COMODO
Creating Trust Online®

Comodo One

Software Version 3.3

Patch Management Module Administrator Guide

Guide Version 2.2.061218

Comodo Security Solutions
1255 Broad Street
STE 100
Clifton, NJ 07013

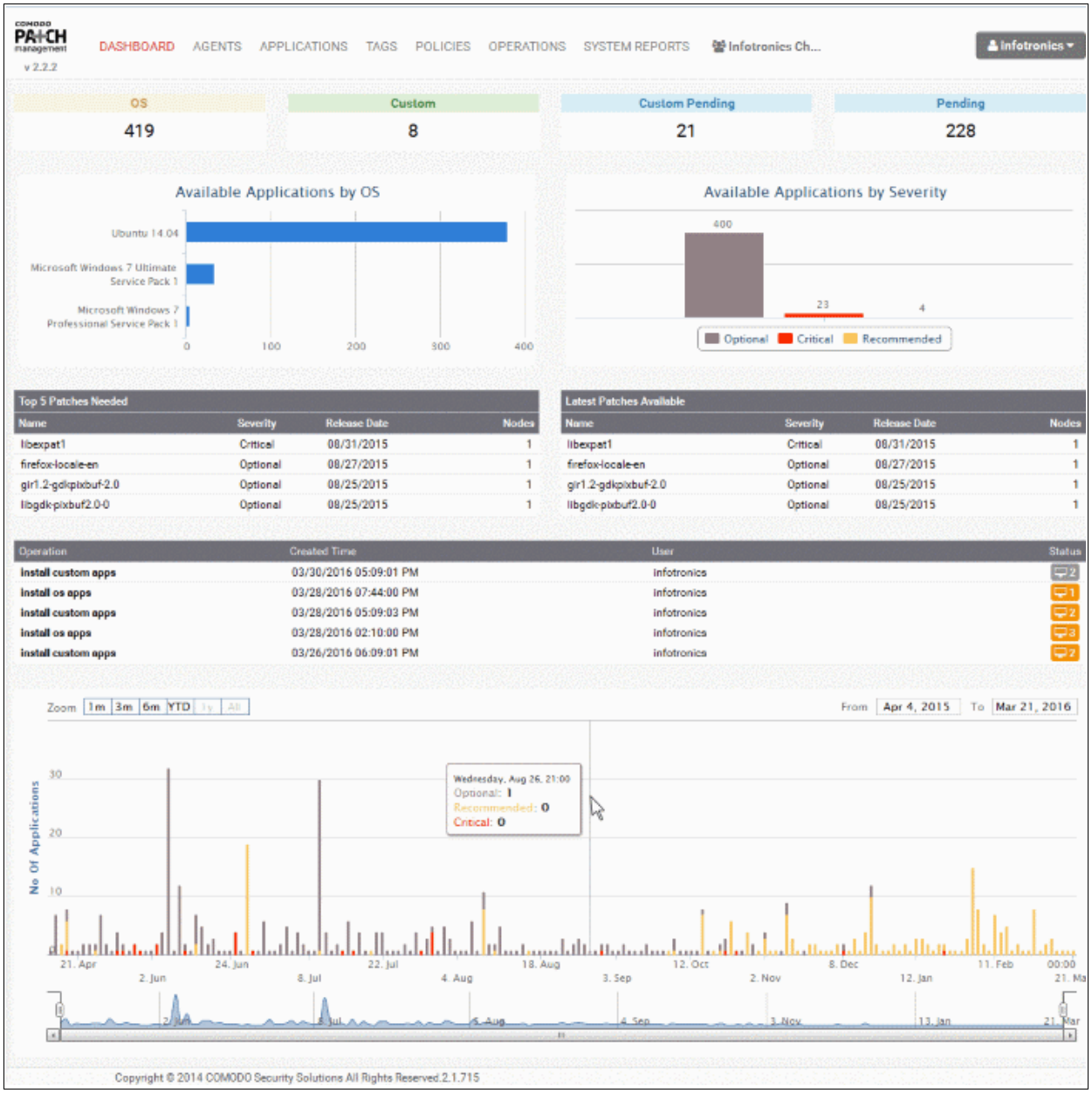
Table of Contents

1 Introduction to the Patch Management Module

Comodo Patch Manager gives administrators and MSPs granular control over the deployment of updates to operating systems and 3rd party applications on network endpoints. Featuring a centralized, easy to use interface, Comodo Patch Manager allows administrators to:

- Remotely deploy operating system updates for Windows, Linux and Mac based machines and 3rd party applications
- View dashboard statistics that provide detailed breakdowns of available updates for endpoint machines
- Identify endpoints which contain vulnerabilities and need to be patched
- Create policies to automatically apply updates to groups of tagged endpoints at scheduled times
- Create custom endpoint tags which can be applied to logical groups of endpoints
- View granular reports on the hardware, software and update history of endpoint machines

Endpoints can be added to the patch management console by installing a simple software agent on each managed endpoint.



This guide will take administrators through the set up and ongoing usage of Comodo Patch Manager and is broken down into the following main sections:

- **Introduction to the Patch Management Module**
  - **Quick Start Guide**
  - **Logging-in to the Patch Management Module**
- **Enrolling Endpoints by Installing the Agent**
- **The Dashboard**
- **Viewing and Managing Agents and Endpoints**
  - **Viewing Endpoint Details**
  - **Initiating Manual Update or Installation Operation**
  - **Remove selected endpoint(s)**
- **Managing OS Updates, Patches and Applications**
  - **Viewing Details of a Patch, Update Package or an Application**
  - **Approving Packages for Automated and Scheduled Installations**

1.1 Quick Start Guide

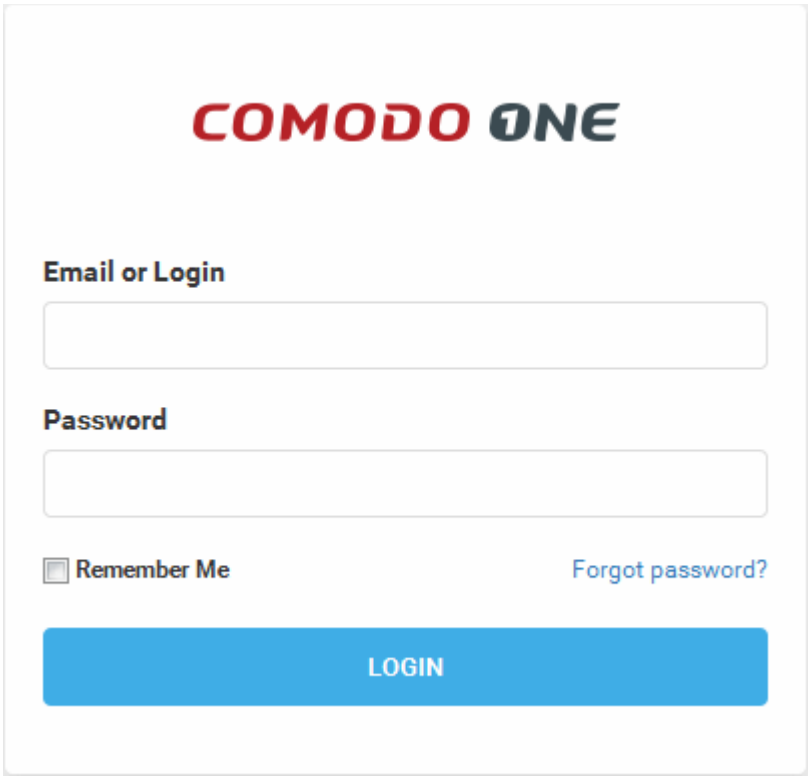
This tutorial briefly explains how an administrator can setup the patch management module for their account. It explains how to create customer accounts, enroll endpoints, create groups, manage patch deployments and view reports.

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

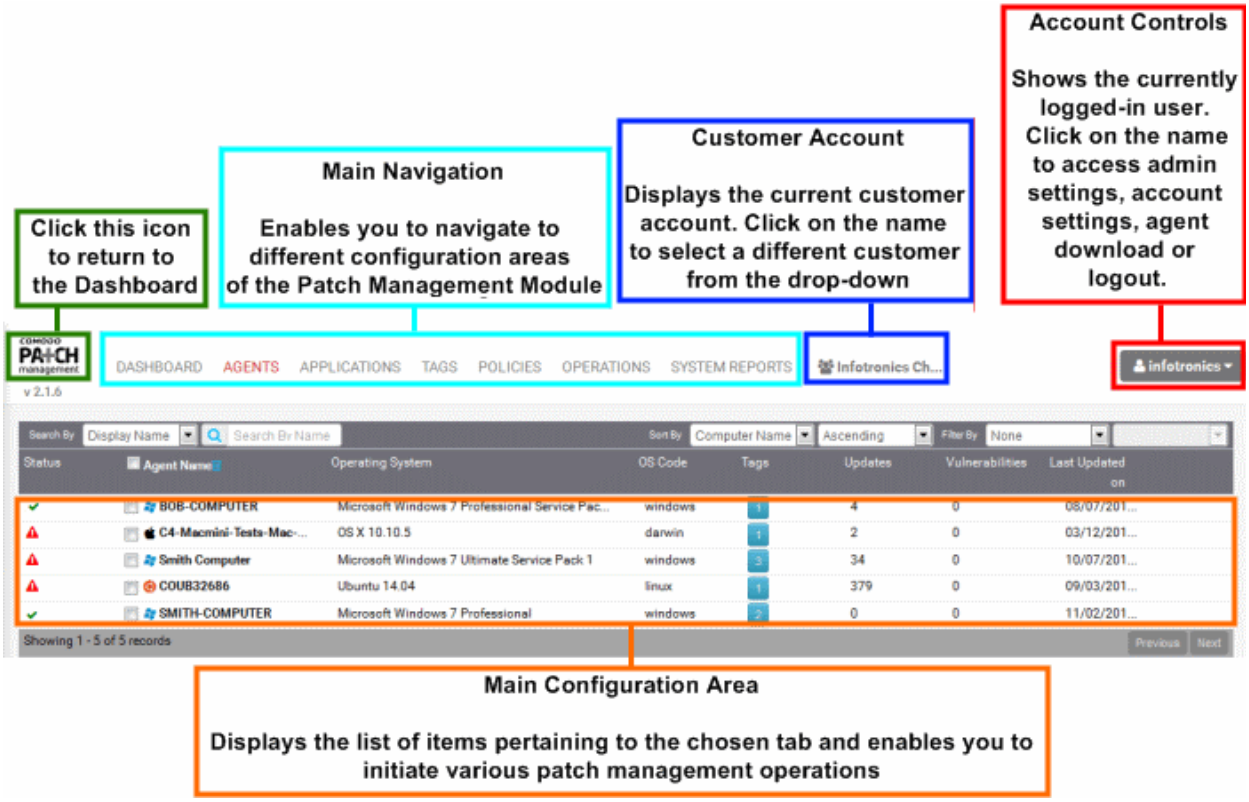
- Step 1 - Login to the patch management module
- Step 2 - Enroll endpoints to customer accounts by installing the agent
- Step 3 - Create tags and form endpoint groups
- Step 4 - Install patches/updates and third-party applications to endpoints or groups of endpoints
  - Manually install items on to endpoints or endpoint groups
  - Create policies for automated patch/updates installation operations
- Step 5 - View patch management operations
- Step 6 - View system reports

Step 1 - Logging-in to the Patch Management Module

To access the Patch Management Module, login into with your user name and password at **https://one.comodo.com/app/login**



- Once logged-in, click 'Licensed Applications' at the top then click 'Patch Management'
- Alternatively, click 'All Licensed Applications' under 'Licensed Applications', then click the 'Patch Management' tile to open the PM module



Step 2 - Enroll endpoints to customer accounts by installing the agent

The next step is to enroll the endpoints for patch management operations by installing the patch management agent on them. The agent is a small piece of software that facilitates communication between the endpoint and the patch

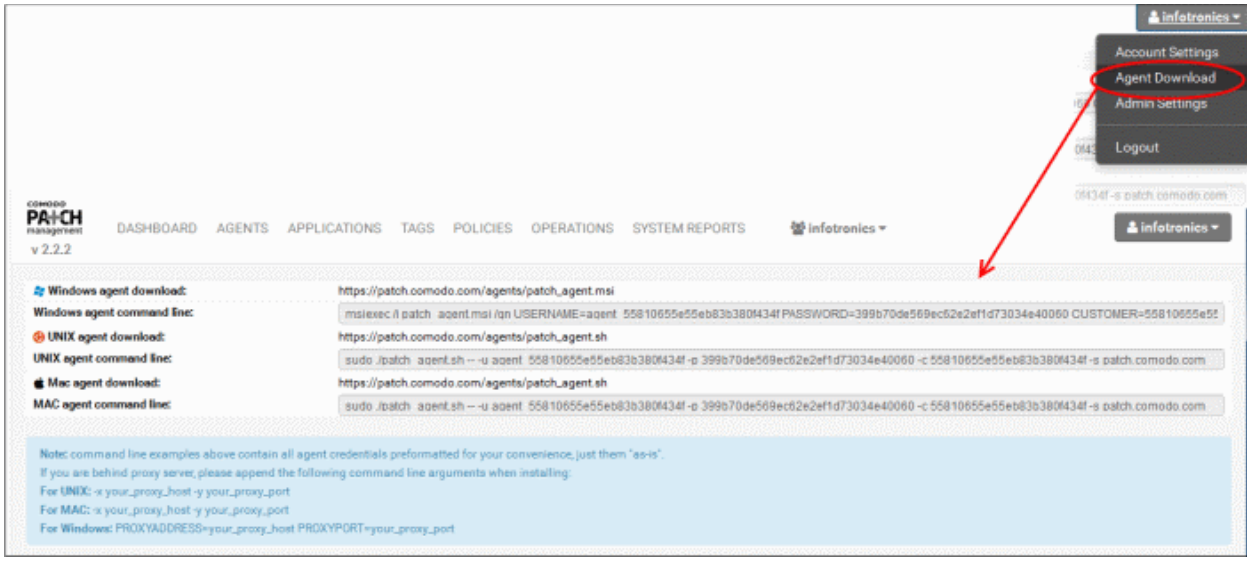
management server.

Note - If the administrator while installing the Remote Monitoring and Management (RMM) agent has opted for both RMM and Patch Management (PM), then the Windows endpoint will automatically report to the PM interface. However, for Linux and Mac endpoints, you have to install the respective agents for enrollment as explained in this step.

This section explains the installation of the agent to Windows endpoints. For details on installing the agent on Linux and Mac endpoints, refer to the section **Enrolling Endpoints by Installing the Agent** in the Administrator Guide.

The agent setup file can be downloaded from the administrative console.

1. Choose the customer account to which the endpoints are to be added from the 'Customer Account' drop-down
2. Click on your login username at the top right and choose 'Download Agent'. The agent download page will open, with the download URLs of setup files and installation instructions.



   - Copy the download URL from the 'Windows agent download' field and paste it in the address bar of any web browser to download the agent setup file.
   - Copy and save the installation command line from the 'Windows agent command line' field. This command is to be executed at the endpoints for silent installation of the agent.
3. Copy the agent installation file to the prospective target endpoint(s) through any means of file transfer like network file sharing or using removable storage media such as DVD, CD, USB memory and store it in an easily accessible location.
4. Open Windows Command Line Interface with administrative privileges
   - Click Start > All Programs > Accessories
   - Right click on 'Command Prompt' and choose 'Run as Administrator' from the context sensitive menu.
5. Execute the installation command for the silent execution.
   - Navigate to the folder in which the agent setup file is saved, from the command line
   - Enter the execution command for silent installation by pasting the command line copied from the 'Windows agent command line' field of the agent download page of the Patch Management Administrative Console.

The agent will be installed silently without displaying any alerts to the end-user. Upon completion of installation, the endpoint will be automatically discovered by the Patch Management server and enrolled for patch management under the specified customer account.

Note: For Windows Vista and previous versions please make sure that Microsoft.net Framework 3.5 SPI and Microsoft Framework 4.5.1 were installed on the machines before agent registration.

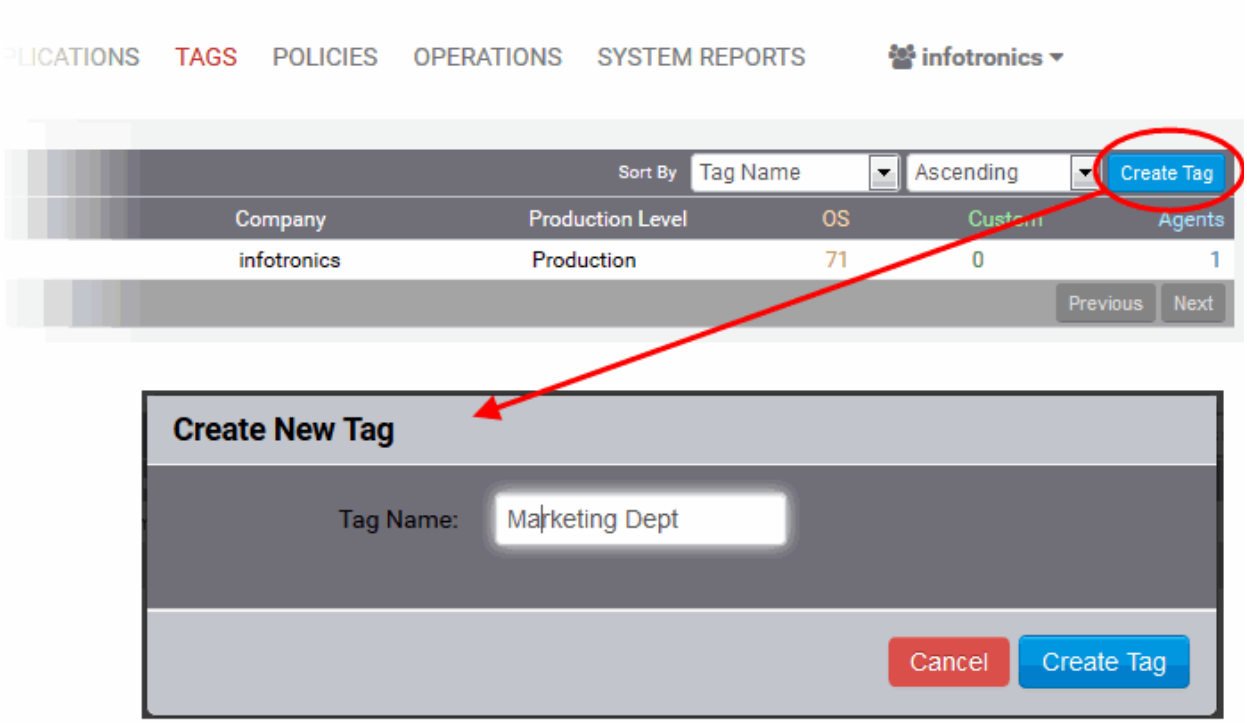
Step 3 - Create tags and form endpoint groups

Tags are identification markers for different criteria, that can be applied to endpoints for creating groups of them. A single endpoint can be applied with any number of tags so that it can be a member of more than one group. You can create multiple tags to cover attributes like operating system and department then apply them to particular endpoints as required. For example, you could create and apply tags called 'Windows XP', 'Windows 7', 'Windows Vista', 'Sales Department', 'IT department', 'DMZ Machines' and 'Accounts' department'.

Applying an action to a tag will apply the action to all endpoints applied with that tag. For example, tags can be selected as a target for any patch installation schedules you deploy in the 'Policies' area. This can save time by allowing you to accurately deploy updates to many endpoints simultaneously.

To create tags

- Select the customer account from the 'Customer Account' drop-down
- Open the tags interface by clicking the 'Tags' tab
- Click the 'Create Tag' button at the top right. The 'Create New Tag' dialog will open:



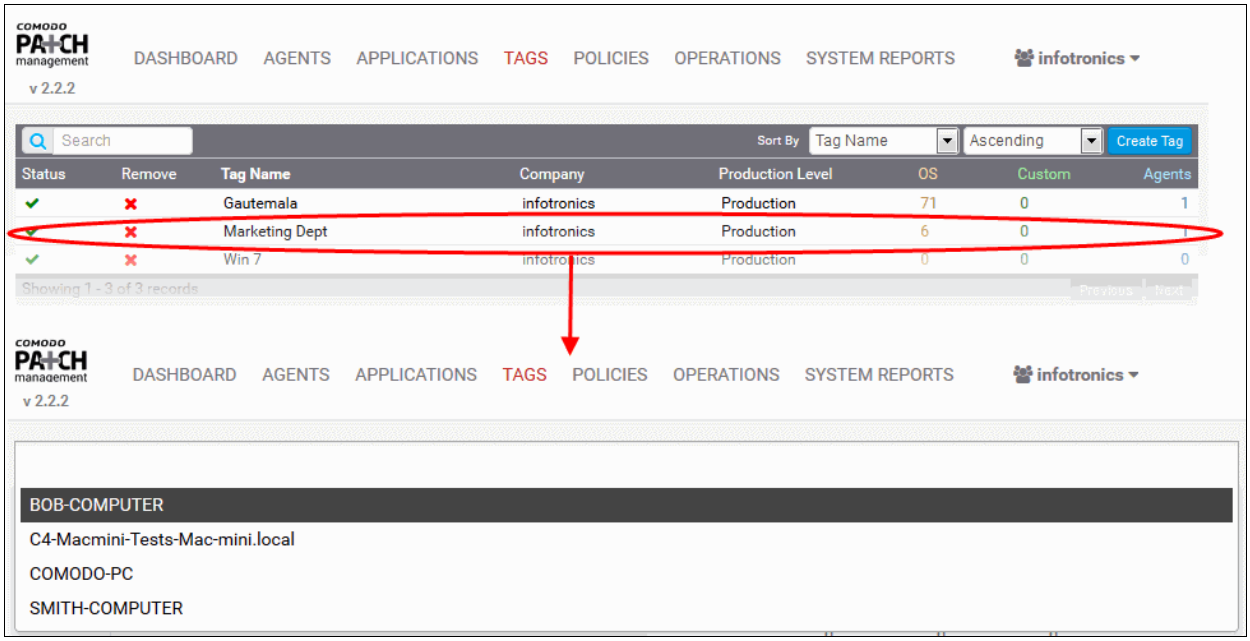
- Enter a short descriptive name to identify endpoints under the tag and click 'Create Tag'.

