Installation of PMD R910.2 on Virtual RHS using ESIS
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 2018 - Honeywell International Sàrl
Contents ......................................................................................................................... 3

Chapter 1 - About this document .................................................................................. 5
  1.1 Revision history ........................................................................................................ 5
  1.2 Related documents ................................................................................................... 5
  1.3 Support and Contacts ............................................................................................... 5
  1.4 Computer names ...................................................................................................... 5
  1.5 Media requirements ................................................................................................ 6

Chapter 2 - Creating PMD RHS on Virtual Machine ....................................................... 7
  2.1 Generate configuration files using system initialization media ............................ 7
  2.2 Create and set up virtual machine .......................................................................... 16
    2.2.1 Create the virtual machine ............................................................................. 16
    2.2.2 Setting up the virtual machine .................................................................... 20
  2.3 Install operating system and Experion PKS ......................................................... 26
  2.4 VMware tool installation ...................................................................................... 27
  2.5 Install Adobe Reader ............................................................................................. 29
  2.6 Verify Firewall ...................................................................................................... 30
  2.7 Install PMD software ............................................................................................. 30
  2.8 Post installation tasks ........................................................................................... 31
    2.8.1 Configure user settings for Administrator users ............................................. 31
    2.8.2 Configure the user settings for PMD users ................................................... 32
    2.8.3 Remove Administrators user groups rights ................................................... 35
    2.8.4 Disable Administrator user .......................................................................... 37
    2.8.5 Password policy settings .............................................................................. 37
    2.8.6 Create users ................................................................................................... 37
    2.8.7 Configure user properties ............................................................................. 38
    2.8.8 Configure station startup for users at log on .................................................. 38
    2.8.9 HMIWeb Display Builder settings ................................................................ 39
    2.8.10 Disable IE ESC ............................................................................................ 40
    2.8.11 Configure remote desktop users group to user properties ......................... 40
  2.9 Setting Remote Desktop Services ......................................................................... 41
    2.9.1 Windows components .................................................................................... 41
    2.9.2 Install remote desktop licensing .................................................................... 42
    2.9.3 Registry settings ............................................................................................. 42
    2.9.4 Activate licensing server ................................................................................ 42
    2.9.5 Install Client Access License (CAL) ............................................................... 43
2.9.6 Configure remote desktop services ............................................ 43
2.10 Install Hotfixes and Antivirus ..................................................... 44
2.11 Remove USB device from the virtual machine .......................... 45
2.12 Verify the PMD RHS system ....................................................... 45
This document provides instructions about production of PMD R910.2 RHS on virtual machines by using the ESIS media.

1.1 Revision history

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>August 2018</td>
<td>Initial release of the document.</td>
</tr>
</tbody>
</table>

1.2 Related documents

The following are the list of documents that are source of reference for content discussed in this publication.

- Experion PKS with PMD Controller Virtualization User's Guide

1.3 Support and Contacts

For any support, contact your local Honeywell Technical Assistance Center (TAC).

<table>
<thead>
<tr>
<th>Finland</th>
<th>Mail: Honeywell Oy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GTAC P3-DCS</td>
</tr>
<tr>
<td></td>
<td>Navitas 1, B-block, 4.kerros, Wredenkatu 2</td>
</tr>
<tr>
<td></td>
<td>FI-78250 Varkaus, Finland</td>
</tr>
<tr>
<td></td>
<td>Phone: +358 20 752 2000</td>
</tr>
<tr>
<td></td>
<td>Email: DL HPS_Q_GTAC_P3_DCS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Elsewhere</th>
<th>Call your nearest Honeywell office.</th>
</tr>
</thead>
</table>


1.4 Computer names

The following list provides the restrictions that must be followed in naming the computers.

- Computer names
- Media requirements
The Automation Network Architecture (ANA) name of the computer must be eight characters or less, in length.

- The computer name must be in the format 001RHS1, 004RHS01.
- The computer name cannot contain spaces or other non-standard characters.

1.5 Media requirements

You need following medias to install PMD R910.2 RHS:

- ESIS USB disk
- Experion PKS System Initialization DVD R210.1 or later
- Microsoft Security Patches SUIT DVD
CREATING PMD RHS ON VIRTUAL MACHINE

- Generate configuration files using system initialization media
- Create and set up virtual machine
- Install operating system and Experion PKS
- VMware tool installation
- Install Adobe Reader
- Verify Firewall
- Install PMD software
- Post installation tasks
- Setting Remote Desktop Services
- Install Hotfixes and Antivirus
- Remove USB device from the virtual machine
- Verify the PMD RHS system

2.1 Generate configuration files using system initialization media

ATTENTION
Ensure that the Setup.exe (which creates the configuration files) from ESIS must be run on a PC with Windows OS loaded on it.
2.1.1 To generate configuration files

1. Go to ESIS Run as Administrator and start \ESIS\EPKS_R510....\Setup.exe.
   The Experion Software Installation Server > Welcome to ESIS Tool page appears.

   ![Welcome To ESIS Tool](image)

   Select OS preparation with/without Product Install check box, and then click Next.

   The Installation option page appears.

   ![Experion PKS System Initialization Wizard](image)

2. Select OS preparation with/without Product Install check box, and then click Next.
   The Installation option page appears.

