COMODO
Creating Trust Online®

COMODO
one

Comodo ONE

Software Version 3.3

Remote Monitoring and Management Quick Start Guide

Guide Version 6.1.116018

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo ONE - Remote Monitoring and Management - 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 Device Manager (CDM) module. Once you have added devices to CDM, 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 CDM, 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 Device Manager as described above.
ii. Enable the RMM extension in Comodo Device 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 alerts, and should be installed on a local workstation or server. To download the console, open CDM > Devices > Device List. 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 CDM (step ii, above). Should the need arise, you can also install the agent manually by clicking Devices > Device List, selecting your target endpoints then clicking 'Install MSI/Packages' > 'RMM Agent'.

Basic Concepts:

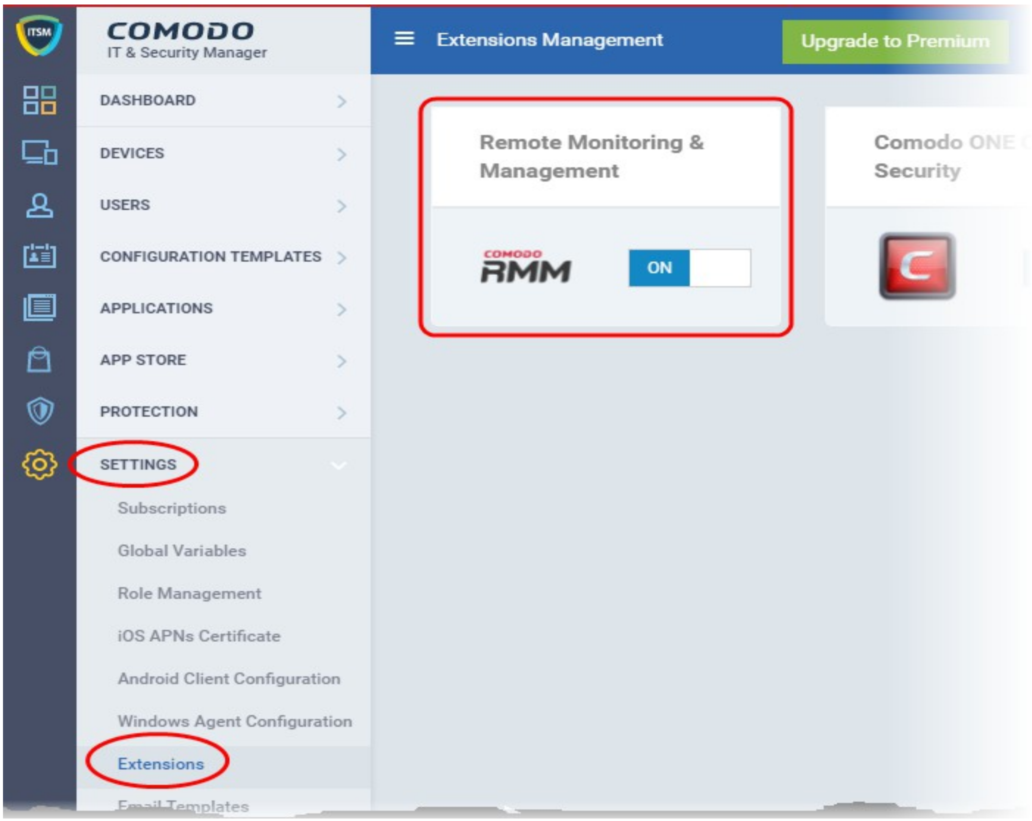
- **Action** – A task which can be run on target endpoints. Examples include install an application, reboot an endpoint, create a system restore point, run a registry cleaning task and more. Actions are added to procedures.
- **Procedure** – A collection of one or more actions. Procedures can be directly 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 send alerts to the administrator if certain conditions are met. You can then investigate the alerts, create a service desk ticket 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.

- **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

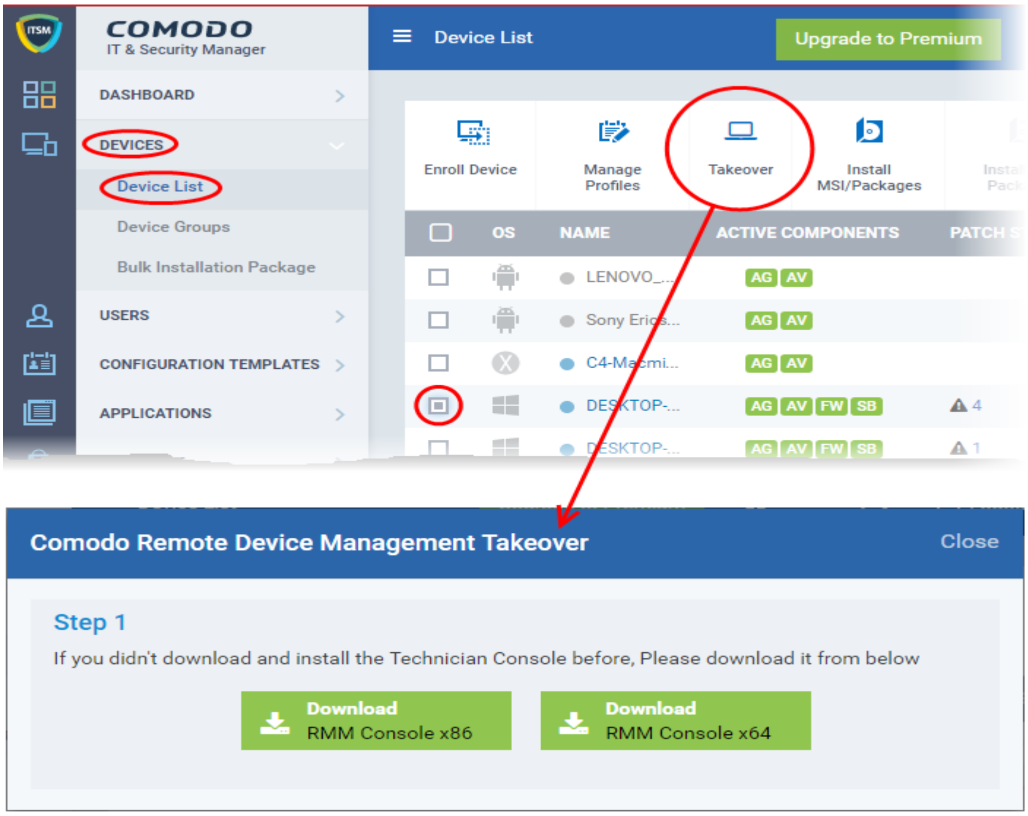
- Login to your Comodo One account at **https://one.comodo.com/app/login**.
- Click the 'Licensed Applications' icon from the top and select 'IT and Security Manager', to open the ITSM console.
- Click 'Settings' at the left and choose 'Extensions' and Ensure 'Comodo RMM' is switched 'ON':



- Next, click 'Devices' > 'Device List' from the left.

All devices added to CDM will be displayed.

- Click the 'Takeover' at the top of the interface. This will start a wizard which allows you to download the RMM console setup files.



Comodo Remote Device Management Takeover

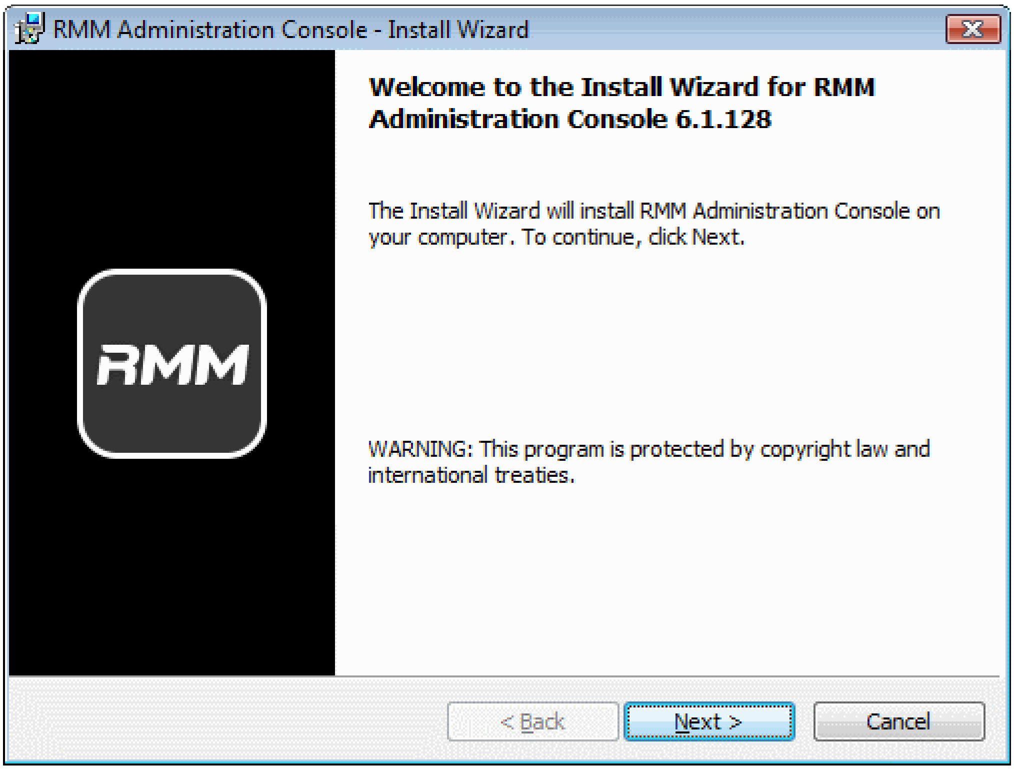
Step 1

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

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:



Welcome to the Install Wizard for RMM Administration Console 6.1.128

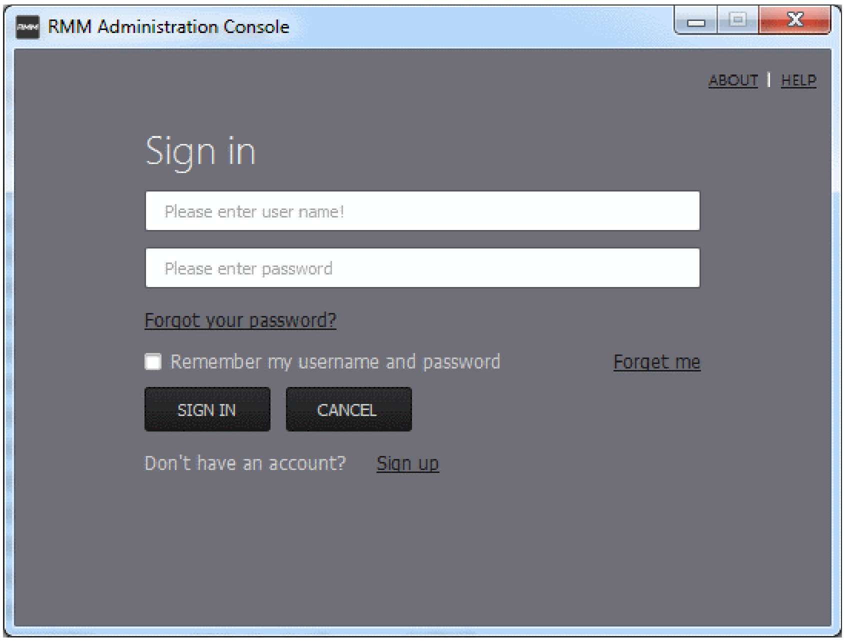
The Install Wizard will install RMM Administration Console on your computer. To continue, click Next.

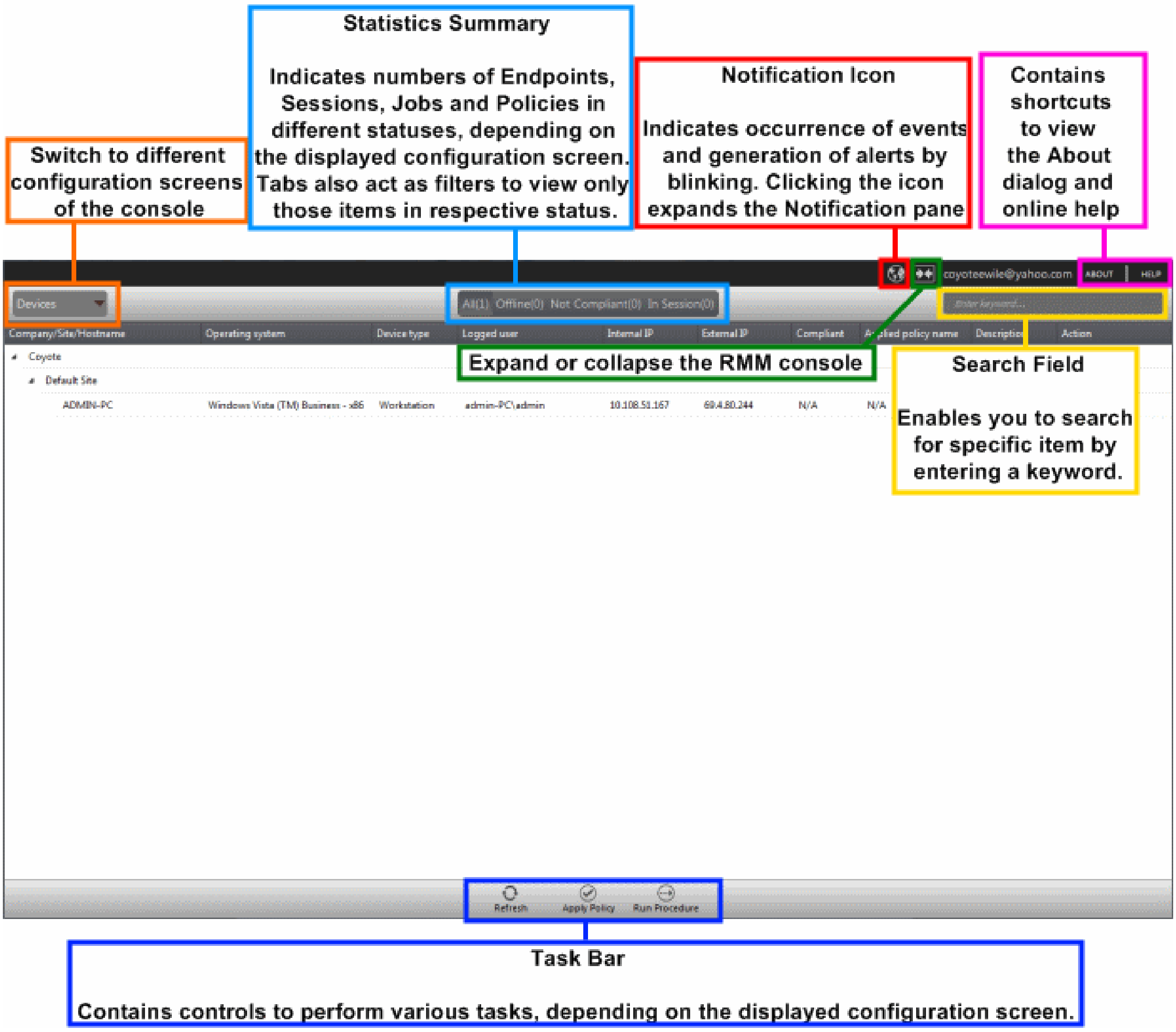
WARNING: This program is protected by copyright law and international treaties.

- 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'.





Statistics Summary

Indicates numbers of Endpoints, Sessions, Jobs and Policies in different statuses, depending on the displayed configuration screen. Tabs also act as filters to view only those items in respective status.

Notification Icon

Indicates occurrence of events and generation of alerts by blinking. Clicking the icon expands the Notification pane

Contains shortcuts to view the About dialog and online help

Switch to different configuration screens of the console

Expand or collapse the RMM console

Search Field

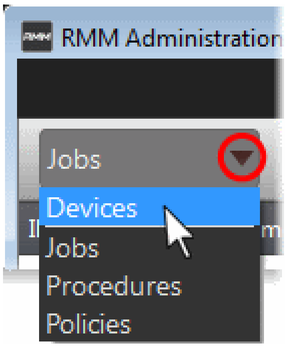
Enables you to search for specific item by entering a keyword.

Task Bar

Contains controls to perform various tasks, depending on the displayed configuration screen.

Company/Site/Hostname	Operating system	Device type	Logged user	Internal IP	External IP	Compliant	A-plied policy name	Descriptio	Action
Coyote									
Default Site									
ADMIN-PC	Windows Vista (TM) Business - x86	Workstation	admin-PC\admin	10.108.51.167	69.4.80.244	N/A	N/A		

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. Alerts 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.