The new tag will be created. The tag can then be applied to endpoints from the 'Tag Properties' screen.

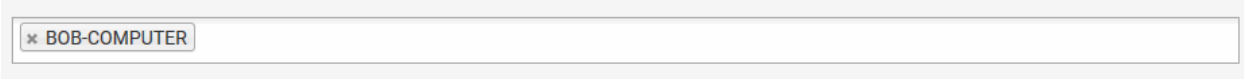
- Repeat the process for adding more number of tags.

To apply the tag to endpoints

- Click on the row of the tag to open the 'Tag Properties' screen.



- Click on the 'Select the agent' field. A drop-down with the endpoints registered for the customer account will open.
- Choose the endpoint. The endpoint will be added to the list.



- Repeat the process to add more endpoints to form the group.

Step 4 - Install patches/updates and third-party applications to endpoints or groups of endpoints

Once the server is uploaded with required patches, updates and third-party applications and endpoints are enrolled for different customer accounts, the administrator can commence patch management operations from the console.

You can install missing OS patches and updates and third-party applications on selected endpoints in two ways:

- **Manually install items on to endpoints or endpoint groups**
- **Create policies for automated patch/updates installation operations**

Manually install items on to endpoints or endpoint groups

The patch management console can display the inventory of patches/updates and third-party applications that have already been installed on each endpoint individually, and lists of those that are available in the server that are eligible for installation on the endpoint, but yet to be installed. The administrator can handpick only required items to be installed on per endpoint basis and initiate an instant installation operation or schedule the installation operation.

The console can also display a consolidated inventory of the items already installed on the group of endpoints covered by each tag and lists of those eligible for the endpoints in the group. The administrator can select the items to be installed on the endpoints in the group and initiate an instant installation operation or schedule the installation operation.

Limitations:

- For Security Patches and OS Update packages – The patch management module can install any patch or update which is auto-loaded to the server, on release by the OS vendor.
- For third-party applications and update patches - The patch management module can install any patch or application whose installation package is of the format as given below:
  - Windows - .exe, .msi, .msp, .msu

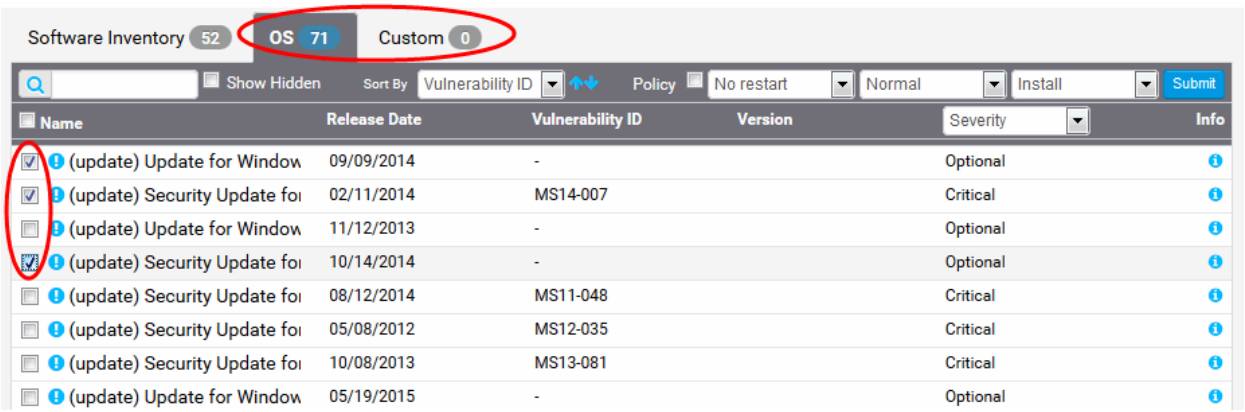
- Ubuntu/Debian - .deb
- CentOS - .rpm
- Mac - .dmg

To initiate patch installation on per endpoint basis

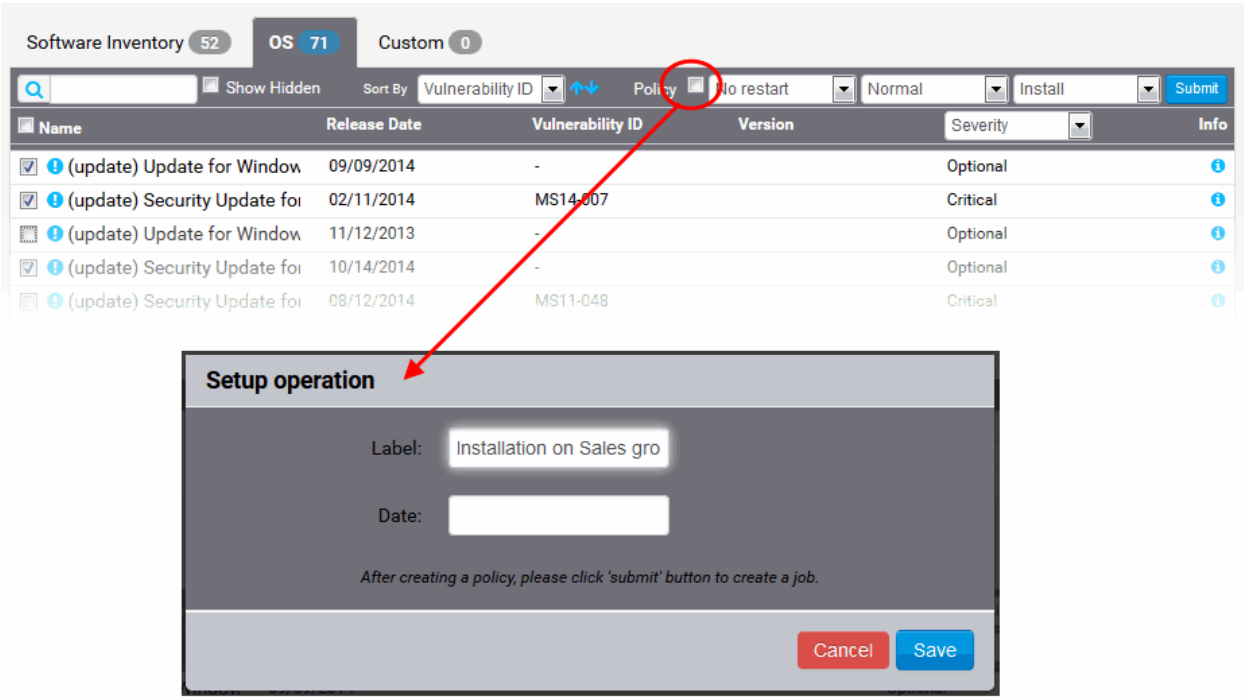
- Select the customer account from the 'Customer Account' drop-down
- Click 'Agents' tab to view the list of endpoints enrolled for the customer
- Select the endpoint on which the patches/updates or third-party application(s) is/are to be installed and click on the endpoint name. The Endpoint Details interface will open.
- Scroll down to the Inventory area at the bottom of the page.
- Select the items to be installed
    - To install patch(es) or updates, click the 'OS' tab
    - To install custom or third-party applications, select the 'Custom' tab
    - Select the item(s) to be installed. You can use the search and filter options to search for the specific patch(es)/update(s) or applications to be installed. Refer to the explanation on **Sorting, Filtering and Search Options** in the section **Viewing Endpoint Details** for more details
- Configure the installation options:

  Restart options – Select whether the endpoint needs to be restarted for the installation to take effect, from the first drop-down at the top right. The options available are:

    - **No Restart** – The endpoint will not be restarted on completion of the installation operation. If the item(s) installed require the endpoint to be restarted for the installation to take effect, it will do so, only after the next manual restart of the endpoint by the end user.
    - **Only if needed** – The patch management module will check whether the item(s) installed require(s) the endpoint to be restarted for the installation to take effect. The endpoint will be restarted upon completion of installation only if it is required.
    - **Forced** – The endpoint will be restarted upon completion of installation operation, regardless of whether the items installed requires to do so, for the installation to take effect.
- **Priority** - Choose the execution priority for the installation operation at the endpoint from the next drop-down. The CPU usage for the installation operation will be set as per the chosen priority. The options available are:
    - Idle
    - Below Normal
    - Normal
    - Above Normal
    - High
- To install the item(s) instantly, click the 'Submit' button

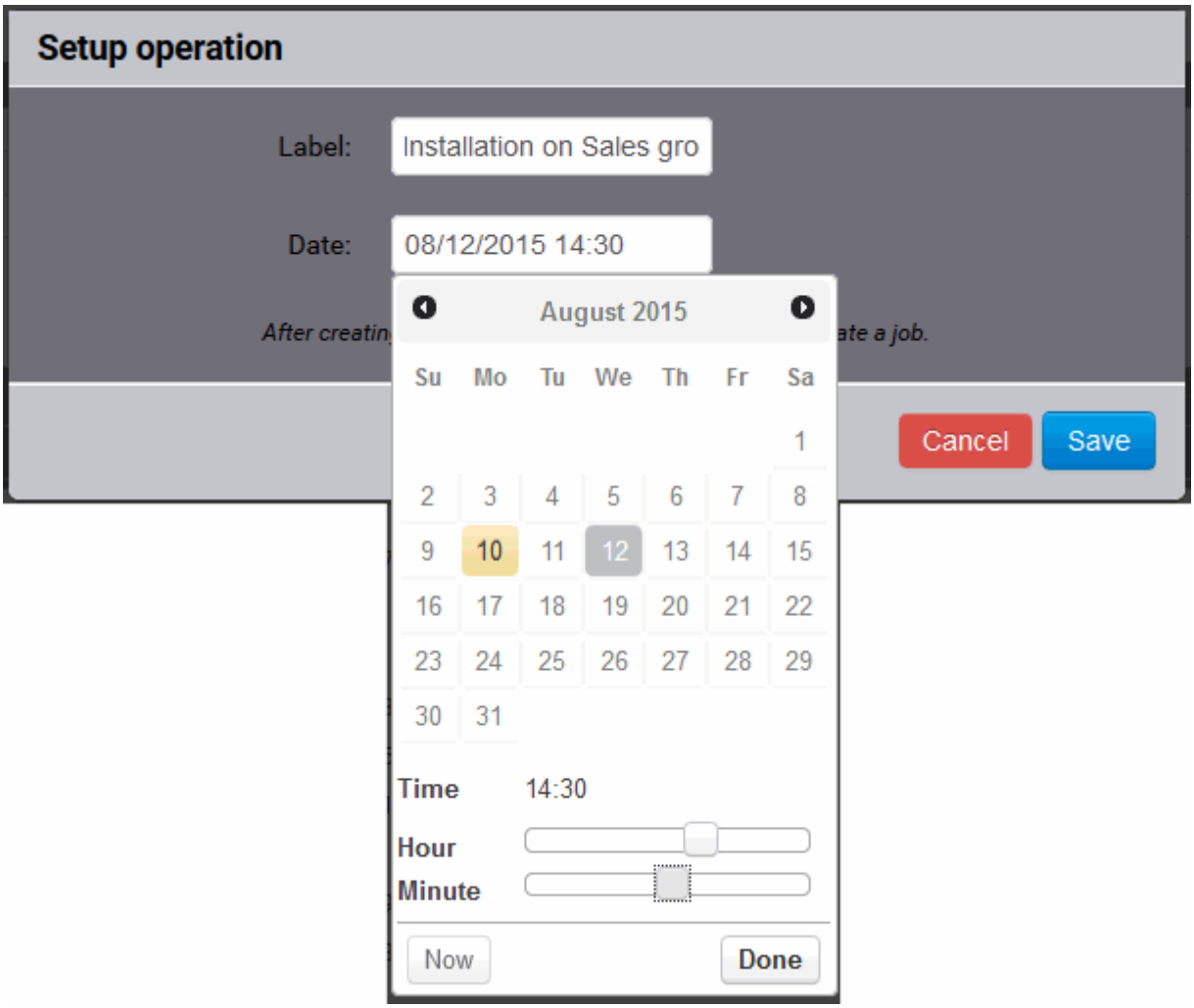


- To install the item(s) at a scheduled time, select the 'Policy' checkbox



The Setup operation dialog will appear to set the schedule.

- Enter a name for the installation operation in the label text box
- Click the Date text box to enter the time and date at which the selected patch(es) or update(s)are to be installed. A calendar drop-down will appear.



- Select the date from the calendar
- Set the time using the Hour and Minute sliders
- Click Done
- Click 'Edit' from the 'Setup operation' dialog.

- Click 'Submit' from the Inventory area.

The installation operation will be created and executed instantly or at scheduled time as chosen.

For an instant installation operation, you can view the progress of the operation from the 'Operations' interface. Refer to the section **Viewing Patch Management Operations**.

For a scheduled installation operation, you can view the schedule displayed under the 'Policies' tab. Refer to the section **Automated Management Policies**.

To initiate patch installation on an endpoint group

- Select the customer account from the 'Customer Account' drop-down
- Click 'Tags' tab to view the list of tags created for the customer account, for grouping the endpoints.
- Select the group of endpoints on which the patches/updates or third-party application(s) is/are to be installed and click on the tag name. The Tag Details interface will open.
- Scroll down to the inventory area.
- Select the items to be installed
  - To install OS patch(es) or updates, click the 'OS' tab
  - To install custom or third-party applications, select the 'Custom' tab
- Select the item(s) to be installed. You can use the search and filter options to search for the specific

patch(es)/update(s) or applications to be installed. Refer to the explanation on **Sorting, Filtering and Search Options** in the section **Viewing Details of a Tag** for more details

- Configure the installation options:

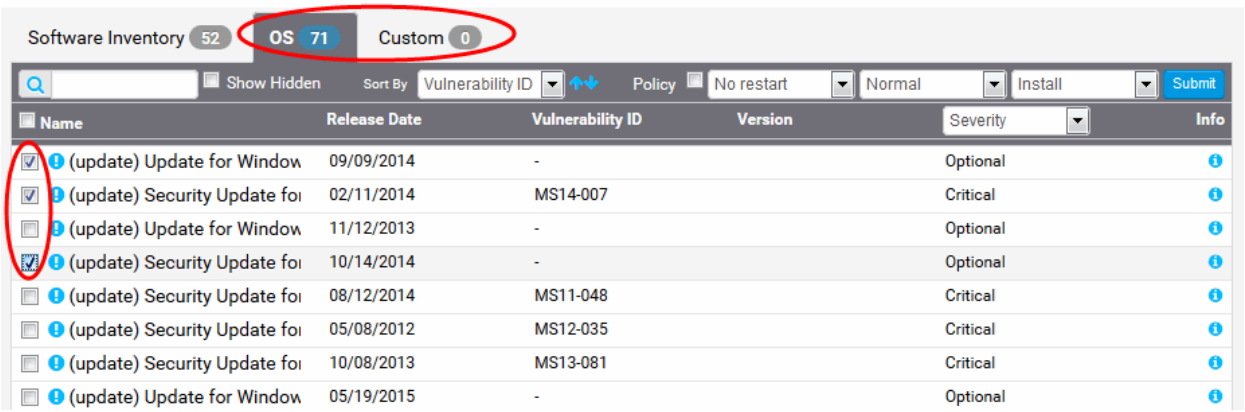
  Restart options – Select whether the endpoints need to be restarted for the installation to take effect, from the first drop-down at the top right. The options available are:

  - **No Restart** – The endpoints will not be restarted on completion of the installation operation. If the item(s) installed require the endpoint to be restarted for the installation to take effect, it will do so, only after the next manual restart of the respective endpoint by the end user.
  - **Only if needed** – The patch management module will check whether the item(s) installed require(s) the endpoint to be restarted for the installation to take effect. The endpoints will be restarted upon completion of installation only if it is required.
  - **Forced** – The endpoints will be restarted upon completion of installation operation, regardless of whether the items installed require(s) to do so, for the installation to take effect.

  Priority - Configure the execution priority for the installation operation at the endpoint from the next drop-down. The CPU usage for the installation operation will be set as per the chosen priority. The options available are:

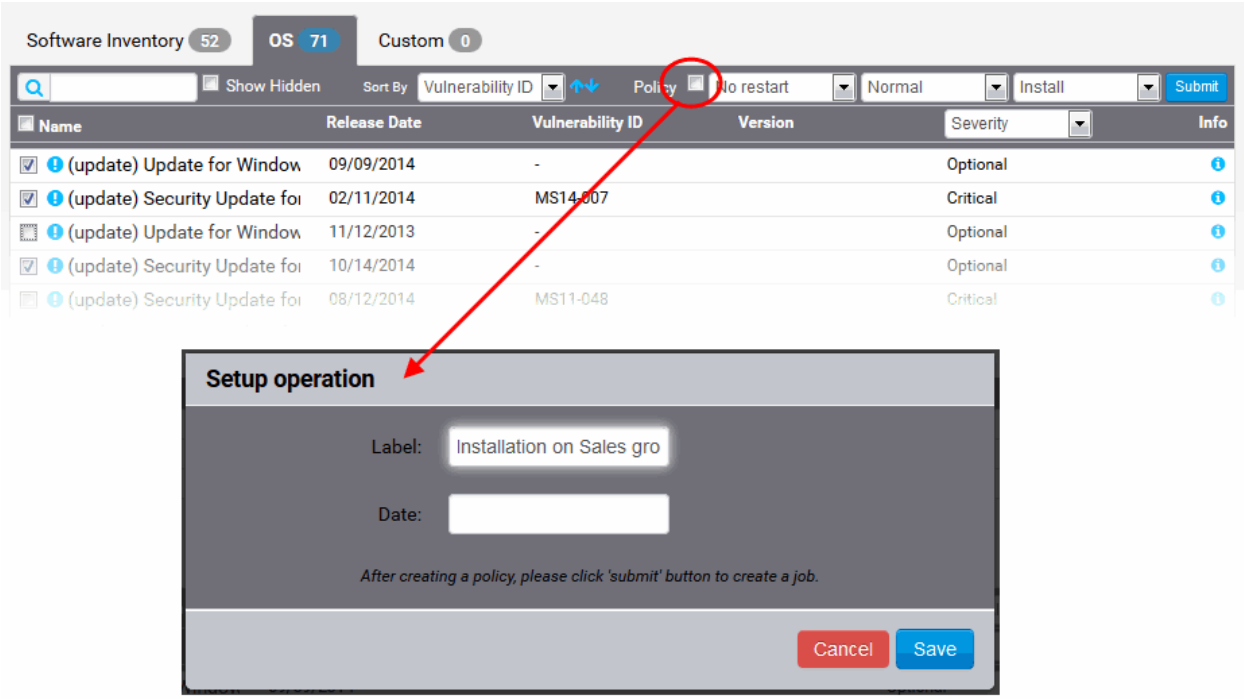
  - Idle
  - Below Normal
  - Normal
  - Above Normal
  - High

- To install the item(s) instantly, click the 'Submit' button



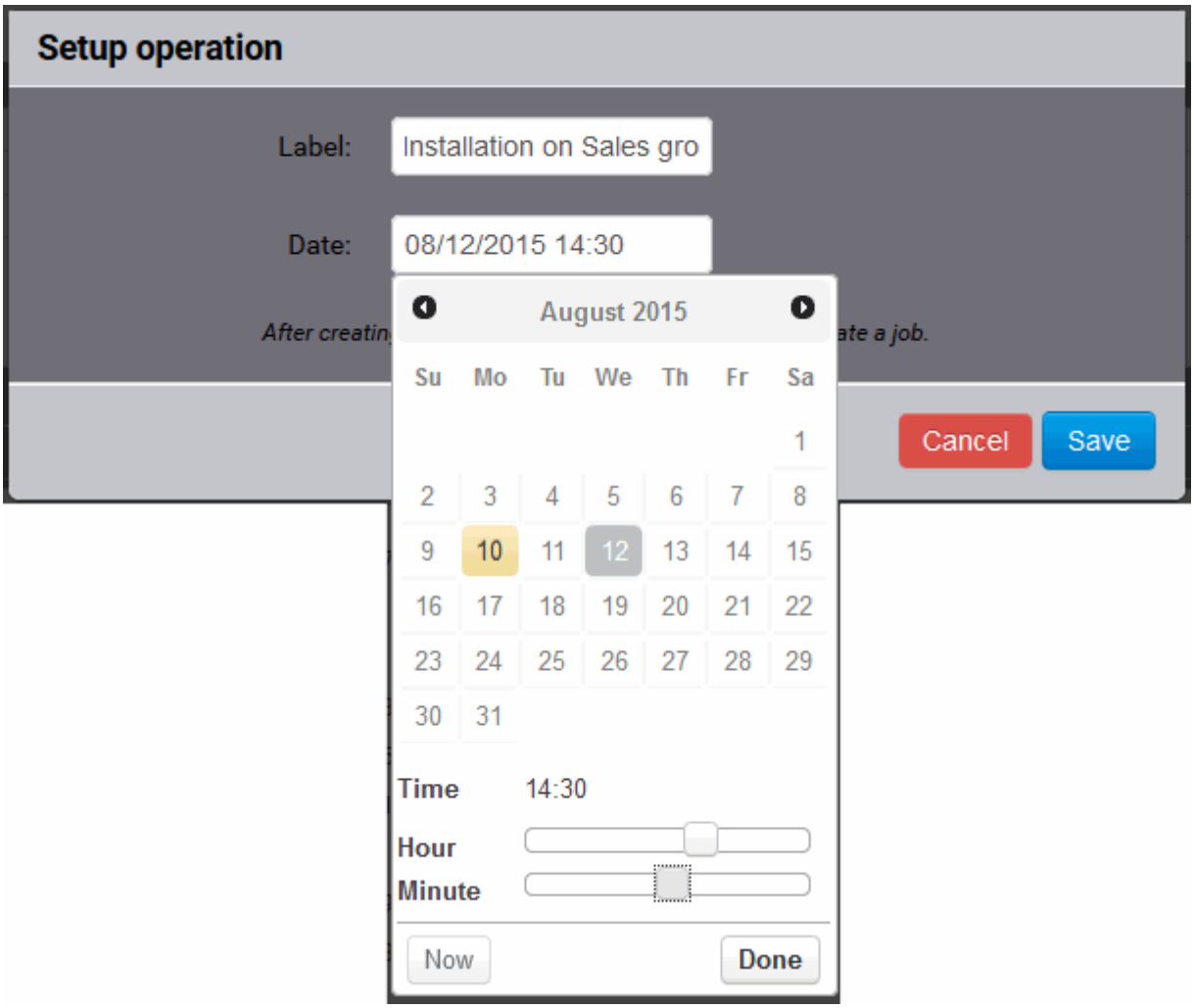
The installation operation command will be sent to the endpoints with operating systems and system requirements satisfying those of the item to be installed and covered by the tag. You can view the progress of the operation from the 'Operations' interface. For more details on viewing the details of the operation, refer to the section **Viewing Patch Management Operations**.

