



COMODO
Creating Trust Online®

COMODO
RMM

Comodo One

Software Version 3.9

Remote Monitoring and Management Administrator Guide

Guide Version 6.1.113018

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Remote Monitoring and Management Module.....	3
1.1 Quick Start Guide.....	6
1.2 System Requirements.....	25
2 Install RMM Administrative Console	26
2.1 Login to the RMM Administrative Console	31
3 The RMM Administrative Console.....	32
4 The Devices Interface	35
4.1 Apply Policies.....	36
4.2 Run Procedures.....	38
5 The Sessions Interface	40
5.1 Support Sessions Interface - An Overview.....	40
5.2 Handle Support Sessions.....	41
5.2.1 Run Procedures from a Support Session.....	43
5.2.2 Use RMM Tools.....	44
5.2.2.1 Access Endpoints through Remote Desktop Connection.....	46
5.2.2.2 Manage Autoruns.....	46
5.2.2.3 System Cleaner.....	50
5.2.2.4 Power Management.....	53
5.2.2.5 Manage Internet Browser Add-ons.....	54
5.2.2.6 Active Connections Manager.....	57
5.2.2.7 Restore a Client System	58
5.2.2.8 Hardware Monitor Tool.....	59
5.2.2.9 Access Command Prompt Window of Client System.....	60
5.2.2.10 Manage Currently Running Processes.....	61
5.2.2.11 Obtain System Inventory Information.....	63
5.2.2.12 Transfer Files From / To Client System	65
6 The Jobs Interface	67
6.1 Manage Jobs.....	68
6.2 Execute Jobs on Endpoints.....	74
7 The Procedures Interface	75
7.1 Manage Procedures.....	76
7.2 Run Procedures on Endpoints.....	79
8 The Policies Interface	81
8.1 Manage Policies.....	82
Appendix - Issue Codes for Monitors	92
About Comodo Security Solutions.....	94

1 Introduction to Remote Monitoring and Management Module

Comodo **Remote Monitoring and Management** (CRMM) grants Managed Service Providers complete visibility and control over the systems they manage. It combines comprehensive endpoint monitoring and alerting with ultra-fast remote desktop sharing, professional services automation (PSA), powerful policy and job creation interfaces, automatic support ticket generation and custom scripting for automated break-fixing. RMM is the single-pane-of-glass that helps MSPs and enterprises to improve the efficiency of their workflows and take the quality of service they provide to customers to the next level.

The screenshot shows the RMM Administration Console interface. At the top, it displays 'RMM Administration Console 6.1.397172.522' and a user profile for 'coyoteewile@yahoo.com'. Below the header, there are navigation tabs for 'Devices', 'All(10)', 'Offline(7)', 'Not Compliant(2)', and 'In Session(0)'. A search bar is present with the placeholder 'Enter keyword...'. The main area is a table with columns: Company/Site/Hostname, Operating system, Device type, Logged user, Internal IP, External IP, Compliant, Applied policy name, Description, and Action. The table is organized into a tree view with folders for 'ABC TV Services', 'Chennai IT Services', 'Coyote', 'Deer Company', and 'Dithers Construction Company'. Under 'Coyote', there is a 'Default Site' folder containing four devices: ADMIN-PC, ALICE-PC, BOB-PC, and BOB-PC. Under 'Deer Company', there is a 'Default Site' folder containing three devices: DESKTOP-8B38R40, DESKTOP-8B38R40, and DESKTOP-8B38R40. The bottom of the console has three buttons: 'Refresh', 'Apply Policy', and 'Run Procedure'.

Company/Site/Hostname	Operating system	Device type	Logged user	Internal IP	External IP	Compliant	Applied policy name	Description	Action
ABC TV Services									
Chennai IT Services									
Coyote									
Default Site									
ADMIN-PC	Windows Vista (TM) Business - x86	Workstation		10.108.51.130	69.4.80.244	No	Workstation monit...		Unavailable
ALICE-PC	Windows Vista (TM) Business - x86	Workstation	ALICE-PC\admin	10.108.51.80	182.74.23.22	N/A	N/A		Unavailable
BOB-PC	Windows Vista (TM) Business - x86	Workstation	BOB-PC\admin	10.108.51.120	182.74.23.22	N/A	N/A		Unavailable
BOB-PC	Windows Vista (TM) Business - x86	Workstation	BOB-PC\admin	10.108.51.119	182.74.23.22	No	Workstation monit...		Unavailable
Deer Company									
Default Site									
DESKTOP-8B38R40	Windows 10 Pro - x64	Workstation	DESKTOP-8B38R40\Bob S...	10.108.51.172	182.74.23.22	N/A	N/A		Unavailable
DESKTOP-8B38R40	Windows 10 Pro - x64	Workstation		10.108.51.172	182.74.23.22	N/A	N/A		Unavailable
DESKTOP-8B38R40	Windows 10 Pro - x64	Workstation	DESKTOP-8B38R40\Bob S...	10.0.2.15	182.74.23.22	N/A	N/A		Takeover
Dithers Construction Company									

Comodo RMM setup and management involves two components - the admin console and the endpoint agent.

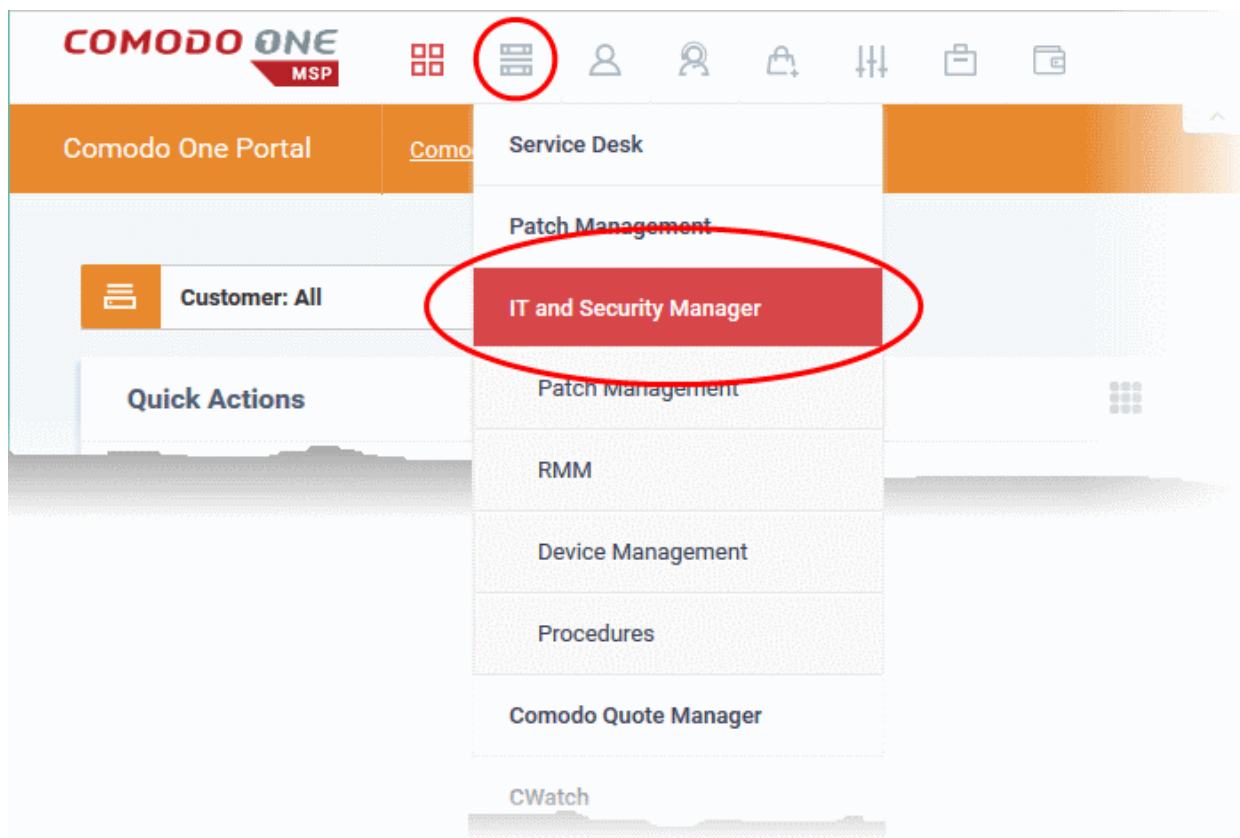
- The admin console is the chief management software and is used to monitor endpoints, define policies and configure/respond to endpoint service desk tickets. The console should be installed on a local workstation or server and can be downloaded from the ITSM.
- The endpoint agent is a small piece of software installed on managed endpoints for communication with the admin console. The agent is responsible for forwarding the monitored data from the endpoints to the console and to apply policies/running procedures at the endpoints. The endpoint agent is automatically installed on each endpoint upon its enrollment to ITSM, so that it is automatically added to the RMM console for management. For more details on adding Windows endpoints to ITSM, refer to the online help page at <https://help.comodo.com/topic-399-1-786-10126-Enrolling-User-Devices-for-Management.html>.

Also, you can manually install the agent at an endpoint if needed, from the ITSM console. For details, refer to the online help page at <https://help.comodo.com/topic-399-1-786-10139-Remotely-Installing-Packages-onto-Windows-Devices.html>.

To Launch the download Screen and Install screen:

You can download the RMM console setup file from the ITSM console interface.

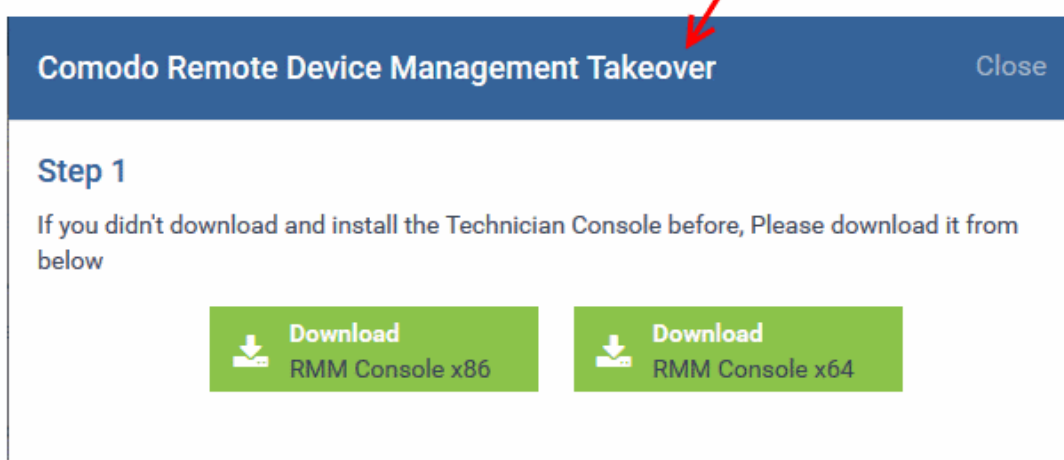
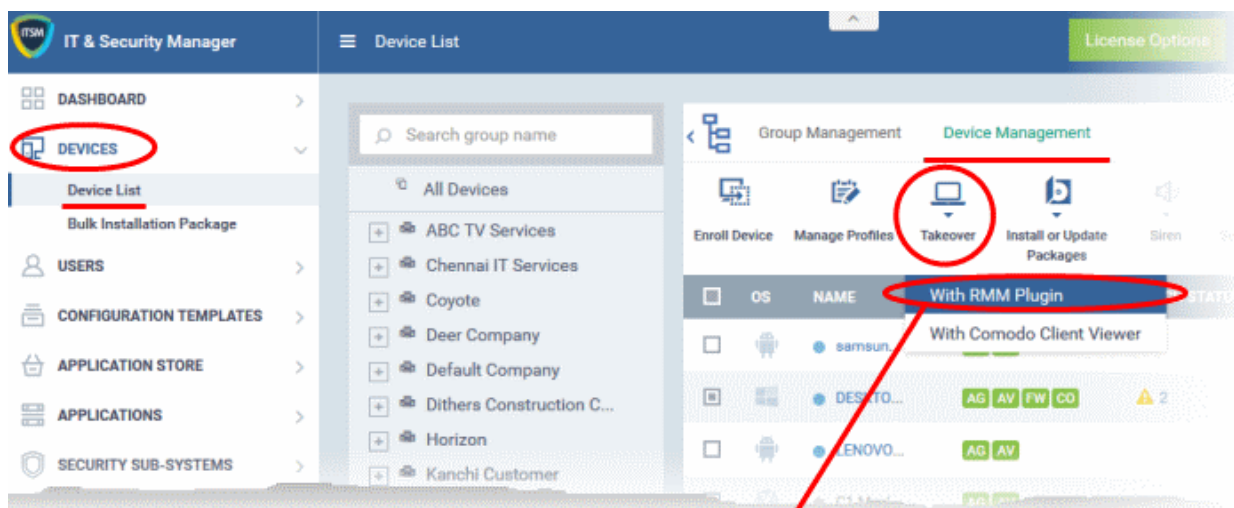
- Log into the Comodo One at <https://one.comodo.com/app/login> with your user name and password
- Click the 'Licensed Applications' icon from the top and select 'IT and Security Manager', to open the ITSM console.



- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

A list of all devices enrolled to ITSM will be displayed by default.

- Choose a 'Windows' device, click 'Takeover' from the top then 'With RMM Plugin'



- Proceed to download by choosing the type of Operating system.

RMM Features and Benefits

- Up-to-the-second inventory of all managed devices in a single console
- Easily configure endpoint security policies using the intuitive policies interface
- Automatically create a service desk ticket if an endpoint falls out of compliance with its policy
- Panoramic, real time information allows you to make better, more informed decisions
- Multiple plug-ins allow you to observe running processes, services, active connections, auto-run applications, browser extensions, system restore points and more
- Ability to run system and registry clean operations with a single click
- Easily transfer files between your computer and endpoint machines
- Built-in RDP software allows you to access client machines directly from the management console
- Run commands in multiple interpreter languages
- Craft and execute procedures which can be used and re-used for common endpoint tasks
- Advanced Procedure Wizard allows you to create and run commands in sequential order
- Remotely restart and shutdown endpoints with the integrated power manager
- Agent runs as a service, the endpoint need not be logged in
- Patent pending rescue option allows administrators to restart endpoints in rescue mode

Guide Structure

This guide is intended to take you through the configuration and use of Comodo RMM and is broken down into the following main sections. The guide can be navigated using the bookmark links on the left.

- **Introduction to Remote Monitoring and Management Module**
 - **Quick Start Guide**
 - **System Requirements**
- **Installing RMM Administrative Console**
 - **Logging-in to the RMM Administrative Console**
- **The RMM Administrative Console**
- **The Devices Interface**
 - **Applying Policies**
 - **Running Procedures**
- **The Sessions Interface**
 - **Support Sessions Interface - An Overview**
 - **Handling Support Sessions**
- **The Jobs Interface**
 - **Managing Jobs**
 - **Executing Jobs on Endpoints**
- **The Procedures Interface**
 - **Managing Procedures**
 - **Running Procedures on Endpoints**
- **The Policies Interface**
 - **Managing Policies**
- **Appendix - Issue Codes for Monitors**

1.1 Quick Start Guide

This tutorial briefly explains how an admin can setup Comodo Remote Monitoring and Management (RMM).

Note - To use Comodo RMM, you must have an active Comodo One Account (<https://one.comodo.com>) and have added devices and users to the Comodo IT and Security Manager (ITSM) module. Once you have added devices to ITSM, you will be able to download the RMM console and push the RMM client to managed endpoints.

For more details on enrolling users and adding devices in ITSM, see <https://help.comodo.com/topic-214-1-771-9485-Creating-New-User-Accounts.html> and <https://help.comodo.com/topic-214-1-771-9486-Enrolling-User-Devices-for-Management.html>.

Basic Setup:

- i. Add devices, endpoints and users to Comodo IT and Security Manager as described above.
- ii. Enable the RMM extension in Comodo IT and Security Manager ('Settings' > 'Extensions' > set RMM switch to 'ON')
- iii. Install the RMM Admin console. The console is used to monitor endpoints, define policies and configure endpoint service desk tickets, and should be installed on a local workstation or server. To download the console, open ITSM > 'Devices' > 'Device List' > 'Device Management'. Select any endpoint from the list and click 'Takeover'. This will allow you to download the console setup files to your local machine.
- iv. Install the RMM client software on target endpoints. The agent facilitates communication between endpoints and the admin console. The agent is automatically installed on managed endpoints once the RMM

extension is enabled in ITSM (step ii, above). Should the need arise, you can also install the agent manually by clicking Devices > Device List' > 'Device Management', selecting your target endpoints then clicking 'Install or Update Packages' > 'Install Additional Comodo Packages' > 'Install RMM Plug-in Agent'.

Basic Concepts:

- **Action** - A task which can be run on target endpoints. Examples include install an application, reboot an endpoint, create a system restore point, run a registry cleaning task and more. Actions are added to procedures.
- **Procedure** - A collection of one or more actions. Procedures can be directly run on target endpoints or can be added to a 'Job'
- **Job** - A collection of one or more procedures. Multiple procedures can be added to a job to create sophisticated tasks.
- **Policy** - Policies are designed to monitor target endpoints and when issues are identified, service desk tickets are automatically generated and sent to the administrator if certain conditions are met. You can then investigate the service desk ticket created and run a procedure/job on the endpoint if required.

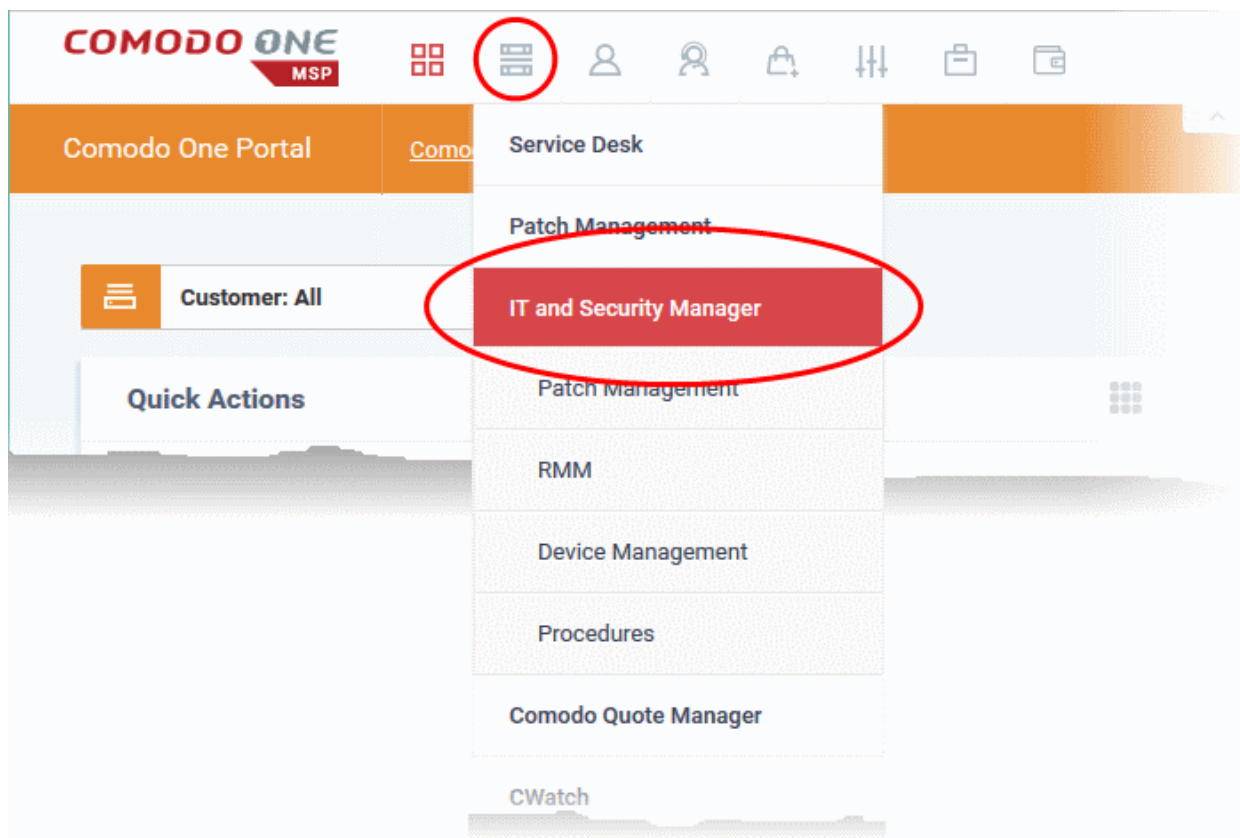
The guide will take you through the basic setup and usage of Comodo RMM. Click any link to go straight to the section you need help with.

- **Step 1 - Login to Comodo One and download the technician console**
- **Step 2 - Install Technician Console**
- **Step 3 - Login to Technician Console**
 - **Create procedures**
 - **Create and execute jobs**
 - **Create and apply monitoring policies**
 - **Handle support sessions**
 - **The Support Sessions Interface**
 - **Execute pre-defined actions on the endpoint**
 - **Access the Endpoint through Remote Desktop Connection**
 - **Run a procedure**

Step 1 - Login to your Comodo One Account and Download the Technician Console

You can download the RMM console setup file from the ITSM console interface.

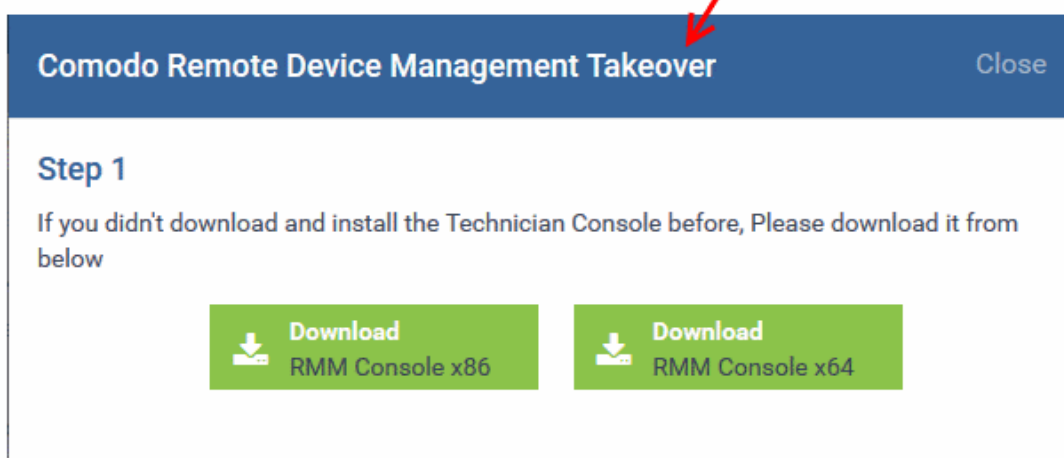
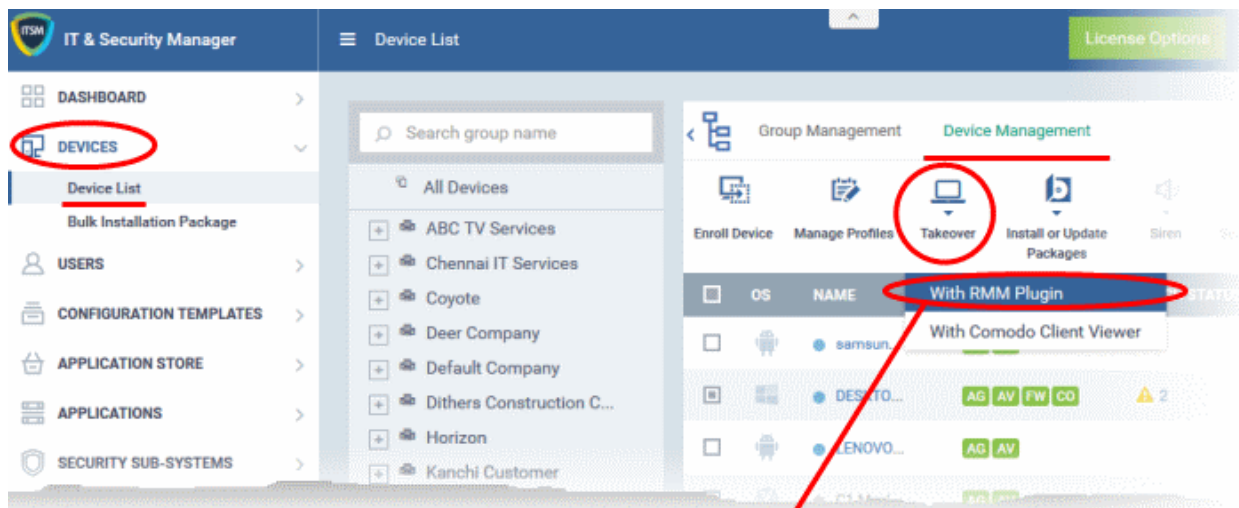
- Log into the Comodo One at <https://one.comodo.com/app/login> with your user name and password
- Click the 'Licensed Applications' icon from the top and select 'IT and Security Manager', to open the ITSM console.



- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

A list of all devices enrolled to ITSM will be displayed by default.

- Choose a 'Windows' device, click 'Takeover' from the top then 'With RMM Plugin'



The setup file is available for 32-bit and 64-bit versions of Windows.

- Choose the version appropriate to the system upon which you want to install the RMM console and click 'Download'.

Step 2 - Install the Technician Console

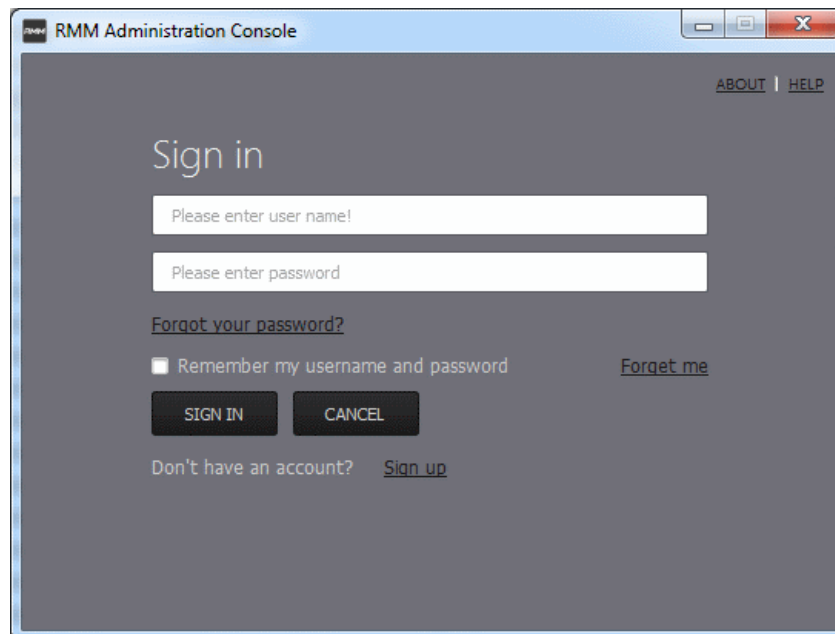
- Double click on the setup file to start the console installation wizard:



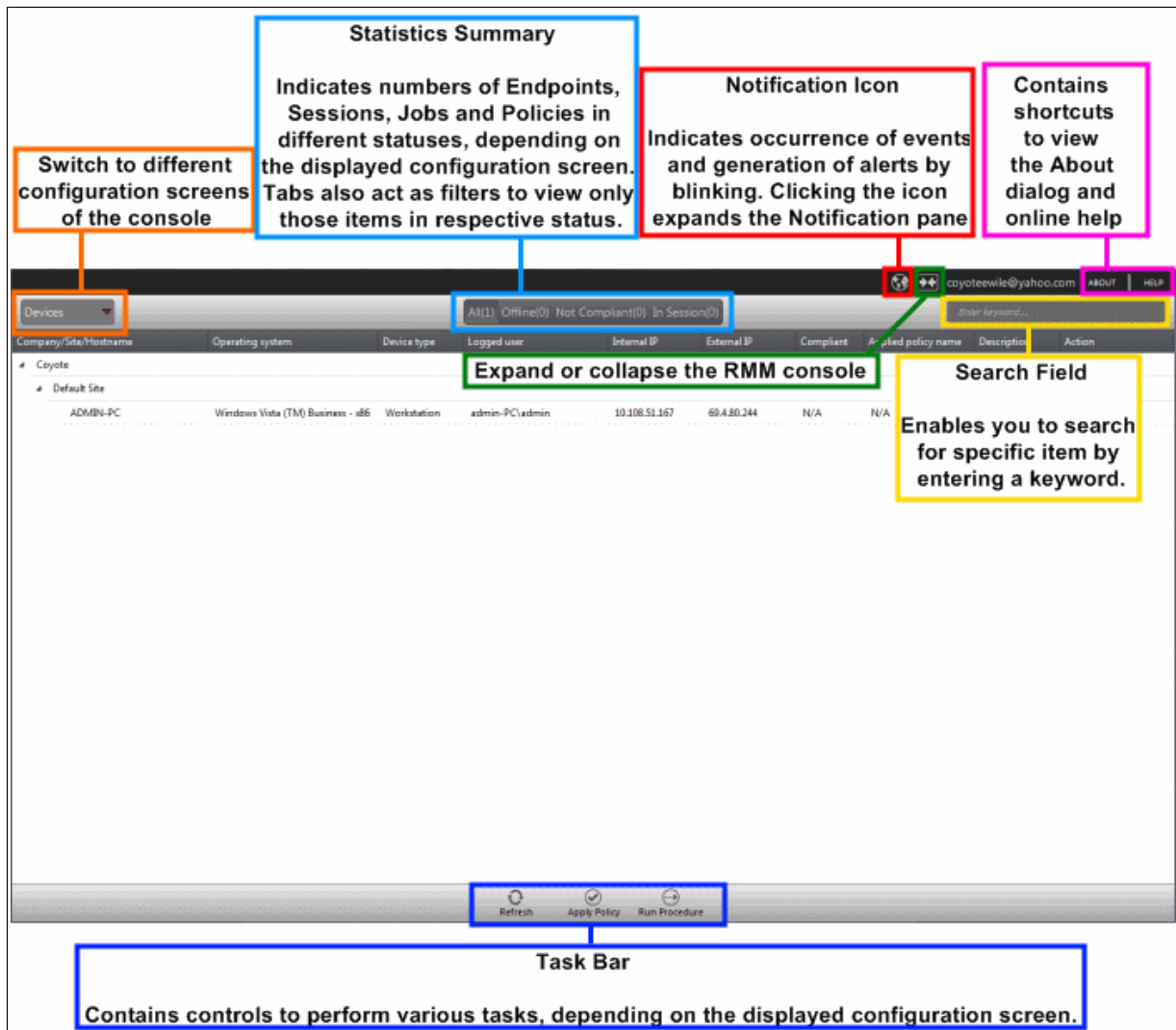
- Follow the wizard and complete the installation.

Step 3 - Login to Technician Console

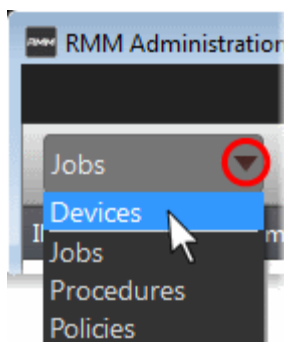
After installation, the console should automatically open at the login screen. Enter your Comodo One username (email address) and password in the respective text fields and click 'SIGN IN'.



You can open the console in future by clicking the RMM desktop shortcut or by clicking 'Start' > 'All Programs' > 'COMODO' > 'RMM Administration Console' > 'RMM Administration Console'.



The console will open.



The drop-down the top left enables you to switch between configuration interfaces:

- **Devices** - Displays enrolled endpoints. You can run procedures and apply policies to endpoints.
- **Jobs** - Lists jobs that are completed and in progress. You can create new jobs with a set of procedures and execute them on desired endpoints.
- **Procedures** - Lists all procedures available for deployment to endpoints. Procedures can be run directly on endpoints and/or can be used in jobs to be executed on selected endpoints.
- **Policies** - Displays active monitoring policies which have been deployed to endpoints. Service desk tickets are generated if a policy is violated. You can view all policies, create new policies and deploy policies to endpoints by clicking the 'Policy Manager' button at the bottom of the interface.

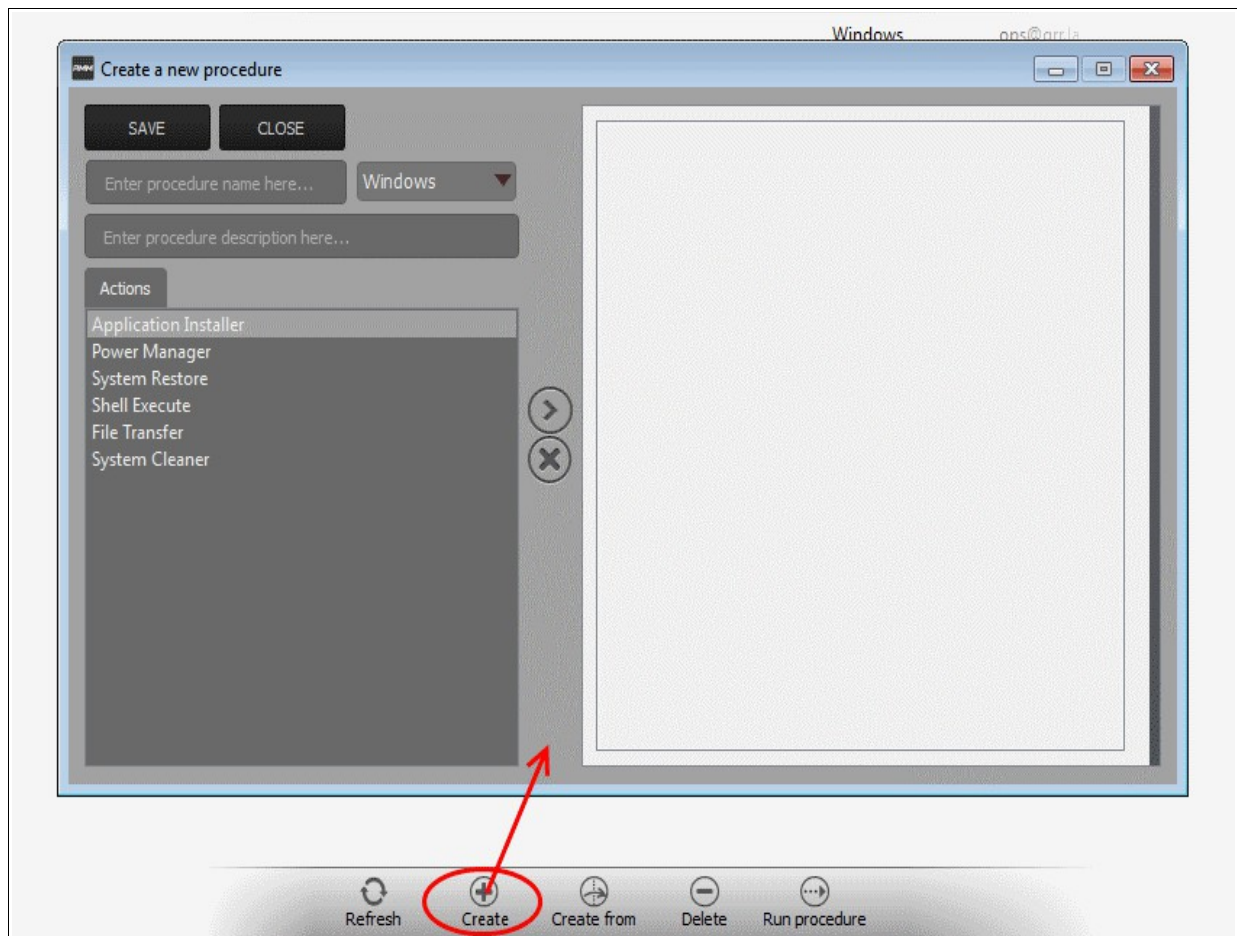
Create Procedures

A 'Procedure' is a sequence of one or more actions which is run on managed endpoints. Procedures can be run ad-hoc on any endpoint and multiple procedures can be added to an RMM 'Job'.

To open the procedures interface, choose 'Procedures' from the drop-down at top left. The interface will list any procedures that have already been created.

