to **Configuration** > **System Configuration** > **Single Sign On**.
2. Select **Enable Single Sign On using Windows Login**.
3. Restart the Entré Client.
4. Create a new operator, adding their Windows domain user and an Entré password. This Entré password is separate from their Windows password and is required to create the operator but is only used if the local user can't be authenticated. The **Windows Account** is the local domain and the windows username, separated by a backslash (\).



TROUBLESHOOTING

Network and DBMS

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

Using Wireshark

Wireshark can help you verify communication between the panel and Entré. The panel network interface card for an XR550 Series or TMSentry 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. Below shows a successful restart command and subsequent connection from Entré to the panel.