- To install the item(s) at a scheduled time, select the 'Policy' checkbox



The Setup operation dialog will appear to set the schedule.

- Enter a name for the installation operation in the label text box
- Click the Date text box to enter the time and date at which the selected patch(es) or update(s)are to be installed. A calendar drop-down will appear.



- Select the date from the calendar
- Set the time using the Hour and Minute sliders
- Click 'Done'
- Click 'Edit' from the 'Setup operation' dialog.

- Click 'Submit' from the Inventory area.

The installation operation command will be sent to the endpoints with operating systems and system requirements satisfying those of the item to be installed and covered by the tag, at the time as specified in the schedule. You can view the schedule displayed under the 'Policies' tab.

- For more details on managing scheduled operations, refer to the section **Automated Patch Management Policies**.

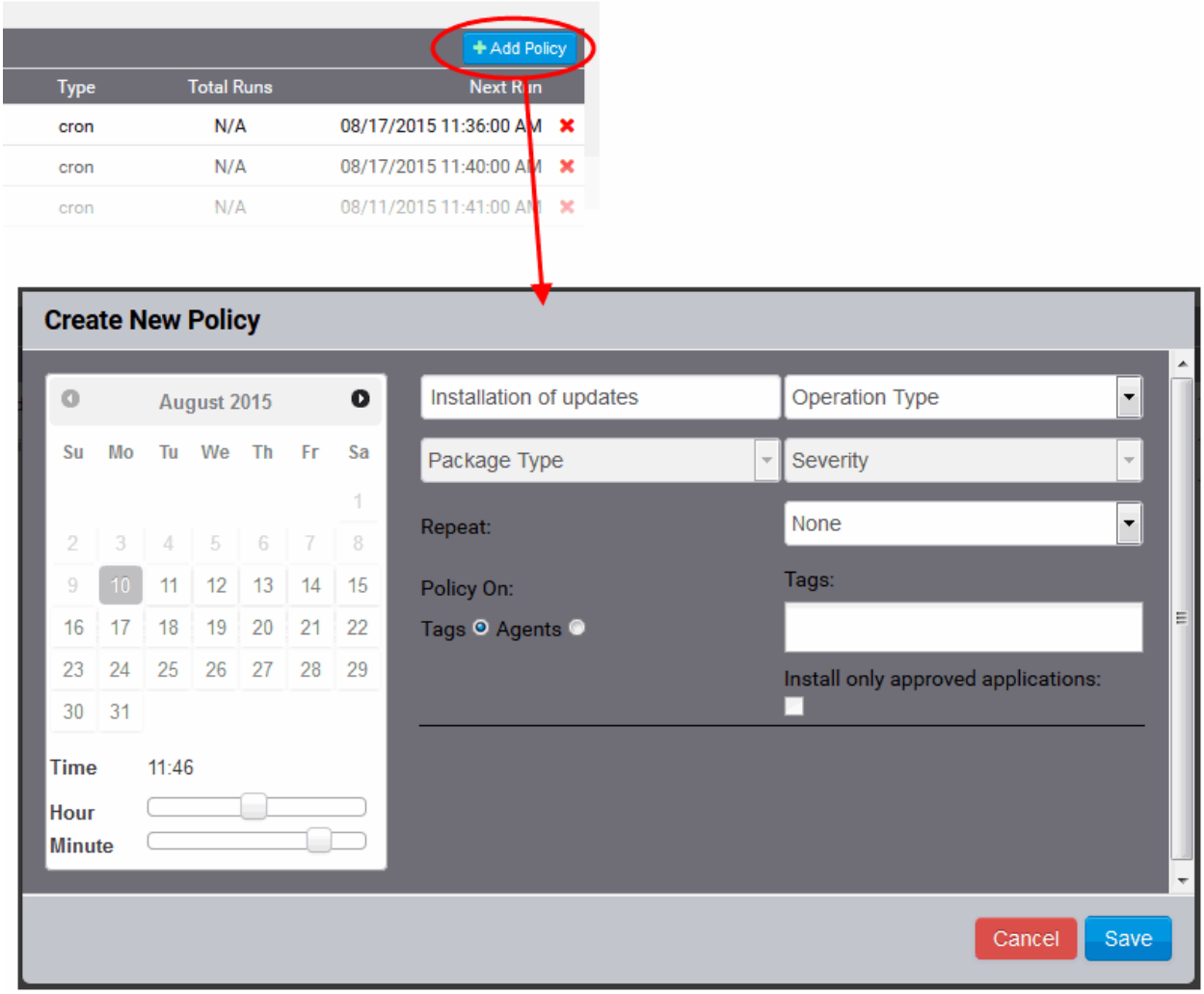
Create policies for automated patch/updates installation operations

You can create policies for automated, periodical and repeated patch management operations of the endpoints. The policies are constructed by specifying:

- The operation, like installation of OS patches/updates or the third-party applications, periodical reboot of the endpoints
- The schedule for the operation
- The endpoints or groups upon which the operations needs to be performed.

To create a policy

- Select the customer account from the 'Customer Account' drop-down
- Open the policies interface by clicking the 'Policies' tab
- Click the 'Add Policy' button at the top right. The 'Create New Policy' dialog will open:



- Configure the parameters as shown below:

Create New Policy Dialog – Table of Parameters	
Parameter	**Description**
Policy Name	Enter a name shortly describing the operation to be executed as per the schedule.
Operation Type	Select the operation to be executed from the drop-down: • Install - Installs the OS patches/updates or third-party applications

	available from the server at the time of execution on to the selected endpoint(s), appropriate to their respective operating systems. • Reboot – Restarts the selected endpoints.
Package Type	Select the type of items to be installed from the drop-down, if you have chosen 'Install' as operation type: • OS - Installs the OS patches and update packages available from the server at the time of execution on to the selected endpoint(s), appropriate to their respective operating systems. • Custom - Installs the third-party applications available from the server at the time of execution on to the selected endpoint(s), appropriate to their respective operating systems. You can filter the items to be installed by choosing the severity level of them.
Severity	Select the severity level of items to be installed from the drop-down. • Any – Installs all the items • Optional – Installs only the optional items • Recommended – Installs only the recommended items • Critical - Installs only the items with 'Critical' severity level
Repeat	Choose the frequency at which the operation is to be performed: None – The operation will be executed only once on the date and time chosen from the calendar at the left. Choose the date from the calendar and time from the Hour and Minute sliders. Every day – The operation will be executed daily at the set time, starting from the date and time chosen from the calendar. Every week - The operation will be repeated weekly once on the day of the week same as that of the date chosen from the calendar, at the set time for the first execution . Every Month - The operation will be repeated monthly once on the day of the month same as that of the date and time chosen from the calendar for the first execution. Every Year - The operation will be repeated yearly once on the day of the year same as that of the date and time chosen from the calendar for the first execution. Custom – Repeats the operation at custom intervals. Refer to the **section below, explaining setting up the custom intervals**.
Policy On	Choose whether the operation is to be executed on selected endpoint(s) or group(s) of endpoints covered by specified tag(s). • Tags – On choosing Tags, click inside the Tags field at the right and select the tags that cover the endpoints upon which the items are to be installed from the drop-down. • Agents - On choosing Agents, click inside the Agents field at the right and select the Endpoints upon which the items are to be installed from the drop-down.
Install only approved applications	Selecting the checkbox installs only those items that are approved for automated installation from the 'Applications' interface. For more details on approving the items, refer the section **Approving Packages for Automated and Scheduled Installations**..

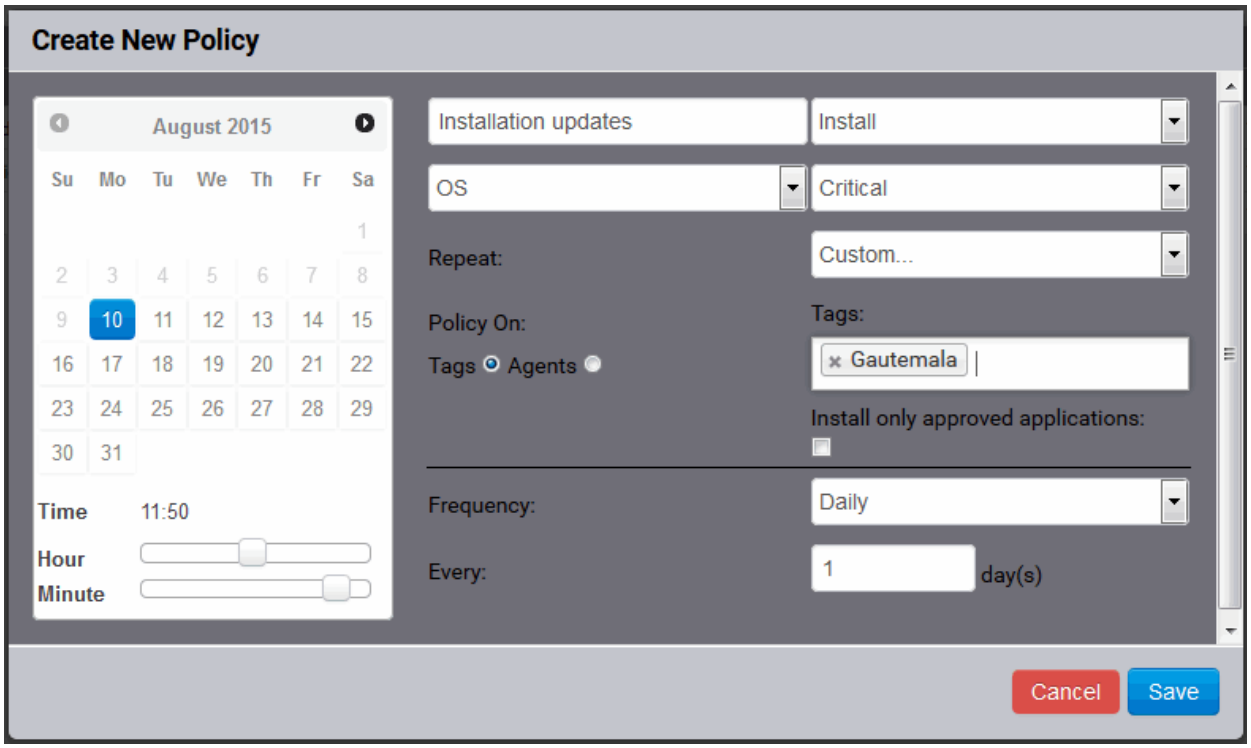
Setting Custom Intervals for Scheduled Patch Management Operation

The administrator can also configure the policies to execute the operation repeatedly at custom time points. The schedule can be set to run the operation once in every:

- **'N' number of days** – The operation will be run once in on every N number of days at the set time
- **'N' number of weeks** - The operation will be run once in on every N number of weeks on the set weekdays at the set time.
- **'N' number of months** - The operation will be run once in on every N number of months on the set days at the set time.
- **'N' number of years** - - The operation will be run once in on every N number of years on the set dates at the set time.

To set a schedule for the operation to run every 'N' number of days

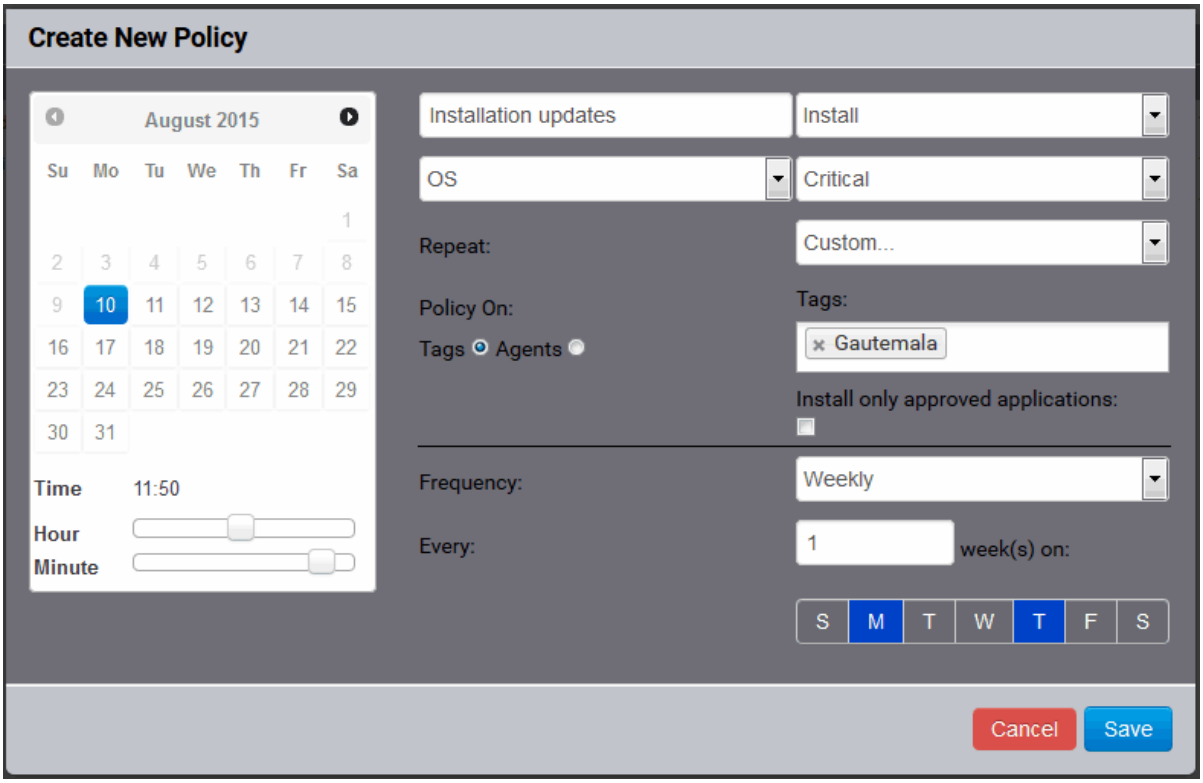
- Choose 'Custom' from the Repeat drop-down.



- Select 'Daily' from the 'Frequency' drop-down.
- Choose the number of days to be set as the interval from the Every drop-down.
- Set the time at which the operation is to be executed from the time slider at the left
- Click Save from the Create New Policy dialog,

To set a schedule for the operation to run every 'N' number of weeks

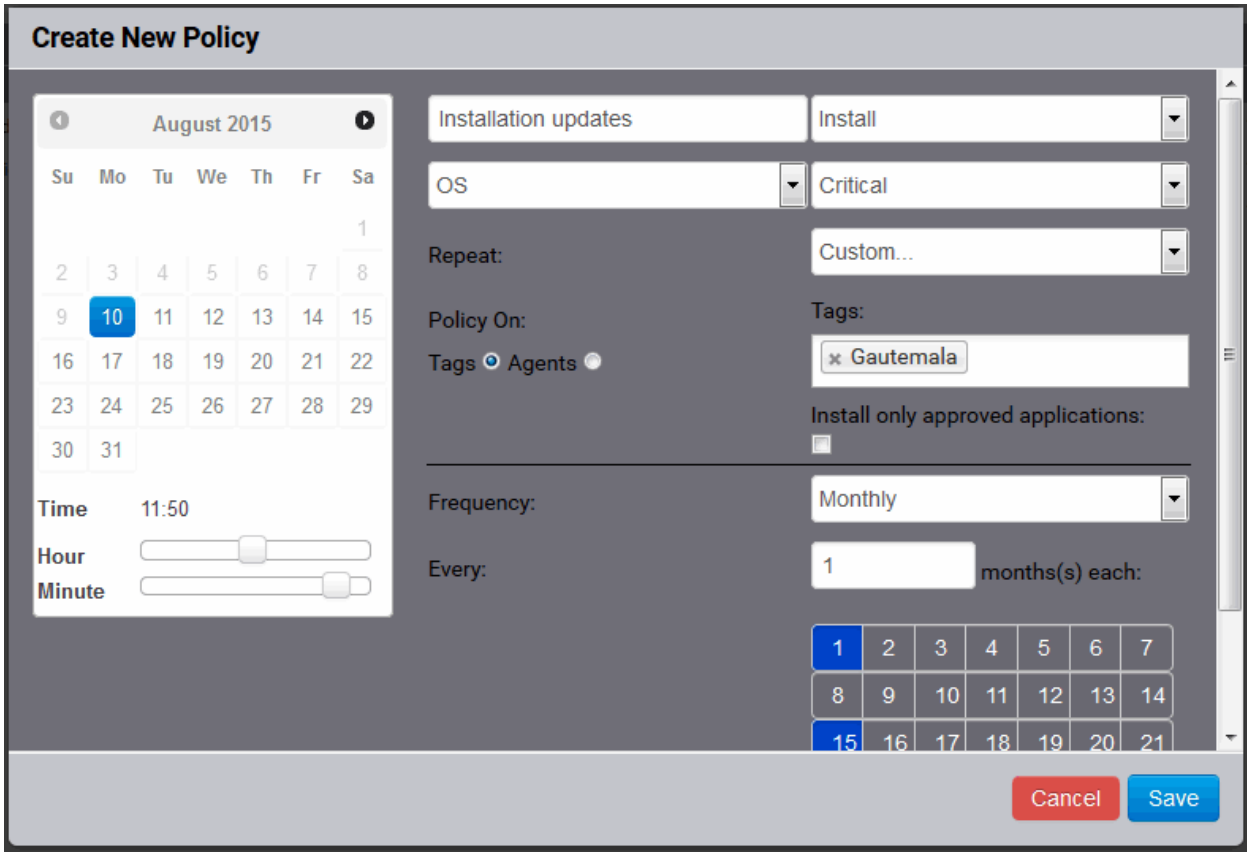
- Choose 'Custom' from the Repeat drop-down.
- Select 'Weekly' from the 'Frequency' drop-down.



- Choose the number of weeks to be set as the interval from the 'Every' drop-down.
- Select the days of the week from the days displayed below 'Every' drop-down.
- Set the time at which the operation is to be executed from the time slider at the left.
- Click 'Save' from the Create New Policy dialog.

To set a schedule for the operation to run every 'N' number of months

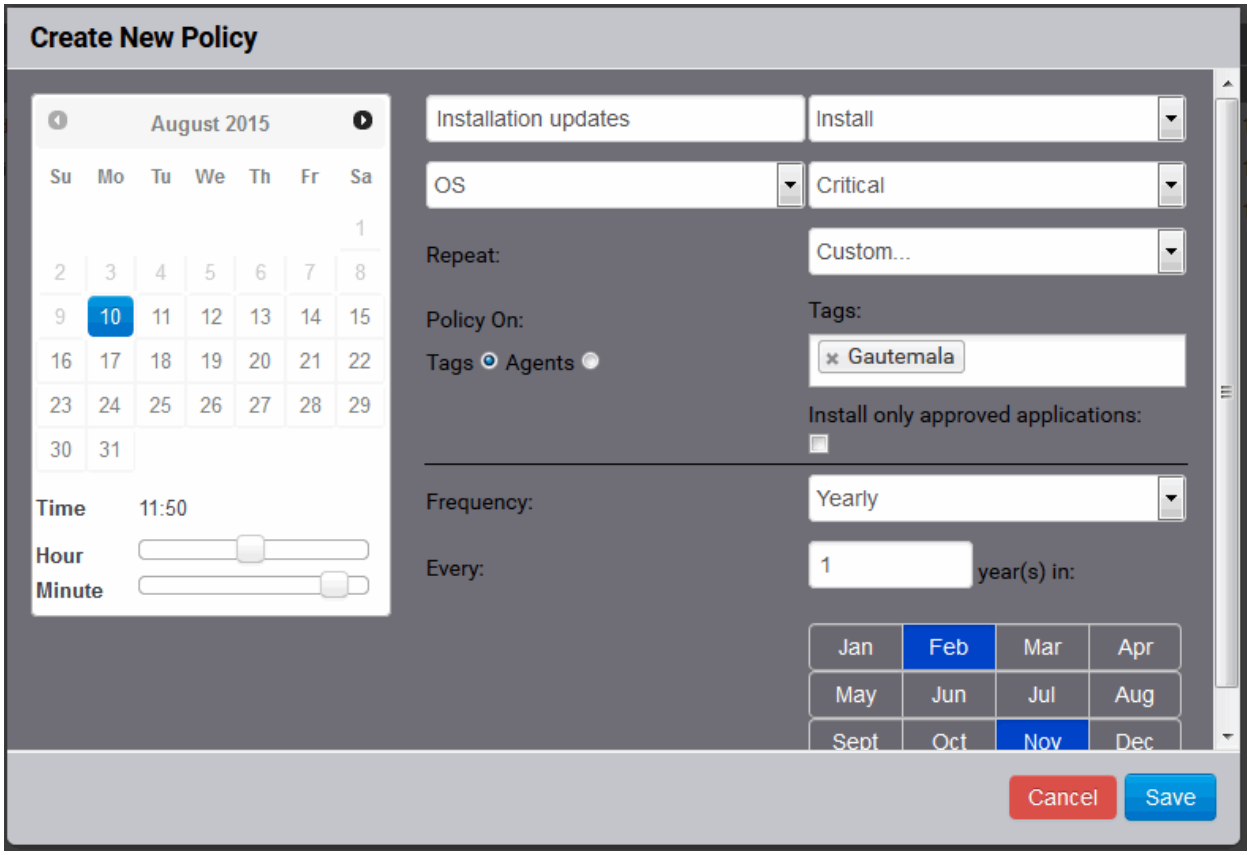
- Choose 'Custom' from the Repeat drop-down.
- Select 'Monthly' from the 'Frequency' drop-down.