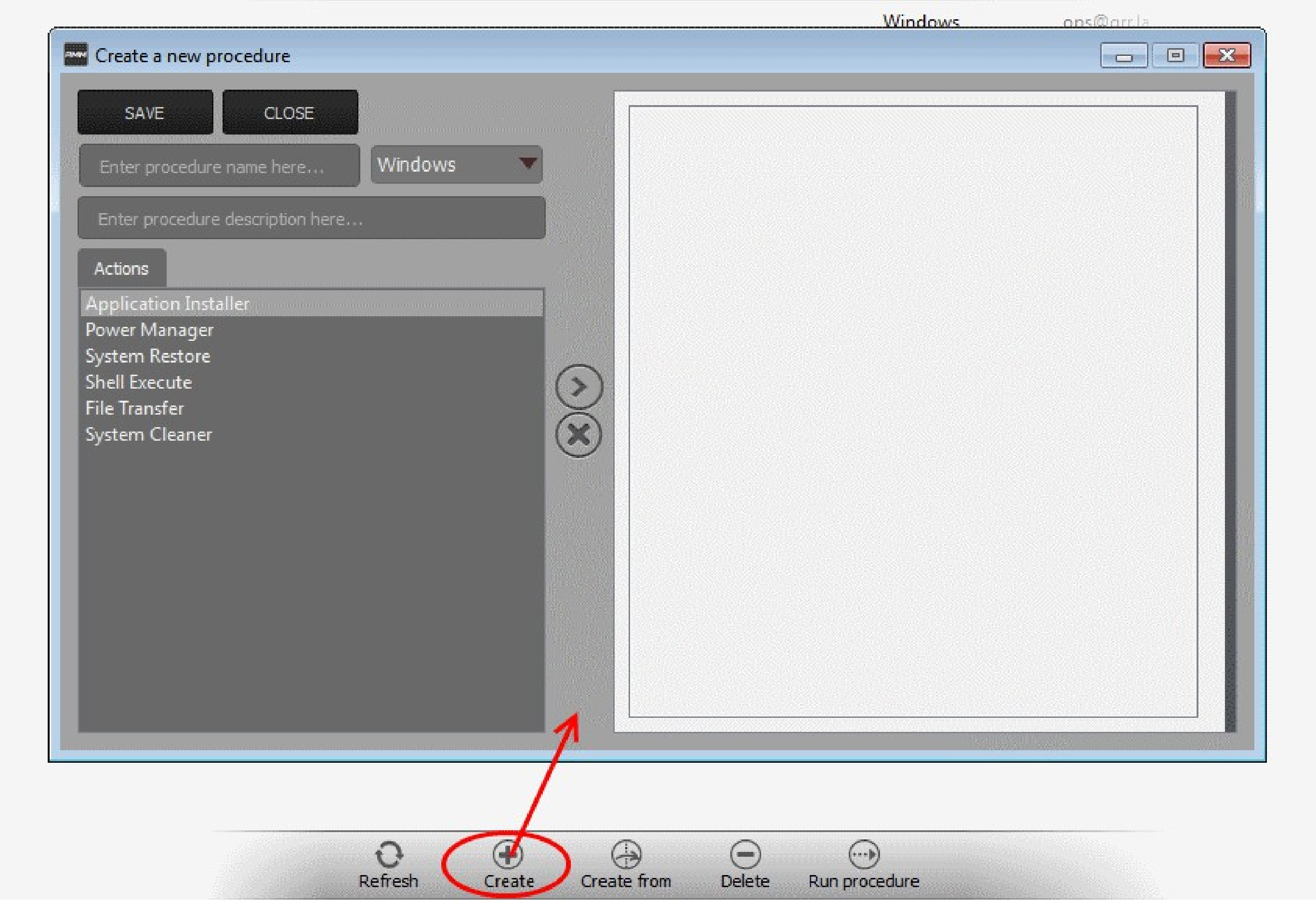
Create Procedures

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: • Application Install • Enter the following parameters: • 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: • Restart • Restart in safe mode

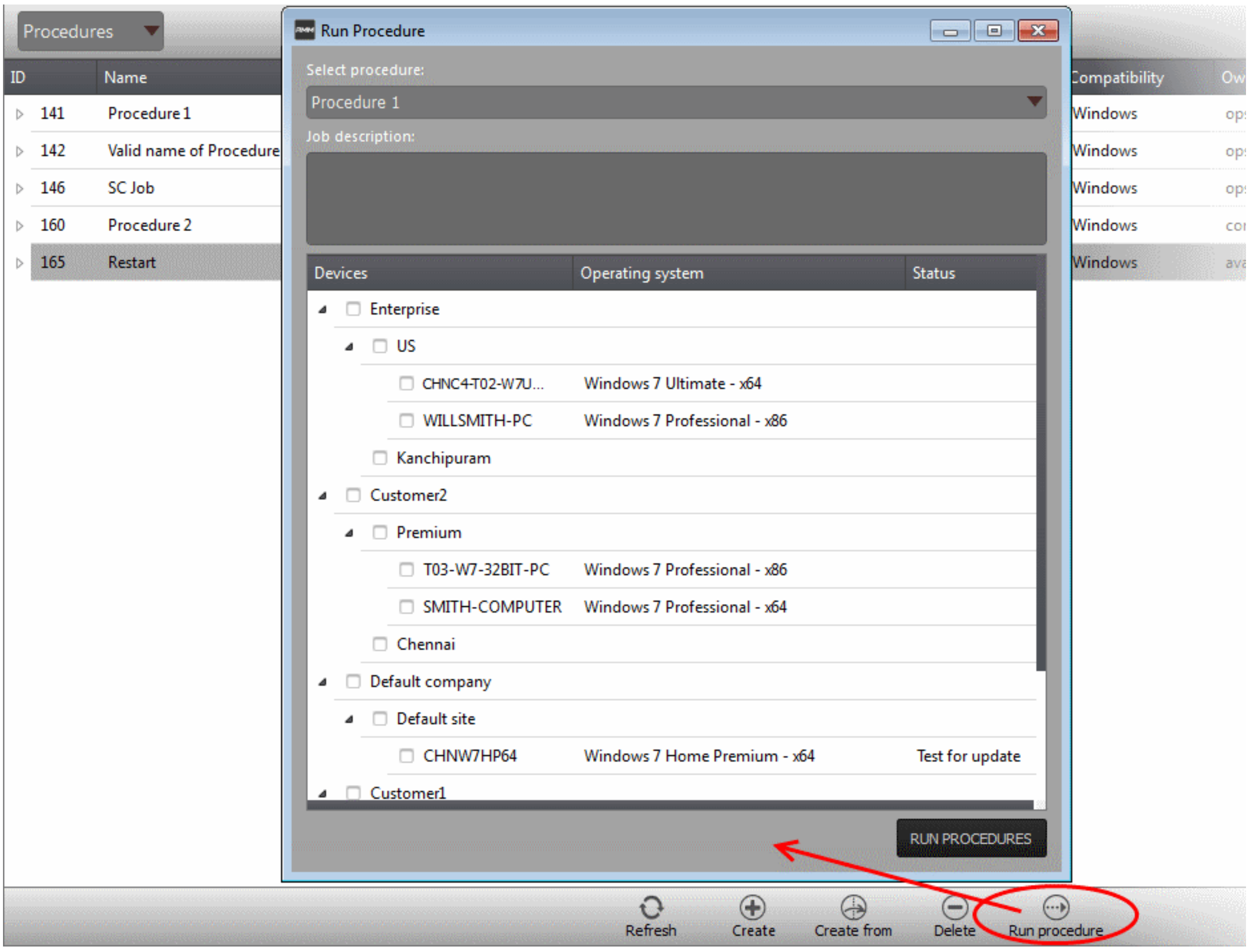
Action	Parameters Required
	- Shutdown
System Restore	Choose whether to create a restore point or to restore the system to a previous state. - Enter the name of the restore point to be created or the name of the restore point, to which the system needs to be rolled back.
Shell Execute	Run a particular file on a managed endpoint Basic - Enter the execution command for the process - Enter the parameters to be passed to the process Advanced - Enter the working directory for the process - Choose the execution options: - 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:\lps-temp\file-transfer at the endpoint.
System Cleaner	Execute one of the following system scanning and cleaning tasks: - 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.



ID	Name	Compatibility	Ow
141	Procedure 1	Windows	ops
142	Valid name of Procedure	Windows	ops
146	SC Job	Windows	ops
160	Procedure 2	Windows	cor
165	Restart	Windows	ava

Select procedure: Procedure 1

Job description:

Devices	Operating system	Status
□ Enterprise		
□ US		
□ CHNC4-T02-W7U...	Windows 7 Ultimate - x64	
□ WILLSMITH-PC	Windows 7 Professional - x86	
□ Kanchipuram		
□ Customer2		
□ Premium		
□ T03-W7-32BIT-PC	Windows 7 Professional - x86	
□ SMITH-COMPUTER	Windows 7 Professional - x64	
□ Chennai		
□ Default company		
□ Default site		
□ CHNW7HP64	Windows 7 Home Premium - x64	Test for update
□ Customer1		

- 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.

