

Honeywell Remote Management

INSTALLATION GUIDE

HRM Overview.....	2
What You Need.....	3
Local / Domain Admin.....	3
Probe Device.....	3
Devices.....	3
Connectivity Requirement.....	3
Log into HRM.....	3
Install Windows Probe.....	5
Device Discovery.....	6
Install Windows Agent.....	11
View Outstanding Issue	12
View All Devices	13
HRM PATCH MANAGEment.....	14
Patch Detection.....	14
Patch Pre-download	14
Patch on Demand.....	15
Patch Installation Window.....	17
Add Reboot Window.....	18
ICT Tasking.....	21
Windows Server Disk Performance	21
Windows Disk Free Space.....	21
Windows CPU Utilization.....	22
Windows Memory Utilization	22
SQL Database Growth Rate.....	23
Active Directory Domain Services Monitoring.....	24
Anti-Virus Agent and Update Status (includes McAfee MOVE).....	25
Backup Job / Copy Job Status / Duration.....	25
DVM Backup Status (Nightly Scripted Database Backup).....	26
LUN (Virtual Disks) Free Space.....	26
Windows Services (Start/Stop/Disabled).....	27
Windows Firewall Status (Servers & Workstations)	27
Windows Updates / Patch Status	28
Monitor HRM agent status	28
Thresholds / Tuning for Monitoring Services	29

HRM OVERVIEW

Honeywell Remote Management (HRM) tool will undertake several automated checks on the server, and workstation status will be run using an automated network monitoring tool.

The tool will centrally capture and analyze key event information relating to the underlying ICT infrastructure and systems to provide an overall health status of the system and better direct technicians' reactive and preventative maintenance activities.

In some cases, the tool can alert technicians to problems before they cause an outage and before we would have normally been able to identify the problems manually. A key benefit of the tool is the earlier identification of actual and potential server problems.

From a preventative maintenance perspective, the tool will monitor key events to minimize the amount of manual routine preventative maintenance checks that need to be done.

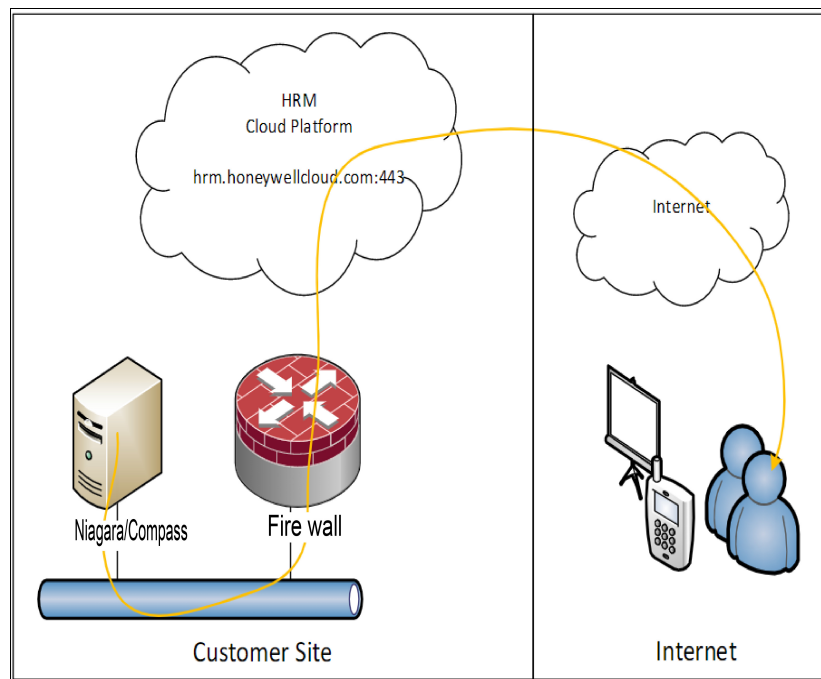


Fig. 1 HRM Overview

WHAT YOU NEED

Local / Domain Admin

Create an account on device local Users and Group or in the client's Active Directory that is part of the Domain Admins group (i, e., Local System administrative privileges) and a password that never expires. We will give this account to run the Windows Probe during installation to allow for Agent install and a host of other functions.

Probe Device

A probe /agent is a software component that resides on a host within a customer's network, behind their firewall or private IP space. Probes provide monitoring and management services for devices on that private network.

The probe should be installed on a host which is protected, ideally a server that is not be constantly rebooted.

Devices

The devices that you want to monitor. This could be servers or client machines connected to the network.

Connectivity Requirement

All devices need to communicate with Honeywell Remote Management (HRM) server that is <https://hrm.honeywell-cloud.com> via port 443.

Please work with the customer IT to change firewall rules to allow the traffic.

LOG INTO HRM

You can use the credential information provided by the HRM admin team to log into HRM <https://hrm.honeywell-cloud.com>.

The username should be your Honeywell email address, and the password will be sent in a separate encrypted email.

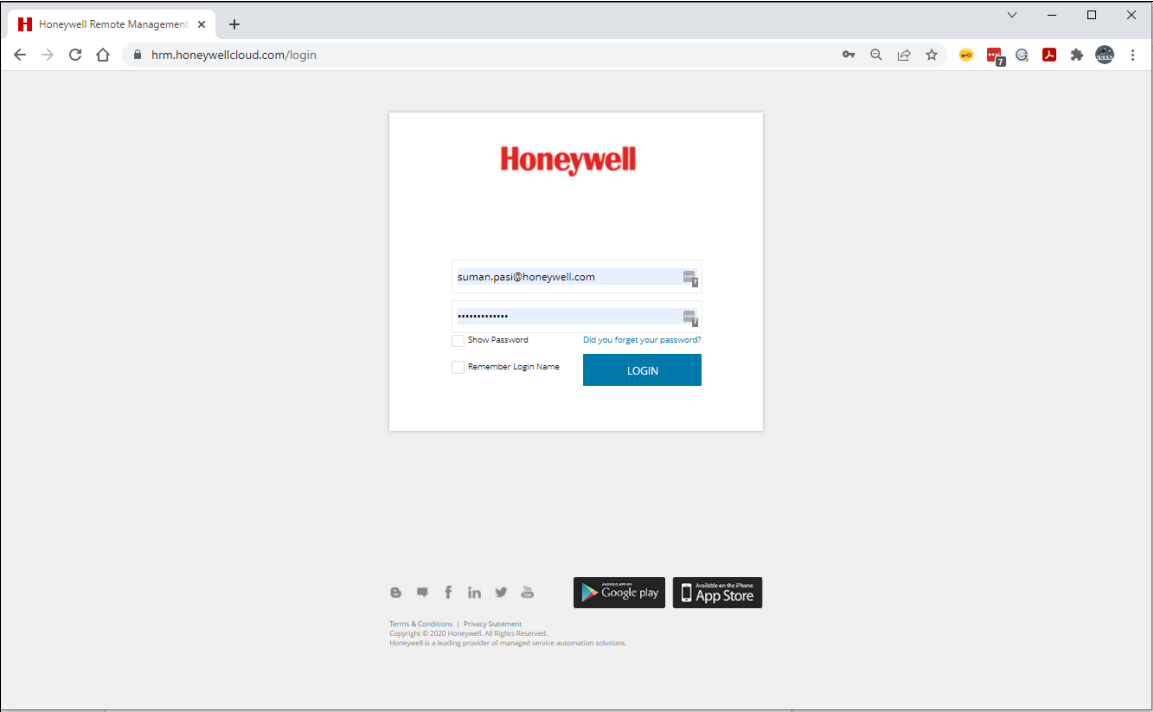


Fig. 2 HRM Login Page

We strongly recommend changing your password the first time you log on to HRM. You could click the link “**Forgot password**” to reset.

You could switch the customer you want to view by clicking the drop-down list.

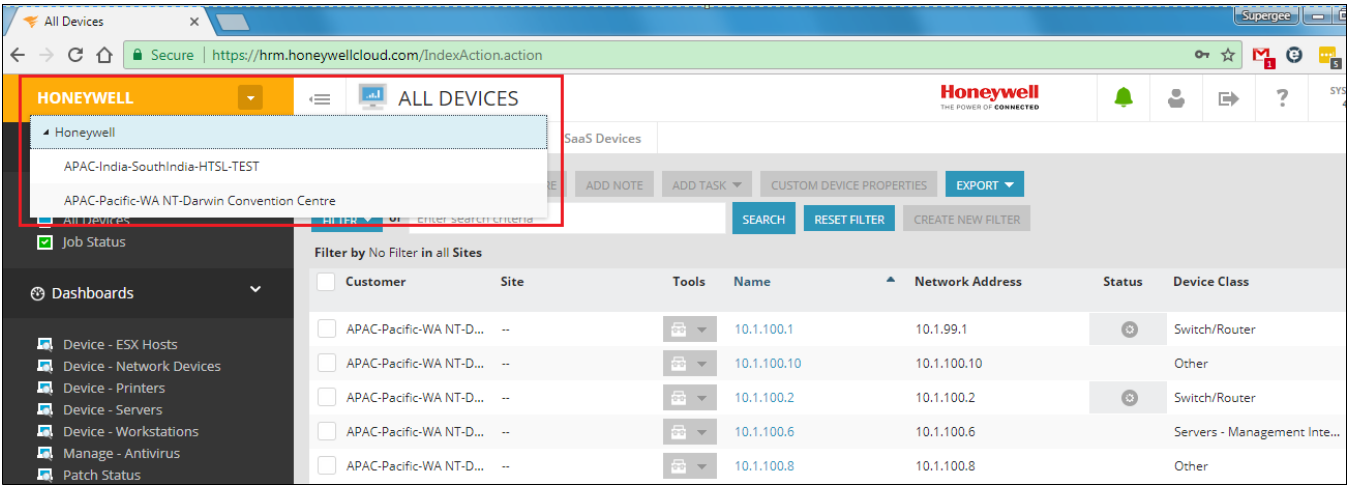


Fig. 3 HRM Page View

INSTALL WINDOWS PROBE

A software named "Probe" must be installed on the gateway server to allow HRM to discover devices on the network.

1. You need to access the HRM website (<https://hrm.honeywellcloud.com>).
2. Go to the customer you want to install Probe.
3. Click **Actions** > **Download Agent/Probe**.
4. Click the **Windows Probe** as circled below.