- Choose the number of months to be set as the interval from the 'Every' drop-down.
- Select the days of the month from the month calendar displayed below 'Every' drop-down.
- Set the time at which the operation is to be executed from the time slider at the left.
- Click 'Save' from the Create New Policy dialog.

To set a schedule for the operation to run every 'N' number of years

- Choose 'Custom' from the Repeat drop-down.
- Select 'Yearly' from the 'Frequency' drop-down.



- Choose the number of years to be set as the interval from the 'Every' drop-down.
- Select the months from the months displayed below 'Every' drop-down.
- Set the day of the month(s) and the time at which the operation is to be executed from the calendar at the left.
- Click 'Save' from the Create New Policy dialog.

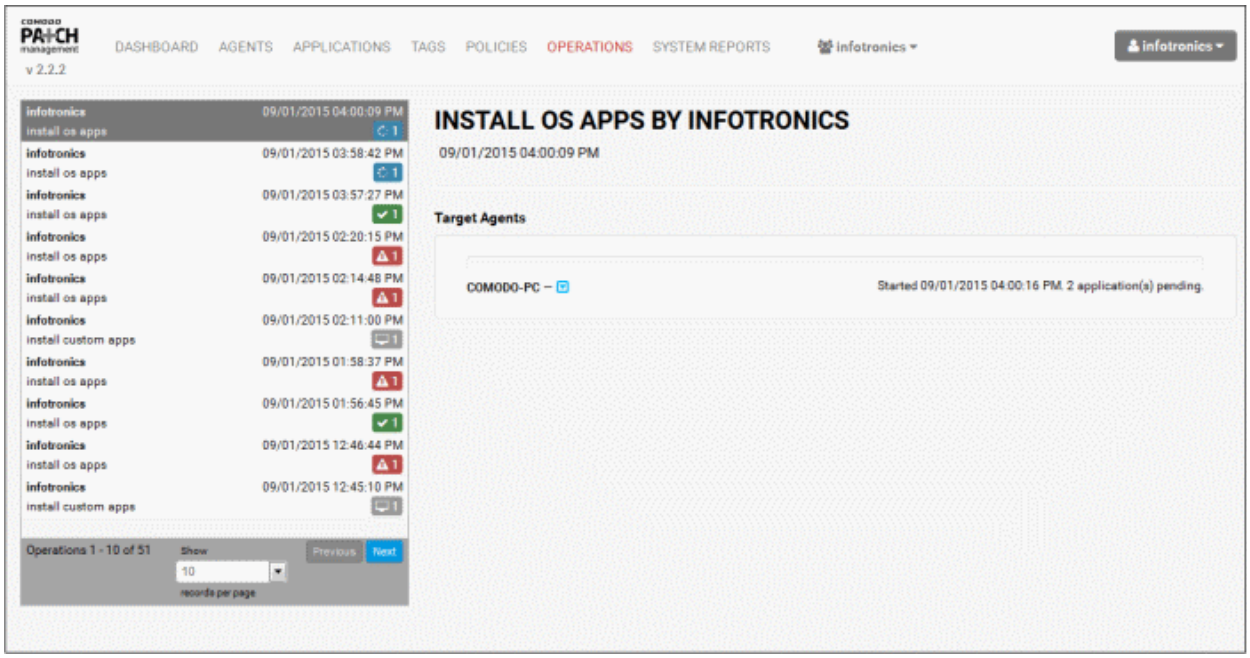
The schedule will be saved and the operation will be executed as per the schedule.

Step 5 - View patch management operations

The administrator can view the progress and details of the patch management that are currently running and the scheduled operations from the 'Operations' interface.

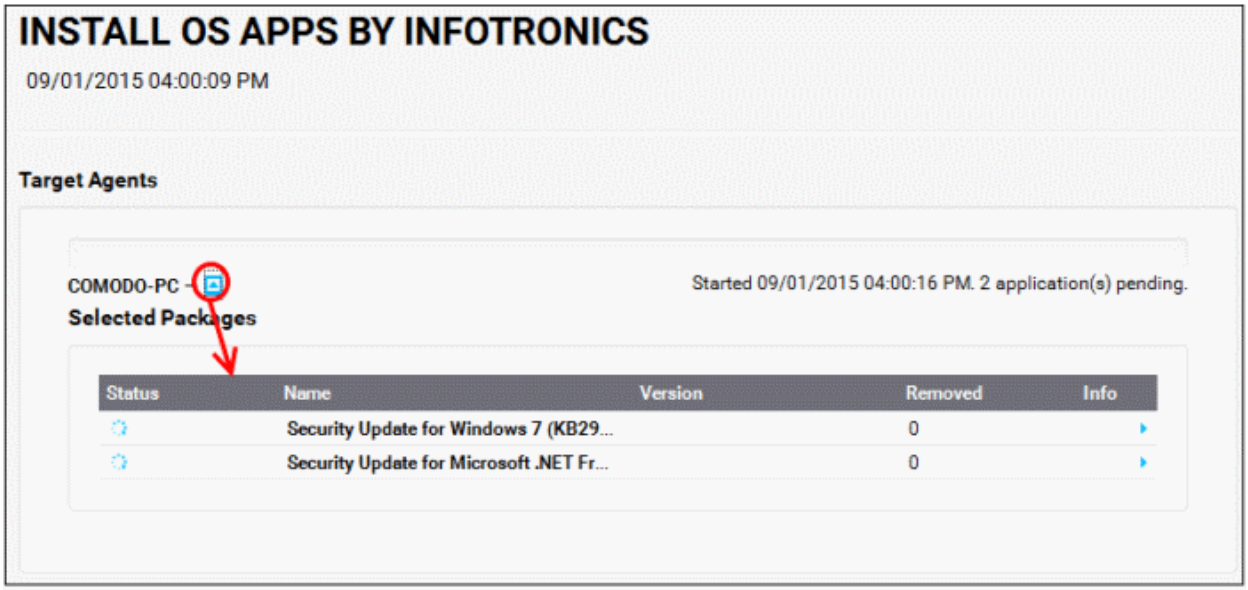
To view the list of operations

- Click the 'Operations' tab.

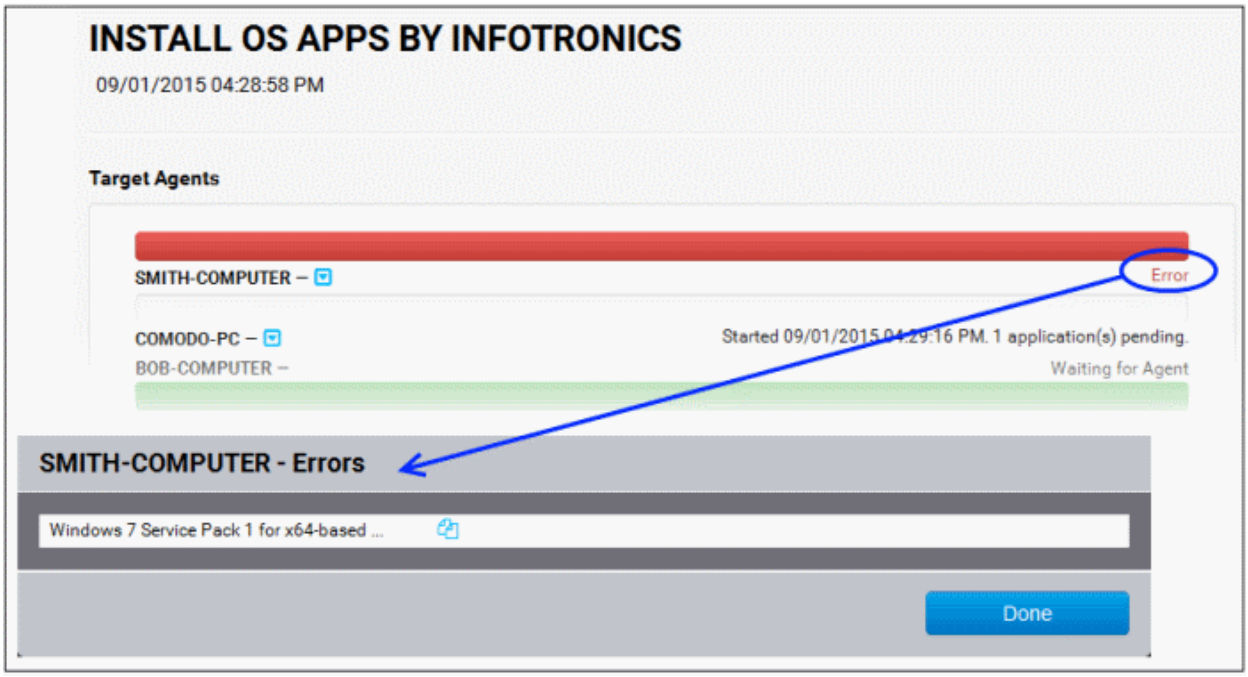


The left hand pane displays the list operations. The right hand pane displays the details of the operation selected from the list with its progress at each endpoint.

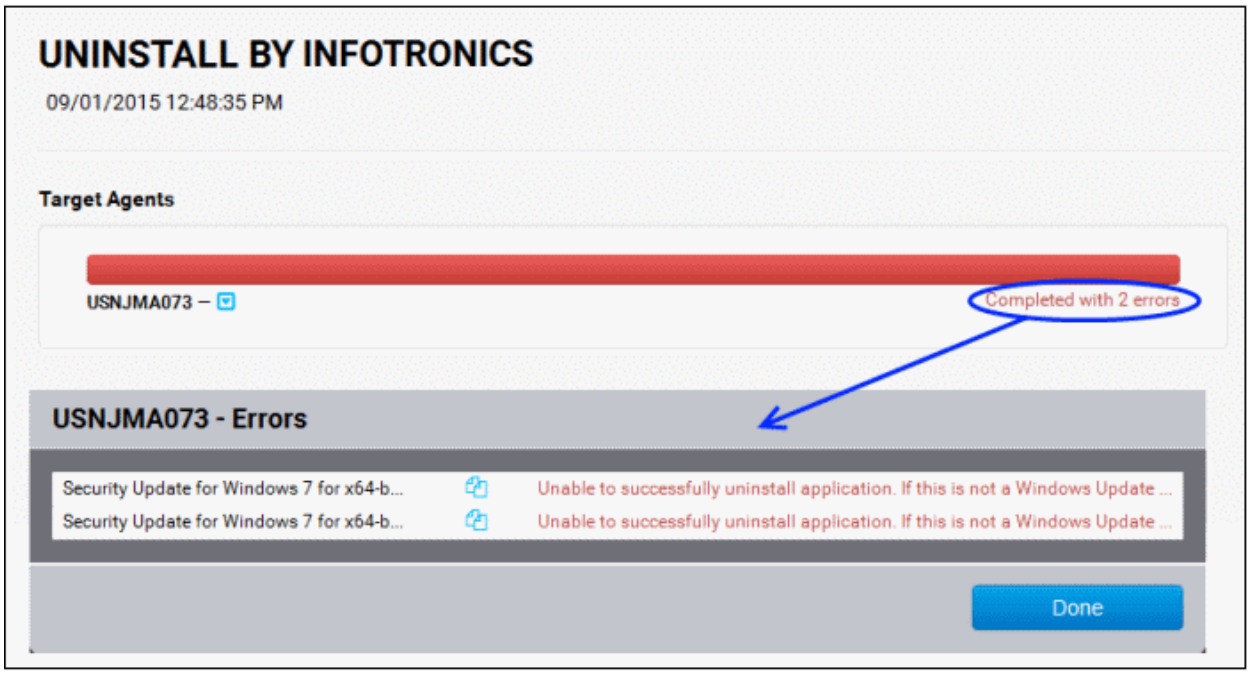
The details pane lists the target endpoints and the progress status of the operation. The administrator can also view the list of items being installed at any endpoint by clicking the blue drop-down beside the endpoint name.



- To view the error messages for operations not completed successfully, Click on the 'Error' link at the right end, for the endpoint you wish to see the error details.



- To view the error messages for operations that are completed with errors, click on the 'Completed with 'N' errors' link at the right end, for the endpoint you wish to see the error details.

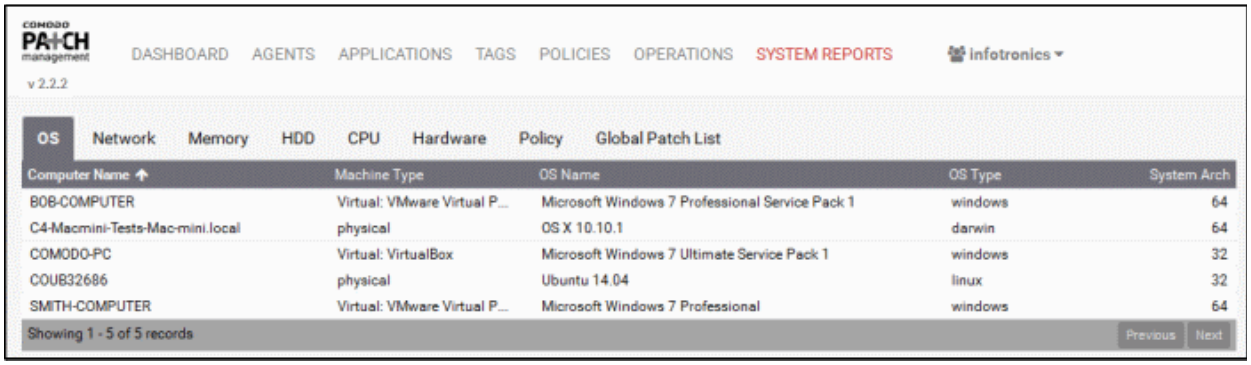


The list of applications that failed to install and the reasons for failure is displayed.

Step 6 - View system reports

The administrator can view the summaries of hardware/software/network details for each endpoint registered for the customer account under the System Reports tab. It also displays the patch management policies active for the customer and an exhaustive list of available OS patches and updates with details of endpoints affected by them.

To view the reports on each endpoint, click the 'System Reports' tab



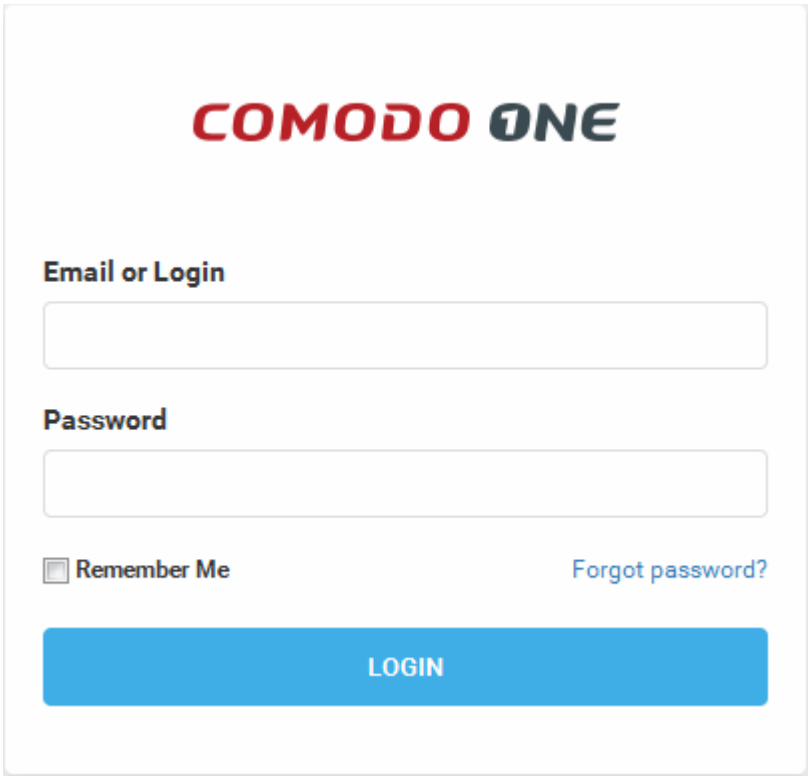
The Interface contains the following tabs:

- **OS** - Displays the details of operating system of each endpoint added to the customer account.
- **Network** - Displays information on the networks to which each endpoints is connected. This includes the type of network and the MAC and IP addresses of the endpoint.
- **Memory** - Displays the size of the system memory (RAM) mounted on each endpoint and the current usage statistics of it.
- **HDD** - Displays the details of the hard disk drive mounted on each endpoint and the current usage statistics of it.
- **CPU** - Displays the details of the CPU usage (in percentage), by user initiated and system initiated processes.
- **Hardware** – Displays information on basic hardware components like HDD, CPU, Display and RAM in each endpoint.
- **Policy** - Displays the policies for automated and scheduled patch management, active for the customer account.
- **Global Patch List** - Displays an exhaustive list of available OS patches and updates with details of endpoints affected by them.

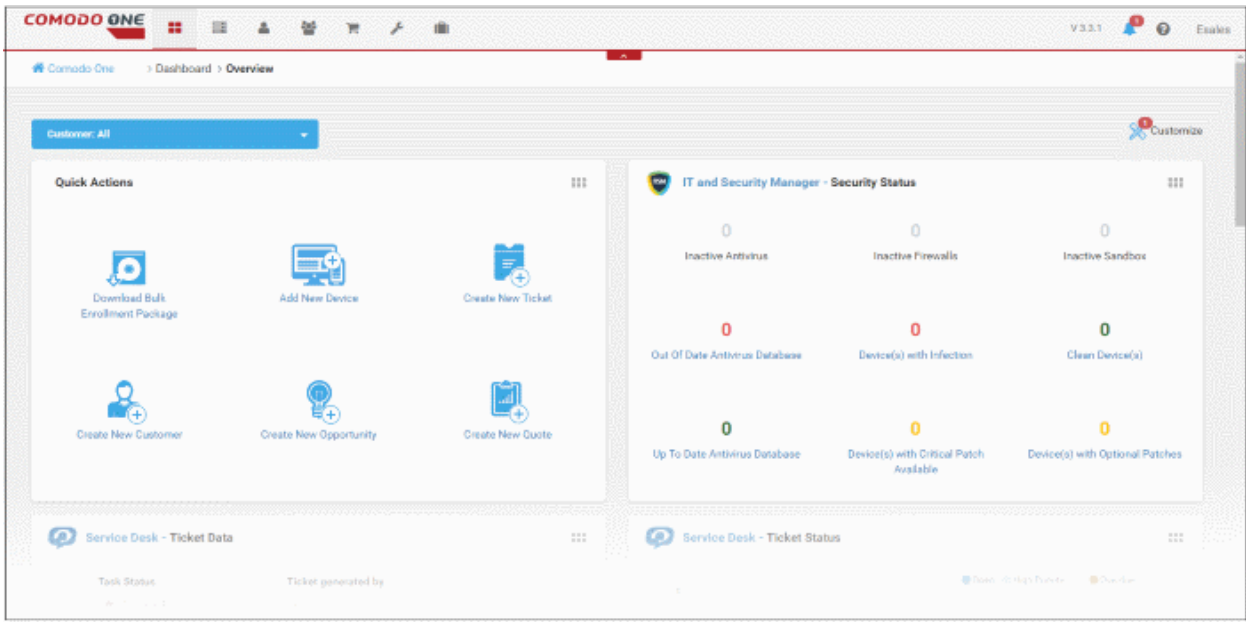
Full details of the information displayed under each tab is available in the section **Viewing Endpoint Report Summaries** of the Administrator Guide.

1.2 Login to the Patch Management Module

To access the Patch Management Module, login into with your user name and password at **https://one.comodo.com/app/login**



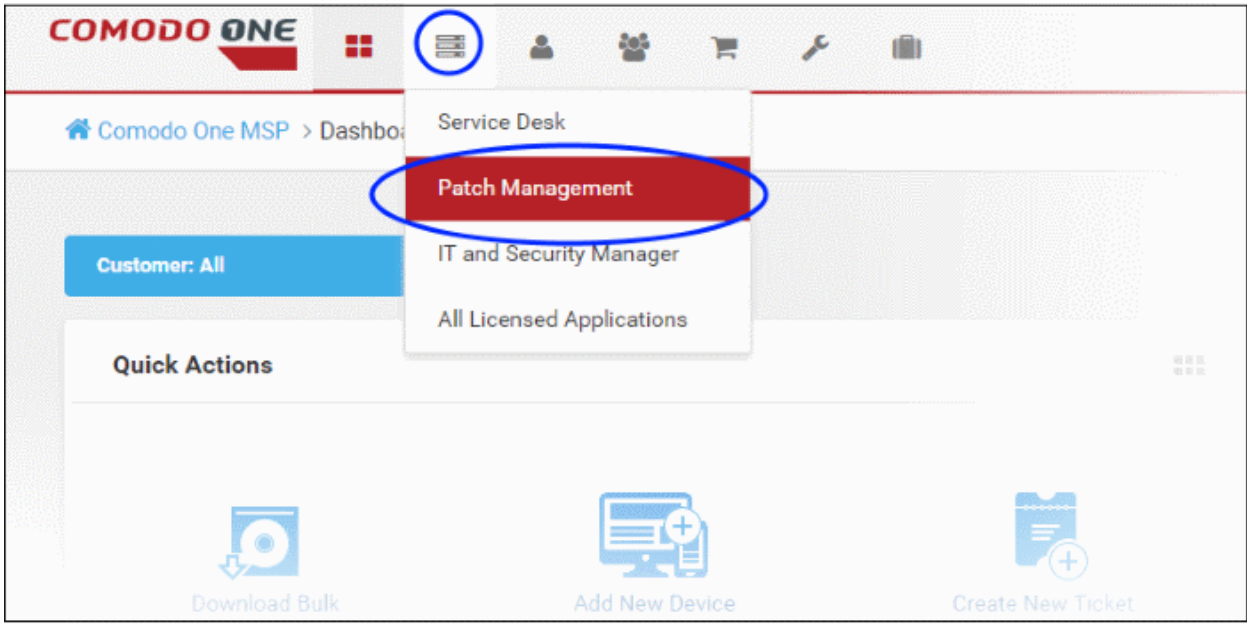
The C1 Dashboard will be displayed.