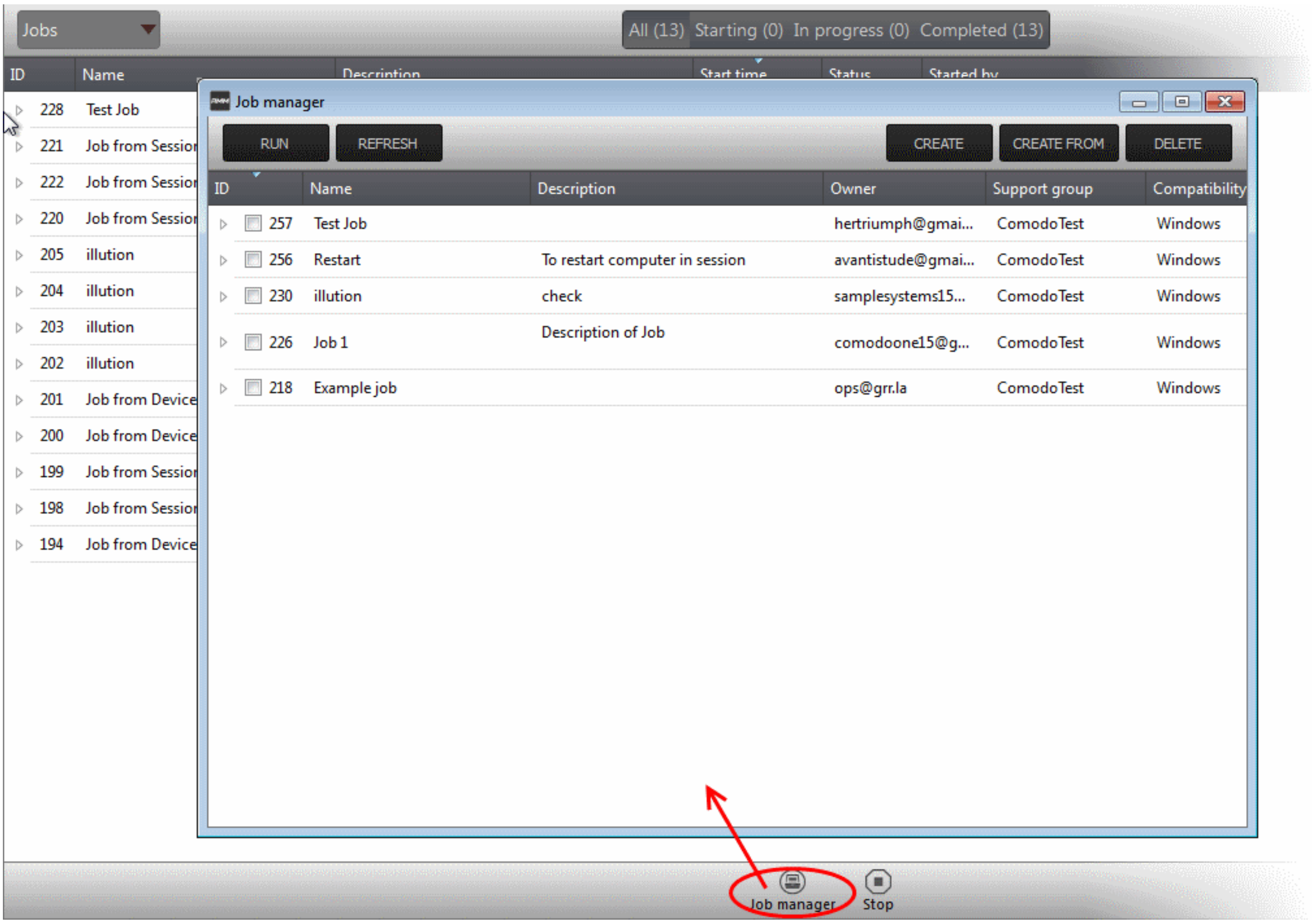
Create and Execute Jobs

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:



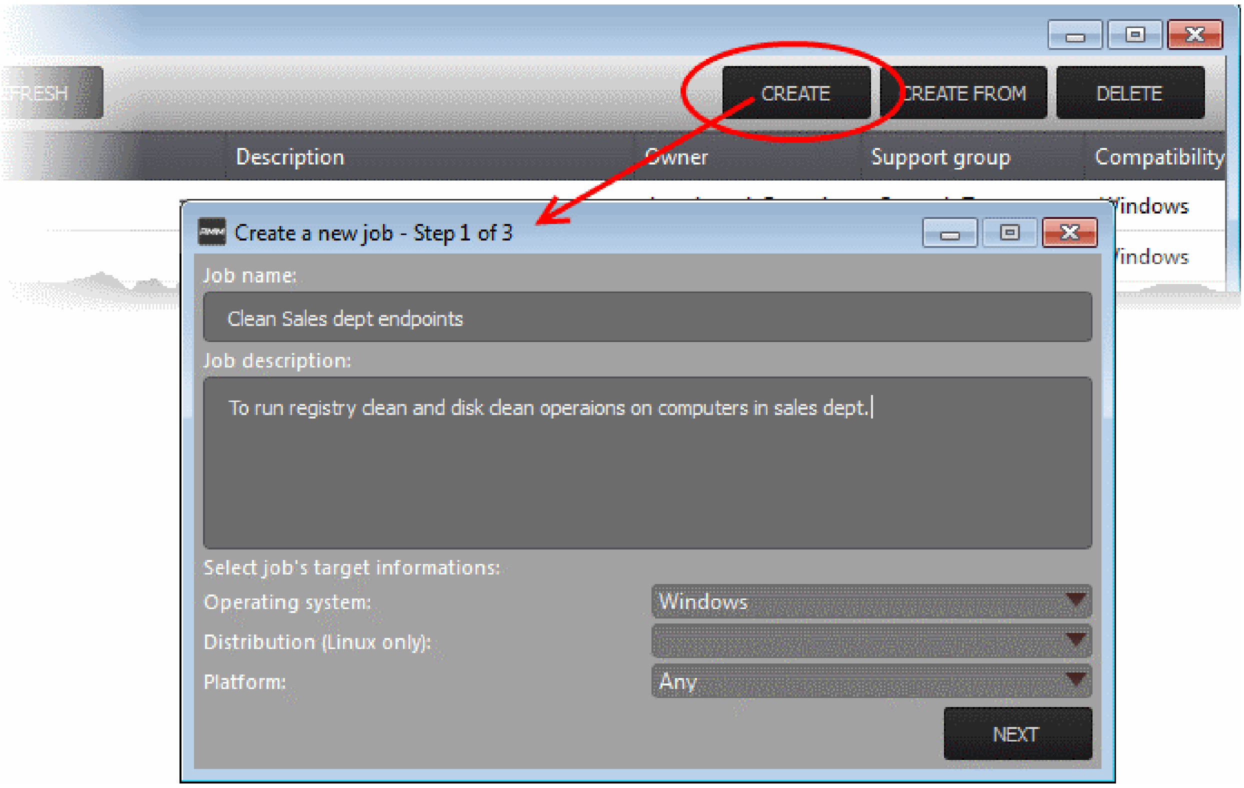
ID	Name
228	Test Job
221	Job from Session
222	Job from Session
220	Job from Session
205	illution
204	illution
203	illution
202	illution
201	Job from Device
200	Job from Device
199	Job from Session
198	Job from Session
194	Job from Device

ID	Name	Description	Owner	Support group	Compatibility
257	Test Job		hertriumph@gmai...	ComodoTest	Windows
256	Restart	To restart computer in session	avantistude@gmai...	ComodoTest	Windows
230	illution	check	samplesystems15...	ComodoTest	Windows
226	Job 1	Description of Job	comodoone15@g...	ComodoTest	Windows
218	Example job		ops@grr.la	ComodoTest	Windows

All jobs created so far will be displayed.

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

The job creation wizard will start.



Job name: Clean Sales dept endpoints

Job description: To run registry clean and disk clean operaions on computers in sales dept.

Select job's target informations:

Operating system: Windows

Distribution (Linux only):

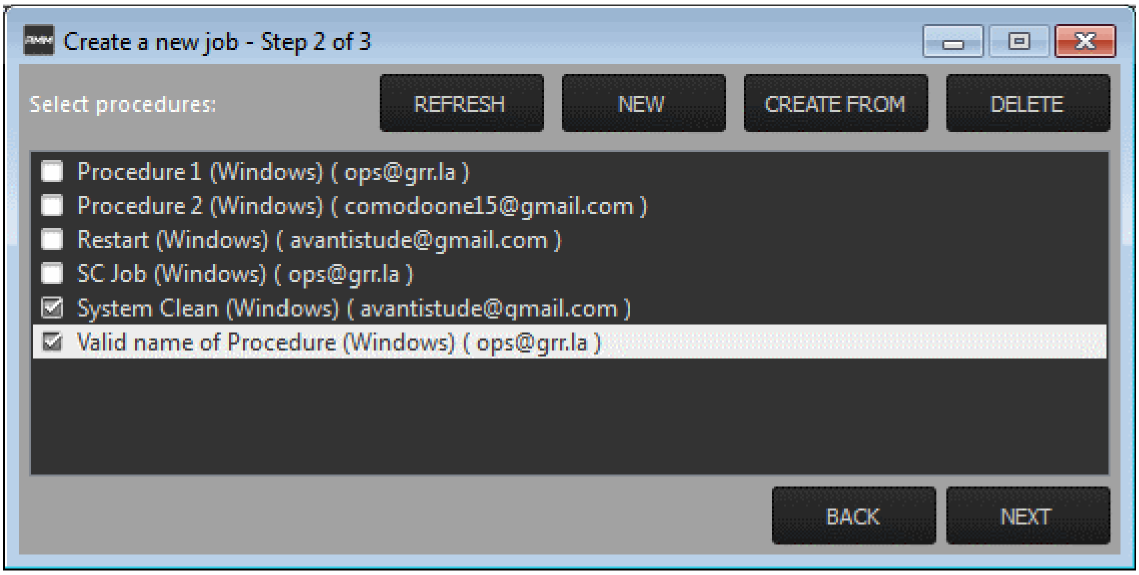
Platform: Any

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**.