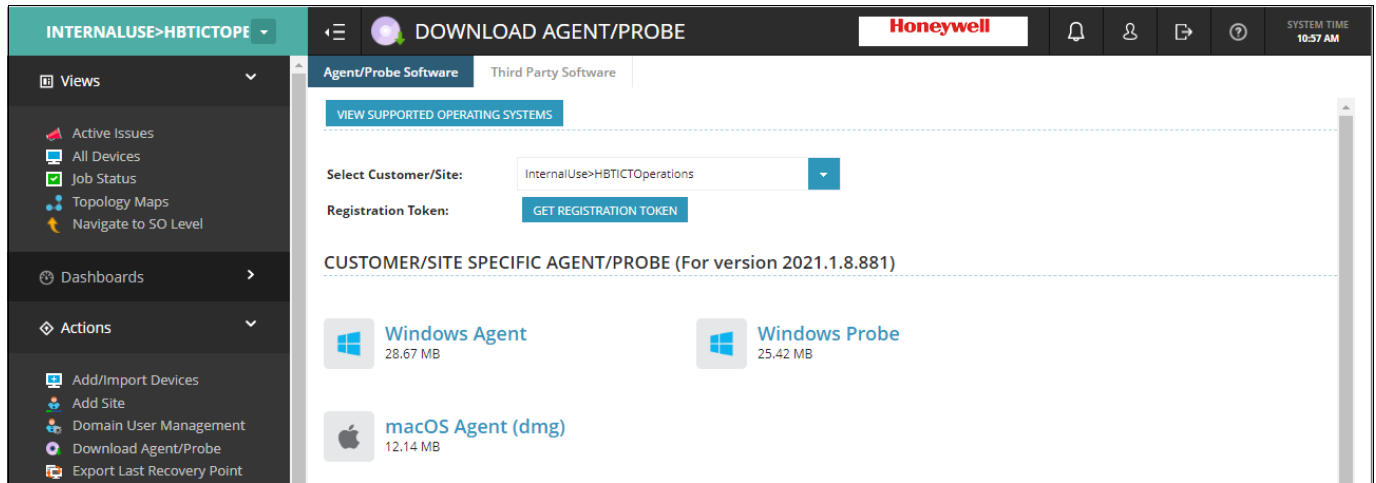


Fig. 4 Windows Probe Installation

Once the Probe software is downloaded, install it in the identified system for Probe communication. Use the default admin account or the specific admin account that was created for the Probe.

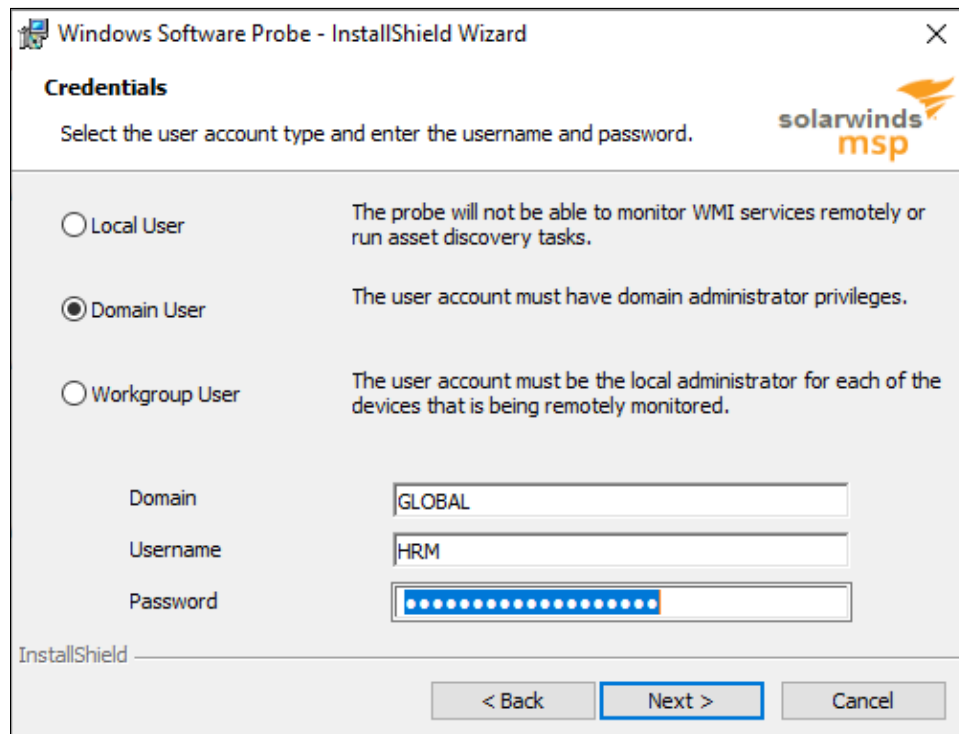


Fig. 5 Windows Software Probe

Once the probe software is installed, verify that the system with a probe is listed in the N-central portal via **Administration > Probe**.

Site	Updating	Probe Name	Network Address	Status	Key	Version	State
--		HBS-DOEU-WEB01 - Windows	10.250.201.4	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-RDS01 - Windows	10.250.200.8	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-Mgmt02 - Windows	10.250.5.5	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-ICT01 - Windows	10.250.201.5	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-DC02 - Windows	10.250.200.7	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-DC01 - Windows	10.250.200.6	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-CC04 - Windows	10.250.13.4	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-CC03 - Windows	10.250.11.4	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-CC02 - Windows	10.250.10.6	✓	GET KEY	2021.1.8.881	ON
--		HBS-DOEU-CC01 - Windows	10.250.10.5	✓	GET KEY	2021.1.8.881	ON

Fig. 6 N-central Portal

DEVICE DISCOVERY

The discovery job is used to detect/import the devices automatically, so you don’t have to add devices manually in HRM.

- 1. You could run the discovery tasks via **Actions > Run a Discovery**.

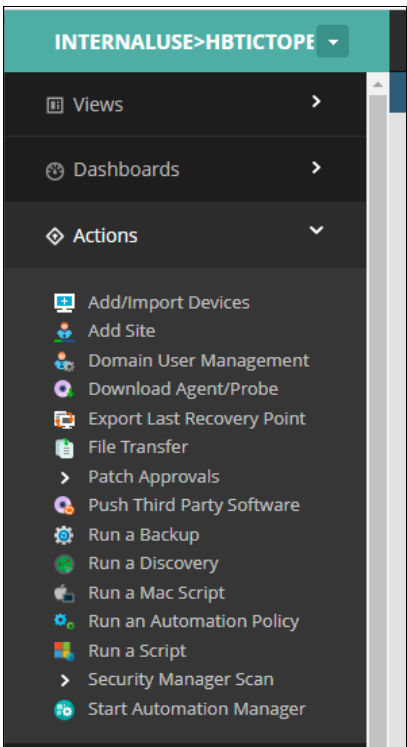


Fig. 7 Run a Discovery

You will be presented with the following display.

2. Fill in the **IP range** for the subnet you wish to discover or a single host address.

ADD DISCOVERY JOB

Name: Discovery Job - 2022-03-14 13h51m13s

Description:

Devices to Discover | Auto Import | Notifications | SNMP Settings | Advanced Settings | VMware Settings | Schedule

Customer: InternalUse>HBTICTOperations

Select a Site: OFF

Site:

Registration Token Valid Until: 2022-04-01 11:59 PM

Probe: CAMEBINCLD - Windows

Discovery Type: ☒ IP Range ☐ IP Address and Netmask

The Target Network: IP Range field contains errors. Specify the IP address of the target network followed by the end value (Ex. 192.168.10.5-200). The end value must be between 1 and 254.

MAC OS X AND LINUX CREDENTIALS

ADD NEW ACCOUNT

User Name	Password	Actions
No accounts exist for this job.		

FINISH CANCEL

Fig. 8 To discover device

3. Switch to the **Auto Import** setting and select the following.

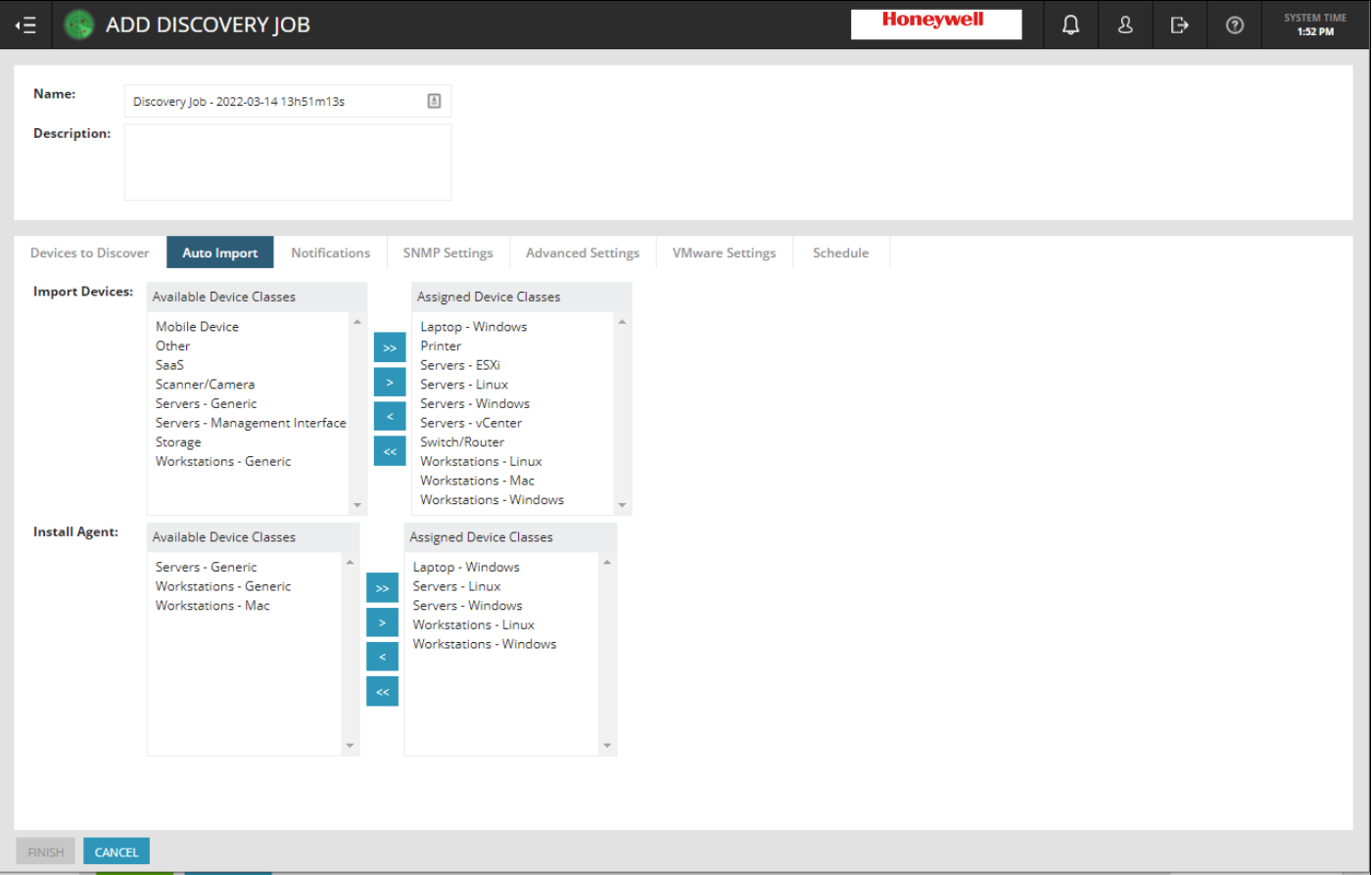


Fig. 9 Auto Import

ADD DISCOVERY JOB

Name: Discovery Job - 2017-10-16 05h47m36s

Description:

Devices to Discover | **Auto Import** | Notifications | SNMP Settings | Advanced Settings | Virtualization Settings

Import Devices:

Available Device Classes

- Mobile Device
- Other
- Printer
- SaaS
- Scanner/Camera
- Servers - Generic
- Servers - Linux
- Servers - Management Interface
- Storage
- Switch/Router

Assigned Device Classes

- Laptop - Windows
- Servers - ESXi
- Servers - Windows
- Workstations - Windows

Install Agent:

Available Device Classes

- Servers - Generic
- Servers - Linux
- Workstations - Generic
- Workstations - Linux
- Workstations - Mac

Assigned Device Classes

- Laptop - Windows
- Servers - Windows
- Workstations - Windows

FINISH **CANCEL**

Fig. 10 Auto Import Devices

- Click on **Finish**. This will schedule the discovery to run. This will normally take 10-30 minutes, depending on the number of devices you want to discover.
- Progress can be checked by selecting **Configuration > Asset Discovery > Discovery Jobs**.

