Honeywell

THE POWER OF **CONNECTED**

Securing MAXPRO® VMS R470 Software

Technical Release Bulletin

November, 2017

Issue 1

Document 800-23557-B - 11/2017

ABOUT THIS DOCUMENT

This Technical Note explains about the mandatory security settings that needs to be performed on VMS R470 software application

Related documents	• MAXPRO® VMS R470 Online Help. • MAXPRO® VMS R470 Commissioning and Installation Guide. • MAXPRO® VMS R470 Known Issues Bulletin. • MAXPRO® VMS R470 Troubleshooting Guide. • MAXPRO® VMS R470 Operator's Guide • MAXPRO® VMS R410 Localization Guide. • MAXPRO® VMS VMS High Availability Installation and Configuration Guide. • MAXPROVMS_Device_Features_Compatibility_Matrix • MAXPROVMS_Alarm_Compatibility_Matrix. • MAXPROVMS_PTZ_Compatibility_Matrix. • MAXPROVMS_HW_SW_Compatibility_Matrix. • MAXPRO VMS Analytics Data Sheet. • MAXPRO® VMS R410 Server VMware ESXi Spec V2 • MAXPRO® VMS R410 SQL Server Installation Reference Guide. pdf
Support	For information about updates to this bulletin, contact your nearest Honeywell office or Technical Assistance Center.

SECURING MAXPRO® VMS R470

INTRODUCTION

This notes explains about the mandatory security settings that needs to be performed on MAXPRO VMS R470.

In this technical notes...

STEP 1: CREATE A NEW SERVICE USER AND DENY LOG ON

1. Click **Start** and navigate to **Control Panel> All Control Panel Items> User Accounts**. The make changes to your use account screen appears.
2. Click **Manage Another account**/**Manage User Account** link. The **choose the account you would like to change** screen appears.
3. Click C**reate a New Account**. The **Name the account and choose the account type** screen appears.
4. Type the **New account name** in the box provided. (For example **VMSServiceUser2**)
5. Click the **Administrator** option and then click the **Create Account** button. the newly created account is displayed under **choose the account you would like to change** screen.

CREATING A PASSWORD FOR THE NEW SERVICE USER ACCOUNT.

1. In the **choose the account you would like to change** screen, click the newly created account. (For example **VMSServiceUser2**). The **Make changes to xxxxx account** screen appears.
2. Click **Create a Password**. The **Create a password for xxxxx account** screen appears.
3. Type the **New Password** in the box provided.
4. Confirm the **Password** in the box provided.
5. Type a **Password Hint** (Optional).
6. Click **Create Password** button.

DENYING LOG ON

1. In **Run** command window, type secpol.msc. The **Local Security Policy** window is displayed.
2. In the **Console** tree, double-click **Local Policies**, and then click **User Rights Assignments**.
3. In the **Details** pane, double-click **deny log on locally**.

4. Click **Add User or Group** and then add the appropriate account (**VMSServiceuser2)** to the list of accounts that possess the **Logon as** a service right.
5. Click **Apply** and then click **OK**.

STEP 2: UPDATE THE VMS SERVICES WITH NEW SERVICE USER ACCOUNT CREDENTIALS

1. Launch the **Services** (**Run > Services.msc**.) window and **Stop** the following services in the order mentioned:
    - TrinityServer
    - TrinityController
    - TrinityWatchDog
    - TrinityScheduler
    - TrinityJobScheduler
    - TrinityAnalyticsService
    - TrinityRecorderGroup
    - TrinityRedundancyManager
    - TrinityRedundancyController
2. Right-click on **TrinityServer** service and then click **Properties**. The **TrinityServer Properties** dialog appears.
3. Click the **Logon** tab.
4. Under **This account** option:
    - Replace the **Username** from **.\Administrator** to **.\VMSServiceUser2** which is created in *Step 1: Create a new Service User and Deny log on* in *Section* .
    - Type the **Password** which is created in **Creating password for the new account** section.
    - Confirm the **Password**.
5. Click **Apply** and then click **OK**.