Create a new job - Step 2 of 3

Select procedures:

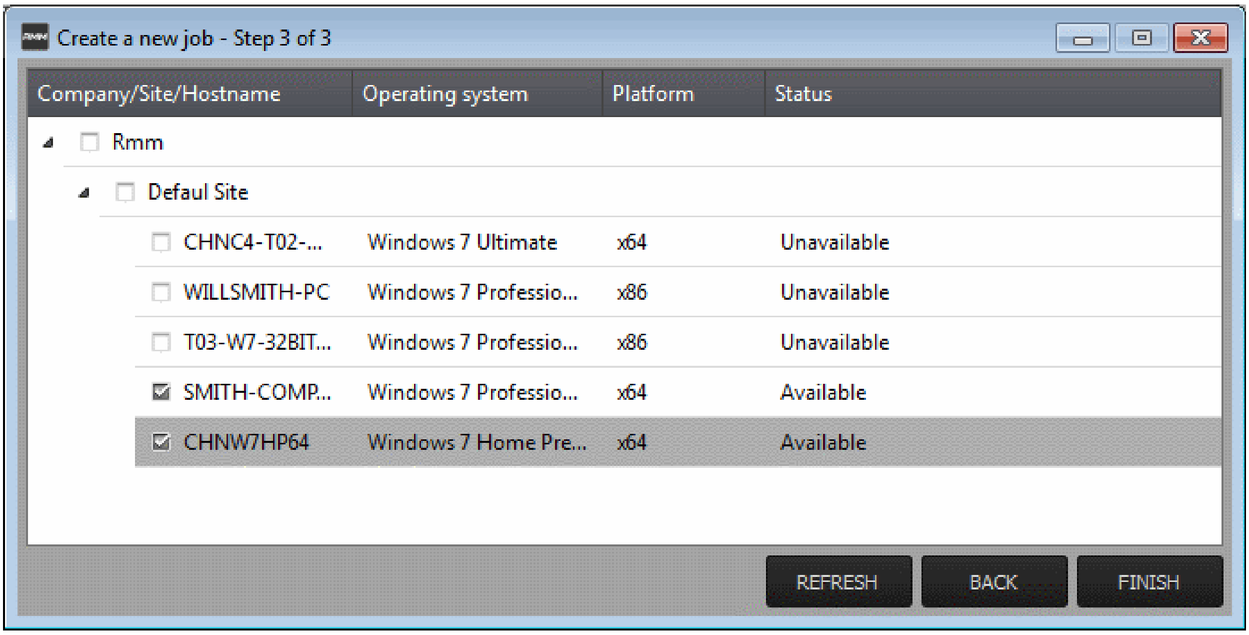
- □ Procedure 1 (Windows) (ops@grr.la)
- □ Procedure 2 (Windows) (comodoone15@gmail.com)
- □ Restart (Windows) (avantistude@gmail.com)
- □ SC Job (Windows) (ops@grr.la)
- ☑ System Clean (Windows) (avantistude@gmail.com)
- ☑ Valid name of Procedure (Windows) (ops@grr.la)

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:



Create a new job - Step 3 of 3

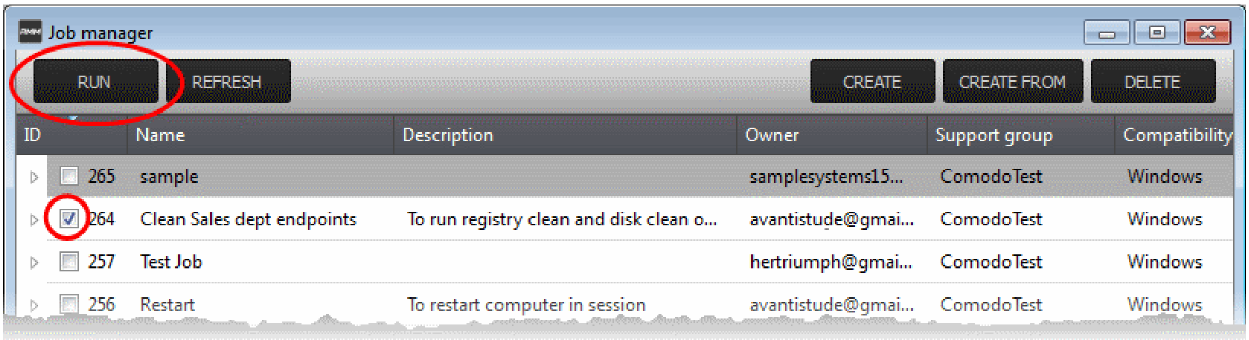
Company/Site/Hostname	Operating system	Platform	Status
□ Rmm			
□ Defaul Site			
□ CHNC4-T02-...	Windows 7 Ultimate	x64	Unavailable
□ WILLSMITH-PC	Windows 7 Professio...	x86	Unavailable
□ T03-W7-32BIT...	Windows 7 Professio...	x86	Unavailable
☑ SMITH-COMP...	Windows 7 Professio...	x64	Available
☑ CHNW7HP64	Windows 7 Home Pre...	x64	Available

- 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

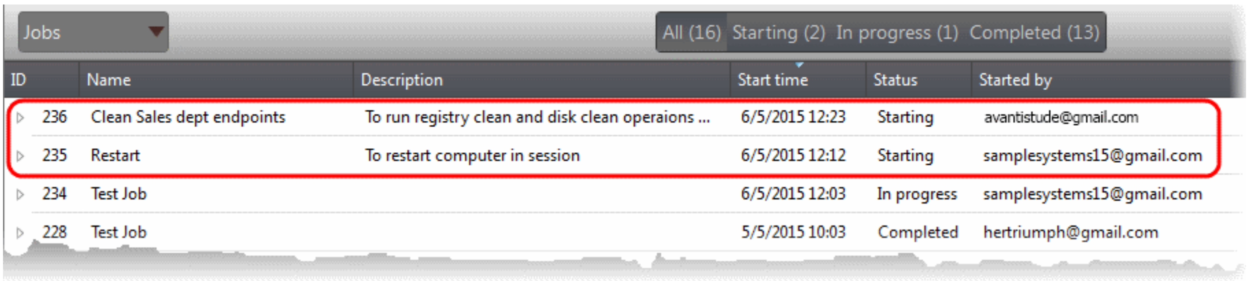


Job manager

ID	Name	Description	Owner	Support group	Compatibility
□ 265	sample		samplesystems15...	ComodoTest	Windows
☑ 264	Clean Sales dept endpoints	To run registry clean and disk clean o...	avantistude@gmai...	ComodoTest	Windows
□ 257	Test Job		hertriumph@gmai...	ComodoTest	Windows
□ 256	Restart	To restart computer in session	avantistude@gmai...	ComodoTest	Windows

- 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.

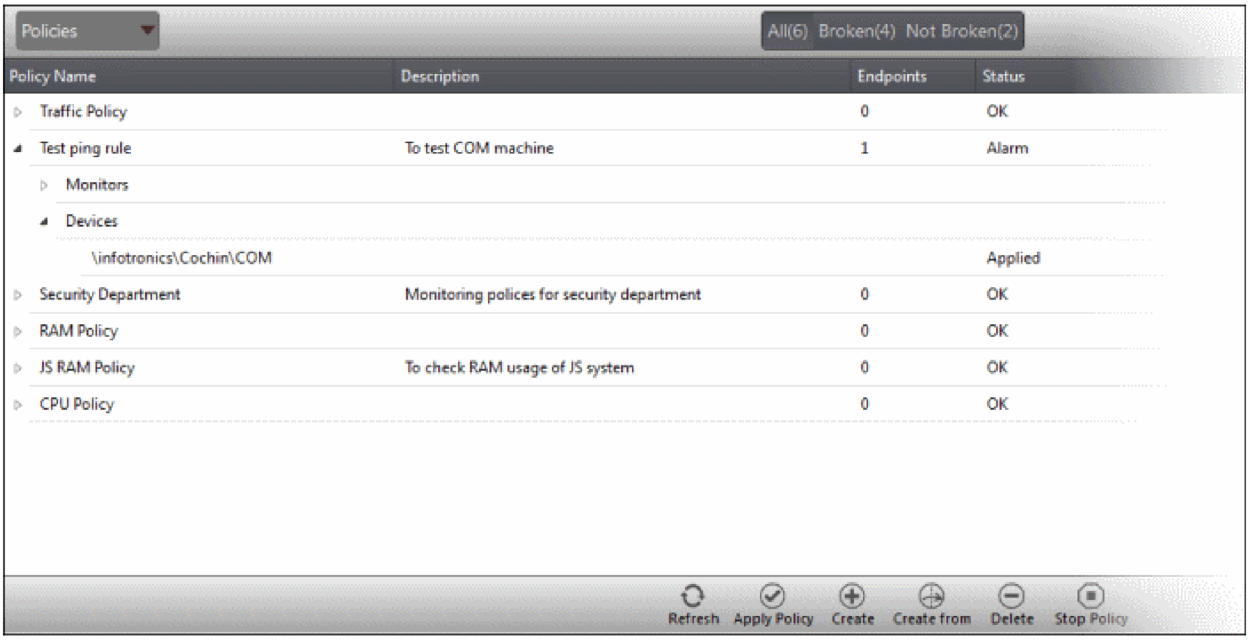


ID	Name	Description	Start time	Status	Started by
236	Clean Sales dept endpoints	To run registry clean and disk clean operaions ...	6/5/2015 12:23	Starting	avantistude@gmail.com
235	Restart	To restart computer in session	6/5/2015 12:12	Starting	samplesystems15@gmail.com
234	Test Job		6/5/2015 12:03	In progress	samplesystems15@gmail.com
228	Test Job		5/5/2015 10:03	Completed	hertriumph@gmail.com

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 alerts and/or service desks tickets are created if an endpoint violates the policy. Alerts can be viewed from the 'Alerts' interface. 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.

