TERMINAL MANAGER
Release 680

Maintenance Guide
TM DOC-X22-en-680A
October 2019
DISCLAIMER

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.
While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.
In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.
Copyright 2019- Honeywell International Sàrl
Contents

1 Contents iii
i About This Guide 5
  Release Information ................................................. 5
  Related Documents ..................................................... 5
  Audience .................................................................. 5
  Symbol Definitions ....................................................... 6
  Acronyms and Meanings ................................................. 7

1 Troubleshooting Data Collection-Related Issues 9

2 Troubleshooting Installation-Related Issues 11
  Troubleshooting Installation-Related Issues ....................... 12
  Security exceptions while opening Terminal Manager application through thick
  client/browser on Experion PKS or Terminal Manager servers ........................................ 12
  Terminal Manager services are not starting ........................................ 14
  E-mail generation process is not canceled automatically after the configured time-out value 15
  E-mail Generation process is not triggered ........................................ 16

3 Troubleshooting Terminal Manager Usage-Related Issues 21
  Troubleshooting scenarios .............................................. 22
  Unable to start the Executables from the Process Monitor Service ............... 22
  PCDET throws the exception “Server Error in Application. Its client machine and hence
cannot show the error messages.” .......................................... 22
  Date-Time and Value Conversions parsing errors reported in Terminal Manager Log files 23
  Unable to logon to the Terminal Manager Administration Tool ....................... 23
  Thick Client tool throws unhandled error “Service Unavailable” ....................... 24
  Terminal Manager application not working if the service account password is changed 24
  Please see “get-help about_signing” for more details ........................................ 27
  An object at specified path \Servername\Diagnostics does not exist ..................... 28
  Users are unable to view SQL jobs after logging on using their SQL credentials ....... 33
  Issues with Notification, missing Notifications or COM exceptions from the Terminal
  Manager application or other Terminal Manager components .......................... 33
  RPC server is unavailable .............................................. 35
  Session lost when using hostname with underscores in URL instead of IP address .... 35
  Menu does not list items in Terminal Manager when Thick Client is invoked with user who
does not have administrator privileges ........................................ 36
Primary Port is invalid. ................................................................. 38
Removed Printers shown in Printer Configuration page. .................. 39
Invalid key pressed ................................................................. 40
PCDET device is invalid .......................................................... 40
Terminal closed ........................................................................ 42
Non-working Terminal time ...................................................... 43
Logon account should have permission for all Shareholders .......... 44
Meter Reconciliation Report shows the start totalizer as zero ......... 47
Meter or tank reconciliation report is generated without data or the error “No reconciliation code is available” is displayed. ......................................................... 48
Touch screen DEU <<Name>> Response not updated to Terminal Manager ......................................................... 49
CardReader App logs cyclic notification (Active/Inactive) in Terminal Manager application and in Experion PKS ................................................................. 49
Transaction batch details has “Zero” quantity updated in case of the BCU power failure during loading ................................................................. 50
In Rail Dispatch, for the loaded quantity less than the preset quantity, the wagon status should display “Partially filled” rather than “EMPTY” ........................................... 50
The target principal name is incorrect ........................................ 51
“Invalid Password” message displayed on entering valid password during validation on BCU workflow ................................................................. 56
Event ID 7034 ........................................................................... 56
Error occurred in open day while using Terminal Manager client ... 58
Unable to print .......................................................................... 59

4 Database Maintenance and Backup 61

5 DCH Certification 65

Change Certificate in Experion Server ........................................ 66
Change Certificate in ERP/Integration Server ............................... 68
To view Thumbprint .................................................................. 70
Trusting the Certificate ............................................................ 71

6 Notices 73
About This Guide

This guide describes the various troubleshooting scenarios.

Release Information

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Document ID</th>
<th>Release Number</th>
<th>Publication Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Manager Maintenance</td>
<td>TMDOC-X222-en-680A</td>
<td>680.1</td>
<td>October 2019</td>
</tr>
<tr>
<td>Guide</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Documents

Further information about Terminal Manager can be found in the following documents.

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Manager Installation Guide</td>
<td>For installing the Terminal Manager application.</td>
</tr>
<tr>
<td>Terminal Manager Configuration Guide</td>
<td>For configuring the Terminal Manager application.</td>
</tr>
<tr>
<td>Terminal Manager User’s Guide</td>
<td>For overall usage of the Terminal Manager application.</td>
</tr>
</tbody>
</table>