    Note: If you are changing the username of a service for the first time then a service Pop message **The account xxxx has been granted the Log On As a service right** is displayed. Click **OK** to proceed.
6. Similarly repeat steps 2 through step 5 to update the account details for the following services.
    - TrinityController
    - TrinityWatchDog
    - TrinityScheduler
    - TrinityJobScheduler
    - TrinityAnalyticsService
    - TrinityRecorderGroup
    - TrinityRedundancyManager
    - TrinityRedundancyController

7. After updating account details, restart the following services in the order mentioned.
    - TrinityServer
    - TrinityController
    - TrinityWatchDog
    - TrinityScheduler
    - TrinityJobScheduler
    - TrinityAnalyticsService
    - TrinityRecorderGroup
    - TrinityRedundancyManager
    - TrinityRedundancyController

Step 3: Updating the Application pools in IIS

1. Launch the Internet **Information Services (IIS) Manager** window. (Run > Inetmgr).
2. Under **Connections** pane expand the main node and then click the **Application pools** node.The list of application pools are displayed in the Application Pools pane.
3. Click **ISOM_Application** and then under **Actions** pane > **Edit Application Pool**, click **Advanced Settings** link. The **Advanced Settings** dialog appears.
4. Under **Process Model** node, click **Identity** and then click the browse button,. The **Application Pool Identity** dialog appears.
5. Under **Custom account** option, click the **Set** button. The **Set Credentials** dialog is displayed.
6. Type the **User name** (For example: **VMSServiceUser2**), **Password** which is created in *Step 1: Create a new Service User and Deny log on* in *Section* and then **Confirm the Password**. Click **OK**.
7. Click **OK** in the **Application Pool Identity** box and **Advanced Settings** box.
8. Under **Connections** pane expand the **Sites** node and then navigate to **Default Web site** > **Live4** node.
9. Under **Actions** pane > **Manage Application**/**Browse Application**, click **Advanced Settings** link. The **Advanced Settings** dialog appears.
10. Under **General**, click **Physical Path Credentials** and then click the browse button. The **Connect as** dialog appears.
11. Under **Specific User** option, click the **Set** button. The **Set Credentials** dialog is displayed.
12. Type the **User name** (For example: **VMSServiceUser2**), **Password** which is created in *Step 1: Create a new Service User and Deny log on* in *Section* and then **Confirm the Password**. Click **OK**.
13. Click **OK** in the **Connect as** box and Advanced Settings box.
14. Similarly repeat the step 8 through step 13 for the following application under **Sites > Default Web site** node.
    - MaxproWeb
    - MediaConverter
    - Playback4
    - UVISOM
15. Logoff and logon once again to the machine.
16. In the **Run** command box type the **IISreset** command to reset the IIS services.

Step 4: SQL Permissions for VMS Service User (Only for SQL Standard/Enterprise Edition)

1. Launch the **SQL Server Management Studio**.
2. Connect to SQL Server using Windows/SQL Authentication.
3. Navigate **SQL Server/Machine Name > Security**, right click on **Login** and then **Select New Login**. The **Login- New** dialog box is displayed.
4. In **Login New** window, type **VMSServiceUser2** in the Search box and then click the **Search** button. The **Select User Group** dialog is displayed.
5. In the **Enter the object name to select**, type the **VMSServiceUser2** and then click the **Check Names** button. The VMS service user name is updated and displayed along with Machine. (For example: R15-VMSPC\VMSServiceUser2) Where **R15-VMSPC** is machine name.)
6. Click **OK** in **Select User Group** dialog.
7. In the **Login New** window, click Windows authentication option. (By default this option is selected)
8. In the **Select a Page** pane, click **Server Roles** node.
9. Under **Server Roles**, select **public** and **sysadmin** check boxes.
10. In the **Select a Page** pane, click **User Mapping** node and then select the **TrinityDatabase** check box under **User mapped to this login** area.
11. Click **OK**. The new login for **VMSServiceUser2** is created.