DISCOVERY JOBS					
ADD IMPORT ASSETS DELETE					
<input type="checkbox"/>	Site	Name	Schedule	Last Report	Monitoring Appliance
<input type="checkbox"/>	--	Discovery Job - 2016-01-27 15h10m54s	Once	2016-Feb-01 10:18	EGRP-NETMAN - Windows
<input type="checkbox"/>	--	Discovery Job - 2016-02-01 09h18m03s	Once	2016-Feb-01 10:21	EGRP-NETMAN - Windows
<input type="checkbox"/>	--	Discovery Job - 2016-02-12 16h41m03s	Once	2016-Feb-12 17:26	EGRP-NETMAN - Windows
<input type="checkbox"/>	--	Discovery Job - 2016-04-26 12h31m18s	Once	2016-Apr-26 13:34	EGRP-NETMAN - Windows
<input type="checkbox"/>	--	Discovery Job - 2016-04-26 14h12m01s	Once	2016-Apr-26 14:56	EGRP-NETMAN - Windows
<input type="checkbox"/>	--	EGRPFM - null	Recurring	2 of 19 Unmanaged	EGRP-NETMAN - Windows

Fig. 11 To discover devices

6. Review the list of devices from **Views > All Devices** and remove the ones you don't want to monitor.

PERTH LAB		ALL DEVICES				
Views Active Issues All Devices Job Status Navigate to SO Level Dashboards Actions Reports My Links Configuration Administration Help		Network Devices Mobile Devices SaaS Devices				
		ADD EDIT DELETE ADD SERVICES APPLY SERVICE TEMPLATES MOVE DEVICES UPDATE MONITORING SOFTWARE ADD NOTE				
		CUSTOM DEVICE PROPERTIES EXPORT				
		FILTER or Enter search criteria SEARCH RESET FILTER CREATE NEW FILTER				
		Filter by No Filter in all Sites				
<input type="checkbox"/>	Site	Tools	Name	Network Address	Status	Device Class
<input type="checkbox"/>	--		10.50.0.131	10.50.0.131		Switch/Router
<input type="checkbox"/>	--		10.50.0.132	10.50.0.132		Switch/Router
<input type="checkbox"/>	--		fxesx01	10.50.0.15		Servers - ESXi
<input type="checkbox"/>	--		HONEYWELL-PC	10.50.0.223		Workstations - Windows
<input type="checkbox"/>	--		HWTAM_SYNOLOGY	10.100.100.25		Servers - Generic
<input type="checkbox"/>	--		IBAMSEB1A	10.50.0.110		Servers - Windows
<input type="checkbox"/>	--		ICT101-AV	10.50.0.55		Servers - Windows
<input type="checkbox"/>	--		ICT101-CB01	10.50.0.46		Servers - Windows
<input type="checkbox"/>	--		ICT101-DCA	10.50.0.50		Servers - Windows
<input type="checkbox"/>	--		ICT101-EBiStation500	ict101-ebistation500.ict101....		Workstations - Windows
<input type="checkbox"/>	--		ICT101-EPO	10.50.0.47		Servers - Windows
		REFRESH NOW ON Refresh in: 10 minutes				

Fig. 12 Network Devices

INSTALL WINDOWS AGENT

If the domain admin account is not available, you need to manually install the Windows agent on each Windows machine to be monitored by HRM.

1. You need to access the HRM website (<https://hrm.honeywellcloud.com>).
2. Go to the customer you want to set up.
3. Click **Actions** > **Download Agent/Probe**.
4. Click the **Windows Agent** as circled below.



Fig. 13 Windows Agent Installation

Once the Windows Agent software is downloaded, install it on the Windows devices with the default setting. Change the Proxy setting appropriately if necessary and continue the installation.

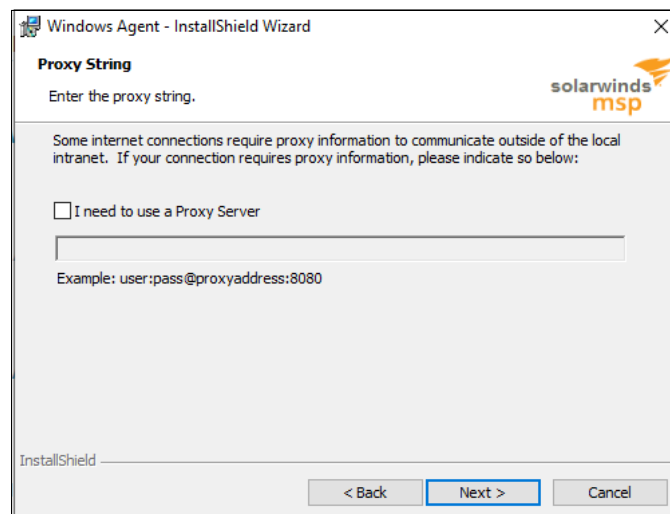


Fig. 14 Windows Agent Proxy Setting Window

The Agent version information can be found via **Views > All devices** when HRM detects it.

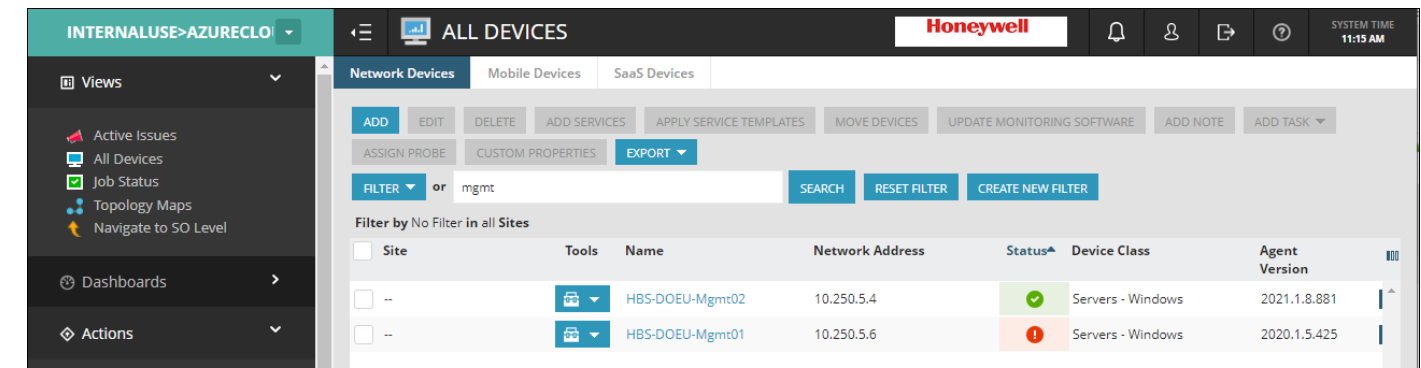


Fig. 15 All Devices

View Outstanding Issues

You could view the outstanding issues by navigating to **Views > Active Issues**.

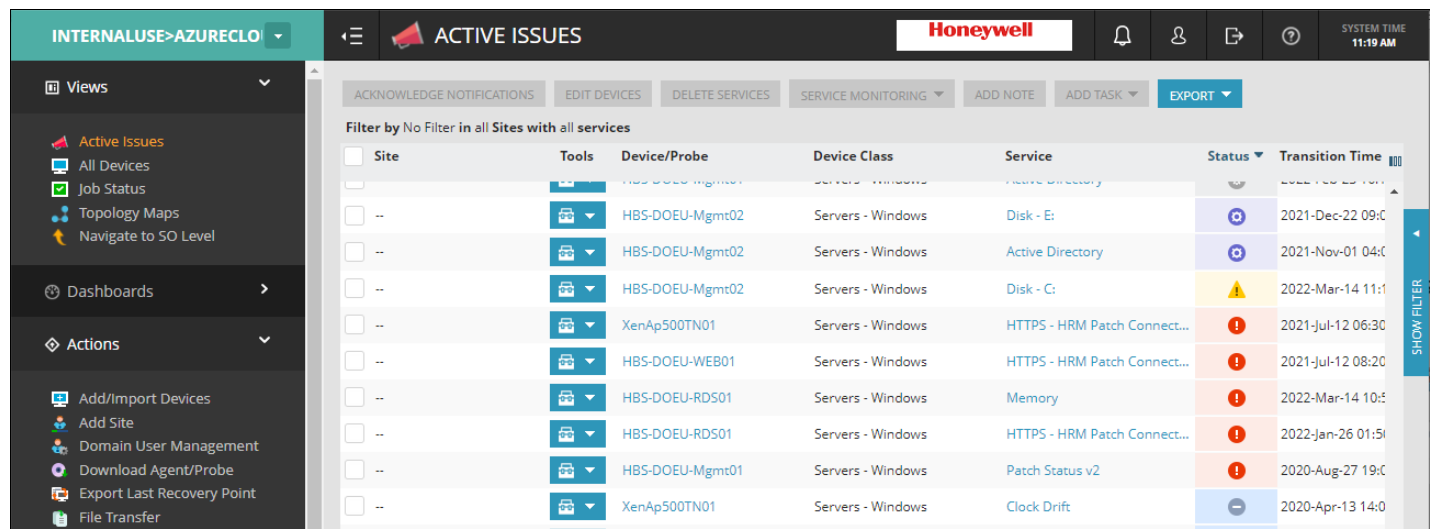


Fig. 16 Active Issues

If you have multi-customer access, you can go to Honeywell (SO level) to view all outstanding issues across all sites. The filter function is available as below to view the only specific site.