3. Click Generate configuration files, and then click Next.
   The Platform Configuration page appears.
4. Under **Choose Configuration**:
   - Select **Platform Configuration** check box, and then select **Reinstall OS and configure system** from the list.
   - Select **Product Installation** check box, then select **R510.x**.

5. Under **Select Platform**:
   - Click **Server**, and then select **VMware Virtual Platform** from the list.

6. Under **Select Operating System**:
   - Click **Server**, and then select **Windows Server 2016 Datacenter (X64)** from the list.

7. Click **Next**.
   The **Operating System Configuration** page appears.
In the **Local Language** list, select English (United States).

In the **Time Zone** list, select the correct Time Zone.

In the **Computer Name** box, type the correct name.

In the **Company Name** box, type Honeywell.

In the **Customer Name** box, type Honeywell.

In the **Workgroup Name** box, type workgroup name, for example, WGPMD.

In the **User Account name** box, type the required user name.

In the **Password** box, type the password.

In the **Confirm Password** box, type the password.

In the **Security Password** box, type the password.

In the **Confirm Security Password** box, type the password.

8. Click **Next**.

The **Network and Input/Output Device Information** page appears.
In the Network Type list, select Ethernet.
In the No. of Adapters list, select 2.
In the Network Link Speed, select 100 mbps Full Duplex option.

9. Click NIC Properties.
   The IP Address dialog box appears.
10. Click **Use the following IP address**.

11. In the **IP Address**, **Subnet Mask**, and **Default Gateway** boxes, type the correct IP address, subnet mask, and default gateway details, respectively.

12. Click **OK**.

13. Click **Next**.

The **Configuration Summary** page appears.
14. Click **Generate Product Install Config Files**.
   The **Welcome** page appears.

15. Click **Next**.
   The **License Agreement** page appears.

16. Select **I accept the terms in the License Agreement** and click **Next**.
   The **Setup type of Node to install** page appears.

17. Select **Flex Station (ES-F)**, and click **Next**.
   The **User and License Information** page appears.
18. In the Name and Company Name boxes, type Honeywell.
19. Select the Do Not Install Software and No options.
20. Click Next.
   The Installation Path(s) Selection page appears.
21. Leave the default paths, and click Next.
   The Experion Network Selection page appears.
22. Select Ethernet, and click Next. 
   The Feature and Options Selection page appears.

23. Perform the following settings:
   - Select Custom
   - Select/Clear Signon Manager based on requirement.
24. Click **Next**.

The **Experion Accounts Password Entry** page appears.

25. Type the password to all **Password** and **Confirm Password** boxes.

26. Add **Additional User Name** and **Password**.

27. Click **Next**.

The **Summary** page appears.

28. Verify the settings, and click **Continue**.

29. Click **Save Config Files** to save the file to USB drive (that is, ESIS disk).

30. Under **ConfigFiles** folder, create Project folder (that is, SID1234_DEPARTMENT) and node name subfolder (that is, 001RH001).

31. Click **OK**.

32. Click **OK**.

33. After saving, click **Finish**.

34. Click **OK**.

35. Safely remove USB drive.

### 2.2 Create and set up virtual machine

- **Create the virtual machine**
- **Setting up the virtual machine**

#### 2.2.1 Create the virtual machine

To create the virtual machine
1. In the **vSphere Web Client** home page, click **vCenter > Host**, select the **Host**.

2. Right-click the **Host** and select **All vCenter Actions > New Virtual Machine**.

   ![Image of vCenter interface with the New Virtual Machine wizard]

   The **New Virtual Machine** wizard appears.

3. Under **Select a creation type**, by default, **Create a new virtual machine** is selected, and click **Next**.

   The **Edit Settings** page appears.
4. Under **Select a name and folder**, in the **Enter a name for the virtual machine** box, type the desired **Virtual Machine** name.

   For example, if the server name is PMDVITRB, provide the same name to the virtual machine. Similarly, if the HMI name is PMD01HMI, provide the same name to the virtual machine or if the RHS name is PMD01RHS, provide the same name to the virtual machine.

   ATTENTION
   The VM name can be different from the windows computer name. Do not use the special characters in Virtual Machine name. For example, !, $, #, %.

5. Under **Select a location for the virtual machine**, select the **desired location (datacenter) for the virtual machine**, and click **Next**.

6. Under **Select a computer resource**, select the **cluster/host/resource pool for the virtual machine** and click **Next**.

7. Under **Select storage**, in the **VM Storage Policy list**, select the **VM Storage Policy**.

8. Select desired storage device, and click **Next**.
Chapter 2 - Creating PMD RHS on Virtual Machine

9. Under Select compatibility, in the Compatible with list, select ESXi 6.0 and later and click Next.

10. Under Select a guest OS, in the select Guest OS Family list, select Windows.
11. In the Guest OS Version list, select Microsoft Windows Server 2016 (64-bit).
12. Click Next.
   The Customize hardware page appears.