To create a new procedure

- Click the 'Create' button at the bottom of the interface:



In the new procedure dialog:

- Enter a name and a short description for your procedure and choose the operating system of the target endpoints
- Choose an action from the 'Action' list and click the right arrow to add it to your procedure.
- Next, you need to configure each action you add to your policy. The following table lists the default actions and associated parameters:

Action	Parameters Required
Application Installer	Choose one of the following install operations: <ul style="list-style-type: none"> • Application Install <ul style="list-style-type: none"> • Enter the following parameters: <ul style="list-style-type: none"> • Download URL of the application • Name of the setup file and any command line switches • Failsafe command for canceling the installation • Patch Management Install
Power Manager	Choose one of the following power control operations: <ul style="list-style-type: none"> • Restart • Restart in safe mode • Shutdown

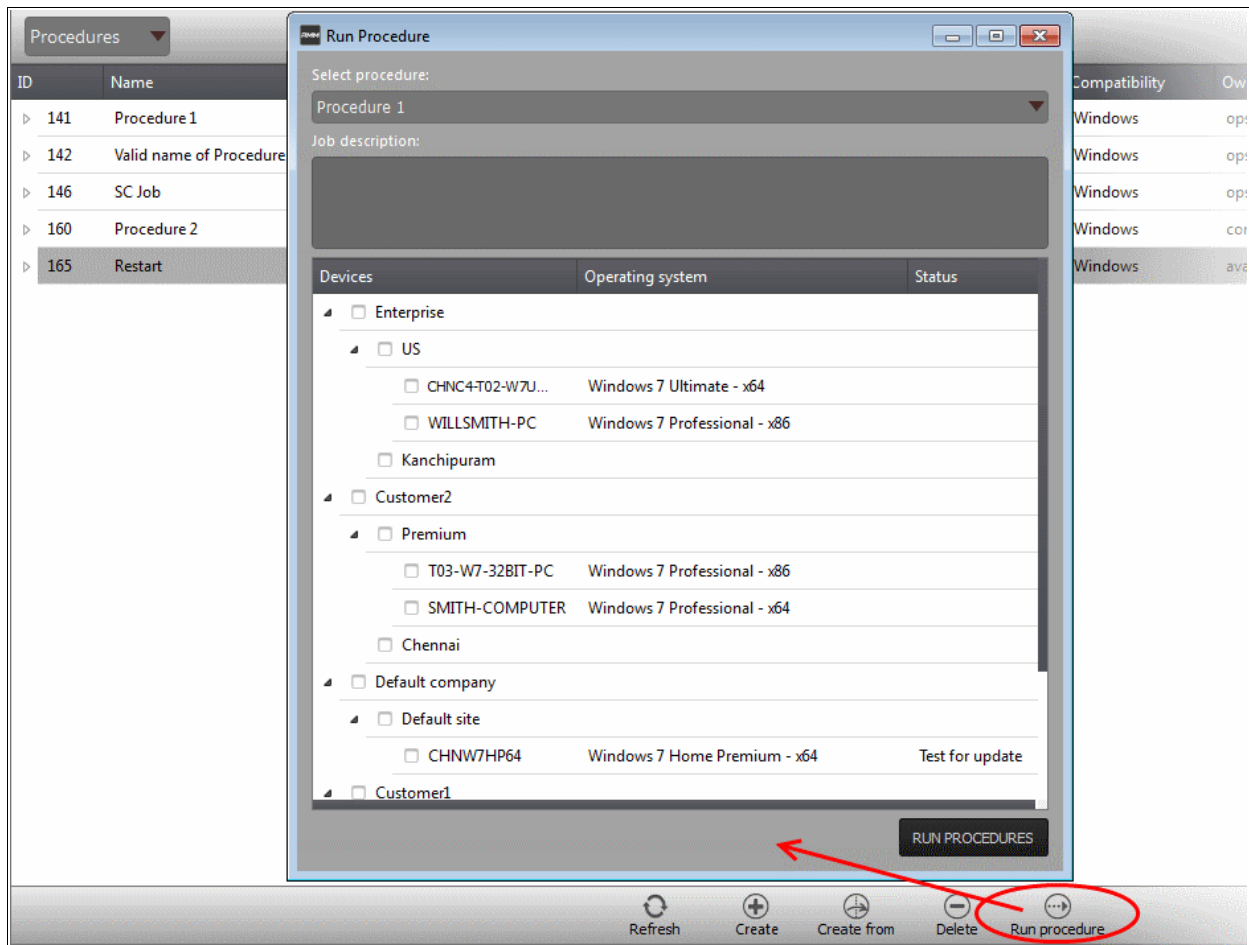
Action	Parameters Required
System Restore	<p>Choose whether to create a restore point or to restore the system to a previous state.</p> <ul style="list-style-type: none"> Enter the name of the restore point to be created or the name of the restore point, to which the system needs to be rolled back.
Shell Execute	<p>Run a particular file on a managed endpoint</p> <p>Basic</p> <ul style="list-style-type: none"> Enter the execution command for the process Enter the parameters to be passed to the process <p>Advanced</p> <ul style="list-style-type: none"> Enter the working directory for the process Choose the execution options: <ul style="list-style-type: none"> Wait for process to finish - Completes the process before termination Hide Window - Executes the process at the background
File Transfer	<p>Enter the path of the source file to be copied from the host computer at which the technician console is installed. The file will be copied to the folder c:\lps-temp\file-transfer at the endpoint.</p>
System Cleaner	<p>Execute one of the following system scanning and cleaning tasks:</p> <ul style="list-style-type: none"> Disk Cleaner Registry Cleaner

- Repeat the process to add more actions to the procedure. Actions will be executed in order from top-to-bottom.
- Click 'SAVE' to save your procedure.
- Your new 'Procedure' will be listed in the 'Procedures' interface. It will be available for inclusion in any job created for target endpoints. The procedure can also be run ad-hoc on any endpoint.
- Repeat the process to add more procedures as required.

Tip: You can create new procedures using an existing procedure as a template. To do so, select an existing procedure and click 'Create From' at the bottom of the interface. Next, edit procedure actions and parameters as required and click 'Save'.

To run a procedure

- Click 'Run Procedure' from the bottom of the interface.



- Choose the procedure you want to run from the drop-down at the top
- Choose the endpoints on which you want to run the procedure and click the 'RUN PROCEDURES' button

A new 'Job' will be automatically created when you directly run a procedure.

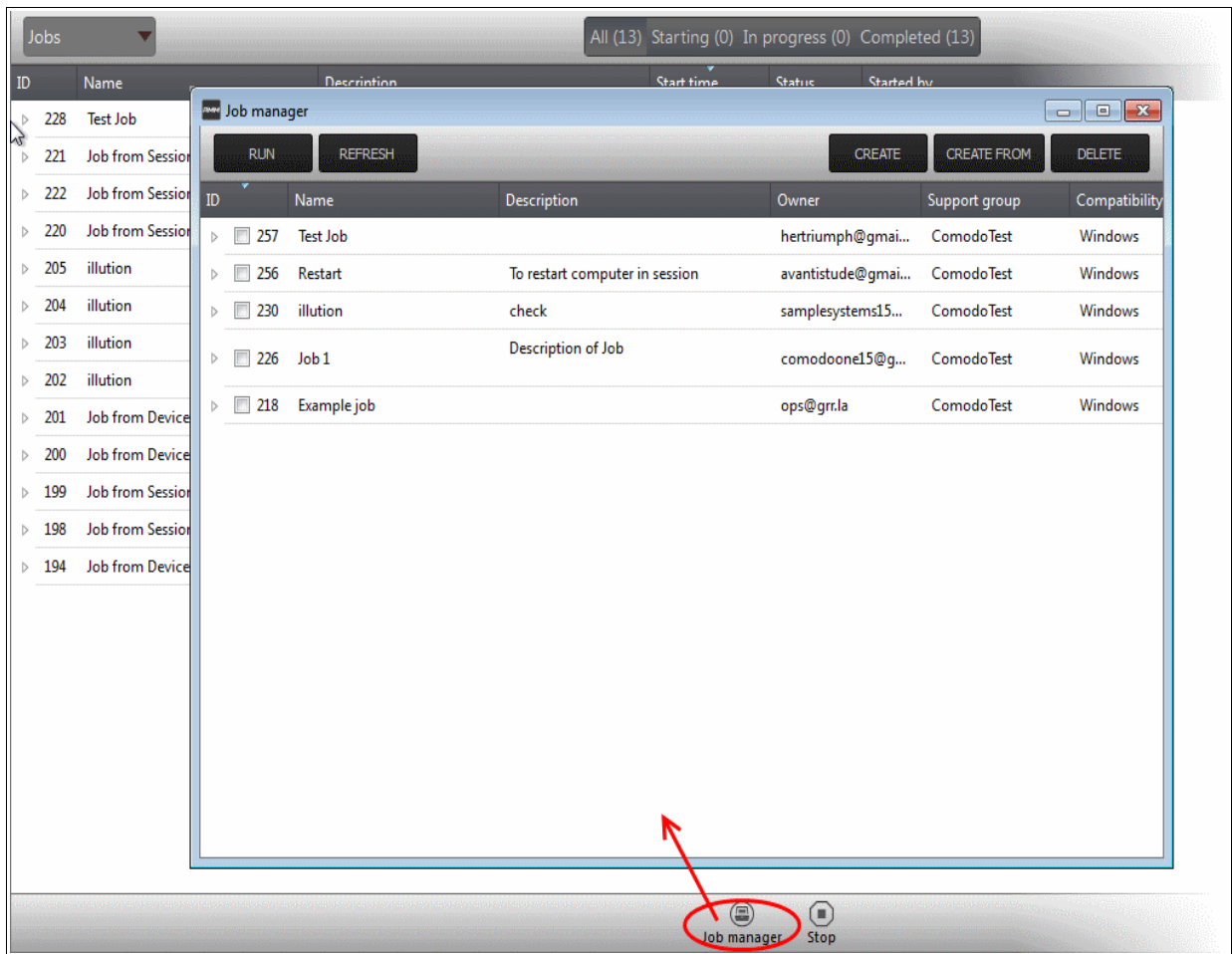
Create and Execute Jobs

A 'Job' is a collection of one or more RMM procedures. You can construct sophisticated jobs by adding multiple procedures to a single job.

- To open the Jobs interface, choose 'Jobs' from the drop-down at the top left. The 'Jobs' interface displays the jobs created and executed by all admins belonging to your MSP / organization

To create a new job

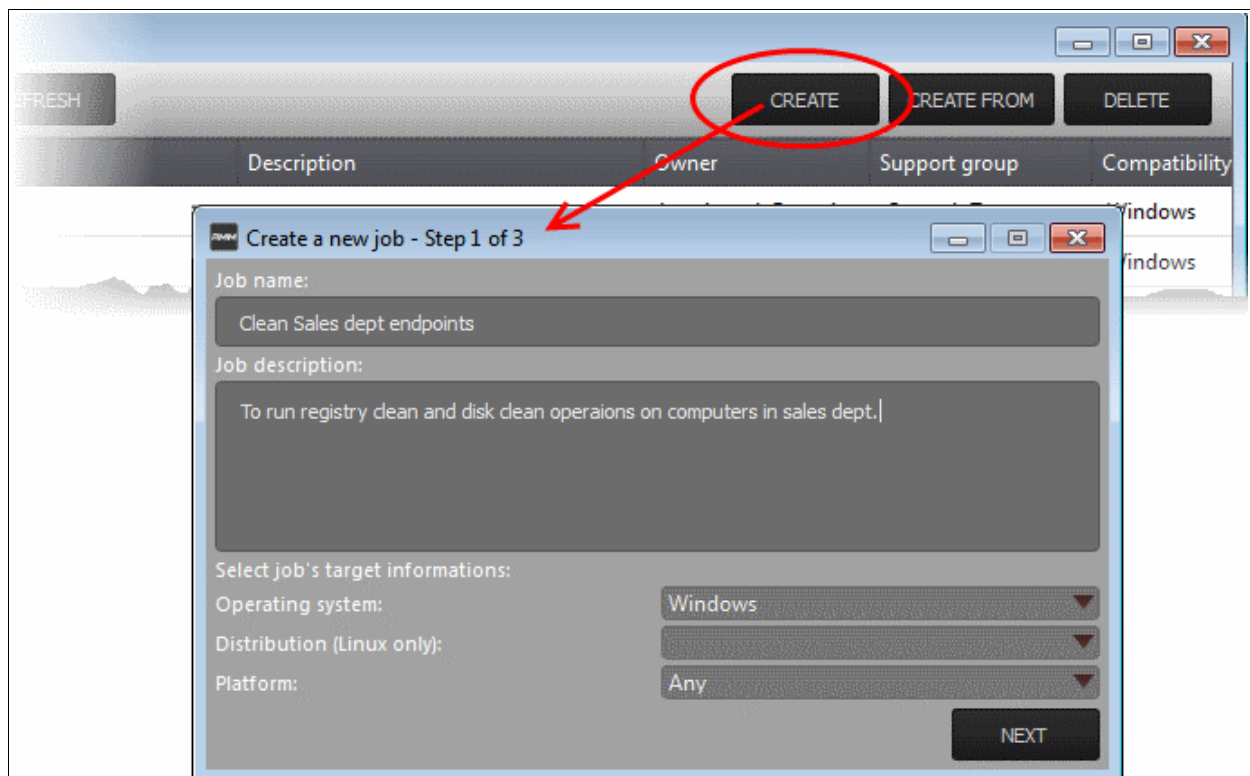
- Click 'Job Manager' from the bottom of the interface:



All jobs created so far will be displayed.

- Click 'CREATE' from the top of the 'Job Manager' dialog.

The job creation wizard will start.

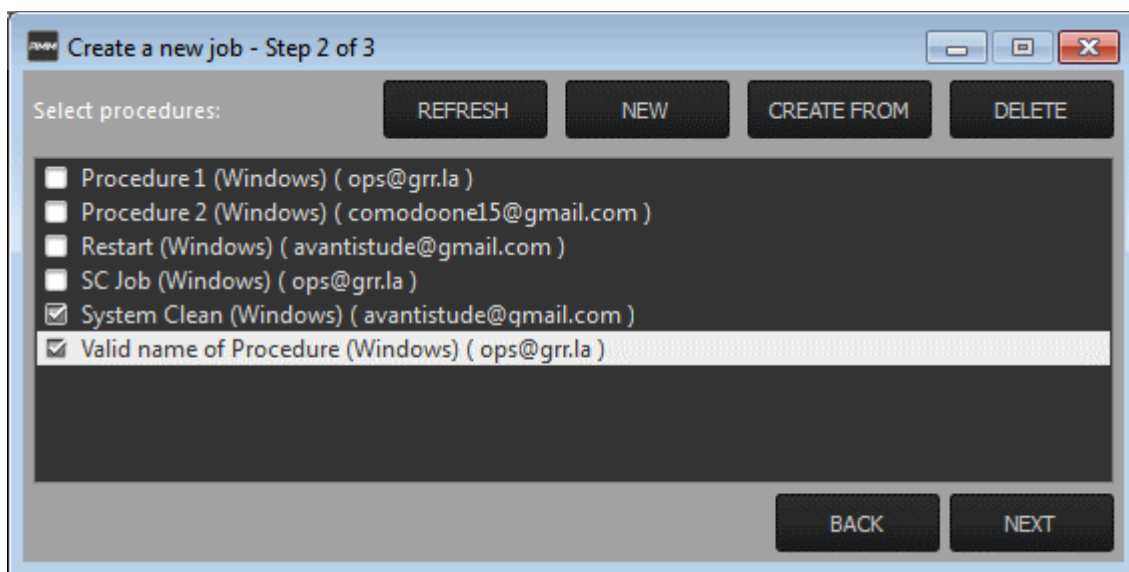


Step 1 - Job Description

- Enter the job details:
 - Job Name - Enter a name for the job
 - Job Description - Enter a short description of the job
 - Operating System - Choose the operating system of the target endpoints
 - Platform - Choose operating system version
- Click 'NEXT' to continue.

Step 2 - Select Procedures

- Select the procedures you wish to add to the job. If you have not yet created any procedures, please refer to [this section of the guide](#).

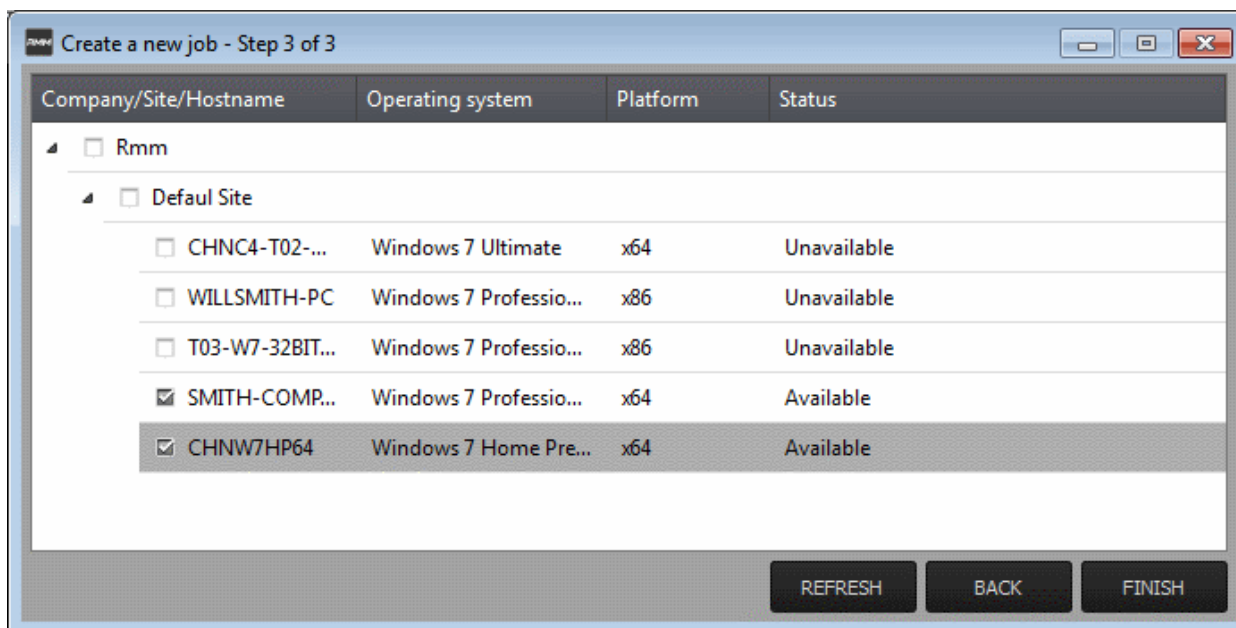


Tip: You can add new procedures from this interface too by clicking 'NEW' from the top of the interface. Refer to the previous section **'Create Procedures'** for more details.

- Click 'Next'

Step 3 - Select Target Endpoints

- Select the endpoints on which you want to execute the job:

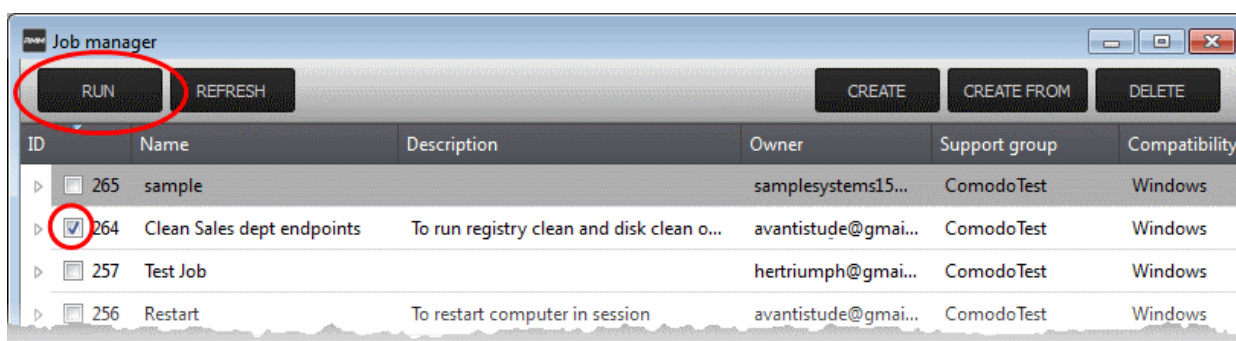


- Click 'FINISH'

The job will be added to the list in the 'Job Manager' interface and will be available for execution at any time.

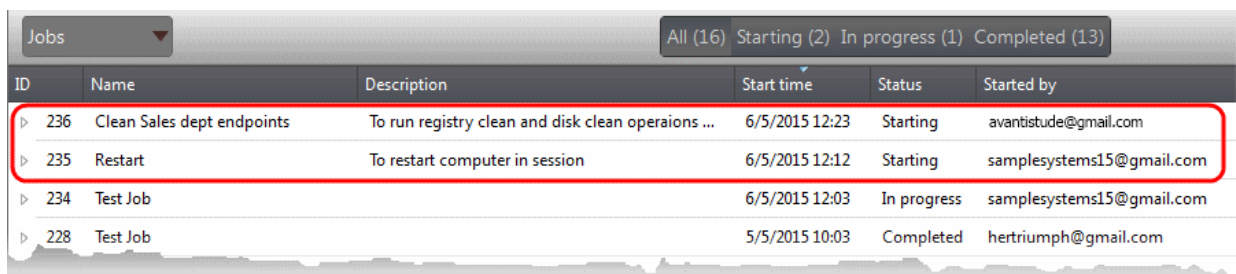
To execute a saved job

- Click 'Job Manager' from the task bar
- Choose the job(s) you want to execute



- Click 'RUN' from the title bar of the Job Manager interface.

The job(s) will be started and their status will be indicated in the 'Jobs' interface.



Create and Apply Monitoring Policies

RMM monitors enrolled endpoints based on the policies applied to them. You can create policies to monitor various system events, and define whether service desks tickets are created if an endpoint violates the policy. Admins can remediate the issues by running jobs or procedures on the endpoint or by initiating a support session with the end-user.

- To open the 'Policies' interface, choose 'Policies' from the drop-down at the top left. The interface displays which policy is in effect on an endpoint and whether or not the endpoint is compliant with its policy. New policies can be created by clicking the 'Create' button at the bottom of the interface.

Policy Name	Description	Endpoints	Status
▶ Traffic Policy		0	OK
▲ Test ping rule	To test COM machine	1	Alarm
▶ Monitors			
▲ Devices			
\infotronics\Cochin\COM			Applied
▶ Security Department	Monitoring polices for security department	0	OK
▶ RAM Policy		0	OK
▶ JS RAM Policy	To check RAM usage of JS system	0	OK
▶ CPU Policy		0	OK

Refresh Apply Policy Create Create from Delete Stop Policy

To create a new policy

- Click 'Create' from the bottom of the interface

The 'Create policy' interface will open.

Create policy

Policy setup

Description:

Triggers an alert if **Any** of the following conditions are met:

CPU Usage **more than** %

For Period **more than** min

Monitor can check if one of the cores exceeded a bottom threshold for more than a specified time period and trigger alert.

CREATE

- Enter a name and a short description for the policy in the respective fields
- Choose the monitoring module from the left.

The parameters pane for the chosen module will open on the right.

- Specify the conditions and thresholds of the rule in the right pane. Your rules are automatically saved as you go along, so you can freely select other modules on the left if you wish to add more rules to the policy.

Tip: You can add any number of conditions for a particular rule by clicking the '+' button at the right. To remove a condition, click the 'X' button to the right.

- Add more modules to the policy by selecting them on the left.

A green check-mark is shown next to modules which are included in the current policy.

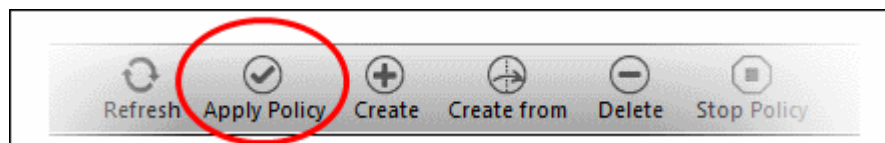
- Click 'Create' to save your policy.

The policy will be added to the list in the 'Policy Manager' interface and will be available for application to desired endpoints at any time.

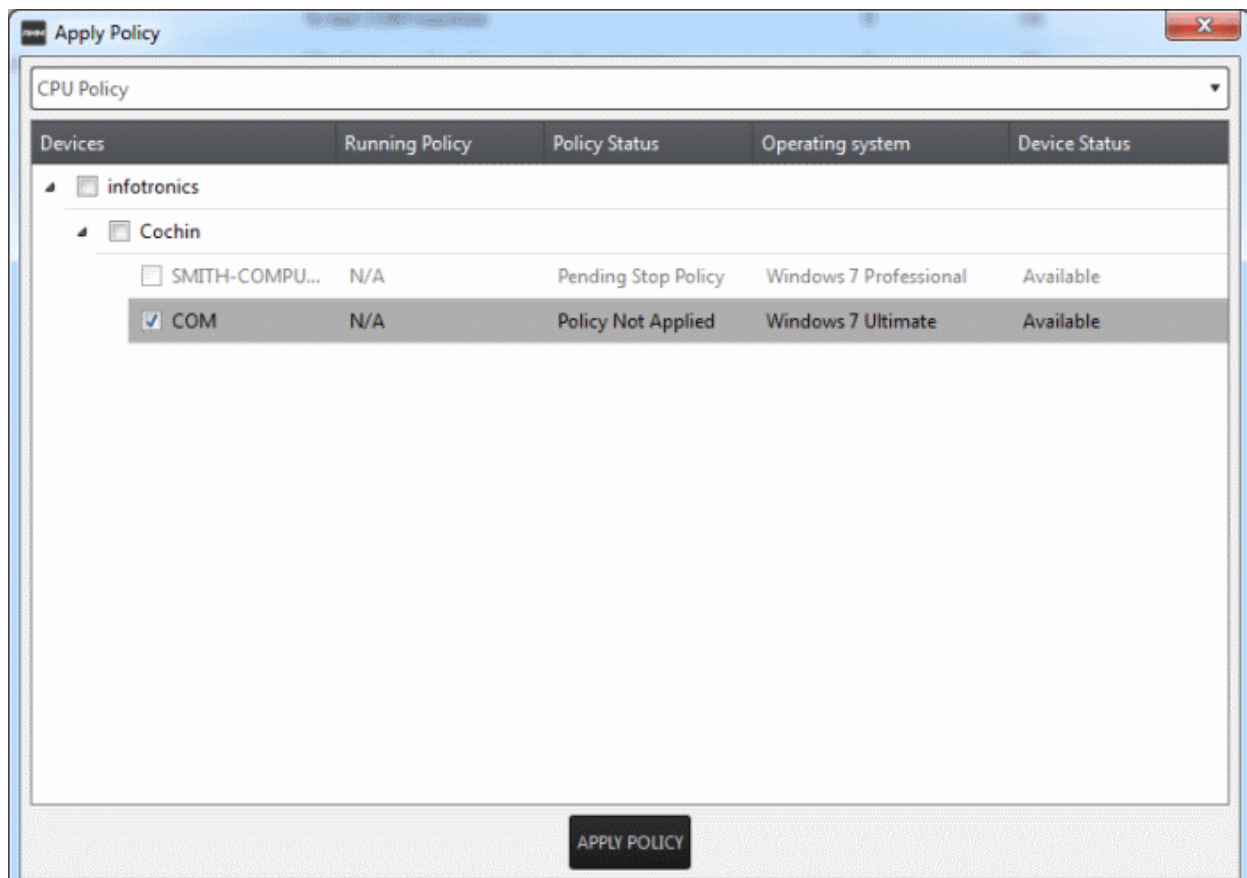
To apply a policy to endpoints

Policies can be applied from the 'Devices' and 'Policies' interfaces.

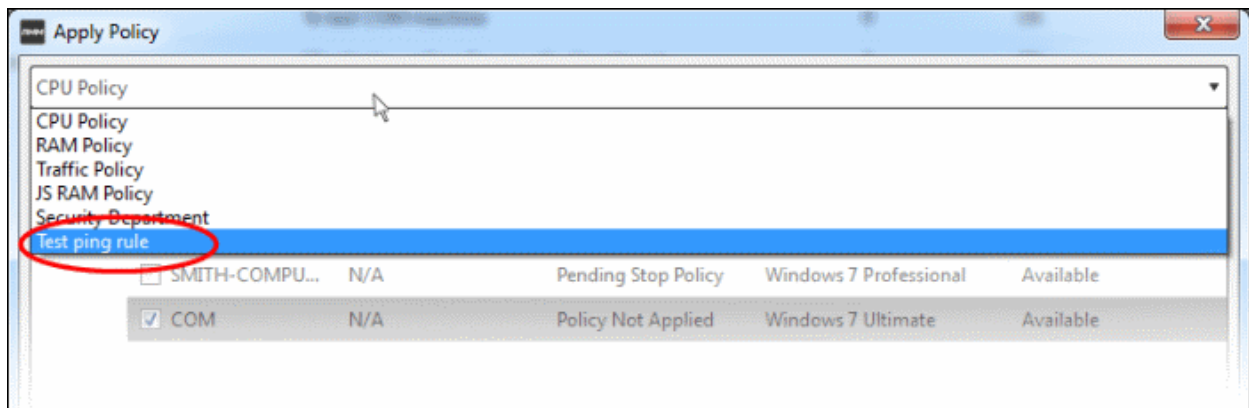
- Click 'Apply Policy' from either of these interfaces



The 'Apply Policy' dialog will open with a list of endpoints enrolled for your account.



- Select the policy you wish to apply from the drop-down at the top



- Choose the endpoints to which the policy should be applied and click 'Apply Policy'.

The policy will be implemented on the selected endpoints and will be listed in the main 'Policies' interface.

Policy Name	Description	Endpoints	Status
Traffic Policy		0	OK
Test ping rule	To test COM machine	1	Alarm
Monitors			
Ping Monitor			
Devices			
\infotronics\Cochin\COM			Applied
Security Department	Monitoring polices for security department	0	OK
RAM Policy		0	OK
JS RAM Policy	To check RAM usage of JS system	0	OK
CPU Policy		0	OK

Tip: Clicking the arrow at the right of a policy name displays the policy's rules.

If any of the monitored parameters exceed the thresholds set by the policy, the endpoint will be indicated as non-compliant (under the 'Compliant' column) in the Devices interface. Also, a support ticket will be automatically created in Service Desk. The Administrator can view the details of the breach by logging-into the Service Desk and resolve the issue by:

- **Running procedures;**
 - **Executing jobs;**
- Or
- **Initiating a support session and taking remote access of the endpoint(s).**

Handle Support Sessions

The support session enables you to take remote desktop control of the client computer and perform maintenance tasks and resolve issues identified in them. By establishing a support session you can:

- Perform actions like cleaning the client's computer, power management, system restore, file transfer, system inventory audit and so on.

- Run procedures to correct issues identified by policy violation service desk tickets.

Initiating a support session from the technician console

If you require to perform a maintenance operation or run procedures you can initiate the session by clicking 'Takeover' from the 'Devices' interface.

- Open the 'Devices' interface by choosing Devices from the drop-down at the top-left

Company	Site	Hostname	Operating system	Device type	Logged user	Internal IP	External IP	Compliant	Applied policy name	Description	Action
infotronics	Cochin	SMTH-COM..	Windows 7 Professional - x64	Workstation	SMTH-COMPUTER\Chand...	10.108.17.233	10.108.17.233	N/A	N/A		Takeover
infotronics	Cochin	COM	Windows 7 Ultimate - x64	Workstation	com\Administrator	10.108.17.197	10.108.17.160	No	Test ping rule		Takeover

- Click 'Take Over' under 'Action' in the row of the device (endpoint) to which the support session is to be started.

Left Hand Side Navigation – Contains controls for running procedures, transferring the session and a list of tools for use in providing support and auditing the endpoint

Main Configuration and Information Area
Each tool deployed on to the endpoint opens a new tab.
The configuration/information screen for the tool is displayed under the respective tab

A session will be established. The Support Session Interface

Left Hand Side Navigation - The left hand side navigation contains controls and buttons for various tasks like running a procedure, deploying tools on to the endpoint to perform various actions and audits, transfer the support session to other clients and so on.

- **END** - Concludes the support session and closes the session window for the endpoint.
- **RUN PROCEDURE** - Allows you to run procedures on the endpoint. You can select procedures from those

that are available in the 'Procedures' interface. Refer to the section **Run a Procedure** for more details.

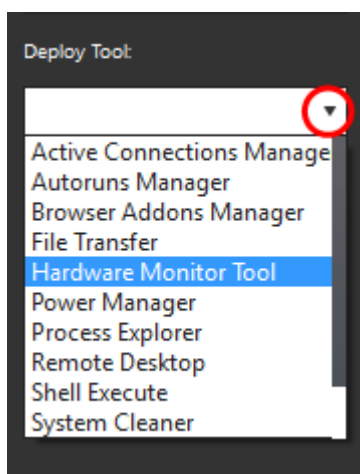
- **Deploy Tool** - Allows you to select tools for performing various tasks such as system cleaning, power management, system restore and so on. Refer to the section **Execute pre-defined actions** on the endpoint for more details

Main Configuration and Information Area - The main configuration and information area displays the configuration screens for the tools selected from the 'Deploy Tool' drop-down.

Next, see:

- **Execute pre-defined actions on the endpoint**
- **Access the Endpoint through Remote Desktop Connection**
- **Run a Procedure**

Execute Pre-Defined Actions on the Endpoint

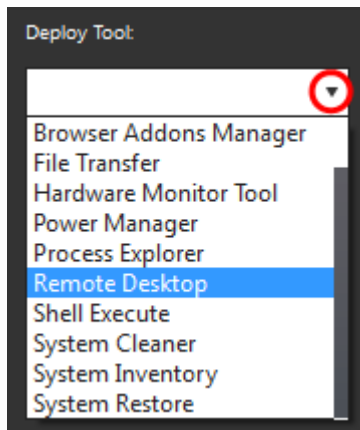


The 'Deploy Tool' drop-down contains handy diagnostic and repair tools which can be deployed to endpoints. For example, you can view all running processes and kill unnecessary processes, access the command line interface of the endpoint, run system clean operations and so on. The service session window console allows any number of tools to be deployed concurrently on to the endpoint. Each tool opens a new tab in the 'main configuration area and displays options and results pertaining to the tool. The following table provides the list of tools available for deployment.

Table of Available Tools for Deployment on to Endpoint	
Tools	Description
Active Connections Manager	Allows you to view all currently active network connections (applications, processes and services), individual connections that each application is responsible for and terminate any unsafe processes that are running on the endpoint.
Autoruns Manager	Allows you to view and edit start-up items, services, drivers, system programs and so forth, that are loaded when the endpoint boots up.
Browser Add-Ons Manager	Allows you to identify the browser add-ons installed on the browsers and to remove unsafe or malicious add-ons.
File Transfer	Allows you to transfer any file between the your computer and the endpoint.
Hardware Monitoring Tool	<ul style="list-style-type: none"> • Allows you to track and monitor the hardware index to check whether the computer is overheating or voltage is out of the acceptable range to preclude an operating system failure.
Power Manager	Allows you to shut down and restart the endpoint, if required after a critical operation like editing the Windows Registry of the endpoint.
Process Explorer	Allows you to quickly identify, monitor and terminate any unsafe processes that are running on the endpoint. The Process Explorer shows ALL running processes, even those triggered by malware in the computer and those that were invisible or very deeply hidden.

Remote Desktop	Allows you acquire control of the client's computer through Remote Desktop connection in order to investigate and resolve issues. Refer to the section ' Access the Endpoint through Remote Desktop Connection ' for more details.
Shell Execute	Allows you to open the command prompt window of the endpoint and execute shell commands.
System Cleaner	Allows you to perform Registry clean operation to remove obsolete and unwanted registry entries to boost up system performance and disk clean operations to remove junk or garbage files which occupy a considerable space in the endpoint.
System Inventory	Allows you to view the hardware and software resources of the endpoint. The 'System Inventory' audit provides a valuable information for determining compatibility of the hardware with the operating systems, and identifying any changes to a system that might develop problems.
System Restore	Allows you to revert the endpoint to a previously created restore point (including system files, installed applications, Windows Registry, and system settings) to that of a previous point in time. You can also create a restore point with the present configuration of the endpoint to restore it to the present condition in future.

Access Endpoints through Remote Desktop Connection

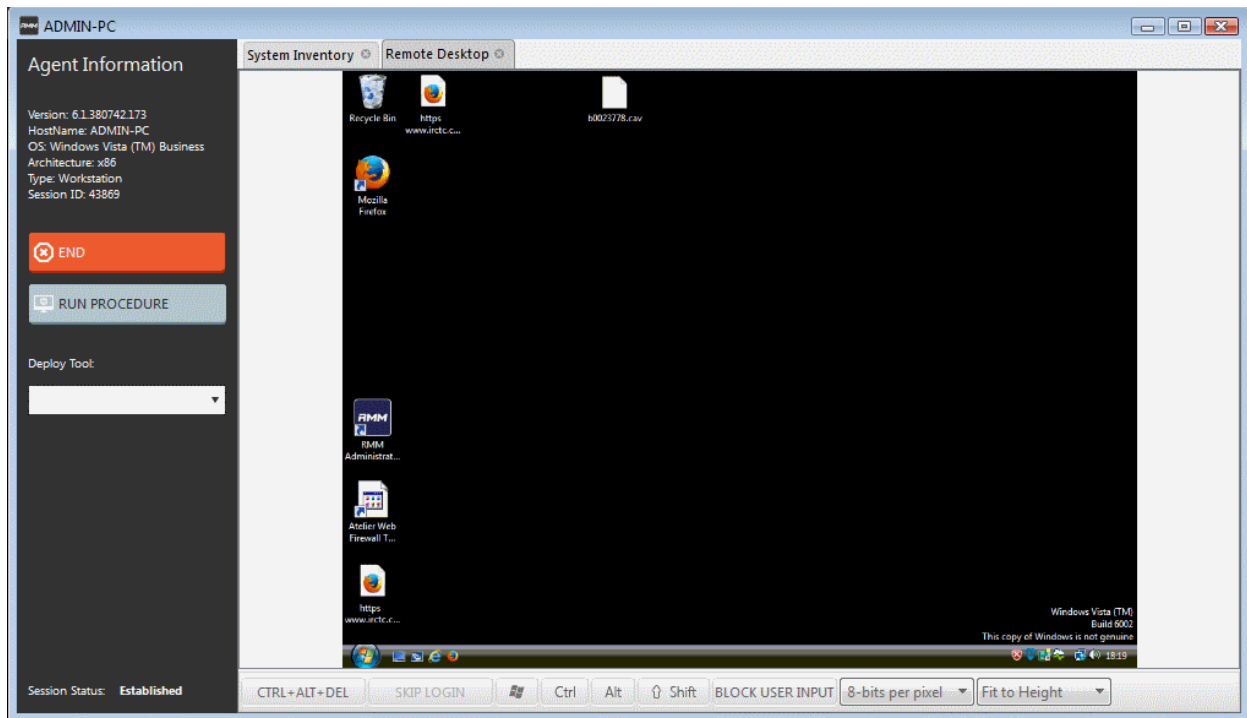


RMM allows you to gain remote desktop access to the endpoint and execute necessary actions to solve issues.

To initiate a remote desktop connection

Take over the endpoint having the RMM client installed and a session is established. Click the remote desktop option and then you can perform tasks like 'Run Procedure'.