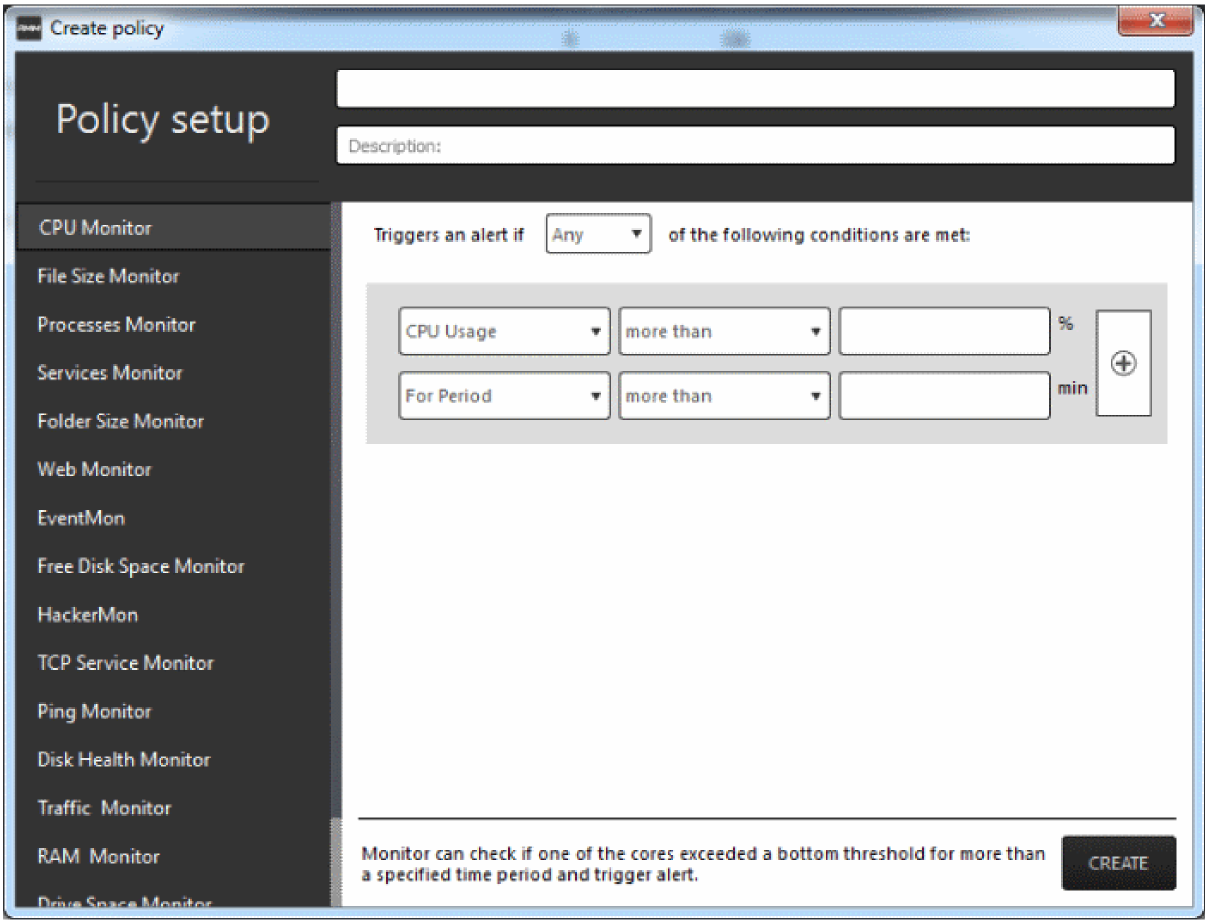


Policy Name	Description	Endpoints	Status
Traffic Policy		0	OK
Test ping rule	To test COM machine	1	Alarm
Monitors			
Devices			
\infotronics\Cochin\COM			Applied
Security Department	Monitoring polices for security department	0	OK
RAM Policy		0	OK
JS RAM Policy	To check RAM usage of JS system	0	OK
CPU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

To create a new policy

- Click 'Create' from the bottom of the interface

The 'Create policy' interface will open.



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

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

- 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.

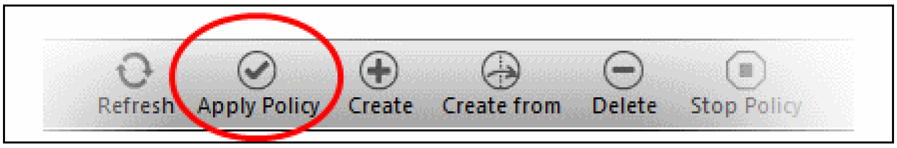
- Click 'Create' to save your policy.

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.

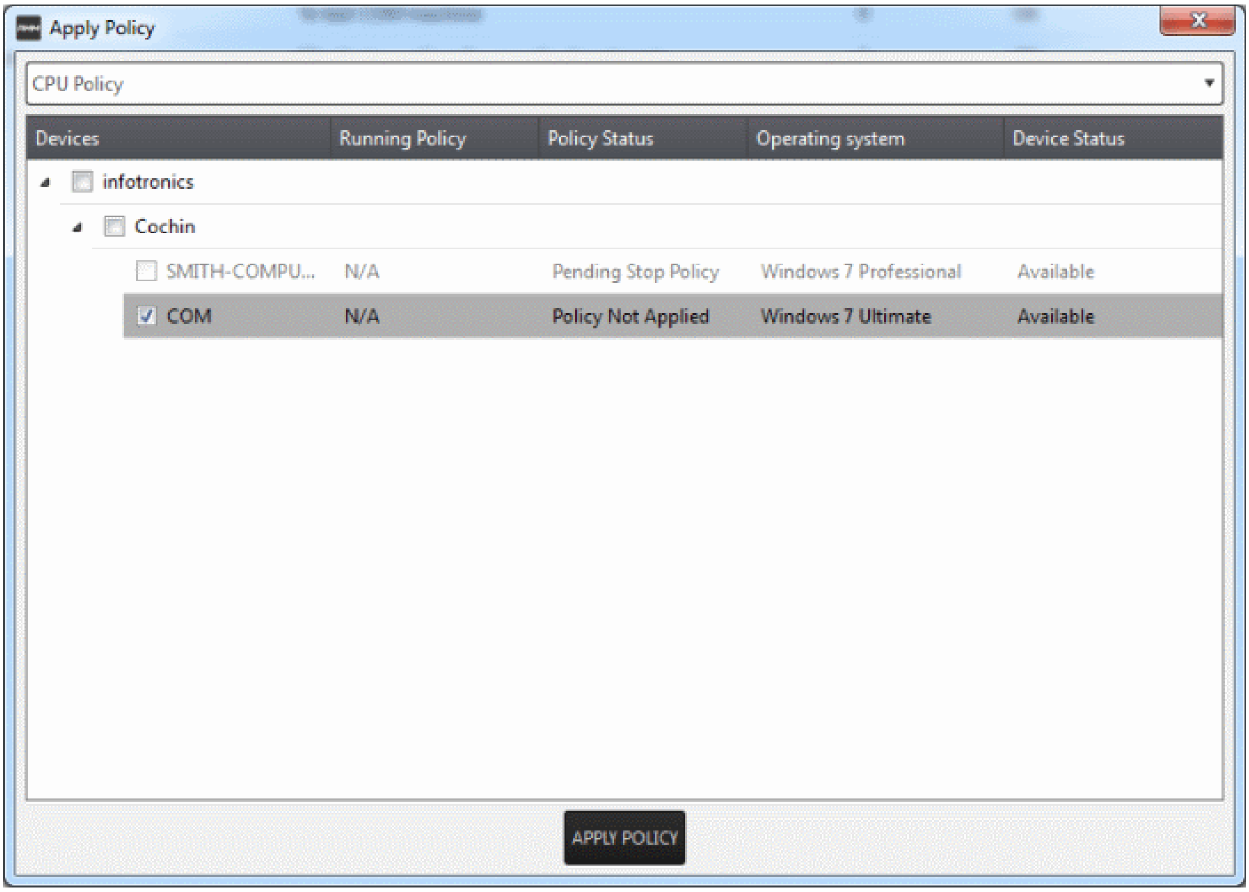
To apply a policy to endpoints

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

- Click 'Apply Policy' from either of these interfaces

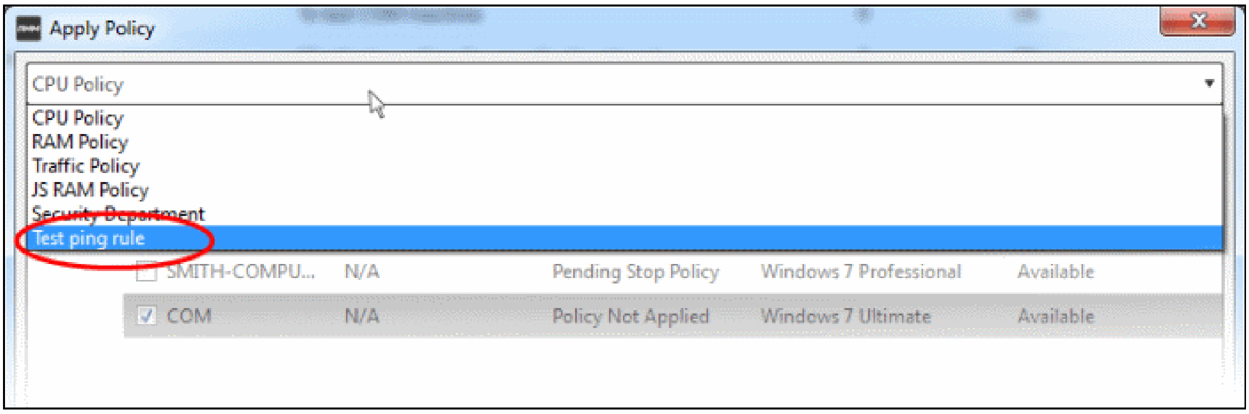


The 'Apply Policy' dialog will open with a list of endpoints enrolled for your account.