Audience

The audiences for this guide are the Terminal Manager operators, planners, supervisors, and managers who are responsible for troubleshooting the error scenarios.
# Symbol Definitions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Attention" /></td>
<td><strong>ATTENTION</strong>: Identifies information that requires special consideration.</td>
</tr>
<tr>
<td><img src="image" alt="Tip" /></td>
<td><strong>TIP</strong>: Identifies advice or hints for the user, often in terms of performing a task.</td>
</tr>
<tr>
<td><img src="image" alt="Caution" /></td>
<td><strong>CAUTION</strong>: Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices. <strong>CAUTION</strong> symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td><strong>WARNING</strong>: Indicates a potentially hazardous situation, which, if not avoided, could result in serious injury or death. <strong>WARNING</strong> symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.</td>
</tr>
<tr>
<td><img src="image" alt="Esd" /></td>
<td><strong>ESD HAZARD</strong>: Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices.</td>
</tr>
<tr>
<td><img src="image" alt="Warning, Risk of Electrical Shock" /></td>
<td><strong>WARNING, Risk of electrical shock</strong>: Potential shock hazard where HAZARDOUS LIVE voltages greater than 30 Vrms, 42.4 Vpeak, or 60 VDC may be accessible.</td>
</tr>
<tr>
<td><img src="image" alt="Reference - Internal" /></td>
<td><strong>REFERENCE - INTERNAL</strong>: Identifies an additional source of information within the bookset.</td>
</tr>
<tr>
<td><img src="image" alt="Reference - External" /></td>
<td><strong>REFERENCE - EXTERNAL</strong>: Identifies an additional source of information outside of the bookset.</td>
</tr>
<tr>
<td>Terminology</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>ATG</td>
<td>Automatic Tank Gauging</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Process</td>
</tr>
<tr>
<td>BCU</td>
<td>Batch Controller Unit</td>
</tr>
<tr>
<td>BOL</td>
<td>Bill of Lading</td>
</tr>
<tr>
<td>COM</td>
<td>Component Object Model</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>DET</td>
<td>Data Entry Terminal</td>
</tr>
<tr>
<td>DEU</td>
<td>Data Entry Unit</td>
</tr>
<tr>
<td>EXE</td>
<td>Executable</td>
</tr>
<tr>
<td>Experion PKS®</td>
<td>Experion Process Knowledge System</td>
</tr>
<tr>
<td>FAN</td>
<td>Filling Advisory Note</td>
</tr>
<tr>
<td>IS ESC</td>
<td>Internet Explorer Enhanced Security Config</td>
</tr>
<tr>
<td>MON</td>
<td>Motor Octane Number</td>
</tr>
<tr>
<td>PCDET</td>
<td>PC-based touch-enabled Data Entry Terminal</td>
</tr>
<tr>
<td>PPM</td>
<td>Parts Per Million</td>
</tr>
<tr>
<td>RON</td>
<td>Research Octane Number</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>UOM</td>
<td>Unit of Measurement</td>
</tr>
<tr>
<td>WIS</td>
<td>Windows Integrated Security</td>
</tr>
<tr>
<td>DCH</td>
<td>Data Clearing House Ex: TABS/TDS</td>
</tr>
</tbody>
</table>
ABOUT THIS GUIDE
1. Troubleshooting Data Collection-Related Issues

The Terminal Manager logs are collected in \textit{C:\ProgramData\Honeywell\TerminalManager\Diagnostics} folder. The sub modules like Workflow and Terminal Manager User Interface are captured in a separate folder under the same path.

If there are any issues in those modules then the user must share the log files from the Diagnostic folder for troubleshooting the issue.
2. Troubleshooting Installation-Related Issues

This chapter describes how to troubleshoot the installation-related issues.
2.1 Troubleshooting Installation-Related Issues

2.1.1 Security exceptions while opening Terminal Manager application through thick client/browser on Experion PKS or Terminal Manager servers

Reason

This exception might occur if you launch the Terminal Manager User Interface in Terminal Manager server. The Terminal Manager Servers run on the Windows Server Operating System. Therefore, the security level is higher in the Terminal Manager Server machines than in the Terminal Manager Client machine.

Resolution

If security exceptions are thrown while opening Terminal Manager through thick client or browser on the Experion PKS or Terminal Manager servers, perform the following steps.

1. Close all the instances of Internet Explorer.

2. Choose Start > Administrative Tools > Server Manager. Right-click Server Manager and select Run as administrator.
The **Server Manager** window appears.

3. In the **Security Information** section, click **Configure IE ESC**.
The Internet Explorer Enhanced Security Configuration dialog box appears.

4 Under Administrators, select Off to disable the enhanced security configuration.

5 Under Users, select Off to disable the enhanced security configuration.

6 Click OK.

The enhanced security configuration is complete. You can launch the Terminal Manager User Interface in Terminal Manager server.

2.1.2 Terminal Manager services are not starting

Reason

The Terminal Manager services do not start when Terminal Manager is installed with different credentials for Process Monitor Service and COM+ services.
TROUBLESHOOTING INSTALLATION-RELATED ISSUES

Resolution
You must configure the Process Monitor service and COM+ service users as a part of Terminal Manager security users.

REFERENCE - EXTERNAL
For more information about creating users, refer to Terminal Manager 680.1 Configuration Guide.

2. 1.3 E-mail generation process is not canceled automatically after the configured time-out value

Reason
This exception might occur if the transaction time-out value is not configured on the primary and secondary web servers.

Resolution
Whenever a report is generated in Terminal Manager, an automated e-mail alert is generated by the e-mail generation process and sent to the configured recipients.
To trigger the e-mail generation process, you must set the transaction time-out value on both the primary and secondary web servers. The process is automatically canceled if it takes longer than the configured time-out value.

Attention
Ensure that you configure the transaction time-out value only if you have installed the Email Service feature.

To configure timeout settings
1 Choose Start > Run.
2 Type dcomcnfg.
The Component Services window appears.
3 Choose Console Root > Component Services > Computers > My Computer.
4 Right-click My Computer and then select Properties.
The My Computer Properties dialog box appears.

5 Click the Options tab.
The default value for the transaction timeout is “60” seconds.

6 In the Transaction timeout (seconds) box, type 300 seconds as the transaction timeout value.

7 Click Apply and then click OK.
The timeout value for the e-mail generation process is configured.

8 Repeat the above steps on the other web server.

2. 1.4 E-mail Generation process is not triggered

Reason
This exception might occur if the Microsoft Distributed Transaction Coordinator (DTC) is not configured on the primary and secondary web servers.
Resolution

If you have installed the e-mail server components on a redundant web server, you must configure the Microsoft Distributed Transaction Coordinator (DTC) on both the primary and secondary web servers, to trigger the e-mail generation process.

To configure DTC settings

1. Choose **Start > Run**.
2. Type `dcomcnfg`.
   The **Component Services** window appears.
3. Choose **Console Root > Component Services > Computers > My Computer > Distributed Transaction Coordinator > Local DTC**.
   The following window appears.
4. Right-click **Local DTC** and then select **Properties**.
The **Local DTC Properties** dialog box appears.

5. Click the **Security** tab.

6. Under **Security Settings**, select the following options.
   - Network DTC Access
   - Allow Remote Clients
   - Allow Inbound
   - Allow Outbound
   - No Authentication Required
   - Enable SNA LU 6.2 Transactions

7. Click **Apply**.
The following dialog box appears asking your confirmation to stop and restart the Microsoft DTC service.