13. In the CPU list, select the number of virtual CPUs for the respective virtual machine. For specification information, refer to the HPS Virtualization Specification document, p/n EP03-700-100.
17. By default, single network card is available, in the New Network list, select FTE Yellow from the list.
18. In the New device list, select the Network, and click Add.
19. In the **New Network** list, select **FTE Green** from the list.
20. Select the **Connect at Power On** checkbox.
21. Retain the default settings.
22. Click **Next**.
   The **Ready to Complete** page appears.
23. Read through the **Settings summary**, and if required, click **Back**, and **Edit** the details.
24. Click **Finish**.

### 2.2.2 Setting up the virtual machine

After the virtual machine is created, perform the following settings:

- **Add CD/DVD Drive to the virtual machine**
- **Add USB controller to the virtual machine**
- **Add USB device to the virtual machine**
- **Resource allocation for virtual machine**
- **BIOS setting to boot from the CD-ROM device**

**Add CD/DVD Drive to the virtual machine**

To set the CD/DVD drive as host device in virtual machine
Chapter 2 - Creating PMD RHS on Virtual Machine

1. In the vSphere Web Client home page, click vCenter > Virtual Machine, click Virtual Machine. The list of Virtual Machine appears.

2. Select the desired Virtual Machine, right-click and select Edit Settings. The Edit Settings window appears.

   - In the New Device list, select CD/DVD drive 1.
   - Select the Host Device.
   - Under Status, select the Connect at Power on check box.
   - Click OK.

Add USB controller to the virtual machine

To add USB controller to the virtual machine
1. In the vSphere Web Client home page, click vCenter > Virtual Machine, click Virtual Machine. The list of Virtual Machine appears.
2. Select the desired Virtual Machine, right-click and select Edit Settings. The Edit Settings window appears.
3. In the New Device list, select USB Controller.
4. Click Add and click OK.

Add USB device to the virtual machine

To add USB device to connect any removable disk
1. In the **vSphere Web Client** home page, click **vCenter > Virtual Machine**, click **Virtual Machine**. The list of **Virtual Machine** appears.

2. Select the desired **Virtual Machine**, right-click and select **Edit Settings**. The **Edit Settings** window appears.

3. In the **New Device** list, select **Host USB Device**.

4. Click **Add** and click **OK**.

**Resource allocation for virtual machine**

**To allocate the resource for the virtual machine**

1. In the **vSphere Web Client** home page, click **vCenter > Virtual Machine**, click **Virtual Machine**. The list of **Virtual Machine** appears.

2. Select the desired **Virtual Machine**, right-click and select **Edit Settings**. The **Edit Settings** window appears.
3. Expand CPU, in the CPU list, select the number of CPUs.

4. In the Reservation list, set Reservation as 50% of limit value.
5. In the Limit list, set the limit value. For specification information, refer to the HPS Virtualization Specification document, p/n EP03-700-100.

![Virtual Hardware settings](image)


7. In the Reservation list, set Reservation as 70% of limit value.

8. Click OK.

### BIOS setting to boot from the CD-ROM device

Set the BIOS to boot from the CD-ROM device, so that computer can boot from CD-ROM.

#### To set BIOS setting to boot from the CD-ROM device

1. In the vSphere Web Client home page, click vCenter > Virtual Machine, click Virtual Machine. The list of Virtual Machine appears.
2. Select the desired Virtual Machine, right-click and select Edit Settings. The Edit Settings window appears.
3. Click the **VM Options** tab, expand **Boot Options**.

4. Under **Firmware**, in the **Choose which firmware should be used to boot the virtual machine** list, select **BIOS (recommended)**.

5. Under **Force Bios setup (*)**, select **The next time the virtual machine boots, force entry into the BIOS setup screen** check box.

6. Click **OK**.

7. In the **vSphere Web Client** home page, click **Summary** tab, then click **Launch Console**.

8. Select the desired **Virtual Machine**, right-click and select **Power On**.

   The **PhoenixBIOS Setup Utility** window appears.

9. Select the **Boot** tab, and select the **CD-ROM Drive**.

10. Press + button, bring to the first.

11. Press F10 to **Save** and **Exit**.

   The **Setup Confirmation** window appears, select **Yes** and press **Enter**.

   The machine restarts.

2.3 **Install operating system and Experion PKS**
2.3.1 To install operating system and Experion PKS

1. Connect both server Ethernet ports to switches or use crossover cable.
2. To start operating system installation, ensure that the latest Experion PKS System Initialization media (R210.1 or later media) is inserted in the DVD drive of the ESXi host.
3. Connect the USB/Pen drive in which the configuration files are saved to the target node.
4. Restart the computer.
5. Press any key if the message *Press any key to boot from CDROM* appears.
6. Click **Browse** and select **InitMediaOptions.xml** configuration file from the USB drive.
7. Click **Next**.
8. Select **Partition Count** as **One**.
9. Provide security password which was entered during **Generate configuration files**.
10. Select the location for installation media as **ESIS from USB**.
11. Select ESIS path (USB Drive\EPKS_R510_ESIS_v5).
12. Click **Next**.
13. Select **I accept the terms in the license agreement**, and click **Install**.
   A message for **Formatting the selected Drive** appears.
14. Click **Yes**
15. Follow the on screen instructions to complete the Experion PKS System Initialization media installation.
   After completing, a message appears to restart the system.
16. Click **Yes**.
17. Log on with the user that was used for generating configuration file. Ensure that the user is added to the product administrator and Local Engineers group.