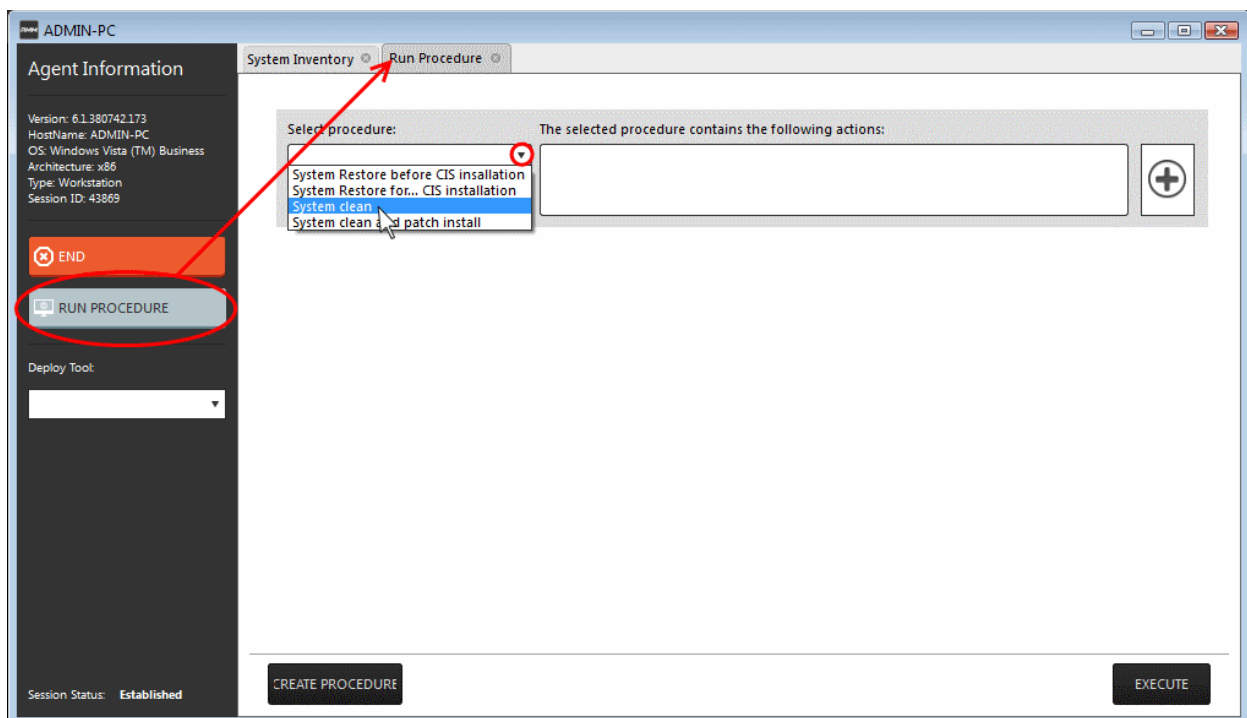
The desktop of the endpoint will open in a new 'Remote Desktop' tab in the main configuration area.



Run Procedures

You can also execute pre-defined procedures on the endpoint from the support session interface.

To run a procedure



- Click RUN PROCEDURE from the left.

A new Run Procedure tab will open in the main configuration area. The Select Procedure drop-down will display the pre-configured procedures which are available at the 'Procedures' interface. For more details on creating and managing procedures, refer to the section **Create Procedures**.

- Choose the procedure to be run at the endpoint from the 'Select procedure' drop-down.

The sequence of actions contained in the chosen procedure will be displayed in the list at the right.

- Repeat the process to add more procedures by clicking the '+' button at the right end
- Click 'Execute'.

A job will be created with the list of selected procedures for the endpoint and will be executed.

1.2 System Requirements

The list below shows supported operating systems and hardware requirements for endpoints running the RMM agent.

Supported Operating Systems

- Microsoft Windows client family
 - Windows XP (32 bit)
 - Windows Vista (32 bit and 64 bit)
 - Windows 7 (32 bit and 64 bit)
 - Windows 8 (32 bit and 64 bit)
 - Windows 10 (32 bit and 64 bit)
- Microsoft Windows Server family
 - Windows 2003 Server (SP2 or higher) x86 and x64 editions
 - Windows 2003 Small Business Server
 - Windows 2003 Small Business Server R2
 - Windows 2008 Server (SP2 or higher) x86 and x64 editions
 - Windows 2008 Small Business Server
 - Windows 2008 Server R2
 - Windows 2011 Small Business Server
 - Windows 2012 Server

Minimum Hardware Requirement

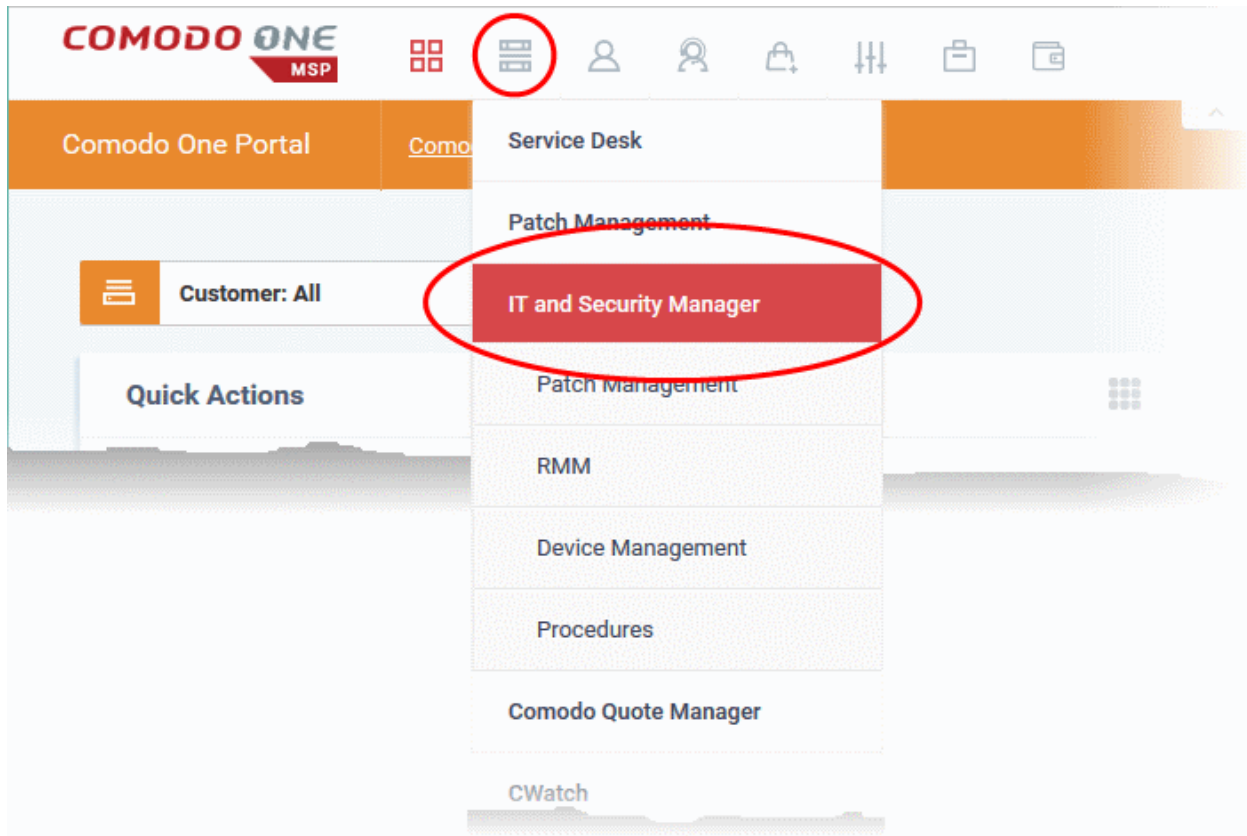
- Disk space - 100 MB
- Memory - 100 MB
- Processor - Single core 1.8 GHz or better

2 Install RMM Administrative Console

Download the RMM Console setup file

You can download the RMM console setup file from the ITSM console interface.

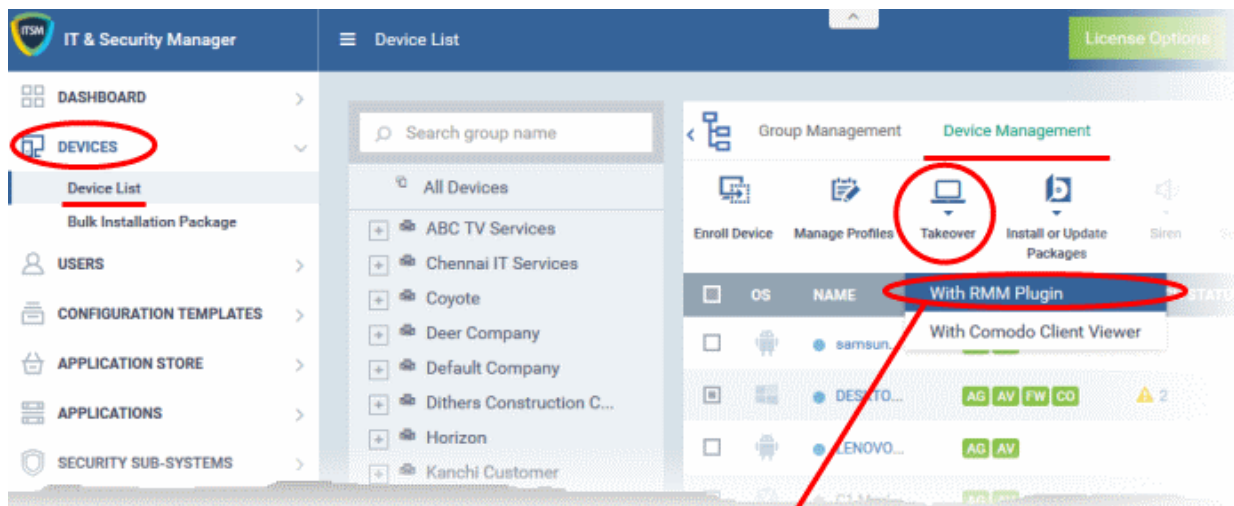
- Log into the Comodo One at <https://one.comodo.com/app/login> with your user name and password
- Click the 'Licensed Applications' icon from the top and select 'IT and Security Manager', to open the ITSM console



- Click the 'Devices' link on the left and choose 'Device List'
- Click the 'Device Management' tab at the top of the main configuration pane

A list of all devices enrolled to ITSM will be displayed by default.

- Choose a 'Windows' device, click 'Takeover' from the top then 'With RMM Plugin'
-





Comodo Remote Device Management Takeover

Close

Step 1

If you didn't download and install the Technician Console before, Please download it from below

 **Download**
RMM Console x86

 **Download**
RMM Console x64

Choose the operating system of the computer on which you have planned to install the console and download the file.

Install the Console

- Double click on the RMM console setup icon

Step 1: Welcome Screen

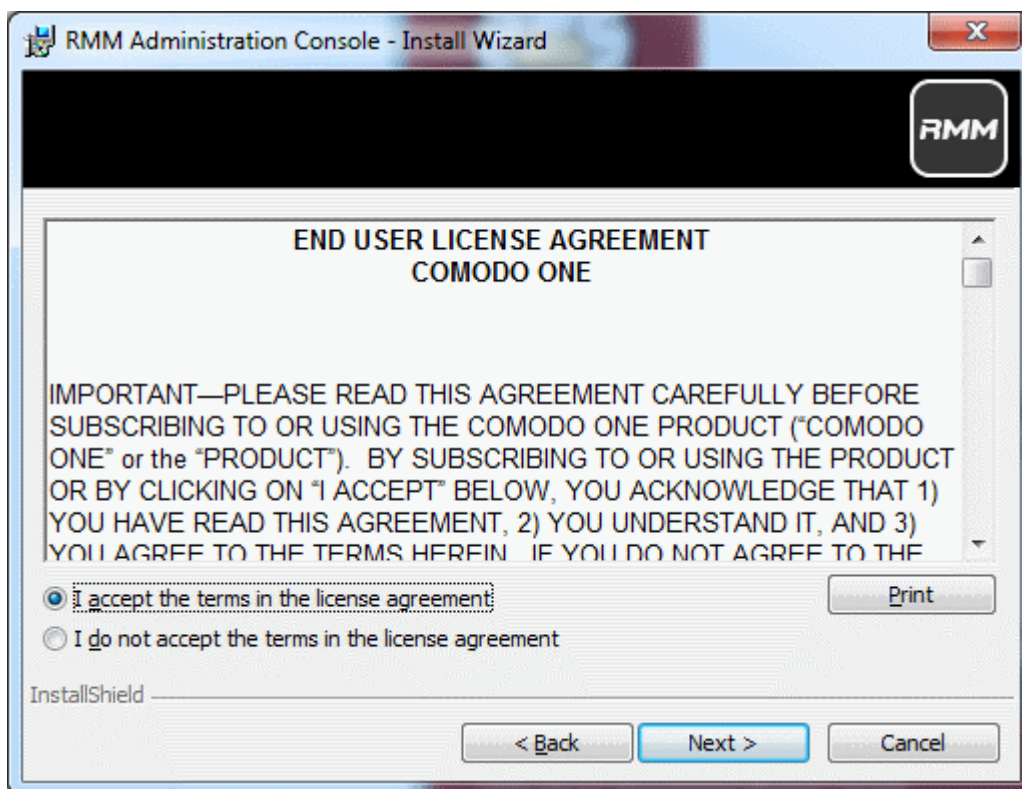
The set up program will start automatically and the 'Welcome screen' of the installation wizard will be displayed.



- Click 'Next' to continue.

Step 2: End User License Agreement

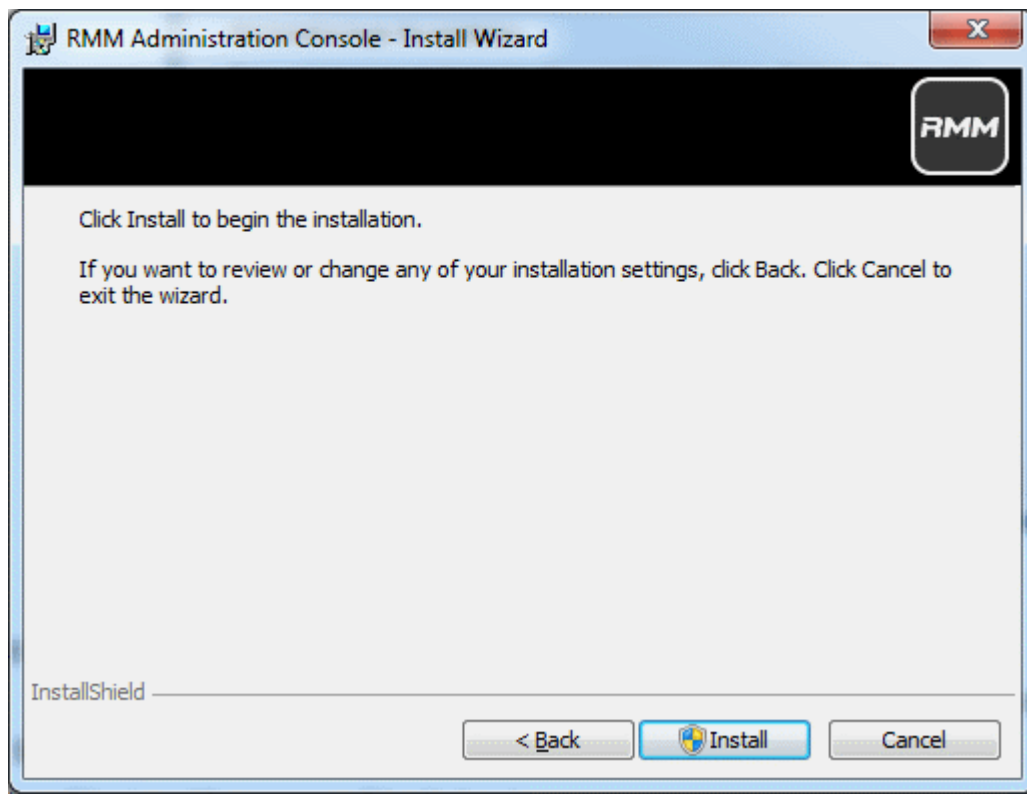
Complete the initialization phase by reading and accepting the End User License Agreement (EULA).



- Click 'I Agree' to continue installation. If you want to cancel the installation, click 'Cancel'.

Step 3: Ready to Install

The next stage is confirmation of the installation settings.

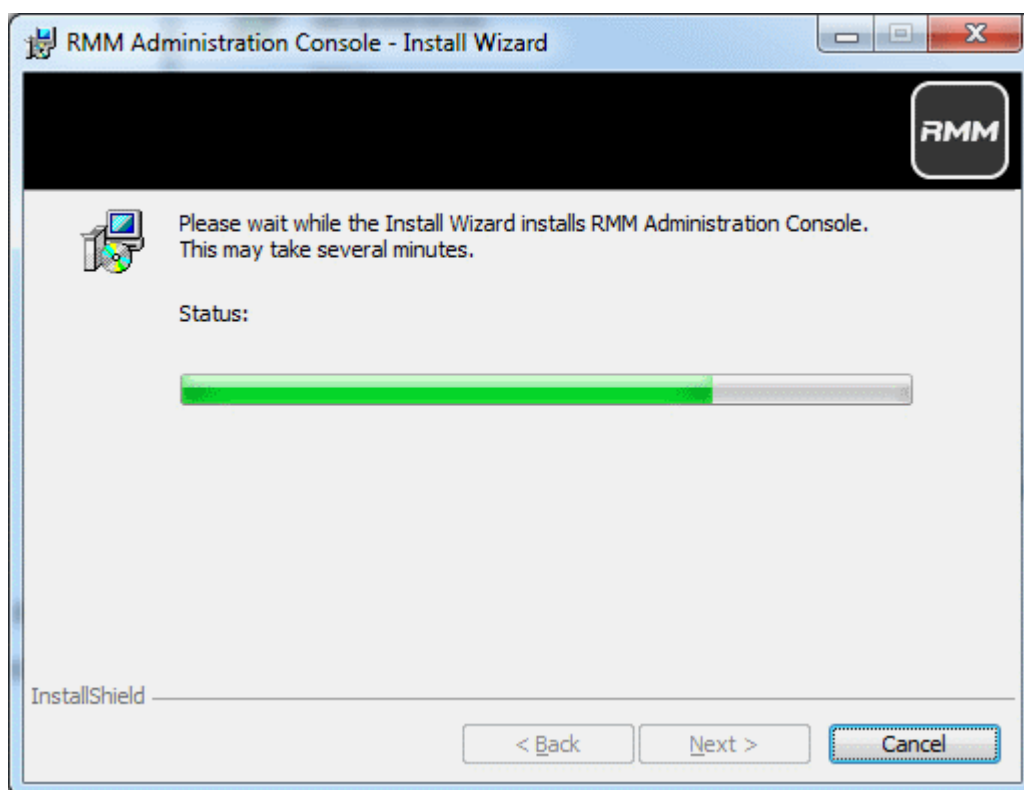


The program will be installed in the default location C:\Program Files\Comodo\RMM Administration Console

- If you want to review the installation settings, click 'Back'. To continue with the installation, click 'Install'.

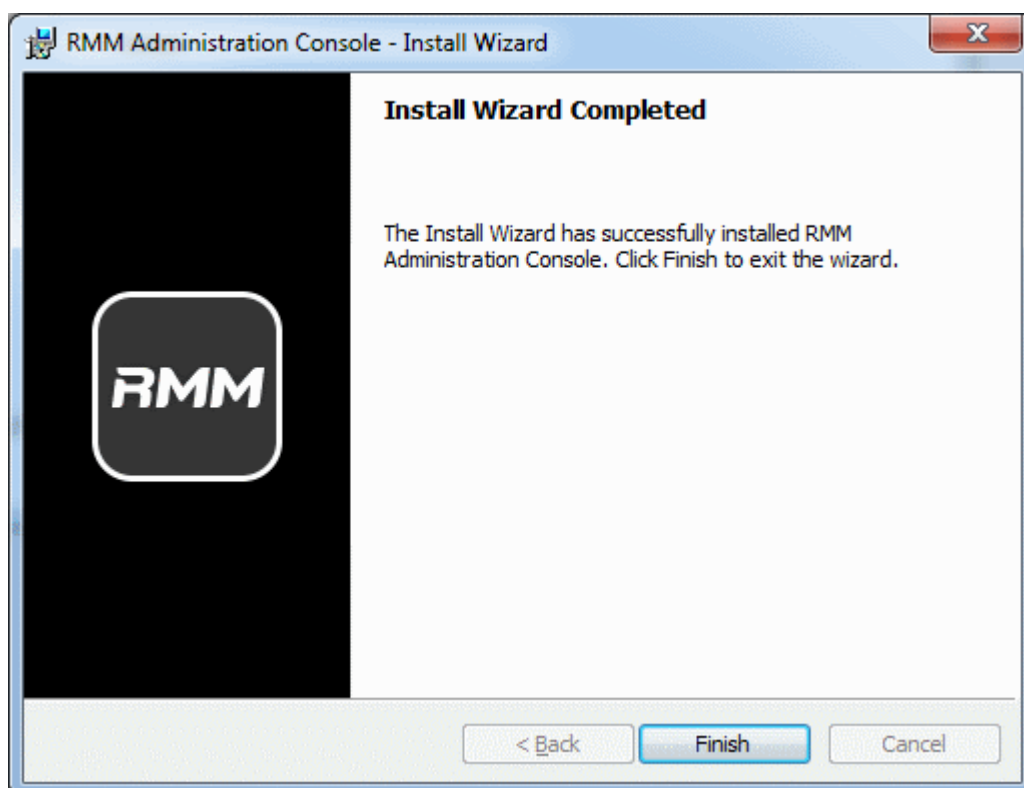
Step 4: Setup Progress

Installation will begin and the progress will be displayed.



Step 5: Finalizing the Installation

On completion, the 'Install Wizard Completed' dialog will be displayed.



- Click 'Finish' to complete installation and exit the wizard.

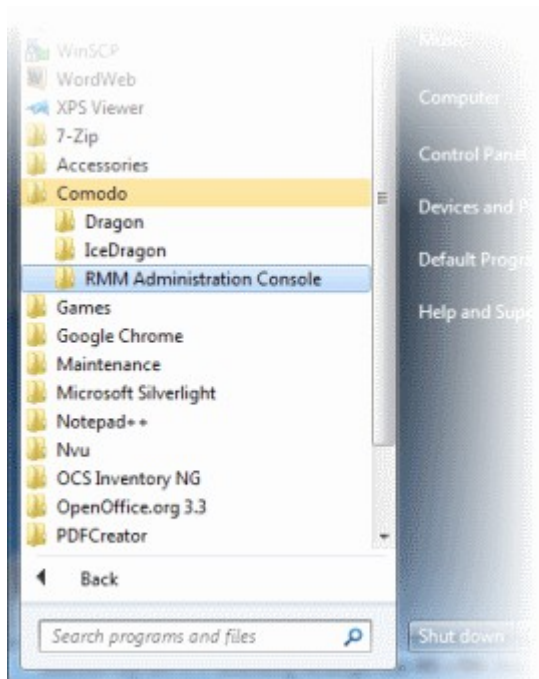
On completion, the login dialog will open. Refer to the next section '[Logging-in to the RMM Administrative Console](#)' for more details.

2.1 Login to the RMM Administrative Console

After installation, the RMM Administrative Console can be started from the Windows Desktop or from the Start menu.

Start Menu

- Click 'Start' and select All Programs > Comodo > RMM Administration Console

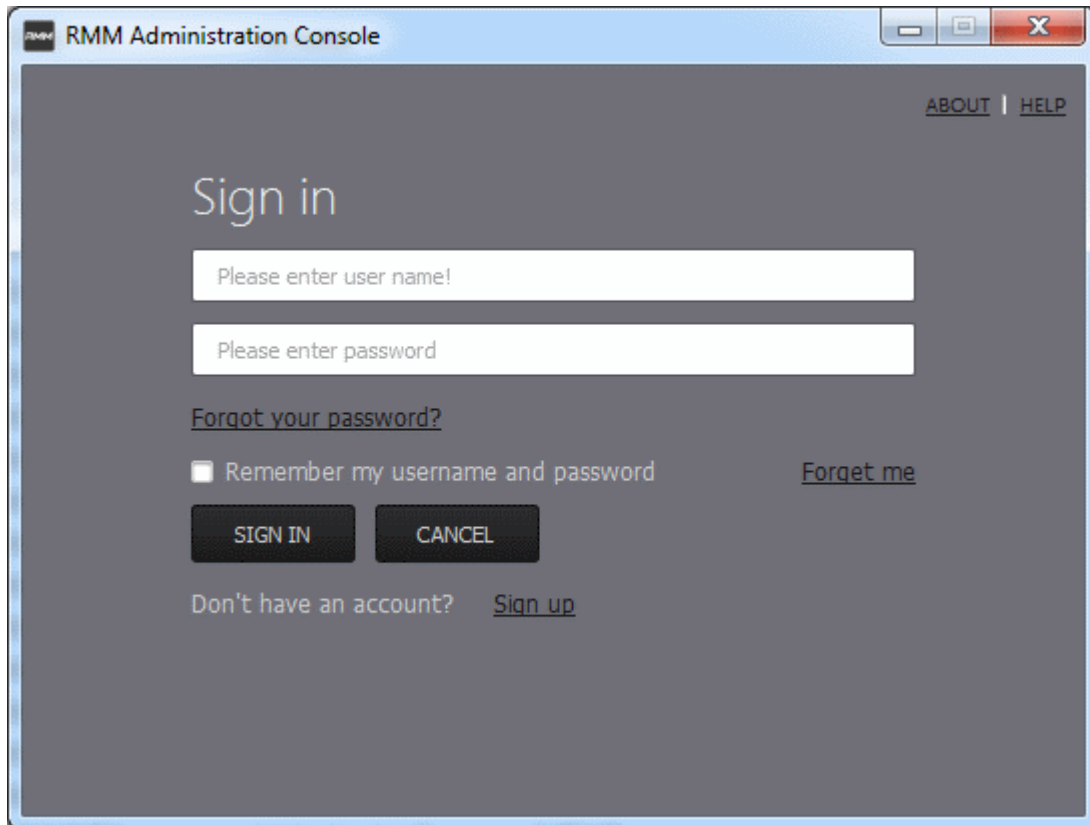


Windows Desktop



- Just double click the RMM icon in the desktop to start RMM Administrative console

The RMM 'Sign in' screen will be displayed.

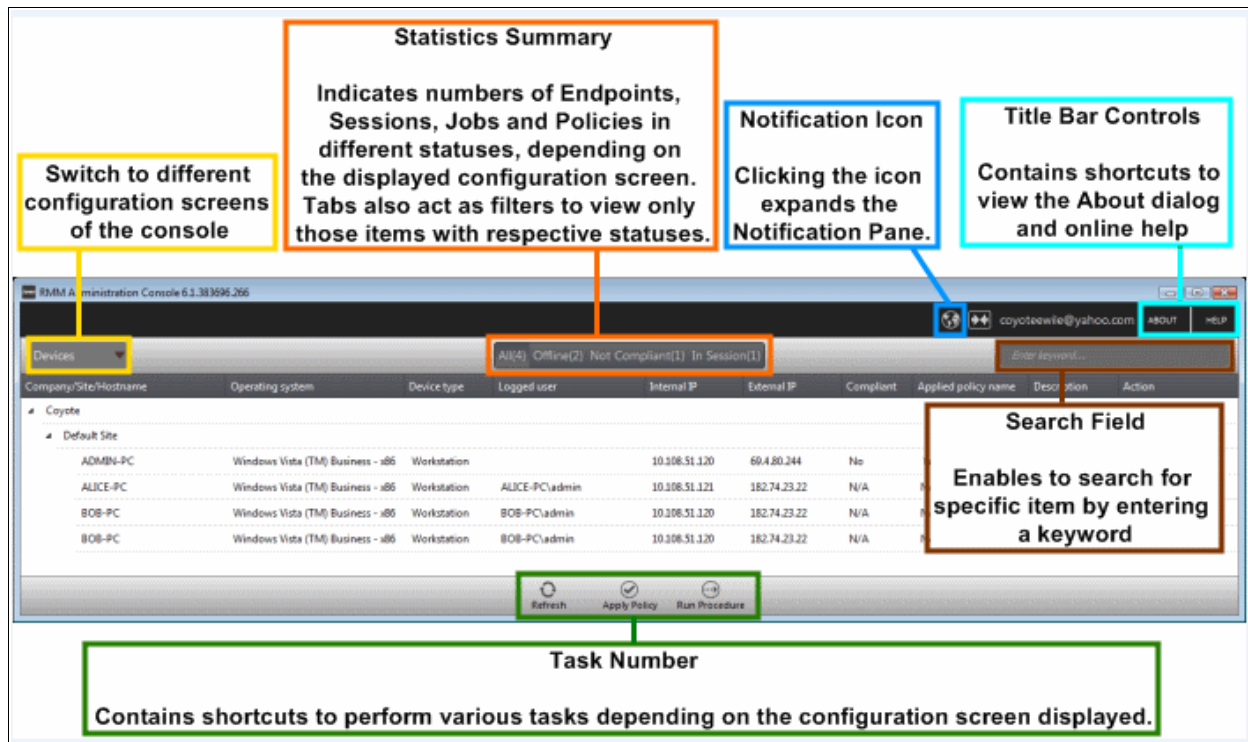


- Enter the Comodo One Client Security credentials or that was reset by you on clicking the verification link in the 'Admin Verification' email.
- If you are using the portable version, just double click on the file and enter the Comodo One Client Security credentials.

On successful verification, the RMM Administration Console will be displayed.

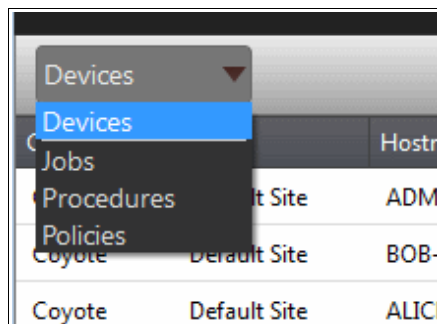
3 The RMM Administrative Console

The Administrative Console is the nerve center of Comodo Remote Monitoring and Management (CRMM), allowing administrators to view details of monitored endpoints, create policies, automatically run procedures and more, on the endpoints.



The console consists of the following main areas that can be selected from the drop-down menu near the top left - 'Devices', 'Jobs', 'Procedures' and 'Policies'.

Main Functional Areas

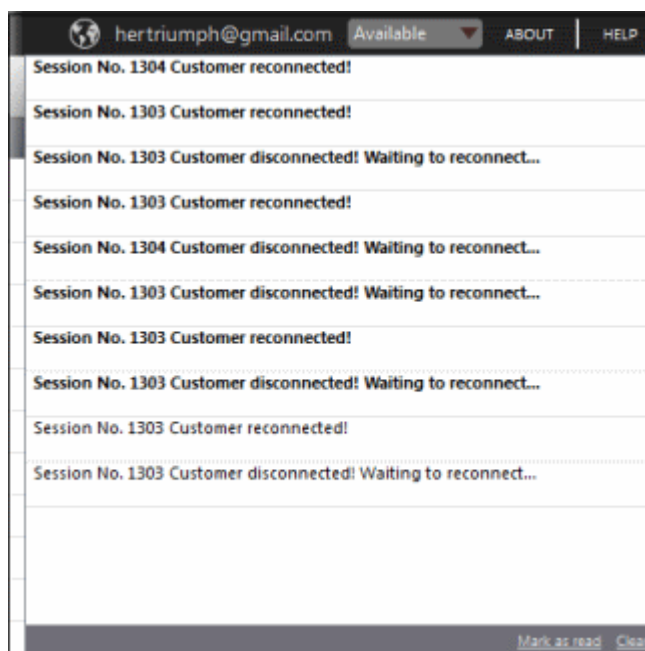


- **Devices** - View the list of monitored devices and manage them. You can run procedures and apply configuration policies on endpoints.
- **Jobs** - View the jobs that are completed, started and in progress. You can also stop the job from this interface.
- **Procedures** - Create procedures from a set of predefined actions such as 'System Restore', 'File Transfer', 'Shell Execute' and run them on endpoints
- **Policies** - Create policies and deploy them onto endpoints so as to generate service desk tickets if policies are violated.

Notification Icon

The notification icon  at the top right of the interface blinks to alert the admin when an endpoint in session is disconnected or reconnected.

- Click on the icon to view the messages

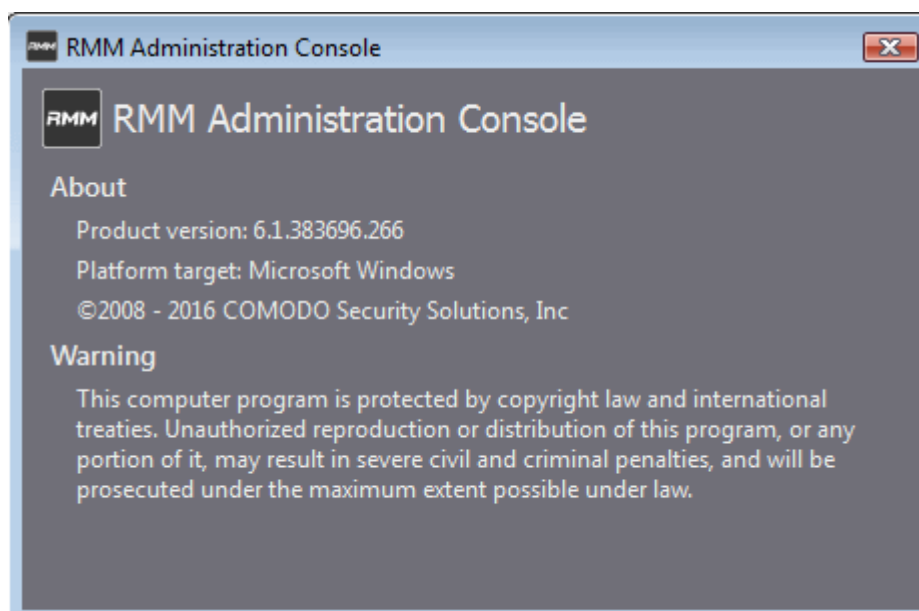


The messages that are in bold indicate that they are not read.

- Click the 'Mark as read' link below the message window after viewing the messages
- Click the 'Clear' link to remove the messages from the window.
- Click on the notification icon again to close the message window.

About

Opens the 'About' dialog of RMM admin console that contains the version number, copyright information, license information and option to purchase and change the license key.



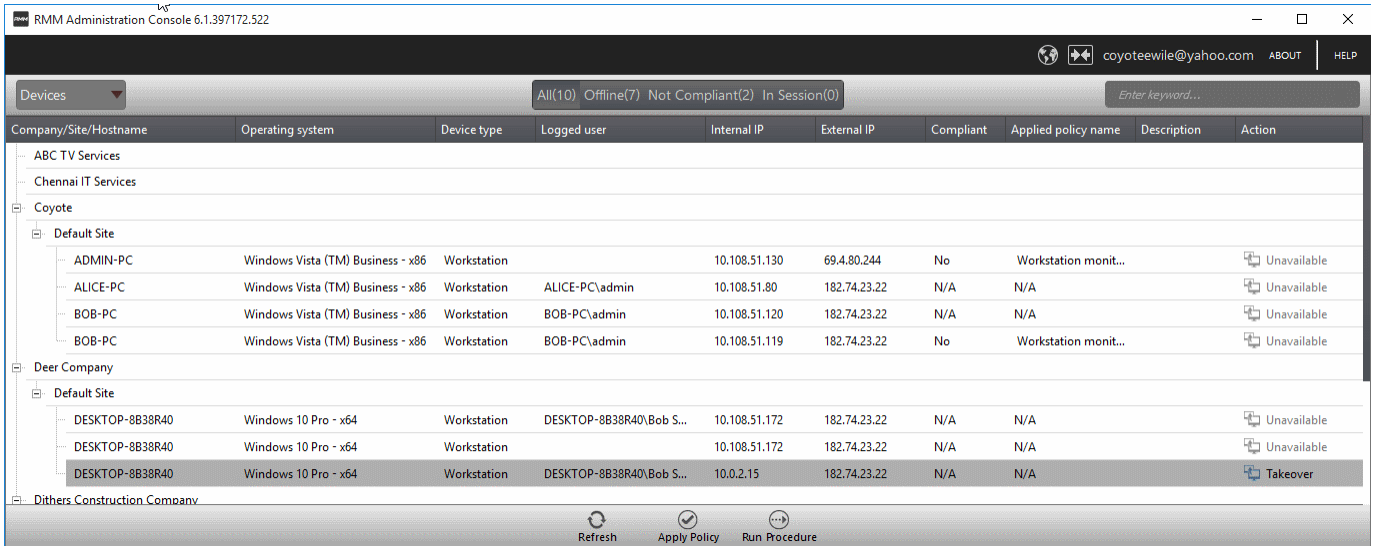
Help

Opens the online help guide main page. The RMM admin help guide contains detailed explanations of the functionality and usage of the application.

4 The Devices Interface

The 'Devices' screen allows admins to view and manage company endpoints which are monitored by the RMM interface. The interface provides address, system and user details about each endpoint and allows administrators to directly apply policies and run procedures.

- To open the 'Devices' screen, choose 'Devices' from the drop-down at the top left.



The list of all Windows devices that are enrolled through for your ITSM console and enabled for management through RMM console by installing the RMM agent will be displayed with their details.

Tip: New endpoints for management through RMM can be added only through ITSM console. Once an endpoint is enrolled to ITSM, the RMM agent will be automatically installed on it, to add it for management by RMM. For more details on enrollment of endpoints to ITSM, refer to the online help page at <https://help.comodo.com/topic-399-1-786-10126-Enrolling-User-Devices-for-Management.html>.

Devices - Column Description	
Column Header	Description
Company	The name of the company under which the devices are enrolled.
Site	The device's location of a company. session - column description
Hostname	The name of the enrolled device.
Operating system	The operating system of the enrolled device
Device type	Indicates whether the device is a workstation or a server
Logged user	The name of the logged user for the device
Internal IP	The IP address of the device inside the internal network
External IP	The IP address of the device in the external network
Compliant	Indicates whether the device is compliant or non-compliant for applied policies. Refer to the section ' Managing Policies ' for more details.
Applied policy name	Displays the name of the policy applied for the device

Description	The description provided for the device while adding
Action	Indicates whether the device is ready for remote session, in session or not available for remote session

To view the details of endpoints enrolled for companies at different sites under a single column, click the 'Company' header twice.

The 'Company/Site/Hostname' headers will be clubbed under a single column and the details displayed.

