



**COMODO**  
Creating Trust Online®

**COMODO**  
**one**

# Comodo ONE

Software Version 1.8

---

## Remote Monitoring and Management Quick Start Guide

Guide Version 1.8.050815

---

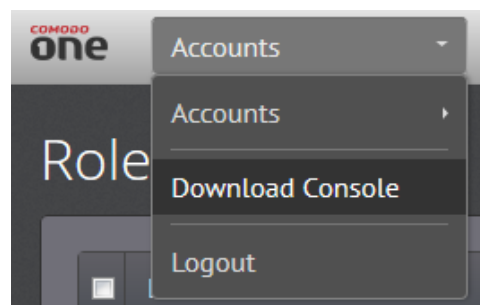
Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

# Comodo ONE - Remote Monitoring and Management - Quick Start Guide

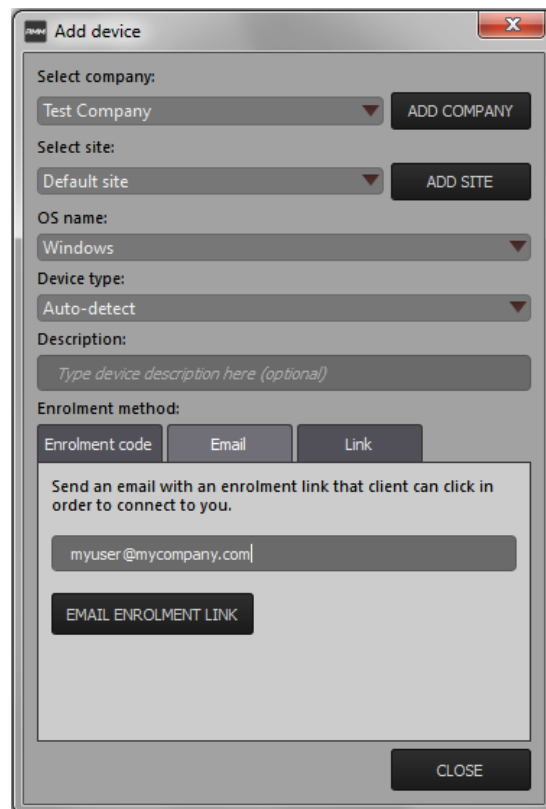
This tutorial briefly explains how an agent can setup Comodo Remote Monitoring and Management (RMM).

Comodo RMM setup and management involves three components - the web interface, the admin console and the endpoint 'client software.

- The RMM web Interface is for user management and can be accessed by logging in at one.comodo.com then opening the RMM module.
- The admin console is the chief management software and is used to monitor endpoints, define policies and configure/respond to endpoint alerts. The console should be installed on a local workstation or server and can be downloaded from the RMM web interface :



- RMM client software must be installed on each endpoint so that it may report to the admin console. To download and provision agents from the admin console:
  - Client software download links can be obtained from the 'Enrollment Method' section of the 'Add Device' interface:

A screenshot of the 'Add device' dialog box in the Comodo ONE web interface. The dialog has a title bar with 'Add device' and a close button. It contains several sections:

- Select company:** A dropdown menu showing 'Test Company' and an 'ADD COMPANY' button.
- Select site:** A dropdown menu showing 'Default site' and an 'ADD SITE' button.
- OS name:** A dropdown menu showing 'Windows'.
- Device type:** A dropdown menu showing 'Auto-detect'.
- Description:** A text input field with the placeholder text 'Type device description here (optional)'.
- Enrolment method:** Three radio buttons: 'Enrolment code', 'Email', and 'Link'. The 'Email' option is selected.
- Email input:** A text input field containing 'myuser@mycompany.com'.
- Buttons:** An 'EMAIL ENROLMENT LINK' button and a 'CLOSE' button at the bottom right.

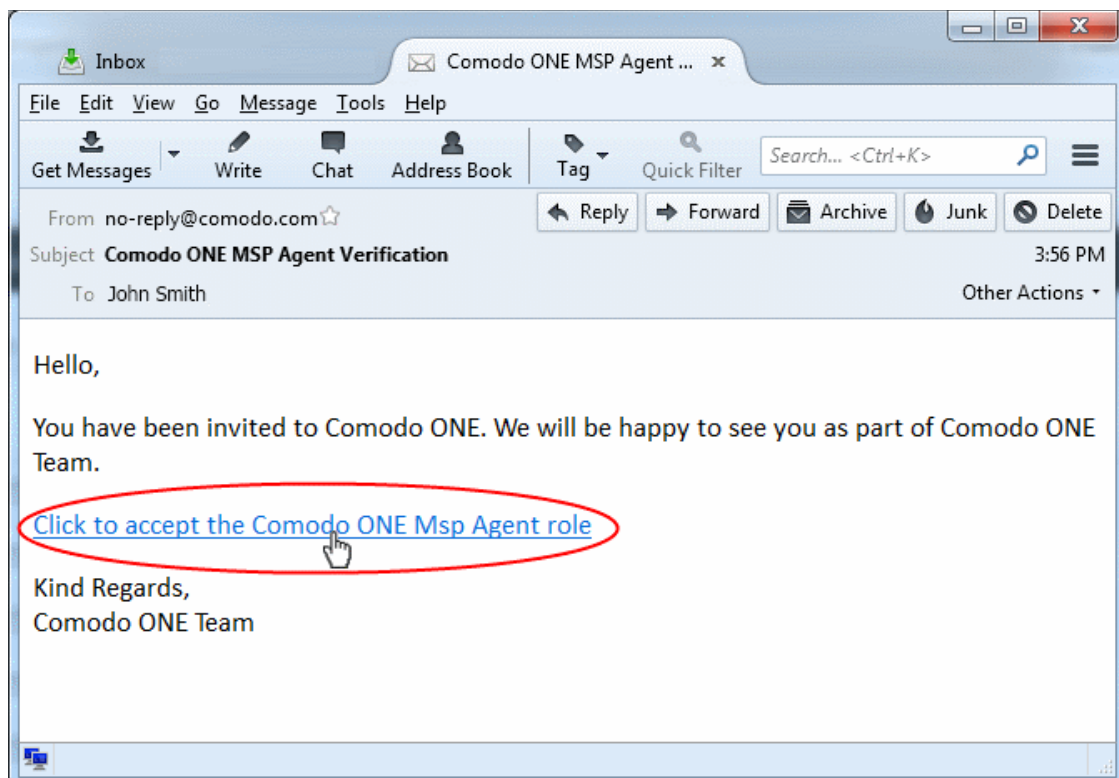
? After the client software has been installed, the endpoint can be managed from the endpoint console.

The guide will take you through the following processes - click on any link to go straight to that section as per your current requirements.

- **Step 1 - Activate your Agent account**
- **Step 2 - Login to RMM web console and download technician console**
- **Step 3 - Install Technician Console**
- **Step 4 - Login to Technician Console**
  - **Add and manage devices**
  - **Create procedures**
  - **Create and execute jobs**
  - **Create and apply monitoring policies**
  - **View Alerts**
  - **Handle support sessions**
  - **The Support Sessions Interface**
    - **Have a chat interaction with the End-user**
    - **Execute pre-defined actions on the endpoint**
    - **Access the Endpoint through Remote Desktop Connection**
    - **Run a procedure**

## Step 1 - Activate your Agent account

Once your MSP Account Administrator has **created an account for you**, you will receive an activation email with a validation link.



- Click the validation link in the email to activate your agent account.

You will be taken to the password setting page of RMM.

The screenshot shows a 'PASSWORD RESET' form. At the top, there is a dark blue header with the text 'PASSWORD RESET' in white. Below the header is the 'COMODO one' logo, with 'COMODO' in red and 'one' in black. The form contains two input fields: 'Password' and 'Password (Again)'. Below these fields is a 'Reset' button.

- Enter a password of your choice and re-enter it for confirmation
- Click 'Reset'

**Note:** Set a secure password with a combination of upper and lower case characters, numbers and special characters, so that it could not be easily guessed. Your password should contain at least one uppercase character, one lower case character, one numeral and one special character.

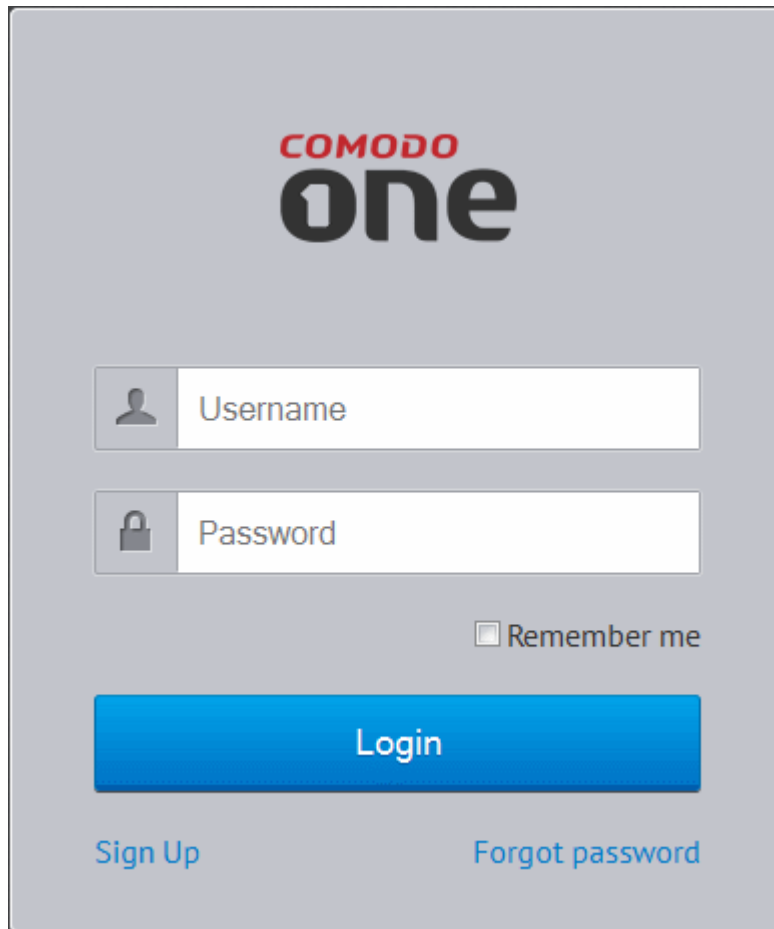
Your password will be set.