**ATTENTION**
Windows keyboard layout is in US-English and might be different than actual keyboard.

18. In the **Experion Welcome** screen, clear **Show this screen next time you start Windows** option, and click **Close**.

2.4 VMware tool installation

After you create a PMD virtual machine, you must install VMware Tools on it.
## 2.4.1 To install VMware tools

1. In the **vSphere Web Client** home page, click **vCenter > Virtual Machine**, select the **Virtual Machine**. The list of Virtual Machine appears.

2. Right-click **Virtual Machine**, select **All vCenter Actions**.

   ![vSphere Web Client home page](image)

   - **Actions - test**
   - **Open Console**
   - **Power On**
   - **Shutdown Guest OS**
   - **Restart Guest OS**
   - **Migrate**
   - **Take Snapshot**
   - **Revert to Latest Snapshot**
   - **Manage Snapshots**
   - **Clone to Virtual Machine...**
   - **Clone to Template...**
   - **Edit Settings...**
     - **More To...**
     - **Rename...**
     - **Assign Tag...**
     - **Remove Tag**
   - **Alarms**
     - **All vCenter Actions**

   - **Upgrade VMware Tools...**
     - **Install VMware Tools...**
     - **Uninstall VMware Tools...**
3. Click **Guest OS**, select **Upgrade VMware Tools**. The **Upgrade VMware Tools** dialog box appears.

4. Select **Automatic Upgrade** option.

   **ATTENTION**
   Ensure that Virtual Machines are powered on before the Automatic upgrade.

5. Click **Upgrade**.

### 2.5 Install Adobe Reader

#### 2.5.1 To install Adobe Reader

1. Go to `ESIS_ID_PDFAdobe ReaderAR 11.0.0`.
   The **Ready to Install Adobe Reader XI** page appears.
3. Click **Next**.
4. Click **Install**.
   After the Adobe Reader 11 is installed successfully, the **Setup Completed** page appears.
5. Click **Finish**.
6. Go to `ESIS_ID_PDFAdobe ReaderAR 11.0.20`.
7. Double-click `AdbeRdrUpd11020`.
   The **Welcome to Patch for Adobe Reader 11.0.20** page appears.
8. Click **Update**.
   After the Adobe Reader 11.0.20 patch is installed successfully, the **Setup Completed** page appears.
9. Click **Finish**.
10. From the desktop, start Adobe Reader.
11. Select Edit > Preferences.
12. Select Updater.
13. Select Do not download or install updates automatically option.
14. Click OK.

2.6 Verify Firewall

2.6.1 To verify Firewall

1. Log on with the user that was used for generating configuration file.
2. Go to Control Panel > Windows Firewall.
3. Click the Advanced Settings.
4. Select the Inbound Rules.
5. Right-click Remote Desktop (Tcp-In) and select Enable Rule.

2.7 Install PMD software

2.7.1 To install PMD software

1. Log on with the user that was used for generating configuration file.
2. Right-click ESIS\PMD_R910.2\Setup, and then click Run as administrator.
   The User Account Control dialog box appears.
3. Click Yes.
   The Experion PKS with PMD Controller wizard appears.
4. Click Next.
   The License Agreement page appears.
5. Read the license agreement.
6. Click I accept the terms in the license agreement, and then click Next.
   The Select the Language page appears.
7. From the Language list, click either Finnish or English.
8. Click Next.
   The Setup Type page appears. You can choose the required options:
   • HMI
   • HMI with non-Redundant PMD Server
9. Click Next.
   The Enter the following details page appears with the default values configured in the installer.

ATTENTION
Use only capital letters for all fields.

10. Clear the default values, and then insert the site-specific values.
11. Click Next.
   The PMD Accounts Password Entry page appears.
12. Type the passwords for all users and click Next. Perform the same on all PMD account fields.
13. Click Next.
   The Destination Folder page appears.
14. Click Next.
   The Ready to Install the Program page appears.
15. Click Install.
16. Click Finish.
17. After the installation is complete, a message appears to restart the computer.
18. Click Yes.
   The computer is restarted.

2.8 Post installation tasks

- Configure user settings for Administrator users
- Configure user Settings for PMD users
- Remove Administrators user groups rights
- Disable Administrator user
- Password policy settings
- Create users
- Configure user properties
- Configure station startup for users at log on
- HM!Web Display Builder settings
- Disable IE ESC
- Configure remote desktop users group to user properties

2.8.1 Configure user settings for Administrator users

To configure the user settings for Administrator users

1. Log on with the user that was used for generating configuration file. Ensure that the user is added to the product administrator group and local engineers group.
   The Computer Management window appears.
3. Click Computer Management > System Tools > Local Users and Groups > Users.
   On the right-pane of the Computer Management window, the list of users appears.
4. Right-click Administrator, and then click Properties.
   The Administrator Properties dialog box appears.
5. Clear the Account is disabled and User must Change Password at next login check boxes.
6. Click Apply, and then click OK.
7. Right-click Administrator user, click Set Password and click Proceed.
   The Set Password dialog box appears.
8. In the Password and Confirm Password boxes, type the password.
9. Click **OK**.
10. Sign Out and Sign In as **Administrator** user.
11. Click **Start > Windows system** and right-click **Command Prompt**, select **Run as Administrator**.
12. Click **Yes**.
13. Go to **ESIS\Software\Product DVD 127_03\UserSettings\R900.X\W2K16_32_64_Bit**.
14. Run **UserSettings.exe**.
15. Type 1, and then press **Enter** to apply windows user settings to the default account.
16. Deselect all selections and click **Apply**.
17. Select Desktop, Network, Control Panel, and User’s Files.
18. Click **Apply** and then **OK**.