Step 5: Restart all the services

- Check if all the below services are running after restarting the machine. Ensure that you manually restart if any of the service is stopped.
    - TrinityServer
    - TrinityController
    - TrinityWatchDog
    - TrinityScheduler
    - TrinityJobScheduler
    - TrinityAnalyticsService
    - TrinityRecorderGroup
    - TrinityRedundancyManager

TrinityRedundancyController

Creating Windows Users and Mapping them to VMS Operator Group

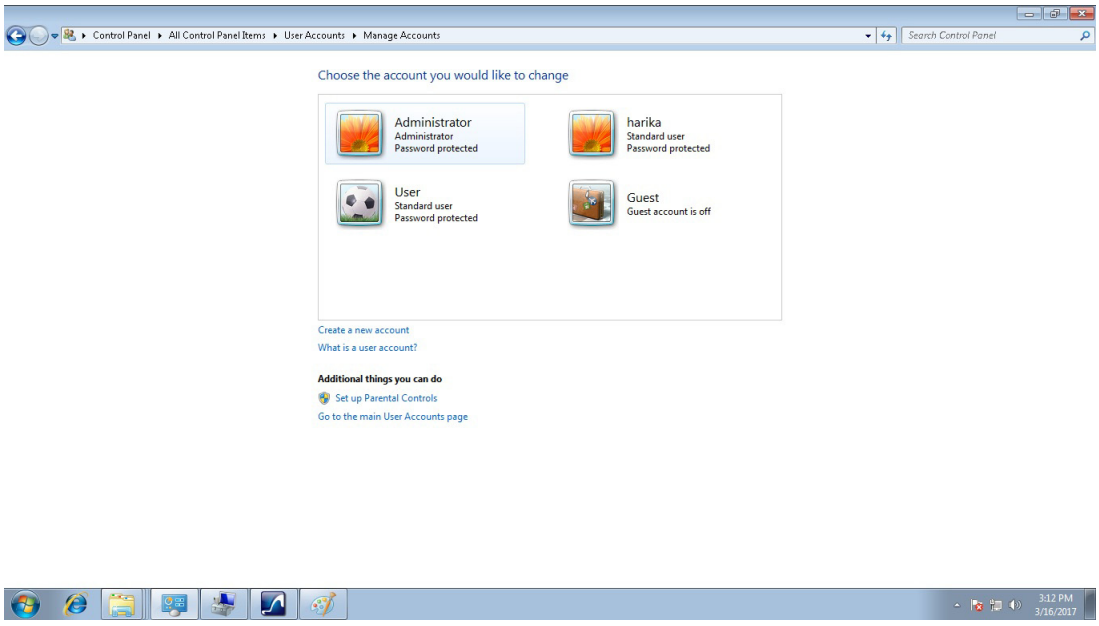
Honeywell recommends you to create Windows user and map the same to VMS User Group. After performing the below task operator privileges will have limited access and permissions.

Note: VMS R470 Installation creates the VMSUSERGROUP in the machine.

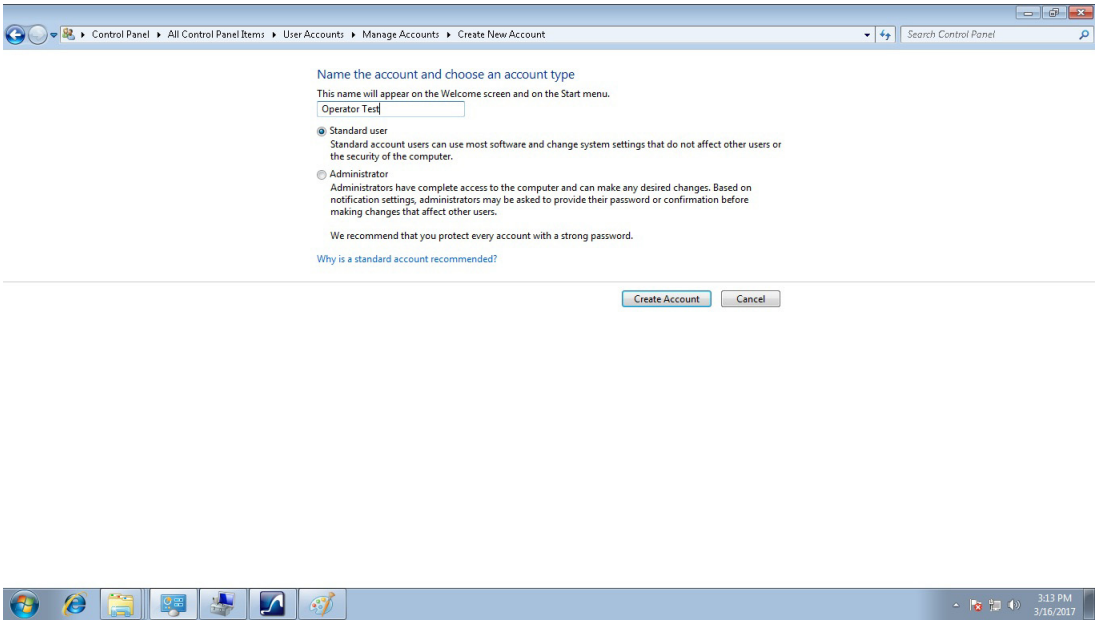
Operator will get only Read and Execute permission on Honeywell folder. Only administrators will have Full control permission on Honeywell folder.