For more details about C1 dashboard, refer to our online guide at **https://help.comodo.com/topic-289-1-716-8730-The-Dashboard.html**

To open the Patch Management module

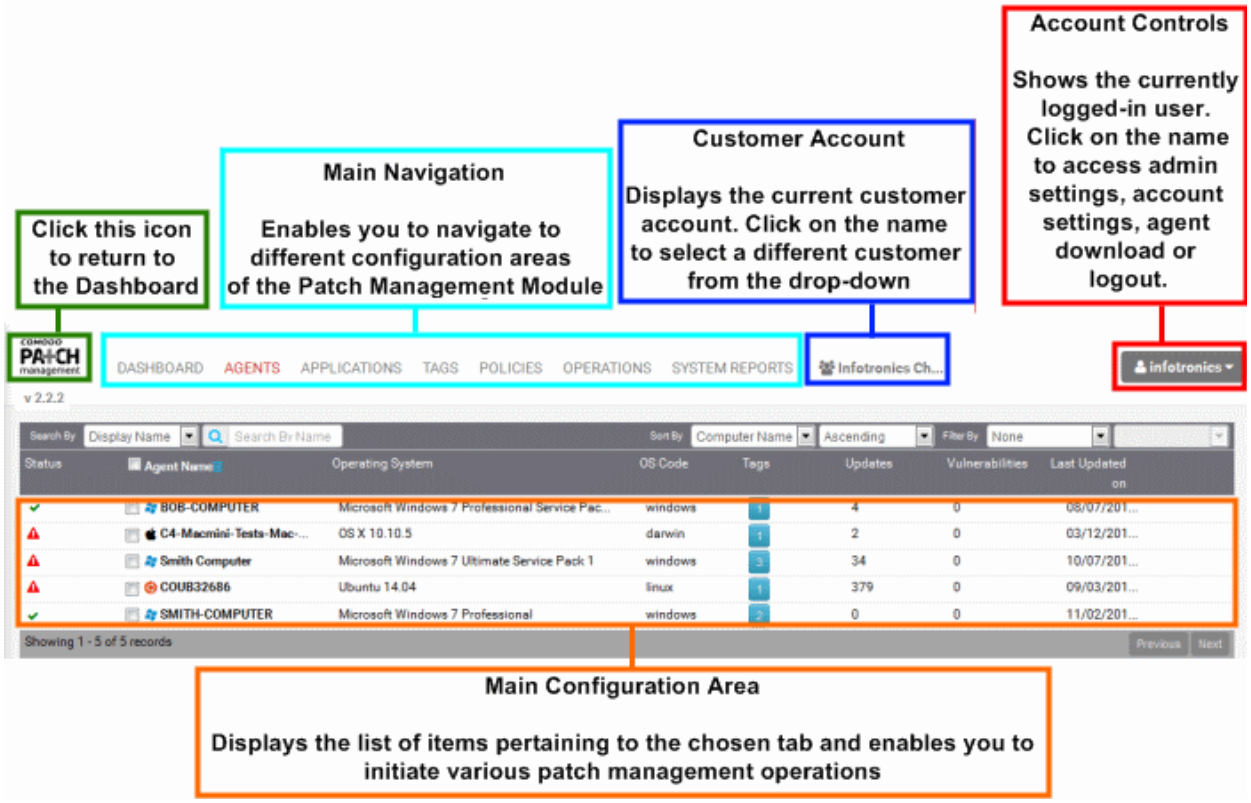
- Once logged-in, click 'Licensed Applications' at the top then click 'Patch Management'
- Alternatively, click 'All Licensed Applications' under 'Licensed Applications', then click the 'Patch Management' tile to open the PM module

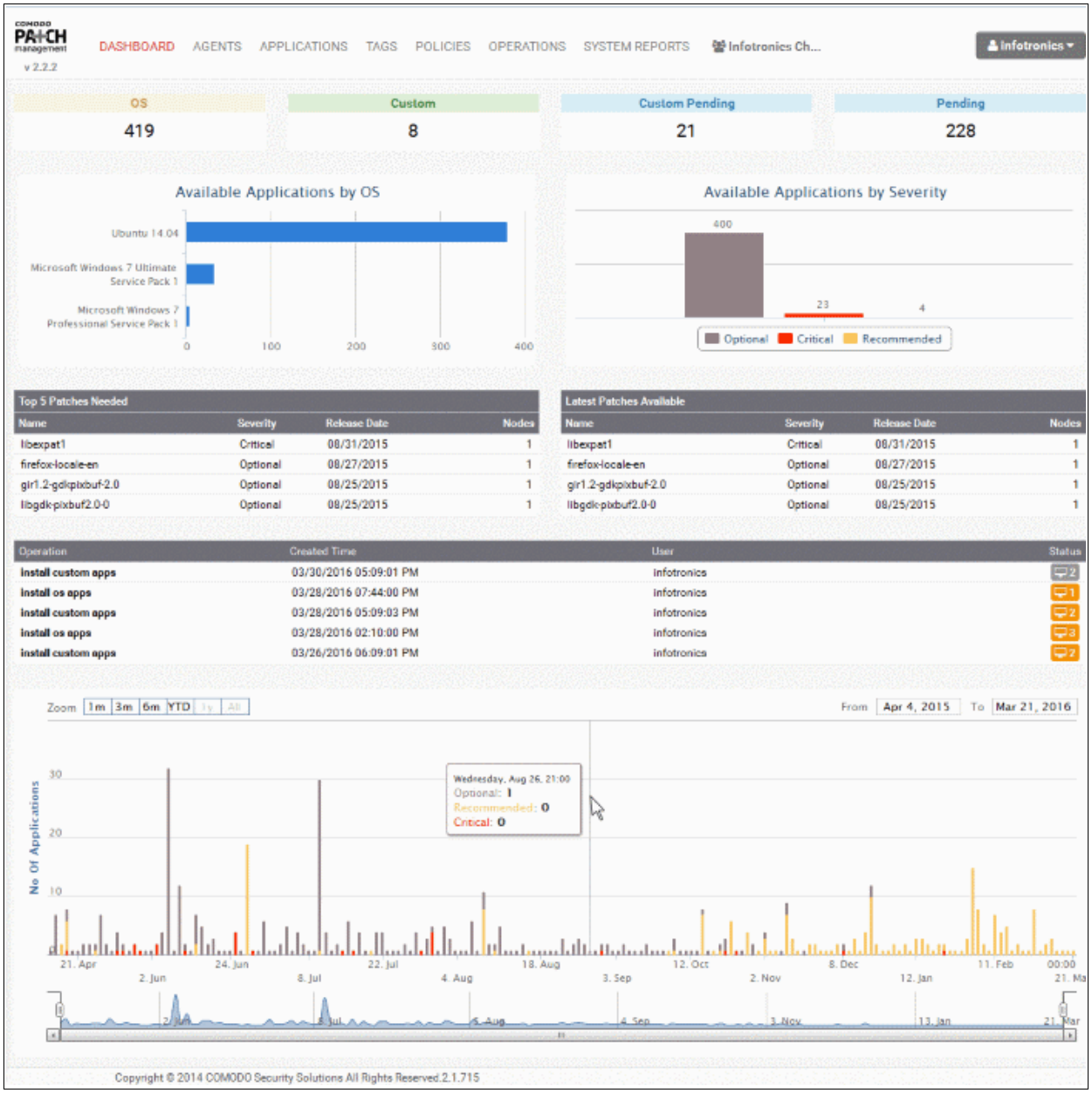


By default, the Patch Management 'Dashboard' screen will be displayed:

1.2.1 The Patch Management Administrative Console

The PM Administrative Console is an easy to use interface which allows administrators to view network-wide patch requirements, create endpoints groups, create polices and assign to endpoint group, view reports and more.





The Tabs

The administrative interface contains seven tabs that allow administrators to navigate to different configuration areas:

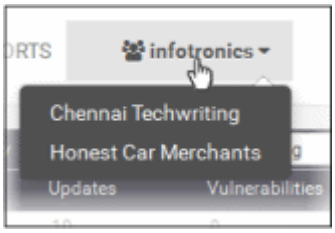
- **Dashboard** – Displays key statistics of the number of OS patches, OS updates and third-party applications available in the server and their installation status at the endpoints. Refer to the section **The Dashboard** for more details.
- **Agents** – Displays the list of endpoints enrolled by installing the patch management agent, for the selected customer account with their details. Clicking on an endpoint opens the Endpoint Details Interface that displays the detailed information of the endpoint and enables to remotely install missing OS patches/updates and third-party applications on to the selected endpoint. Refer to the section **Viewing and Managing Agents and Endpoints** for more details.
- **Applications** - Displays the list of OS patches and updates and custom third-party applications available in the patch management server. Clicking on an item opens the Applications Details Interface that displays the detailed information of the item and enables to remotely install the item on selected endpoints. Refer to the section **Managing OS Updates, Patches and Applications** for more details.
- **Tags** - Displays all current tags which can be assigned to endpoints. Clicking on a tag will display all

endpoints covered by the tag and allow administrators to remotely install any outstanding updates on them. Refer to the section **Adding Tags and Managing Endpoint Groups** for more details.

- **Policies** – Displays the list of policies created for automated and scheduled patch management operations configured to periodically run on selected endpoints or endpoint groups. The interface also allows administrators to create new policies for patch management. Refer to the section **Automated Patch Management Policies** for more details.
- **Operations** – Displays the list of manually initiated and scheduled patch management operations that were completed and currently running. Clicking on an item displays the details of the operation, including the items installed and endpoints affected. Refer to the section **Viewing Patch Management Operations** for more details.
- **System Reports** - Displays summaries of hardware/software/network details for each endpoint registered for the customer account. It also displays the patch management policies active for the customer and an exhaustive list of available OS patches and updates with details of endpoints affected by them. Refer to the section **Viewing Endpoint Report Summaries** for more details.

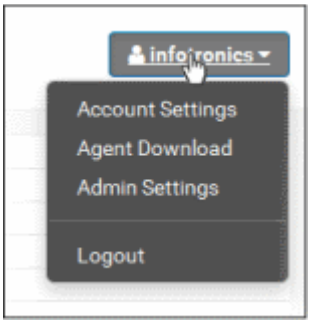
Customer Account

The customer account selected for the patch management operations is displayed at the right end of the title bar. Clicking the drop-down arrow enables the administrator to switch to different customer accounts for management.



Account Controls

The username of the currently logged-in administrative user is displayed at the top right of the patch management console interface. Clicking on the name displays a drop-down with options for administrative settings for the account, view the details of the currently logged-in administrator and to log out of the console.



- **Account Settings** – Displays the details of the currently logged in administrator such as their login name, email name and more. Refer to the section **Viewing Administrator Account Settings** for more details.
- **Agent Download** – Opens the agent download and installation instructions interface that contains download URLs for the setup files and installation instructions patch management agent. The patch management agent should be installed at each endpoint for remotely installing agents and applications. Refer to the section **Enrolling Endpoints by Installing the Agent** for more details.
- **Admin Settings** – Allows administrators to configure Syslog server settings, email settings and notifications settings. Refer to the section **Admin Management** for more details.

2 Enroll Endpoints by Installing the Agent

The patch management module requires a small software agent to be installed on each managed endpoint to facilitate communication with the console. The agent will provide constantly updated statistics about the endpoint to the console and is required for remote installation/uninstallation of patches and remote power operations.

Once the agent is installed, the endpoint is automatically discovered and enrolled by the patch management server. The administrator can then add tags to the endpoint, add it to endpoint groups, apply patch management policies, view hardware/software/network details and more.

Note - The customer account for which the endpoints are to be added, should be chosen from the 'Customer Account' drop-down prior to enrolling the endpoints. The agent installation parameters will be different for each customer account.

The following sections provide detailed explanations about downloading and installing the agent on to endpoints of different operating systems:

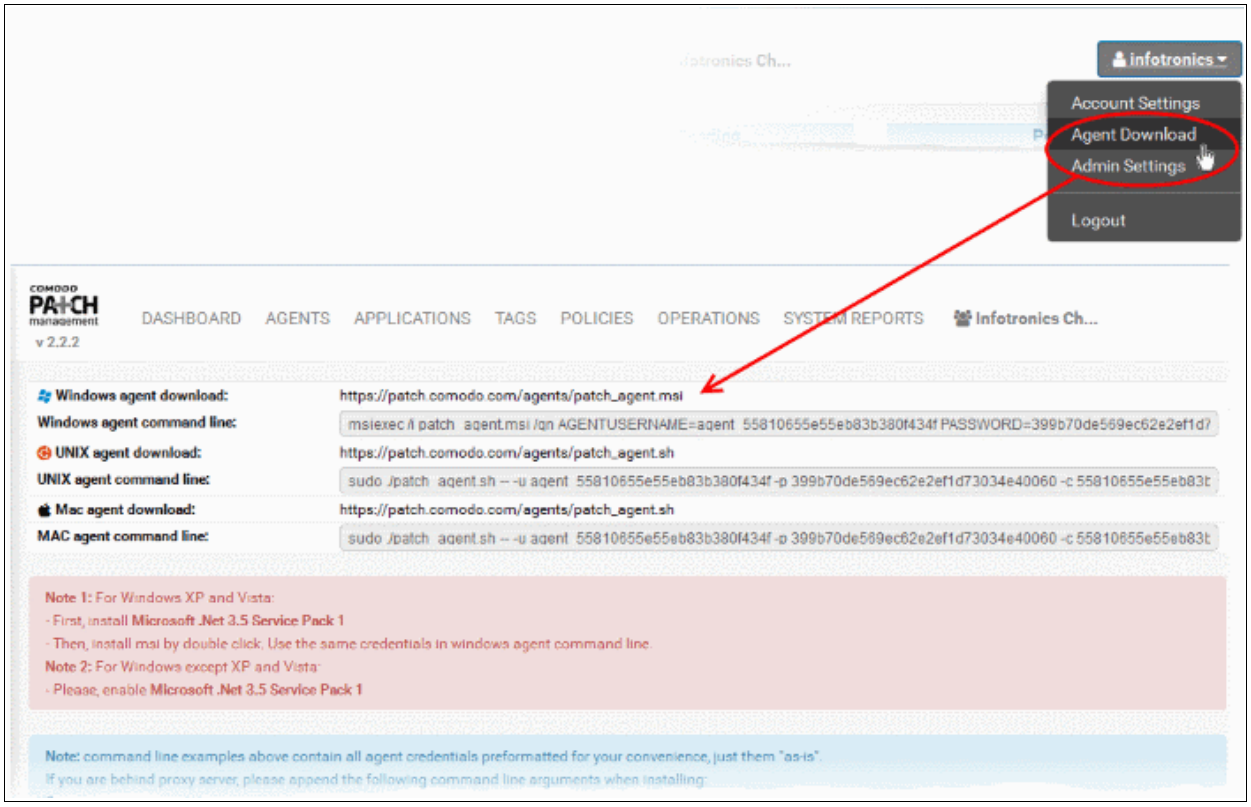
- **Downloading the Agent Installation Files**
- **Installing the agent on Windows endpoints**
- **Installing the agent on Linux endpoints**
- **Installing the agent on MAC endpoints**

Downloading the Agent Installation Files

The agent setup files for Windows, Linux and Mac endpoints can be downloaded from the administrative console.

To download the agent setup file

- Choose the customer account to which the endpoints are to be added from the 'Customer Account' drop-down
- Click on your login username at the top right and choose 'Agent Download'



The agent download page will open, with the download URLs of setup files and installation instructions.

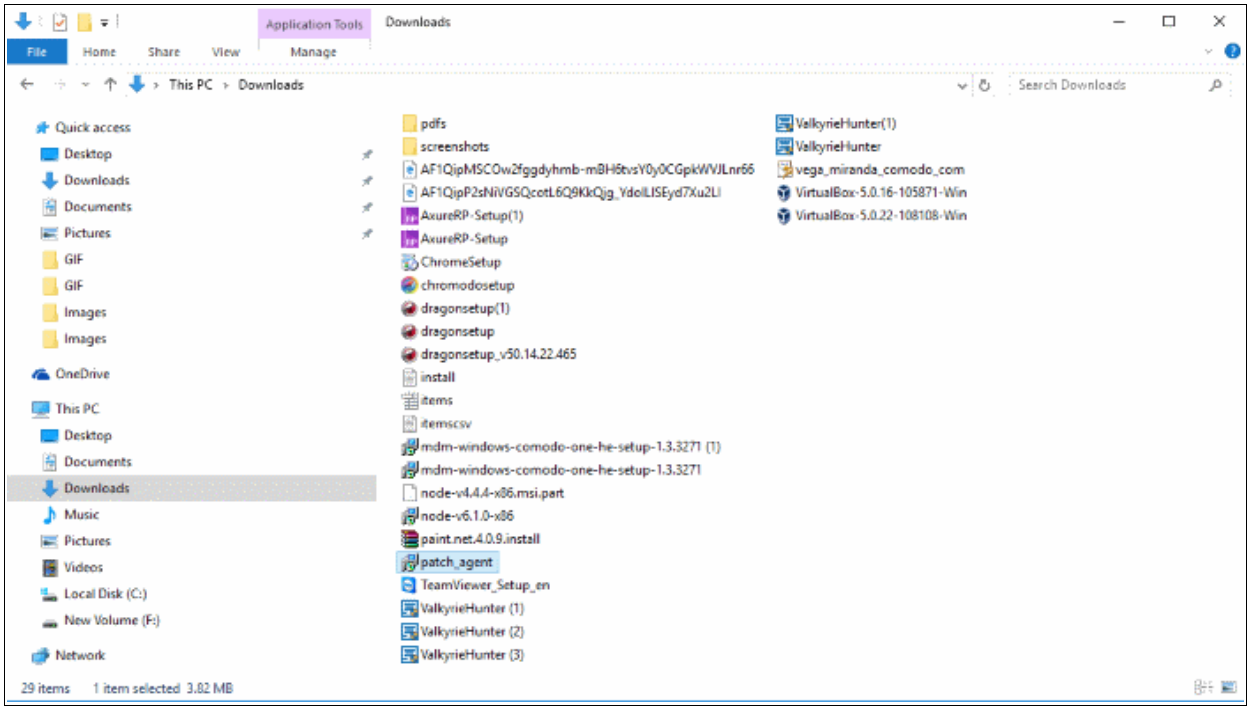
- **Windows agent download** - The URL for downloading the agent setup file for Windows endpoints. Copy the URL and paste to the address bar of any web browser to download the setup file and copy and save the setup file to the endpoint(s) to be enrolled.
- **Windows agent command line** - The execution command for silent installation of the agent at Windows endpoints. Copy and save the command line for execution at the endpoints for installing the agent. Please note if the administrator while installing the Remote Monitoring and Management (RMM) agent has opted for both RMM and Patch Management (PM), then the Windows endpoint will automatically report to the PM interface.
- **UNIX agent download** - The URL for downloading the agent setup file for Linux endpoints. Copy the URL and paste to the address bar of any web browser to download the setup file and copy and save the setup file to the endpoint(s) to be enrolled.
- **UNIX agent command line** - The execution command for silent installation of the agent at Linux endpoints. Copy and save the command line for execution at the endpoints for installing the agent at the background.
- **Mac agent download** - The URL for downloading the agent setup file for Mac endpoints. Copy the URL and paste to the address bar of any web browser to download the setup file and copy and save the setup file to the endpoint(s) to be enrolled.
- **MAC agent command line** - The execution command for silent installation of the agent at Mac endpoints. Copy and save the command line for execution at the endpoints for installing the agent at the background.

Installing the agent on Windows endpoints

Please run the setup file with administrative privileges. Installation will be carried out from the Windows command line interface.

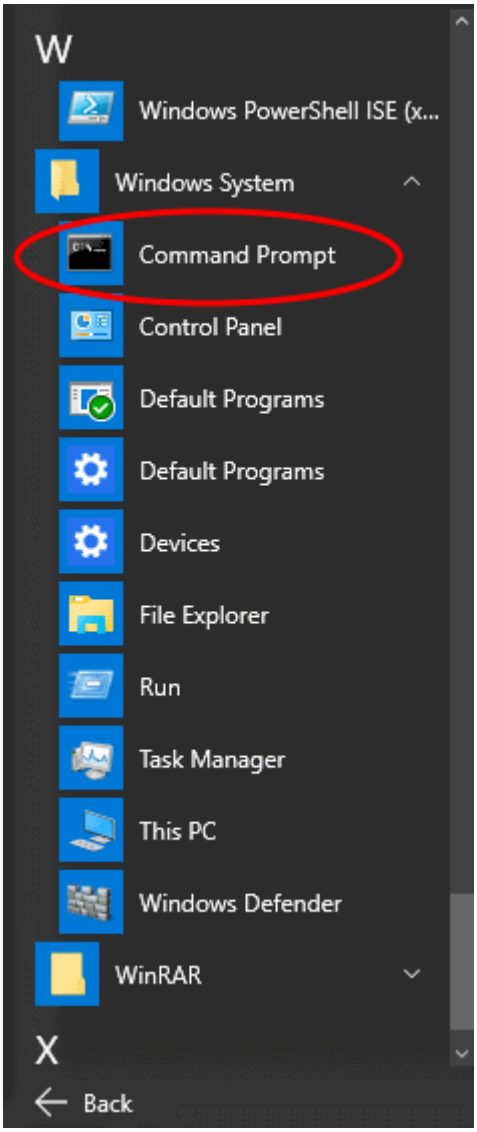
Step 1 – Transfer the agent installation file to the target endpoint.

- Copy the agent installation file to the prospective target endpoint through any means of file transfer like network file sharing or using removable storage media such as DVD, CD, USB memory and store it in an easily accessible location.