The screenshot shows a 'LOGIN' form. At the top, there is a dark blue header with the text 'LOGIN' in white. Below the header is the 'COMODO one' logo, with 'COMODO' in red and 'one' in black. A green success message box with a checkmark icon contains the text 'Your password is reset successfully.'. Below this message are two input fields: 'Email' and 'Password'. Below the 'Email' field is a 'Remember Me' checkbox and a 'Forgot password?' link. At the bottom is a 'Login' button.

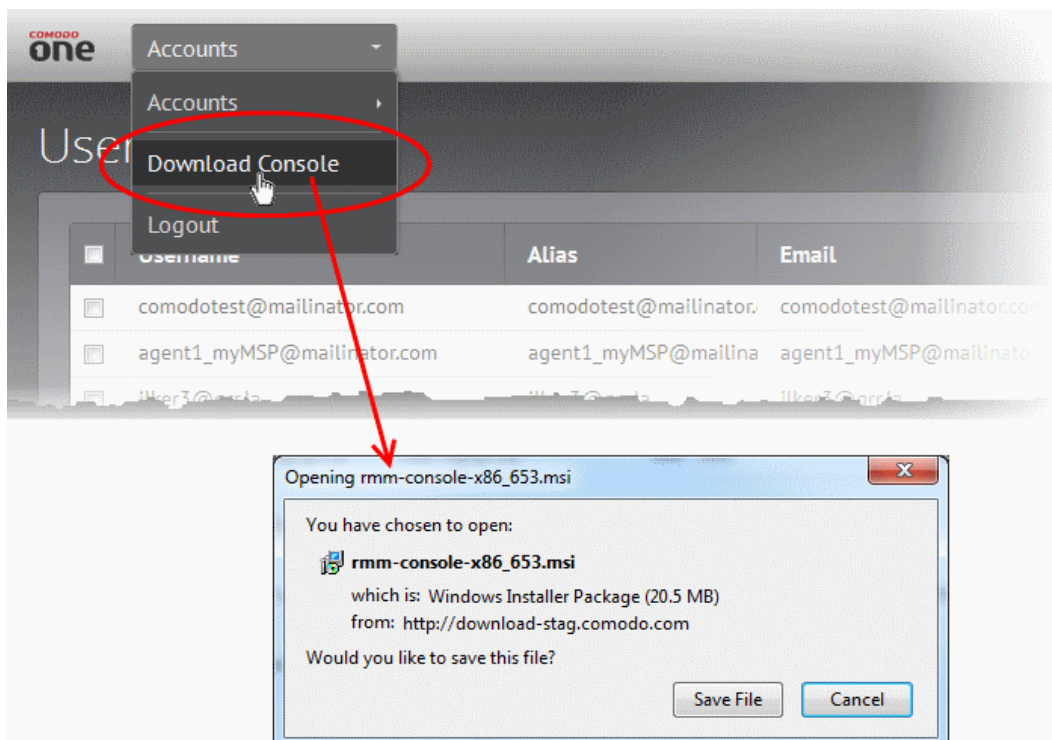
You can login to the 'Comodo ONE' web console by clicking 'Login' in the next screen and entering your email address and password.

## Step 2 - Login to RMM web console and download technician console

You can access the RMM web console by logging in at [one.comodo.com](http://one.comodo.com) and clicking 'Open Module' in the RMM tile. Alternatively you can login to the RMM web console directly at <https://manage.comodo.com>.



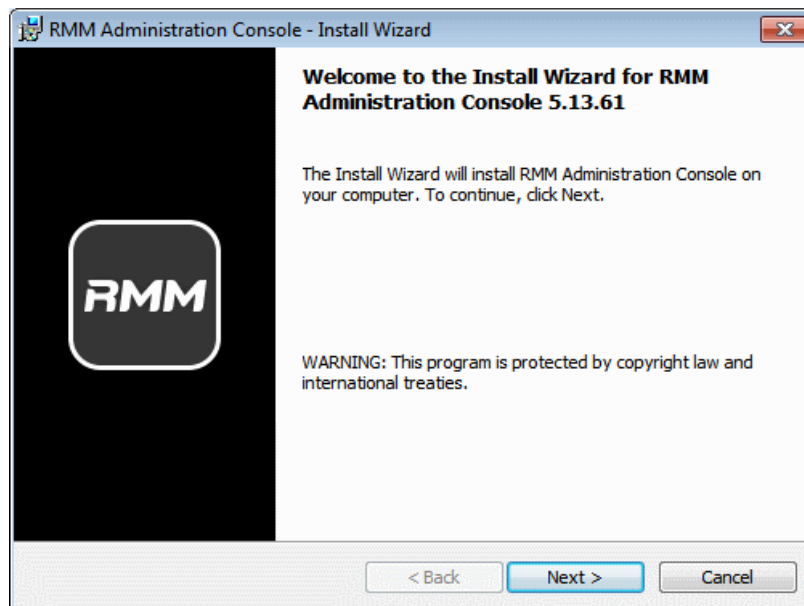
- Enter your email address as your username, enter your password and click 'Login'. The RMM web console will open.



- Choose 'Download Console' from the drop-down at the top left of the RMM web console and save the setup file.

### Step 3 - Install the Technician Console

- Double click on the downloaded file to start the Technician Console installation wizard




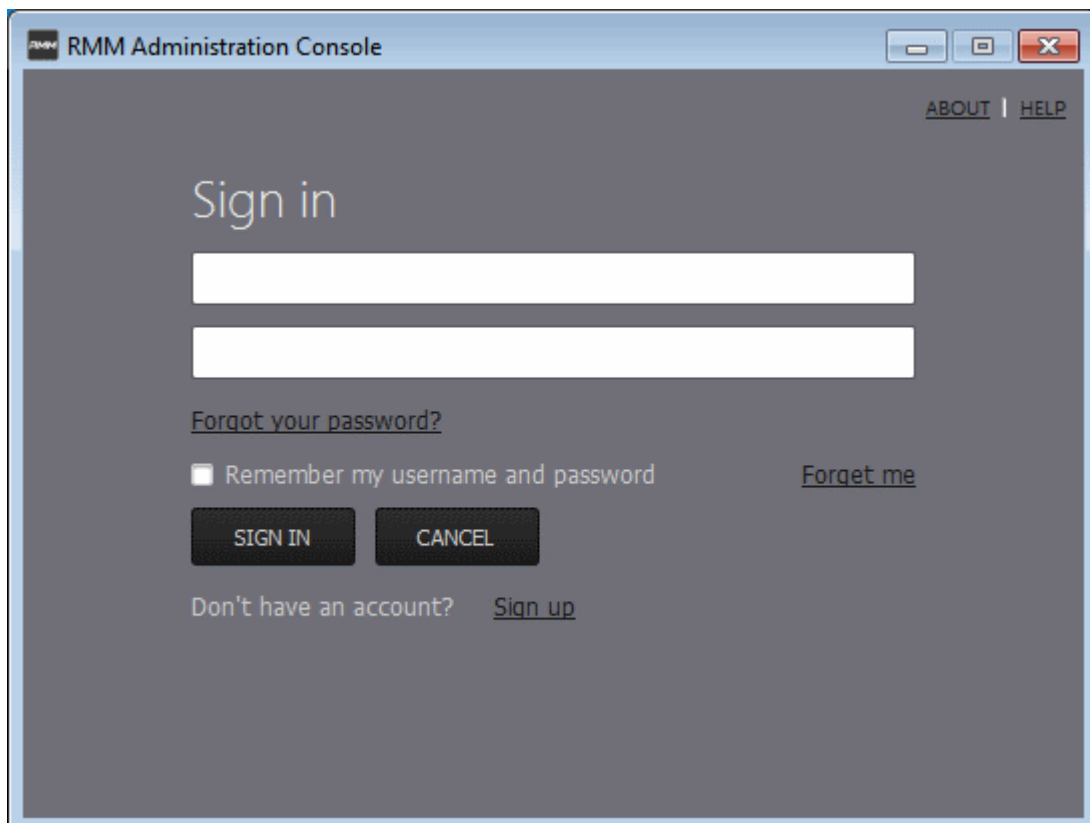
- Follow the wizard and complete the installation.

### Step 4 - Login to Technician Console

On successful completion of the installation, the console will open. Also, you can open the console manually by clicking the



Technician Console desktop icon  or by clicking 'Start' > 'All Programs' > 'COMODO' > 'RMM Administration Console' > 'RMM Administration Console' from the Windows Start menu.



- Enter your username (email address) and password in the respective text fields and click 'SIGN IN'.

The console will open.

**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

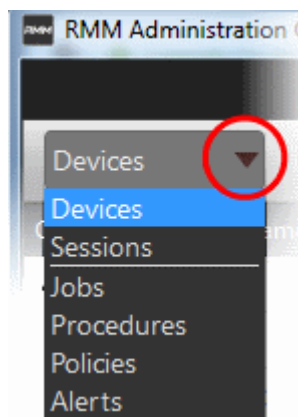
**Title Bar Controls**  
Enables to logout and contains shortcuts to view the About Dialog and online help

**Switch to different configuration screens of the console**

**Search Field**  
Enables to search for specific item by entering a keyword

**Task Bar**  
Contains shortcuts to perform various tasks depending on the configuration screen displayed.

Company/Site/Hostname	Operating system	Device type	Logged user	Internal IP	External IP	Compliant	Applied policy name	Desc	Action
Enterprise									
US									
WILLSMITH-PC	Windows 7 Professional - x86	Workstation	WillSmith-PC\Will smith	10.0.2.15	10.108.17.248	N/A			
ILKER-ULTRABOOK	Windows 8.1 Pro - x64	Workstation	ILKER-ULTRABOOK\Iker	192.168.1.5	199.222.104.149	N/A			
CHNC4-T02-W7U64	Windows 7 Ultimate - x64	Workstation	CHNC4-T02-W7U64\CHN...	10.108.17.155	10.108.17.155	N/A			
Chennai									
Default company									
Default site									
CHNW7HP64	Windows 7 Home Premium - x64	Workstation	chnw7hp64\Administrator	10.108.17.230	10.108.17.230	N/A	N/A	Test	Display
Customer2									
Premium									
T03-W7-32BIT-PC	Windows 7 Professional - x86	Workstation	T03-W7-32Bit-PC\T03-W7-...	10.108.17.202	10.108.17.202	N/A	N/A		Unavailable
Customer1									
Universal									
WIN7-PC	Windows 7 Professional - x86	Workstation	win7-PC\win 7	10.108.17.180	10.108.17.225	N/A	N/A		Unavailable
Company1									
Default site									



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

- **Devices** – Displays the list of client endpoints devices enrolled for monitoring and management to your MSP account. You can also add new devices, companies, manage sites, run procedures and apply policies to endpoints.
- **Sessions** – Displays the endpoints that are currently in service/support sessions with an agent. You can take over service sessions transferred to you or start sessions with endpoints in the queue.
- **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 to create jobs to be executed on selected endpoints. You can create new procedures from this interface.
- **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.
- **Alerts** – Displays alerts generated on endpoints and allows you to run a fix or a procedure.