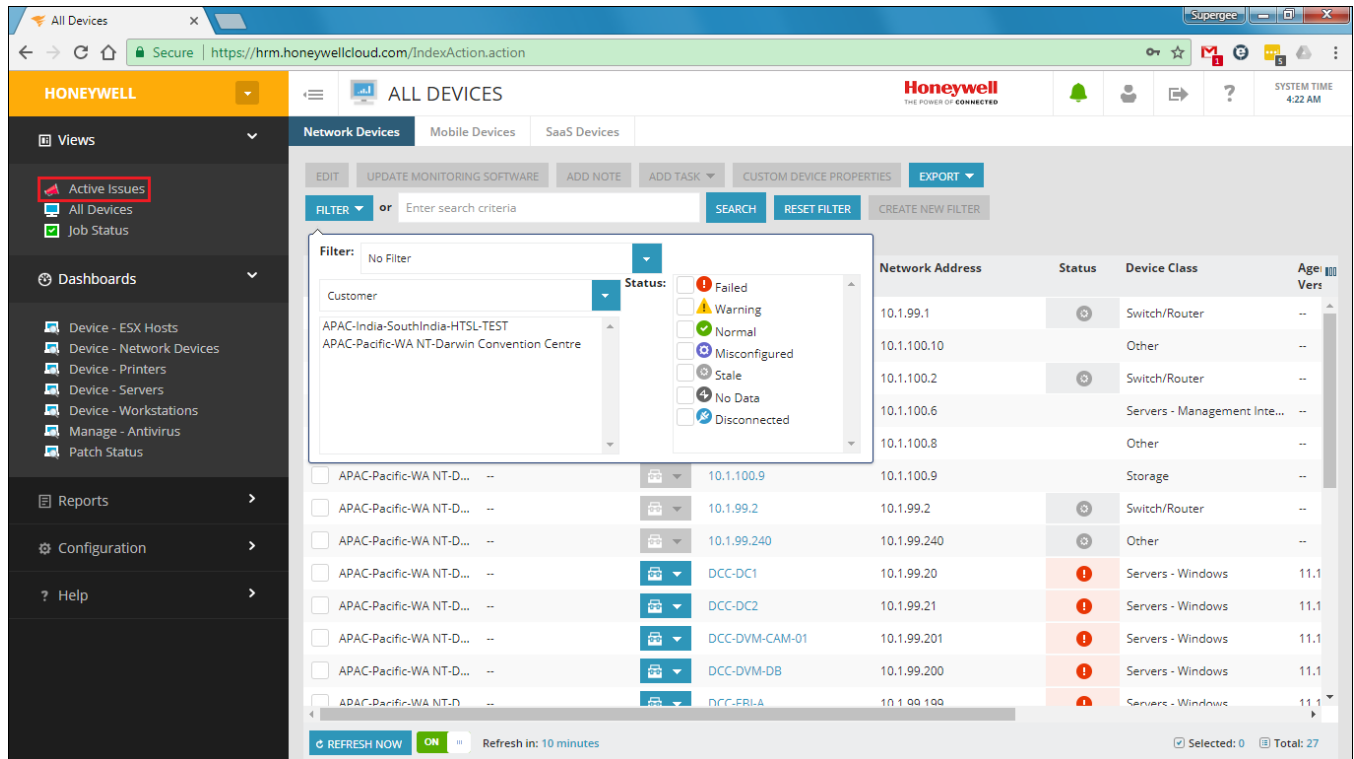



Fig. 17 To filter issues

Click the failure  icon, then you can see the details about the failure.

View All Devices

To view the list of devices managed on your site, click **Views > All Devices**.

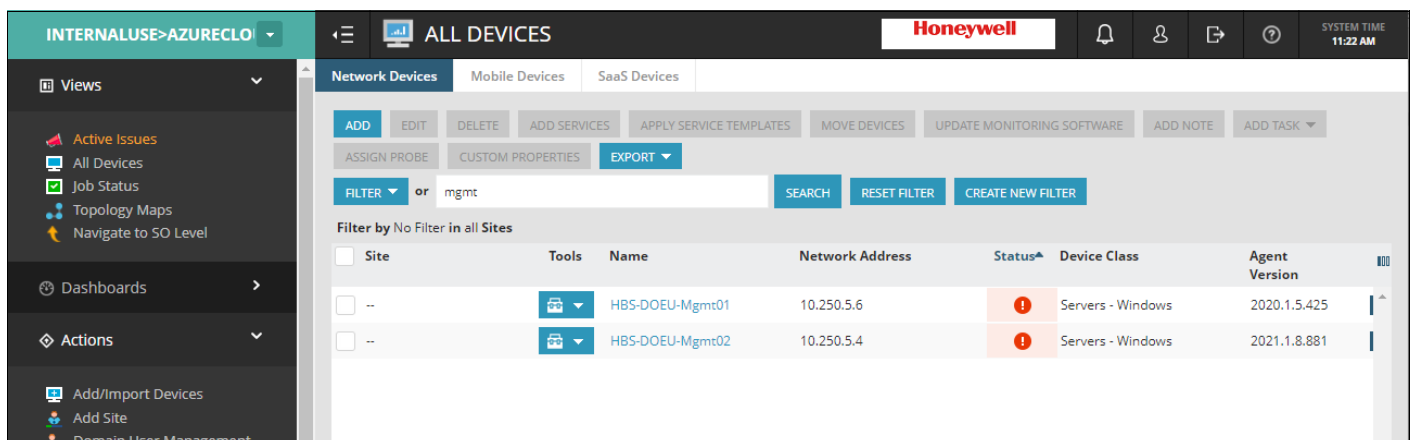


Fig. 18 To view all device

HRM PATCH MANAGEMENT

The Patch v2 Management module can effectively manage the downloading and installation of Microsoft and third-party software patches across your customers networks.

HRM Patch Management can automate processes related to patching or allow very granular control of every step. This can be done using Patch Approval Rules, Patching Maintenance Windows related to detecting, downloading, installing, and potential rebooting of devices.

- Patch Detection
- Patch Download
- Patch On-Demand
- Adding Patch installation Window
- Patch Reboot

Patch Detection

The Patch Detection Maintenance Window specifies when, and for how long, devices check for new updates and communicate this information to MSP HRM. This is important for workstations and servers hosted in virtual environments, where detection can result in cumulative loads and slower performance overall.

Adjust the frequency of maintenance windows to match the frequency of software patches. For example, you can reduce the detection frequency if a server is patched only monthly or quarterly. Also, consider that this process is also for Third-Party Software updates.

We have set up the patch detection windows for all Windows servers at 1 am every day via the rule “Window Server.”

HONEYWELL **RULE DETAILS**

Type: ☒ Public ☐ Private

Name: a - Windows Server Rule

Description:

Devices to Target | Network Device Configuration Options | Mobile Device Configuration Options | Scheduled Task Profiles | Monitoring Options | **Maintenance Windows** | Grant Customers & Sites Access

MAINTENANCE WINDOWS

The MSP N-central Agent can be configured to automatically complete tasks for various N-central features according to a defined schedule.

ADD

Name	Last Modified By	Last Modified Time	Type	Schedule
Patch Detection	supergee he	September 01, 2017 17:39	Patch Detection	1:00 AM every day of every month.
Patch Pre-Download	supergee he	September 01, 2017 17:41	Patch Pre-Download	2:30 AM every day of every month.

Fig. 19 Patch Detection

Patch Pre-download

The Pre-download Maintenance Window defines the period when you want to download approved patches to the device for installation. A best practice is to download at least two hours before you plan to install the patch to allow for sufficient time to obtain the installation packages.

The pre-download window is when the patches get downloaded, either via the Probe or directs to the Agent, depending on your Profile settings.

We have set up the pre-download window at 2:30 am every day.

The screenshot shows the 'RULE DETAILS' page in the Honeywell N-central console. The rule is named 'a - Windows Server Rule' and is of type 'Public'. The 'MAINTENANCE WINDOWS' section shows a table of scheduled tasks. The 'Patch Pre-Download' task is highlighted with a red box, showing a schedule of '2:30 AM every day of every month.'

Name	Last Modified By	Last Modified Time	Type	Schedule
Patch Detection	supergee he	September 01, 2017 17:39	Patch Detection	1:00 AM every day of every month.
Patch Pre-Download	supergee he	September 01, 2017 17:41	Patch Pre-Download	2:30 AM every day of every month.

Fig. 20 Patch Pre-download

Patch on Demand

This is the recommended approach when you don't have the regular maintenance window agreed with the customer, or you want to apply critical patches urgently.

You can initiate a patch cycle on one or more devices outside your regular schedule or "On Demand." This lets you patch customers without a set install schedule and update outlying systems only available during random intervals. You can also include a reboot in the process.

Select your devices and initiate Patch On-Demand.

Select the device from all devices list > **ADD TASK** > **Patch Management** > **Patch On Demand**.

The screenshot shows the 'ALL DEVICES' page in the Honeywell N-central console. The 'ADD TASK' dropdown menu is open, showing the 'Patch Management' option, which has a sub-menu with 'Patch On Demand' selected. The 'Patch On Demand' sub-menu includes options like 'Patch Detection On Demand', 'Patch Reboot On Demand', 'Add Multiple Windows Wizard', 'Clear Device Level Patch Windows', 'Add Detection Window', 'Add Pre-Download Window', 'Add Installation Window', and 'Add Reboot Window'.

Fig. 21 Patch on Demand

A new patch on-demand window appears, update patch classifications window, select Patch On-demand window, update Reboot Options window, and click on **SAVE** to select Patch On-Demand.

MAINTENANCE WINDOW - PATCH ON DEMAND

Selecting a large group of devices may result in considerable consumption of bandwidth in your customer environment(s) and a heavy load on your N-able N-central server.

PATCH ON DEMAND

Name of the Task: Patch On Demand - 2022-03-14 15h19m04s

Classifications to Install:

Critical Updates
Definition Updates
Drivers
Feature Packs
Security Updates
Service Packs
Third Party
Tools
Update Rollups
Updates

>>
>
<
<<

PATCH ON DEMAND SCHEDULE

Schedule Type: Now

Start Date: March 14, 2022

Start Time: 3:19 PM

Maintenance Window Should Last For: 120 minutes

REBOOT ACTION

Reboot After Install:

REBOOT OPTIONS

Reboot Method: Force user to reboot in the maintenance window

A warning dialog will be displayed if a system reboot is required. The user may choose to save their files or postpone the reboot.

Prompt and Countdown For: 15 minutes before continuing with reboot.

Message From: Default Custom Name

Message: Default Custom

Place Device in Downtime During Reboot: ☒

Force Device out of Downtime After: 240 minutes

Save Current System State: ☒

SAVE CANCEL

Fig. 22 Maintenance Window

Patch Installation Window

Patch installation windows allow the field professional to configure a pre-determined window for patches to automatically be applied. HRM can download, install and reboot the machines automatically without any intervention from the field professional.

1. Select the device from all devices list > **ADD TASK** > **Patch Management** > **Add Installation Window**.

The screenshot displays the HRM interface with the 'Network Devices' tab selected. A table lists devices with columns for Site, Tools, Name, Network Address, and Status. Two devices are listed: HBS-DOEU-Mgmt01 and HBS-DOEU-Mgmt02. The 'ADD TASK' dropdown menu is open, showing options like File Transfer, Push Third Party Software, Run a Mac Script, Run a Script, Run an Automation Policy, Security Manager Scan, Maintenance, and Patch Management. The 'Patch Management' option is selected, and its submenu is visible, showing options like Patch On Demand, Patch Detection On Demand, Patch Reboot On Demand, Add Multiple Windows Wizard, Clear Device Level Patch Windows, Add Detection Window, Add Pre-Download Window, Add Installation Window, and Add Reboot Window. The 'Add Installation Window' option is highlighted.

Site	Tools	Name	Network Address	Status
✓ --		HBS-DOEU-Mgmt01	10.250.5.6	
✓ --		HBS-DOEU-Mgmt02	10.250.5.4	

Fig. 23 Patch Installation Window

2. Now choose a name for the task or accept the default name.
3. Select the patch classifications for installation
4. Select **"Install patches only at a schedule time."**
5. Adjust the maintenance window duration if you have a long list of patches to be applied. It's 180 minutes by default.
6. Setup the schedule based on the agreement with your customer.
7. Click **Save**.