Create a Windows User Account

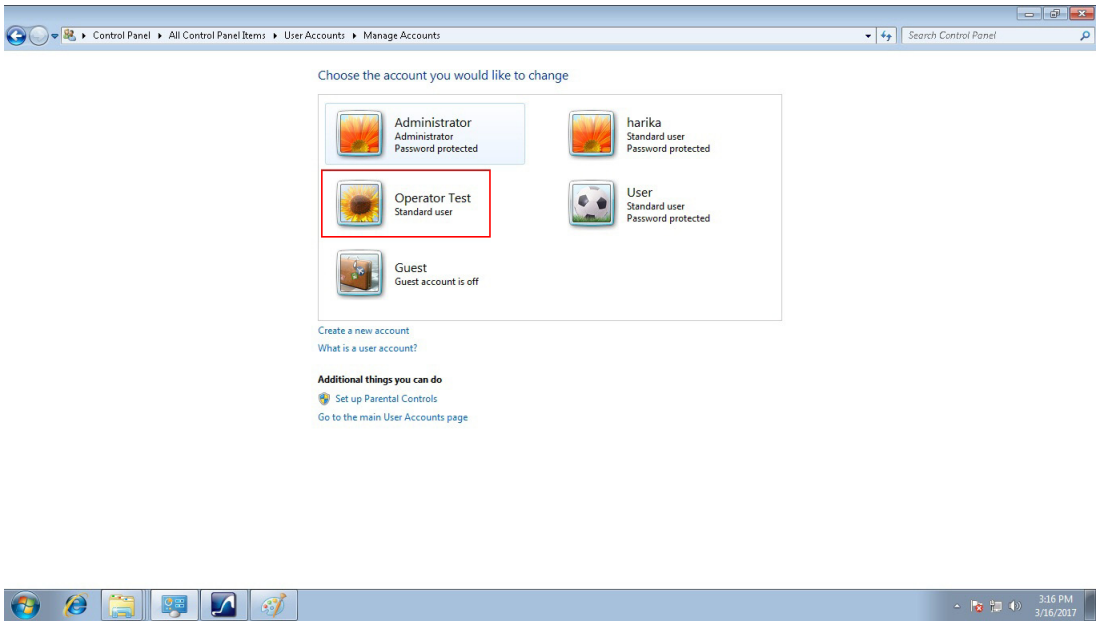
1. Navigate to **Control Panel > All Control Panel Items > User Accounts**. The **Control panel Home** screen appears.
2. Click **Manage Another account**. The **Choose the account you would like to change** screen appears as shown below.