8 Click **Yes**.

A dialog box appears indicating that the MSDTC service is restarted.

9 Click **OK**.

10 Click **OK** to close the **Local DTC Properties** dialog box.

The DTC settings are configured.

11 Repeat the above steps on the other web server.
3. Troubleshooting Terminal Manager Usage-Related Issues

This chapter describes how to troubleshoot the Terminal Manager day-to-day usage-related issues.
3.1 Troubleshooting scenarios

3. 1.1. Unable to start the Executables from the Process Monitor Service

Reason

Process Monitor service is not visible in the Services list.

Resolution

If you are not able to see the Process Monitor Service, perform the following steps to install process monitor manually.

To install the Process Monitor Service manually:

1. Choose Start > All Programs > Accessories > Command Prompt.
2. Right-click Command Prompt and then select Run as administrator. The Command Prompt window appears.
3. Type the following command:

   `sc create Honeywell.TerminalManager.Redundancy.ProcessMonitor
binpath= "C:\Program Files (x86)\Honeywell\TerminalManager\Redundancy\Honeywell.TerminalManager.Redundancy.ProcessMonitor.Service"
displayname= "Honeywell TM ProcessMonitor"

   A pop up message appears asking you to enter the log on credentials.
4. Enter the log on credentials. The Process Monitor service appears.

3. 1.2. PCDET throws the exception “Server Error in Application. Its client machine and hence cannot show the error messages.”

Reason

The error might occur due to issues in Domain Name System (DNS).

Resolution

To resolve this issue, perform the following steps:
**On the web server**

1. Open the “hosts” file available in the `C:\Windows\System32\drivers\etc` folder.
2. Add a line at the end of the file with IP and hostname of the client.
   For example: If the client machine name is “ABC” and if the IP is “10.1.10.100”, then add the line as “10.1.10.100 ABC”.

**On the client machine**

1. Open the “hosts” file available in the `C:\Windows\System32\drivers\etc` folder.
2. Add a line at the end of the file with IP and hostname of the server.
   For example: If the server machine name is “SVR” and the IP is “10.1.10.200”, then add the line as “10.1.10.200 SVR”.

**3. 1.3. Date-Time and Value Conversions parsing errors reported in Terminal Manager Log files**

**Reason**

This error might occur if the regional settings in the server machine are not set to “English (United States)”.

**Resolution**

To configure regional settings

1. Choose **Start > Control Panel**.
   The **Control Panel** window appears.
2. Click **Region and Language**.
   The **Region and Language** dialog box appears.
3. In the **Formats** tab, click **English (United States)** in the **Formats** drop-down list.
4. Click **OK**.
   The regional settings are configured.

**3. 1.4. Unable to logon to the Terminal Manager Administration Tool**

**Reason**

If an administrator changes the system password in the login credentials, then the administrator cannot logon to the Terminal Manager Administration tool.
Resolution

It is recommended to configure multiple administrators for the system. The administrator who has changed the system password for the login credentials must log off. Another administrator can log on to the system and open the Terminal Manager Administration tool and then change the services password.

3. 1.5. Thick Client tool throws unhandled error “Service Unavailable”

Reason

After a successful database switchover, when the thick client is refreshed, the thick client fails to connect to the active web server.

Resolution

Close and open the Thick Client tool.

3. 1.6. Terminal Manager application not working if the service account password is changed

Reason

The Terminal Manager Administration tool derives authentication from the COM+ security which in turn depends on the bootstrap user account. If the bootstrap user changes the password in the Domain Controller machine, there is a deadlock for login to Terminal Manager. Therefore, no user can change the password and the Terminal Manager functionalities do not work.

Resolution

The user cannot change the password of the Terminal Manager components through the Terminal Manager Administration tool. In this case, the user has to manually change the password in the COM+ applications and then use the Terminal Manager Administration tool to reset the password for other Terminal Manager services.

To change password

1. Choose Start > Run, and then type dcomcnfg.
The Component Services window appears.

2 Choose Component Services > Computers > My Computer > COM+ Applications.

3 In the right-pane, right-click TerminalManagerApplication, and then select Properties.
The TerminalManagerApplication Properties dialog box appears.

4 Click the Identity tab.
5 Under This user, perform the following:
   a. Verify the user name.
   b. In the Password box, type the new password for the service account.
   c. In the Confirm Password box, re-type the new password for the service account.
6 Click OK.
   The password is changed for the service account.
7 Right-click TerminalManagerApplication and select Shut Down.
8 Right-click **TerminalManagerApplication** and select **Start**. The Terminal Manager Administration Tool opens.

3.1.7. Please see “get-help about_signing” for more details

**Reason**

This error occurs when you access a destination server's log files from Diagnostic tool installed in a remote client machine. The error occurs as the PowerShell access mode is set as “Restricted”. Therefore, PowerShell does not allow information to be fetched from server.

**Resolution**

You must change the access mode for PowerShell to “Unrestricted”.

Perform the following steps to change the access mode for PowerShell.

1. To open PowerShell, choose **Start > Run**, and type **Powershell**.
2. Enter **Set-Executionpolicy unrestricted**.

**Note**

For a 64-bit machine, execute this command in both 32-bit and 64-bit versions of PowerShell.exe.

A confirmation message appears.

3. Press **Y** to continue.
3.18. An object at specified path `\Servername\Diagnostics` does not exist

Reason

The error occurs if the Diagnostics folder is either not present or it is not shared.

Resolution

Perform the following:

1. Browse to the path `<Drive>/ProgramData/Honeywell/TerminalManager/Diagnostics`. If the path does not exist, create the path.
The following window appears.

2 Share the Diagnostics folder. To share the Diagnostics folder, perform the following steps:
   a. Right-click the Diagnostics folder and click Properties.
The **Diagnostics Properties** dialog box appears.