MAINTENANCE WINDOW - PATCH INSTALLATION

MAINTENANCE OPTIONS

Name:

Patch Installation - 2022-03-14 15h36m49s

Classifications to Install:

Critical Updates
Definition Updates
Drivers
Feature Packs
Security Updates
Service Packs
Third Party
Tools
Update Rollups
Updates

>>
>
<
<<

INSTALLATION SCHEDULE

When to Install Patches:

☐ Install patches as soon as they are approved

☒ Install patches only at a scheduled time

Maintenance Window Should Last For:

180 minutes

Schedule:

Custom

Start Time:

ADD
DELETE
CLEAR ALL

02:00

Days of the Week:

☐ Every day

☒ Selected days

Sun Mon Tue Wed Thu Fri Sat All Clear

Days of the Month:

☒ Every day

☐ Last day

☐ Selected dates

1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31 All Clear

Months of the Year:

☒ Every month

☐ Selected months

Jan Feb Mar
Apr May Jun
Jul Aug Sep
Oct Nov Dec
All Clear

SAVE CANCEL

Fig. 24 Patch Installation Maintenance Window

Add Reboot Window

The Reboot Maintenance Window defines the period when the device can be rebooted. The reboot maintenance window will not be triggered if the server is not required to reboot after patch installation.

The reboot countdown timer gives the user a grace period to save files and close applications before the reboot occurs.

It's recommended that you leave enough time between patch installation and reboot windows to allow enough time for patches to be applied, for example, 3 hours.

hours.

31-00541-01

18

The screenshot shows the Honeywell Remote Management interface. At the top, there are tabs for 'Network Devices', 'Mobile Devices', and 'SaaS Devices'. Below these are various action buttons: 'ADD', 'EDIT', 'DELETE', 'ADD SERVICES', 'APPLY SERVICE TEMPLATES', 'MOVE DEVICES', 'UPDATE MONITORING SOFTWARE', 'ADD NOTE', 'ADD TASK', 'ASSIGN PROBE', 'CUSTOM PROPERTIES', and 'EXPORT'. A filter bar is present with a search input containing 'mgmt' and buttons for 'SEARCH', 'RESET FILTER', and 'CREATE NEW FILTER'. Below the filter bar, a table lists devices with columns for 'Site', 'Tools', 'Name', 'Network Address', and 'Status'. Two devices are listed: 'HBS-DOEU-Mgmt01' and 'HBS-DOEU-Mgmt02'. The 'ADD TASK' button is open, showing a dropdown menu with options: 'File Transfer', 'Push Third Party Software', 'Run a Mac Script', 'Run a Script', 'Run an Automation Policy', 'Security Manager Scan', 'Maintenance', and 'Patch Management'. The 'Patch Management' option is selected, opening a sub-menu with options: 'Patch On Demand', 'Patch Detection On Demand', 'Patch Reboot On Demand', 'Add Multiple Windows Wizard', 'Clear Device Level Patch Windows', 'Add Detection Window', 'Add Pre-Download Window', 'Add Installation Window', and 'Add Reboot Window'.

Site	Tools	Name	Network Address	Status
✓ --		HBS-DOEU-Mgmt01	10.250.5.6	
✓ --		HBS-DOEU-Mgmt02	10.250.5.4	

Fig. 25 Add Reboot Window

From the “**All devices**” option, select one or multiple devices from the device list.

Now select **Add Task > Patch Management > Add Reboot Window**.

MAINTENANCE WINDOW - PATCH REBOOT

MAINTENANCE OPTIONS

Name:

Patch Reboot - 2022-03-14 15h40m42s

REBOOT OPTIONS

Reboot Method:

Force user to reboot in the maintenance window

A warning dialog will be displayed if a system reboot is required. The user may choose to save their files or postpone the reboot.

Prompt and Countdown For:

30 minutes before continuing with reboot.

Message From:

Default

Custom Name

Honeywell Connected Buildings Customers

Message:

Default

Custom

This message is from {{MessageFrom}}. Your computer has been scheduled to be restarted in order to complete important system updates.

Place Device in Downtime During Reboot:

Force Device out of Downtime After:

120 minutes

Save Current System State:

REBOOT SCHEDULE

When to Reboot:

Prompt for reboot immediately when required

Prompt for reboot only at a scheduled time

Maintenance Window Should Last For:

180 minutes

Schedule:

Custom

Start Time:

ADD

03:00

DELETE

CLEAR ALL

Days of the Week:

Every day

Selected days

Sun

Mon

Tue

Wed

Thu

Fri

Sat

All

Clear

Days of the Month:

Every day

Last day

Selected dates

Months of the Year:

Every month

Selected months

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

All

Clear

Jan

Feb

Mar

Apr

May

Jun

Jul

Aug

Sep

Oct

Nov

Dec

All

Clear

SAVE

CANCEL

Fig. 26 Reboot Maintenance Window

31-00541-01

20

ICT TASKING

Here is the list of ICT tasks being monitored in HRM.

Windows Server Disk Performance

Select the “**Monitoring**” tab and click on the **Disk I/O** metrics.

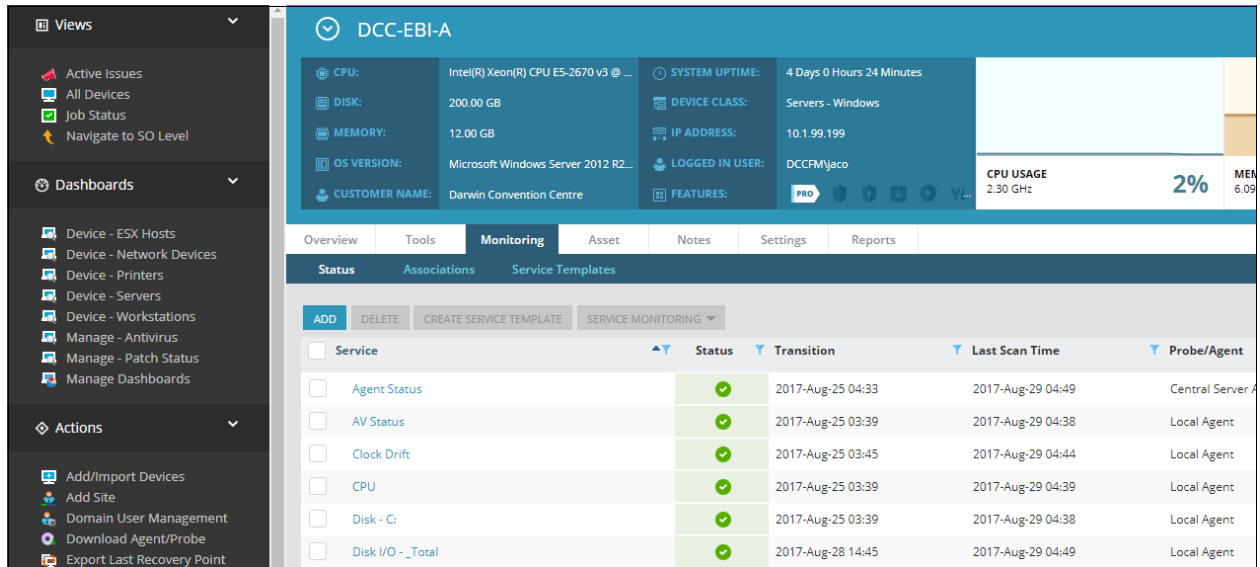


Fig. 27 Windows Server Disk Performance

Windows Disk Free Space

Select the “**Monitoring**” tab and click on the disk partition you would like to check to see the current disk usage metrics.

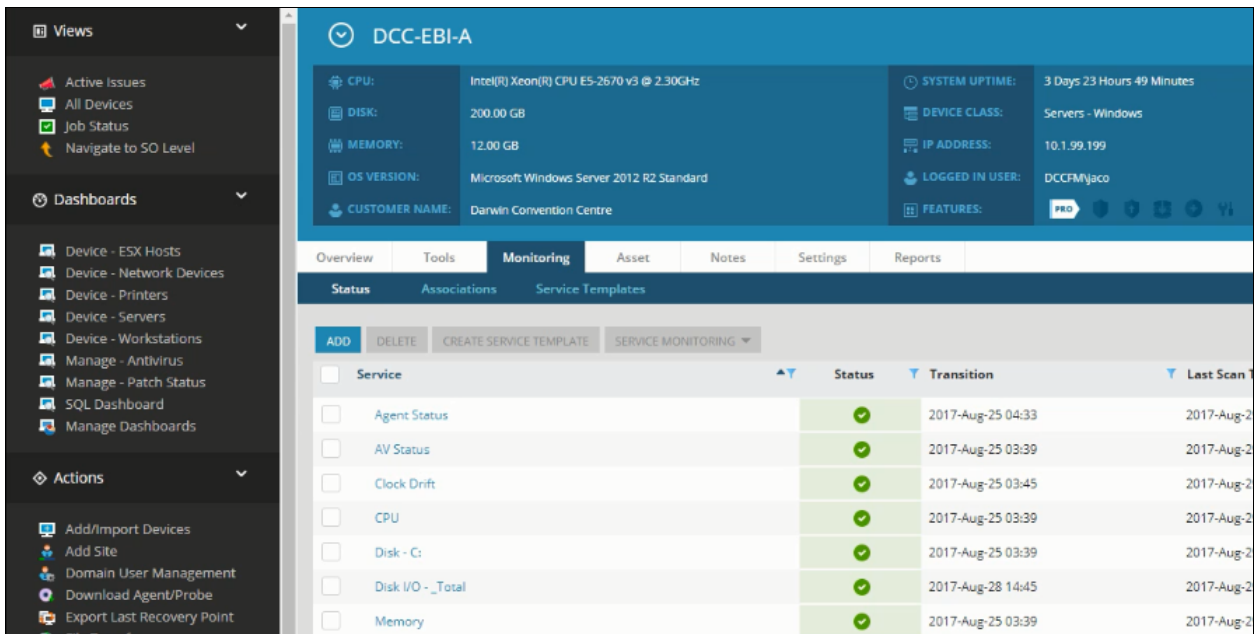


Fig. 28 Windows Disk Free Space

Windows CPU Utilization

Select the “Monitoring” tab and Click on **CPU**.

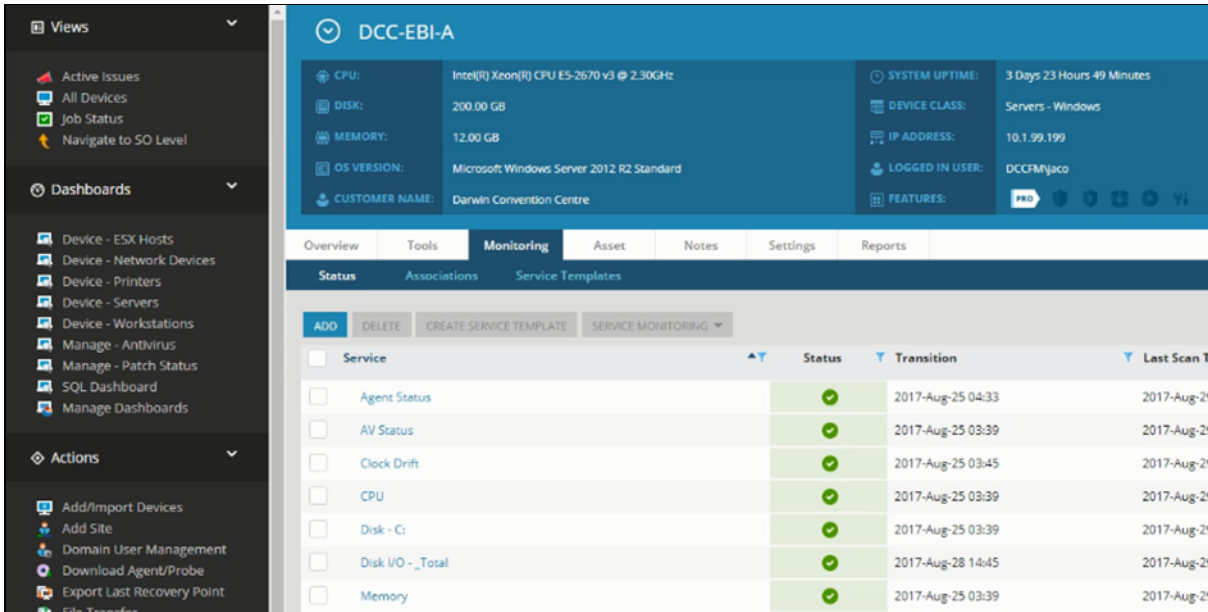


Fig. 29 Windows CPU Utilization

Windows Memory Utilization

Select the “Monitoring” tab and Click on **Memory**.