- Click the  button beside a row to expand or collapse the section

From the 'Devices' interface an admin can:

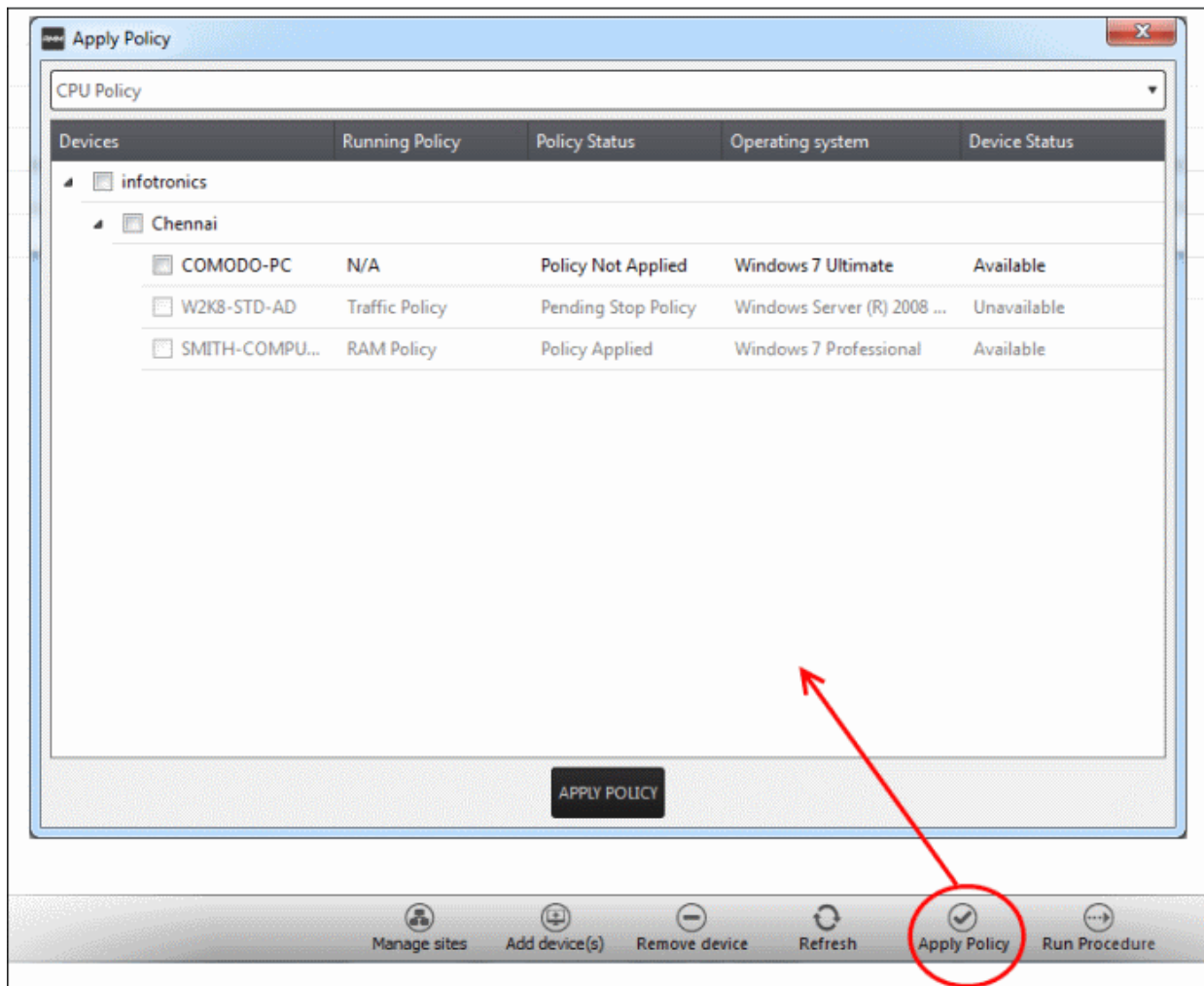
- **Apply Policies**
- **Run Procedures**

4.1 Apply Policies

Policies help your team respond to potential issues on managed endpoints by allowing you to set thresholds for CPU usage, RAM usage, Drive Space and more. Policies are constructed by setting conditions in one or more 'Monitors'. If the conditions of a monitor are met then a ticket is created in the Service Desk module. For example, you can configure the 'RAM Monitor' to notify you/create a ticket if RAM usage exceeds a certain % for a certain length of time.

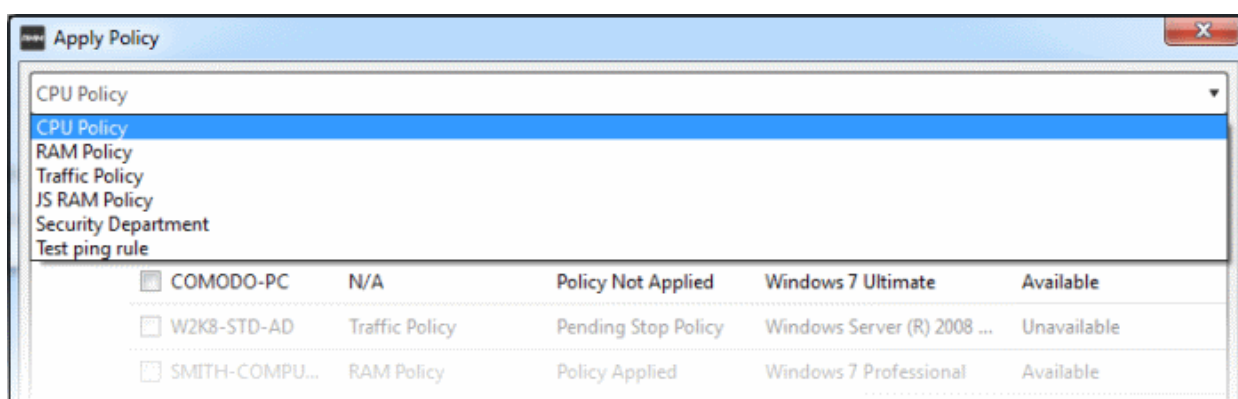
Policies are created from the 'Policy Manager' interface and can be deployed from there as well as from the 'Devices' screen. Refer to the section '**The Policies Interface**' for more details about creating policies.

To apply a policy from the 'Devices' screen, click the 'Apply Policy' button at the bottom of the interface

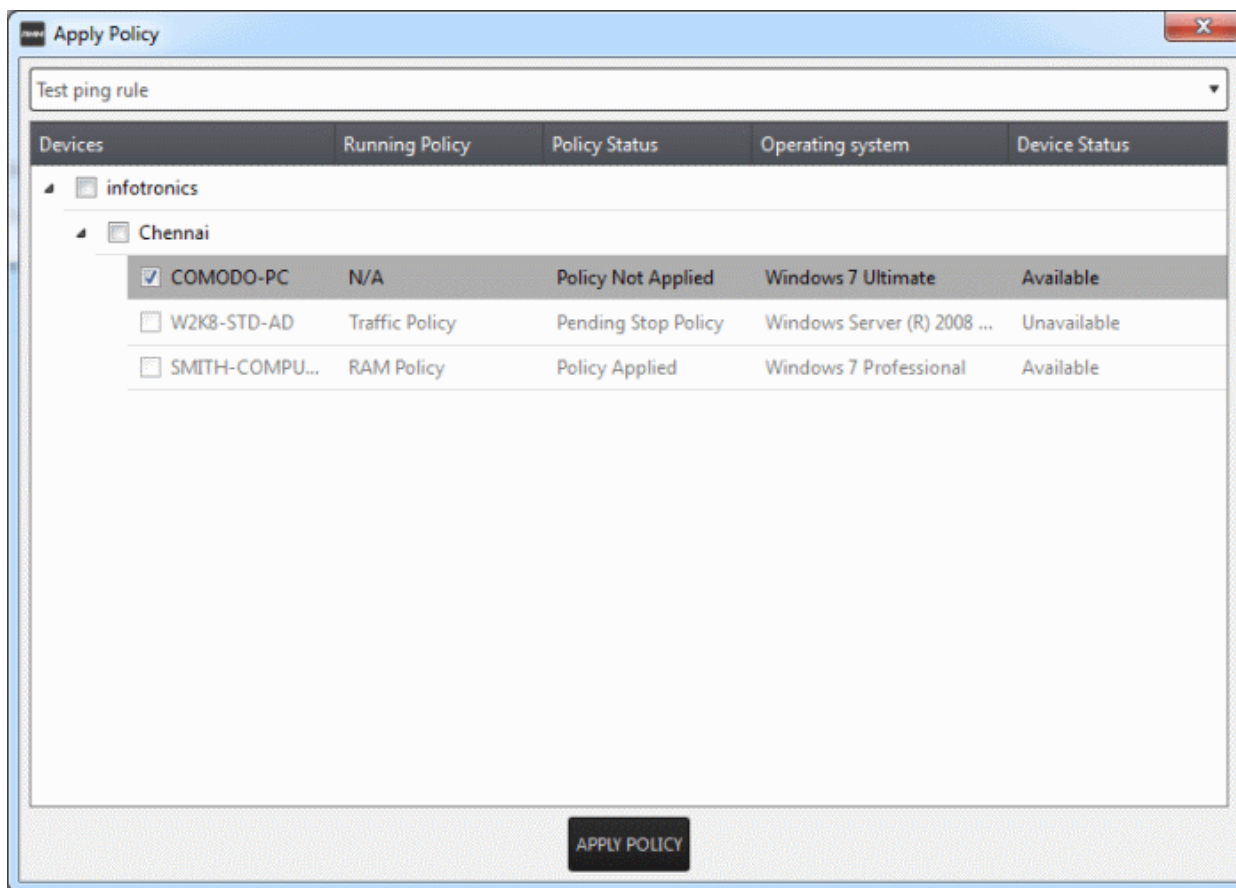


The 'Apply Policy' dialog will be displayed.

- Select the policy to be applied from the drop-down. The policies are created from the 'Policies' screen. Refer to the section **'Managing Policies'** for more details.

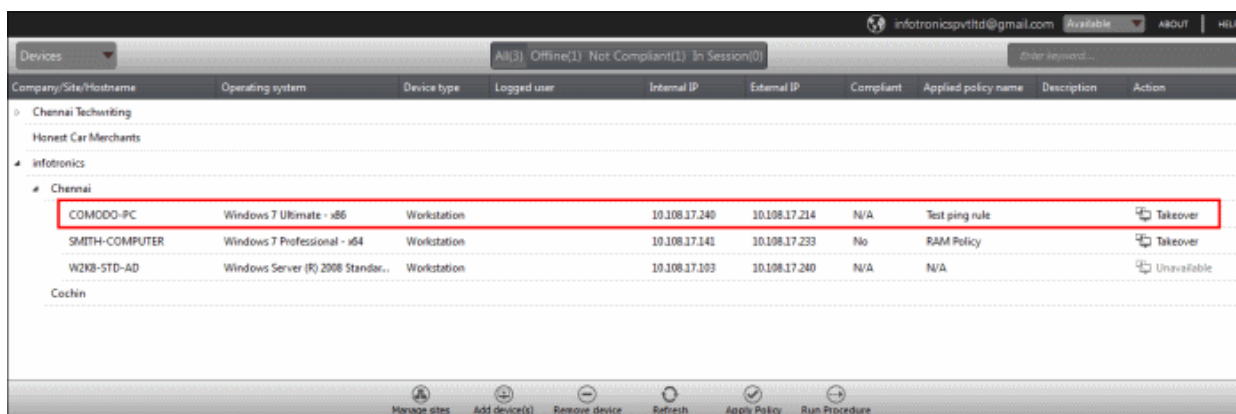


- Next, select the endpoint(s) that should be deployed the chosen policy. Please policies can be applied to endpoints that are 'Available' under the 'Status' column



- Click the 'Apply Policy' button at the bottom.

The policy will be deployed onto the selected endpoint(s) and displayed on the 'Devices' screen.

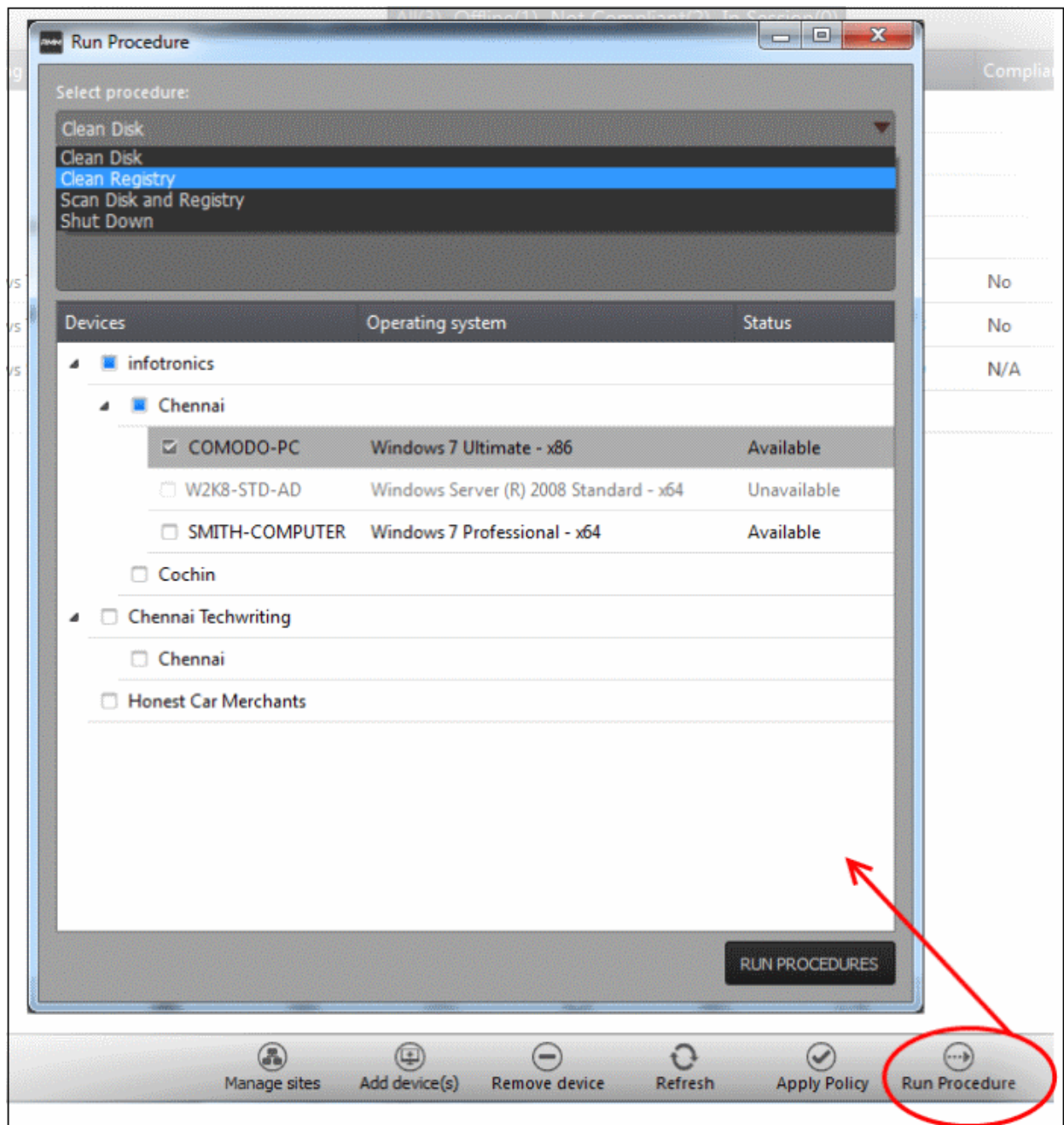


If you want to stop a policy applied to an endpoint, it can be done from the 'Policies' interface. Refer to the section **'Managing Policies'** for more details.

4.2 Run Procedures

A 'Procedure' is a set of actions such as 'Restart' in 'Power Manager' to be run on an endpoint. You can also configure a series of actions with parameters, to be performed in sequence while creating a procedure. The 'Procedures' are created in **'The Procedures Interface'** and you can run a procedure from the 'Devices' screen as well as from the 'Procedures' screen. Refer to the section **'The Procedures Interface'** for more details about how to create and manage procedures.

To run a procedure from the 'Devices' screen, click the 'Run procedure' button at the bottom of the interface



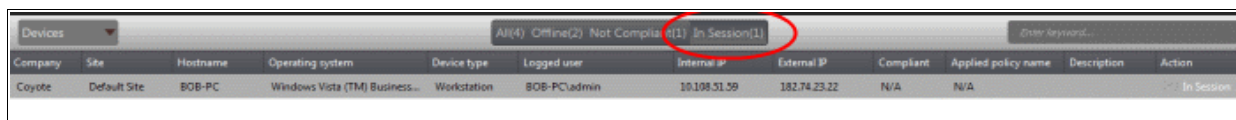
- Select the procedure that you want to run from the 'Select procedure' drop-down at the top. Refer to the section **'Managing Procedures'** for more details about how to create and manage procedures.
- Enter the name of the job in the 'Job description' field
- Select the endpoints from the 'Devices' list that you want to run the procedure
- Click the 'Run Procedures' button at the bottom

The procedure will be run on the selected endpoints and it will be created as a job and displayed in the **'Jobs'** interface with its status showing 'Starting', 'In-progress' or 'Completed'. Refer to the section **'The Jobs Interface'** for more details.

5 The Sessions Interface

CRMM allows admins to establish support sessions with users and take over endpoints remotely in order to assess the nature of problem and then take corrective actions such run procedures and deploy tools. You can also transfer a session to another admin from the support sessions interface.

To open the 'Sessions' screen, click 'In Sessions' from the top middle pane.



Sessions - Column Description	
Column Header	Description
Company	The name of the company under which the devices are enrolled.
Site	The device's location of a company.
Hostname	The name of the enrolled device.
Operating system	The operating system of the enrolled device
Device type	Indicates whether the device is a workstation or a server
Logged user	The name of the logged user for the device
Internal IP	The IP address of the device inside the internal network
External IP	The IP address of the device in the external network
Applied policy name	Displays the name of the policy applied for the device
Description	The description provided for the device while adding
Action	Indicates whether the device is ready for remote session, in session or not available for remote session
Applied policy name	Displays the name of the policy applied for the device

5.1 Support Sessions Interface - An Overview

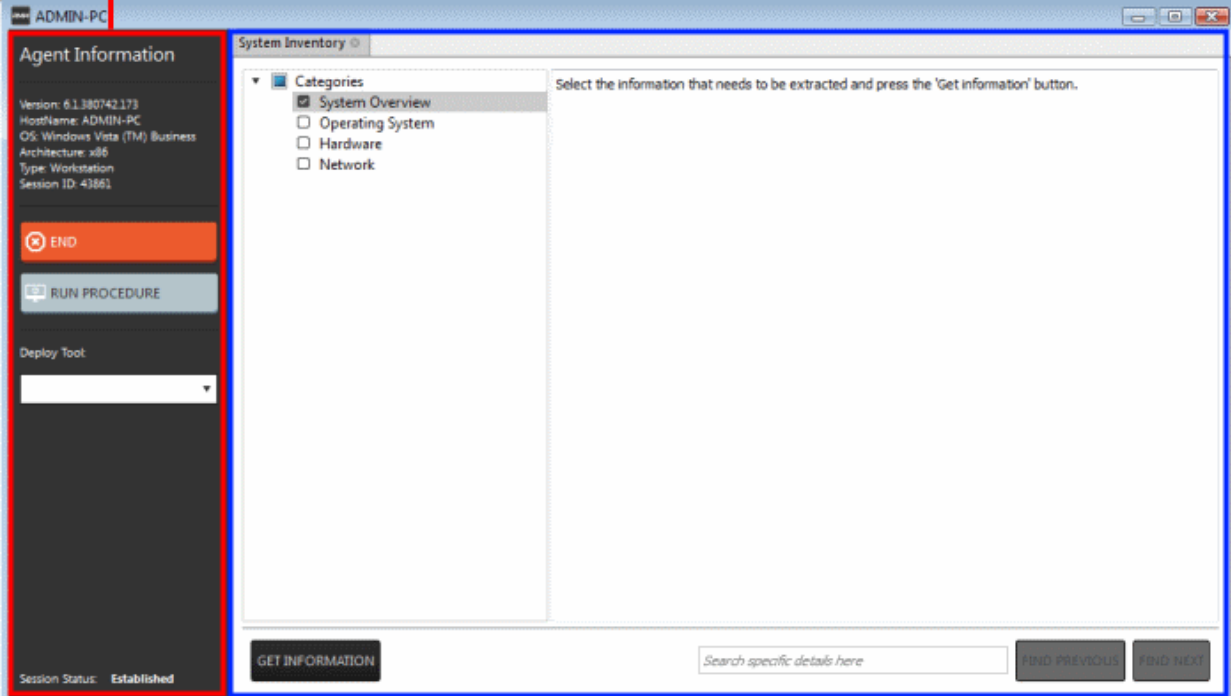
The Support Sessions Console has a streamlined interface that provides fingertip access and control over all the features and functions of the service.

The left hand side of the interface contains the sessions area which contains the controls for transferring a session, running procedures and a list of tools for use in providing support. The deploy tools drop-down, which contains a set of diagnostic tools that can be deployed on a remote computer. These utilities are an invaluable resource when troubleshooting issues on a client computer.

Left Hand Side Navigation - The left hand side navigation contains controls and buttons for various tasks like running a procedure, deploying tools on to the endpoint to perform various actions and audits, transfer the support session to other clients and so on.

- **END** - Concludes the support session and closes the session window for the endpoint.

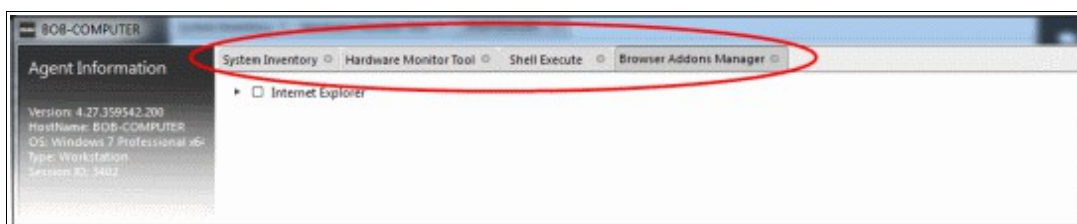
Left Hand Side Navigation – Contains controls for running procedures, transferring the session and a list of tools for use in providing support and auditing the endpoint



Main Configuration and Information Area
Each tool deployed on to the endpoint opens a new tab. The configuration/information screen for the tool is displayed under the respective tab

- **RUN PROCEDURE** -Allows you to run procedures on the endpoint. You can select procedures from those that are available in the 'Procedures' interface. Refer to the section '**Running Procedures from Support Sessions Interface**' for more details.
- **Deploy Tool** - Allows you to select tools for performing various tasks such as system cleaning, power management, system restore and so on. Refer to the section '**Using RMM Tools**' for more details

Main Configuration and Information Area - The main configuration and information area displays the configuration screens for the tools selected from the 'Deploy Tool' drop-down.



5.2 Handle Support Sessions

The support sessions interface allows admins to accept support requests from customers through emails or service

desk requests. By establishing a support session you can:

- Take remote desktop control of the client computer
- Perform actions like cleaning the client's computer, power management, system restore, file transfer, system inventory audit and so on.

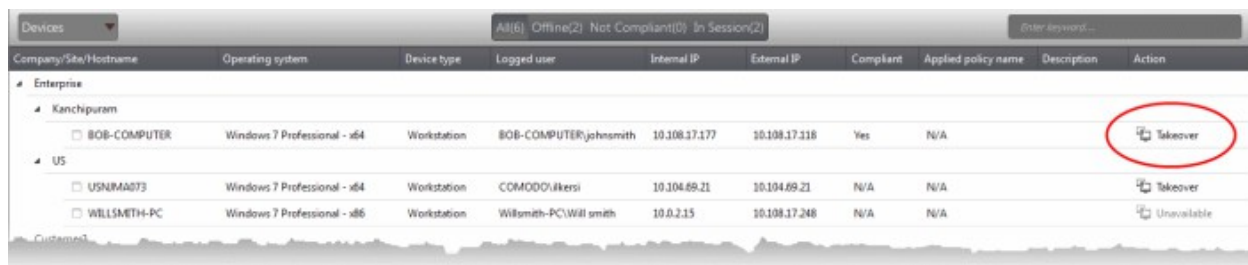
A support session can be initiated from the RMM admin console. Refer to the section '**Initiating a support session from the RMM admin console**' for more details.

Initiating a support session from the RMM admin console

If you require to perform a maintenance operation or run procedures you can initiate the session by clicking 'Takeover' from the 'Devices' interface.

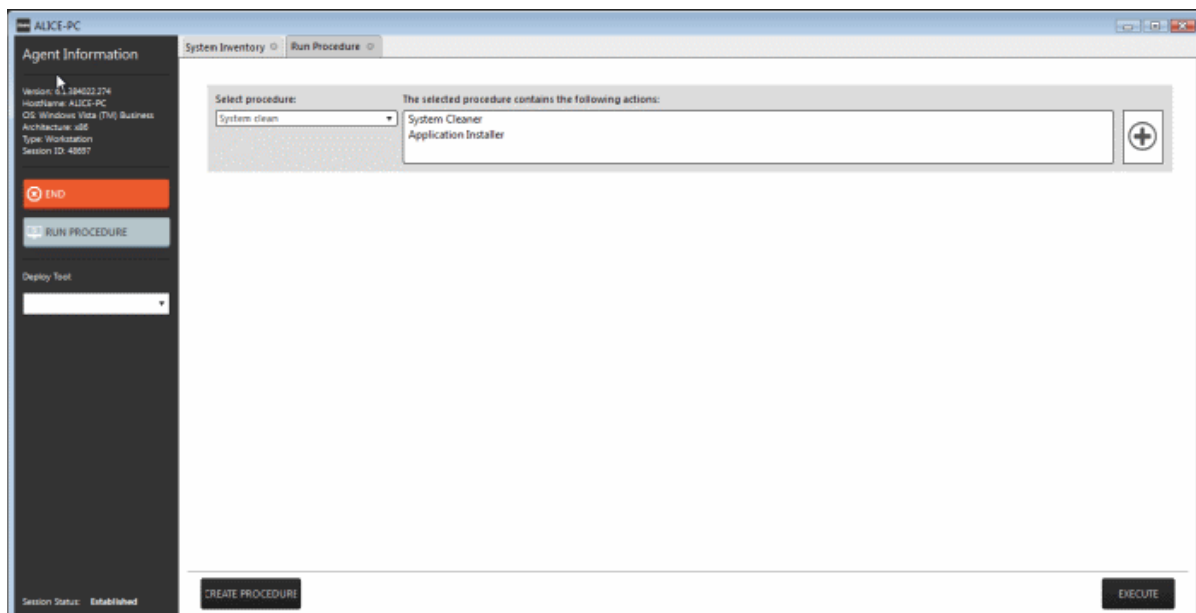
To start a support session

- Open the 'Devices' interface by choosing 'Devices' from the drop-down at the top-left

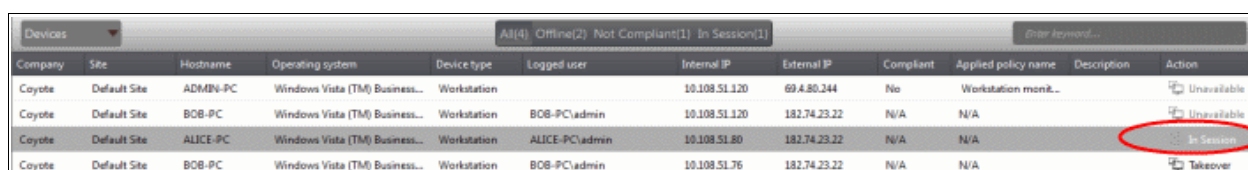


- Click 'Take Over' under 'Action' in the row of the device (endpoint) to which the support session is to be started.

A session will be established.



Now, the action will have the status 'In_session' that indicates that the session is taken over and will be available in the 'Devices' and the 'Sessions' screens.



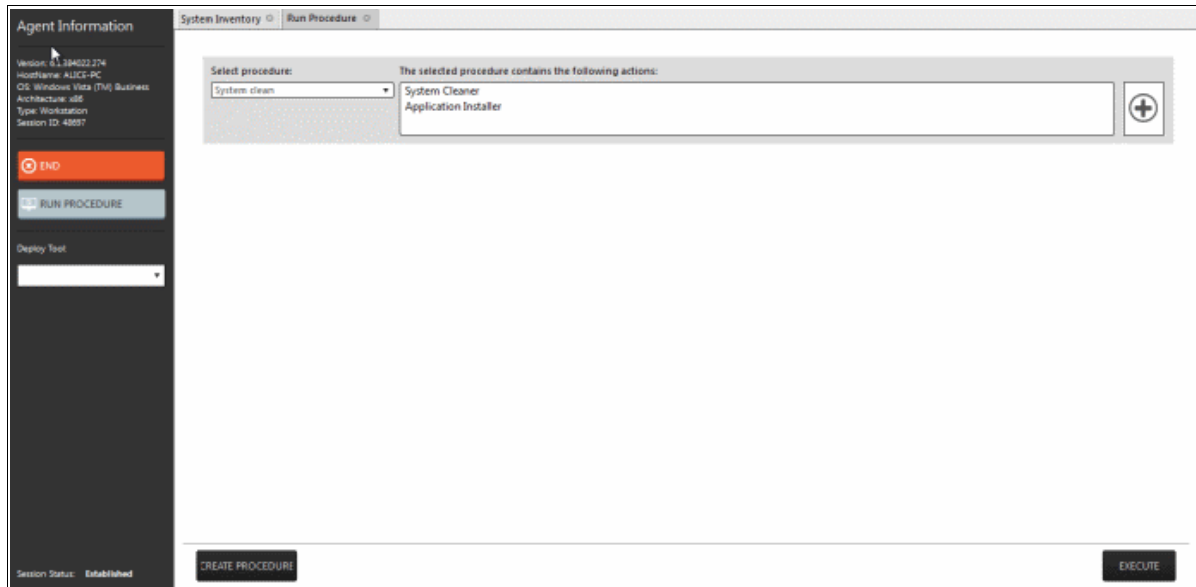
The Support Session Interface

Refer to the section '[Support Sessions Interfaces - An Overview](#)' for more details about the interface.

- To conclude a support session and close the session window, click the 'End' button

Refer to the following sections for more details about:

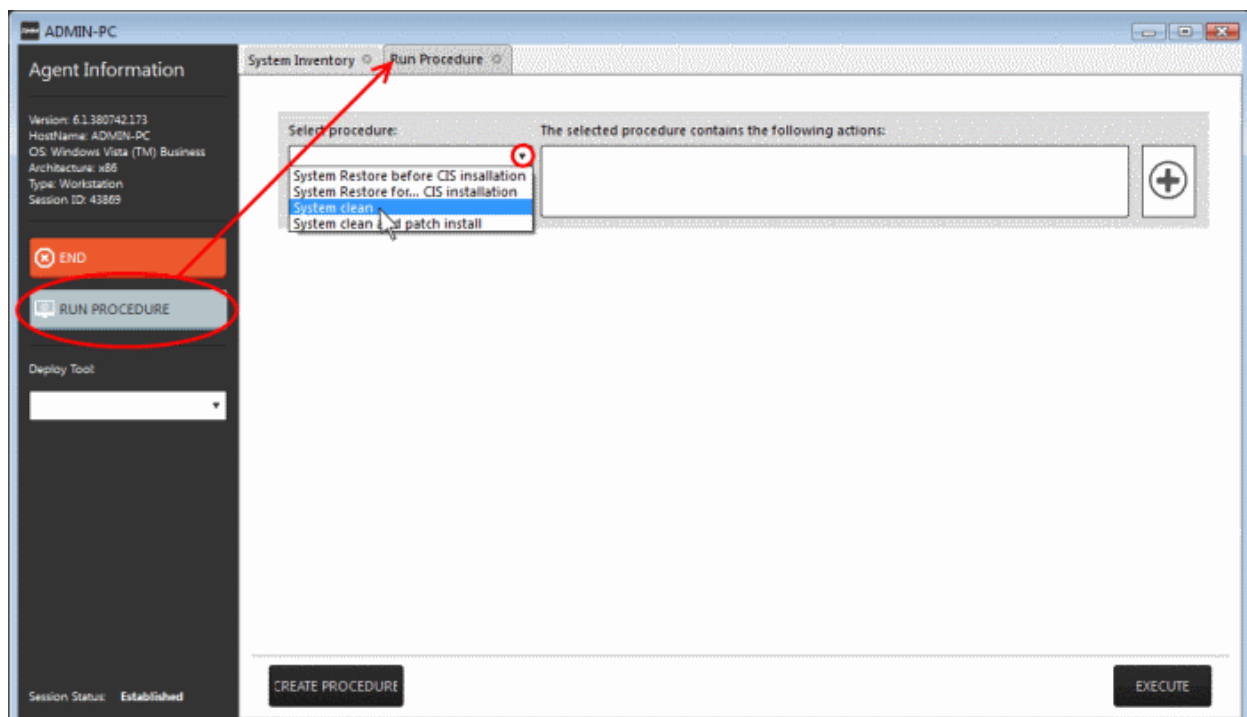
- [Run a Procedure](#)
- [Using RMM Tools](#)



5.2.1 Run Procedures from a Support Session

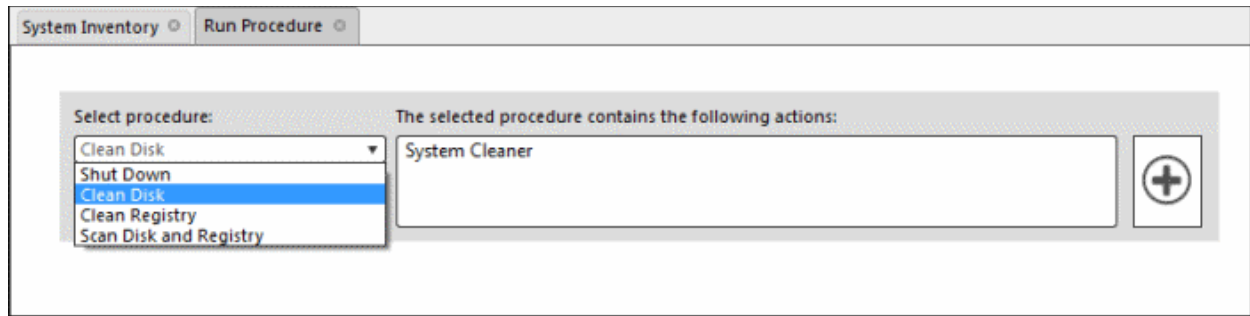
'Procedures' that are created in '[The Procedures Interface](#)' can be executed on an endpoint from the support session interface. A 'Procedure' is a set of predefined actions that can be run on endpoints. For example, you can execute Disk and Registry clean-up, enable/disable Windows Processes, manage System Restore points, configure power management, install third-party applications and so on. Refer to the section '[Managing Procedures](#)' for more details about creating a new procedure.

To run a procedure from the 'Support Sessions' interface, click the 'Run Procedure' button on the left



A new 'Run Procedure' tab will open in the main configuration area.


- Click the 'Select procedure' drop-down



The drop-down will display available procedures. Refer to the section '[Managing Procedures](#)' for more details about creating a new procedure.

- Select the procedure that you want to run on the endpoint

The sequence of actions contained in the chosen procedure will be displayed in the list at the right.

- Repeat the process to add more procedures by clicking the  button on the right
- Click the 'Execute' button at the bottom

A job will be created with the list of selected procedures for the endpoint and will be executed in sequence. The 'Run Procedure' tab will no longer be available in the support session interface after the procedure is executed. Refer to the section '[The Jobs Interface](#)' for more details about jobs.

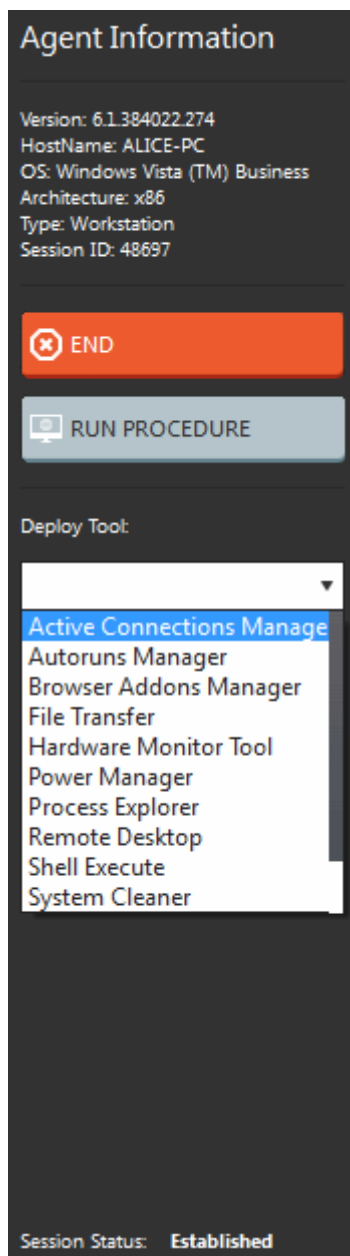
Tip: You can add new procedures from this interface too by clicking the 'Create Procedure' button at the bottom of the interface. Refer to the section '[Managing Procedures](#)' for more details.

5.2.2 Use RMM Tools

CRMM ships with a set of handy diagnostic and repair tools that allow admins to quickly analyze and run fixes on an endpoint. For example, you can view all running processes, kill unnecessary processes, access the command line interface of the endpoint, run system clean operations and so on. The support session window allows you to deploy any number of tools onto the endpoint. Each tool opens a new tab in the main configuration area and displays options and results pertaining to the tool.

To deploy a tool

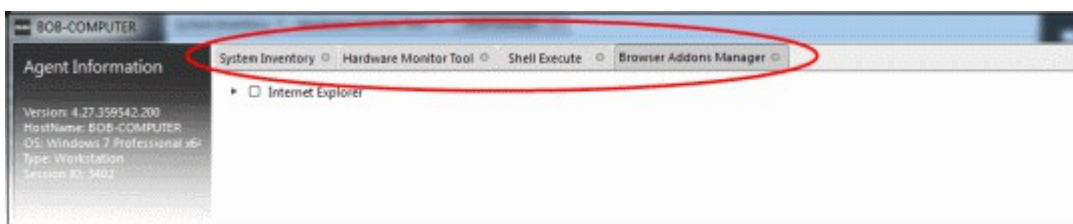
- Click on the 'Deploy Tool' drop-down from the support sessions interface



- Choose the tool that you want to deploy on the endpoint in session from the drop-down

Tip: You can choose several tools concurrently from the drop-down to be deployed on to the endpoint

The selected tools will be available as separate tabs in the main configuration area and each tab displays options and results pertaining to the tool.



- Click on a tab to open the tool page to view the tool options.