Step 2 – Open Windows Command Line Interface with administrative privileges

- Click Start > All Programs > Accessories
- Right click on 'Command Prompt' and choose 'Run as Administrator' from the context sensitive menu...



… and click 'Yes' in the confirmation dialog.

Step 3 – Execute the installation command for the silent execution.

- Navigate to the folder in which the agent setup file is saved, from the command line
- Enter the execution command for silent installation by pasting the command line copied from the 'Windows agent command line' field of the agent download page of the Patch Management Administrative Console.

The agent will be installed silently without displaying any alerts to the end-user. Upon completion of installation, the endpoint will be automatically discovered by the Patch Management server and enrolled for patch management under the specified customer account.

Note: For Windows Vista and previous versions please make sure that Microsoft.net Framework 3.5 SPI and Microsoft Framework 4.5.1 were installed on the machines before agent registration.

Installing the agent on Linux endpoints

The agent setup file is called 'patch_agent.sh' and can be found amongst the files extracted from the original .tar file. The agent should be copied to and installed on each target endpoint.

Step 1 – Transfer the agent installation file to the target endpoint.

- Copy the agent setup file downloaded from the agent download interface of the administrative console to

the prospective target endpoint through any means of file transfer like network file sharing or using removable storage media such as DVD, CD, USB memory and store it in an easily accessible location.

Step 2 - Open Ubuntu Terminal Prompt in root

- Open Ubuntu terminal window and enter the 'su' command and enter the super-admin password.
- Navigate to the location where the agent setup file is saved using the 'cd' command.

Step 3 – Executing installation command

- Enter the execution command for silent installation by pasting the command copied from the 'Unix agent command line' field of the agent download page of the Patch Management Administrative Console

After entering the command, a message, for example ' "Verifying archive integrity... Uncompressing C1Agent autoinstaller 2.1.734' will be displayed, which indicates that the agent has been successfully installed and is running.

Installing the agent on MAC endpoints

The agent setup file is called patch_agent.sh' and can be downloaded from PM server. The agent should be copied to and installed on each target endpoint.

Step 1 – Transfer the agent installation file to the target endpoint

- Copy the agent setup file downloaded from the agent download interface of the administrative console to the prospective target endpoint through any means of file transfer like network file sharing or using removable storage media such as DVD, CD, USB memory and store it in an easily accessible location.

Step 2 - Open MAC Terminal Prompt in root

- Open MAC terminal window and enter the 'su' command and enter the super-admin password.
- Navigate to the location where the agent setup file is saved using the 'cd' command.

Step 4 – Change access permission to agent setup file

- Apply 'chmod' command to agent setup file via terminal to allow access permission for setup file. Example : chmod 777 patch_agent.sh

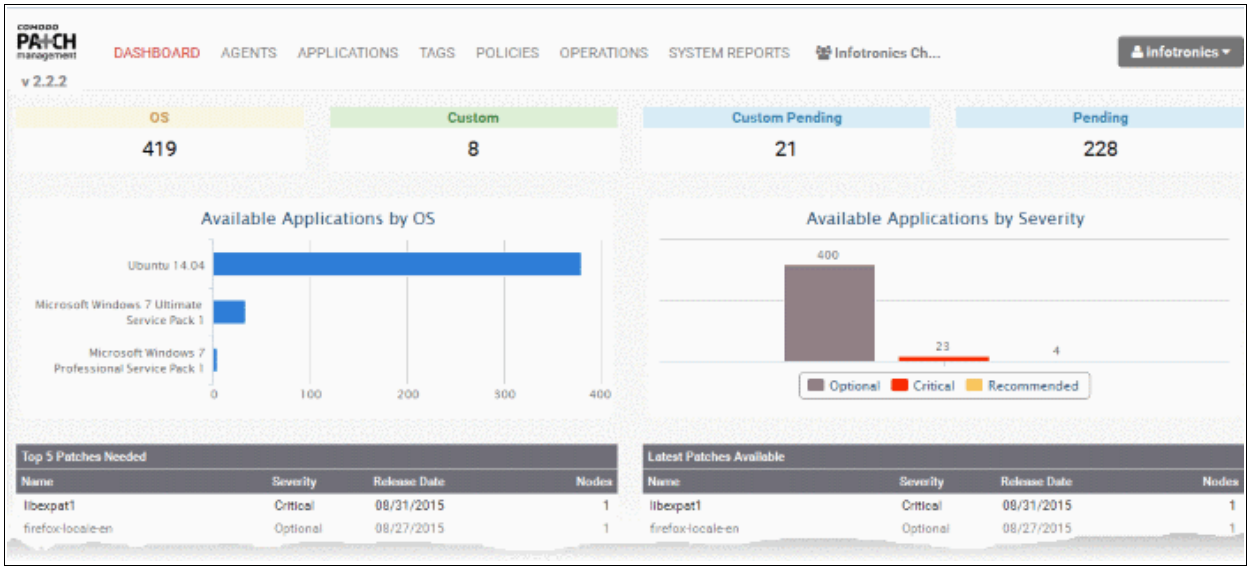
Step 3 – Executing installation command

- Enter the execution command for silent installation by pasting the command copied from the 'MAC agent command line' field of the agent download page of the Patch Management Administrative Console

After entering the command, a message, for example, ' "Verifying archive integrity... Uncompressing Comodo One Agent autoinstaller 3.0.0' will be displayed, which indicates that the agent has been successfully installed and is running.

3 The Dashboard

The patch management dashboard provides a easy to understand summary of key statistics and pending tasks. This includes the number of OS patches, OS updates and third-party applications available in the server and their installation status at the endpoints. The dashboard also displays a log of recent patch management operations and a upload history of packages to the patch management server.



The dashboard displays contains the following areas. Each area is explained in detail after the list.

- **Numerical Summary of OS patches/updates and custom/third-party applications available from the server for installation on to endpoints and numbers of that same, being currently installed**
- **Barcharts showing the numbers of available packages, breakdown with respect to their applicable OS versions and their severity levels**
- **Top 5 patches needed and top 5 latest patches available for installation**
- **A log of recent patch management operations**
- **A time-line chart showing the upload history of patches, updates and applications**

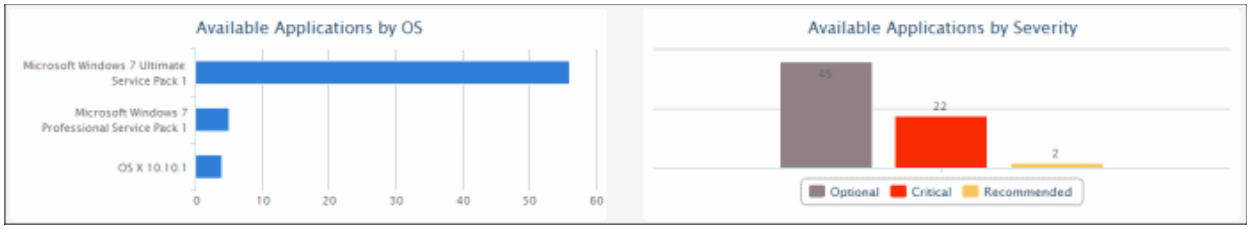
Available and Pending Packages

The first row of boxes show the numbers of available packages and currently installed packages.

- **OS** – The OS patches and updates that are available at the server and eligible for installation on to endpoints depending on their operating systems. Clicking the number takes you to 'Applications' interface with the 'OS' tab opened and applied with 'Available' filter that displays the items available under the category. Refer to the section **Managing OS Updates, Patches and Applications** for more details.
- **Custom** - The custom and third-party applications that are available at the server and eligible for installation on to endpoints depending on their operating systems. Clicking the number takes you to 'Applications' interface with the 'Custom' tab opened and applied with 'Available' filter that displays the items available under the category. Refer to the section **Managing OS Updates, Patches and Applications** for more details.
- **Custom Pending** - The custom and third-party applications whose installation on to endpoints has been initiated and currently in progress. Clicking the number takes you to 'Applications' interface with the 'Custom' tab opened and applied with 'Pending' filter, that displays the items being currently installed. Refer to the section **Managing OS Updates, Patches and Applications** for more details.
- **Pending** - The OS patches and updates whose installation on to endpoints has been initiated and currently in progress. Clicking the number takes you to 'Applications' interface with the OS tab opened and applied with 'Pending' filter, displaying the items being currently installed. Refer to the section **Managing OS Updates, Patches and Applications** for more details.

Bar Charts

The dashboard displays bar charts to show an at-a-glance summary of the numbers of patches, updates and applications, sorted based on OS versions to which they can be applied and their severity level.



Hovering the mouse cursor over the bars displays the number of applications that fall under the selected category.

Top 5 and Latest Patches

The 'Top 5 Patches Needed' table displays a list of top 5 OS patches and updates ranked based on number of endpoints upon which they can be installed.

Top 5 Patches Needed

Name	Severity	Release Date	Nodes
Definition Update for Windows Defender -...	Optional	08/28/2015	1
Digital Camera RAW Compatibility Update	Optional	08/17/2015	1
iTunes	Optional	08/13/2015	1
Update for Windows 7 for x64-based Syst...	Optional	08/04/2015	1
Security Update for Windows 7 (KB30799...	Critical	07/20/2015	1

The 'Latest Patches Available' table displays a list of top 5 latest OS patches and updates available at the server, ranked based on their release dates

Latest Patches Available

Name	Severity	Release Date	Nodes
Definition Update for Windows Defender -...	Optional	08/28/2015	91
Digital Camera RAW Compatibility Update	Optional	08/17/2015	2
iTunes	Optional	08/13/2015	3
Update for Windows 7 for x64-based Syst...	Optional	08/04/2015	305
Upgrade to Windows 10 Pro	Optional	07/23/2015	0

The tables display the severity level, release date and number of eligible endpoints for each item.

Clicking on any item in the table opens the 'Applications' interface displaying the complete details of the item, which also allows the administrator to install the item to selected endpoints. For more details on the Application Details interface, refer to the section **Viewing Details of a Patch, Update Package or an Application**.

Recent Log of Patch Management Operations

The logs area displays the list of recent patch management, application installation and power management activities remotely carried out by the patch management module on the endpoint.

Logs table - Column Descriptions	
Column	**Description**
Operation	The name of the manual or scheduled job executed.
Created Time	Precise date and time at which the command was sent to the endpoint.
User	The administrative user that initiated/created the job.
Status	The running/completion status of the job. The number in the status indicates the number of applications installed/updated. 2 - The job(s) was/were successfully executed. 3 - The job(s) is/are under progress 1 - The job execution failed. 3 - Indicates the number of jobs that are yet to be processed by the PM agent.

Clicking on a log entry opens the Operations interface with the selected operation page selected. The Operations interface displays granular details of the operations executed. For more details on the Operations interface, refer to the section **Viewing Patch Management Operations**.

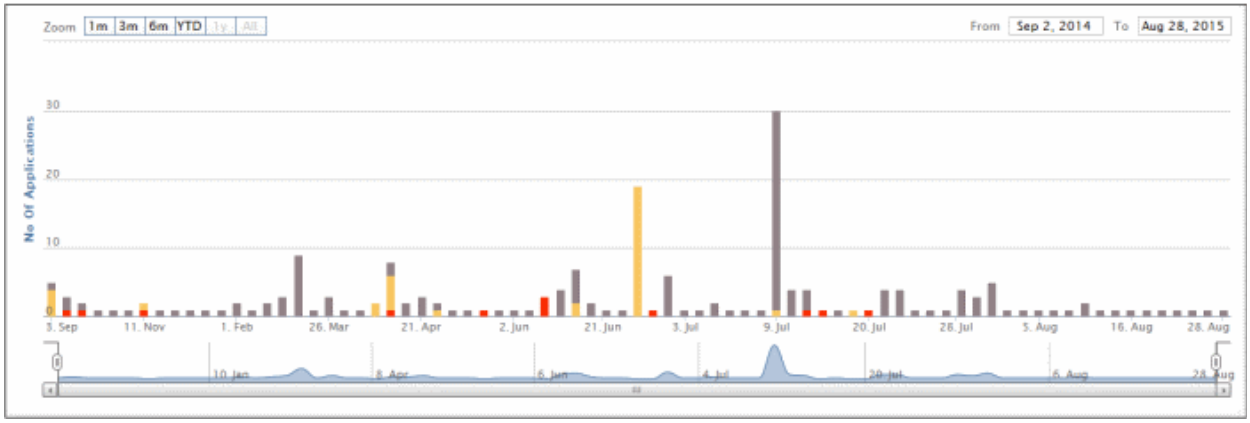
Upload History

The dashboard displays a time-line chart showing the history of patches, updates and applications uploaded to the patch management server. The bars are color coded to indicate the numbers of items of different severity levels.

Red - Indicates the number of items of 'Critical' severity uploaded on that day

Yellow - Indicates the number of items of 'Recommended' severity uploaded on that day

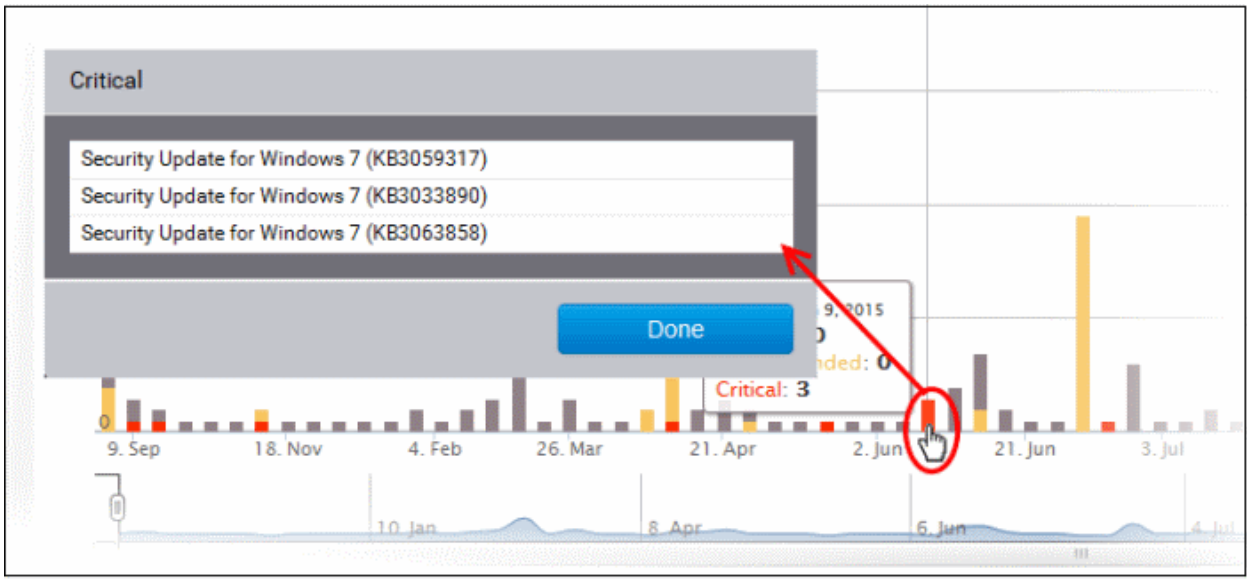
Gray - Indicates the number of optional items uploaded on that day



The chart can be re-scaled to display the history for selected period by choosing the preset period options at the top left and further customized using the slider pointers at the bottom.

Hovering the mouse cursor over a bar displays the number of items uploaded on the selected day.

Clicking on a specific colored portion of the bar displays the list of items falling under the severity level, uploaded on that day.



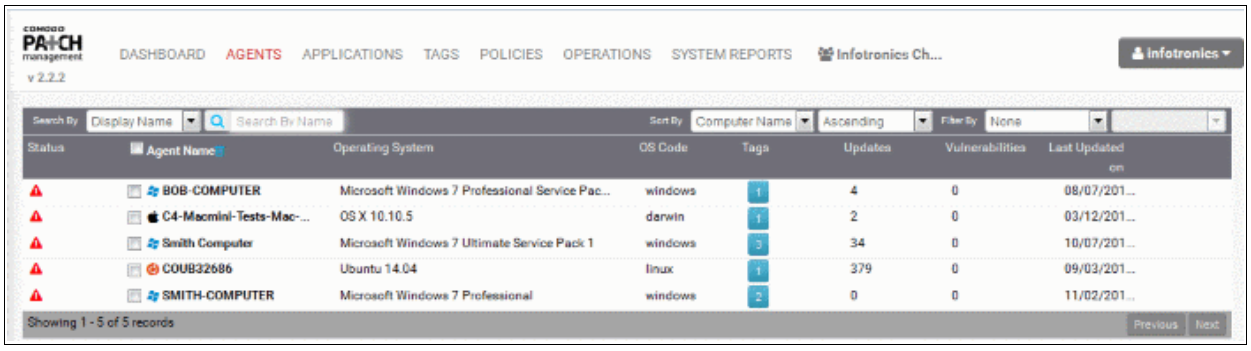
Clicking on an item name opens the 'Applications' interface displaying the complete details of the item, which also allows the administrator to install the item to selected endpoints. For more details on the Application Details interface, refer to the section **Viewing Details of a Patch, Update Package or an Application**.

4 View and Manage Agents and Endpoints

The Agents interface summarizes key information about endpoints that have the agent installed and which belong to the selected customer account.

Administrators can use this interface to view endpoint details, remove an endpoint, transfer endpoints among customers, initiate remote updates, apply patches and install applications.

Clicking on any row will open a detailed properties page which contains important status and activity information about the endpoint.



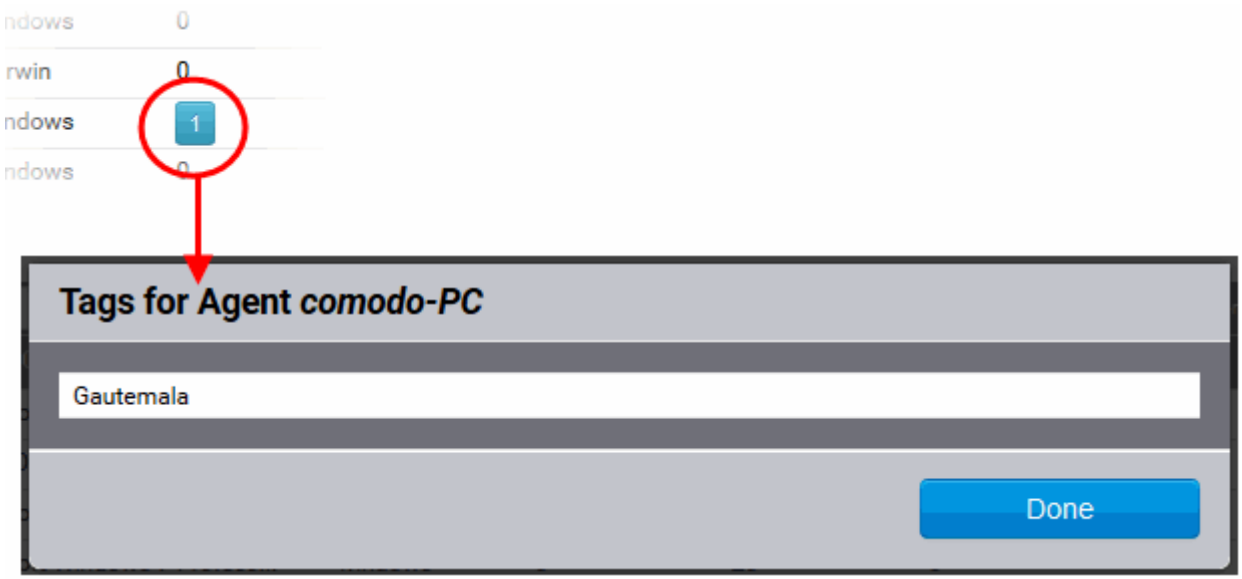
Agents table - Column Descriptions	
Column	**Description**
Status	Indicates the running status of the agent on the endpoint ✔ - PM Agent is installed and responding correctly ⚠ - PM Agent not responding. Endpoint may be down or agent not reachable

	⚠ - Endpoint needs to be restarted to apply patches and updates
Agent Name	The 'Display name' of the endpoint on which the PM agent is installed. If a display name is not assigned for the endpoint, its host name is displayed. Refer to the explanation under **Computer Details** in the section **Viewing Endpoint Details** for more details on assigning the display names.
Operating System	The version of the operating system on the endpoint
OS Code	The base code of the operating system
Tags	Displays the number of tags assigned to the endpoint. Clicking on the number displays the tags that represent the groups to which the endpoint is a member. Refer to the explanation under '**Identifying the Groups of an Endpoint**' for more details. **Background Note**: Tags are labels used to reference groups of endpoint agents. Applying an action to a tag will apply the action to all endpoints with that tag. For example, tags can be selected as a target for any policies you deploy in the 'Policies' area. This can save time by allowing you to accurately deploy updates to many endpoints simultaneously. Ideally, you should create multiple tags to cover attributes like operating system and department then apply them to particular endpoints/agents as required. For example, you could create and apply tags called 'Windows XP', 'Windows 7', 'Windows Vista', 'Sales Department', 'IT department', 'DMZ Machines' and 'Accounts' department'. For more details on creating new tags and applying them to the endpoints, refer to the section **Adding Tags and Managing Endpoint Groups**.
Updates	Indicates the number of recommended OS updates for the endpoint
Vulnerabilities	Indicates the number of security threats identified at the endpoints, which can be cleared by applying OS updates that are recommended for the endpoint
Last Updated on	The date and time of the most recent update operation on the endpoint.

Identifying the Groups of an Endpoint

The 'Tags' column displays the number of groups to which the endpoint is added as a member for group management. Refer to the section **Managing Endpoint Groups** for more details on groups.

- To view the group names, click on the number as shown below.



Sorting and Searching Options

Sorting the Entries

You can sort the entries in the ascending or descending order of different criteria like host names and display names, last update period and so on.