## Add and Manage Devices

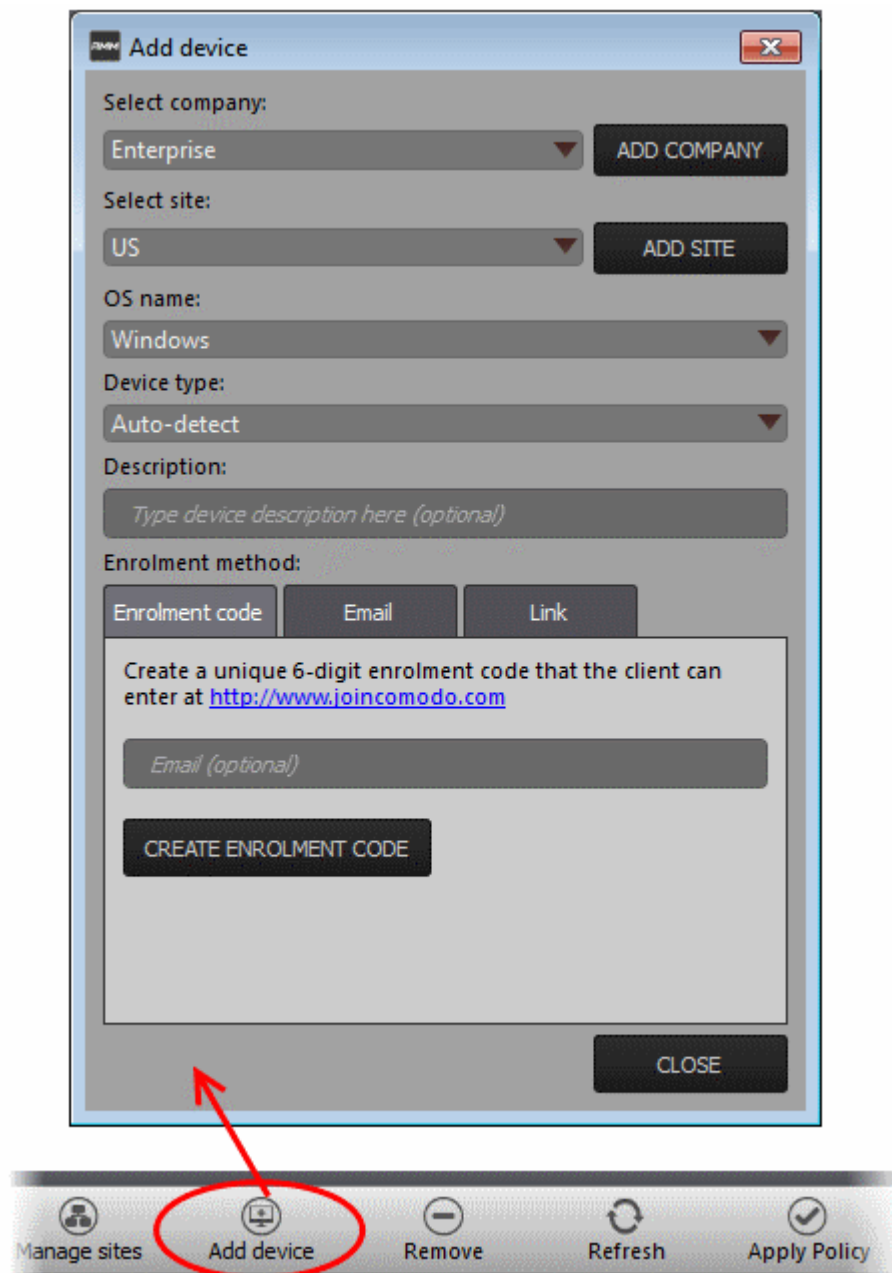
RMM requires client software to be installed on each endpoint in order to deploy monitoring policies, receive alerts, execute jobs/procedures and for the technician to provide support through a support chat session. While enrolling a new device, the agent can instruct the end-user to download and install the client after authenticating them to RMM.

- Open the Devices interface by choosing Devices from the drop-down at the top left. The list of endpoints enrolled for

monitoring and management is displayed.

## To add new endpoints

- Click 'Add device' from the bottom of the interface



The 'Add a device' dialog will open.

- Select company – Choose the company to which the endpoint belongs. If you are adding a device for a new company, click ADD COMPANY and create the new company
- Select site - Choose the site at which the endpoint is located. If you are adding a device at a new site, click ADD SITE and create the new site
- OS name – Choose the operating system of the endpoint added
- Device type – Choose whether the endpoint is a workstation (PC) or a server. If you are not sure, choose 'Auto-detect'
- Description - Enter a short description of the device
- Choose the 'Enrollment Type' by clicking on the respective tab
  - Enrollment code** – Clicking 'CREATE ENROLLMENT CODE' will generate a 6 digit code which will be used to authenticate new users. You can forward the code to users via out-of-band communication such as email. You should instruct the end-user to download the client console from <http://www.joincomodo.com> after



entering the enrollment code.

- **Email** – Enter the email address of an end-user whose endpoint you wish manage. RMM will send an email to the end-user containing a download link for the client.
- **Link** - Generates a download link for the client setup file. You can forward the link to the end-user through any out-of-band communication method like e-mail and instruct the end-user to download and install the agent.

Once the end-user downloads the client setup and **installs** it, he/she will be able to initiate a support chat session with any RMM technician by opening the client.

- Click 'CLOSE' to add the device.

Repeat the process to add more devices. You will be able to apply monitoring policies, view alerts and manage endpoints after the client software has been installed on the endpoint.

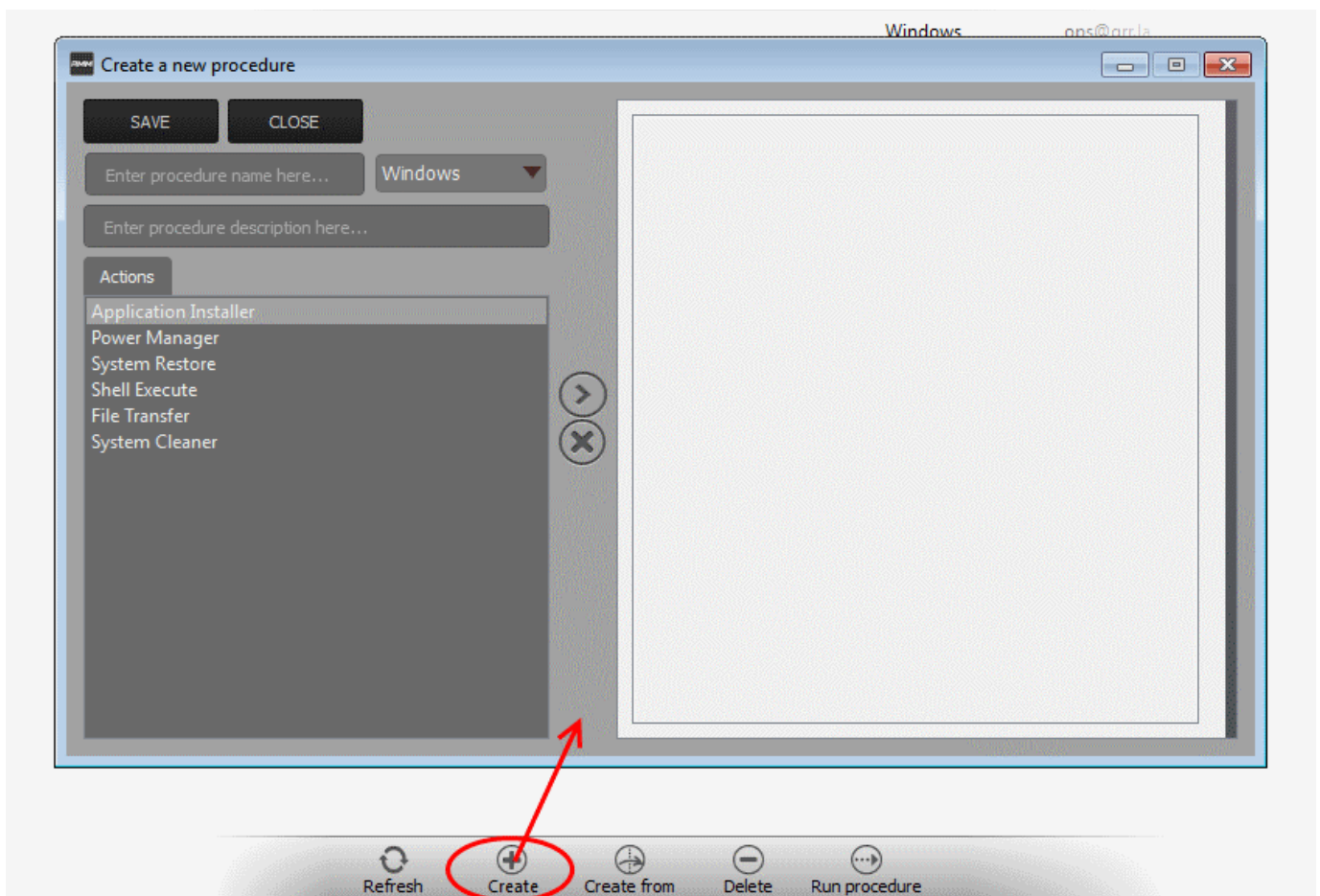
## Create Procedures

A 'Procedure' is a set of actions to be run on an endpoint. You can select a series of actions with defined parameters, to be performed in sequence while creating a procedure. The 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).

- Choose 'Procedures' from the drop-down at the top left . A list of available procedures will be displayed.

### To create a new procedure

- Click 'Create' from the bottom



The 'Create a new procedure' dialog will open.

- 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 right arrow to add the action to the list at the right
- 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"> <li>• Download URL for the application</li> <li>• Name of the setup file and command line parameters</li> <li>• Command for canceling installation for failsafe reasons</li> </ul>
Power Manager	Choose the power control operation from: <ul style="list-style-type: none"> <li>• Restart</li> <li>• Restart in safe mode</li> <li>• Shutdown</li> <li>• Restart in rescue mode</li> </ul>
System Restore	Choose whether to create a restore point or to restore the system to a previous state. <ul style="list-style-type: none"> <li>• Enter the name of the restore point</li> </ul>
Shell Execute	Basic <ul style="list-style-type: none"> <li>• Enter the execution command for the process</li> <li>• Enter the parameters to be passed to the process</li> </ul> Advanced <ul style="list-style-type: none"> <li>• Enter the working directory for the process</li> <li>• Choose the execution options:                             <ul style="list-style-type: none"> <li>• Wait for process to finish – Completes the process before termination</li> <li>• Hide Window – Executes the process at the background</li> </ul> </li> </ul>
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	Select the cleaner modules to be applied: <ul style="list-style-type: none"> <li>• Disk Cleaner</li> <li>• Registry Cleaner</li> </ul>

- Repeat the process to add more actions to the procedure. Upon running the procedure, the actions will be executed in order.
- Click 'SAVE' to save your procedure.