![Diagnostics Properties dialog box](image)

b. Click the **Sharing** tab and then click **Advanced Sharing**.
The Advanced Sharing dialog box appears.

c. Select the Share this folder check box. Provide the share name similar to the folder name.

d. Click Permissions.
The Permission for Diagnostics dialog box appears.

![Permission for Diagnostics dialog box](image)

e. Click Add.
The Select Users, Computers, Service Accounts, or Groups dialog box appears.

![Select Users, Computers, Service Accounts, or Groups dialog box](image)

f. In the Enter the object names to select box, type the non-administrator user or group.

g. Click OK.
The permissions to access the diagnostics folder by a non-administrative user is provided.
3.1.9. Users are unable to view SQL jobs after logging on using their SQL credentials

**Reason**

The SQL credentials used by the current user might not be authorized to view the SQL jobs for the database server and it appears empty.

**Resolution**

It is recommended to either use the default Windows authentication or the credentials of a designated SQL user who has the authority to view the SQL jobs in the database server.

3.1.10. Issues with Notification, missing Notifications or COM exceptions from the Terminal Manager application or other Terminal Manager components

**Reason**

Terminal Manager uses COM+ applications for specific functionalities and you may receive the following exception.

```
“Stem.Runtime.InteropServices.COMException (0x80080005): Server execution failed (Exception from HRESULT: 0x80080005 (CO_E_SERVER_EXEC_FAILURE))”.
```

**Resolution**

You must restart the COM+ components to raise notifications and make Terminal Manager functional again. Perform the following:

1. Launch Terminal Manager redundancy monitor using the desktop shortcut `TMRedundancyMonitor`.
2. Click **Stop TM Services** and wait until the services are stopped.
3. After the services are stopped, click **Start TM Services**. The Terminal Manager COM+ applications are restarted.
Verify whether the Terminal Manager is working and also if the notifications are logged.

If this does not resolve the issue, then you must manually restart the COM+ components from the Windows snap-in. Perform the following:

2. Type dcomcnfg and then click OK. The Component Services window appears.
3. Right-click TerminalManagerApplication and then click Shut down.
4. Verify whether the Terminal Manager is working and also if the notifications are logged.
3. 1.11. RPC server is unavailable

Reason
This error occurs when you want to view the COMPlus applications in the Terminal Manager Monitor tool if the firewall is enabled on the Terminal Manager server.

Resolution
You must disable the firewall on the Terminal Manager server to view the COMPlus applications in the Terminal Manager Monitor tool.

3. 1.12. Session lost when using hostname with underscores in URL instead of IP address

Reason
Session variables are lost when page is posted back if the hostname used in the URL has underscore (_) in it.

Resolution
The hostname must contain only the ASCII letters 'a' through 'z' (in a case-insensitive manner), the digits '0' through '9', and the hyphen ('-'). You must not use any other symbols, punctuation characters, or white space.
3. 1.13. Menu does not list items in Terminal Manager when Thick Client is invoked with user who does not have administrator privileges.

Reason

When a non-administrator user opens Terminal Manager in Thick Client, the user might receive an error and the system might not allow the user to add the Terminal Manager to trusted sites.

Resolution

Add the user to Domain Administrator groups and then open Thick Client. When the user opens Thick Client, the system prompts the user to add Terminal Manager to the trusted sites. Add the Terminal Manager to the trusted sites. After the Terminal Manager is added to the trusted sites, the user can work Terminal Manager on Thick Client. The user can then remove the non-administrator user from Domain Administrator groups. Perform the following procedure for each user when the user logs on to the Terminal Manager on Thick Client for the first time.

To add Terminal Manager to trusted sites

1. Open Internet Explorer.
2. In the menu bar, choose Tools > Internet Options.
The **Internet Options** dialog box appears.

3. Click the **Security** tab, and then click **Trusted sites**.
4. Click **Sites**.
The **Trusted sites** dialog box appears.

5 In the **Add this website to the zone** box, type `http://localhost/tmui`, and then click **Add**.

6 Click **Close** and then click **OK**.

   The Terminal Manager is added to the trusted sites for the logged on user.

7 Repeat the above steps for each user when the user logs to the Terminal Manager on Thick Client for the first time.

### 3.1.14. Primary Port is invalid.

**Reason**

When a non-integer value greater than 2,147,483,647 is entered for the channel port number, while creating and/or updating a device.

**Resolution**

While you are creating and/or updating a device, ensure that you enter a valid integer value less than 2,147,483,647 for the channel port number.
3. 1.15. Removed Printers shown in Printer Configuration page

Reason

When a printer is removed from the Terminal Manager server, the printer name appears with an exclamation mark in the Printer Configuration page. If reports are configured for this printer, then the report print is sent to the unavailable printer. Therefore, the report print fails.

Resolution

The printers that are removed from the Terminal Manager server must be disassociated from the associated locations. To disassociate printer from all the associated locations, perform the following steps.

To disassociate printers

1. From the Terminal Manager menu bar, choose **MISCELLANEOUS > PRINTER CONFIGURATION**.
   The **Printers** page appears.

2. In the **Printer Name** list, click the name of the printer that is removed from the Terminal Manager server.
   The **Printer Configuration** page appears.

3. In the **Report Printer Configuration** tab, clear all the check boxes corresponding to the reports that are configured for this printer associated to the location.

4. Click **Save**.

5. Repeat step 3 for all the locations to which the printer is associated.

6. Click the **Location Printer Configuration** tab.

7. On the left pane, click the location code to which the printer is associated.
   On the right pane, the selected location code and all its associated printers are displayed.

8. Under **Printers**, clear the check box corresponding to the printer that is removed from the server.

9. Repeat steps 7 and 8 for all the locations to which the printer is associated.

10. Click **Save**.
    The printer is disassociated from all the locations.
3. 1.16. Invalid key pressed

Reason

The Contrec 1010CJ BCU does not generate a button press event in BCU when the STOP key is pressed. This clears the displayed message.