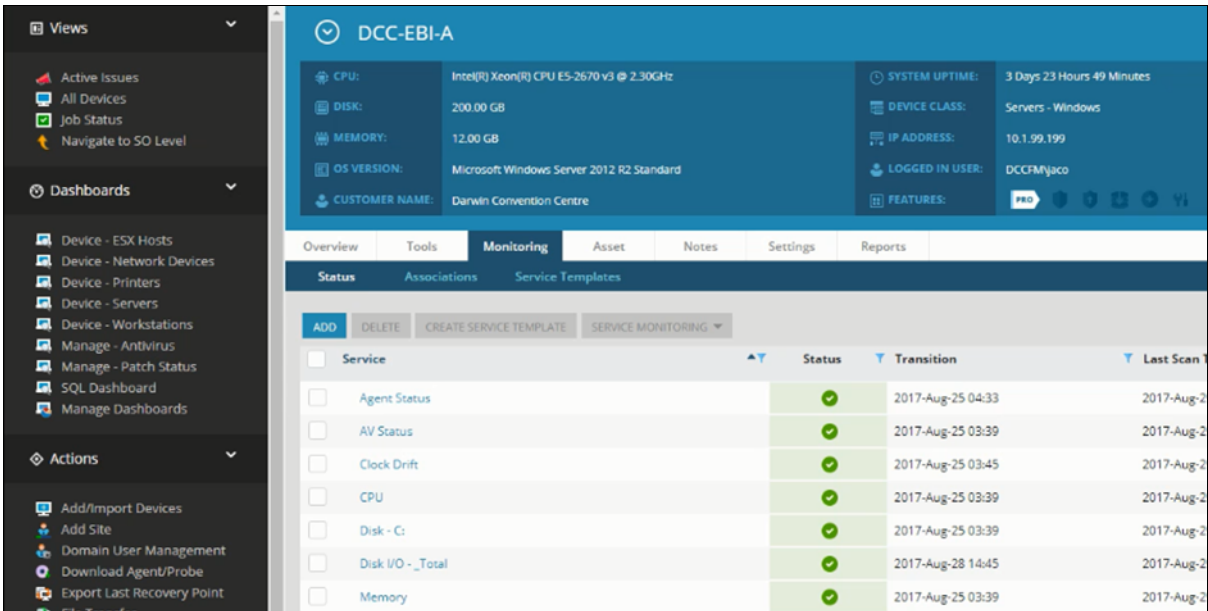


Fig. 30 Windows Memory Utilization

SQL Database Growth Rate

Select the **“Monitoring”** tab. User will see the available SQL Database Growth Check options for the database required. Select the required database options.

The screenshot shows the Honeywell Remote Management interface. The left sidebar contains navigation menus for 'Views', 'Dashboards', and 'Actions'. The main content area is titled 'DEVICE DETAILS' for device 'EBITINYB'. The 'Monitoring' tab is selected, showing a table of services. A red box highlights the 'SQL Database Growth Check' options.

Service	Status	Transition	Last Scan Time
Patch Status	❌	2017-Nov-10 11:43	2017-Nov-12 21:06
Reboot Required	✅	2017-Nov-12 11:36	2017-Nov-13 04:35
SQL Database Growth Check - acsdld	✅	2017-Nov-10 21:34	2017-Nov-13 04:35
SQL Database Growth Check - activator	✅	2017-Nov-07 21:34	2017-Nov-13 04:35
SQL Database Growth Check - CloudConnector	✅	2017-Nov-07 21:34	2017-Nov-13 04:35
SQL Database Growth Check - CMS	✅	2017-Oct-27 21:34	2017-Nov-13 04:35
SQL Database Growth Check - gs	✅	2017-Oct-27 21:34	2017-Nov-13 04:35
SQL Database Growth Check - hwreports	✅	2017-Oct-27 21:34	2017-Nov-13 04:35
SQL Database Growth Check - hwsystem	✅	2017-Nov-06 21:34	2017-Nov-13 04:35
SQL Database Growth Check - irldb	✅	2017-Nov-11 21:35	2017-Nov-13 04:35
SQL Last Backup Datetime - MSSQLSERVER\acsdld	✅	2017-Oct-27 18:40	2017-Nov-13 04:40

Fig. 31 Example of SQL Database Growth Rate Options

Active Directory Domain Services Monitoring

Select the “**Monitoring**” Tab and Click on the relevant Services Active Directory, DNS, Process lsass.exe, and the Windows Event Logs specifically to ADDS.

>

DCC-DC1

Overview

Tools

Monitoring

Asset

Notes

Status

Associations

Service Templates

ADD

DELETE

CREATE SERVICE TEMPLATE

SERVICE MONITORING ▼

☐

Service

▲▼

Status

☐

Active Directory

☒

☐

Agent Status

☒

☐

AV Status

☒

☐

Clock Drift

☒

☐

CPU

☒

☐

Disk - C:

☒

☐

Disk I/O - _Total

☒

☐

DNS

☒

☐

DNS Performance Counters

☒

☐

Memory

☒

☐

Process - lsass.exe

☒

☐

Reboot Required

☒

☐

Uptime

☒

☐

Windows Event Log

☒

☐

Windows Event Log - AD (Directory Service Log)

☒

☐

Windows Event Log - AD (System Log)

☒

☐

Windows Event Log - DHCP Server

☒

☐

Windows Event Log - DNS

☒

Fig. 32 Active Directory Domain Services

Anti-Virus Agent and Update Status (includes McAfee MOVE)

Select the “**Monitoring**” tab and Click on “**AV Status.**”

Service	Status	Transition	Last Scan Time
Agent Status	✓	2017-Aug-25 04:33	2017-Aug-25 04:33
AV Status	✓	2017-Aug-25 03:39	2017-Aug-25 03:39
Clock Drift	✓	2017-Aug-25 03:45	2017-Aug-25 03:45
CPU	✓	2017-Aug-25 03:39	2017-Aug-25 03:39
Disk - C:	✓	2017-Aug-25 03:39	2017-Aug-25 03:39
Disk I/O - _Total	✓	2017-Aug-28 14:45	2017-Aug-28 14:45
Memory	✓	2017-Aug-25 03:39	2017-Aug-25 03:39

Fig. 33 AV Status

Backup Job / Copy Job Status / Duration

Select the “**Monitoring**” tab and Click on “**Acronis backup with WMI**” for Physical servers or “**VEEAM JOB MONITOR**” for virtual servers.

Monitoring						
Status Associations Service Templates						
ADD DELETE CREATE SERVICE TEMPLATE SERVICE MONITORING						
Service	Status	Transition	Last Scan Time	Probe/Agent		
Acronis Backup Log Check - C:\backupresult.txt	✓	2017-Sep-01 04:00	2017-Sep-01 04:59	Local Agent		
Acronis Backup With WMI	✓	2017-Sep-01 05:11	2017-Sep-01 05:44	Local Agent		
Agent Status	✓	2017-Aug-22 01:15	2017-Sep-01 05:45	Central Server Asset		
AV Status	✓	2017-Aug-07 08:02	2017-Sep-01 05:40	Local Agent		
Clock Drift	✓	2017-Aug-07 08:11	2017-Sep-01 05:44	Local Agent		
CPU	✓	2017-Aug-29 14:47	2017-Sep-01 05:40	Local Agent		
Disk - C:	✓	2017-Aug-07 08:02	2017-Sep-01 05:40	Local Agent		

Fig. 34 Acronis backup with WMI

DVM Backup Status (Nightly Scripted Database Backup)

Select the “**Monitoring**” tab and Click on “SQL LAST BACKUP DATETIME - MSSQLSERVER\DVM.”

Overview Tools Monitoring Asset Notes Settings Reports					
Status Associations Service Templates					
<div> ADD DELETE CREATE SERVICE TEMPLATE SERVICE MONITORING </div>					
Service	Status	Transition	Last Scan Time	Probe/Agent	
<input type="checkbox"/> Patch Status	!	2017-Oct-13 15:31	2017-Oct-24 15:31	Local Agent	
<input type="checkbox"/> Reboot Required	✓	2017-Oct-13 03:18	2017-Oct-25 00:58	Local Agent	
<input type="checkbox"/> SQL Database Information - MSSQLSERVER_Total	✓	2017-Oct-13 03:24	2017-Oct-25 01:01	Local Agent	
<input type="checkbox"/> SQL Last Backup Datetime - MSSQLSERVER\DVM	✓	2017-Oct-13 03:30	2017-Oct-25 00:33	Local Agent	
<input type="checkbox"/> Windows Event Log	✓	2017-Oct-24 16:10	2017-Oct-25 01:10	Local Agent	
<input type="checkbox"/> Windows Event Log - DHCP Server	✓	2017-May-17 03:18	2017-Oct-25 01:10	Local Agent	
<input type="checkbox"/> Windows Event Log - DNS	✓	2017-May-17 03:18	2017-Oct-25 01:10	Local Agent	
<input type="checkbox"/> Windows Event Log - McAfee 8.5i	✓	2017-Jul-24 05:51	2017-Oct-25 01:10	Local Agent	
<input type="checkbox"/> Windows Event Log - SQL 2008	✓	2017-Aug-29 06:17	2017-Oct-25 01:10	Local Agent	

Fig. 35 DVM Backup Status

LUN (Virtual Disks) Free Space

Select the “**Monitoring**” tab and Click on “Datastore (VMware).”