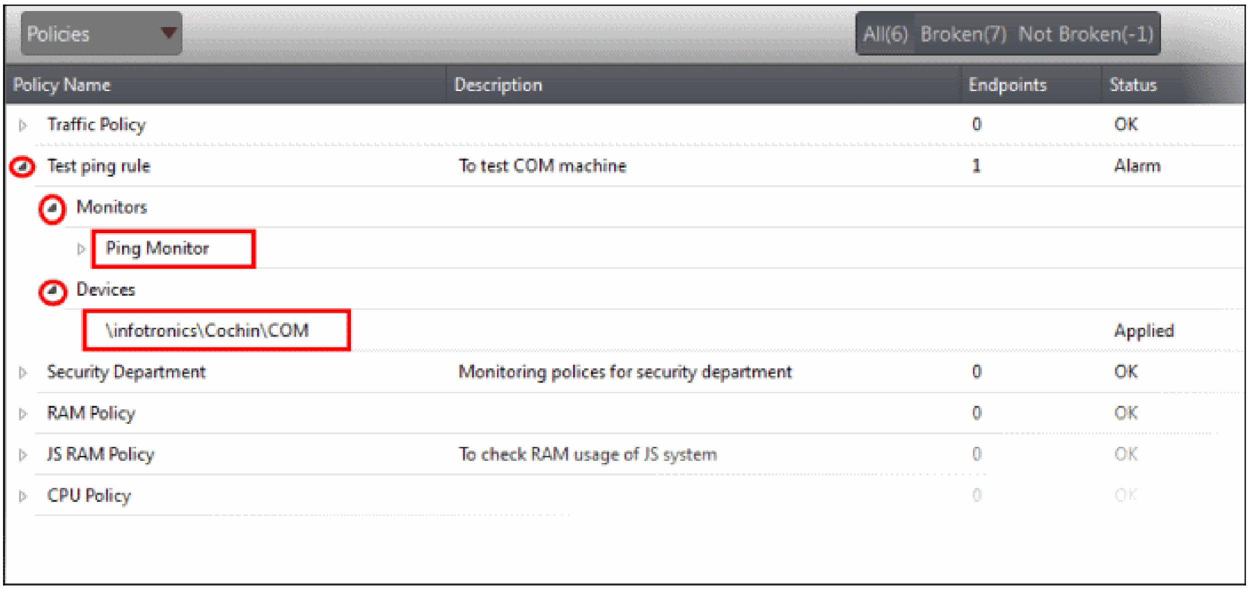
Devices	Running Policy	Policy Status	Operating system	Device Status
□ infotronics				
□ Cochin				
□ SMITH-COMPU...	N/A	Pending Stop Policy	Windows 7 Professional	Available
☑ COM	N/A	Policy Not Applied	Windows 7 Ultimate	Available

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


Apply Policy
CPU Policy
CPU Policy
RAM Policy
Traffic Policy
JS RAM Policy
Security Department
Test ping rule
SMITH-COMPU... N/A Pending Stop Policy Windows 7 Professional Available
COM N/A Policy Not Applied Windows 7 Ultimate Available

- 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

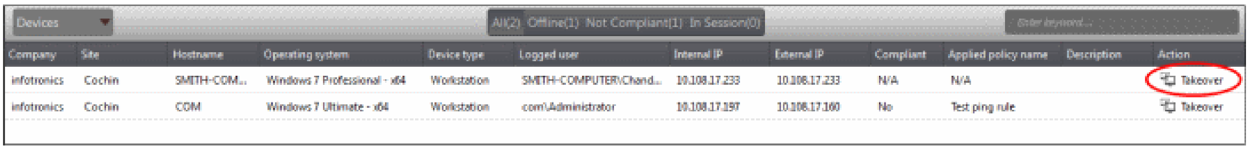
The support session enables you to take remote desktop control of the client computer and perform maintenance tasks and resolve issues identified in them. By establishing a support session you can:

- 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 alerts

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

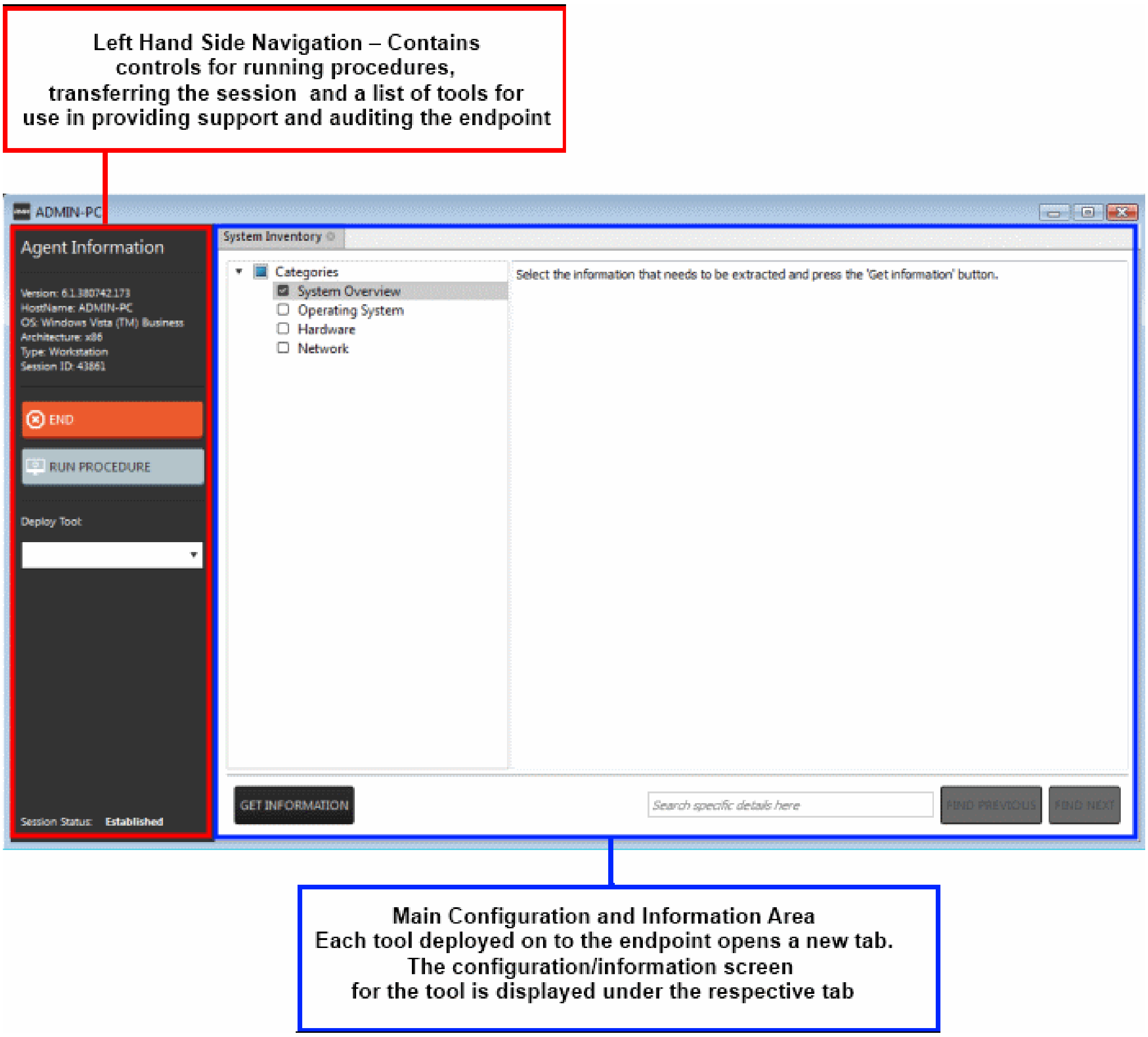


Company	Site	Hostname	Operating system	Device type	Logged user	Internal IP	External IP	Compliant	Applied policy name	Description	Action
infotronics	Cochin	SMITH-COM...	Windows 7 Professional - x64	Workstation	SMITH-COMPUTER\Chand...	10.108.17.233	10.108.17.233	N/A	N/A		Takeover
infotronics	Cochin	COM	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.