Resolution

Continue pressing the actual response to be selected, even if the screen is black after pressing the STOP key. The following section describes a sample scenario.

1. The BCU displays a message Enter Preset.
2. Press the STOP key.
3. Observe whether the message is cleared in BCU.
4. Press Cancel.
   Or
   Enter the actual preset and then press the Enter key, even if the message is not being displayed.
   Workflow proceeds based on the response.

3. 1.17. PCDET device is invalid

Reason

If the client machine is not configured as a location in site view.
Resolution

1. Configure the client machine as a data entry unit in Terminal Manager.
2. Associate the client machine to a location such as entry gate, exit gate, or weighing area in site view configuration.

REFERENCE - EXTERNAL
For more information about configuring devices and locations, refer to *Terminal Manager 680.1 Configuration Guide*. 
3. 1.18. Terminal closed

Reason

If the current date is configured as a holiday in Terminal Manager.

Resolution

If for any reason, the current day is not a holiday, then remove current day from holiday configuration in the Weekend and Holiday Configuration page and open the terminal day in the EOD Administration page.

REFERENCE - EXTERNAL

For more information about configuring holidays and opening terminal day, refer to Terminal Manager 680.1 Configuration Guide.
3. 1.19. Non-working Terminal time

Reason

During the EOD validations at any location, one of the following messages might appear.

- Terminal Closed
- Non-working Terminal time
- WeekEnd time terminal closed
- Terminal under maintenance

The above messages appear due to the Shift, EOD, Weekend and Holiday configuration provided for the terminal in Terminal Manager. If the current terminal time is not within the time range configured for any of the shifts, then the Non-Working Terminal Time message appears.

The above messages might also appear in the batch controller unit during the EOD validations. If you want to change any configurations in the BCU, you must...
use the BCU in the “Password” mode. However, the Workflow application might not allow you to use the BCU in the “Password” mode when the terminal is closed.

Resolution

Perform either or both of the following:

- Ensure that the terminal day is open and the current time is within the time range configured for any of the shifts.
- To use the BCU in “Password” mode when the terminal is closed, you must stop the Workflow application by setting its Status to Locked on the Process Configuration page in the Terminal Manager.

3. 1.20. Logon account should have permission for all Shareholders

Reason

If the role under which PCDET is running on the server does not have the privileges for all shareholders.
Resolution

The user account under which the **PCDETA**pp**P**ool is running must be associated to all shareholders.

REFERENCE - EXTERNAL

For more information about configuring roles, refer to *Terminal Manager 680.1 Configuration Guide*.

1. Choose **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**. Right-click **Internet Information Services (IIS) Manager** and then select **Run as administrator**.

   Or

   Choose **Start > Run**, and then type **inetmgr**.

   The **Internet Information Services (IIS) Manager** window appears.
2. Expand the web server, click **TMPCDETUI**, and then click **Application Pools**.

3. In the **Name** list, click **PCDETTAppPool**.

4. In the **Edit Application Pool** section on the right pane, click **Advanced Settings**.
   
   The **Advanced Settings** dialog box appears.

   ![Advanced Settings dialog box](image)

   - **CPU**
     - Limit: 0
     - Limit Action: NoAction
     - Limit Interval (minutes): 5
     - Processor Affinity Enabled: False
     - Processor Affinity Mask: 4294967295

   - **Process Model**
     - **Identity**
       - Idle Time-out (minutes): 20
       - Load User Profile: True
       - Maximum Worker Processes: 1
       - Ping Enabled: True
       - Ping Maximum Response Time (s): 50

5. In the **Process Model** section, click **Identity**, and then view the user details.
6 Verify whether the user under which the **PCDETTappPool** is running is associated to all shareholders configured in Terminal Manager.

If the user is not associated to all shareholders, perform the following:

a. From the Terminal Manager menu bar, choose **ADMINISTRATION > SECURITY > USERS**.
   The **Users** page appears.

b. In the **First Name** list, select the user under which the **PCDETTappPool** is running.

c. In the **Primary Shareholder** drop-down list, select the primary shareholder to whom the user must be associated.

d. Under **Secondary Shareholder**, select the check boxes to associate the user to the secondary shareholders.

e. Click **Save**.

---

3. 1.21. **Meter Reconciliation Report shows the start totalizer as zero**

**Reason**

This error occurs if there is no meter activity during the reconciliation duration, some leakage records are observed, and/or the end totalizer has changed from the previous run.
Resolution

In order to correct the meter reconciliation report, you can manually enter the transaction details through the Meter Unaccounted Transactions page. Ensure that you provide accurate totalizer values, so that these values are considered when reconciliation is performed again.

You can find the details of missing totalizers records, if any, in the Bay Loading Summary report. You can appropriately make corrections from the Meter Unaccounted Transactions page.

3. 1.22. Meter or tank reconciliation report is generated without data or the error “No reconciliation code is available” is displayed

Reason

This error might occur if there is any mismatch between data and execution time.
Resolution
Whenever the meter and tank reconciliation reports are generated without any data, a background job runs and updates the reconciliation report data into the Terminal Manager database.

You can view the reconciliation data available in the reconciliation report from the **Product Reconciliation Reports** page in Terminal Manager. You can also print or export the data into PDF and/or Excel formats for analysis.

3. 1.23. **Touch screen DEU <<Name>> Response not updated to Terminal Manager**

**Reason**
If the PCDET is not functioning properly, the response is not updated to Terminal Manager.

**Resolution**
Ensure the PCDET is functioning properly so that the Terminal Manager is displayed correctly.

3. 1.24. **CardReader App logs cyclic notification (Active/Inactive) in Terminal Manager application and in Experion PKS**

**Reason**
After the EOD, card reader device logs cyclic messages namely “Inactive” and “Active” in Terminal Manager and Experion PKS. This is a behavior of the card reader device.

**Resolution**
To suppress notifications in Experion PKS, perform one of the following:

- From the **Notification Messages** page in Terminal Manager, set the value of **Notification Location** as **TM Database** for the message code “CardReaderWorkflow0001”.