**To add user rights to the required PMD users**

1. To add Administrators user group right to PMD users, perform the below steps.

 ATTENTION

To run **Win2K16_32_64_Bit**, user should be part of Administrators user group.

 ATTENTION

Note the PMD users to which the Administrators user groups rights are added. After configuring the user settings, Administrators user group rights to be removed from noted PMD users.

2. Click **Start > Windows Administrative Tools > Computer Management**. The **Computer Management** window appears.
3. Click **Computer Management > System Tools > Local Users and Groups > Users**. On the right-pane of the **Computer Management** window, the list of users appears.
4. Right-click **Users**, and then click **Properties**. The **Users Properties** dialog box appears.
5. Click **Member Of** tab and verify the **Administrators** user group is added.
6. If **Administrators** user group is not added then, click **Add**. The **Select Groups** dialog box appears.
7. Click **Advanced** and then **Find Now**.
8. Double-click **Administrators** group and then click **OK**.
9. Click **OK** on **Properties** dialog box.
10. Sign Out from the existing user.

2.8.2 **Configure the user settings for PMD users**

 NOTE
Chapter 2 - Creating PMD RHS on Virtual Machine

The steps from the section Configure the user settings to Other Windows settings are performed on all required PMD users manually.

- Configure user settings
- Configure Windows Media Player
- Configure keyboard settings
- Configure IE settings
- Update Adobe Reader
- Configure date, time, and time zone settings
- Other Windows settings

Configure the user settings

To configure the user settings

1. Sign In with the required PMD user to run the UserSettings tool.
2. Go to ESIS\Software\Product DVD 127_03\UserSettings\R900.X\W2K16_32_64_Bit.
4. Type 2, and then press Enter to apply windows user settings to the default account.
5. If the Desktop Icon settings window appears, then deselect all selections and then click Apply.
7. Click Apply and then OK.

Configure Windows Media Player

To configure Windows Media Player

1. Go to Start > Windows Accessories > Windows Media Player.
   The Windows Media Player dialog box appears.
2. Click the Recommended setting option.
3. Click Finish.
   After the installation is complete, close the window.

Configure keyboard settings

To configure keyboard settings

1. Click Start > Windows system > Control Panel > Clock, Language and Region
2. Click Language >Add a language.
3. Select Language from the list. For example, Finnish.
4. Click OK
5. Select the Advanced settings > Override for default input method from the list.
6. From drop down list select Default Input Language.
7. Click Save.
8. Start Registry Editor (Regedit.exe), and click Yes.
9. Choose `HKEY_USERS.DEFAULT\Keyboard Layout\Preload`.

10. Modify the value 1.

11. Enter the correct keyboard layout code to value data. The most common codes are as follows:

<table>
<thead>
<tr>
<th>Codes</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000409</td>
<td>English (United States)</td>
</tr>
<tr>
<td>00000809</td>
<td>English (United Kingdom)</td>
</tr>
<tr>
<td>0000040b</td>
<td>Finnish</td>
</tr>
<tr>
<td>0000040c</td>
<td>French (Standard)</td>
</tr>
<tr>
<td>00000407</td>
<td>German (Standard)</td>
</tr>
<tr>
<td>00000816</td>
<td>Portuguese (Standard)</td>
</tr>
<tr>
<td>00000419</td>
<td>Russian</td>
</tr>
</tbody>
</table>


12. Click OK and close Registry Editor.

**Configure IE settings**

1. Click Start > Windows Accessories > Internet Explorer, right-click Internet Explorer, select Run as Administrator, and then click Yes.

   The Windows Internet Explorer 11 dialog box appears.

2. Click Use recommended security and compatibility settings and Send Do Not Track requests to tell sites you prefer not be tracked, and click OK.

3. Enable the AddIns.

4. Right-click Menu bar, select Menu bar and Lock the toolbars options.

5. Go to Tools > SmartScreen Filter, and click Turn on SmartScreen Filter.

   The Microsoft SmartScreen Filter dialog box appears.

6. Select Turn off SmartScreen Filter option.

7. Go to Tools > Manage Add-ons > Accelerators.

8. Select Email with Windows Live, Map with Bing, and Translate and then click Disable.

9. Click Close.

10. From the Tools menu, click Internet Options.

11. Under the Home Page, click Type about:blank.

12. Click Security tab.

13. Select Trusted sites and click Sites.

14. Insert https://<Server Name> (that is, https://001RHS1) and click Add, and then Close.
Chapter 2 - Creating PMD RHS on Virtual Machine

15. Click **Advanced** tab.
16. Clear **Notify when download complete** check box.
17. Clear **Enable Automatic Image Resizing** check box.
18. Select **Empty Temporary Internet Files Folder When Browser Is Closed** check box.
19. Click **OK** and close the window.