The following sections provide detailed explanations on the available tools:

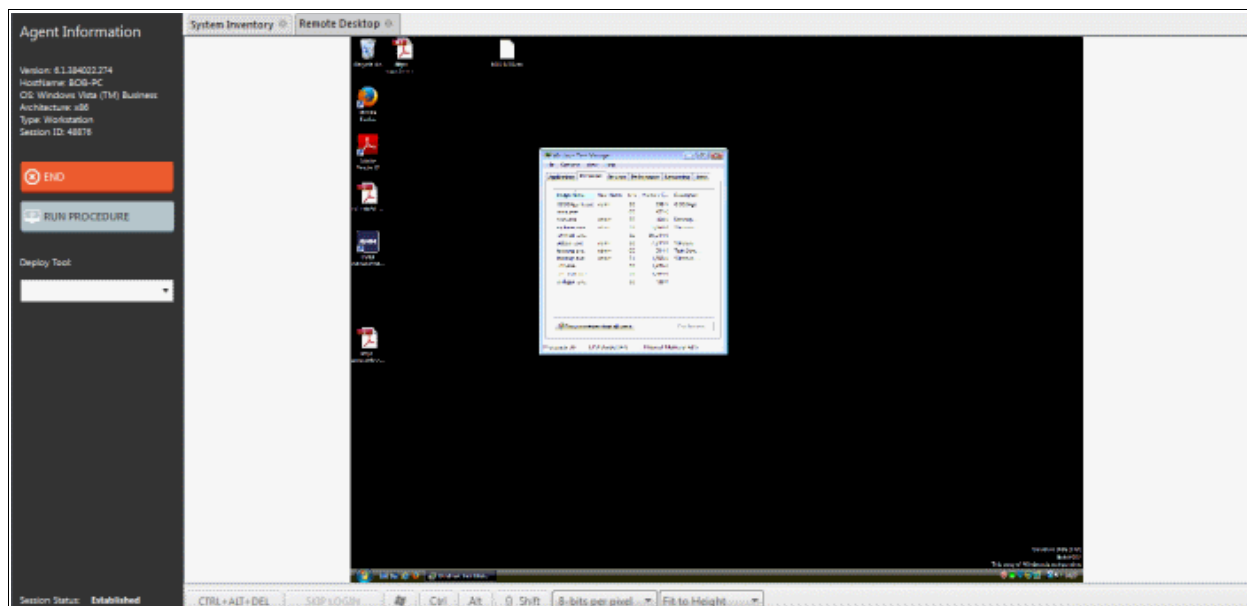
- Remote Desktop
- Autoruns Manager
- System Cleaner
- Power Manager
- Browser Add-Ons Manager
- Active Connections Manager
- System Restore
- Hardware Monitoring Tool
- Shell Execute
- Process Explorer
- System Inventory
- File Transfer

5.2.2.1 Access Endpoints through Remote Desktop Connection

RMM allows you to gain remote desktop access to the endpoint and execute necessary actions to solve issues. During the time that you are working with the endpoint, the end-user can view the actions taken by you and can operate the computer if required.

To initiate a remote desktop connection

- Select 'Remote Desktop' from the 'Deploy Tool' drop-down on the left



The desktop of the endpoint will open in a new 'Remote Desktop' tab in the main configuration area. You can take all the necessary measures to rectify the problems in the endpoint.

5.2.2.2 Manage Autoruns

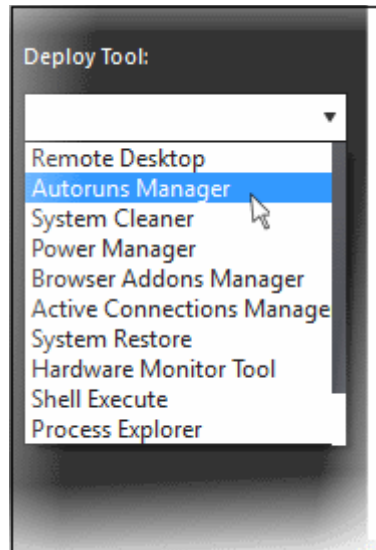
The Autoruns Manager tool allows admins to view and edit endpoint start-up items which are loaded when the system boots-up. Unnecessary start-up items can hog system resources and lead to the system becoming sluggish or unresponsive.

Start-up items can also have a significant impact on the security of the computer. Some forms of malware will add a start-up item to run in the background which facilitates the execution of key loggers, rootkits, buffer overflows and

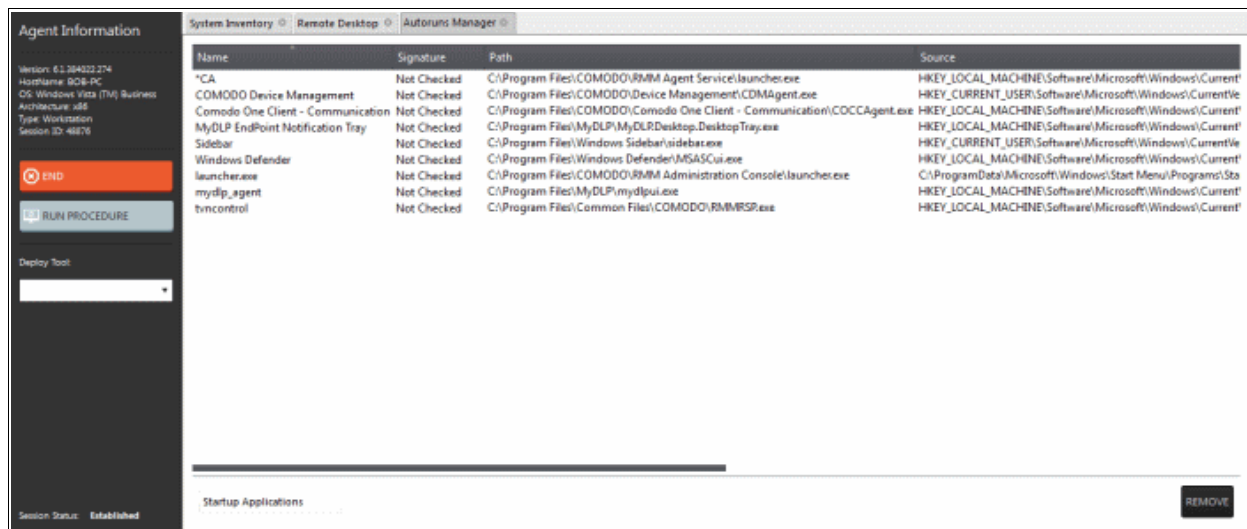
Denial of Service (DoS) attacks.

To deploy the Autoruns Manager tool

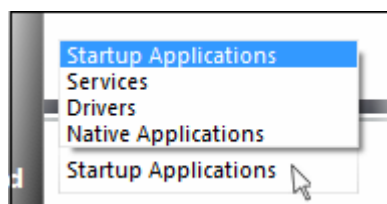
- Select 'Remote Desktop' from the 'Deploy Tool' drop-down on the left



A new 'Autoruns Manager' tab will be created in the main configuration area.



Select the category of the start-up item from the drop-down at the bottom:



- **Startup Applications** - Displays the autorun items identified from standard autostart locations such as the Startup folder for all users, the Registry Run keys, and standard application launch locations.
- **Services** - Displays the modules loaded as Windows Services.
- **Drivers** - Displays the kernel-mode drivers that are in currently enabled on the system.
- **Native Applications** - Displays the native system applications that

are currently running on the system.

Startup Applications

Selecting 'Startup applications' displays the autorun items identified from standard autostart locations such as the Startup folder for all users, the Registry Run keys, and standard application launch locations, whether they are digitally signed, the path and source of the application.

Name	Signature	Path	Source
*CA	Signed	C:\Program Files (x86)\Comodo\RMM Agent\launcher.exe	HKEY_LOCAL...
GoogleChromeAutoLaunch_361C1DD22E1256C6B68316A32E8B1949	Signed	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	HKEY_CURR...
launcher.exe	Signed	C:\Program Files (x86)\Comodo\RMM Agent\launcher.exe	C:\Program[...
tvncontrol	Signed	C:\Program Files (x86)\Common Files\COMODO\RMMRSP.exe	HKEY_LOCA...

Startup Applications REMOVE

- To remove a startup application, select it and click the 'Remove' button at the bottom. The selected item will be removed only from the startup item. The user will be able to run the application manually in future.

Services

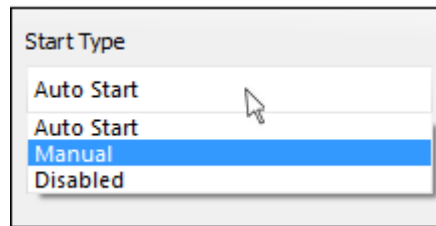
Selecting 'Services' applications displays Windows Services that are currently loaded in to the system with their current running status, whether the service is digitally signed and the path of the application.

Name	Status	Signature	Path	Start Type
ALG	Stopped	Not Found	C:\Windows\System32\alg.exe	Auto Start
AeLookupSvc	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
AppIDSvc	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
AppMgmt	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
Appinfo	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
AudioEndpointBuilder	Running	Not Signed	C:\Windows\System32\svchost.exe	
AudioSrv	Running	Not Signed	C:\Windows\System32\svchost.exe	
AxInstSV	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
BDESVC	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
BFE	Running	Not Signed	C:\Windows\System32\svchost.exe	
BITS	Running	Not Signed	C:\Windows\System32\svchost.exe	
Browser	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
CLPSLauncher	Running	Signed	C:\Program Files (x86)\Common Files\COMODO\launch	
COMSysApp	Stopped	Not Signed	C:\Windows\System32\dllhost.exe	
CertPropSvc	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
CryptSvc	Running	Not Signed	C:\Windows\System32\svchost.exe	
CscService	Running	Not Signed	C:\Windows\System32\svchost.exe	
DPS	Running	Not Signed	C:\Windows\System32\svchost.exe	
DcomLaunch	Running	Not Signed	C:\Windows\System32\svchost.exe	
Dhcp	Running	Not Signed	C:\Windows\System32\svchost.exe	
Dnscache	Running	Not Signed	C:\Windows\System32\svchost.exe	
EFS	Stopped	Not Found	C:\Windows\System32\lsass.exe	
EapHost	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
EventSystem	Running	Not Signed	C:\Windows\System32\svchost.exe	
FDResPub	Running	Not Signed	C:\Windows\System32\svchost.exe	
Fax	Stopped	Not Found	C:\Windows\system32\fxssvc.exe	
FontCache	Running	Not Signed	C:\Windows\System32\svchost.exe	
FontCache3.0.0.0	Stopped	Signed	C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\Pre:	
HomeGroupListener	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
HomeGroupProvider	Stopped	Not Signed	C:\Windows\System32\svchost.exe	
IEEtwCollectorService	Stopped	Not Found	C:\Windows\system32\IEEtwCollector.exe	

Services STOP PAUSE UNINSTALL APPLY

- To view the start type of a service, select it and the 'Start Type' drop-down displays its status
- To totally remove a service from the computer, select it and click 'Uninstall'

- To stop a running service, select it and click 'Stop'
- To restart a stopped service, select it and click 'Start'
- To change how a service should start, select it, choose the option from the 'Start Type' drop-down and click 'Apply'.



Drivers

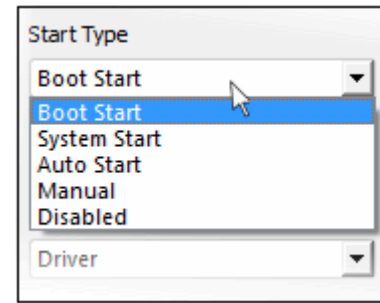
Selecting Drivers displays the device drivers that are currently loaded into the system with their current running status and whether the driver is digitally signed.

The screenshot shows the 'Autoruns Manager' application window. It features a table with columns for Name, Status, Signature, and Action State. A right-hand sidebar contains settings for Start Type, Error, and Type. At the bottom, there are buttons for STOP, UNINSTALL, and APPLY, and a search box labeled 'Drivers'.

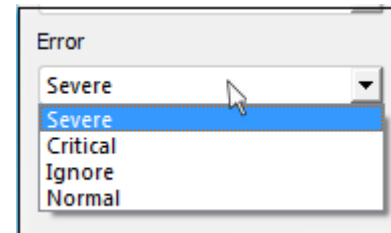
Name	Status	Signature	Action State
1394ohci	Stopped	Not Found	
ACPI	Running	Not Found	
AFD	Running	Not Found	
AcpiPmi	Stopped	Not Found	
AmdK8	Stopped	Not Found	
AmdPPM	Stopped	Not Found	
AppID	Stopped	Not Found	
AsyncMac	Running	Not Found	
BTHMODEM	Stopped	Not Found	
Beep	Running	Not Found	
BrFiltLo	Stopped	Not Found	
BrFiltUp	Stopped	Not Found	
BrSerWdm	Stopped	Not Found	
BrUsbMdm	Stopped	Not Found	
BrUsbSer	Stopped	Not Found	
Brserid	Stopped	Not Found	
CLFS	Running	Not Found	
CNG	Running	Not Found	
CSC	Running	Not Found	
CmBatt	Running	Not Found	
Compbatt	Running	Not Found	
CompositeBus	Running	Not Found	
DXGKrnI	Stopped	Not Found	
DfsC	Running	Not Found	
Disk	Running	Not Found	
E1G60	Running	Not Found	
ErrDev	Stopped	Not Found	
FileInfo	Running	Not Found	
Filetrace	Stopped	Not Found	
FltMgr	Running	Not Found	
FsDepends	Stopped	Not Found	
HDAudioBus	Stopped	Not Found	

- To remove a driver from the system, select it and click 'Uninstall'
- To start/stop a driver, select it and click the 'Start/Stop' button

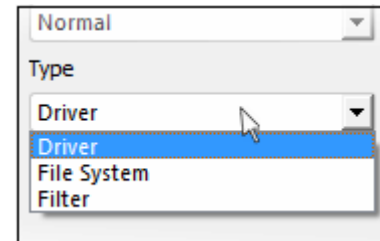
To change the way a driver should start, select it and choose the option from the 'Start Type' drop-down



To change the error severity of a driver, select it and choose the option from 'Error' drop-down



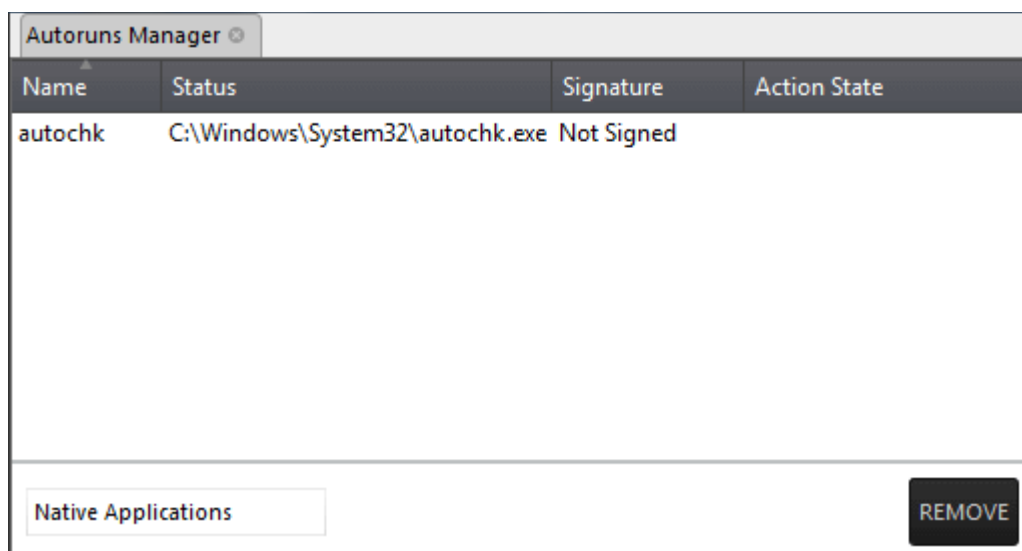
To change the file type of a driver, select it and choose the option from the 'Type' drop-down



- Click 'Apply' for your changes to take effect

Native Applications

Selecting Native Applications displays the native system applications currently loaded into the system.



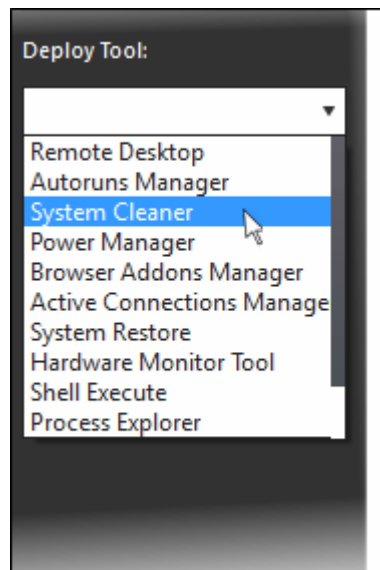
- To remove an application, select the item and click 'Remove'.

5.2.2.3 System Cleaner

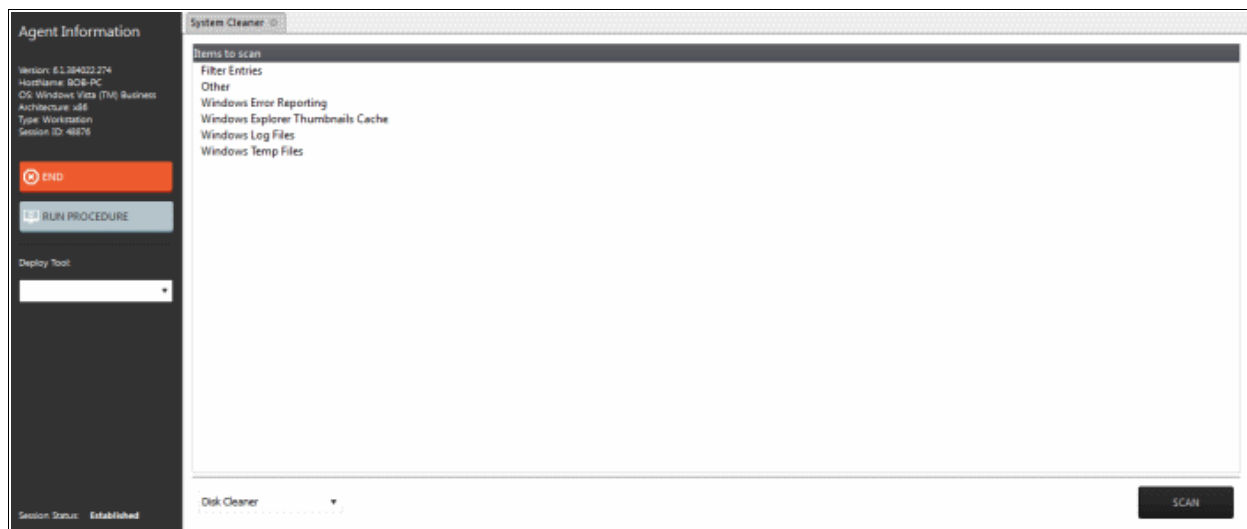
The System Cleaner tool allows admins to improve the security, performance and usability of systems of damaging and/or wasteful files which generally enhances the performance of the system. It optimizes and repairs your Windows registry and erases your digital paper trail by cleaning history, cache, cookies, needless archives.

To run the System Cleaner

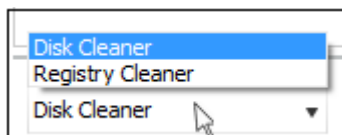
- Select 'System Cleaner' from the 'Deploy Tool' drop-down on the left



A new 'System Cleaner' tab will be created in the main configuration area.



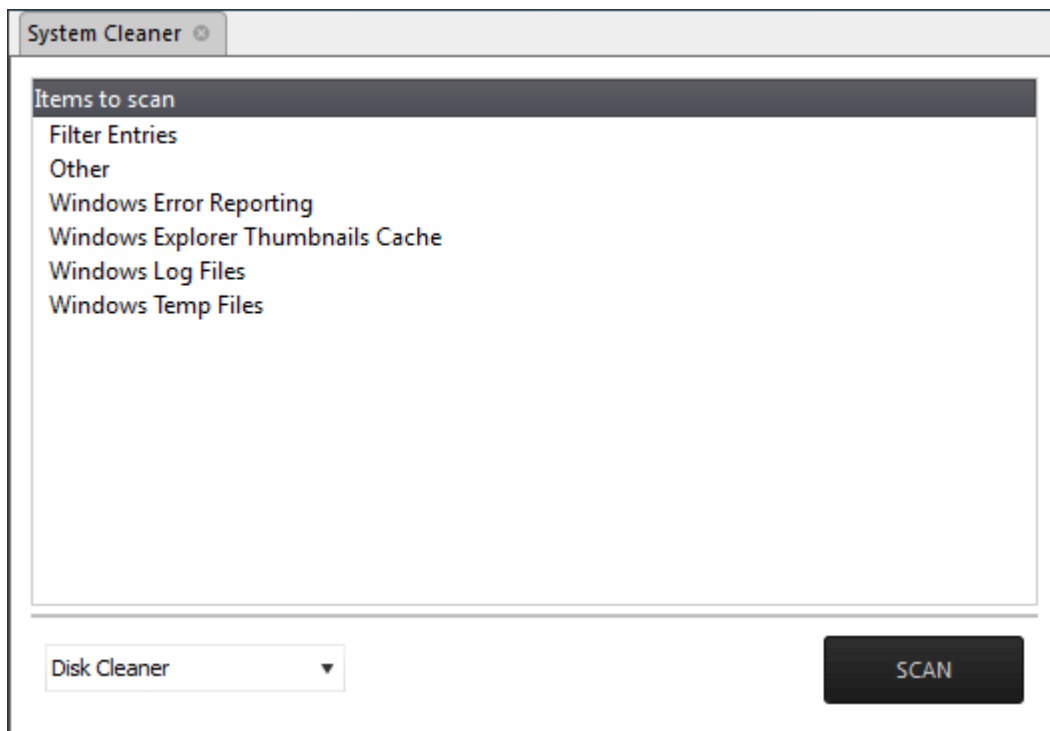
- Select the category of the clean-up task from the drop-down at the bottom:



- **Disk Cleaner** - Scans and removes junk or garbage files, potentially unwanted files from a computer. (temporary files, trash, old backups and web caches, local shared objects, log files or any other trace and so on).
- **Registry Cleaner** - Cleans and repairs Windows registry by scanning and removing unnecessary and corrupted entries to increase the performance and stability boost.

Disk Cleaner

Selecting 'Disk cleaner ' displays the list of items to be scanned such as Filter Entries, Windows Error Reporting and so on.



- Select the items to be scanned
- Click 'Scan'

The scanner will start and identify the files to be cleaned.

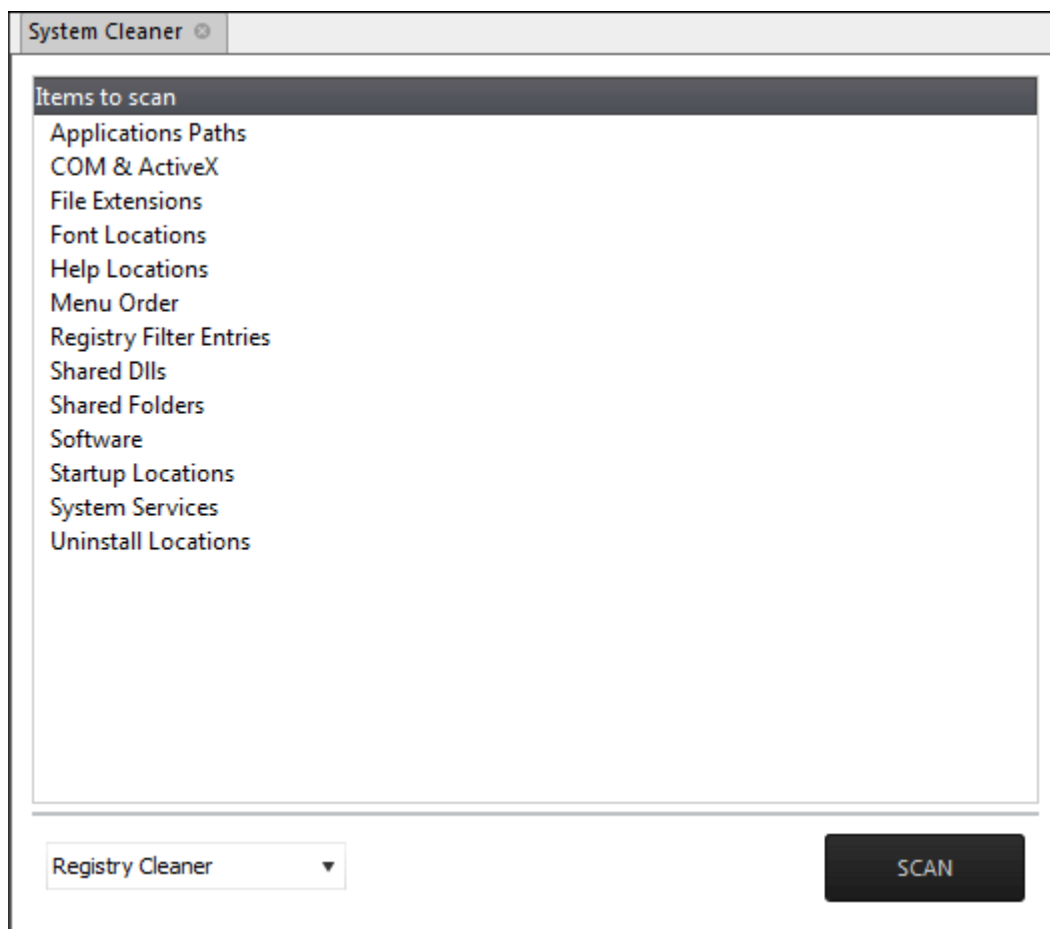
- Click 'Back' to select the new item(s) to be scanned.
- Click 'Clean' to remove junk files.



The scanner will remove the junk files. Click 'OK' to return to the 'Disk Cleaner' screen.

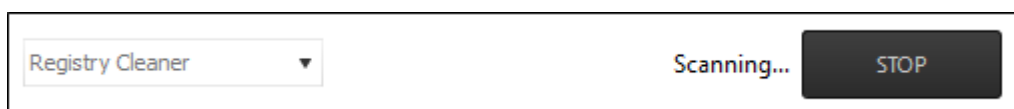
Registry Cleaner

Selecting 'Registry Cleaner' from drop-down displays the items that might maintain invalid entries.



- Select the item to be scanned
- Click 'Scan'

The scanning process will start.



- Click 'Stop' to abort the scan process.



- Click 'Back' to select the new item(s) to be scanned
- Click 'Clean' to remove invalid entries

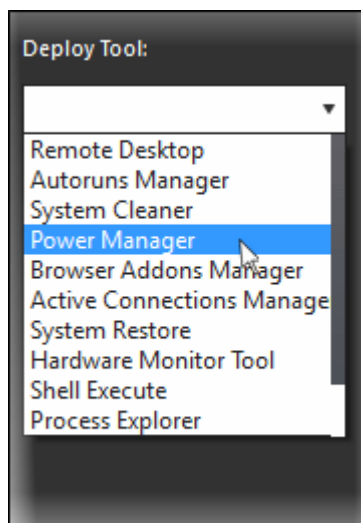
The scanner will remove the junk entries. Click 'OK' to return to the 'Registry Cleaner' screen.

5.2.2.4 Power Management

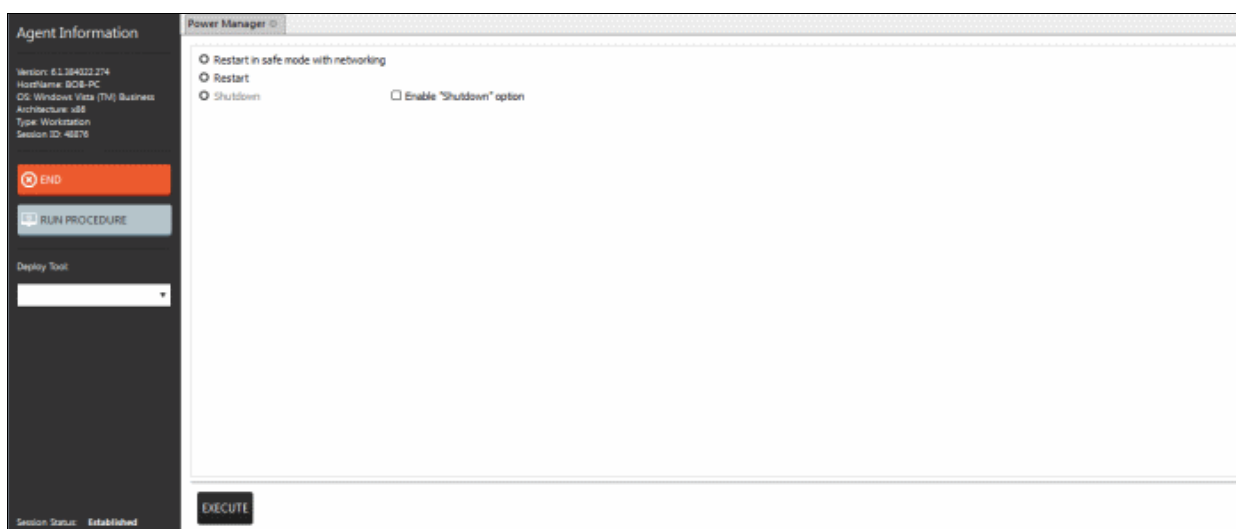
The 'Power Manager' tool in the support session window enables the technician to shut down and restart an endpoint, if required after a critical operation like editing the Windows Registry of the client's computer.

To deploy the Power Manager tool

- Select 'Power Manager' from the 'Deploy Tool' drop-down on the left



A new 'Power Manager' tab will be created in the main configuration area.



Select the power-off option

- To reboot the endpoint in Safe Mode, select 'Restart in Safe Mode with networking'. Upon restarting, the endpoint will automatically reconnect to your support session.
- To reboot the endpoint, select 'Restart'. Upon restarting, the endpoint will automatically reconnect to your support session.
- To shutdown the endpoint, select 'Shutdown'. The Shutdown option is not enabled by default. If you need the option, first select the 'Enable Shutdown option' check box.
- Click the 'Execute' button at the bottom.

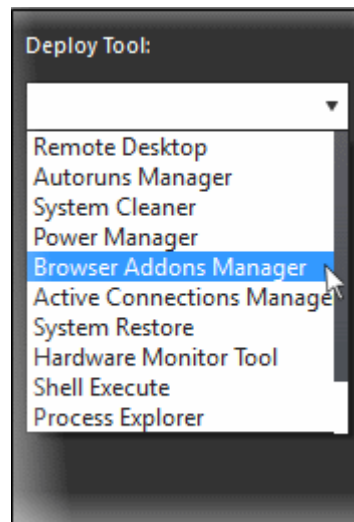
The power-off action as per your selection will be executed immediately.

5.2.2.5 Manage Internet Browser Add-ons

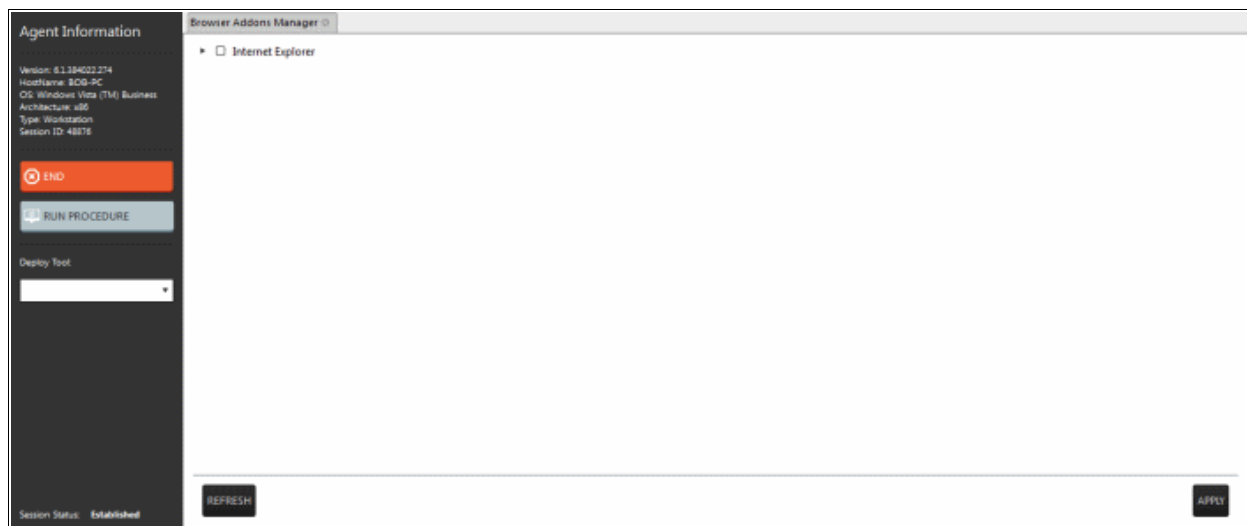
Some of the websites and program downloaded from Internet install browser extensions silently on to the browsers in the computers, without the knowledge of the user. These add-ons, like extensions, plug-ins and so on, can be used by hackers to execute malicious activities on the user computers, including stealing confidential and sensitive information like credit card numbers and passwords typed in the web-based forms. The 'Browser Addons Manager' tool in the support session console enables the admin to identify the browser add-ons installed on the browsers and to remove unsafe or malicious add-ons.

To deploy the Browser Addons Manager tool

- Select 'Power Manager' from the 'Deploy Tool' drop-down on the left

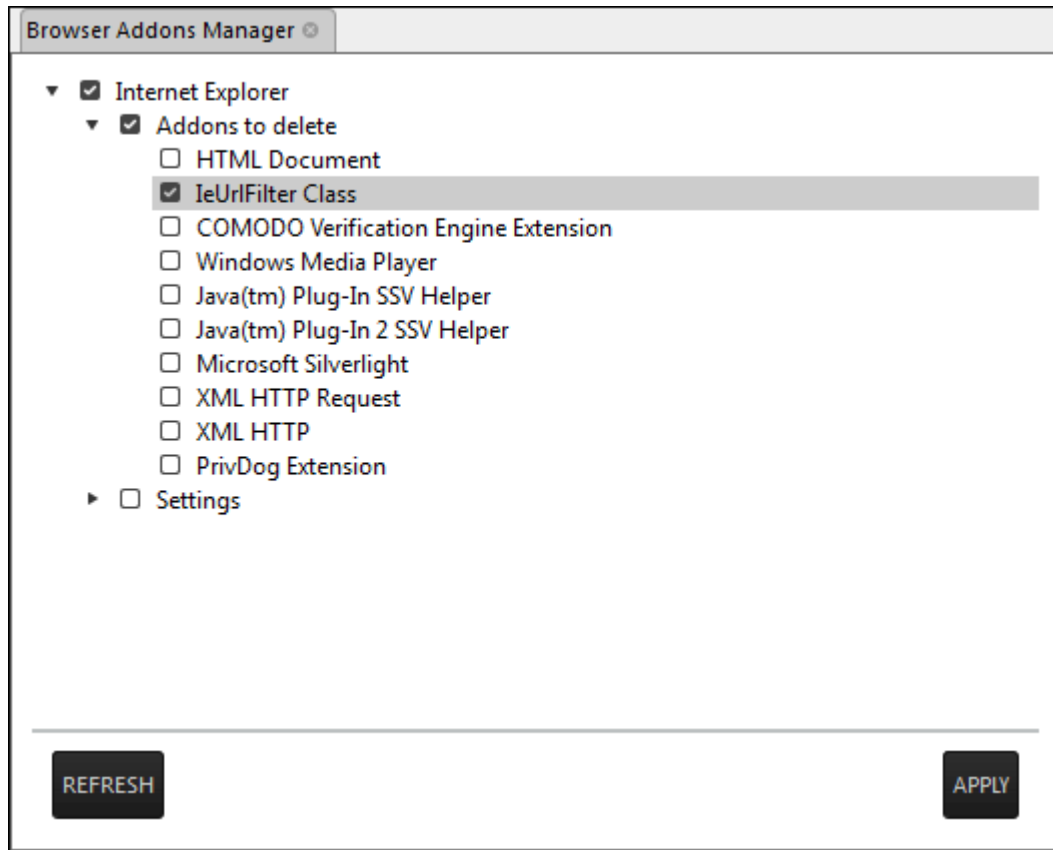


A new 'Browser Addons Manager' tab will be created in the main configuration area.

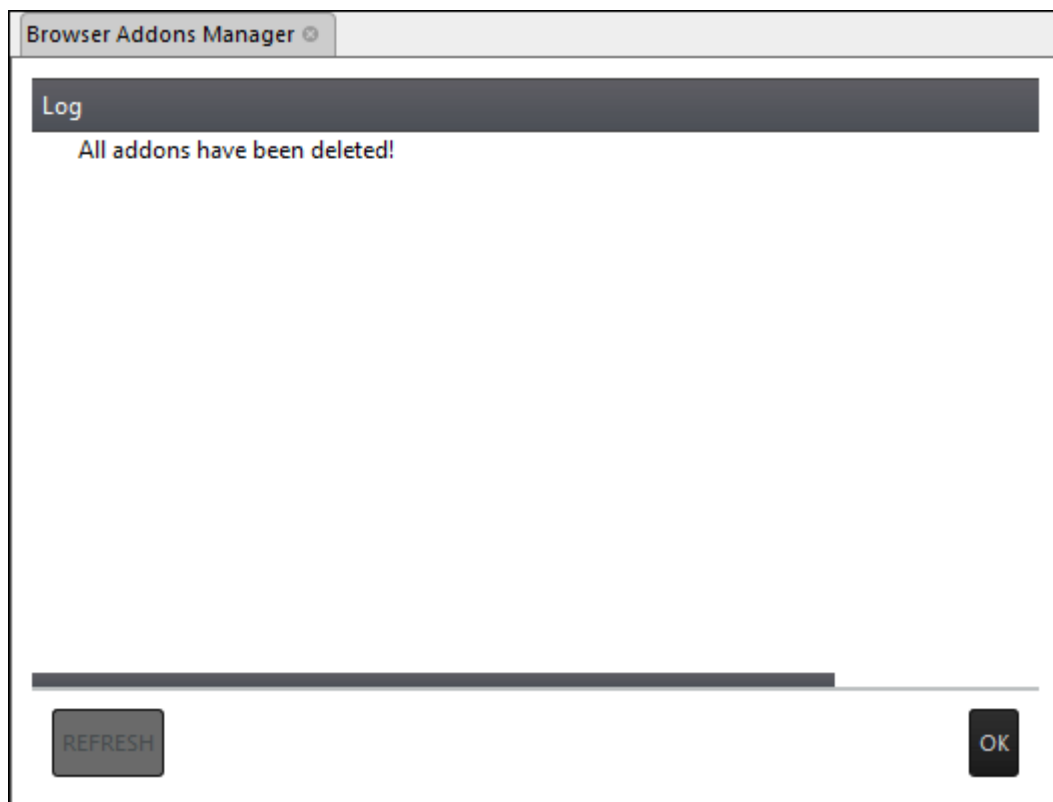


The tab will display all the browsers on the endpoint.

- Click on the ► beside a browser to expand it to a tree structure



- To remove a browser add-on(s), select the check boxes(s) beside them and click the 'Apply' button at the bottom



All the selected add-ons will be removed at-once from the endpoint.