Overview Monitoring Asset Notes Settings Reports					
Status Associations Service Templates					
<div> ADD DELETE CREATE SERVICE TEMPLATE SERVICE MONITORING </div>					
Service	Status	Transition	Last Scan Time	Probe/Agent	
<input type="checkbox"/> Connectivity (VMware)	✓	2017-Oct-13 03:17	2017-Oct-25 06:34	ICT101-VEEAM - Windows	
<input type="checkbox"/> Connectivity	✓	2017-Oct-13 03:16	2017-Oct-25 06:31	ICT101-VEEAM - Windows	
<input type="checkbox"/> CPU (VMware)	✓	2017-Oct-21 05:45	2017-Oct-25 06:33	ICT101-VEEAM - Windows	
<input type="checkbox"/> Datastore (VMware) - FX2-ESX01-LOCAL	✓	2017-Oct-25 05:30	2017-Oct-25 06:30	ICT101-VEEAM - Windows	
<input type="checkbox"/> Datastore (VMware) - FX2-RAID10-VOL1	!	2017-Oct-20 10:00	2017-Oct-25 06:32	ICT101-VEEAM - Windows	
<input type="checkbox"/> Datastore (VMware) - FX2-RAID10-VOL2	✓	2017-Oct-16 17:34	2017-Oct-25 06:31	ICT101-VEEAM - Windows	
<input type="checkbox"/> Datastore (VMware) - FX2-RAID10-VOL3	✓	2017-Oct-25 04:30	2017-Oct-25 06:30	ICT101-VEEAM - Windows	
<input type="checkbox"/> Datastore (VMware) - FX2-RAID10-VOL4	✓	2017-Oct-25 06:01	2017-Oct-25 06:30	ICT101-VEEAM - Windows	
<input type="checkbox"/> Datastore (VMware) - FX2-RAID10-VOL5	✓	2017-Oct-24 18:53	2017-Oct-25 06:31	ICT101-VEEAM - Windows	
<input type="checkbox"/> Fan Status (VMware) - Fan1A	✓	2017-Oct-23 11:34	2017-Oct-25 06:34	ICT101-VEEAM - Windows	
<input type="checkbox"/> Fan Status (VMware) - Fan1B	✓	2017-Oct-24 23:03	2017-Oct-25 06:34	ICT101-VEEAM - Windows	

Fig. 36 LUN (Virtual Disks) Free Space

Windows Services (Start/Stop/Disabled)

Select the “**Monitoring**” tab and Click on “**Windows Service – (service name).**”

Overview Tools Monitoring Asset Notes Settings Reports					
Status Associations Service Templates					
ADD DELETE CREATE SERVICE TEMPLATE SERVICE MONITORING					
Service	Status	Transition	Last Scan Time	Probe/Agent	
Windows Firewall Status	✓	2017-Oct-13 03:19	2017-Oct-25 01:19	Local Agent	
Windows Service - EBI Server Daemon	✓	2017-Oct-13 03:19	2017-Oct-25 01:25	Local Agent	
Windows Service - EBI Server Database	✓	2017-Oct-13 03:19	2017-Oct-25 01:25	Local Agent	
Windows Service - EBI Server Desktop	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	
Windows Service - EBI Server Operator Management	✓	2017-Oct-13 03:19	2017-Oct-25 01:25	Local Agent	
Windows Service - EBI Server Replication	✓	2017-Oct-13 03:19	2017-Oct-25 01:25	Local Agent	
Windows Service - EBI Server Service Framework	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	
Windows Service - EBI Server System	✓	2017-Oct-13 03:19	2017-Oct-25 01:25	Local Agent	
Windows Service - IIS Admin Service	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	
Windows Service - SQL Server (MSSQLSERVER)	✓	2017-Oct-13 03:19	2017-Oct-25 01:25	Local Agent	
Windows Service - SQL Server Agent (MSSQLSERVER)	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	
Windows Service - SQL Server Analysis Services (MSSQLSERVER)	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	
Windows Service - SQL Server Reporting Services (MSSQLSERVER)	✓	2017-Oct-13 03:19	2017-Oct-25 01:25	Local Agent	
Windows Service - World Wide Web Publishing Service	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	

REFRESH NOW ON Refresh in: --

Fig. 37 Windows Services

Windows Firewall Status (Servers & Workstations)

Select the “**Monitoring**” tab and Click on “**Windows Firewall Status**”.

Overview Tools Monitoring Asset Notes Settings Reports					
Status Associations Service Templates					
ADD DELETE CREATE SERVICE TEMPLATE SERVICE MONITORING					
Service	Status	Transition	Last Scan Time	Probe/Agent	
SQL Last Backup Datetime - MSSQLSERVER\MSS	✓	2017-Oct-13 03:29	2017-Oct-25 01:28	Local Agent	
SQL Last Backup Datetime - MSSQLSERVER\rs	✓	2017-Oct-13 03:29	2017-Oct-25 01:28	Local Agent	
SQL Last Backup Datetime - MSSQLSERVER\hwreports	✓	2017-Oct-13 03:29	2017-Oct-25 01:28	Local Agent	
SQL Last Backup Datetime - MSSQLSERVER\hwsystem	✓	2017-Oct-13 03:29	2017-Oct-25 01:28	Local Agent	
SQL Last Backup Datetime - MSSQLSERVER\irldb	✓	2017-Oct-13 03:29	2017-Oct-25 01:28	Local Agent	
Windows Event Log	✓	2017-Oct-25 00:04	2017-Oct-25 01:03	Local Agent	
Windows Event Log - McAfee 8.5i	✓	2017-Jul-24 04:30	2017-Oct-25 01:03	Local Agent	
Windows Firewall Status	✓	2017-Oct-13 03:19	2017-Oct-25 01:19	Local Agent	
Windows Service - EBI Server Daemon	✓	2017-Oct-13 03:19	2017-Oct-25 01:30	Local Agent	
Windows Service - EBI Server Database	✓	2017-Oct-13 03:19	2017-Oct-25 01:30	Local Agent	
Windows Service - EBI Server Desktop	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	
Windows Service - EBI Server Operator Management	✓	2017-Oct-13 03:19	2017-Oct-25 01:30	Local Agent	
Windows Service - EBI Server Replication	✓	2017-Oct-13 03:19	2017-Oct-25 01:30	Local Agent	
Windows Service - EBI Server Service Framework	✓	2017-Oct-13 03:19	2017-Oct-25 01:28	Local Agent	

REFRESH NOW ON Refresh in: 10 minutes

Fig. 38 Windows Firewall Status

Windows Updates / Patch Status

Select the “Monitoring” Tab and Click on “Patch Status”.

Status Associations Service Templates					
ADD DELETE CREATE SERVICE TEMPLATE SERVICE MONITORING					
Service	Status	Transition	Last Scan Time	Probe/Agent	
<input type="checkbox"/> CPU	✓	2017-Oct-12 02:20	2017-Oct-25 06:12	Local Agent	
<input type="checkbox"/> Disk - C:	⚠	2017-Oct-12 02:20	2017-Oct-25 06:09	Local Agent	
<input type="checkbox"/> Disk - D:	✓	2017-Oct-12 02:20	2017-Oct-25 06:09	Local Agent	
<input type="checkbox"/> Disk - F:	✓	2017-Oct-12 02:20	2017-Oct-25 06:09	Local Agent	
<input type="checkbox"/> Disk I/O - _Total	✓	2017-Oct-24 04:42	2017-Oct-25 06:16	Local Agent	
<input type="checkbox"/> Memory	✓	2017-Oct-22 15:21	2017-Oct-25 06:12	Local Agent	
<input type="checkbox"/> Patch Status	⚠	2017-Oct-13 01:26	2017-Oct-24 16:34	Local Agent	
<input type="checkbox"/> Reboot Required	!	2017-Oct-13 05:45	2017-Oct-25 06:15	Local Agent	
<input type="checkbox"/> SQL Database Growth Check - acsdld	✓	2017-Oct-12 03:00	2017-Oct-25 06:00	Local Agent	

Fig. 39 Windows Updates

Monitor HRM agent status

Select the “Monitoring” Tab and Click on “Agent Status”.

Overview	Tools	Monitoring	Asset	Notes	Settings	Reports
Status	Associations	Service Templates				
<div>ADDDELETECREATE SERVICE TEMPLATESERVICE MONITORING</div>						
<input type="checkbox"/> Service	▲▼	Status	▼	Transition		
<input type="checkbox"/> Agent Status		✓		2017-Nov-09 12:43		
<input type="checkbox"/> AV Status		!		2017-Nov-09 09:46		
<input type="checkbox"/> Clock Drift		⚙		2017-Nov-09 09:52		
<input type="checkbox"/> CPU		✓		2017-Nov-07 19:07		
<input type="checkbox"/> Disk - C:		✓		2017-Nov-09 09:46		
<input type="checkbox"/> Disk I/O - _Total		✓		2017-Nov-09 09:46		

Fig. 40 HRM agent Status

Thresholds / Tuning for Monitoring Services

Threshold tuning is useful to configure the thresholds of service to show the results in the All Services tab.

On the device dashboard, go to “**Active issues**” to find the current issue with the C drive. Click “**Disk – C:**” to see the details.

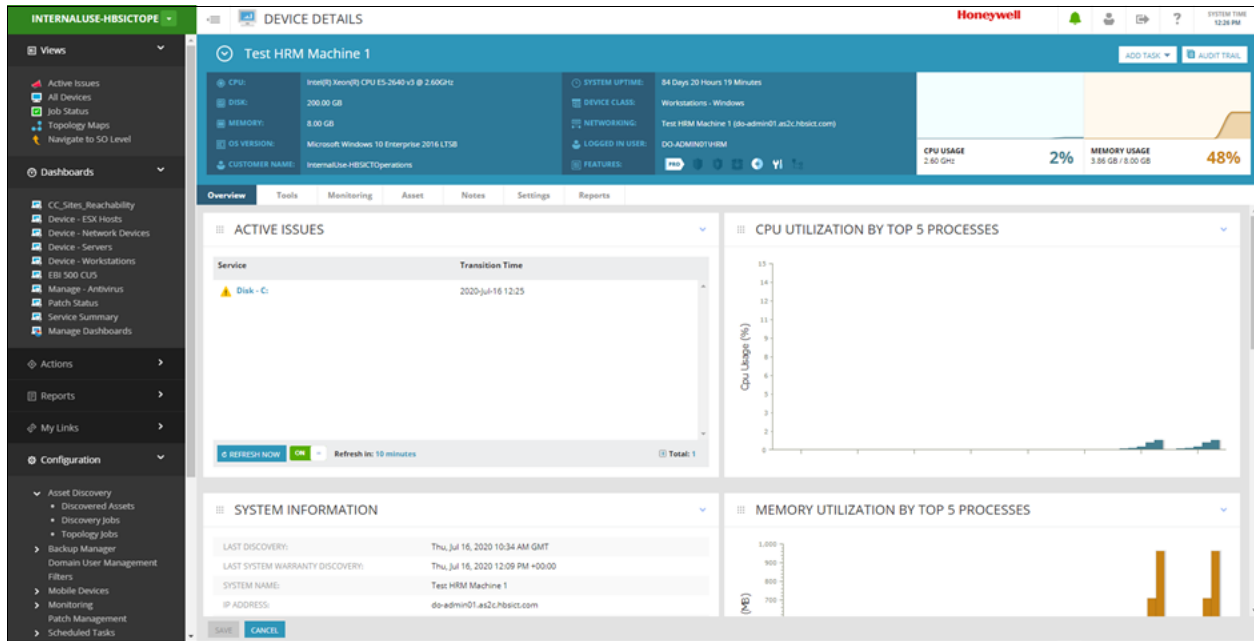


Fig. 41 Active Issues

This will load the service status page, where you will be able to see the service status details and configured thresholds.

You can see that the total capacity of the C drive is 200GB. 178 GB is currently being used, and free disk space is around 22 GB.