3. Click **Create a new account**. The **Name the account and Choose the Account Type** screen appears as shown below.

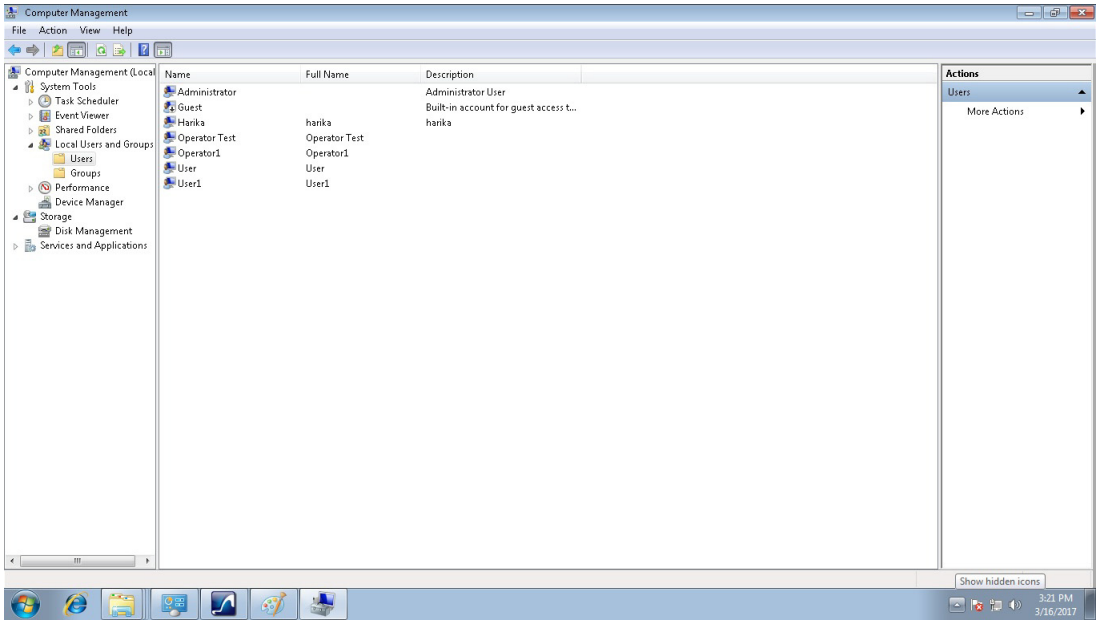


4. Type the name (**Operator Test**) and then select the **Standard User** option.
5. Click the **Create Account** button. The new account will be created and listed under **Choose the account you would like to change** screen as shown below.