A session will be established.

The Support Session Interface



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

ADMIN-PC

Agent Information

Version: 6.1.380742.173
HostName: ADMIN-PC
OS: Windows Vista (TM) Business
Architecture: x86
Type: Workstation
Session ID: 43861

Deploy Tool:

Session Status: Established

System Inventory

- Categories
  - ☑ System Overview
  - □ Operating System
  - □ Hardware
  - □ Network

Select the information that needs to be extracted and press the 'Get information' button.

Search specific details here

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

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.

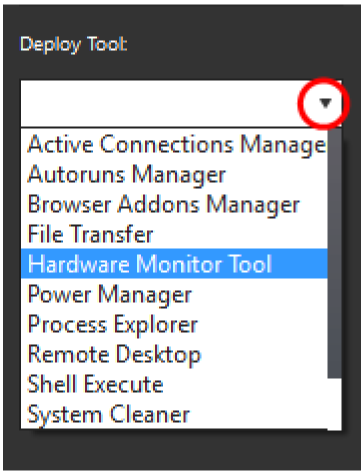
- **END** – Concludes the support session and closes the session window for the endpoint.
- **RUN PROCEDURE** – Allows you to run procedures on the endpoint. You can select procedures from those that are available in the 'Procedures' interface. Refer to the section **Run a Procedure** for more details.
- **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


Deploy Tool:

- Active Connections Manage
- Autoruns Manager
- Browser Addons Manager
- File Transfer
- Hardware Monitor Tool
- Power Manager
- Process Explorer
- Remote Desktop
- Shell Execute
- System Cleaner

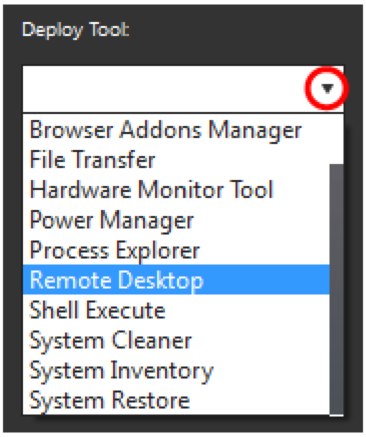
The 'Deploy Tool' drop-down contains handy diagnostic and repair tools which can be deployed to endpoints. For example, you can view all running processes and kill unnecessary processes, access the command line interface of the endpoint, run system clean operations and so on. The service session window 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 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	• 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

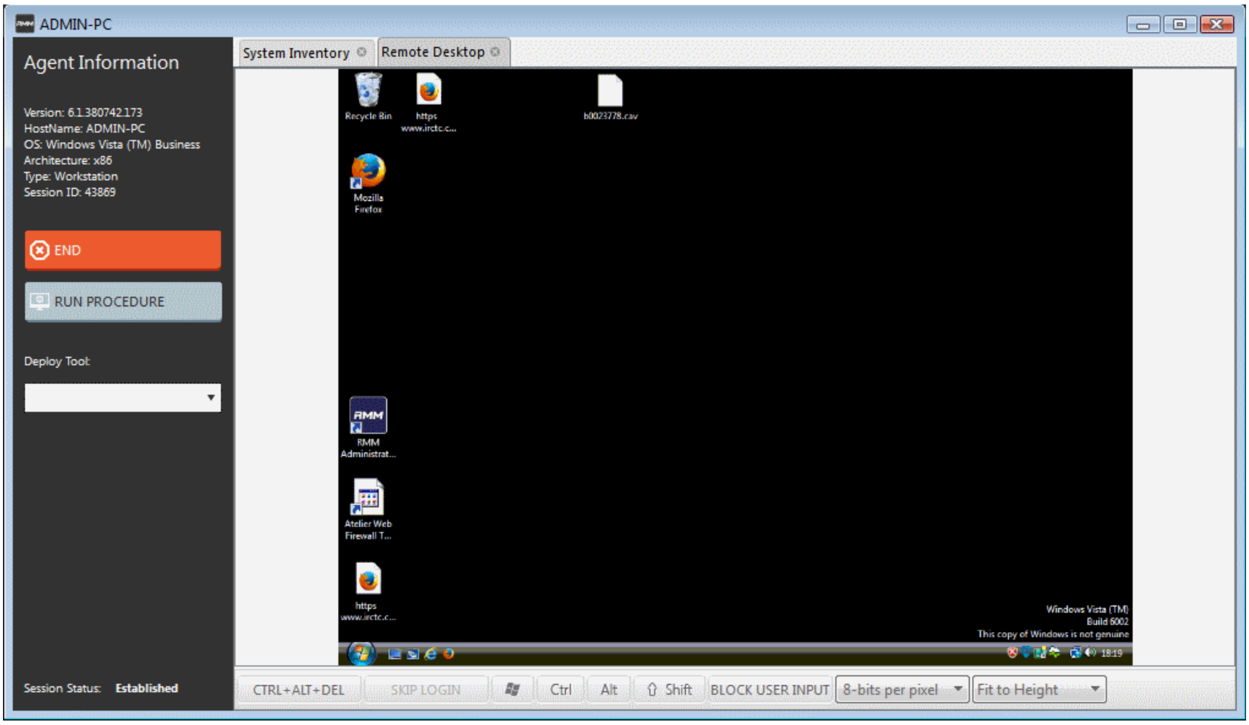


RMM allows you to gain remote desktop access to the endpoint and execute necessary actions to solve issues. During the time the you are working with the endpoint, the end-user can view the actions taken by you and can operate the computer simultaneously. If the end-user wishes, he/she can even terminate the desktop connection by clicking Disconnect from the client chat window.

To initiate a remote desktop connection

- Enter a message in the chat window to request remote desktop access
- Once the client accepts the connection request, choose Remote Desktop from the Deploy Tool drop-down at the left

The desktop of the endpoint will open in a new 'Remote Desktop' tab in the main configuration area. During the session you will be able to continue the conversation over the chat window.


ADMIN-PC

Agent Information

Version: 6.1.380742.173
HostName: ADMIN-PC
OS: Windows Vista (TM) Business
Architecture: x86
Type: Workstation
Session ID: 43869

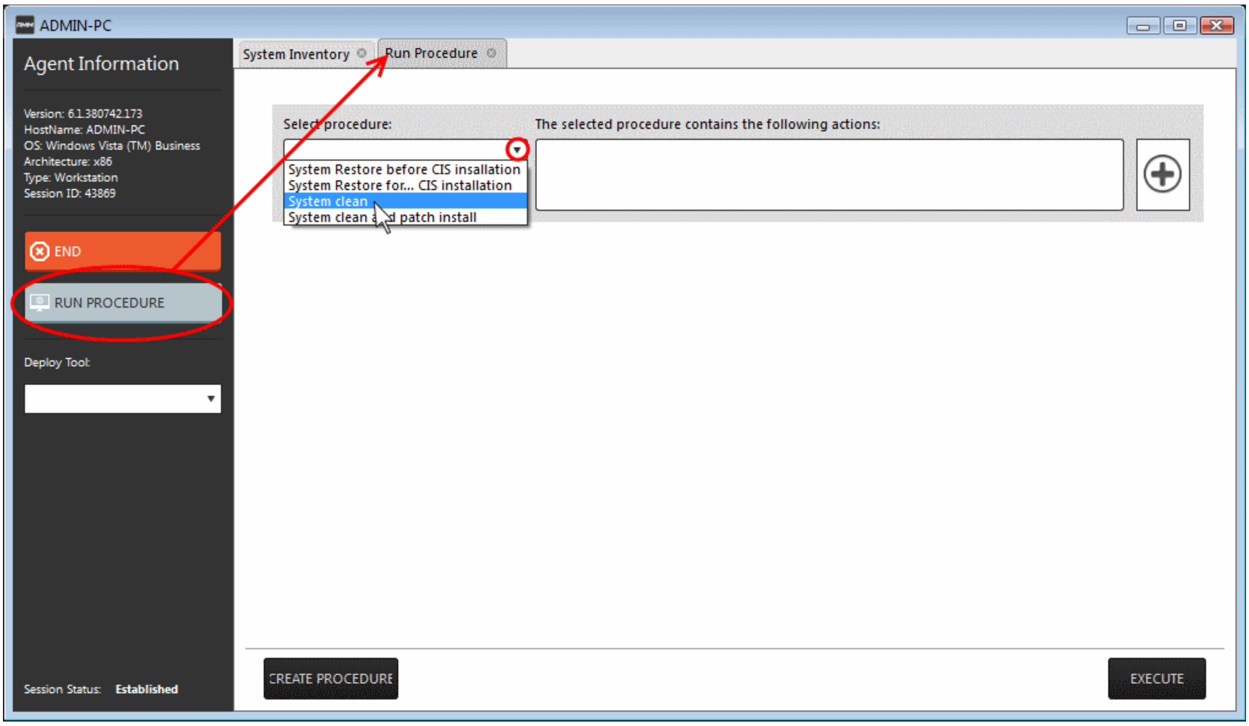
Session Status: Established

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.

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 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**