- If you want to suppress notifications in Experion PKS, set the value of “Notification Location” for the notification codes “CardReaderWorkflow00001” and “CardReaderWorkflow00002” in Terminal Manager database to “2”. The notifications are logged only in Terminal Manager.
3. 1.25. Transaction batch details has “Zero” quantity updated in case of the BCU power failure during loading

**Reason**

This error might occur if the BCU power fails during loading. After you restart the BCU, the transaction might take some time to commit before the workflow can retrieve the correct batch data. The BCU expects a confirmation of the power failure from the operator. Until the confirmation is received, the transaction is not committed. Therefore, the transaction batch details has Zero quantity.

**Resolution**

Perform the following:

1. When the BCU power fails, set the BCU status as **Inactive** in the **Device Configuration** page.
   
   The workflow stops communication with the BCU.

2. When the power is restored back in the BCU and the BCU comes back ON successfully, set the BCU status as **Active**.
   
   The transaction is committed successfully and the workflow updates the transaction details correctly.

---

3. 1.26. In Rail Dispatch, for the loaded quantity less than the preset quantity, the wagon status should display “Partially filled” rather than “EMPTY”

**Reason**

To calculate the loaded status of the wagon, the tolerance quantity UOM of the finished product is used. If tolerance quantity UOM is not configured, then NULL value is used for calculating the loaded status which will result in the above issue.
Resolution

Perform the following:

1. Launch TMUI > Product Info > Finished Product. A list of finished products are displayed.
2. Click on the finished product code which is to be loaded into the wagon.
3. In the finished product details page, enter the tolerance quantity and select the UOM from the drop-down list. Click Save.

3. 1.27. The target principal name is incorrect

Reason

This issue occurs if the e-mail or SMS client components cannot uniquely identify an instance of the respective services. The error is logged in the “Honeywell TM EmailTransmitterService” or “Honeywell TM SMSTransmitterService” log files.

Resolution

Configure a Service Principal Name (SPN) which enables the client to uniquely identify an instance of the service.

To configure SPN for E-mail service

1. Choose Start > Command Prompt.
2. Right-click and select Run as administrator.
   The Command Prompt window appears.
3. Type the command setspn -s EmailProcessor/<MachineName>,<FullyQualifiedDomainName>:<EmailPortNumber><Domain>\<UserAccount>.
   For example: setspn -S EmailProcessor/TMWebserver.TMDomain.com:9001 TMDomain\TMAdmin
4. Browse to the folder where the Honeywell.TerminalManager.EmailProcessorService.exe.config file is available.
   The default path for the file is <InstallPath>/Program Files (x86)/Honeywell/TerminalManager/Email.
5. Open the Honeywell.TerminalManager.EmailProcessorService.exe.config file.
The file appears as follows.

```xml
<services>
  <service behaviorConfiguration="Honeywell.TerminalManager.SNSProcessor.ServiceBehavior" name="Honeywell.TerminalManager.SNSProcessor.SNSProcessor">
    <endpoint binding="netTcpBinding" bindingConfiguration="SNSTcpBinding" name="SNSProcessor" contract="IInterface.ISNSProcessor">
      <identity>
        <servicePrincipalName value="<DomainName>\<UserAccount>/"/>
        <userPrincipalName/>
      </identity>
    </endpoint>
    <endpoint address="net.tcp://localhost:5002/SNSProcessor" />
  </service>
</services>
</configuration>
```

6. In the *identity* string, type:

```xml
<servicePrincipalName value="<DomainName>\<UserAccount>/"/>
<userPrincipalName/>
```

7. Save the file.

8. Browse to the folder where the

   `Honeywell.TerminalManager.EmailTransmitterService.exe.config` file is available.

   The default path for the file is `<InstallPath>/Program Files (x86)/Honeywell/TerminalManager/Email`.

9. Open the

   `Honeywell.TerminalManager.EmailTransmitterService.exe.config` file.
The file appears as follows.

10 In the identity string, type
   
   `<servicePrincipalName value="<DomainName>\<UserAccount>"/>

11 Save the
   
   Honeywell.TerminalManager.EmailTransmitterService.exe.config file.
   
   The SPN settings for the e-mail service is configured.

To configure SPN for SMS service

1 Choose Start > Command Prompt.

2 Right-click and select Run as administrator.
   
   The Command Prompt window appears.

3 Type the command `setspn -s SMSProcessor/`<MachineName>,<FullyQualifiedDomainName>:<SMSPortNumber>
   
   `<Domain>\<UserAccount>`.
   
   For example: setspn -s SMSProcessor/TMWebserver.TMDomain.com:9002 TMDomain\TMAdmin

4 Browse to the folder where the
   
   Honeywell.TerminalManager.SMSProcessorService.exe.config file is available.
   
   The default path for the file is `<InstallPath>/Program Files (x86)/Honeywell/TerminalManager/SMS`. 
5 Open the `Honeywell.TerminalManager.SMSProcessorService.exe.config` file.

The file appears as follows.

```xml
<services>
  <service behaviorConfiguration="Honeywell.TerminalManager.SMSProcessor.ServiceBehavior" name="Honeywell.TerminalManager.SMSProcessor.SMSProcessor">
    <endpoint binding="netTcpBinding" bindingConfiguration="SMSTcpBinding" name="SMSTextPoint" contract="IMGetMessageExchange"/>
    <identity>
      <servicePrincipalName value="<DomainName>\<UserAccount>"/>
      <userPrincipalName/>
      <dns/>
    </identity>
  </service>
</services>
```

6 In the `identity` string, type

```xml
  <servicePrincipalName value="<DomainName>\<UserAccount>"/>
  <userPrincipalName/>
  <dns/>
```