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.

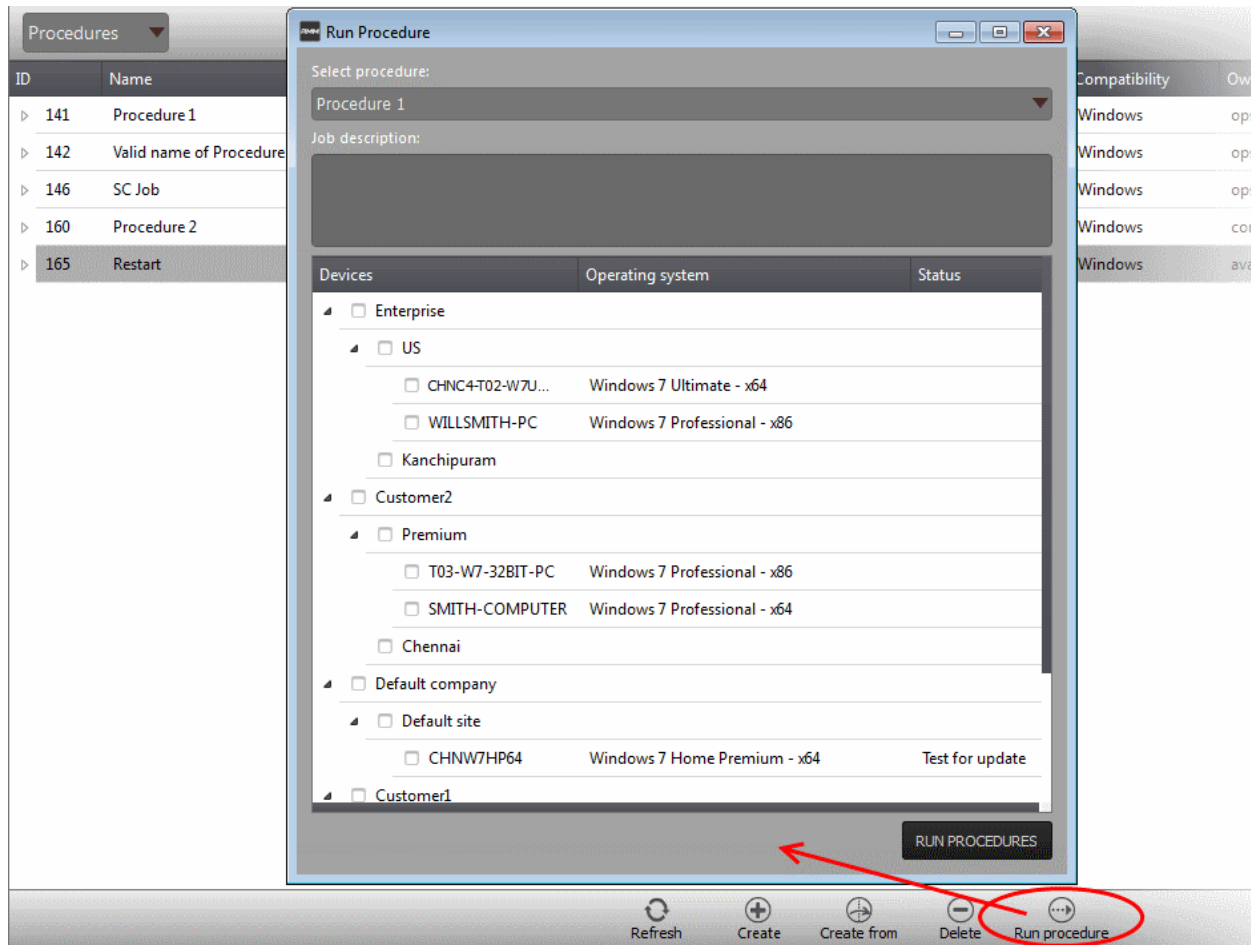
- Repeat the process to add more procedures as required.

**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 to create a new procedure.

### To run a procedure

- Click 'Run Procedure' from the bottom

The 'Run Procedure' dialog will open.



- Choose the procedure to be run from the drop-down at the top
- Select the endpoints on which the procedure is to be run and click 'RUN PROCEDURES'

A Job will be automatically created for running the selected procedure and will be executed.

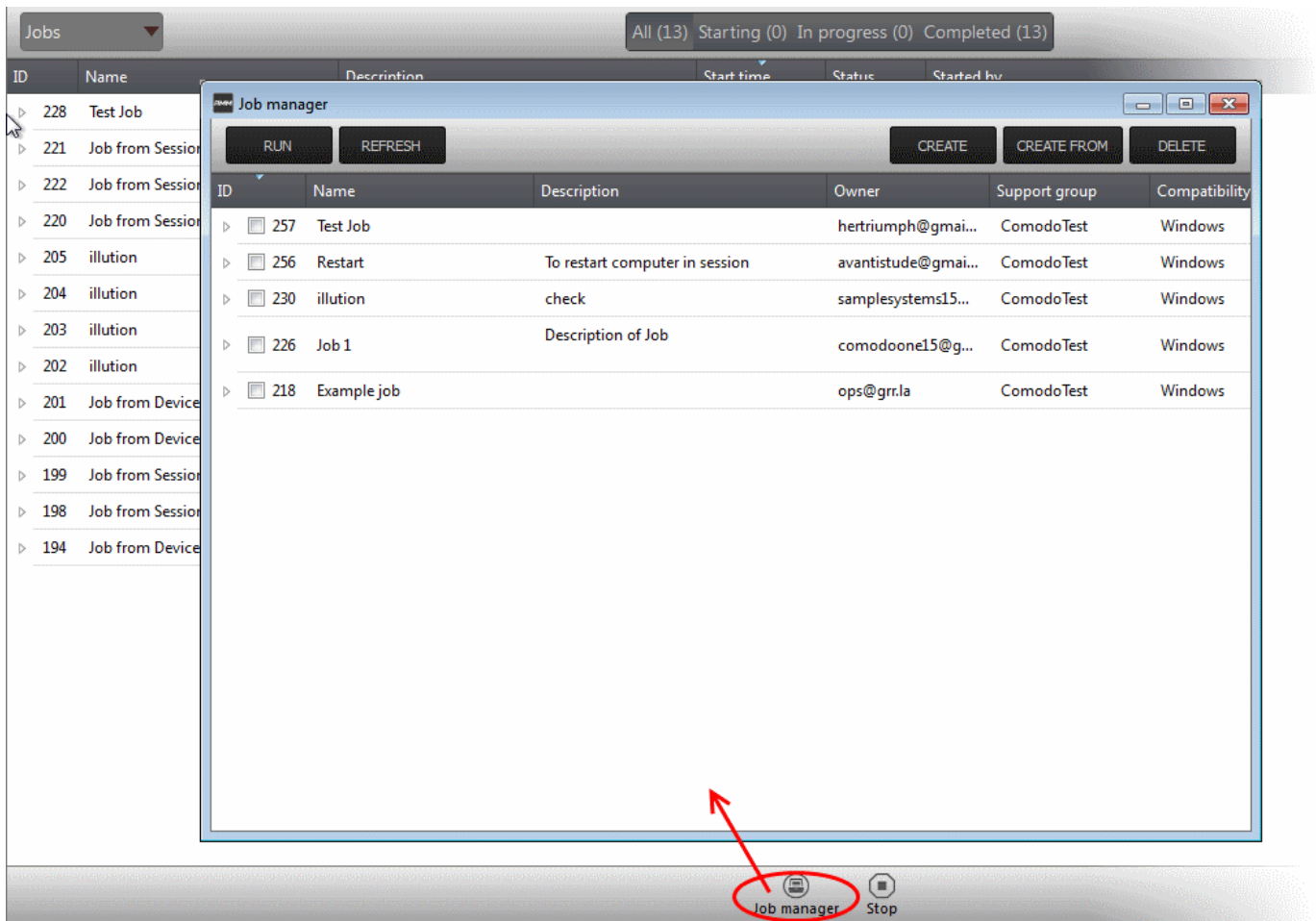
## Create and Execute Jobs

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.

- 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 agents belonging to your MSP.

### To create a new job

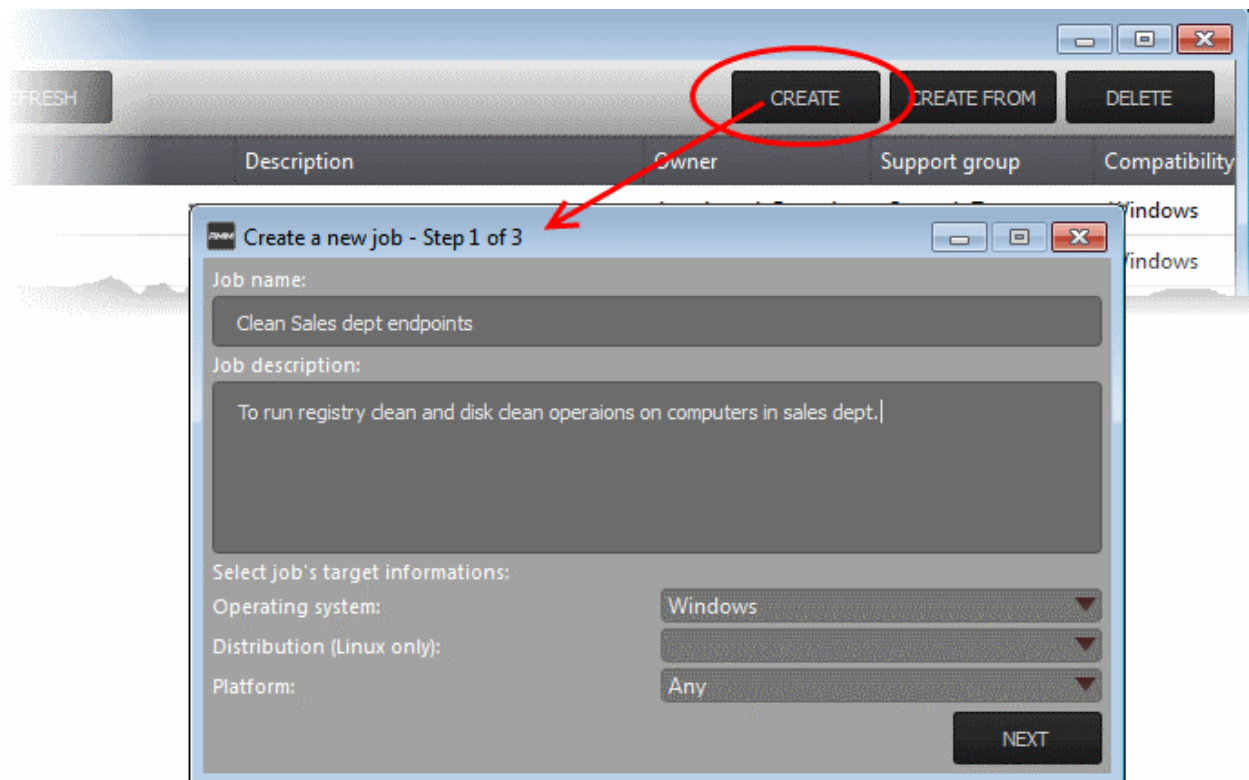
- Click 'Job Manager' from the bottom of the interface



All jobs created so far will be displayed.