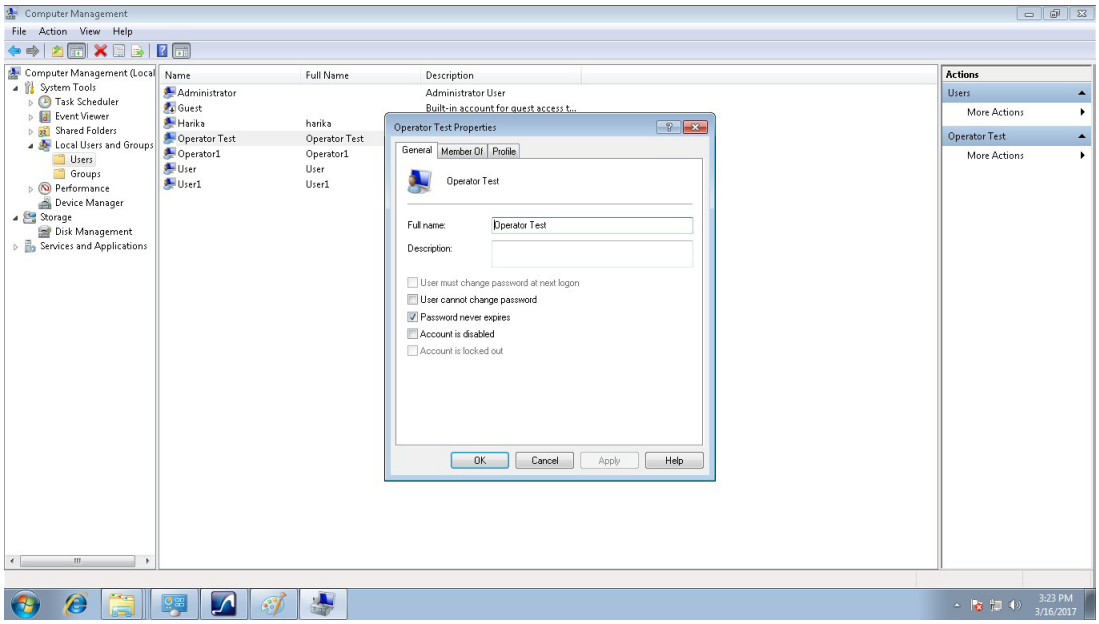


MAP THE NEW ACCOUNT TO VMS OPERATOR GROUP

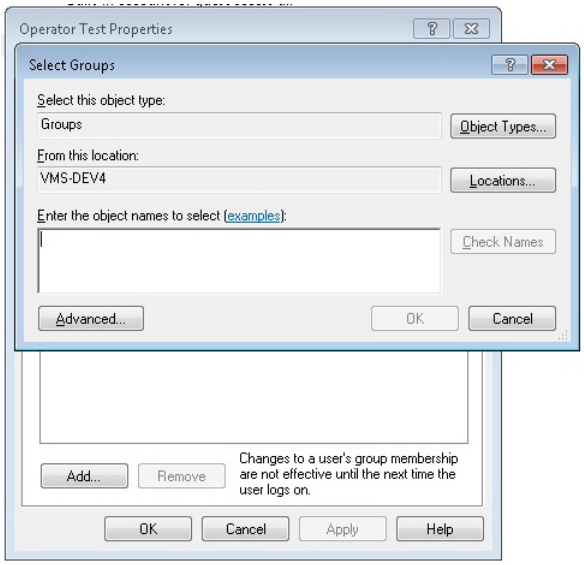
1. Choose **Start** > **Computer** and then right-click on the **Computer** to select **Manage**. The **Computer Management** Screen is displayed.
2. Navigate to **System Tools** > **Local Users and Groups** > **Users**. The list of users are displayed on the right pane as shown below.



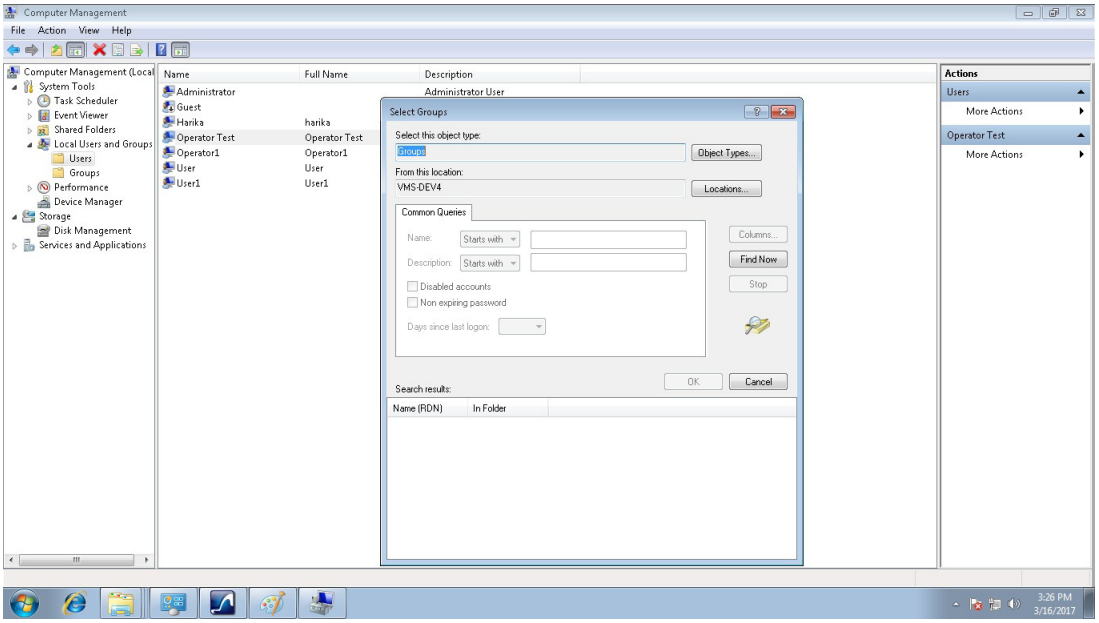
3. Right-click on the user created in the above section (**Operator Test**) and then select **Properties**. The **Operator Test Properties** dialog is displayed as shown below.