- Select the criteria from the 'Sort by' drop-down. The available options are:

Criteria	Sorts the entries based on...
Computer Name	the host names of the endpoints
Display Name	the display names of the endpoints
OS Code	the base code of the operating systems at the endpoints
OS String	the version of operating system at the endpoints
Agent Status	the running status of the agent at the endpoints
Last Updated	the date/time of the last update carried out at the endpoints

- Choose whether the entries are to be sorted on ascending or descending order of the selected criteria from the next drop-down

Filtering the Entries

You can filter the entries based on different criteria like Operating Systems, agent status and more.

- Select the criteria from the 'Filter by' drop-down. The available options are:

Criteria	Filters the entries based on...
None	No filter will be applied.
OS Code	the base code of the operating systems chosen from the next drop-down.
OS String	the version of operating system chosen from the next drop-down.
Agent Status	the running status of the agent chosen from the next drop-down.
Production Level	the purpose of the endpoints based on which they are grouped, chosen from the next drop-down. Refer to the explanation under **Production State** in the next section **Viewing Endpoint Details** for more details.

Searching the Endpoints

You can search for specific endpoint(s) by entering their host name, IP address or MAC address as search criteria.

- Choose the criteria from the 'Search by' drop-down. The available options are:

Criteria	Parameter Required
Display Name	Enter the Display name of the endpoint in part or full in the search text box
IP Address	Enter the IP Address of the endpoint
MAC Address	Enter the physical address of the endpoint without colons or dashes between the digits (Example: 0A1BC2D3E4F5)

The interface allows the administrator to:

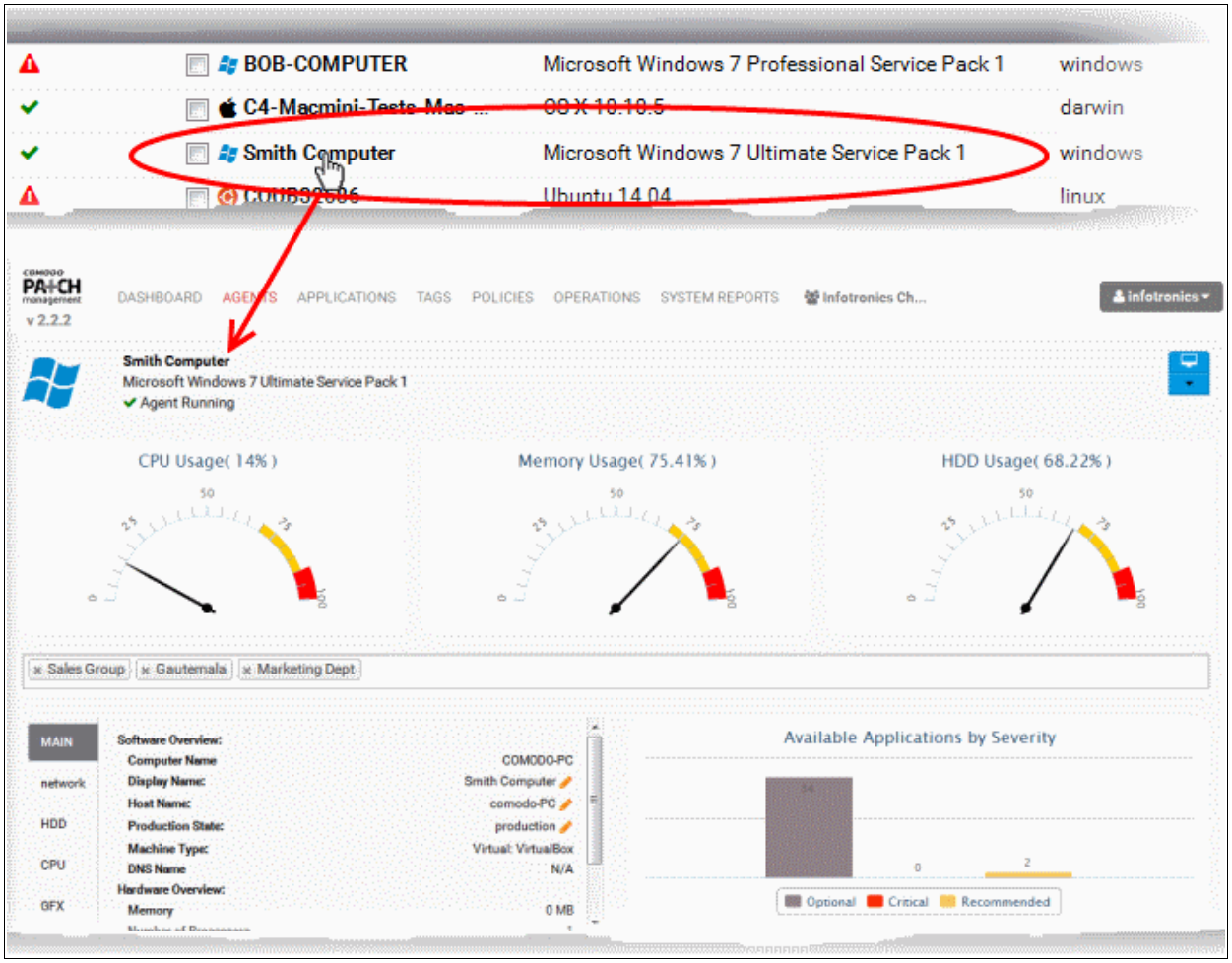
- **View details of an endpoint**
- **Initiate manual update or patch/application installation operation**

- **Remove selected endpoint(s)**

4.1 View Endpoint Details

Clicking on any endpoint listed in the 'Agents' area will open detailed information about the selected endpoint. This includes hardware usage, endpoint tags, software/hardware/network details and a summary of updates that are available for the endpoint. Administrators can also use this interface to remotely restart or shutdown the endpoint, view logs of previous operations and to manually install/uninstall applications and patches.

To view endpoint details, click anywhere in the row of selected endpoint. The Endpoint Details screen will be displayed:



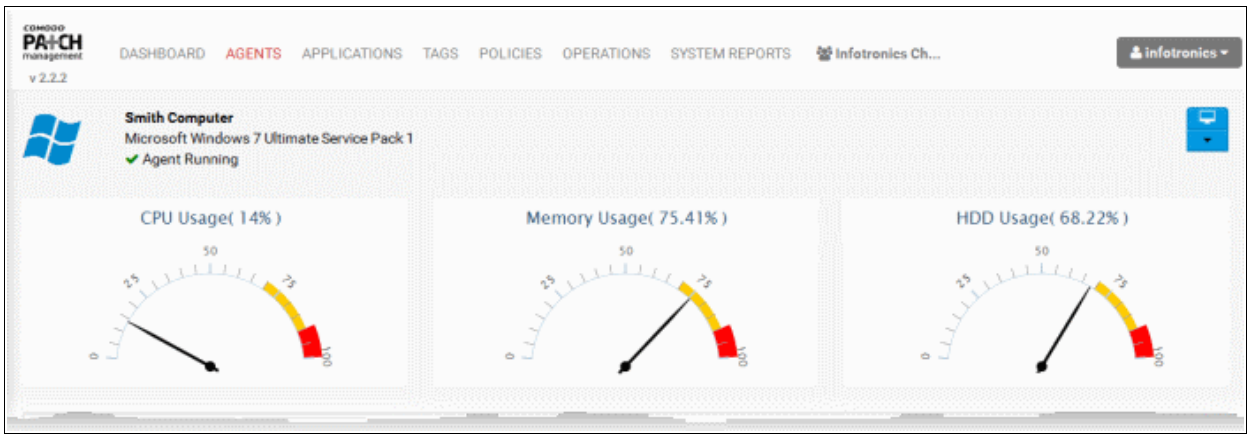
The interface contains the following areas. Each area is explained in detail after the list.

- **A graphical snapshot summary of the OS and current hardware resource usage details. You can shutdown/restart the endpoint or remove the endpoint from this area.**
- **The groups to which the endpoint is added by application of tags. Also, you can add the endpoint to different groups and remove the membership from a selected group**
- **The OS, Software/Hardware/Network Details**
- **Graphical Summaries of patches and applications available at the server for installation on to the endpoint**
- **Log of Recent Patch Management Operations**
- **List of OS updates, patches and third-party applications installed on the endpoint and the lists of OS patches and custom third-party applications that are available for installation at the endpoint by**

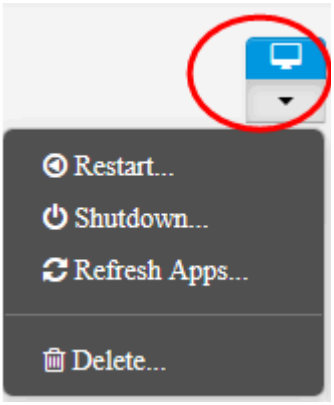
the patch management module. You can uninstall a patc

Endpoint Statistics Summary

The upper area of the computer details interface displays the hostname or display name of the computer, the version of the Operating System, the agent running status. The current hardware resource usage statistics like CPU usage, physical system memory usage and the hard disk space are indicated in the respective dials.



The drop-down at the top right allows the administrator to remotely restart/shutdown the endpoint or remove the endpoint from the patch management module.

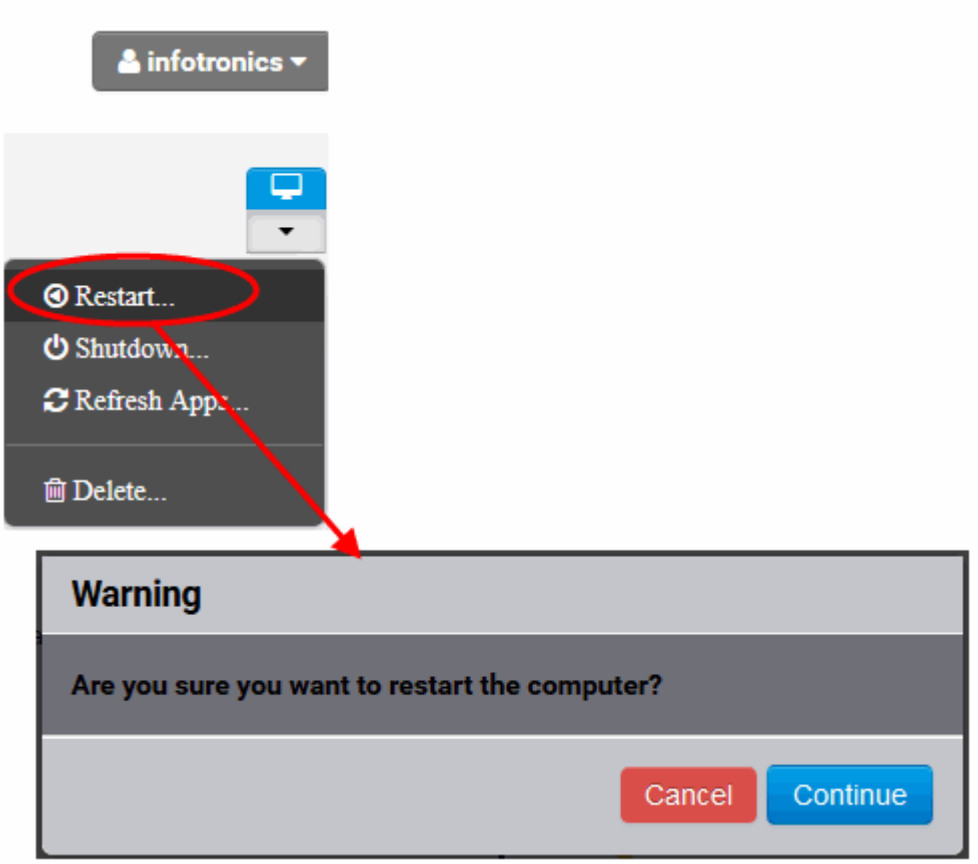


- **Restart** – Reboots the computer with a delay of one minute after confirmation.
- **Shutdown** – Shuts down the endpoint computer after confirmation.
- **Refresh Apps** – The patch management module re-polls the agent and shows the latest resource usage statistics and software inventory details
- **Delete** – Uninstalls the patch management agent from the endpoint and removes the end point computer from the patch management module, after confirmation.

Warning: Once an endpoint is removed, the agent will be automatically uninstalled from the endpoint and all the details pertaining to the endpoint will be deleted from the server. If the endpoint needs to be re-enrolled to the patch management module, the agent should be reinstalled and the endpoint will be added as a new endpoint to the patch management system.

To remotely restart the endpoint

- Open the endpoint properties interface for the selected endpoint by clicking on it from the Agents interface.
- Click the drop-down at the top right and choose 'Restart'. A confirmation dialog will appear.

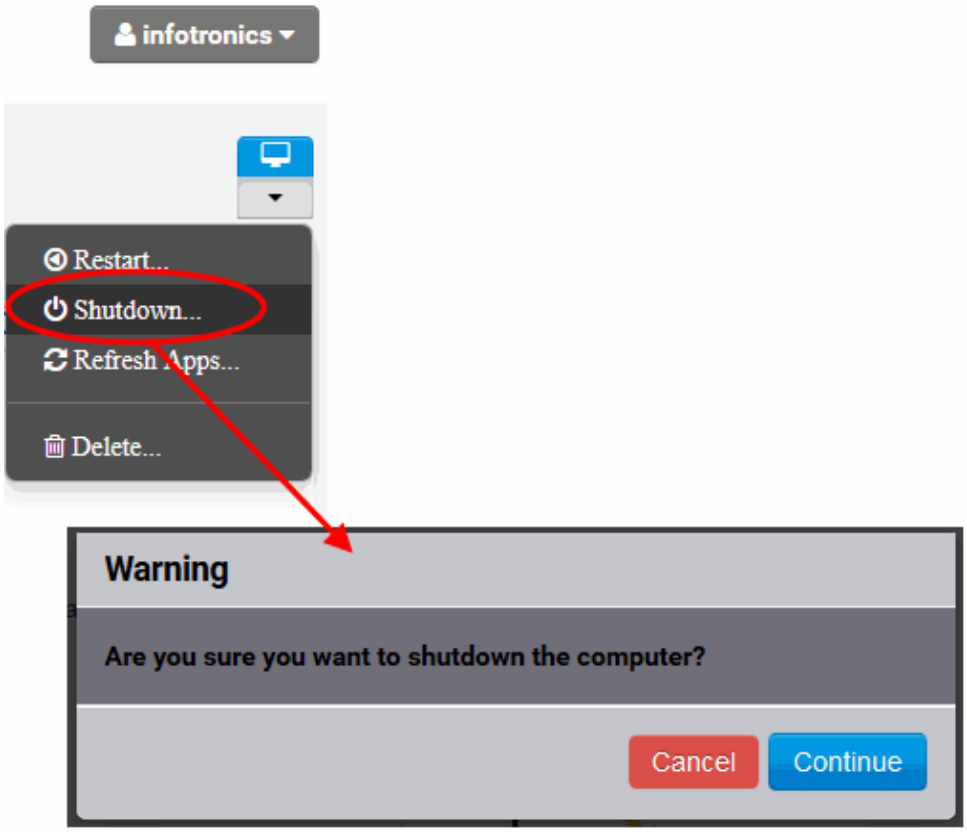


- Click 'Continue' in the confirmation dialog.

A message will be displayed to the end-user at the endpoint and the endpoint will be restarted after 60 seconds.

To remotely shutdown an endpoint

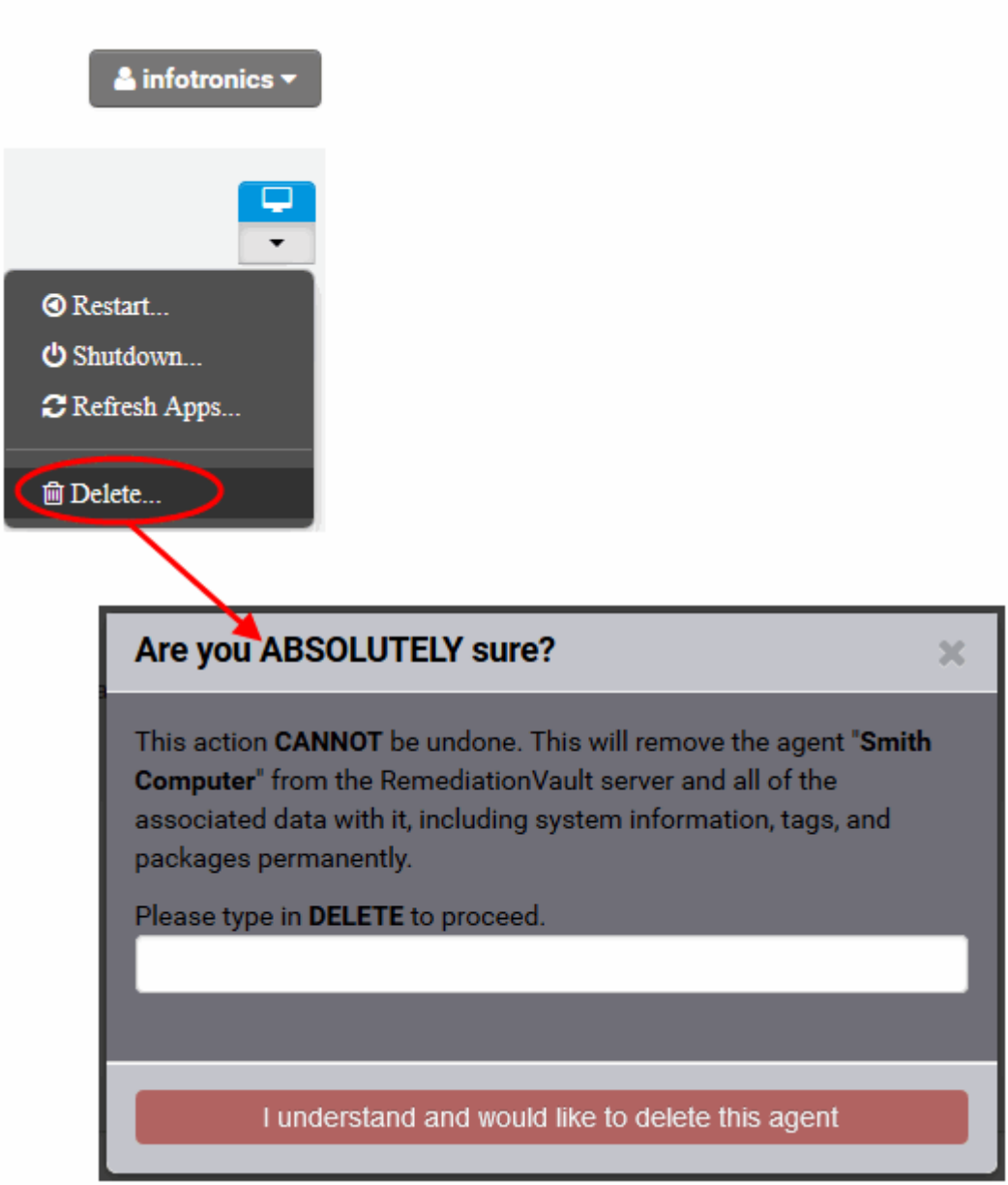
- Open the endpoint properties interface for the selected endpoint by clicking on it from the 'Agents' interface.
- Click the drop-down at the top right and choose 'Shutdown'. A confirmation dialog will appear.



- Click 'Continue'. The endpoint will be shutdown immediately.

To remove an endpoint from the patch management module

- Open the endpoint properties interface for the selected endpoint by clicking on it from the 'Agents' interface.
- Click the drop-down at the top right and choose 'Delete'. A confirmation dialog will appear.

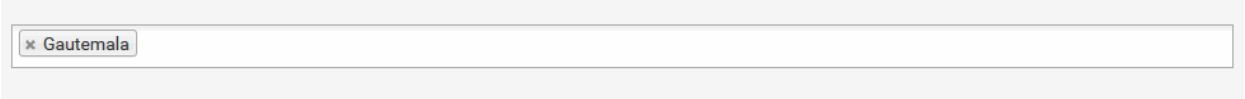


- If you are sure on removing the endpoint, type “DELETE” in the text box and click 'I understand and would like to delete this agent'

The agent will be uninstalled from the endpoint and the endpoint will be removed from the patch management module.

Tag Details

The text box below the graphs displays the tags that are applied to the endpoint.



Background Note: Tags are labels used to reference groups of endpoint agents. Applying an action to a tag will apply the action to all endpoints with that tag. For example, tags can be selected as a target for any policies you deploy in the ‘Policies’ area. This can save time by allowing you to accurately deploy updates to many endpoints simultaneously. Ideally, you should create multiple tags to cover attributes like operating system and department then apply them to particular endpoints/agents as required. For example, you could create and apply tags called

'Windows XP', 'Windows 7', 'Windows Vista', 'Sales Department', 'IT department', 'DMZ Machines' and 'Accounts' department'. For more details on creating new tags and applying them to the endpoints, refer to the section **Adding Tags and Managing Endpoint Groups**.

The administrator can add the endpoint to new groups or remove the membership from the existing groups. For more details on creating and managing endpoint groups, refer to the section **Adding Tags and Managing Endpoint Groups**.