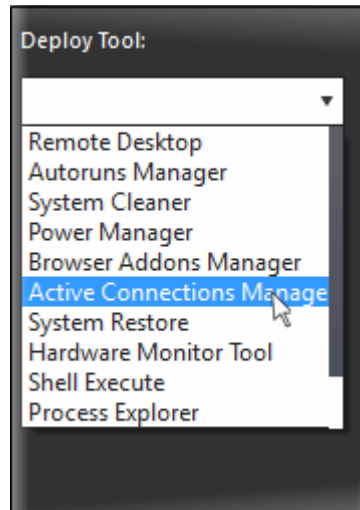
- Click 'OK' to switch back to the list of browser add-ons.

5.2.2.6 Active Connections Manager

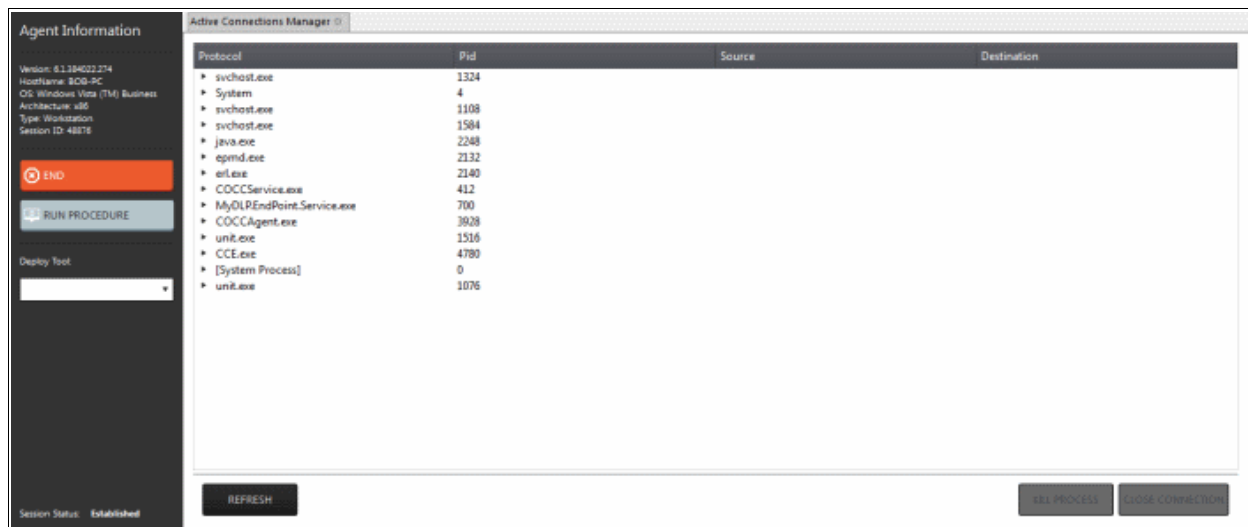
The 'Active Connection Manager' tool provides a high-performance solution for technicians to view all currently active connections (applications, processes and services), individual connections that each application is responsible for and terminate any unsafe processes that are running on an endpoint.

To manage active connections

- Select 'Active Connections Manager' from the 'Deploy Tool' drop-down on the left



A new 'Active Connections Manager' tab will be created in the main configuration area.



The tab will display all the active connections on the endpoint.

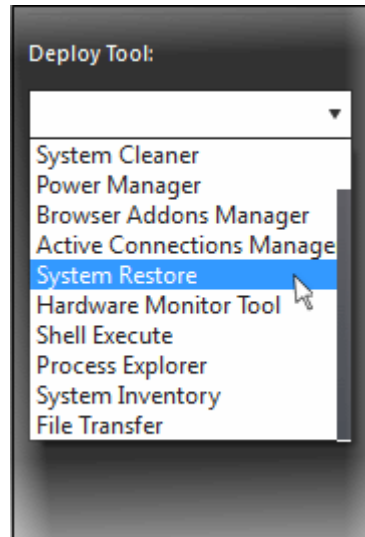
- Protocol - Displays a list of applications and system process that are running on the endpoint.
- Pid - Displays the Process Identification number of the processes invoked by the application.
- Source - Shows the source IP address and source port that the application is connecting through
- Destination - Shows destination port address that the application is connecting to.
- To close unsafe connections, select the connection to be closed and click the 'Close Connection'.
- To stop an active process, select the connection and click the 'Kill Process'.

5.2.2.7 Restore a Client System

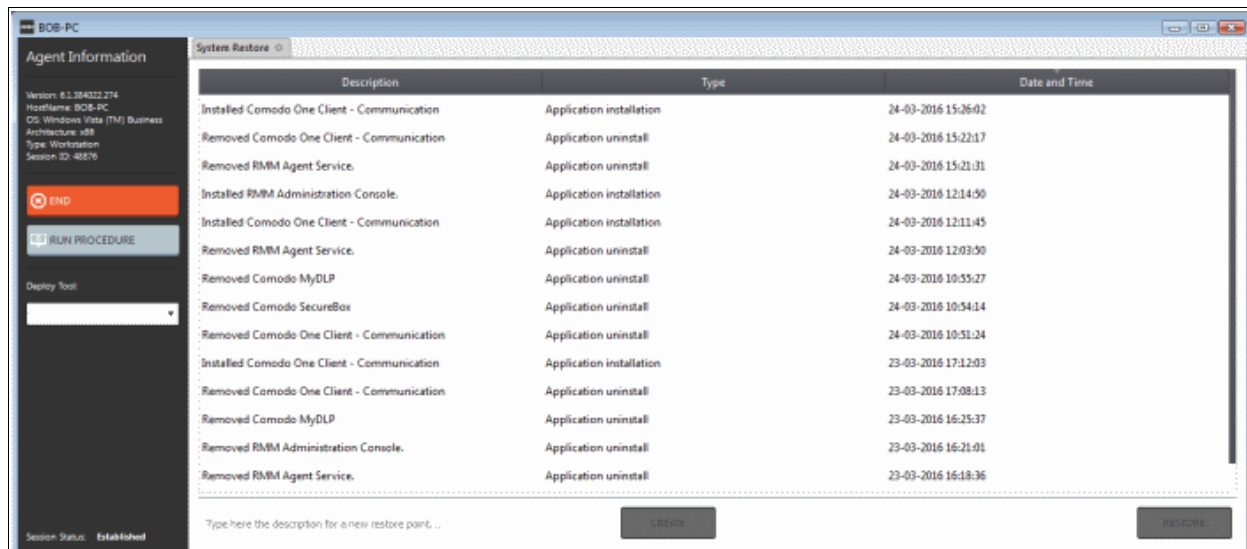
The 'System Restore' tool enables an admin to revert an endpoint to a previously created restore point (including system files, installed applications, Windows Registry, and system settings) and also create a new restore point for future use.

To create a 'System Restore' point

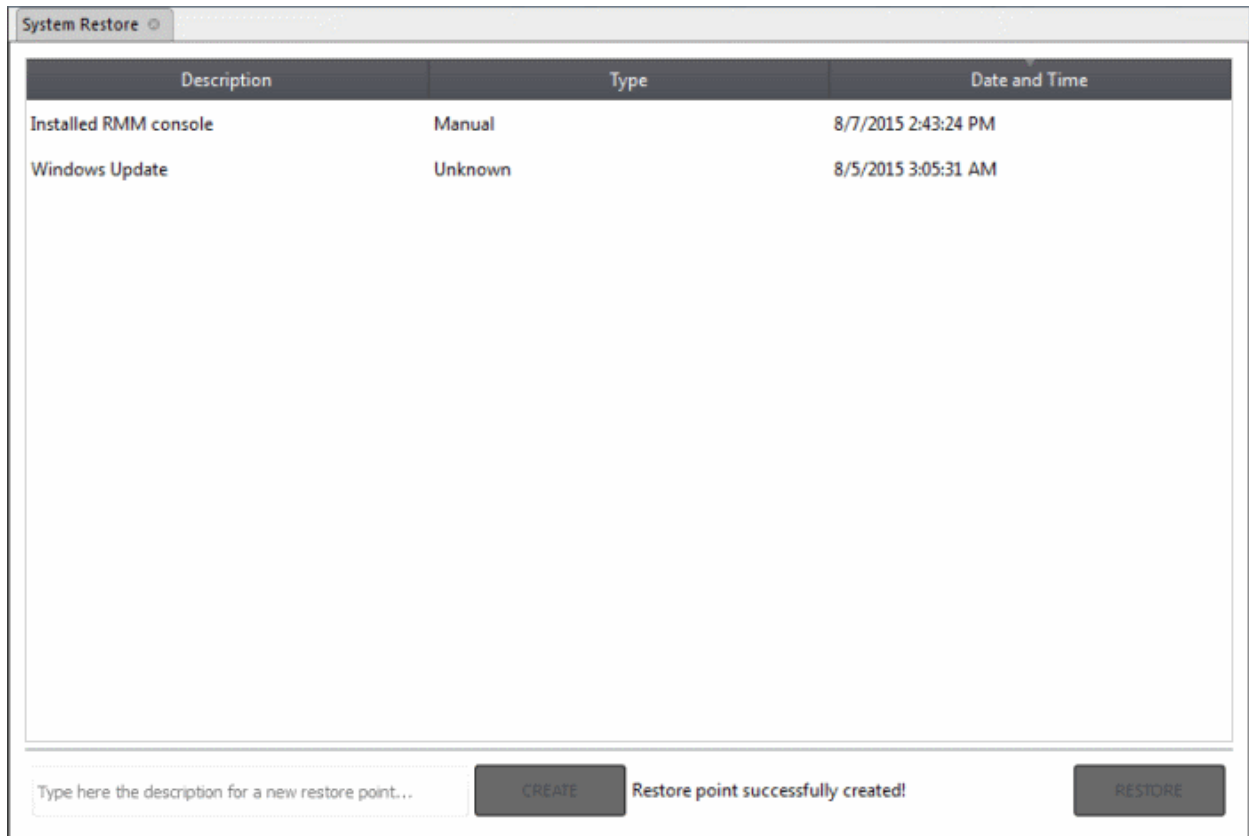
- Select 'System Restore' from the 'Deploy Tool' drop-down on the left



A new 'System Restore' tab opens in the main configuration area. From here you can create a restore point manually or restore system.



- Type a description of the restore point and click 'Create' to start the process. On successful completion, the newly created restore point will appear in the session window.



- To restore the endpoint to a previous point, select it from the list and click the 'Restore' button at the bottom

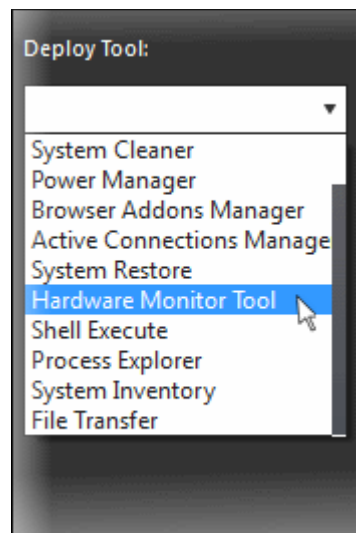
A system restore request will be sent to the endpoint and the system will be set to be restored. The user now can restore the system to the restore point selected by the admin.

5.2.2.8 Hardware Monitor Tool

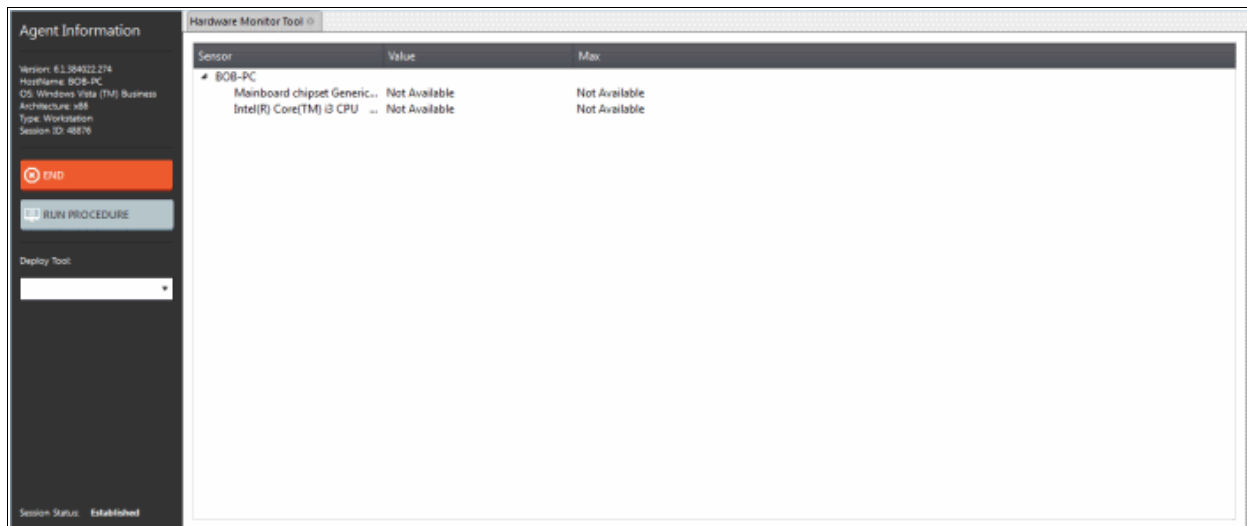
Hardware Monitor tool displays real time temperature of each processor core of CPU.

To monitor endpoint's hardware

- Select 'Hardware Monitor Tool' from the 'Deploy Tool' drop-down on the left



A new 'Hardware Monitor Tool' tab will be displayed in the main configuration area.



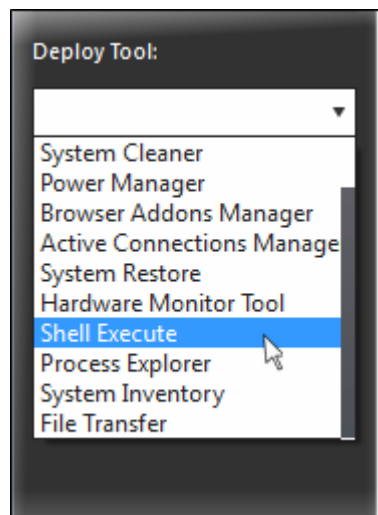
- **Sensor** - Displays the details of the endpoint's CPU
- **Value** - Real time temperature of a core in centigrade
- **Max** - The maximum temperature recorded for a core

5.2.2.9 Access Command Prompt Window of Client System

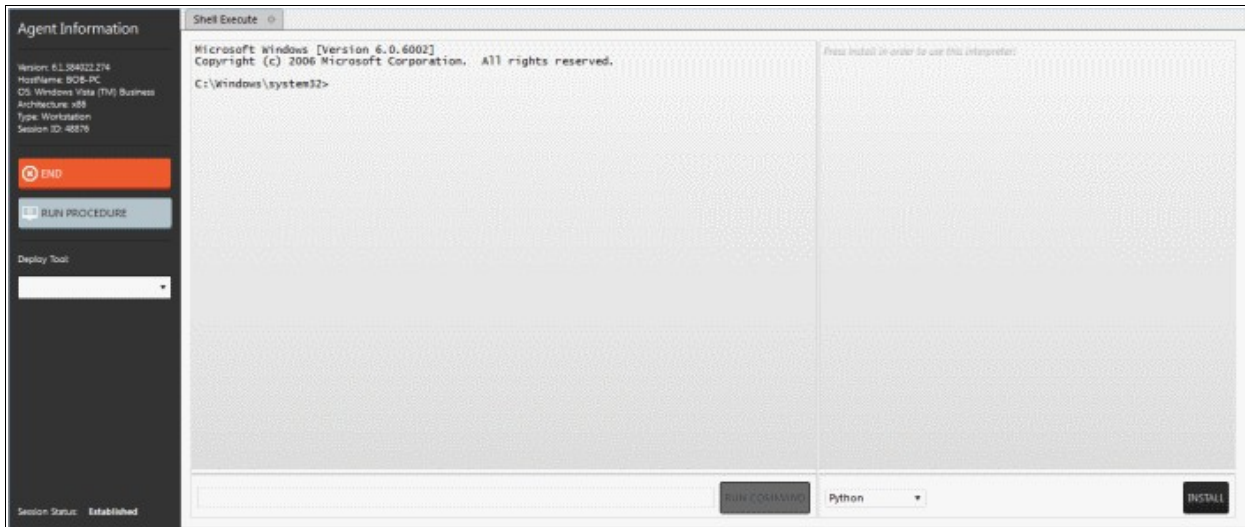
Highly infected computers would not allow the command prompt window to be opened in the computer to perform the corrective actions. But the 'Shell Execute' tool in the support session window allows an admin to open the command prompt window of the endpoint. The administrator can execute programs to cleanup and repair highly infected computers, from the command line through the Shell Execute tool.

To deploy the 'Shell Execute' tool

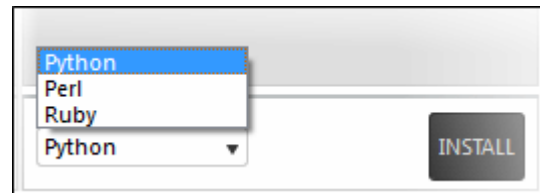
- Select 'Shell Execute' from the 'Deploy Tool' drop-down on the left



A new 'Shell Execute' tab opens in the main configuration area. From here you can install script languages and run the commands.



- To execute a Windows Shell command or a DOS command, type the command in the field beside 'Run command' and press 'Run command'.
- To run third-party scripts languages, select the scripts language from the drop-down



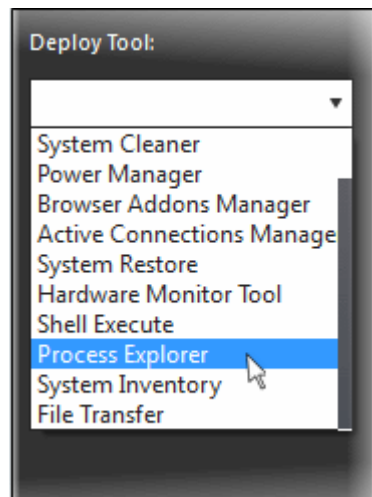
- Click 'Install' to install the language interpreter to interact with the operating system.

5.2.2.10 Manage Currently Running Processes

The 'Process Explorer' is an advanced system monitoring tool that allows admins to quickly identify, monitor and terminate any unsafe processes that are running on endpoints. The Process Explorer shows ALL running processes, even those triggered by malware in the computer and those that were invisible or very deeply hidden. The administrator can identify which of those running processes are unsafe and shut them down with a single click.

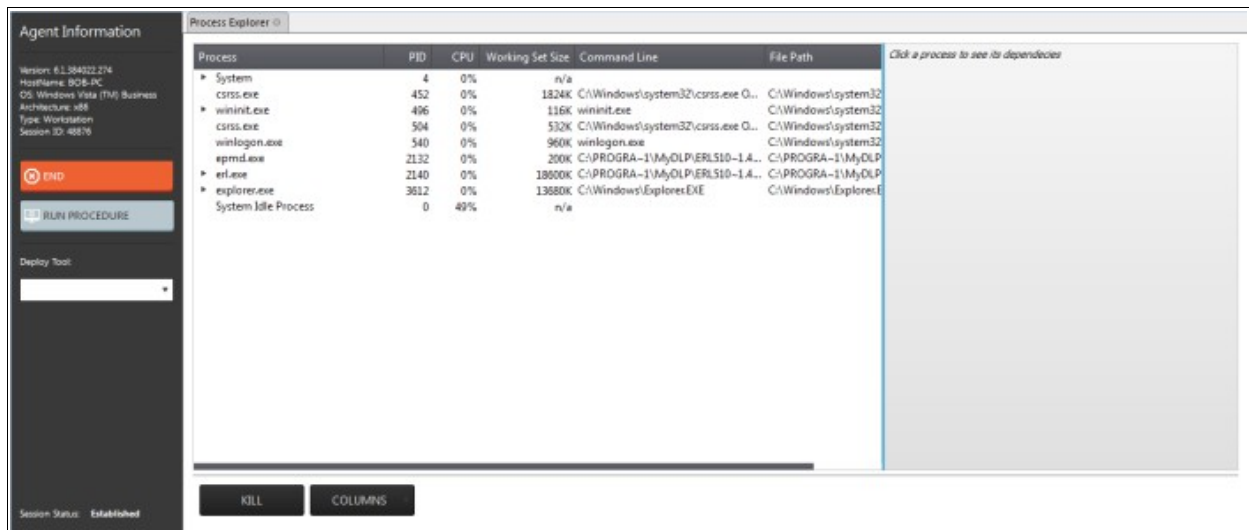
To deploy the 'Process Explorer' tool

- Select 'Process Explorer' from the 'Deploy Tool' drop-down on the left

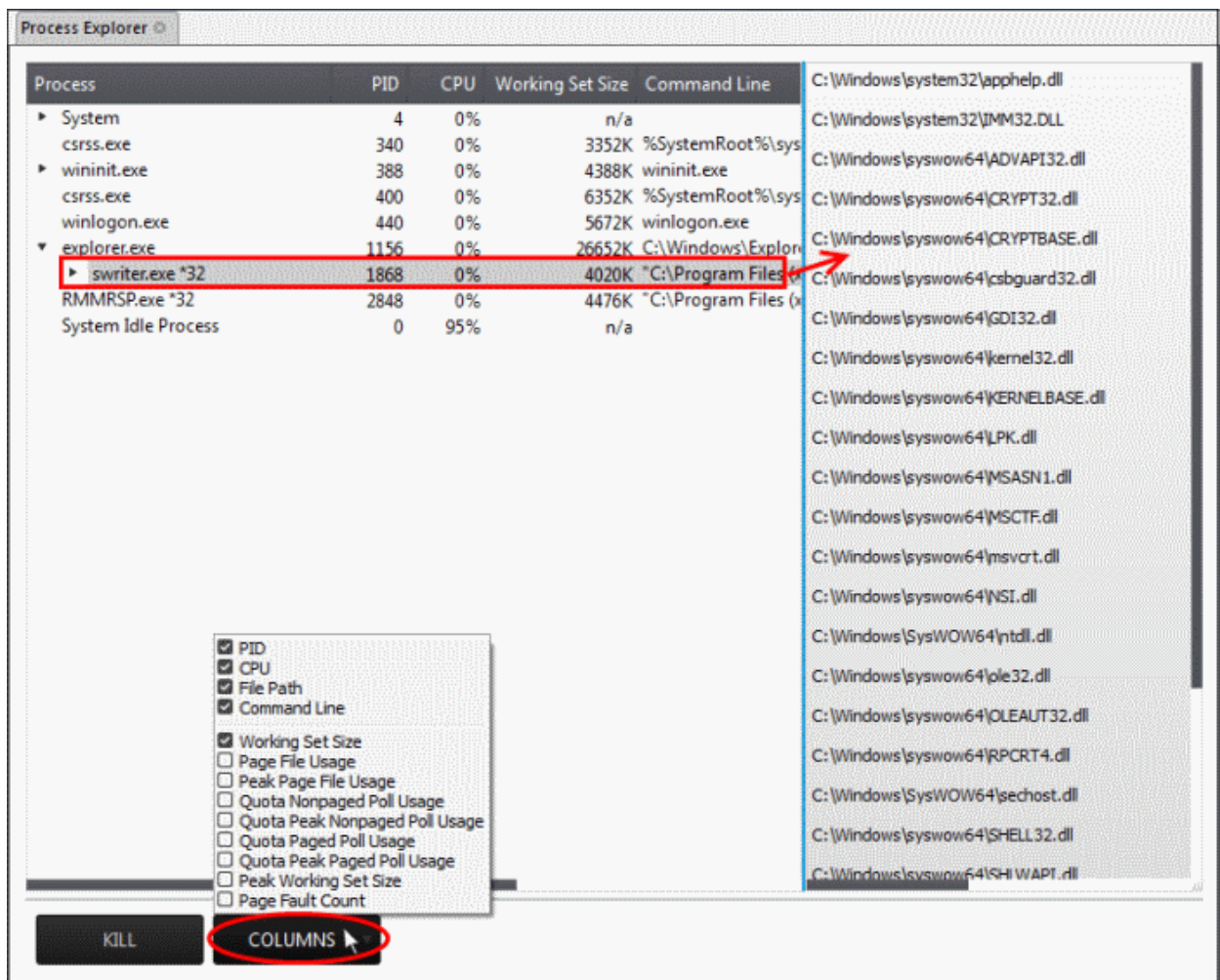


A new 'Process Explorer' tab opens in the main configuration area. All the processes currently running on the

endpoint will be listed.



- Click on the ▶ beside an item to expand it to a tree structure
- To view the dependent processes, handles and DLLs of a process, select the process from the list. The dependent processes will be displayed on the next pane.



By default, the Process Explorer window displays the details of the process under five columns. To view more granular details of each process, an admin can add more columns to the window.

- To add more columns, click on the 'Columns' drop-down and select the details to be displayed for each process.

Process Explorer - Descriptions of Columns	
Column	Description
PID	Displays the Process Identification number. Clicking on the column header enables sorting the entries in ascending or descending order of the PID numbers.
CPU	Displays the CPU usage of the process as a portion of overall CPU usage by the process in percentage. Clicking on the column header enables sorting the entries based on the CPU usage.
File Path	Displays the location of the executable that has initiated the process
Command Line	Displays the command line command of the executable that has initiated the process
Working Set Size	Shows the size (in KB) of the virtual memory, occupied by the page files, referenced by the process. Clicking on the column header enables sorting the entries based on working set. Background Note: The working set of a process is the collection of information referenced by the process periodically. This collections are stored as page files in the secondary memory, such as the portion of the hard disk partitions allotted as virtual memory.
Page File Usage	Indicates the memory space occupied by the process in the virtual memory, created in the hard disk drive
Peak Page File Usage	Indicates the highest memory space occupied by the process in the virtual memory since the process has been started.
Quota Nonpaged Pool Usage	Indicates the quota amount of physical memory space (in KB) allotted for non paged pool usage by the process. The non paged memory pool consists of virtual memory addresses that would reside in physical memory as long as the corresponding kernel objects of the process are allocated.
Quota Peak Nonpaged Pool Usage	Indicates the maximum quota amount assigned for non paged pool usage for the process since the process has been started.
Quota Paged Pool Usage	Indicates the quota amount of virtual memory space (in KB) allocated for the process for paging.
Quota Peak Paged Pool Usage	Indicates the maximum quota amount of virtual memory space (in KB) for the paged pool usage by the process since it has been started.
Peak Working Set Size	Indicates the maximum working set size of the process, since it has been started.
Page Fault Count	Indicates the number of interrupts occurred during the read/write access by the process to the virtual memory location, that is marked ' <i>not present</i> '.

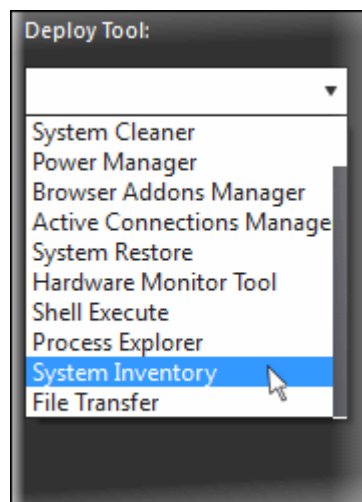
- To terminate unsafe or unwanted process, select the process and click the 'Kill' button at the bottom. Repeat the process to terminate more processes.

5.2.2.11 Obtain System Inventory Information

The System Inventory tool enables an admin to retrieve the hardware and software resources of endpoint. The 'System Inventory' report provides a valuable information to the admin for determining compatibility of the hardware with the operating systems, and identifying any changes to a system that might develop problems.

To deploy 'System Inventory' tool

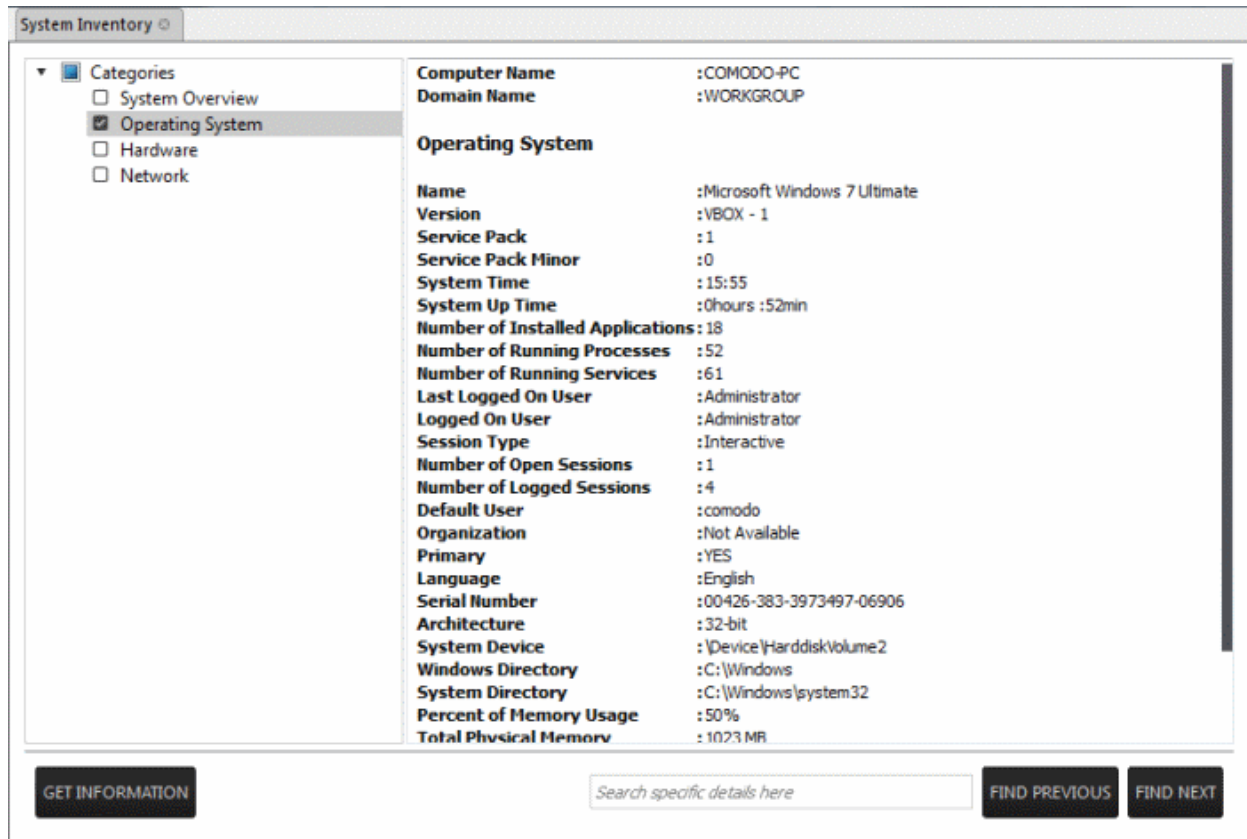
- Select 'System Inventory' from the 'Deploy Tool' drop-down on the left



A new 'System Inventory' tab will be displayed in the main configuration area.



- Click on the ► beside 'Categories' to expand/collapse the category list



- Select the category(ies) of information you wish to view.
- Click 'Get Information'

The information on the selected category(ies) will be displayed in the next pane.

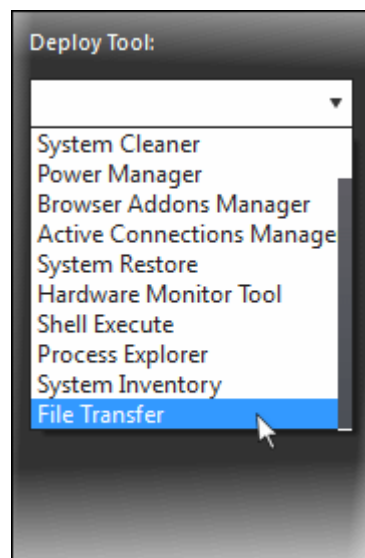
- To search for a specific information, type the search criteria in the 'Search specific details here' text box and click 'Find Next' or 'Find Previous'

5.2.2.12 Transfer Files From / To Client System

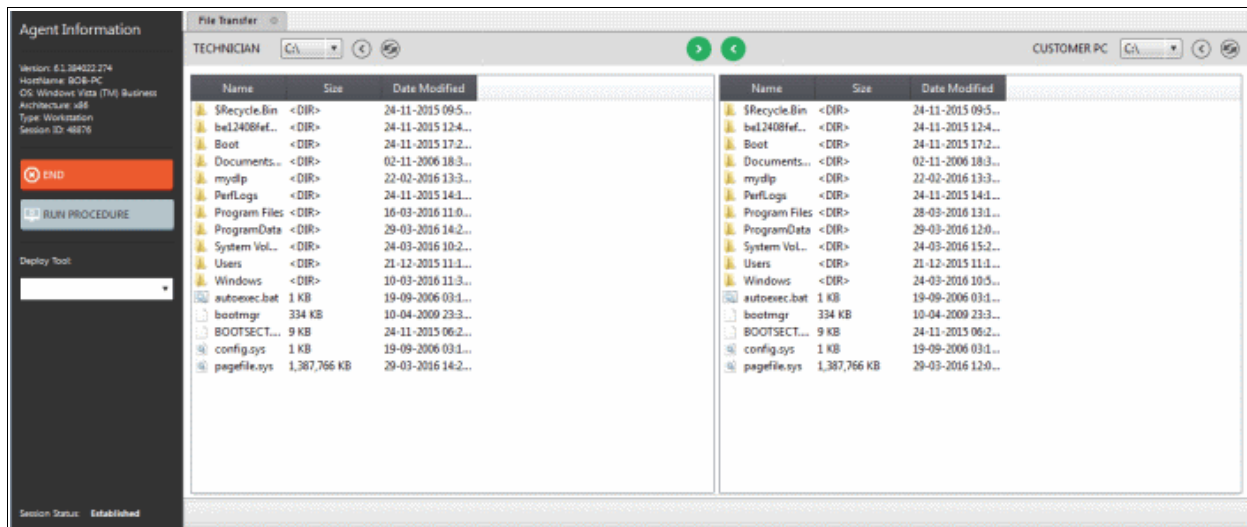
The 'File Transfer' tool allows an administrator to transfer files both ways between the host and endpoints.

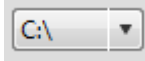




To transfer files

- Select 'File Transfer' from the 'Deploy Tool' drop-down on the left

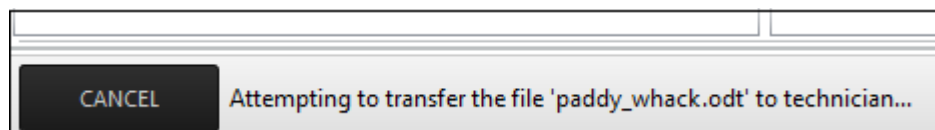


A new 'File Transfer' tab will be displayed in the main configuration area.



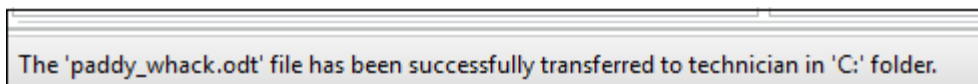
- Navigate to the location using the 'Drive' drop-downs  and select the source/destination for file transfer
- Select the files to be transferred to host/user computer
- Click the  button to go back to the parent folder
- Click the  button to refresh the list
- Click the  button to transfer files from host to endpoint
- Click the  button to transfer files from endpoint to the admin computer

The file transfer progress will be displayed at the bottom.



- Click the 'Cancel' button to abort the file transfer process

A confirmation message will be displayed at the bottom.



6 The Jobs Interface


A 'Job' is a collection of **procedures** compiled to run on selected endpoints. You can create new jobs by including the existing procedures and selecting the endpoints for execution. Procedures that are run from the 'Devices', 'Procedures' and 'Sessions' interfaces are also created as jobs and displayed on the 'Jobs' screen.

To open the 'Jobs' screen, click 'Jobs' from the drop-down at the top left

ID	Name	Description	Start time	Status	Started by
247	Test Job2	Book of Jobs	7/5/2015 09:33	Completed	hertriumph@gmail.com
246	Job from Session context	1302	7/5/2015 09:25	Completed	hertriumph@gmail.com
245	Clean Sales dept endpoints	To run registry clean and disk clean operations ...	7/5/2015 08:30	Completed	hertriumph@gmail.com
244	Job from Session context	1291	7/5/2015 07:32	Completed	hertriumph@gmail.com
243	Job from Session context	1291	7/5/2015 07:30	Completed	hertriumph@gmail.com
242	Job from Devices context	Test Chennai Job2	7/5/2015 07:29	Completed	hertriumph@gmail.com
241	Job from Devices context	Test Chennai Job	7/5/2015 07:24	Completed	hertriumph@gmail.com
240	Job from Devices context		7/5/2015 07:04	Completed	hertriumph@gmail.com
236	Clean Sales dept endpoints	To run registry clean and disk clean operations ...	7/5/2015 06:10	Completed	hertriumph@gmail.com
238	Job from Devices context		6/5/2015 13:04	Completed	samplestems15@gmail.com
234	Test Job		6/5/2015 12:48	Completed	samplestems15@gmail.com
237	Job from Devices context		6/5/2015 12:48	Completed	samplestems15@gmail.com
235	Restart	To restart computer in session	6/5/2015 12:12	Starting	samplestems15@gmail.com
228	Test Job		5/5/2015 10:03	Completed	hertriumph@gmail.com
221	Job from Session context	1108	4/5/2015 05:12	Completed	comodoone15@gmail.com
222	Job from Session context	1108	4/5/2015 05:12	Completed	comodoone15@gmail.com
220	Job from Session context	1108	4/5/2015 05:11	Completed	comodoone15@gmail.com
205	ilution	check	30/4/2015 13:51	Completed	samplestems15@gmail.com
204	ilution	check	30/4/2015 13:50	Completed	samplestems15@gmail.com
203	ilution	check	30/4/2015 13:49	Completed	samplestems15@gmail.com
202	ilution	check	30/4/2015 13:48	Completed	samplestems15@gmail.com
201	Job from Devices context		30/4/2015 13:22	Completed	samplestems15@gmail.com

Jobs - Column Description

Column Header	Description
ID	The ID number of the job
Name	Name of the job provided while creating. Procedures that are run from the 'Devices', 'Procedures' and 'Sessions' interfaces are also created as jobs and their names displayed on the 'Jobs' screen.
Description	Description of the job
Start time	Details of date and time when the job was executed
Status	Displays the status of the job whether it is 'Starting', 'In Progress' or 'Completed'
Started by	Displays the details of the admin who executed the job

- Click the button  beside a row to expand or collapse the Job details section

ID	Name	Description	Start time	Status	Started by
249	Test Job 5	To test available endpoints	7/5/2015 10:22	Completed	hertriumph@gmail.com
	SMITH-COMPUTER			Completed	2 of 2
	Test Procedure 1			Completed	100%
	Test Procedure 2			Completed	99%
	CHNW7HP64			Completed	2 of 2
	Test Procedure 1			Completed	100%
	Test Procedure 2			Completed	99%
248	Test job 4	To check execution of jobs on available and un...	7/5/2015 10:06	Completed	hertriumph@gmail.com
247	Test Job2	Book of Jobs	7/5/2015 09:33	Completed	hertriumph@gmail.com

The expanded section for a Job ID displays the names of the endpoints and below them, the names of procedures that were executed.