**Update Adobe Reader**

**To update Adobe Reader**

1. From the desktop, start **Adobe Reader**.
2. Select **Edit > Preferences**.
3. Select **Updater**.
4. Select **Do not download or install updates automatically** option.
5. Click **OK**.

**Configure date, time, and time zone settings**

**To configure date, time, and time zone settings**

1. Click **Start > Windows System > Control Panel > Date and Time**.
   The **Date and Time** dialog box appears.
2. Click **Change date and time**.
   The **Date and Time Settings** dialog box appears.
3. Set the time and date, and click **OK**.
4. Click **Change time zone**.
   The **Time Zone Settings** dialog box appears.
5. Set the time zone, and click **OK**.
6. Click **OK**.

**Other Windows settings**

1. Double-click **This PC**, choose **View** tab.
2. Verify if **Show Hidden items** is selected and **File name extensions** is deselected from **Folder Options**.
3. On the **Desktop**, right-click, and then select **View > Auto arrange icons**.
4. Sign Out from the existing user.

**NOTE**
Perform the sections from **Configure the user settings** to **Other Windows settings** for required PMD users.

2.8.3 **Remove Administrators user groups rights**

1. After configuring the user settings, remove the Administrators user group rights for required PMD users. To remove the Administrators user group rights for required PMD users perform the below
2. Sign In to the computer with the user that was used for generating configuration file.

3. Click Start > Windows Administrative Tools > Computer Management.
   The Computer Management window appears.

   On the right-pane of the Computer Management window, the list of users appears.

5. Right-click Users, and then click Properties.
   The Users Properties dialog box appears.

6. Click Member Of tab.

7. Select Administrators user groups and click Remove.
2.8.4 Disable Administrator user

To disable administrator user

1. From the Start menu, right-click Computer, and then click Manage.
2. Select Local Users and Groups > Users.
3. Right-click Administrator, and then click Properties.
4. Select Account is disabled check box.
5. Click OK.
6. Restart the system.

2.8.5 Password policy settings

For password policy settings

   The Local Security Policy window appears

2. Select Account Policies > Password Policy.
3. Double-click Password must meet complexity requirements.
4. Select Disabled and click OK.

2.8.6 Create users

To create users

   The Computer Management window appears.
2. Click Computer Management > System Tools > Local Users and Groups > Users.
4. In the User name box, type the user name.
5. In the Password and Confirm password boxes, type password.
6. Clear User must change password at next logon check box.
7. Select **Password never expires** check box.
8. Click **Create** and **Close**.
9. Right-click on the user created in Step 2 and then click **Properties**.
10. Go to **Member Of** tab and click **Add**.
11. Click **Advanced** and **Find Now**.
12. Select **Local View Only** users and **Remote Desktop** users.
13. Click **OK**, **OK**, and **OK**.
14. Right-click **Command Prompt**, select **Run as Administrator** and click **Yes**.
15. On the **Command Prompt**, go to **ESIS\Software\HWSUS CD 108\**.
16. Type command **AddDMZ-RHSUsers.cmd** and press **Enter**.

### 2.8.7 Configure user properties

#### To configure user properties

1. Click **Start** > **Windows Administrative Tools** > **Computer Management**.
   The **Computer Management** window appears.
2. Click **Computer Management** > **System Tools** > **Local Users and Groups** > **Users**.
3. Right-click the user you want modify, and then click **Properties**.
4. Perform the following settings to users:

<table>
<thead>
<tr>
<th>Action</th>
<th>Affected users</th>
</tr>
</thead>
<tbody>
<tr>
<td>On <strong>Remote Desktop Services Profile</strong> tab: Select <strong>Deny this user permissions to log on to Remote Desktop Session Host server</strong> check box.</td>
<td>All users except: DEPT_RUser DEPT_Admin RHS_Admin RHS_User1 DMZ_Admin DMZ_User1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>On <strong>General</strong> tab: Select <strong>Password never expires</strong> check box.</td>
<td>RHS_Admin RHS_User1 DMZ_Admin DMZ_User1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>On <strong>Member Of</strong> tab: Add user to <strong>Remote Desktop Users</strong> group</td>
<td>DEPT_Admin</td>
</tr>
</tbody>
</table>

### 2.8.8 Configure station startup for users at log on

#### To configure registry for log on
1. Sign In to the computer with the user that was used for generating configuration file.
2. Start Registry Editor (Regedit.exe), and click Yes.
   The Registry Editor dialog box appears.
3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services.
4. On right pane, right-click and select New > DWORD (32-bit) Value.
5. Rename registry as fQueryUserConfigFromDC.
6. Double-click on the registry and type the Value data as 1.
7. Click OK.
8. Close the Registry Editor.

To configure station startup for users at log on

   The Computer Management window appears.
2. Click Computer Management > System Tools > Local Users and Groups > Users.
3. Right-click DEPT_RUser, and then click Properties.
4. Click Environment tab, and select the Start the Following Program at logon check box.
5. Under the Program file name, type C:\Program Files (x86)\Honeywell\Experion PKS\clientStation\Station.exe "C:\ProgramData\Honeywell\Experion PKS\clientStation\PMDRHSA.stn"
6. Under the Start in, type C:\Program Files (x86)\Honeywell\Experion PKS\clientStation.
7. Click Apply, and then OK.