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

The job creation wizard will start.

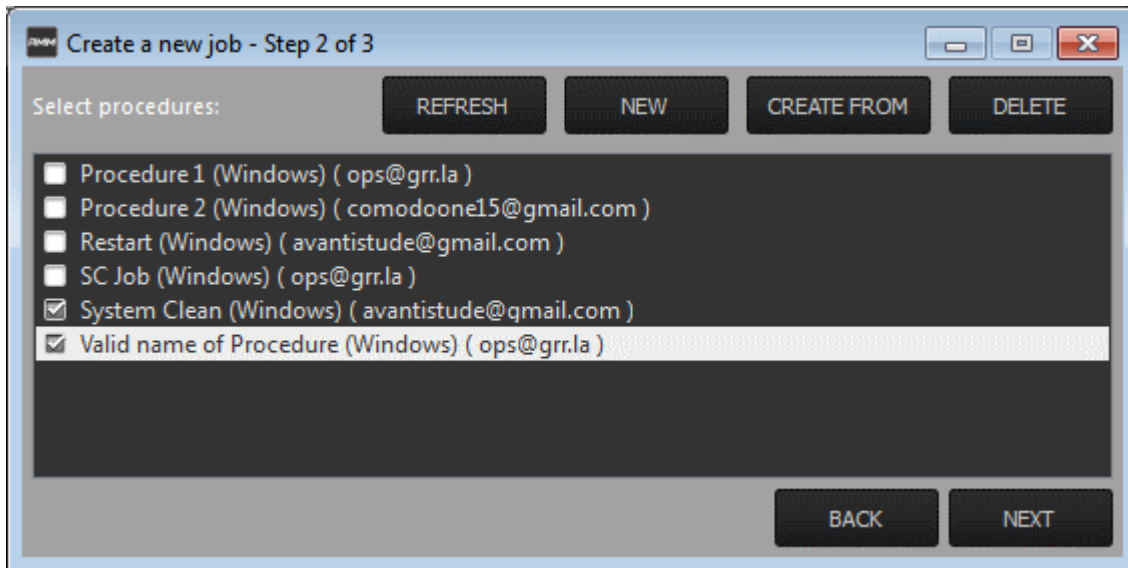


## Step 1 – Job Description

- 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 endpoints to which the job is to be applied
  - Platform – Choose the version of the operating system
- Click 'NEXT' to continue.

## Step 2 – Select Procedures

- Select the procedures to be run as per the job.

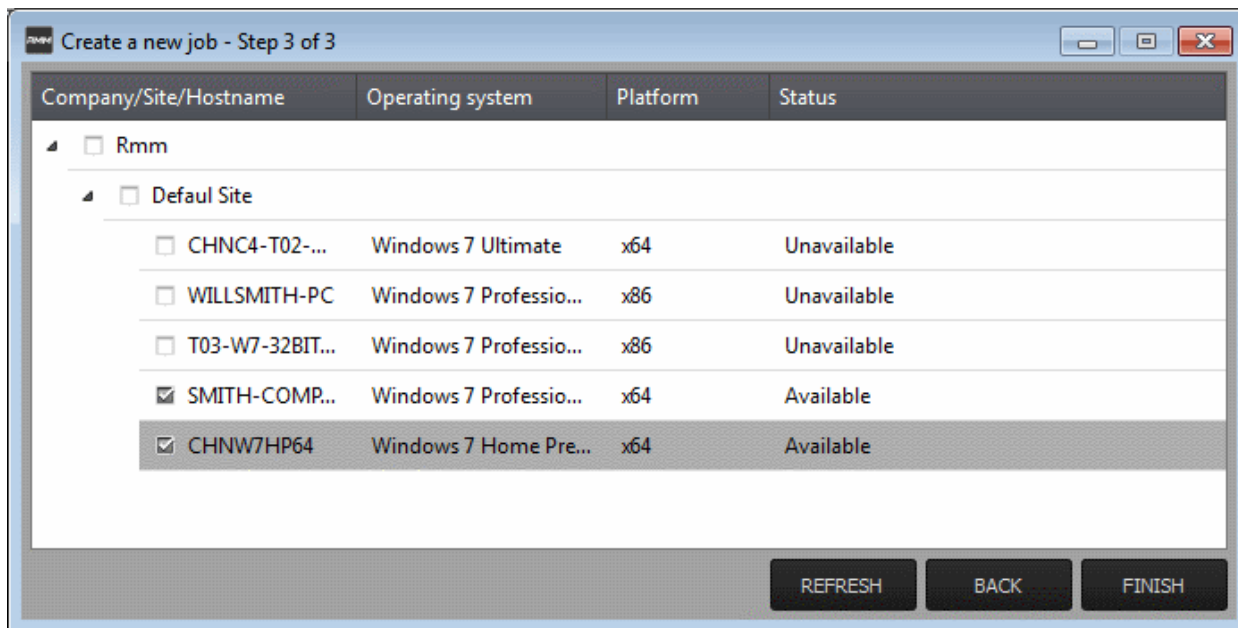


**Tip:** You can add new procedures from this interface too by clicking 'NEW' from the top of the interface. Refer to the previous section '[Create Procedures](#)' for more details.

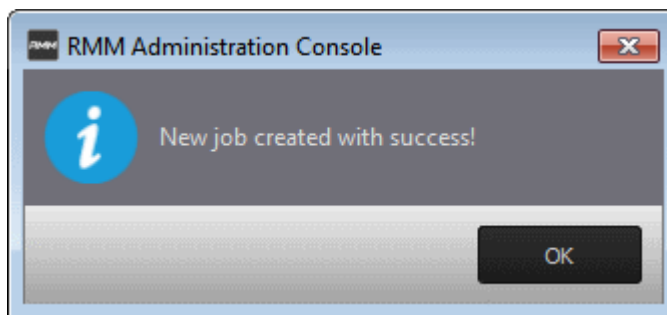
- Click 'Next'

## Step 3 – Select Target Endpoints

- Select the endpoints on which the job is to be executed



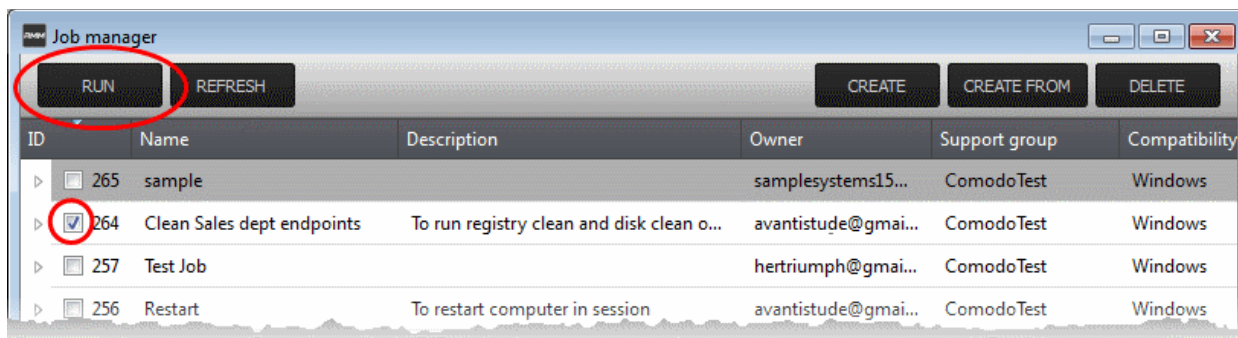
- Click 'FINISH'



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

### To execute a saved job

- Open the 'Job Manager' interface by clicking 'Job Manager' from the task bar of the Jobs interface
- Choose the job(s) to be executed



- 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 operations ...	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 parameters and events and an alert will be generated if an endpoint violates the policy. Alerts can be viewed from the 'Alerts' interface. Agents 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 'Policies' interface displays policies which are currently applied to endpoints, and the endpoint's current compliance with the policy. New policies are created in the 'Policy Manager'.