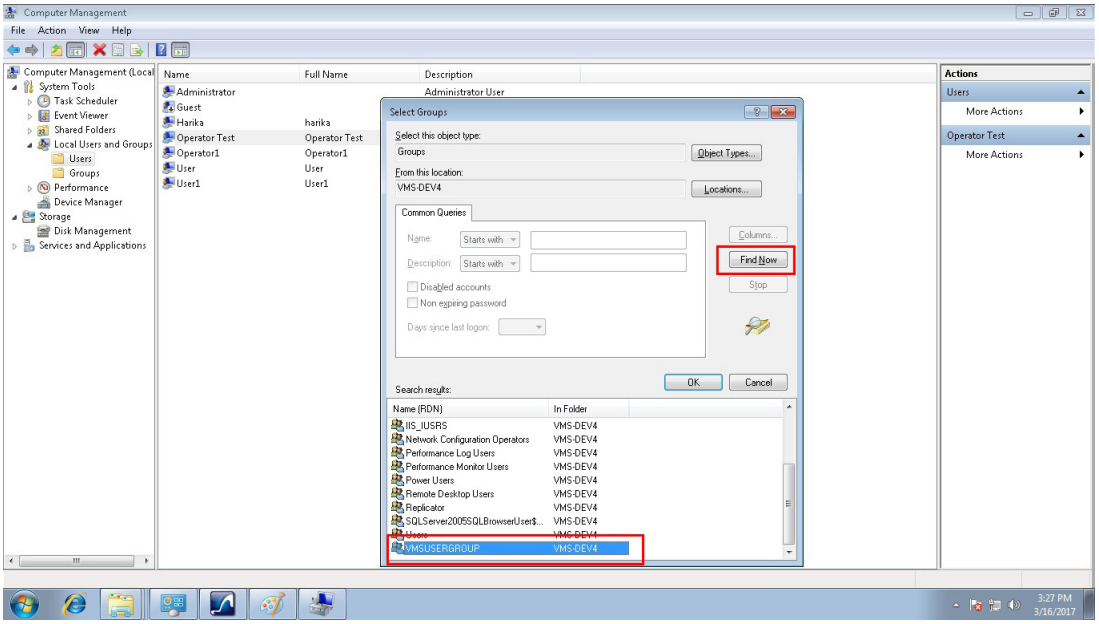
4. Click **Member of** tab and then click **Add**. The **Select Groups** dialog appears as shown below.



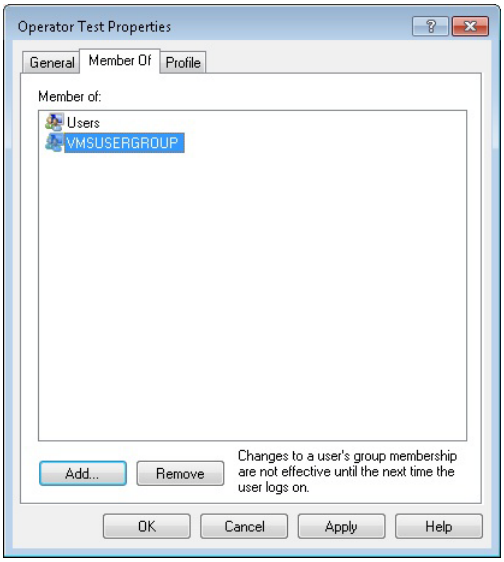
5. Click **Advanced**. The **Select Groups** windows appears as shown below.



6. Click **Find Now** to display the list of groups and then locate **VMSUSERGROUP**. Click **OK**. The group is displayed under **Select Groups** dialog as shown below.



7. Click **OK**. The group is displayed under the **Operator Test Properties** dialog as shown below.



8. Click **Apply** and then click **OK**.

Firewall Settings

See the following tables while configuring the firewall settings for MAXPRO VMS.

Server Side Configuration

The following server side application executable files need to be excluded with the following port configuration.

Application	Description	Port	Type	Port Number
Trinity.SystemServices.exe	Server Operations	TCP	Custom	20007
	Controller	TCP	Custom	26026
	DNS Server	TCP	Custom	53
Trinity.Controller.exe	Controller Operations	TCP	Custom	26026
Scheduler	Scheduler Operations	TCP	Custom	20010
HVA	Honeywell Video Analytics	TCP	Custom	20008

RECORDERS

	Ports	Port	Type	Port Number
Programs	DCOM Services	TCP	Standard	135
	File and Printer Sharing	TCP	Standard	139, 445
		TCP	Standard	137, 138
	DNS Server	TCP	Standard	53
	Client and Server Communication	TCP	Standard	80
Applications	Application Description	Executable File Name		
	IP Engine Camera Service	HWDVSCameraManager.exe		
	IP Engine COM Host Service	System32\DllHost.exe		
	IP Engine Event Service	HWDVSEventServer.exe		
	IP Engine Integrity Service	HWDVSDBSIntegrity.exe		
	IP Engine Multi Monitor Coordinator	HWDVSMonitoeCoOrdinator.ex		
Services	Application Description	Executable File Name		
	IP Engine Camera Service	HWDVSCameraManager.exe		
	IP Engine COM Host Service	System32\DllHost.exe		