2.8.9 HMIWeb Display Builder settings

For the HMIWeb Display Builder settings

1. Select Start > Honeywell Experion Tools > HMIWeb Display Builder, right-click HMIWeb Display Builder and then click Properties.
2. Go to Shortcut tab.
3. In the Target box, at the end of the Target line, change the startmode to PMD.
4. Click OK and Continue.
5. Go to the directory ESIS\PMD_R910.2\PMD_R910.2\MEDIA\PMD Display Object Library and right-click PMD Display Object Library 150 application and select Run as Administrator and click Yes.
6. Click Unzip.
7. Click OK and close the WinZip window.

ATTENTION
Shape path is a user-specific setting, so it must be performed on all users that use HMIWeb Display Builder.

8. Click Start > Honeywell Experion Tools > HMIWeb Display Builder.
10. Go to Shapes tab, and then click Add.
11. Click the **Browse[...]**.
12. Browse to `C: Program Files (x86)\Honeywell\PMD\HMIWeb Display Builder\PMD Display Object Library 150 \PMD Display Object Library` and then click **OK**.
13. Click **OK** and then close the **Options** dialog box.
14. Select **View > Toolbox**.

### 2.8.10 Disable IE ESC

**To disable Internet Explorer (IE) Enhanced Security Configuration (ESC) on all nodes**

1. Click **Start > Server Manager**.
   The **Server Manager** window appears.
2. Click **Local Server** in left pane.
3. Click **IE Enhanced Security Configuration** in right pane.
   The **Internet Explorer Enhanced Security Configuration** dialog box appears.
4. Under **Administrator** and **Users**, click **Off**.
5. Click **OK**.
6. Restart the system.

### 2.8.11 Configure remote desktop users group to user properties

**ATTENTION**

The virtual machine is accessed through WYSE client in the later part of configuration and operation. Hence, remote desktop user must be added to the remote desktop users group that is used for logging on to the machine. The following are the standard users:

- For Server nodes, add only Depart_Admin user.
- For HMI and RHS nodes, add the two users:
  - Depart_Admin
  - Depart_UserX
- For DM nodes, add the two users:
  - Depart_Admin
  - Depart_EngrX

Based on the project requirement, you can add or modify the required users.
To configure remote desktop users group to user properties

   The Computer Management window appears.
2. Click System Tools > Local Users and Groups > Users > Department_Admin.
3. Right-click the DEPT_Admin, and click Properties.
   The Properties dialog box appears.
4. In the Member of tab, click Add.
   The Select Groups dialog box appears.
5. Select Remote Desktop Users Groups.
6. Click OK.
7. Click OK in the Member Of tab.

2.9 Setting Remote Desktop Services

- Windows components
- Install remote desktop licensing
- Registry settings
- Activate licensing server
- Install Client Access License (CAL)
- Configure remote desktop services

2.9.1 Windows components

For windows components settings

1. From the Start menu, right-click Computer, and then click Manage.
2. Select Features, and then click Add Features.
3. Select Background Intelligent Transfer Service (BiTS) Server Extensions.
4. Click Add required Role Services option.
5. Click Next.
6. Click Next.
7. Select the following Components.
   - FTP Server
   - Leave all other options as default values.
8. Click Next.
9. Click Install.
10. Click Close.
11. Create folder C:\inetpub\www_ftp_root.
14. Provide Full Control for Users group to that folder.
2.9.2 Install remote desktop licensing

To install remote desktop licensing

1. Start > Server manager.
2. Click Manage > Add Roles and features.
3. Click Add.
4. The Roles and features wizard appears.
5. Click Next.
6. Select Role based or feature based installation.
7. Click Next.
8. Click Next on Server Selection.
10. Under Remote Desktop Services, Select Remote Desktop Licensing and Remote Desktop Session Host, and on Add Roles and Features wizard click Add Features.
11. Click Next and follow the on screen instructions.
12. After completing, click Install.
13. After installing, click Close.

2.9.3 Registry settings

For registry settings

1. Ensure to create the following registry keys.

ATTENTION
You can use file ESIS\Software\HWSUS CD 108\KeepAlive.reg to do below registry settings.

2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
   KeepAliveInterval = 1000
   KeepAliveTime = 5000
   TcpMaxDataRetransmissions = 5

ATTENTION
All keys are DWORD keys. Enter the values for as decimal.

2.9.4 Activate licensing server

To activate the licensing server
1. Click **Start > Windows Administrative Tools > Remote Desktop Licensing Manager.**
2. Click **Yes.**
3. From **All Servers** list, select the desired server.
4. Right-click and select **Activate server** from Action menu.
   The Activation wizard appears, click **Next.**
5. Select activation method as **Web browser.**
7. Select **Activate a license server,** and click **Next.**
8. Enter **Product ID** from Remote Desktop License Activation Wizard and customer information, and then click **Next.**
9. Verify if the information is correct. Click **Next.**
   The **License Server ID** code displays. Print or write that down.
10. Go back to **Remote Desktop Activation Wizard,** and then enter the **Licence Server ID.** After it is complete, click **Next** and **Finish.**

### 2.9.5 Install Client Access License (CAL)

**Prerequisites**

- By default, RHS server with Windows Server 2016 operating system does not have any Client Access licenses.
- RHS needs 10 licences, since the standard delivery includes 10 sessions.
- Licenses must be purchased even more, if the RHS server’s scope of supply includes more than ten simultaneous logins.