Filter and search options

The filter buttons at the top of the interface provide at-a-glance statuses of jobs executed.

All (26) Starting (1) In progress (0) Completed (25)

- Click on any of the item to display the filtered entries
- To search for a particular item, enter the details partly or fully in the search field on the right side.
- Click on a column header to sort the items in alphabetical/ascending/descending order

From the 'Jobs' interface an admin can:

- **Manage Jobs**
- **Execute Jobs on Endpoints**

6.1 Manage Jobs

The 'Jobs' interface allows admins to create new jobs that are to be executed on endpoints. A new job created cannot be edited but can be deleted from the list.

To create jobs, click the 'Job Manager' button at the bottom of the 'Jobs' interface

The screenshot shows a 'Job manager' window with a table of jobs. The table has columns for ID, Name, Description, Owner, Support group, and Compatibility. Below the table, there are buttons for 'RUN', 'REFRESH', 'CREATE', 'CREATE FROM', and 'DELETE'. At the bottom of the interface, there is a 'Job manager' button circled in red, with a red arrow pointing to it from the text above.

ID	Name	Description	Owner	Support group	Compatibility
280	Test Job 5	To test available endpoints	hertriumph@gmai...	ComodoTest	Windows
279	Test job 4	To check execution of jobs on availabl...	hertriumph@gmai...	ComodoTest	Windows
278	Test job 3	To check unavailable endpoints	hertriumph@gmai...	ComodoTest	Windows
276	Test Job2	Book of Jobs	hertriumph@gmai...	ComodoTest	Windows
266	sample 3		samplesystems15...	ComodoTest	Windows
265	sample		samplesystems15...	ComodoTest	Windows
257	Test Job		hertriumph@gmai...	ComodoTest	Windows
256	Restart	To restart computer in session	avantistude@gmai...	ComodoTest	Windows
230	illusion	check	samplesystems15...	ComodoTest	Windows
226	Job 1	Description of Job	comodoone15@g...	ComodoTest	Windows
218	Example job		ops@grr.la	ComodoTest	Windows

Job Manager - Column Description	
Column Header	Description
ID	The ID number of the job
Name	Name of the job provided while creating.
Description	Description of the job
Owner	Username of the admin who created the job
Support group	Displays the name of the customer account
Compatibility	Displays the name of OS for which the job can be executed

- Click on a column header to sort the items in alphabetical/ascending/descending order

The 'Job Manager' screen allows an admin to:

- **Create a new job**
- **View details of a job**
- **Delete a job**
- **Execute a job on endpoints**

To create a new job

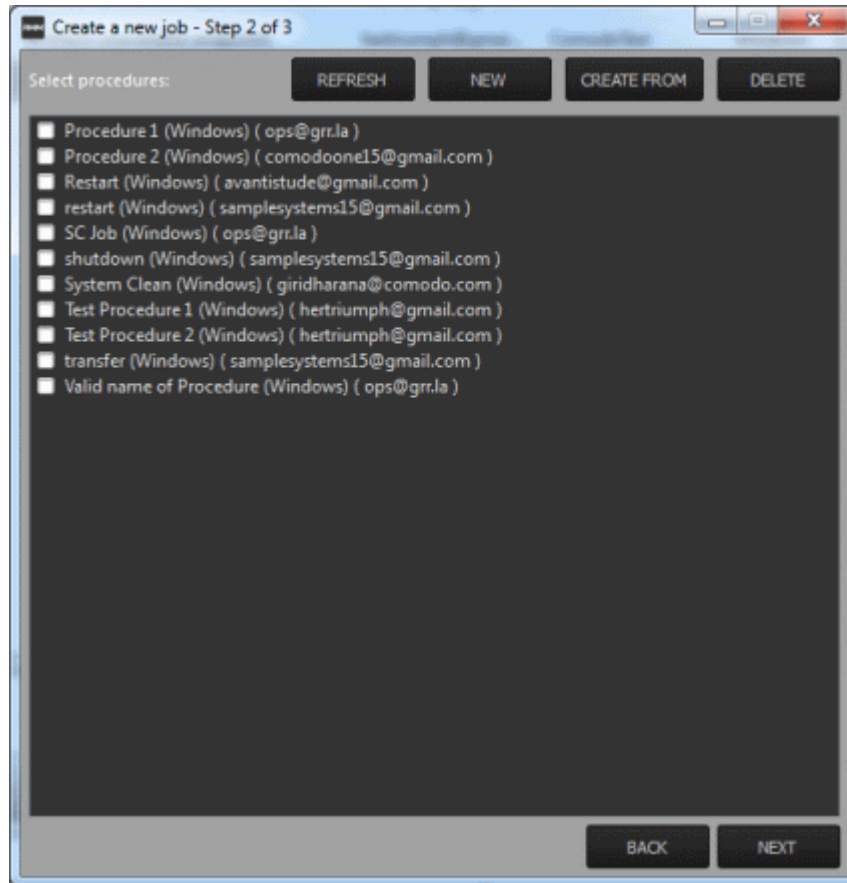
- Click the 'Create' button at the top of the interface

Step 1

- Enter the name of the job in the 'Job name' field
- Enter an appropriate description for the job in the 'Job description' section
- Select the OS details of the endpoints for which the job should be executed below the 'Select job's target information' section at the bottom of the screen
- Click the 'Next' button

Step 2

The next step is to select the procedures that are pre populated in the screen for the job.

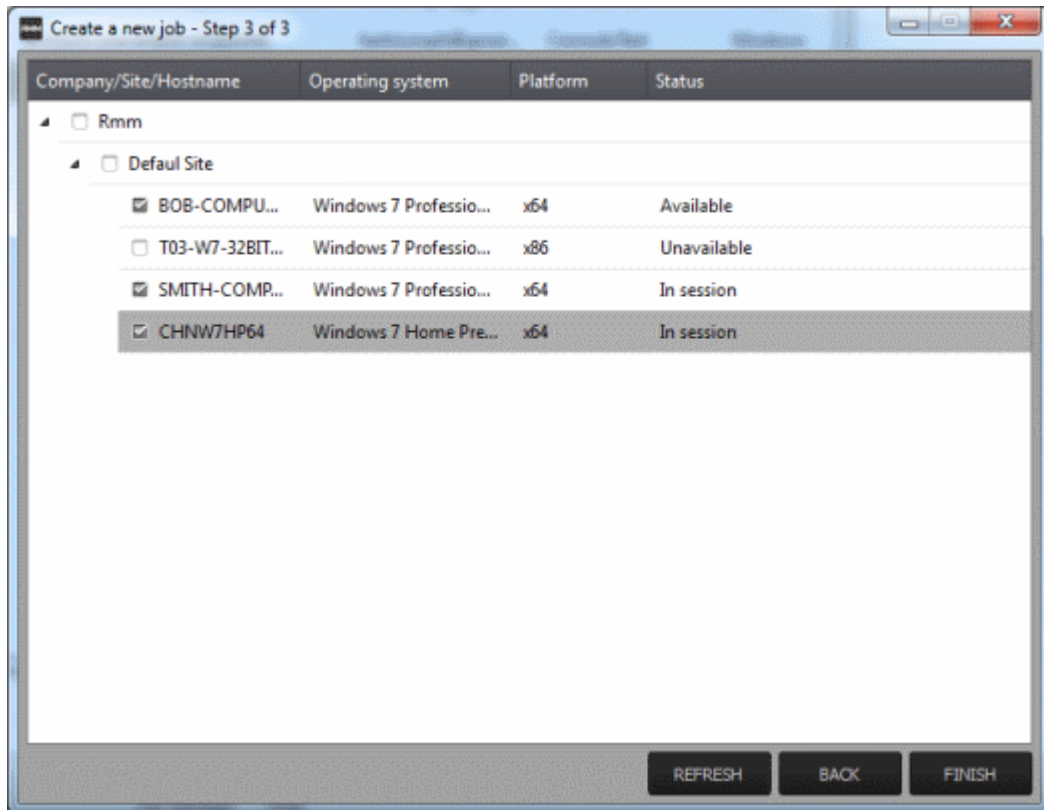


You can also create a new procedure afresh or from an existing procedure from the screen by clicking the 'New' or 'Create From' buttons. Refer to the section '**Managing Procedures**' for more details about how to create procedures.

- Click the 'Refresh' button to update the procedures list in the screen
- Select the procedure(s) from the list that you want to add for the job
- Click the 'Next' button

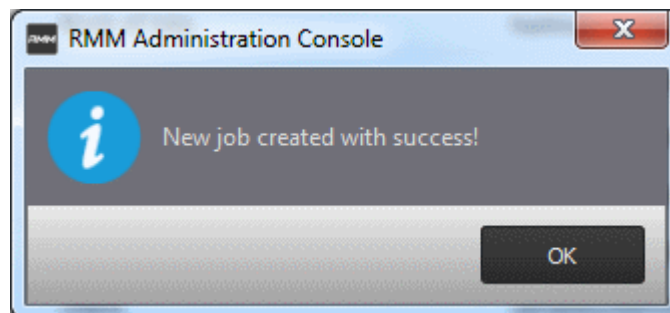
Step 3

The next step is add the endpoints onto which the job should be executed.



- Select the endpoints from the list and click the 'Finish' button

A success confirmation message will be displayed.



- Click 'OK'

The new job will be created and be listed on the screen.

Tip: You can create new jobs using an existing job as a template. To create a new job, select an existing job and click the 'Create From' button. The 'Create a new job' dialog will open with the actions pertaining to the existing job preselected. You can edit the parameters and create a new job.

Now that a job is created you can run it anytime. Refer to the section '**Executing Jobs on Endpoints**' for more details.

To view details of a job

- Click the button ▸ beside a row to expand or collapse the Job details section

ID	Name	Description	Owner	Support group	Compatibilit
280	Test Job 5	To test available endpoints	hertriumph@gmai...	ComodoTest	Windows
	Devices				
	WILLSMITH-PC				
	CHNW7HP64				
	Procedures				
	Test Procedure 1				
	Test Procedure 2				
279	Test job 4	To check execution of jobs on availabl...	hertriumph@gmai...	ComodoTest	Windows

The expanded section for an Job ID displays the names of the endpoints below 'Devices' and below the names of procedures below 'Procedures'.

To delete a job

- Select the job(s) from the list that you want to remove

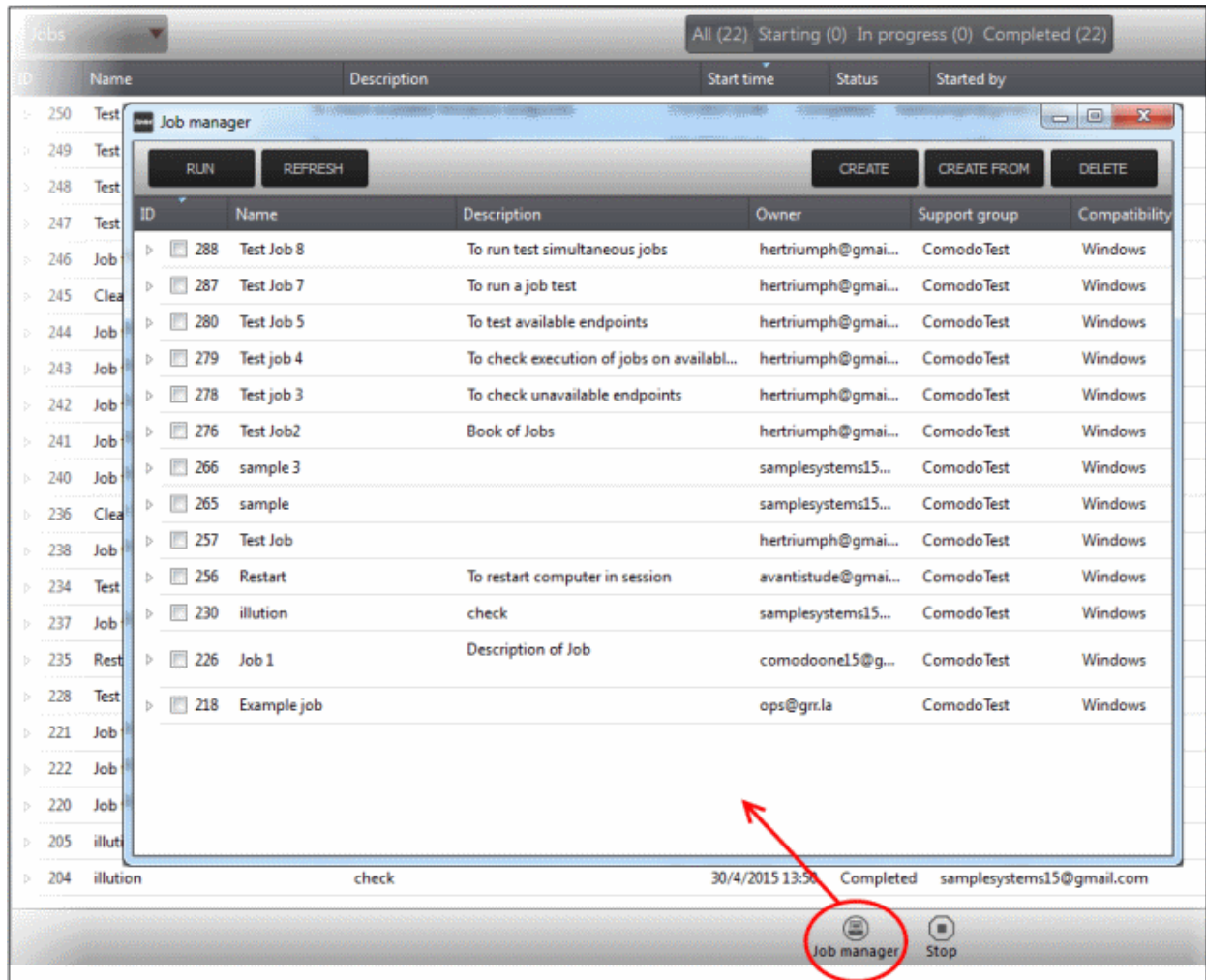
ID	Name	Description	Owner	Support group	Compatibility
280	Test Job 5	To test available endpoints	hertriumph@gmai...	ComodoTest	Windows
279	Test job 4	To check execution of jobs on availabl...	hertriumph@gmai...	ComodoTest	Windows
278	Test job 3	To check unavailable endpoints	hertriumph@gmai...	ComodoTest	Windows
276	Test Job2	Book of Jobs	hertriumph@gmai...	ComodoTest	Windows
266	sample 3		samplesystems15...	ComodoTest	Windows
265	sample		samplesystems15...	ComodoTest	Windows
257	Test Job		hertriumph@gmai...	ComodoTest	Windows
256	Restart	To restart computer in session	avantistude@gmai...	ComodoTest	Windows
230	illusion	check	samplesystems15...	ComodoTest	Windows
226	Job 1	Description of Job	comodoone15@g...	ComodoTest	Windows
218	Example job		ops@grr.la	ComodoTest	Windows

- Click the 'Delete' button at the top right

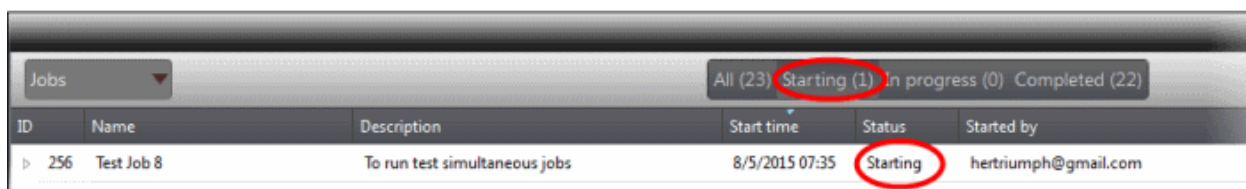
6.2 Execute Jobs on Endpoints

Jobs that are **created** can be run anytime from the 'Job Manager' interface. Please note that only one job can be executed at a time.

To execute a job, click the 'Job Manager' button at the bottom of 'Jobs' interface

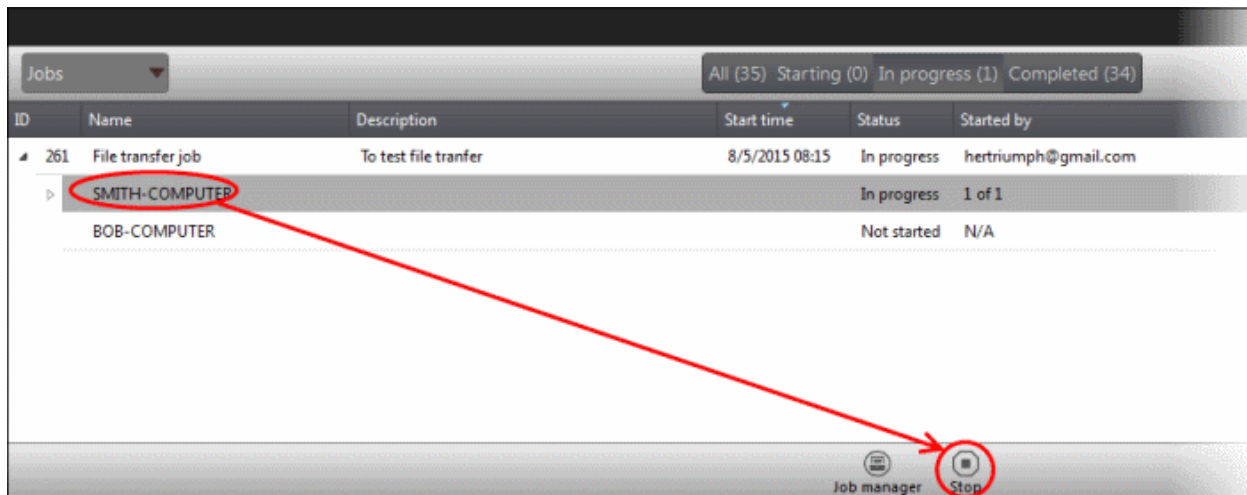


- From the 'Job Manager' screen, select the job that you want to execute and click the 'Run' button at the top. The selected job will start and its stages of execution will be displayed in the 'Jobs' screen.



The stages of a job execution are, 'Starting', 'In progress' and 'Completed'

To stop a job midway, click the button ▶ beside a row, select the device below 'Devices' and click the 'Stop' button.

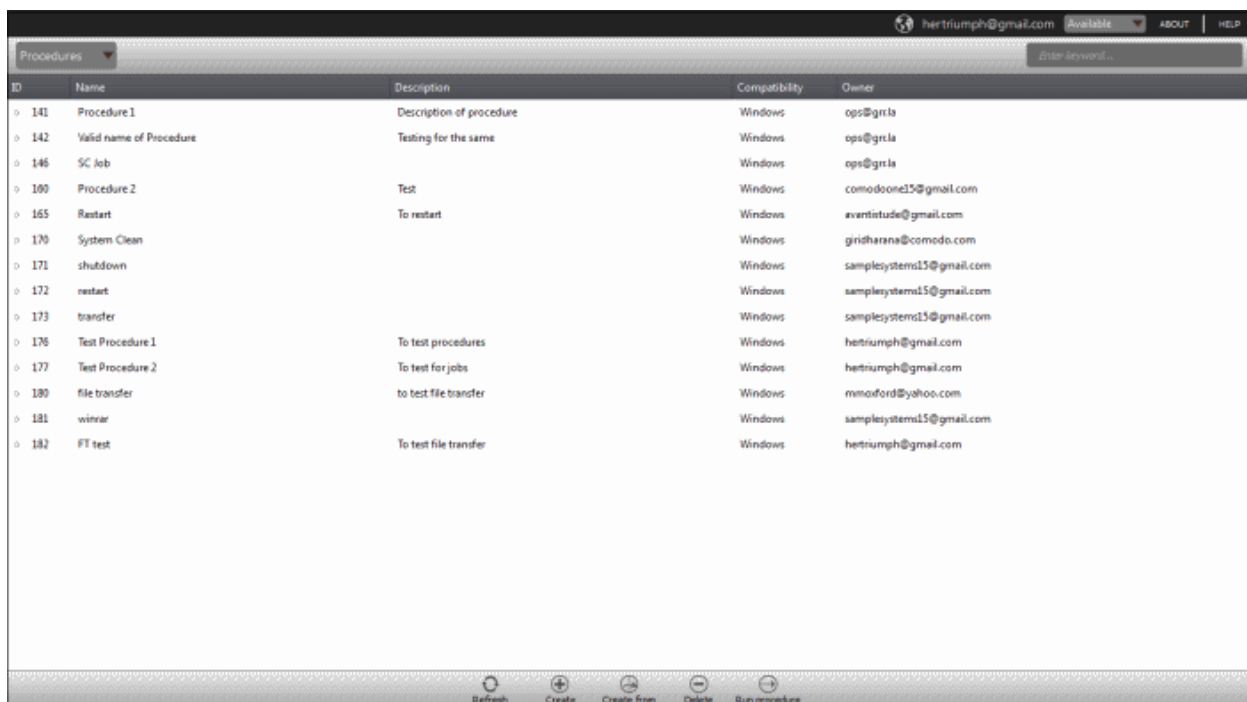


The job execution will be canceled.

7 The Procedures Interface

A 'Procedure' is a set of actions to be run on endpoints. CRMM is shipped with a set of predefined actions such as 'Application Installer', 'Power Manager', 'System Restore' and you can define parameters for each of the action. The configured actions in a procedure are performed in sequence while executing it. A procedure can be run ad-hoc on any endpoint and can also be used while creating a job to be executed on specific endpoint(s).

To open the 'Procedures' screen, click 'Procedures' from the drop-down at the top left.

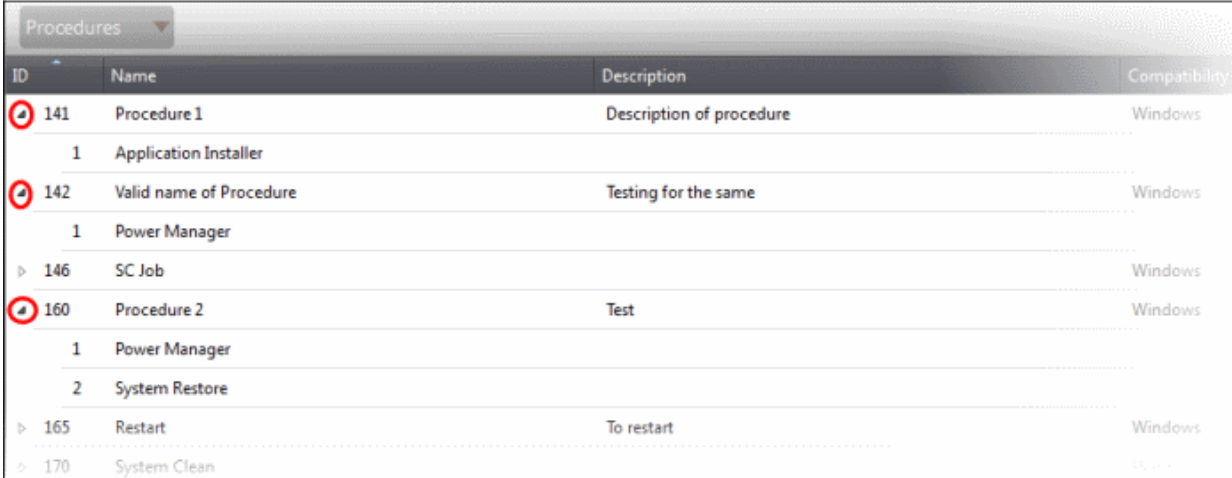


Procedures - Column Description

Column Header	Description
ID	The ID number of the procedure
Name	Name of the procedure provided while creating

Description	Description of the procedure
Compatibility	Displays on which operating system the procedure can be run
Owner	The user name of the admin who created the procedure

- Click the button  beside a row to expand or collapse the 'Procedure' details section



ID	Name	Description	Compatibility
141	Procedure 1	Description of procedure	Windows
1	Application Installer		
142	Valid name of Procedure	Testing for the same	Windows
1	Power Manager		
146	SC Job		Windows
160	Procedure 2	Test	Windows
1	Power Manager		
2	System Restore		
165	Restart	To restart	Windows
170	System Clean		Windows

The expanded section of a 'Procedure' displays the names of the configured actions in sequence below the name of a procedure.

Sort and search options

- To search for a particular item, enter the details partly or fully in the search field on the right side.
- Click on a column header to sort the items in alphabetical/ascending/descending order

From the 'Procedures' interface an admin can:

- **Manage Procedures**
- **Run Procedures on Endpoints**

7.1 Manage Procedures

The 'Procedures' interface allows admins to create new procedures that are to be executed on endpoints. A new procedure created cannot be edited but can be deleted from the list.

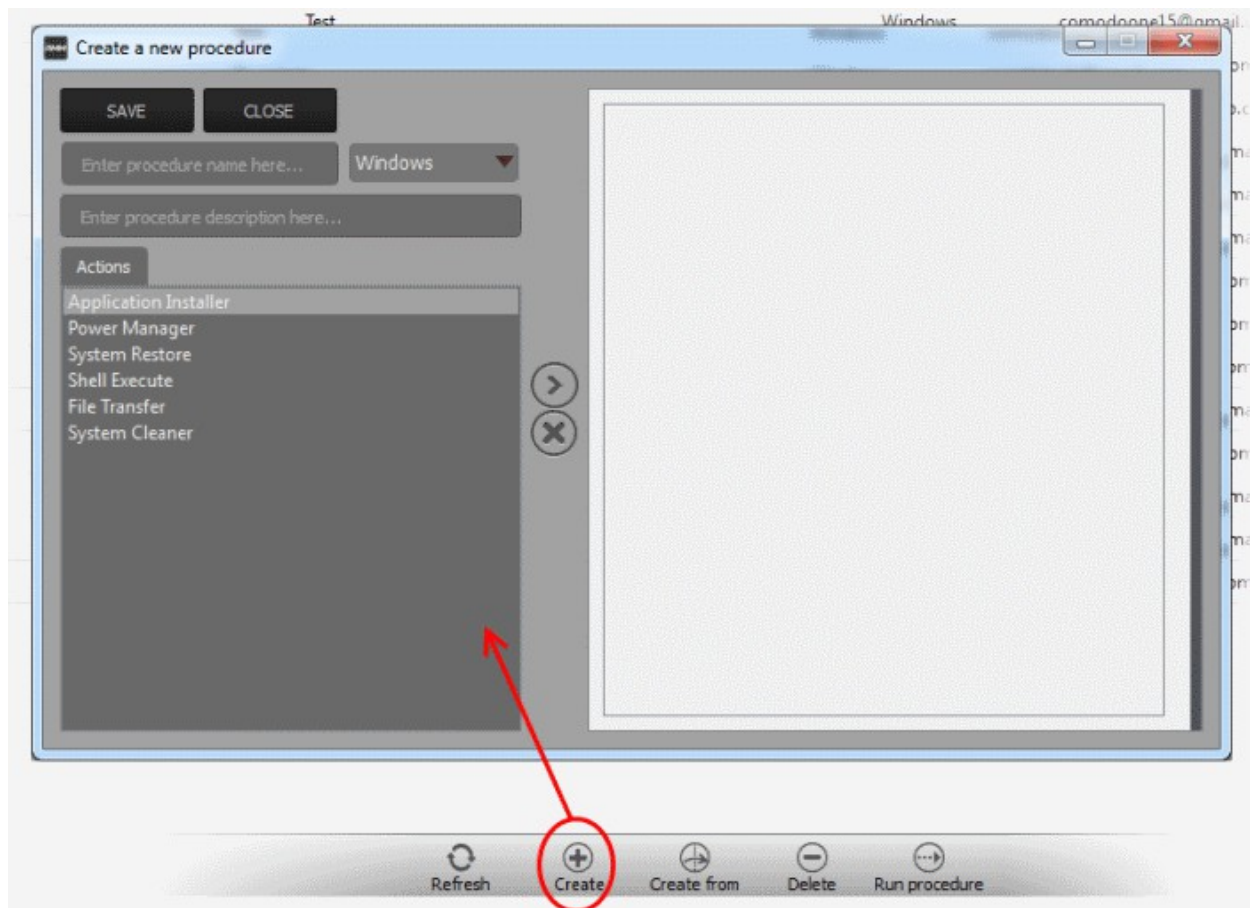
The 'Procedures' screen allows an admin to:


- **Create a new procedure**
- **Delete a procedure**
- **Run a procedure on endpoints**

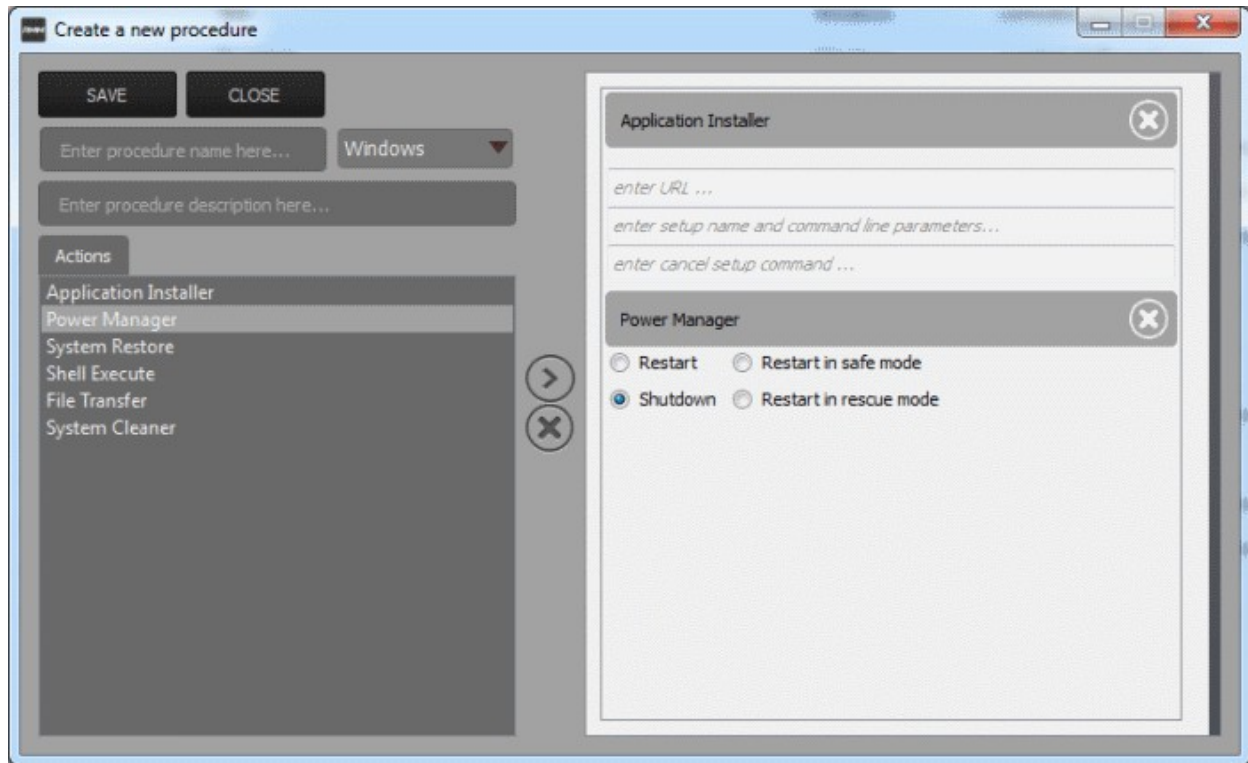
To create a new procedure



- Click 'Create' from the bottom

The 'Create a new procedure' dialog will be displayed.



- Enter a name and a short description in the respective fields and choose the operating system from the drop-down at the left.
- Choose an action from the 'Action' list at the left and click the  button to add the action to the list at the right
- Repeat the process to add more actions



- To remove an action from the right side, click the  button at the top right of the respective action
- To remove all the actions from the right side, click the  button on the center
- Select the options and/or set the parameters for the action.

Action	Parameters Required
Application Installer	Enter the following parameters: <ul style="list-style-type: none"> • Download URL for the application • Name of the setup file and command line parameters • Command for canceling installation for failsafe reasons
Power Manager	Choose the power control operation from: <ul style="list-style-type: none"> • Restart • Restart in safe mode • Shutdown • Restart in rescue mode
System Restore	Choose whether to create a restore point or to restore the system to a previous state. <ul style="list-style-type: none"> • Enter the name of the restore point
Shell Execute	Basic <ul style="list-style-type: none"> • Enter the execution command for the process • Enter the parameters to be passed to the process Advanced

Action	Parameters Required
	<ul style="list-style-type: none"> Enter the working directory for the process Choose the execution options: <ul style="list-style-type: none"> Wait for process to finish - Completes the process before termination Hide Window - Executes the process at the background
File Transfer	Enter the path of the source file to be copied from the host computer at which the technician console is installed. The file will be copied to the folder c:\ips-temp\file-transfer at the endpoint.
System Cleaner	Select the cleaner modules to be applied: <ul style="list-style-type: none"> Disk Cleaner Registry Cleaner

- Click the 'Save' to save the procedure. Upon running the procedure, the actions will be executed sequentially.

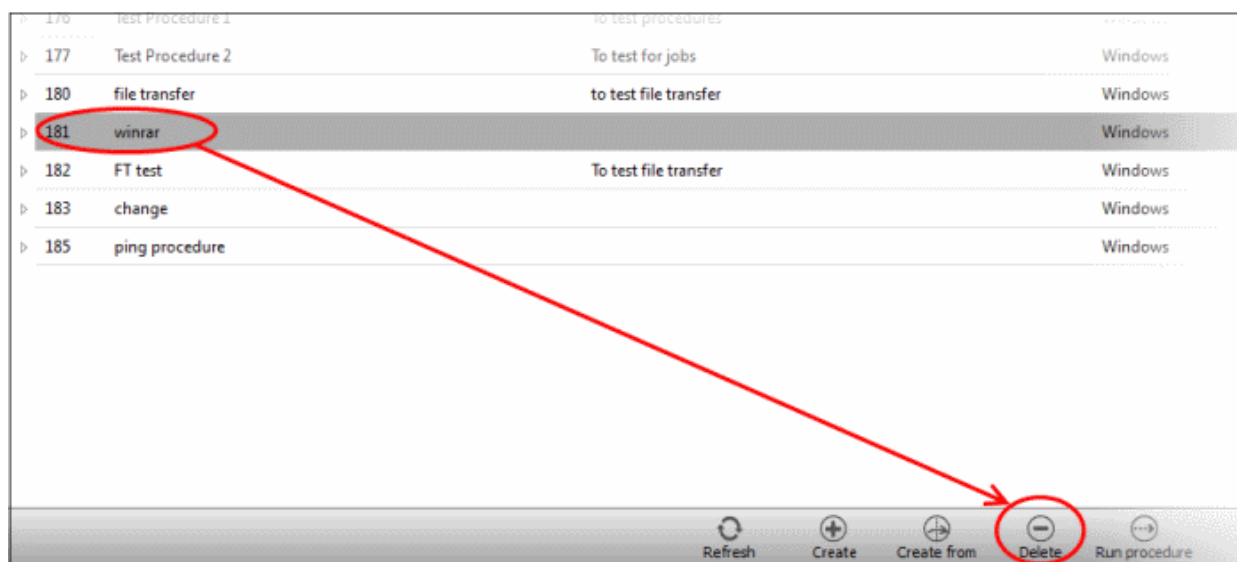
The 'Procedure' will be added to the list and will be available for inclusion in a **job created** for a specific endpoint. The procedure can also be run ad-hoc on any desired endpoint. Refer to the section **Running Procedures on Endpoints** for more details.

- Repeat the process to add more procedures as required.

Tip: You can create new procedures using an existing procedure as a template. To create a new procedure, select an existing procedure and click 'Create From' from the bottom. The 'Create a new procedure' dialog will open with the actions pertaining to the existing procedure preselected. You can edit the parameters and create the new procedure.