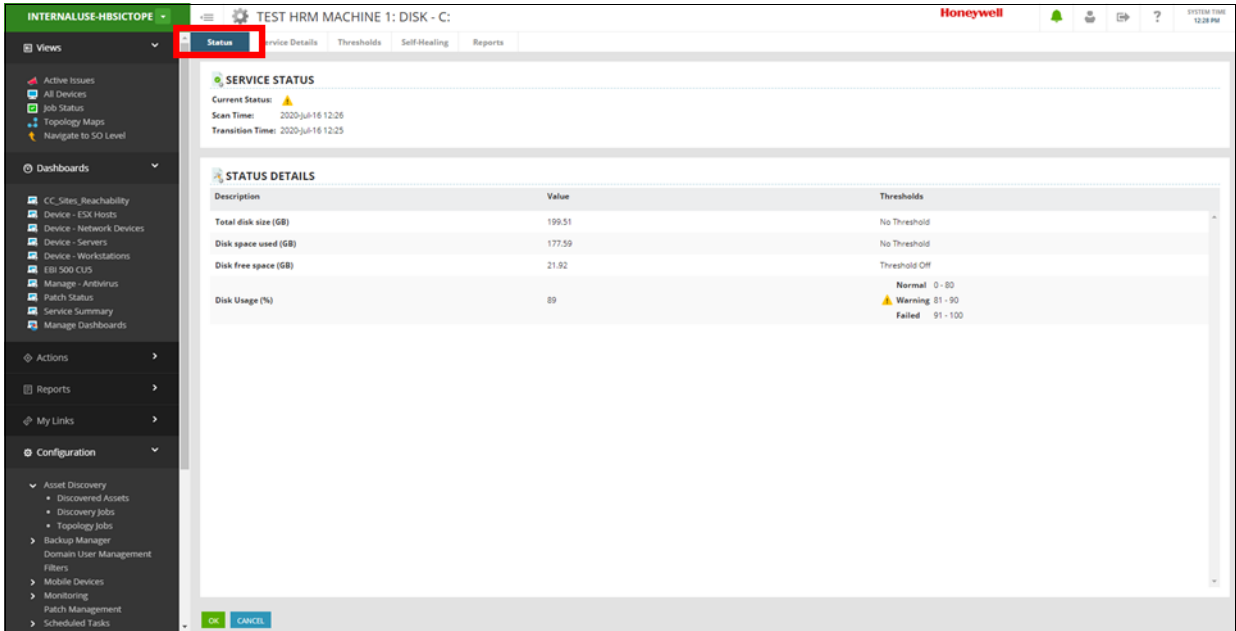


Fig. 42 Status Details

The “**Thresholds**” tab in HRM defines the threshold range that is, NORMAL, WARNING, and FAILED and triggers alerts/notifications that are sent to technicians via emails.

As the current thresholds are configured to report a warning status when disk space is greater than 61% utilization, it will report a warning status. If the disk exceeds 86% capacity, you will receive a failed status in the dashboard.

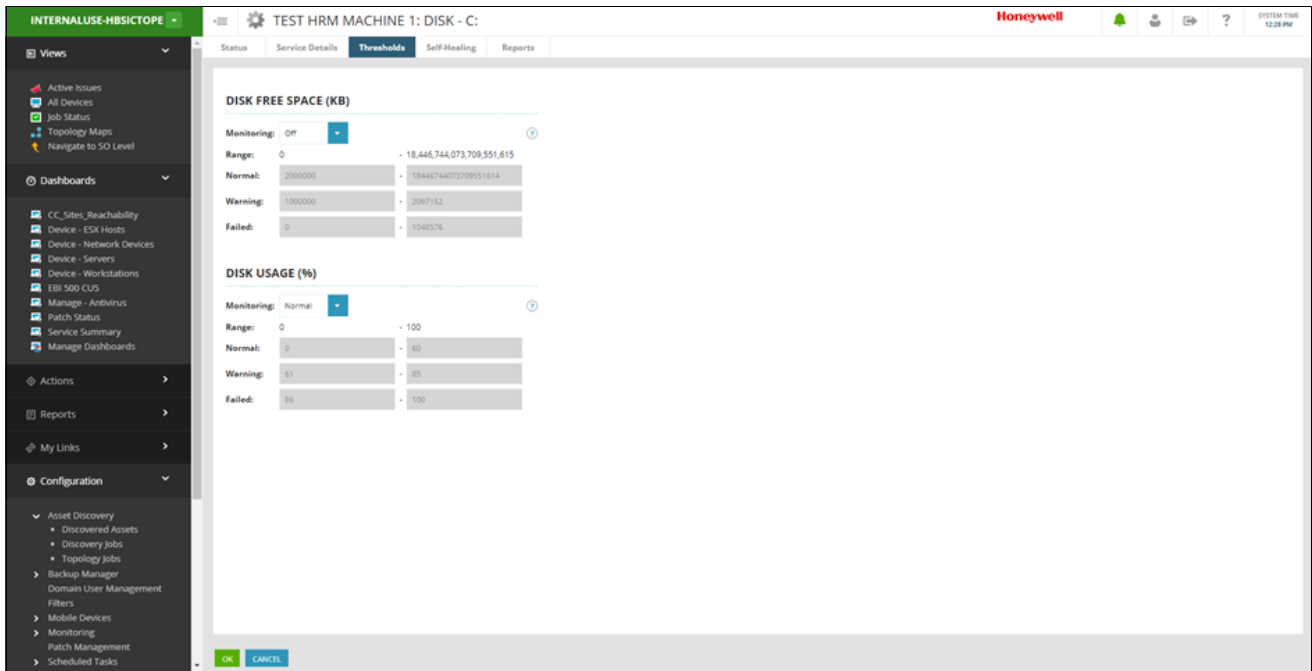


Fig. 43 Disk Space

To configure custom thresholds, change the “**Monitoring**” options from “**Normal**” to “**Custom**” using this option. We can also turn off monitoring for this device by selecting OFF. However this is not recommended unless the equipment is out of service or being maintained.

Changing the thresholds, in this case, will apply the following monitoring thresholds:

- Drive size between 0-85% utilization is within the normal range and will show in green color.
- Drive size between 86%-95% utilization is within warning range and will show in yellow color.
- Drive size above 96% utilization is within the failed range and will show in red color.

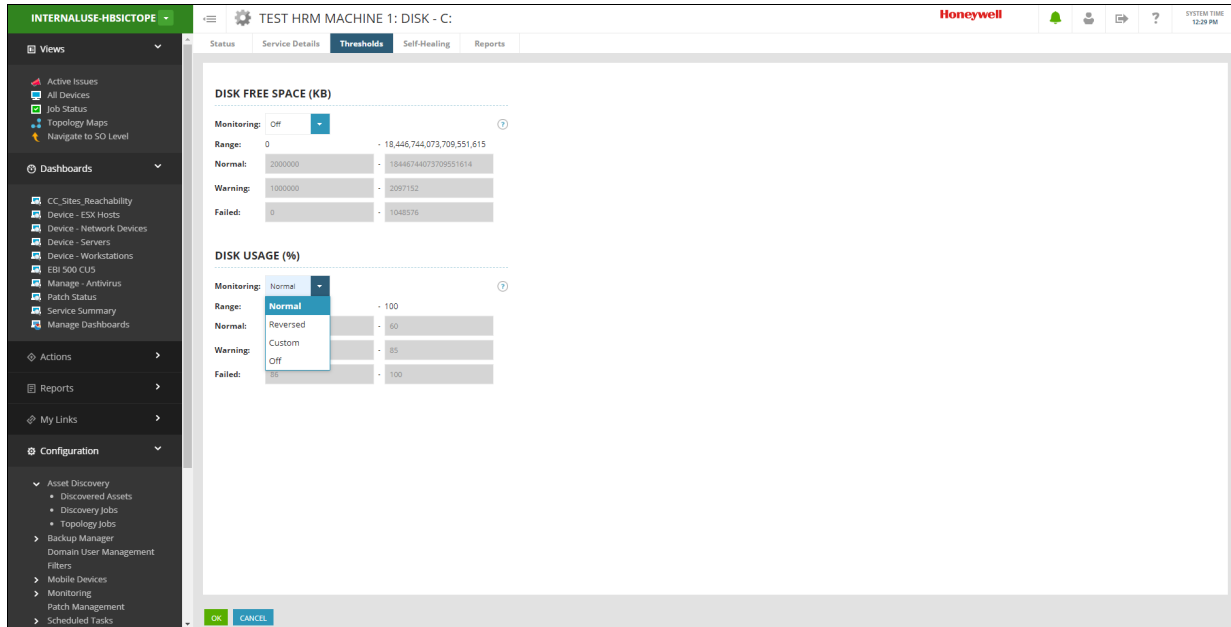


Fig. 44 Acronis backup with WMI

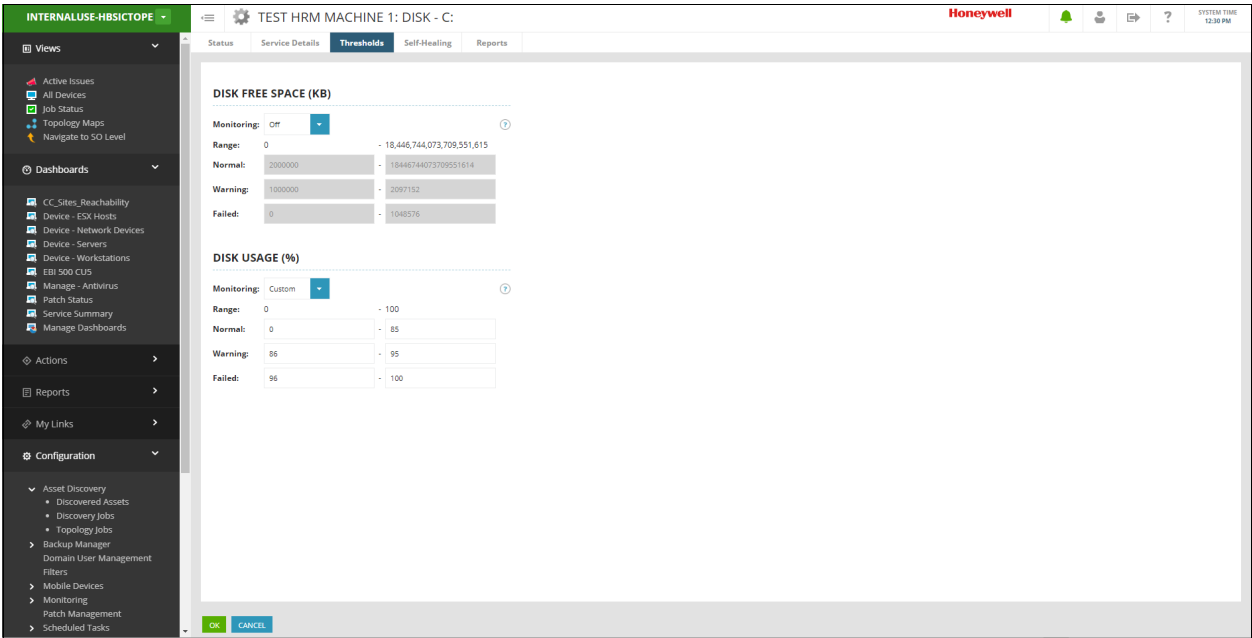


Fig. 45 Disk Usage

The material in this document is for information purposes only. The content and the product described are subject to change without notice. Honeywell makes no representations or warranties with respect to this document. In no event shall Honeywell be liable for technical or editorial omissions or mistakes in this document, nor shall it be liable for any damages, direct or incidental, arising out of or related to the use of this document. No part of this document may be reproduced in any form or by any means without prior written permission from Honeywell.

Honeywell Building Technologies

715 Peachtree St NE
Atlanta, Georgia 30308
customer.honeywell.com
buildings.honeywell.com

® U.S. Registered Trademark
©2022 Honeywell International Inc.
31-00541-01I Rev. 04-22