**To install Client Access License (CAL)**

1. Click **Start > Windows System\Windows Administrative Tools > Server Manager.**
   The **Server Manager** window appears.
2. Click **Remote Desktop Services.**
3. From **All Servers** list, select the desired server.
4. Right-click the **Server** and click **RD licensing manager.** RD licensing Manager appears.
5. Select the server and click **Install Licenses,** and then click **Next.**
6. Go to [https://activate.microsoft.com](https://activate.microsoft.com) and select **Install Client Access License** tokens.
7. The Remote Desktop CAL installation Wizard provides you License ID, enter that ID to web page and company information. Select **License Program Open License.** Click **Next.**
8. Select **Product Type: Windows Server 2016 RDS Per User CAL.**
9. Set **Quantity and type Authorization and License Numbers** from email. Click **Next.**
10. Verify if the information is correct and click **Next.**
    You receive a License Key Pack ID. Print or write that down, and then click **Finish.**
11. Enter **License Key Pack ID** to RDS CAL Installation Wizard and click **Next.**
12. Click **Finish.**

### 2.9.6 Configure remote desktop services

**To configure remote desktop services**
1. From the Start menu, right-click Computer, and then click Manage. The Server Manager window appears.
2. Click Roles > Remote Desktop ServicesRemote Desktop Session Host Configuration.
3. Select Remote Desktop Session Host Configuration, and then right-click RDP-Tcp, and select Properties.
4. Click General tab and update Comment as RHS Server.
5. Click Logon Settings tab. Click Always prompt for password check box.
6. Select Sessions tab.
7. Select Override user settings check box, and then set End a disconnected session as 1 minute.
8. Set Idle session limit as 15 minutes.
9. Select Override user settings check box, and then click End session option.
10. Click OK.
12. Select the Per User option and click Add. The Add License Server dialog box appears.
13. Select Server, click Add and click OK.
15. Select the Per User option and click Add. The Add License Server dialog box appears.
16. Select Server, click Add and click OK.
17. On General tab, clear Restrict each user to a single session.
18. Click Apply and click OK.

2.10 Install Hotfixes and Antivirus

2.10.1 To install Hotfixes

1. Insert the latest SUIT ISO media to DVD drive of ESXI host to run the latest validated Microsoft hotfixes on the node. If it is not started automatically, browse to UPDatemanager on SUIT DVD, right-click and select Run as Administrator and click Yes. This should last several minutes.

   ATTENTION
   Some SUIT versions installs PreRequirements and reboot the server. After reboot start the SUIT installation again.

2. Restart the server.

   ATTENTION
   If keyboard and mouse is not responding restart the server by using power switch.
2.10.2 To install Antivirus

- Install latest McAfee or Symantec SEP antivirus based on the requirement.

2.11 Remove USB device from the virtual machine

To remove a USB device from a virtual machine, you need to disconnect it in the virtual-machine based operating system.

2.11.1 To remove USB device from the virtual machine

1. Right-click the Virtual Machine, and select Edit Settings. The Virtual Machine Properties window appears.
2. Select USB device.
3. Click Remove.
4. Click OK.

2.12 Verify the PMD RHS system

2.12.1 To verify the system

1. Verify the functions of the applications when logged on as DEPT_Admin user.
   - HMIWeb Display Builder
     - Start > Honeywell Experion Tools > HMIWeb Display Builder
     - Shortcut Start mode = PMD
     - Verify Shape path
     - Select View > Toolbox.
   - Station
     - Start > Honeywell Experion > Experion Station, right-click Open file location > Experion Station
     - For systems delivered to Finland, verify that C:\Localization Toolkit exist and the System Menu is in Finnish.
   - Adobe Reader
     - Select Edit > Preferences.
     - Select Updater.
     - Select Do not download or install updates automatically option.
     - Click OK and close the program.

2. Verify the computer settings.
   - Services
     - Background Intelligent Transfer Service = Started, Automatic
     - Microsoft FTP Service = Started, Automatic
     - Windows Time = Enabled
     - Windows Firewall = Started and Automatic
   - Device Manager is error free
Verify Show Hidden Devices
If there are any items in Other Device, install them.
After installing, right-click the **Computer name**, and then select **Scan for Hardware Changes**.

3. Keyboard layout from **Control Panel > Region and Languages > Keyboards and languages tab > Change Keyboards**

4. Empty the recycle bin.

5. Safely remove ESIS USB disk from target node.

6. Verify the computer for viruses (following instructions are for McAfee offline Virusscan):
   - Click **Start > Windows System > Command Prompt**, right-click **Command Prompt**, select **Run as Administrator**. Click **Yes**.
   - Go to the Virusscan folder.
   - Type command “Virusscan_run -64”.

7. Verify the network connection for functionality and the settings.

8. Disable **Backup Supervisory Network** if it is not used.

9. Verify that **Activation** has been performed from the **Computer Properties** or perform it if necessary.

10. Verify that there are no disks in the drives.
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:


Submit the requested information to Honeywell using one of the following methods:
• Send an email to security@honeywell.com; or.
• Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC).

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.