To delete a procedure

- Select the procedure from the list that you want to remove



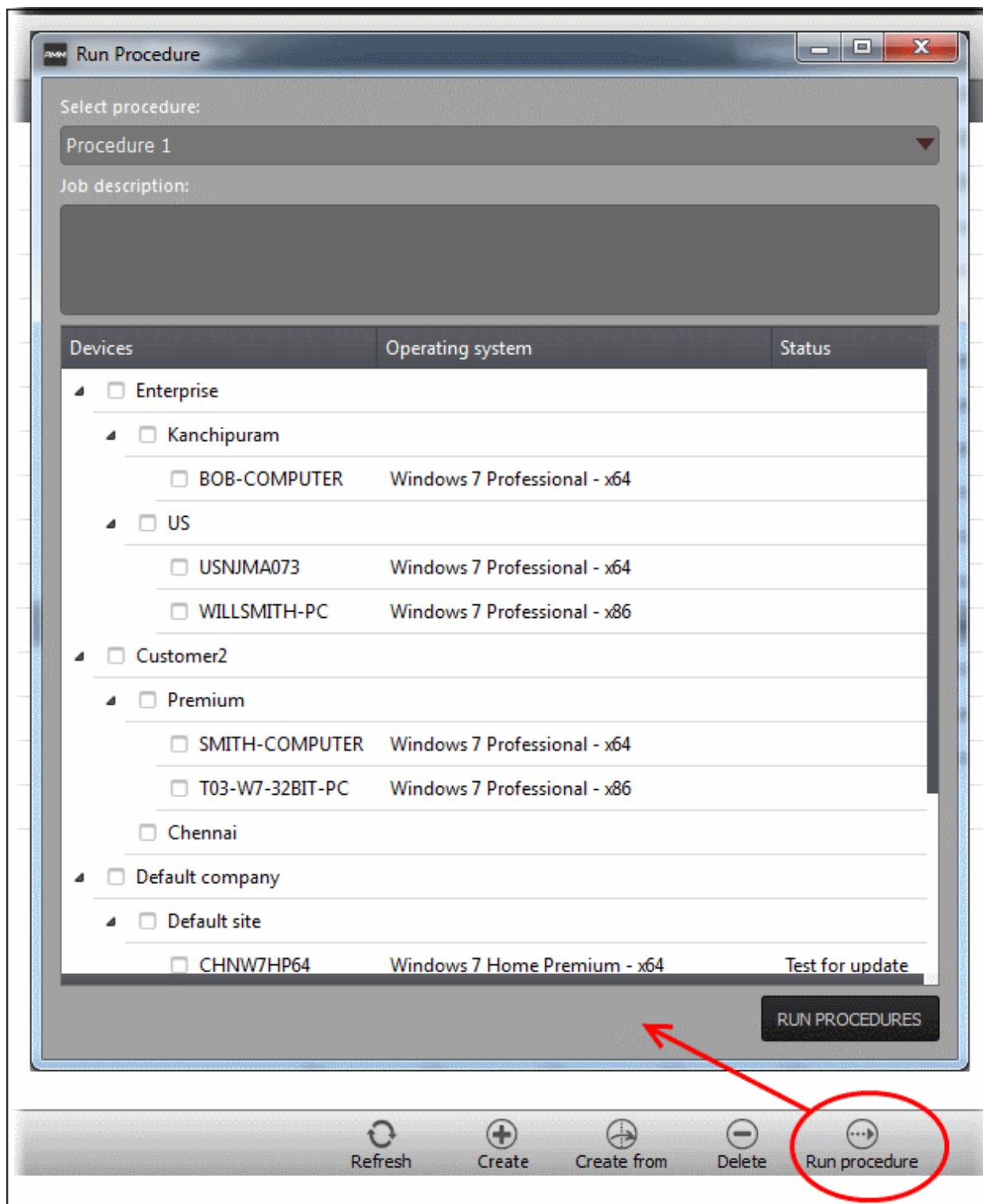
- Click the 'Delete' button at the bottom

7.2 Run Procedures on Endpoints

Procedures that are **created** can be run anytime from multiple interfaces - The 'Procedures' interface, the **'Devices'**

interface and the **'Sessions'** interface.

To run a procedure from the 'Procedures' screen, click the 'Run procedure' button at the bottom of the interface .



- Select the procedure that you want to run from the 'Select procedure' drop-down at the top. Refer to the section **'Managing Procedures'** for more details about how to create and manage procedures.
- Enter the name of the job in the 'Job description' field
- Select the endpoints from the 'Devices' list that you want to run the procedure
- Click the 'Run Procedures' button at the bottom

The procedure will be run on the selected endpoints and it will be created as a job and displayed in the **'Jobs'**

interface with its status whether 'Starting', 'In-progress' or 'Completed'. Refer to the section **'The Jobs Interface'** for more details.

8 The Policies Interface

Policies help MSPs/organizations/departments to monitor endpoints effectively and efficiently. RMM allows administrators to create policies based on predefined system parameters such as RAM monitor, traffic monitor, disk health monitor and so on. You can configure settings for each monitored item while creating a policy then deploy it to endpoints.

To open the 'Policies' screen, click 'Policies' from the drop-down at the top left.



Policies - Column Description	
Column Header	Description
Policy Name	Displays the name of the monitoring policies
Description	The description provided for the policy while creating it
Endpoints	Indicates the number of endpoints a policy is applied
Status	Indicates whether the applied policy is violated or not <ul style="list-style-type: none"> OK - Policy is not violated Alarm - Policy is breached. A service desk ticket is also automatically created in the Service Desk module.

- Click the ▶ button beside an applied policy to expand or collapse the section

Policy Name	Description	Endpoints	Status
<input checked="" type="radio"/> CPU Policy ▶ Devices ▶ Monitors		1	OK
<input checked="" type="radio"/> JS RAM Policy ▶ Devices ▶ Monitors	To check RAM usage of JS system	1	Alarm
▶ Drive Space Policy		0	OK
▶ RAM Policy		0	OK
▶ Traffic Policy		0	OK
▶ CASG Policy	Monitoring CASG web interface connection	0	OK
▶ Security Department	Monitoring polices for security department	0	OK

The monitor details of the policy and endpoints that are applied the policy will be displayed below it. Refer to the section '[View details of a policy](#)' for more details.

Filter and search options

The filter buttons at the top of the interface provide at-a-glance statuses of the policies.

All(7) Broken(1) Not Broken(6)

- Click on any of the item to display the filtered entries
- To search for a particular item, enter the details partly or fully in the search field on the right side.
- Click the 'Refresh' button to update the interface
- Click on a column header to sort the items in alphabetical/ascending/descending order

The buttons at the bottom of the 'Policies' interface allows admins to create policies, deploy them on endpoints, stop the applied policies and delete policies. Refer to the section '[Managing Policies](#)' for more details.

8.1 Manage Policies

The 'Policies' interface allows admins to create new policies and apply them onto endpoints as per an organization's requirement. For example you can create a policy by including multiple monitoring modules such as 'Traffic Monitor', 'RAM Monitor', 'Disk health Monitor' and so on in order to meet the specific needs of an organization/department and apply the policy to endpoints.

If a policy is violated by an endpoint, a service desk ticket will also be created in the Service Desk module. A new policy created cannot be edited but can be deleted from the list.

To manage policies, open the 'Policies' screen, by clicking 'Policies' from the drop-down at the top left

Policy Name	Description	Endpoints	Status
Traffic Policy		0	OK
Security Department	Monitoring polices for security department	0	OK
RAM Policy		0	OK
JS RAM Policy	To check RAM usage of JS system	1	Alarm
DSP for JS system		0	OK
Drive Space Policy		0	OK
CPU Policy		1	OK
CASG Policy	Monitoring CASG web interface connection	0	OK

The interface displays all the created policies.

From the 'Policies' screen an admin can:

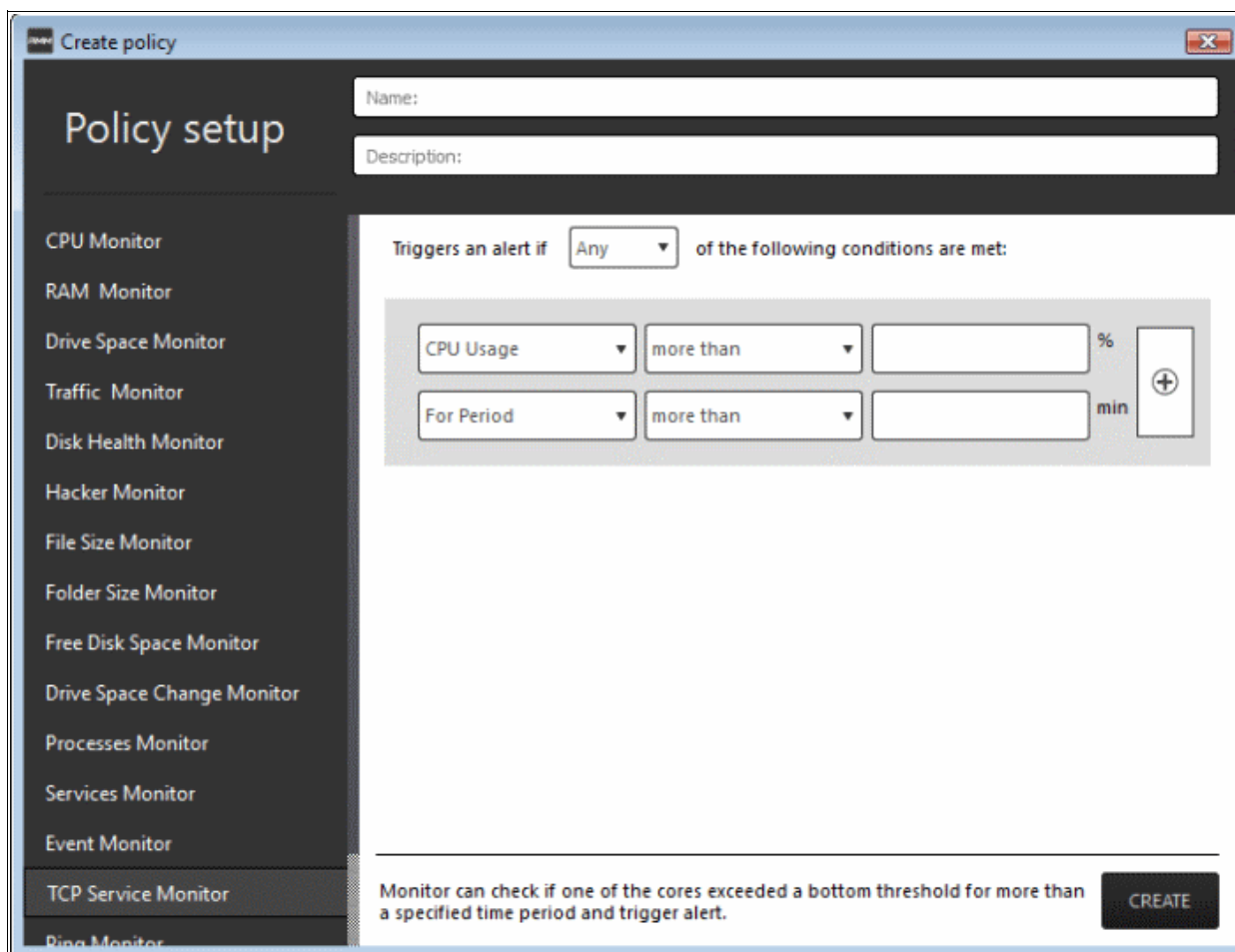
- **Create a new policy**
- **View details of a policy**
- **Delete a policy**
- **Apply policy to an endpoint**
- **Stop an applied policy**

To create a new policy

- Click the 'Create' button at the bottom of the interface



The 'Create Policy' dialog will be displayed:



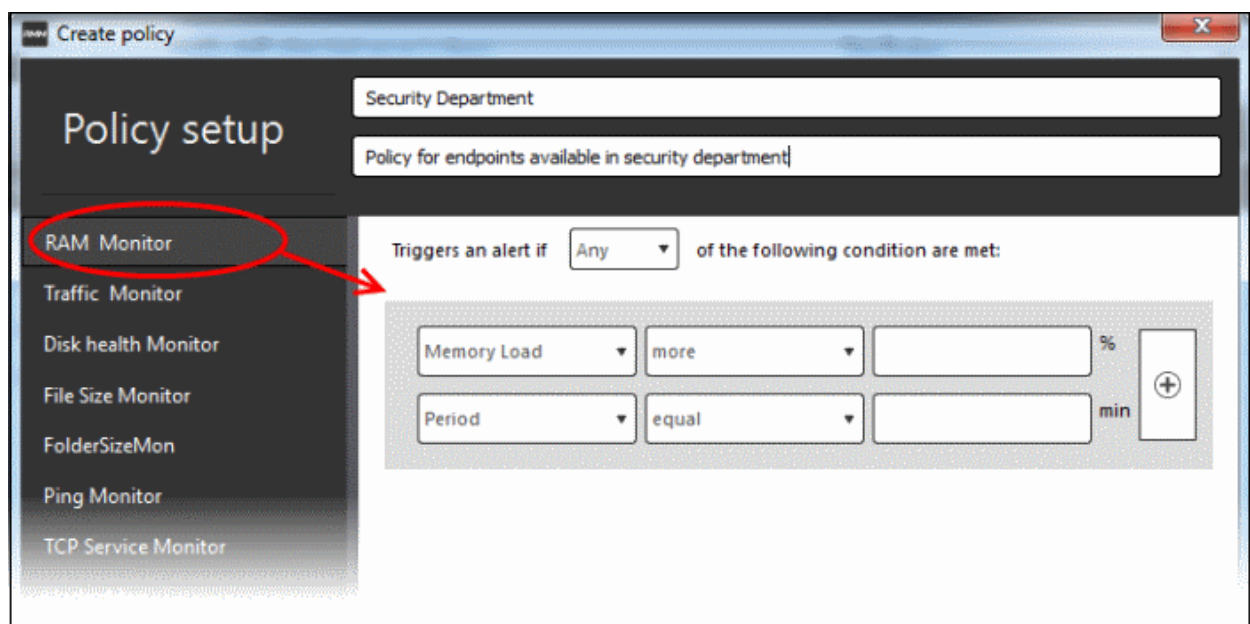
The monitoring modules are displayed on the left side of the screen and on the right side, you can configure the parameters for a selected a module. The table below provides the details of the monitoring modules.

Monitoring Modules	
Name	Description
RAM Monitor	Checks if RAM memory usage exceeds a bottom threshold for more than a specified time and generates a service desk ticket.
Traffic Monitor	Checks if network traffic exceeds a bottom threshold for more than a specified time and generates a service desk ticket.
Disk Health Monitor	Uses 'Windows Management Instrumentation' (WMI) to check if any 'Self-Monitoring, Analysis and Reporting Technology' (SMART) disks are reporting errors to the OS. A service desk ticket is generated if any errors are reported.
File Size Monitor	Checks the disk space used by a file on target computers and generates a service desk ticket when a specific file exceeds the maximum size specified.
Folder Size Monitor	Checks the disk space used by a directory/folder on target computers and generates a service desk ticket when a specific folder exceeds the maximum specified size.
Ping Monitor	Pings a device using its hostname, fully qualified domain name or an IP Address and generates a service desk ticket if no response is recieved.
TCP Service Monitor	Checks periodically attempts to connect to a specified domain/IP:port. This allows to check for services that should be running and generates a service desk ticket when ports that should be closed become open.

Hacker Monitor	Keeps track of unsuccessful login attempts on the monitored device for the past 24 hours and generates a service desk ticket if the total number of attempts exceeds the specified number.
CPU Monitor	Checks if one of the cores exceeds a bottom threshold for more than a specified time and generates a service desk ticket..
Free Disk Space Monitor	Checks for free disk space and generates a service desk ticket whenever the hard disk free space fall below the specified value.
Process Monitor	Checks if a set of processes are running and generates a service desk ticket. if any them is stopped.
Services Monitor	Checks periodically if the specified services are matching the required status, for example, running, stopped, not started.
Web Monitor	Checks periodically a web page identified by URL:port and passes the test as long as it responds with the entered text.
Drive Space Monitor	Keeps track of free space on OS drive partition and generates a service desk ticket if the specified value is exceeded. This monitor also checks if the data on the drive has changed by more than the set threshold and creates a service desk ticket.
Drive Space Change Monitor	Keeps track of the rate of data change on the drive and generates a service desk ticket if the data on the drive is changed more within the configured period.
Event Monitor	Checks Windows Event logs on endpoints. Service desk tickets are generated when a Windows event with the specified Event Sources, Event IDs or Even level occurs.

- Enter a name and a short description for the policy in the respective fields
- Choose the monitoring module from the left.

The selected module's parameters pane will be displayed on the right side.



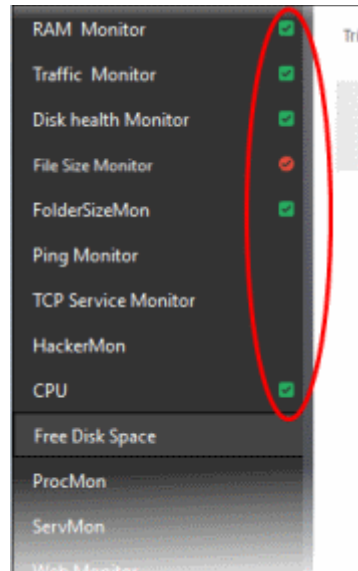
- Specify the conditions and thresholds of the rule in the right pane. Your rules are automatically saved as you go along, so you can freely select other modules on the left if you wish to add more rules to the policy.

You can add any number of conditions for a particular rule by clicking the  button at the right. To remove a

condition, click the  button to the right.

- Add more monitoring modules if required for the policy by selecting them on the left.

A check-mark is shown next to modules which are included in the current policy.




A check-mark in green background indicates parameters are correctly configured and a check-mark in red background indicates it is wrong configured.

- Click 'Create' to save your policy.

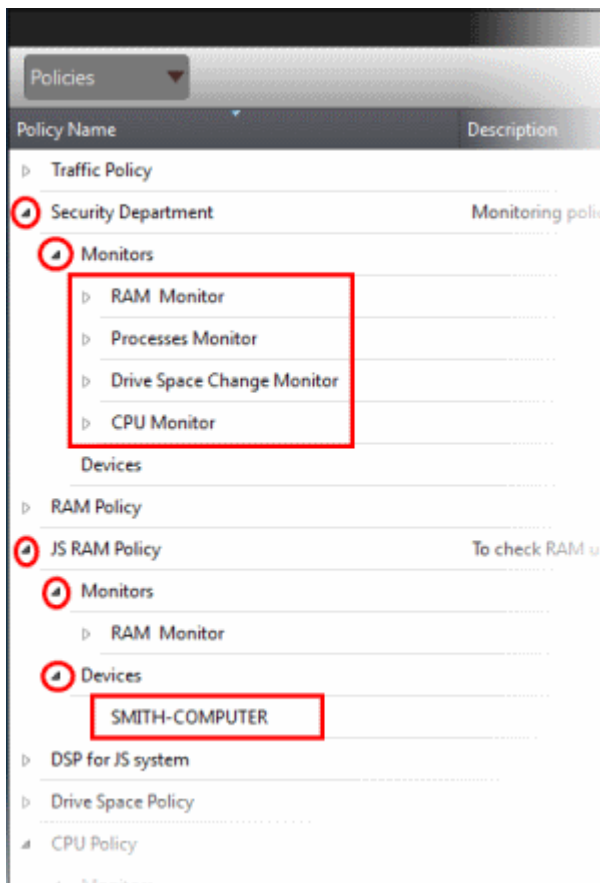
The policy will be added to the list in the 'Policy Manager' interface and will be available for deployment to desired endpoints at any time. Refer to the section '[Apply policy to an endpoint](#)' for more details.

Tip: You can create new policies using an existing policy as a template. To create a new policy, select an existing policy and click the 'Create From' button. The 'Create policy' dialog will open with the monitoring modules pertaining to the existing policy preselected. You can edit the parameters to create a new policy.

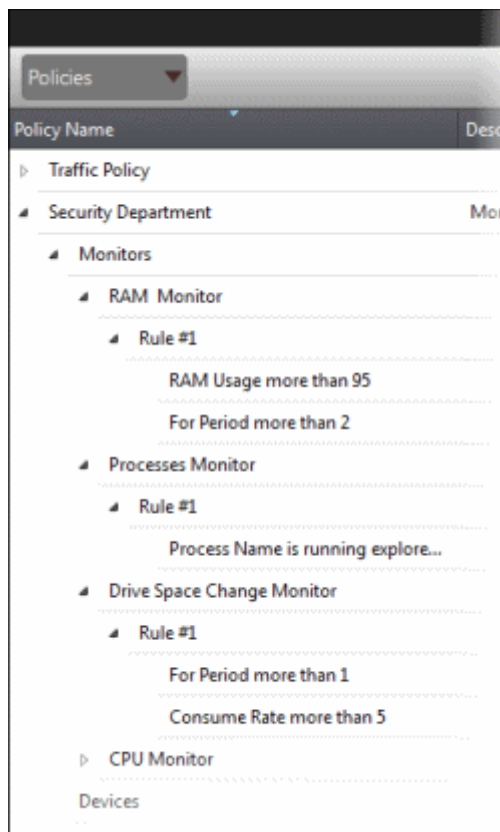
To view details of a policy

- Click the  button beside a policy to expand the section

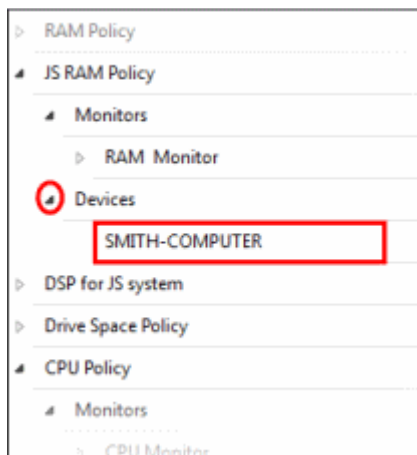
The monitoring modules added for a policy and endpoints that are applied the policy are displayed below the name of the policy.



The modules and endpoints are displayed below the labels 'Monitors' and 'Devices', respectively. To view the details of conditions for the rules configured for each monitoring module, click the ▶ button beside the respective module and rule.

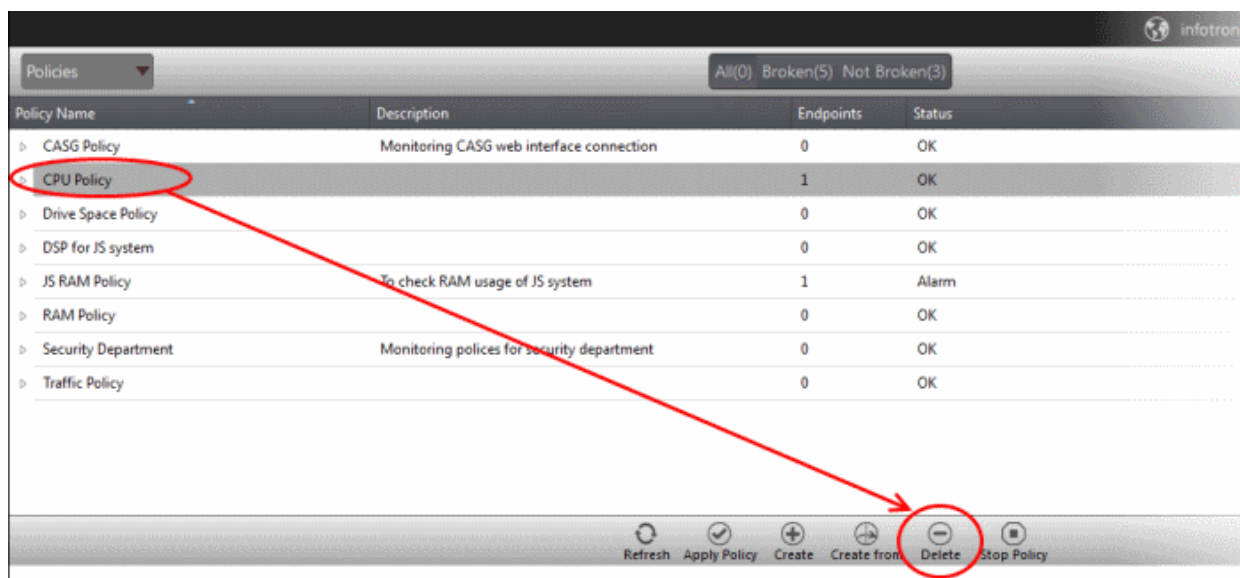


To view the details of endpoint that is applied the policy, click the ▶ button beside 'Devices'



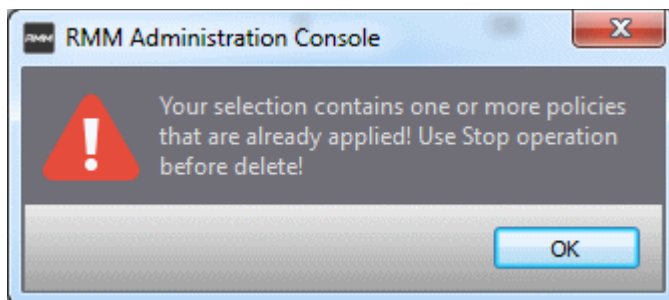
To delete a policy

- Select the policy from the list that you want to remove



The selected policy will be deleted.

Note: Make sure the policy that you want to delete is not in force on endpoints. A warning will be displayed if you are trying to delete a policy that is in force.



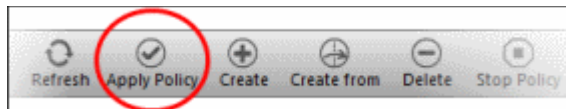
Refer to the section '**To stop a policy**' for more details.

To apply a policy to an endpoint

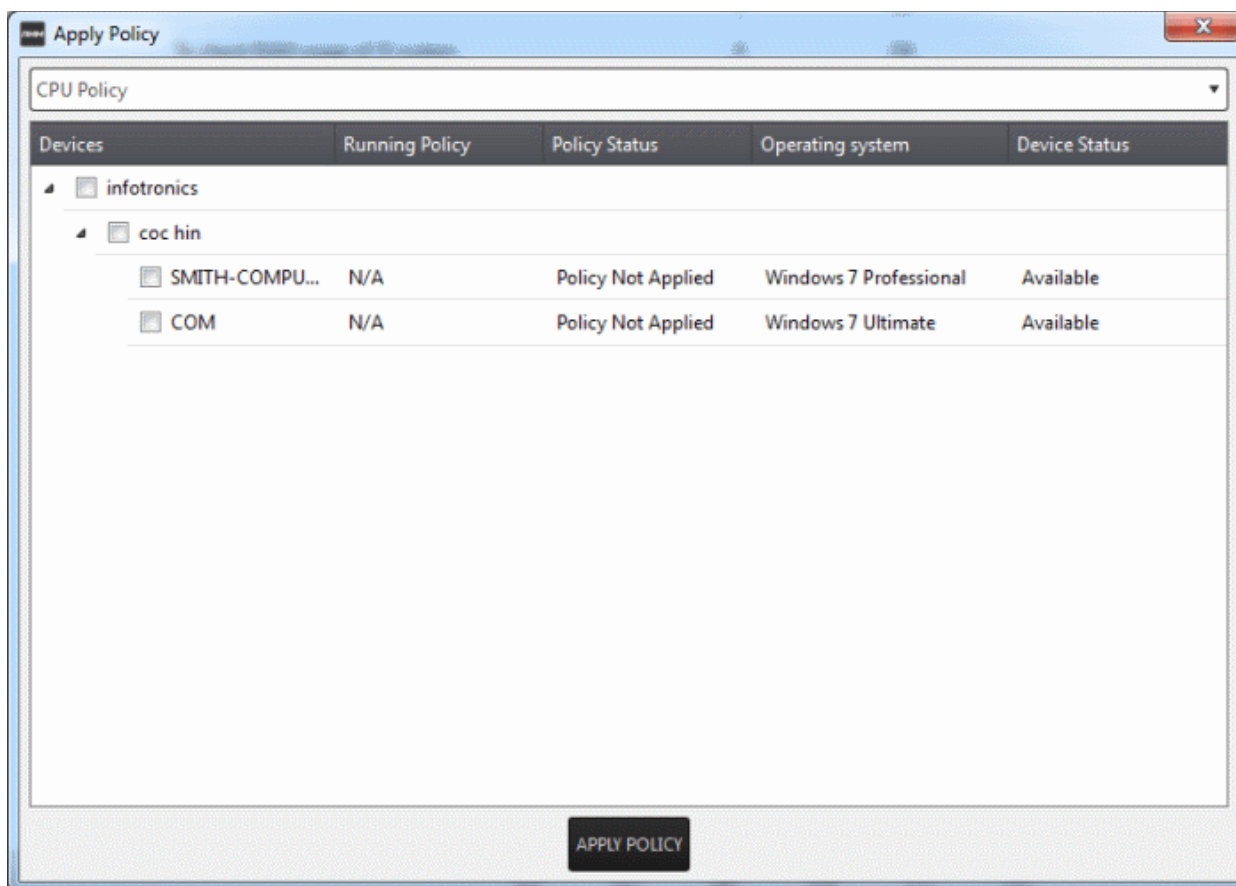
Note:

- You can apply only one policy to an endpoint
- An endpoint that is taken remotely cannot be applied a policy.
- You can apply a policy from the 'Devices' interface also. Refer to the section '[Applying Policies](#)' for more details.

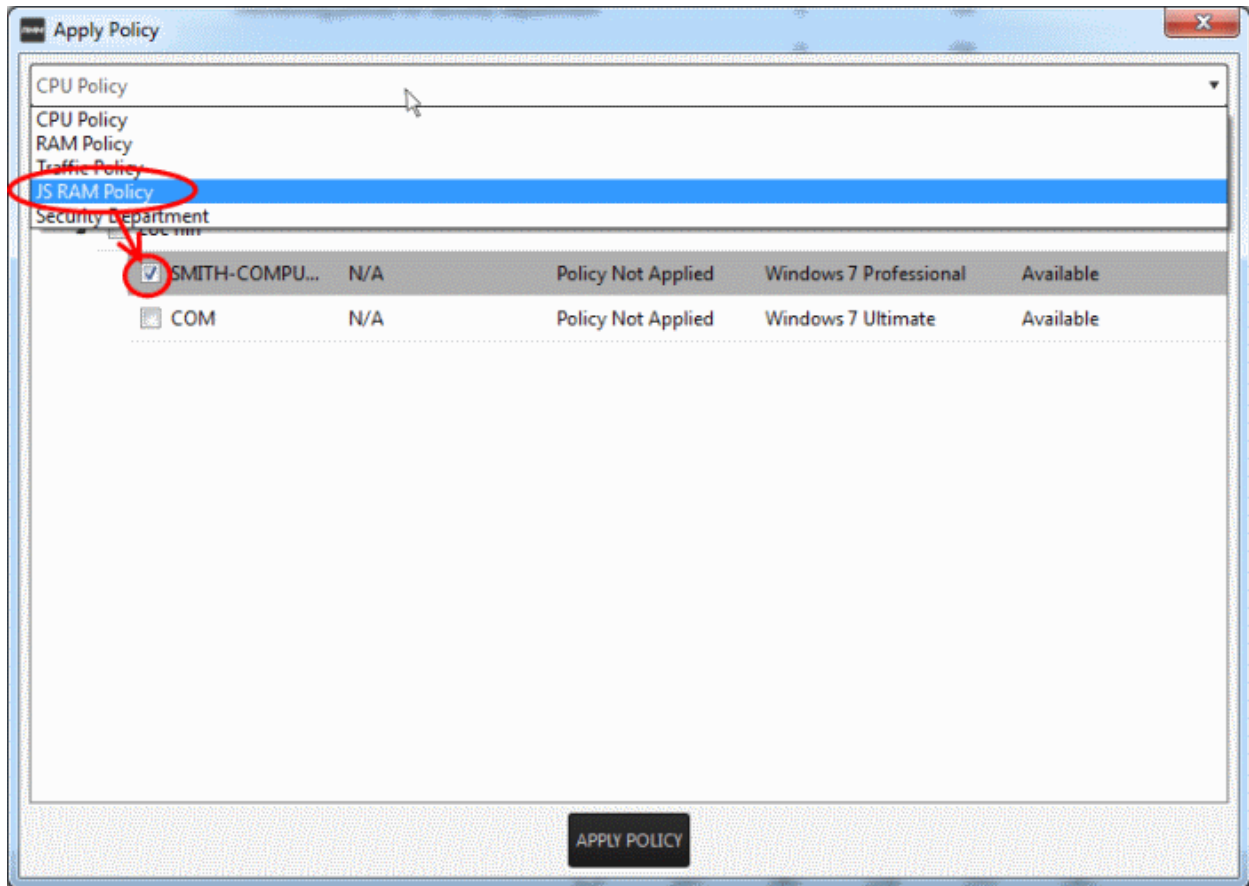
- Click the 'Apply Policy' button at the bottom of the 'Policies' interface



The 'Apply Policy' dialog will be displayed.



- Select the endpoint(s) from the list

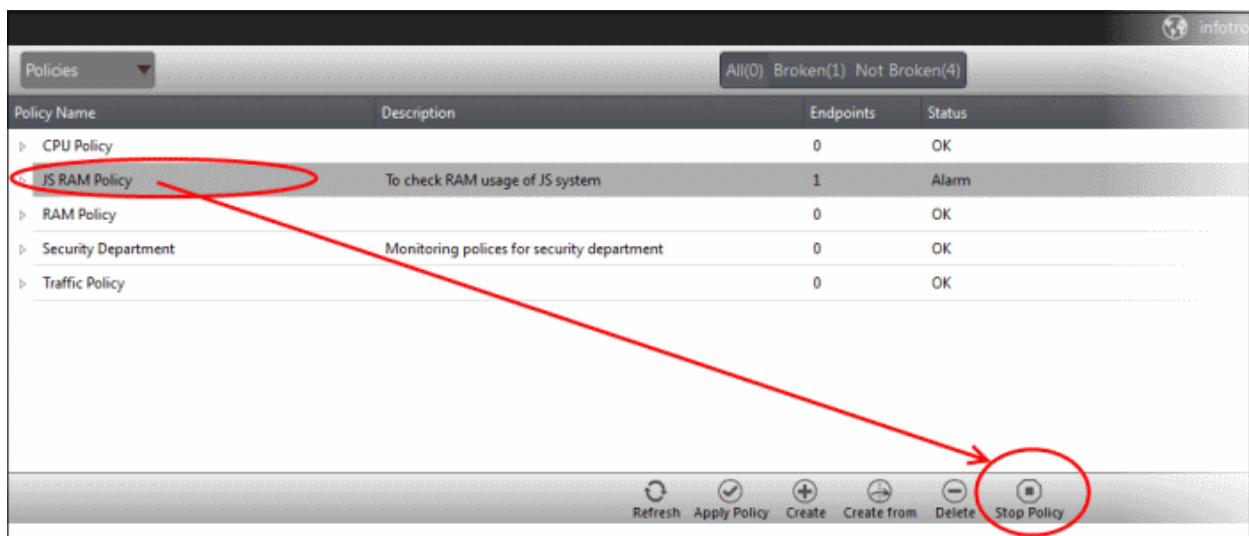


- Select the policy that you wish to apply to the selected endpoint from the drop-down at the top
- Click the 'Apply Policy' button

The policy will be deployed on the selected endpoints and will be listed in the main 'Policies' interface.

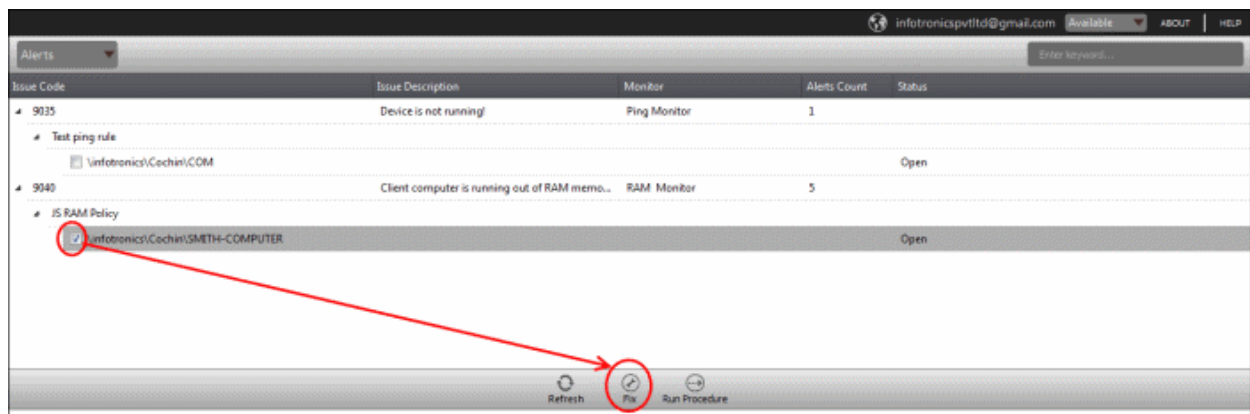
To stop a policy

- Select the policy from the list



- Click the 'Stop Policy' button.

The policy will no longer be applied for the endpoint(s). Now, if required, you can delete the policy. Refer to the section '**To delete a policy**' for more details.



Appendix - Issue Codes for Monitors

Issue Codes for Monitors, Description and Recommended Procedures				
Monitor	Issue Code & Name	Description	Advice	Procedure (if any)
RAM Monitor	9040 - Client computer is running out of RAM memory!	The RAM threshold has been reached	Check the list of running programs / services to see which is using more RAM, maybe there is a memory leak	Stop that program / service
Traffic Monitor	9038 - Network traffic exceeded the threshold value	The traffic limit imposed by the policy has been exceeded	Check the list of running programs / services to see which is using more bandwidth	Stop that program / service
Disk Health Monitor	9037 - Disk error detected!	A disk error was detected during check operation	Make sure the disk isn't damaged and backup the data before it fails completely	Scan and attempt to fix the disk errors
File Size Monitor	9029 - File size exceeds the limit allowed	The selected file has exceeded the size imposed by the policy	Check for reasons why the file size is exceeding in application logs and in system events	None
Folder Size Monitor	9030 - Folder size exceeds the limit allowed	The selected folder has exceeded the size imposed by the policy	Check for reasons why the folder size is exceeding in application logs and in system events	None
Ping Monitor	9035 - Device is not running	The specified device is offline or it could not be reached	Check if the device is ON and if the connection is ok	You can try to reboot the device
TCP Service Monitor	9034 - TCP service is running!	The specified TCP service is running	Check why the service started running	Stop that service
Hacker Monitor	9033 - Too many failed login attempts!	The limit of failed login attempts has been reached	Check if someone is trying to brute-force access into the system	You can disable the brute-forced account
CPU Monitor	9026 - High CPU Load	The CPU on the endpoint has been running at greater capacity and time than the entered values	High CPU levels for prolonged periods could indicate the need for a hardware upgrade or that too many processes are running concurrently. If the service desk ticket is generated repeatedly on the same endpoints then investigation may be	None

			required.	
Free Disk Space Monitor	9032 - PC is running out of free disk space	The disk quota specified by the policy was exceeded	Check for reasons why the disk space was exceeded	Cleanup the disk space (temporary files, cookies, etc...)
Process Monitor	9027 - Process not running	The selected process was not in the list of running processes.	Check the logs and system events to see why the process stopped	Start the process again
Services Monitor	9028 - Service not running	The selected service was not in the list of running services.	Check the logs and system events to see why the service stopped	Start the service again
Drive Space Monitor	9045 - OS drive is running out of free disk space	The operating system drive is running out of space	Check the logs, temporary files and user installed apps to see which one consumes more space	Clean unnecessary files
Drive Space Change Monitor	9046 - Drive space is consumed at a rapid rate	The drive space is being consumed with a rate higher than the selected threshold	Check the logs, temporary files and user installed apps to see which one consumes more space	You can get a bigger hard drive or you can reconfigure / uninstall that app
Web Monitor	9048 - Web page is up	Web page contains the specified data	Please check the machine to see why the web service is started. The service was supposed to be stopped.	None
Event Monitor	9031 - Windows Event Triggered	An event was triggered in windows events which matches the policy parameters	Please check the windows events log for details	None

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com