7 Save the `Honeywell.TerminalManager.SMSProcessorService.exe.config` file.

8 Browse to the folder where the `Honeywell.TerminalManager.SMSTransmitterService.exe.config` file is available.

The default path for the file is `<InstallPath>/Program Files (x86)/Honeywell/TerminalManager/SMS`. 
9  Open the **Honeywell.TerminalManager.SMSTransmitterService.exe.config** file. The file appears as follows.

```xml
<appSettings>
  <add key="TagPay" value="SOFTWARE\Wow6432Node\Honeywell\ETAS"/>
  <add key="PrimaryWebServerIPHostName" value="PrimaryWebServer"/>
  <add key="SecondaryWebServerIPHostName" value="SecondaryWebServer"/>
  <add key="PortNumber" value="8088"/>
  <add key="CommandInterval" value="2000"/>
  <add key="MessageInterval" value="1000"/>
  <add key="CommitFailureRetry" value="3"/>
</appSettings>

<system.serviceModel>
  <bindings>
    <netTcpBinding>
      <binding name="SMSSendPoint" closeTimeout="00:01:00" openTimeout="00:01:00" receiveTimeout="00:10:00" sendTimeout="00:10:00" transactionFlow="false">
        <readerQuotas maxDepth="32" maxStringContentLength="8192" maxArrayLength="16384" maxBytesPerRead="65536" maxNameTableCharCount="16384"/>
        <reliableSession ordered="true" inactivityTimeout="00:10:00" enabled="false"/>
        <security mode="Transport"/>
        <transport clientCredentialType="Windows" protectionLevel="None"/>
        <message clientCredentialType="Windows"/>
      </binding>
    </netTcpBinding>
  </bindings>
  <client>
    <endpoint binding="netTcpBinding" bindingConfiguration="SMSSendPoint" contract="SMSServiceReference.ISMSProcessor" name="SMSSendPoint">
      <![CDATA[
        <servicePrincipalName value="\{DomainName}\{UserAccount}"/>
      ]]>
    </endpoint>
  </client>
</system.serviceModel>
</configuration>
```

10  In the *identity* string, type

    `<servicePrincipalName value="\{DomainName}\{UserAccount}"/>

11  Save the **Honeywell.TerminalManager.SMSTransmitterService.exe.config** file.

    The SPN settings for the SMS service is configured.
3. 1.28. “Invalid Password” message displayed on entering valid password during validation on BCU workflow

Reason

This message is displayed in the BCU when a driver tries to enter the password for the access ID configured in Terminal Manager. This issue occurs if different data encryption keys are configured while installing Terminal Manager on various servers.

Resolution

Ensure that the same data encryption key is configured while installing Terminal Manager on various servers.

If required, you can also change the data encryption key using the Terminal Manager Administration Tool.

REFERENCE - EXTERNAL

For more information about changing the data encryption key/pass phrase, refer to Terminal Manager 680.1 Configuration Guide.

3. 1.29. Event ID 7034

Reason

This message is displayed in the Event Viewer window when the “Honeywell TM SMSTransmitterService” stops automatically.

Resolution

You must configure the settings to automatically restart the “Honeywell TM SMSTransmitterService” after any failures.

To change the recovery settings

2. Type services.msc and then click OK.
   The Service window appears.
3. In the Name column, right-click Honeywell TM SMSTransmitterService, and then select Properties.
The Honeywell TM SMSTransmitterService Properties window appears.

4 Click the Recovery tab.
5 Select Restart the Service from the following drop-down lists:
   - First failure
   - Second failure
   - Subsequent failures
6 Click Apply and then click OK.
   The recovery settings for the “Honeywell TM SMSTransmitterService” are configured.
3. 1.30. Error occurred in open day while using Terminal Manager client

Reason

This error occurs if the SchedulerProcessor.config file is corrupted.

Resolution

Perform the following:

1. Verify whether the Honeywell Scheduler service is running.
2. Verify whether the below tables are available in database.
   - EOD
   - EXECUTEDINFO
   - EXECUTION
   - HOLIDAYS
   - JOB
   - RECURRANCE
   - WEEKENDS
3. Verify whether the SchedulerProcessor.config file is empty.
   If the file is empty:
   - Stop all the Terminal Manager services using redundancy monitor tool.
   - Copy the below contents in to the “<TMInstallLocation>\Honeywell\TerminalManager\Scheduler\SchedulerProcessor.config file”.

<Configuration>
  <ListeningPort>3623</ListeningPort>
  <Default_TotalExecutionTime>10</Default_TotalExecutionTime>
  <LogFilePath>C:\Program Files\Honeywell\TerminalManager\Scheduler\SchedulerLog.txt</LogFilePath>
  <DBSyncronizeFilePath>C:\Program Files\Honeywell\TerminalManager\Scheduler\RecDbSync.xml</DBSyncronizeFilePath>
  <SmtpServer>
  </SmtpServer>
  <FromEmailAddress>
  </FromEmailAddress>
  <Persistence>
  </DBPersist>/
7s13Y+w0Prx8AwUcZXggwmdCKhDij1HQ0u3D6+7rLRLIT+ot7T56K6lkyFah
Start only the redundancy monitor service using services.msc. Wait for all the Terminal Manager services and Honeywell Scheduler services to start.

Verify whether the errors are stopped logging in the schedulerlog file.

Repeat the same procedure for redundant machines.

Open the day in Terminal Manager to confirm issue is resolved.

### 3. 1.31. Unable to print

**Reason**

If you try to print before configuring the printer, you will be unable to print even after configuring the printer.
Resolution

In the TMPrintQueue table, delete the records if the printer name is displaying ‘invalid printer’ and configure the printer again.
4. Database Maintenance and Backup

This chapter describes the procedure of database maintenance in redundancy environment.
The following task should not be performed while there are any active operations in Terminal Manager and is recommended for a huge database.

**Note**

It is recommended to test the following procedures in an offline test environment before performing them on a production system.