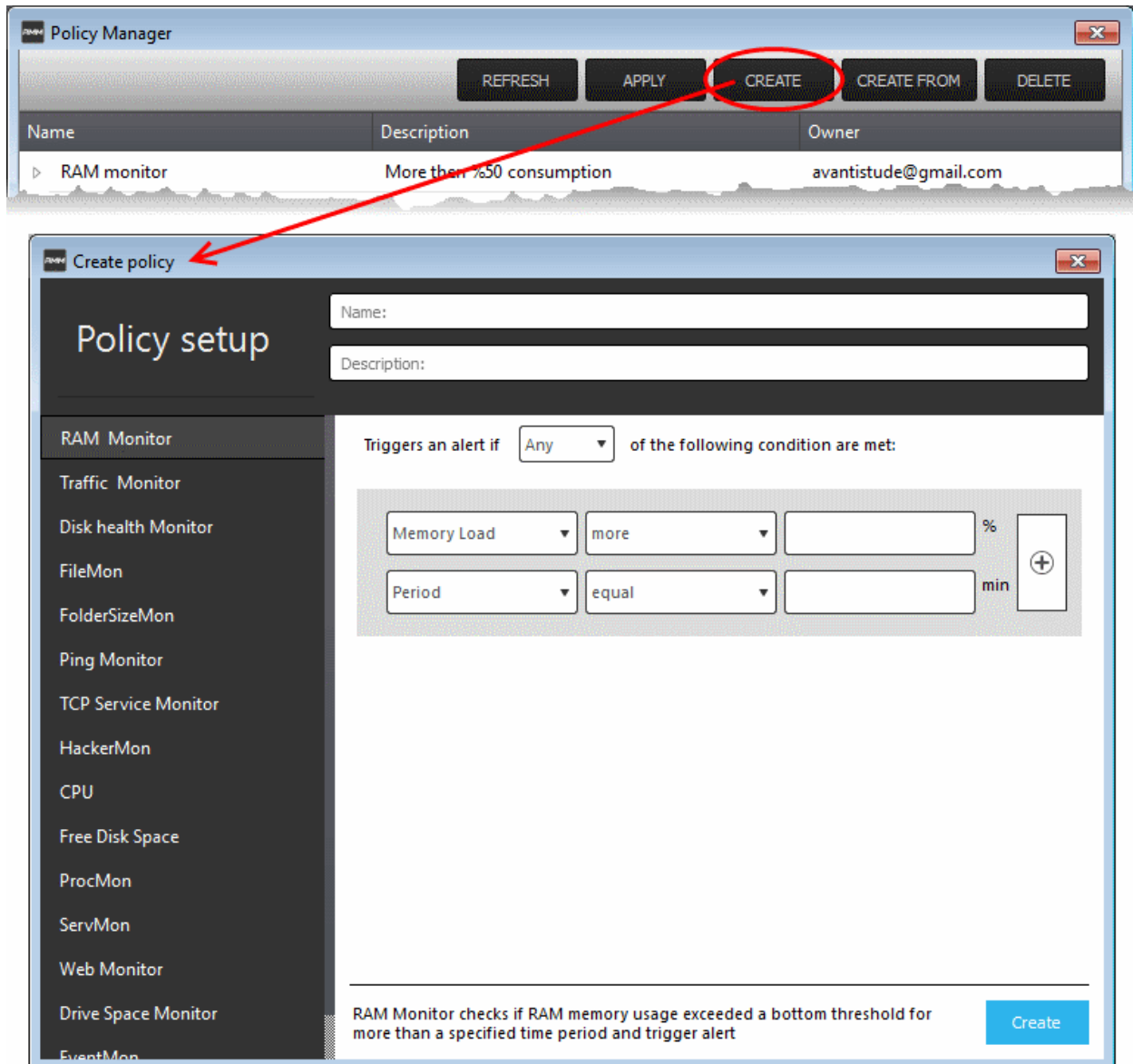
The screenshot shows the 'Policies' interface with a table of services and a 'Policy Manager' dialog box. The 'Policy Manager' dialog has buttons for REFRESH, APPLY, CREATE, CREATE FROM, and DELETE. It contains a table of policies:

Name	Description	Owner
RAM monitor	More then %50 consumption	avantistude@gmail.com
Traffic Monitor		ops@grr.la
Disk Monitor		ops@grr.la
Policy RAM Monitor	Policy description 2 condition	comodoone15@gmail.com
Free disk space monitor	To ensure free disk space at endpoints	avantistude@gmail.com
free disk space 20	to ensure free space more than 20 gb	avantistude@gmail.com
check website	test	samplesystems15@gmail.com
newsonair	test	samplesystems15@gmail.com
test policy	check	samplesystems15@gmail.com

### To create a new policy

- Click 'Policy Manager' from the bottom of the interface.
- Click 'CREATE' from the top of the 'Policy Manager' dialog.

The 'Create policy' interface will open.



- 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.

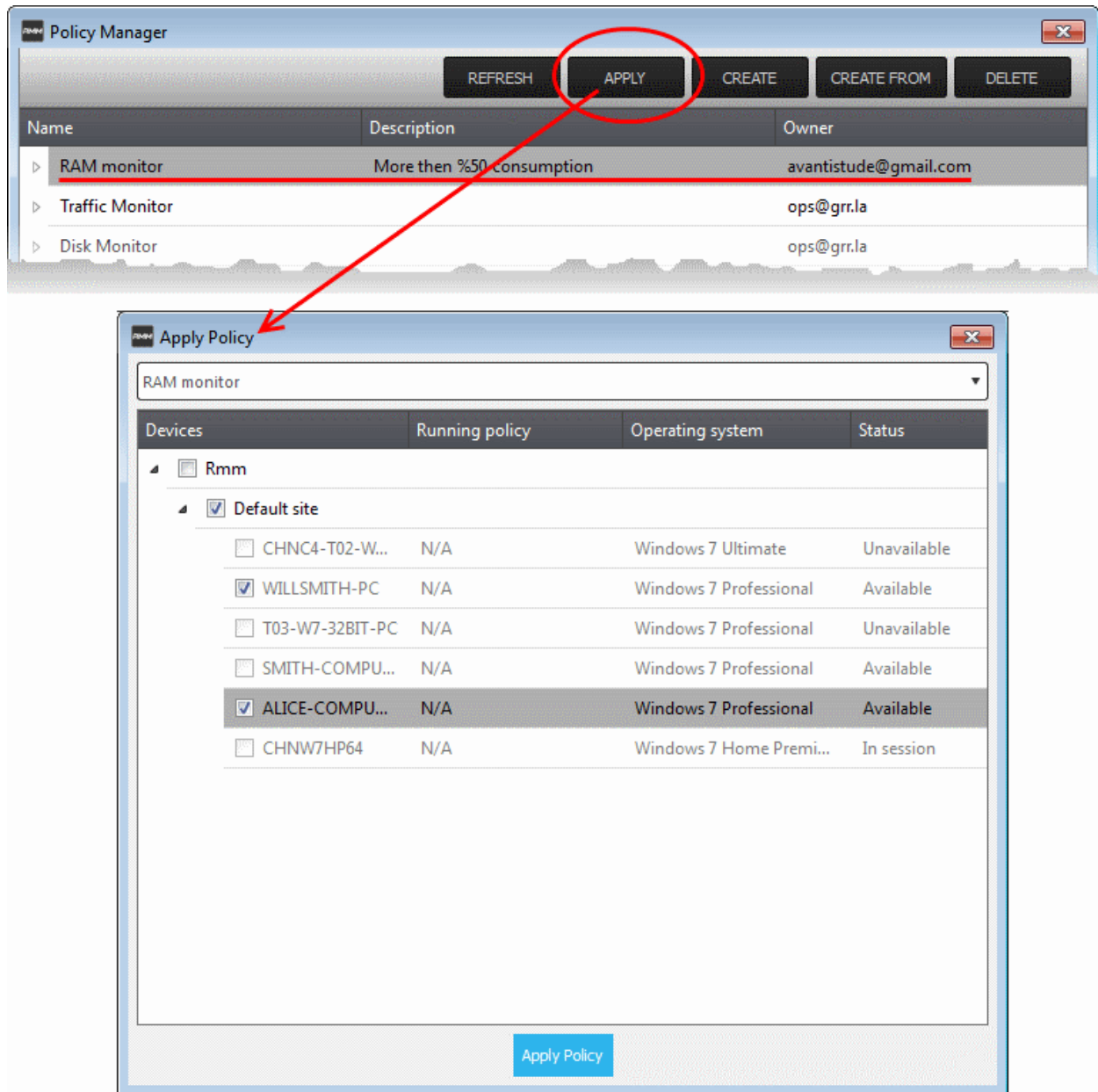
The policy will be added to the list in the 'Policy Manager' interface and will be available for application to desired endpoints at any time.

### To apply a policy to endpoints

- Open 'Policy Manager'
- Click 'APPLY' from the title bar

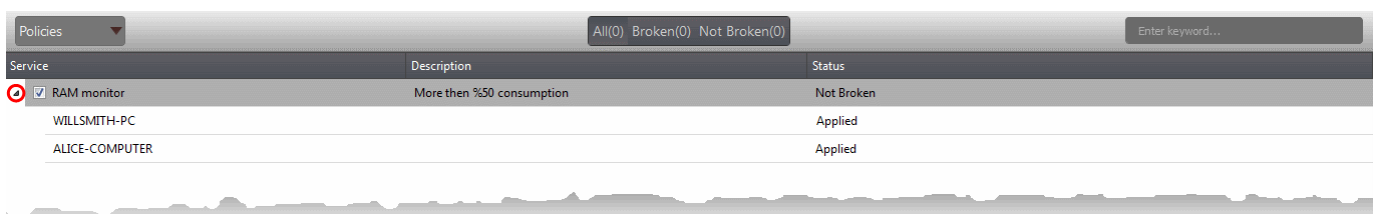


The 'Apply Policy' dialog will open with a list of endpoints enrolled for your account.



- 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.



**Tip:** Clicking the arrow at the right of the policy name displays the endpoints on which the policy is applied.

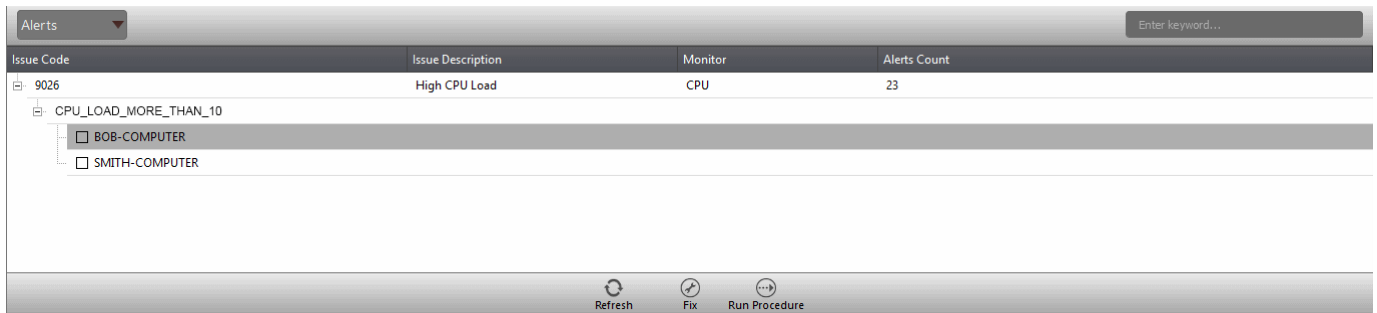
An alert will be generated if any of the monitored parameters exceed the thresholds set by the policy. You can view the alert from the Alerts interface.

## View Alerts

RMM generates alerts in the event of a policy violation by a monitored endpoint and displays them in the 'Alerts' interface. Every time an alert is generated, the notification icon  at the top right blinks to attract your attention. You can click the notification icon, to check whether a new alert has been generated and switch to the 'Alerts' interface to view the alert(s).

- To view the alerts, choose 'Alerts' from the drop-down at the top left.