OTHER RECORDERS

Recorder Name	Port	Type	Port Number
Fusion	TCP	Custom	4000
RapidEye	TCP	Custom	10000
Enterprise	TCP	Custom	2377
	TCP	Custom	2367
	TCP	Custom	2703
	TCP	Custom	1056

Recorder Name	Port	Type	Port Number
HRXD	TCP	Custom	8016
	TCP	Custom	10019
HRDP	TCP	Custom	4000
Digital Sentry	TCP	Custom	18772
MileStone	TCP	Custom	1237
MAXPRO NVR	TCP	Custom	20007
	TCP	Custom	26026
	TCP	Custom	10000
Embedded Recorder	TCP	Custom	37777

Client Configuration

Application Name	Purpose	Type	Port Number
MMShell.Exe	Server Connection	Custom	20007
	Rendering Connection	Custom	20009
	Controller	Custom	26026
	DNS Server	Standard	53
Trinity.RenderingServer.exe	Client Connection	Custom	20007
	DNS Server	Standard	53

UltraKey

To avoid UltraKey device from going offline on a firewall enabled environment, please allow the following in the firewall rules.

- ICMP 'echo-request' (type 8) packets out.
- ICMP 'echo-reply' (type 0) packets in.

Note: Firewall rule configuration should be done so that the Ultra Key socket connection accepts only from specified Ips.

Honeywell Security and Fire
Products Americas (Head Office)
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299, USA
www.honeywell.com/security
☏ +1 800 323 4576

Honeywell Security and Fire Europe/South Africa
Aston Fields Road, Whitehouse Industrial Estate
Runcorn, WA7 3DL, United Kingdom
www.honeywell.com/security/uk
☏ +44 (0) 1928 754 028

Honeywell Security and Fire Products Americas
Caribbean/Latin America
9315 NW 112th Ave.
Miami, FL 33178, USA
www.honeywell.com/security/clar
☏ +1 305 805 8188

Honeywell Security and Fire Asia Pacific
35F Tower A, City Center, 100 Zun Yi Road
Shanghai 200051, China
www.asia.security.honeywell.com
☏ +86 21 2219 6888

Honeywell Security and Fire Middle East/N. Africa
Emaar Business Park, Sheikh Zayed Road
Building No. 2, Office No. 301
Post Office Box 232362
Dubai, United Arab Emirates
www.honeywell.com/security/me
☏ +971 (0) 4 450 5800

Honeywell Security and Fire Northern Europe
Ampèrestraat 41
1446 TR Purmerend, The Netherlands
www.honeywell.com/security/nl
☏ +31 (0) 299 410 200

Honeywell Security and Fire Deutschland
Johannes-Mauthe-Straße 14
72458 Albstadt, Germany
www.honeywell.com/security/de
☏ +49 (0) 7431 801-0

Honeywell Security and Fire France
Immeuble Lavoisier
Parc de Haute Technologie
3-7 rue Georges Besse
92160 Antony, France
www.honeywell.com/security/fr
☏ +33 (0) 1 40 96 20 50

Honeywell Security and Fire Italia SpA
Via della Resistenza 53/59
20090 Buccinasco
Milan, Italy
www.honeywell.com/security/it
☏ +39 (0) 2 4888 051

Honeywell Security and Fire España
Avenida de Italia, n° 7, 2ª planta
C.T. Coslada
28821 Coslada, Madrid, Spain
www.honeywell.com/security/es
☏ +34 902 667 800

Honeywell

THE POWER OF **CONNECTED**

www.honeywell.com/security
+1 800 323 4576 (North America only)
https//honeywellsystems.com/ss/techsupp/index.html

www.honeywell.com/security/uk
+44 (0) 1928 754 028 (Europe only)
https//honeywellsystems.com/ss/techsupp/index.html

Document: 800-23557-B – 11/2017