1. Close all the Terminal Manager services and stop IIS.
2. Remove the mirroring using redundancy monitor client tool. Close redundancy monitor tool.
3. Take the backup of primary DB server.
4. Shrink the database, see “Shrink the Database“.
5. Setting up mirroring, see “Setting up Mirroring”.
6. Start the Terminal Manager services and IIS.

**Shrink the Database**

a. Take the backup of experiontas.mdf and ldf files.

b. Execute the following queries to shrink the database:
   
   ```
   Alter database ExperionTAS set recovery simple;
   go
   DBCC SHRINKFILE(ExperionTAS_log, TRUNCATEONLY) (ExperionTAS_log- Name of Experion Tas log file).
   go
   Alter database ExperionTAS set recovery FULL;
   ```

**Setting up Mirroring**

Perform the following steps in master database:

a. Execute in primary server
   
   ```
   CREATE ENDPOINT [TMDBMirroring]
   ```
   
   ```
   STATE=STARTED AS TCP (LISTENER_PORT = 5022, LISTENER_IP = ALL) FOR DATA_MIRRORING (ROLE = PARTNER, AUTHENTICATION = WINDOWS NEGOTIATE, ENCRYPTION = REQUIRED ALGORITHM RC4)
   ```
   
   ```
   GRANT CONNECT ON ENDPOINT::TMDBMirroring TO [tmuseraccount] (replace tmuseraccount to login account).
   ```
b. Execute in secondary server
Create endpoint [TMDBMirroring]
STATE=STARTED AS TCP (LISTENER_PORT = 5022, LISTENER_IP = ALL)
FOR DATA_MIRRORING (ROLE = PARTNER, AUTHENTICATION = WINDOWS NEGOTIATE, ENCRYPTION = REQUIRED ALGORITHM RC4)
grant connect on endpoint::TMDBMirroring to [tmuseraccount]
(replace tmuseraccount to login account).

c. Execute in primary server
backup database ExperionTAS to disk = @DBPath with init--
@DBPath=<Foldername>\ExperionTAS_Mirroring_Init_Full.bak
backup log ExperionTAS to disk = @DBPath with init
( @DBPath=<Foldername>\ExperionTAS_Mirroring_Init_log.trn).

d. Copy the .bak and .trn files from primary server to secondary server manually.

e. Execute in secondary server

Note
As a safety measure take the backup of database in secondary server before performing below steps.

restore database ExperionTAS from disk = @DBPath with replace, norecovery
( @DBPath=<secondary server Foldername>\ExperionTAS_Mirroring_Init_Full.bak).
restore log ExperionTAS from disk = @DBPath with norecovery
( @DBPath=<secondary server Foldername>\ExperionTAS_Mirroring_Init_log.trn).

f. Execute in secondary Server
alter database ExperionTAS set partner = 'TCP://
<PrimaryServerName>:5022';

g. Execute in primary Server
alter database ExperionTAS set partner = 'TCP://
<SecondaryServerName>:5022';
5. DCH Certification

This chapter describes about certificate maintenance for DCH communication.
5.1 Change Certificate in Experion Server

To change the certificate in Experion server, perform the following steps:

1. Place the new certificate in certificate store, “Certificates (Local Computer) > Personal > Certificates”.

2. The new certificate must be trusted in the ERP/Integration server.

3. Change the Thumbprint of the certificate in the below config files:
   - C:\Program Files (x86)\Honeywell\TerminalManager\DCH\InternalService\Honeywell.TM.BSIInternalCommunicationService.exe.config.
   - Multiload Workflow exe config file client and MSCWorkflow exe config file end point behavior located in C:\Program Files (x86)\Honeywell\TerminalManager\Workflow\BCU.
   - Web.config file located in C:\Program Files (x86)\Honeywell\TerminalManager\TMUI.
4 If the Subject/DNS name is not the same as the host name of Experion server, change the DNS value in MSC-L Workflow config file client end point, Multiload config file client end point.

```xml
<client>
  <endpoint address="net.tcp://localhost:8734/HoneywellTMBSIIInternalCommu"
  <identity>
    <dn value="R510-NAME"/>
  </identity>
</endpoint>
</client>
```
5.2 Change Certificate in ERP/Integration Server

To change the certificate in ERP/Integration server, perform the following steps:

1. Place the new certificate in certificate store, “Certificates (Local Computer) > Personal > Certificates”.
2. The new certificate must be trusted in the Experion server.
3. Change the Thumbprint of the certificates in the below config files:
   C:\Program Files (x86)\Honeywell\TerminalManager\DCH\ExternalService\Honeywell.TM.BSIExternalCommunicationService.exe.config.

Note

To view Thumbprint, refer to section “To view Thumbprint” on page 70.
4 If the Subject/DNS name is not the same as host name of ERP/Integration server, change the DNS value in internal communication service client file client end point.

```xml
<client>
  <endpoint address="net.tcp://HS5020DIT:8733/HoneywellONDONIEnternalCommunicationService"
    binding="netTcpBinding" bindingConfiguration="netTcpBinding_IExternalInteractionService" contract="HSIExtServiceRef.IExternalInteractionService" name="netTcpBinding_IExternalInteractionService"/>
</client>
```
5.3 To view Thumbprint

To view Thumbprint of the certificate:

1. Expand “Certificates (Local Computer) > Personal > Certificates” in the certificate store.

2. In the Certificate dialog box:
   - Select the Details tab.
   - Select Thumbprint in the list and read or copy the thumbprint.
5.4 Trusting the Certificate

Place the certificate in the below locations:

- “Certificates (Local Computer) > Trusted People”.
- “Certificates (Local Computer) > Trusted Root Certification Authorities”.
Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

ControlEdge™ is a trademark of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

Matrikon® and MatrikonOPC™ are trademarks of Matrikon International. Matrikon International is a business unit of Honeywell International, Inc.

Movilizer® is a registered trademark of Movilizer GmbH. Movilizer GmbH is a business unit of Honeywell International, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.

Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at: http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to: hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC).
How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:


Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

Training classes

Honeywell holds technical training classes that are taught by process control systems experts. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.