The 'Alerts' interface displays the alerts generated so far and allows you to take measures by running appropriate procedures/jobs or by accessing the endpoint through Remote Desktop session.



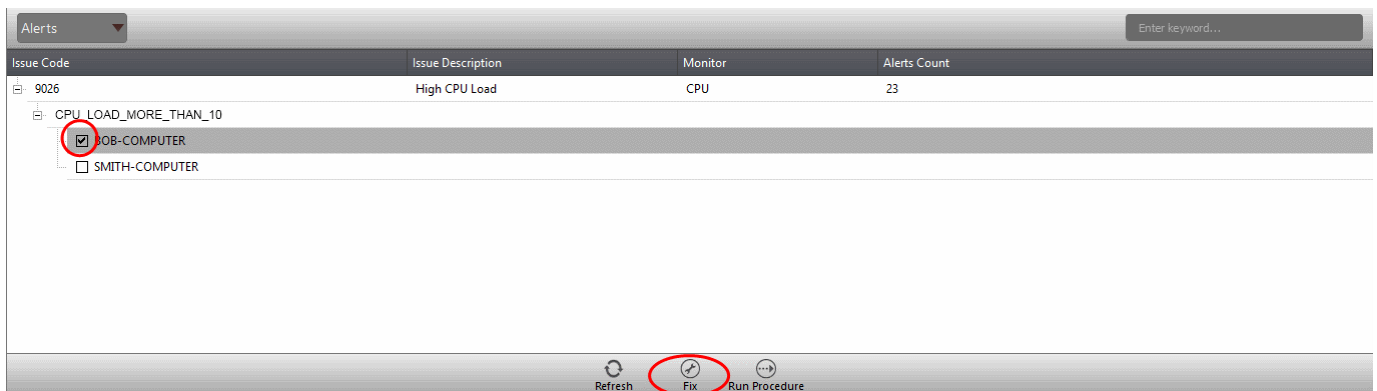
The alerts raised by each policy are grouped together.

- Clicking on the '+' button beside the issue code expands the list of endpoints on which the alert is generated.

Depending on the nature of the issue reported by the alert, you can resolve the issue by:

- Running procedures;**
- Executing jobs;**
- Or
- Initiate a support sessions and take remote access of the endpoint(s).**

Once the issue has been resolved, you can remove the entry from the list of alerts by selecting the endpoint(s) under the alert and clicking Fix from the bottom of the interface.



## Handle Support Sessions

The support session enables you to accept support requests from your customers. By establishing a support session you can:

- Engage in chat sessions with clients to advise on and resolve problems.
- 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.
- Run procedures to correct issues identified by policy violation alerts

A support session can be initiated in two ways:

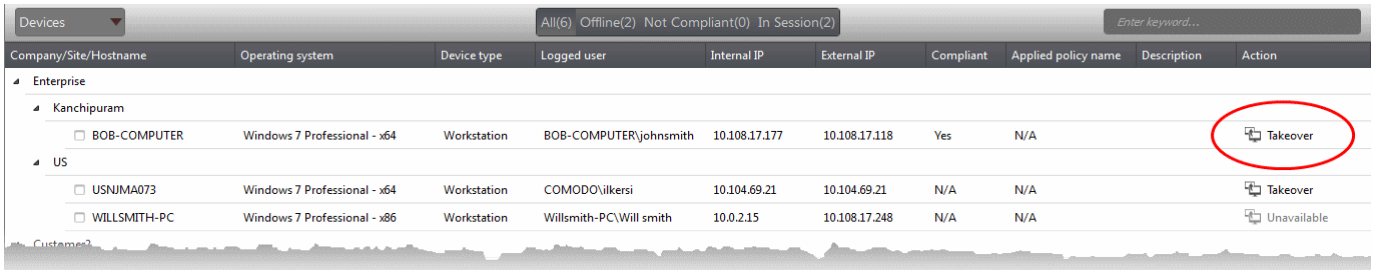
- From the technician console. Refer to the section '**Initiating a support session from the technician console**' for more details.

- By accepting a support request from an end-user. Refer to the section **Accepting support request from an end-user** for more details.

## Initiating a support session from the technician console

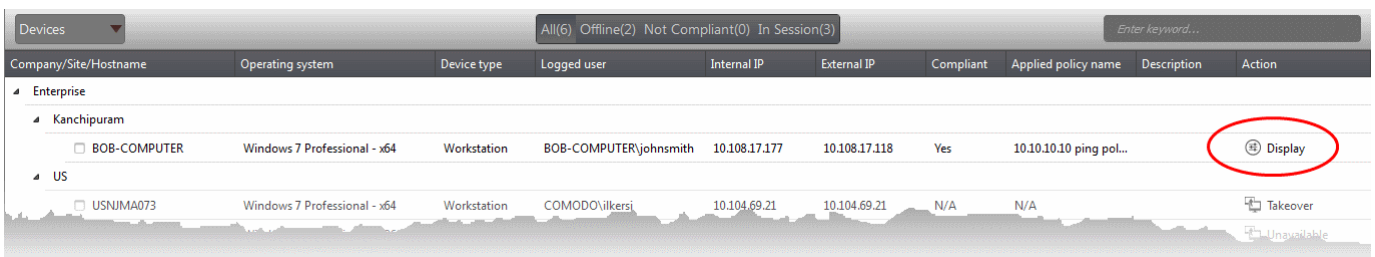
If you require to perform a maintenance operation or run procedures you can initiate the session by clicking 'Takeover' from the 'Devices' interface.

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



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

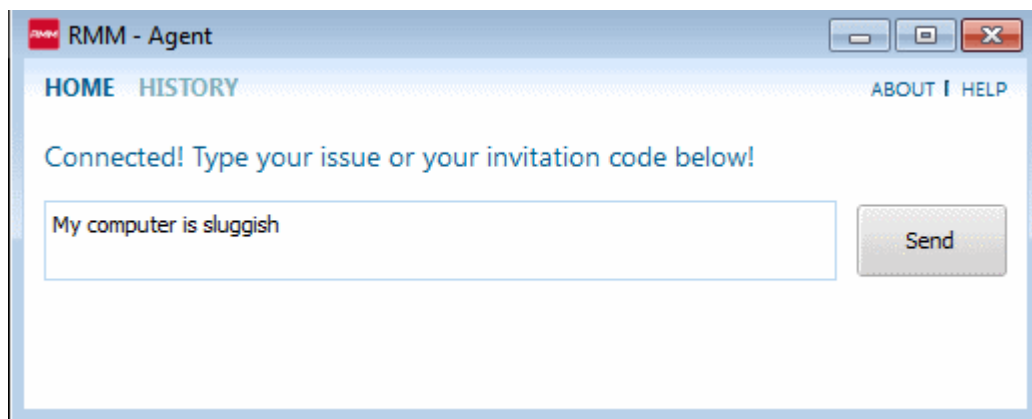
A session will be established.



- Click 'Display' under 'Action' to open the support session interface.

## Accepting a support request from an end-user

An end-user requiring a support from a technician can initiate a support session by opening the RMM client installed on their endpoint, and describing their issue in the chat window that is displayed.



Once an end-user starts the support session, the number beside 'Waiting' in the Sessions interface will be incremented by one.



You can accept the support request and start the support session from the 'Sessions' window.

## To accept a support request

- Open the 'Sessions' interface by choosing Sessions from the drop-down at top left.
- Click the 'Waiting' tab to view pending session requests.

Session ID	Host	All	All	All	Language	Source	Action
1355	BOB-COMPUTER	Free	Valid	Waiting	English	Inbound	Approach

- Click 'Approach' under 'Action' in the row of the device (endpoint) to which the support session is to be started. A session will be established.

Session ID	Host	All	All	All	Language	Source	Action
1360	BOB-COMPUTER	Free	Valid	Established	English	Inbound	Display

- Click 'Display' under 'Action' to open the support session interface.

## 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**

**The Chat Window displays the conversation between you and the end-user**

**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.
- TRANSFER** – Allows you to transfer the support session to another technician.
- TRANSFER BACK IN QUEUE** – Allows you to transfer the support session to the queue under the Sessions interface and allows any technician to approach and run the session

- **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.

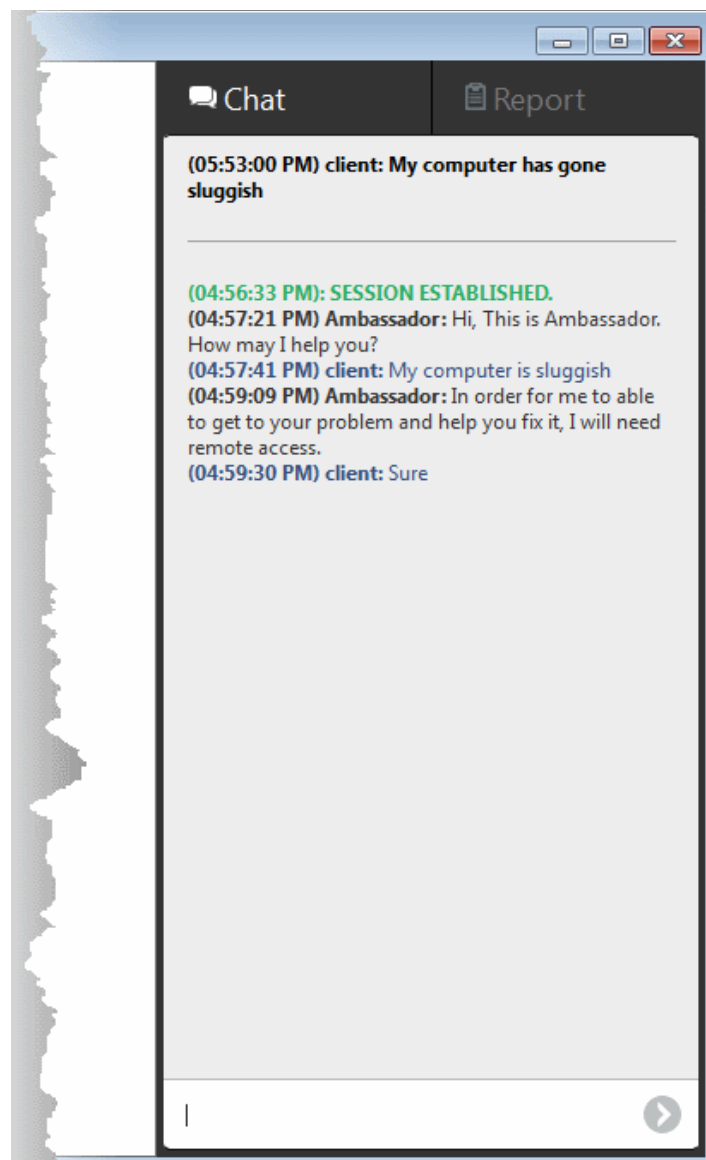
**Chat Window** – Allows you to start a support chat with the user. Refer to the section **Have a chat interaction with the End-user** for more details.

Next, see:

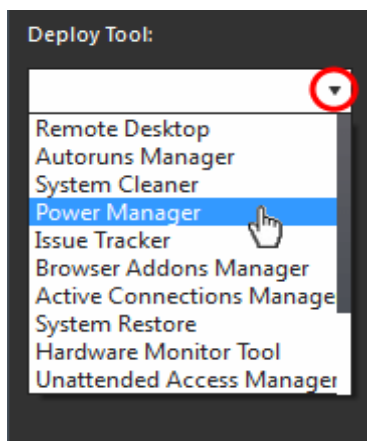
- **Have a chat interaction with the End-user**
- **Execute pre-defined actions on the endpoint**
- **Access the Endpoint through Remote Desktop Connection**
- **Run a Procedure**

## Chatting with End-users

The chat window at the right of the session window allows you to communicate with the user to discuss the problem. You can also request permission to execute remote fixes or to access the endpoint through remote desktop connection.



## 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
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 ' <a href="#">Access the Endpoint through Remote Desktop Connection</a> ' for more details.
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.
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.
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.
Issue Tracker	Displays the list of common problems identified at the endpoint that affect its security and operational efficiency and allows you to fix them .
Browser Add-Ons Manager	Allows you to identify the browser add-ons installed on the browsers and to remove unsafe or malicious add-ons.
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.
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.
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.
Unattended Access Manager	Provides access to the endpoint when the end-user is not in front of it and enables you to connect to the endpoint at any time for emergency work or routine maintenance.
Shell Execute	Allows you to open the command prompt window of the endpoint and execute shell commands.
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.
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.
File Transfer	Allows you to transfer any file between the your computer and the endpoint.

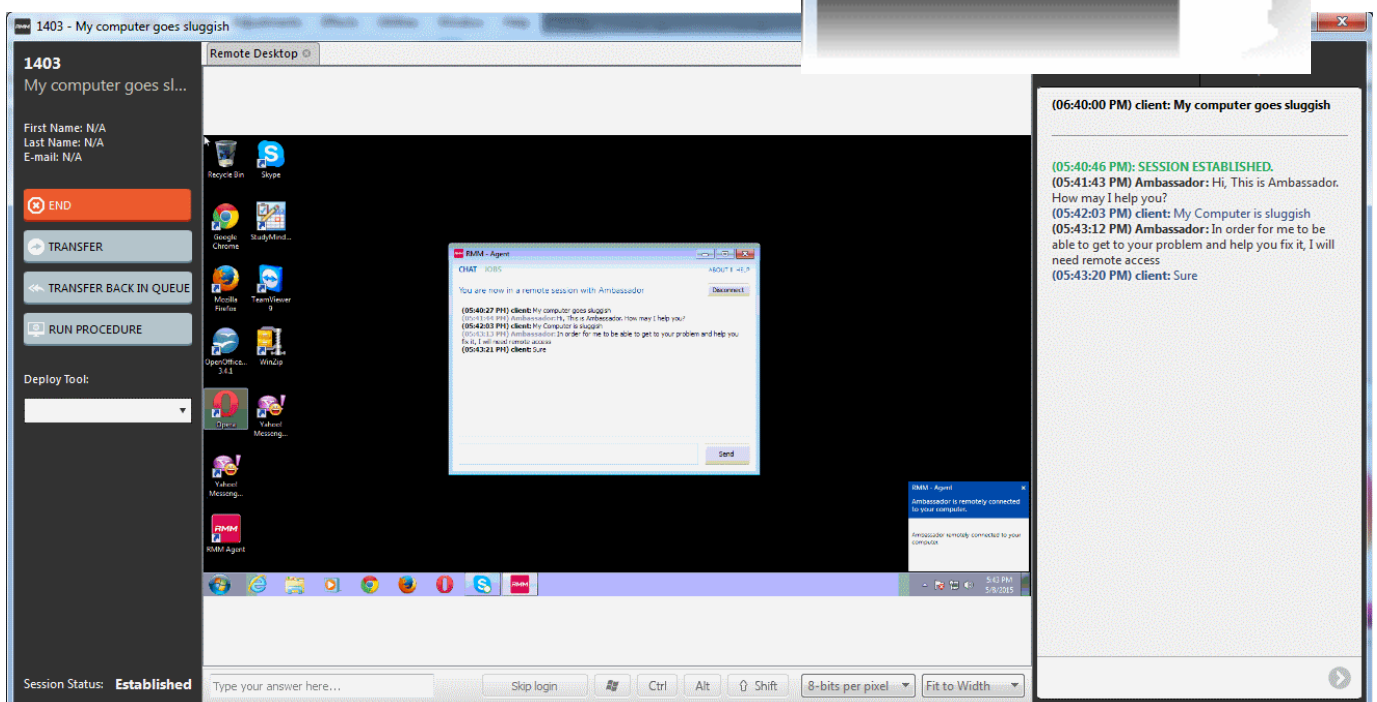
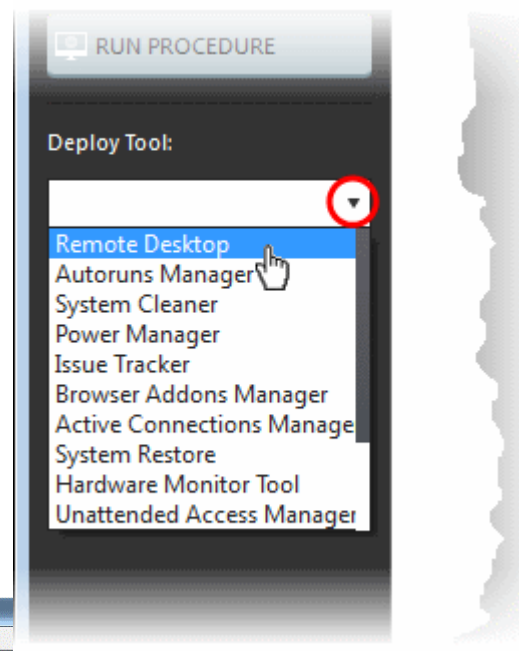
## Access Endpoints through Remote Desktop Connection

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.



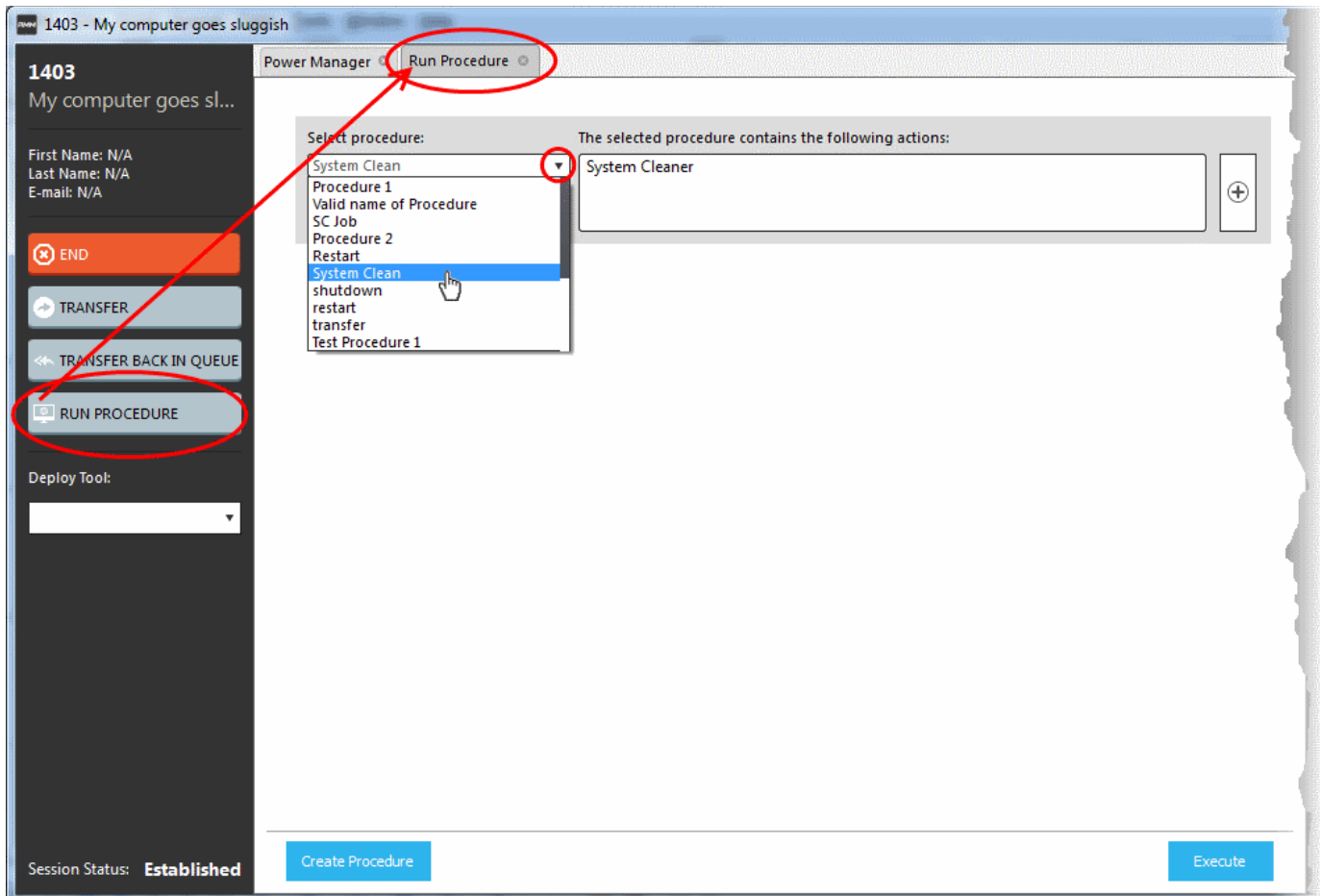
If required, the end-user can terminate the remote desktop connection by clicking the 'Disconnect' button at the top of the chat window..

## 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

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

### **Comodo Security Solutions, Inc.**

1255 Broad Street  
Clifton, NJ, 07013  
United States  
Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)

### **Comodo CA Limited**

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,  
Salford, Greater Manchester M5 3EQ,  
United Kingdom.  
Tel : +44 (0) 161 874 7070  
Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.comodo.com>.