To add a new tag to the endpoint

- Click inside the tags text box
- A drop-down with the list of tags existing with the customer account will be displayed

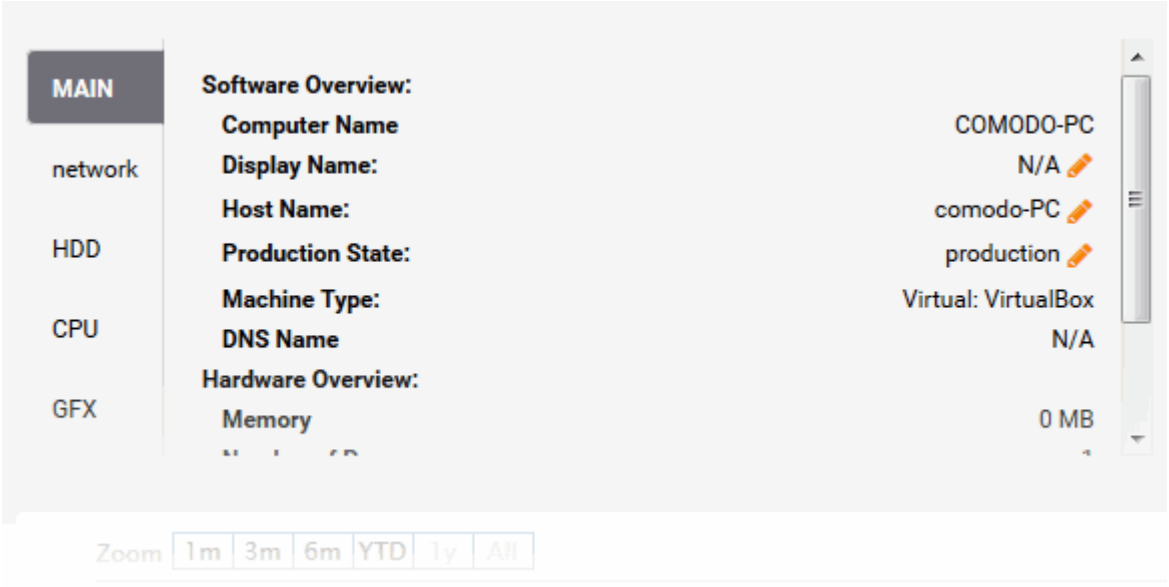
- Choose the tag for adding the endpoint to it

To remove the endpoint from a group

- Click the 'X' mark at the left of the tag name

Computer Details

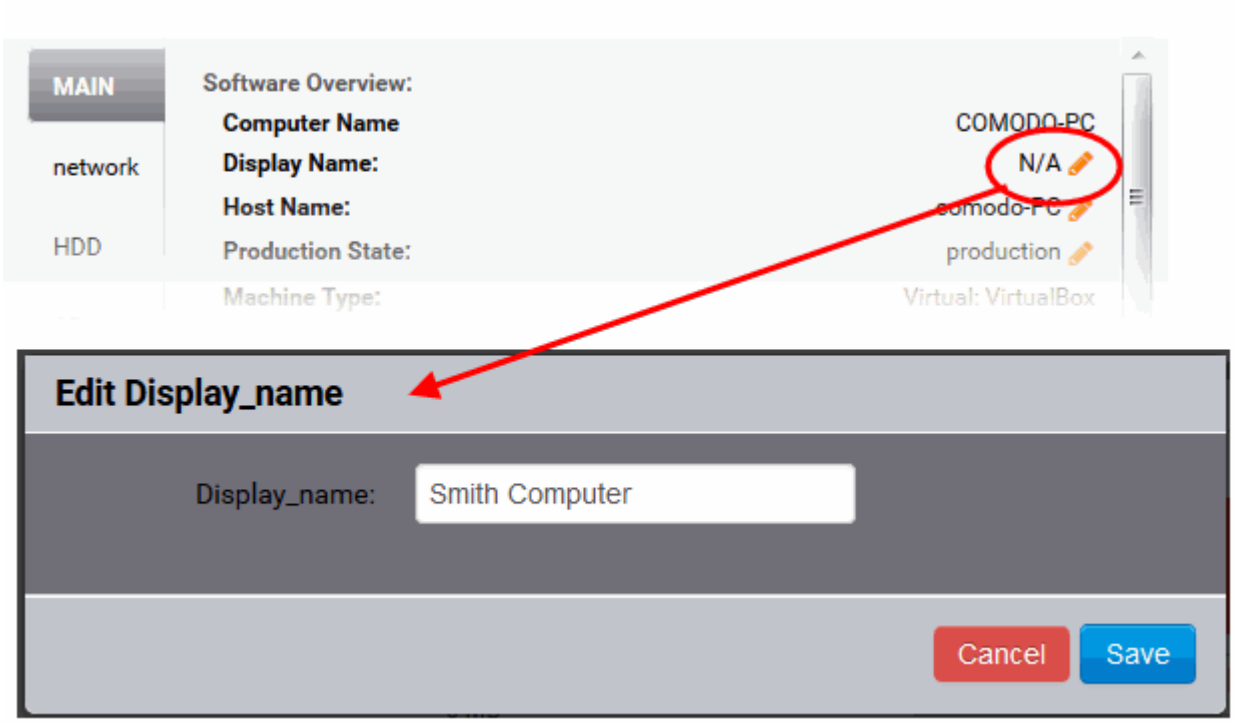
The Computer Details area provides the details on Software/Hardware overview, network details, Hard disk, CPU and Graphics Card details of the endpoint in separate tabs. The Computer Details area also allows the administrator to edit the display name, Host Name and production level of the endpoint.



Tab	Details Displayed
Main	An overview of software and hardware details of the endpoint like the computer name, display name, hostname and more. This tab also allows the user to edit the following details: • Display Name – The name by which the endpoint is displayed in the patch management module • Host Name – The name by which the endpoint is identified in the network • Production State – The purpose (like production, testing, training, network server, web server etc.) for which the endpoint is utilized in the network. By default, the 'Production State' for any newly added endpoint is set as 'production'. The administrator can specify the purpose by editing the value. Setting the 'Production State' is useful for grouping the computers based in their purpose and filtering them in different interfaces. Refer to the explanation **below** for more details.
Network	The IP Address, MAC Address of the endpoint and the network to which the endpoint is connected
HDD	The details like partitions, size and free space of the hard disk drive mounted on the endpoint
CPU	The details of the central processing unit (CPU), like the model, speed and number of processing cores
GFX	The speed and memory size of the graphics processor mounted on the endpoint

To change the name by which the endpoint is displayed in the patch management module interface

- Click the pencil icon beside Display Name



The 'Edit Display Name' dialog will appear.

- Enter the new name for the endpoint in the 'Display Name' text box and click 'Save'

The endpoint will be displayed with the new name in the Patch Management console interface.

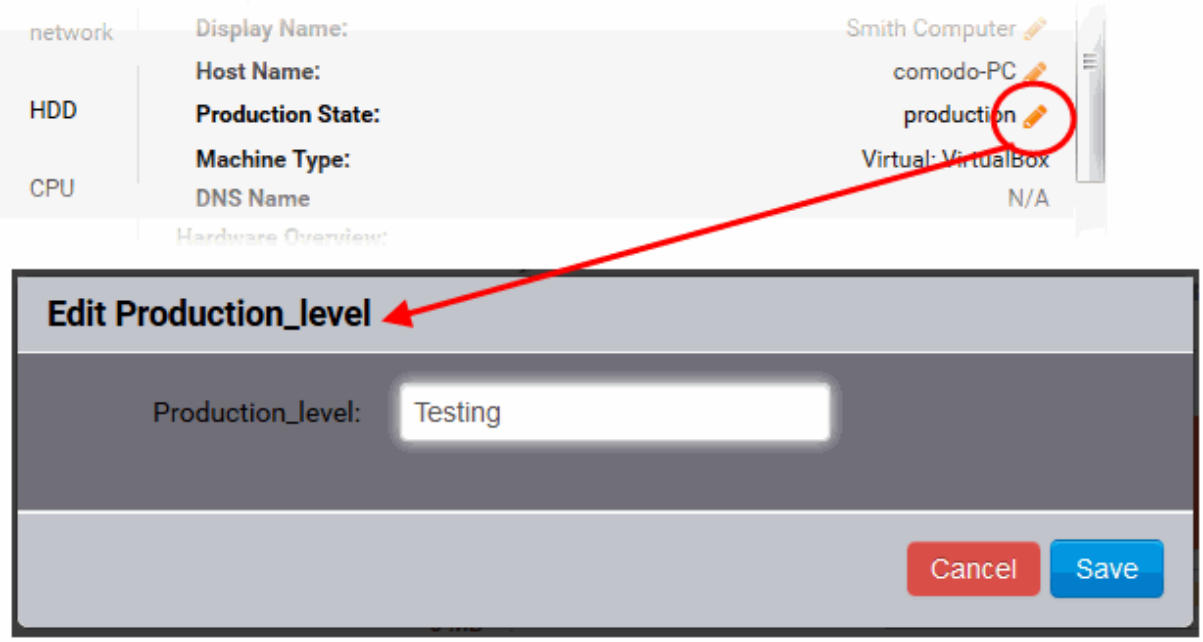
To change the host name of the endpoint

- Click the pencil icon beside 'Host Name'. The 'Edit Hostname' dialog will appear.
- Enter the new host name for the endpoint in the 'Hostname' text box and click 'Save'.

The host name of the endpoint will be updated immediately.

To change the production state of the endpoint

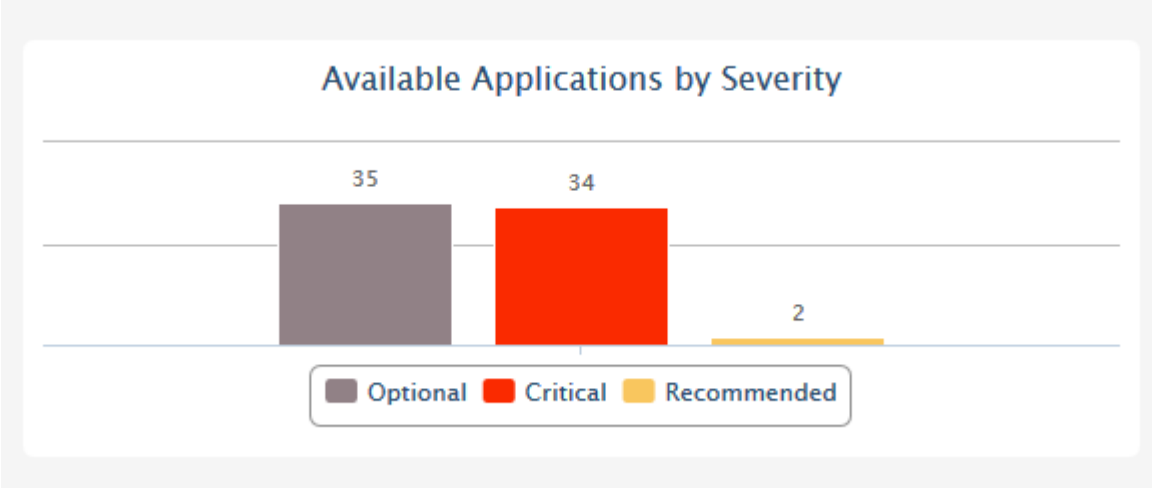
- Click the pencil icon beside 'Production State'. The 'Edit Production Level' dialog will appear.
- Enter the new purpose of the endpoint and click Edit.



The production state of the endpoint will be updated immediately.

Graphical Summary of Available Applications

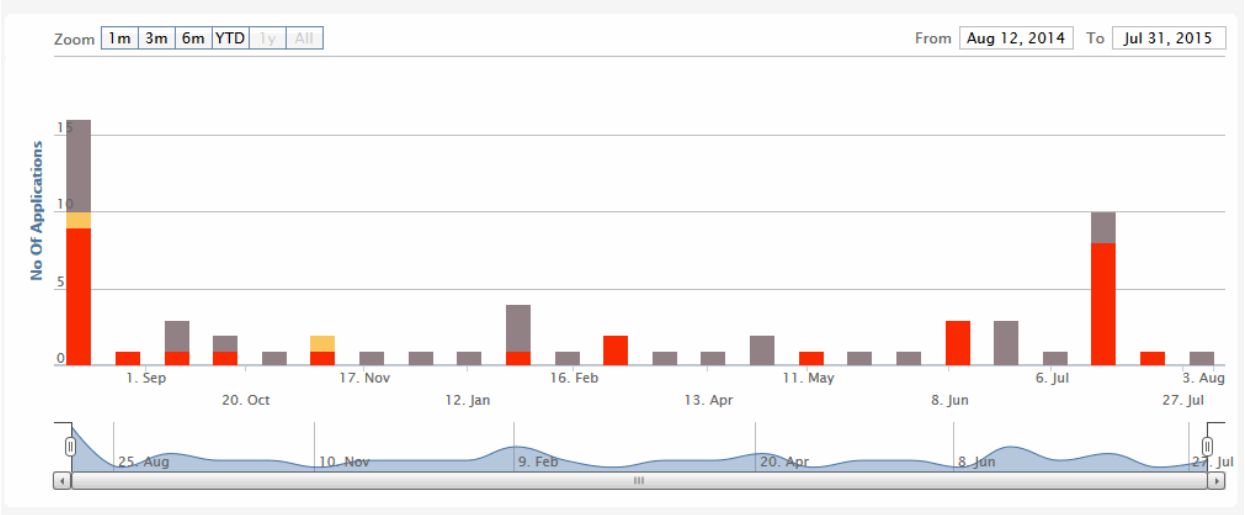
The Endpoint Details interface displays the statistics of OS patches, updates and third-party applications that are available in the patch management server and are eligible for installation onto the endpoint as a bar chart based on their severity.



Hovering the mouse cursor over the bars displays the number of applications that fall under the selected severity level.

The administrator can also view a time-line chart showing the upload history of patches, updates and applications that are eligible for the endpoint. The bars are color coded to indicate the numbers of items of different severity levels.

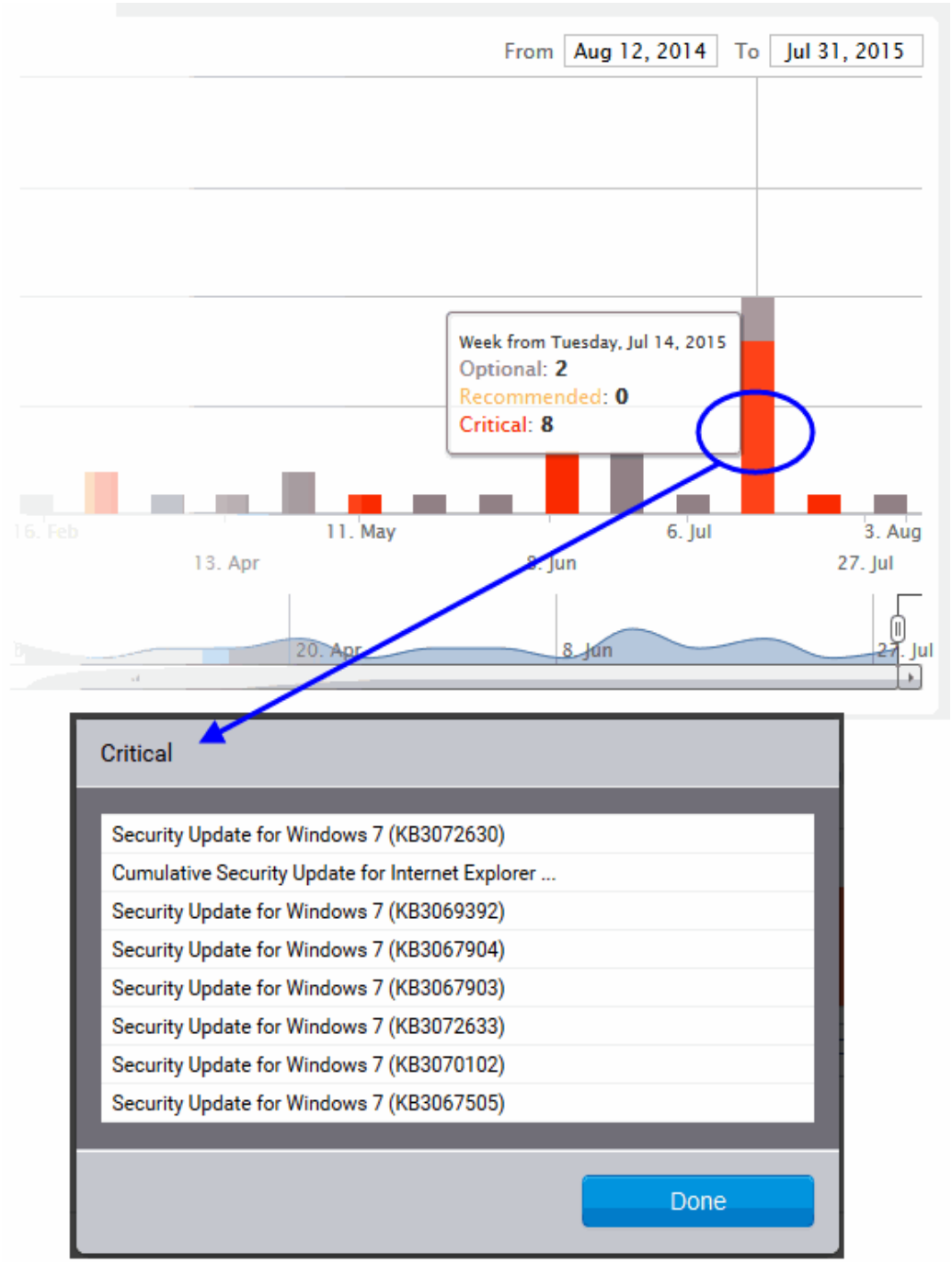
Red	-	Indicates the number of items of 'Critical' severity uploaded on that day.
Yellow	-	Indicates the number of items of 'Recommended' severity uploaded on that day.
Gray	-	Indicates the number of optional items uploaded on that day.



The chart can be re-scaled to display the history for selected period by choosing the preset period options at the top left and further customized using the slider pointers at the bottom.

Hovering the mouse cursor over a bar displays the number of items uploaded on the selected day.

Clicking on a specific colored portion of the bar displays the list of items falling under the severity level, uploaded on that day.



Clicking on an item name opens the 'Applications' interface displaying the complete details of the item, which also allows the administrator to install the item to selected endpoints. For more details on the Application Details interface, refer to the section **Viewing Details of a Patch, Update Package or an Application**.

Recent Log of Patch Management Operations

The logs area displays the list of recent patch management, application installation and power management activities remotely carried out by the patch management module on the endpoint.

Logs table - Column Descriptions	
Column	**Description**
Operation	The name of the manual or scheduled job executed.
Created Time	Precise date and time at which the command was sent to the endpoint.
User	The administrative user that initiated/created the job.

Status	The running/completion status of the job. The number in the status indicates the number of applications installed/updated.  - The job(s) was/were successfully executed.  - The job(s) is/are under progress  - The job execution failed.  - Indicates the number of jobs that are yet to be processed by the PM agent.

Clicking on a log entry opens the Operations interface with the selected operation page selected. The Operations interface displays granular details of the operations executed. For more details on the Operations interface, refer to the section **Viewing Patch Management Operations**.

The Inventory

The inventory list at the bottom of the interface displays:

- The list of OS update packages, patches and third-party applications that have been installed at the endpoint
- The lists of OS updates, security patches and custom third-party applications that are available in the server and eligible for installation on to the endpoint.

The administrator can initiate a manual patch management or remote application installation/uninstallation operation from this area. For more details on remote patch management or application installation, refer to the section **Initiating Manual Update or Installation Operation**.

The inventory area contains three tabs:

- **Software Inventory** – Displays the list of OS updates and service packs and third-party applications that have been installed at the endpoint. The number at the tab indicates the number of items in the list. The administrator can remotely uninstall unwanted patches or OS update packages from the endpoint.

Note: For Windows computers, the patch management agent uses Windows API to query the OS database for the applications installed on it. Hence only those applications installed through the Windows installer will be listed in the 'Software Inventory' column. Applications that were installed using custom installers or using unconventional installation processes will not be displayed in the list.

- **OS** - Displays the list of OS update packages and security patches that are available at the patch management server and could be installed on to the endpoint. The number at the tab indicates the number of items in the list. The administrator can remotely install these updates and patches on to the endpoint.
- **Custom** - Displays the list of custom and third-party applications that are available at the patch management server and could be installed on to the endpoint. The number at the tab indicates the number of items in the list. The administrator can remotely install these applications on to the endpoint.

The Inventory table - Column Descriptions	
Column	**Description**
Name	The name of the update package/patch/application
Installed Date/Release Date	For Software Inventory - The date at which the item was installed at the endpoint For OS and Custom tabs - The date at which the item was released by the vendor
Vulnerability ID	The OS vulnerability addressed by the update or the patch
Version	The version number of the item

The Inventory table - Column Descriptions	
Column	**Description**
Severity	The severity level of the item. The possible severity levels are: • Critical • Recommended • Optional Selecting the Severity level from the drop-down filters the items that fall under the chosen category.
Info	Clicking the info icon opens the Applications interface and displays the details of the item. Refer to the section **Managing OS Updates, Patches and Applications** for more details.

Sorting, Filtering and Search options

Displaying Hidden Items

The patch management module allows the administrator to hide selected OS Update packages, OS patches or custom applications available from the Patch Management server, but are not required or reserved for specific endpoints. More details on hiding the items are available in the section Managing OS Updates, Patches and Applications.

Such hidden items are not displayed in the inventory lists in the Inventory area. If you want those hidden items to be displayed in the list, select the 'Show Hidden' checkbox.

Searching OS Updates or custom application

You can search for a specific OS Update package, OS patch or a custom application from the lists under the Inventory area.

- Switch to the respective tab
- Enter the name of the item in part or full in the Search text box and click the magnifier icon

Sorting the Items

You can sort the items in the ascending or descending order of different criteria like Application Name, Vulnerability ID or the Installed/Release Date.

- Switch to the respective tab
- Select the criteria from the 'Sort by' drop-down. The available options are:
  - Application Name
  - Installed/Release Date
  - Vulnerability ID
- Choose whether the entries are to be sorted on ascending or descending order by clicking the blue UP or Down blue arrow next to the drop-down

Filtering the Entries

You can filter the items based on the severity level

- Switch to the respective tab
- Select the severity level from the drop-down at the 'Severity Level' column

Only the items that fall under the selected severity level will be displayed.

4.2 Initiate Manual Update or Installation Operation

The 'Inventory' area at the bottom of the endpoint properties interface displays lists of:

- OS Update packages, OS security patches, third-party update patches and custom third-party applications that have been installed at the endpoint
- OS Update packages, OS security patches, third-party update patches and custom third-party applications that are available at the Patch Management server and applicable for installation on to the endpoint.

The items are also indicated as Critical, Recommended or Optional based on their severity level.

The administrator can initiate a manual instant or scheduled patch uninstallation and patch/application installation operations from this area.

The following sections explain more on:

- **Uninstalling Security Patches, Updates or third party applications from the endpoint**
- **Installing Security Patches, Updates or third party applications from the server**

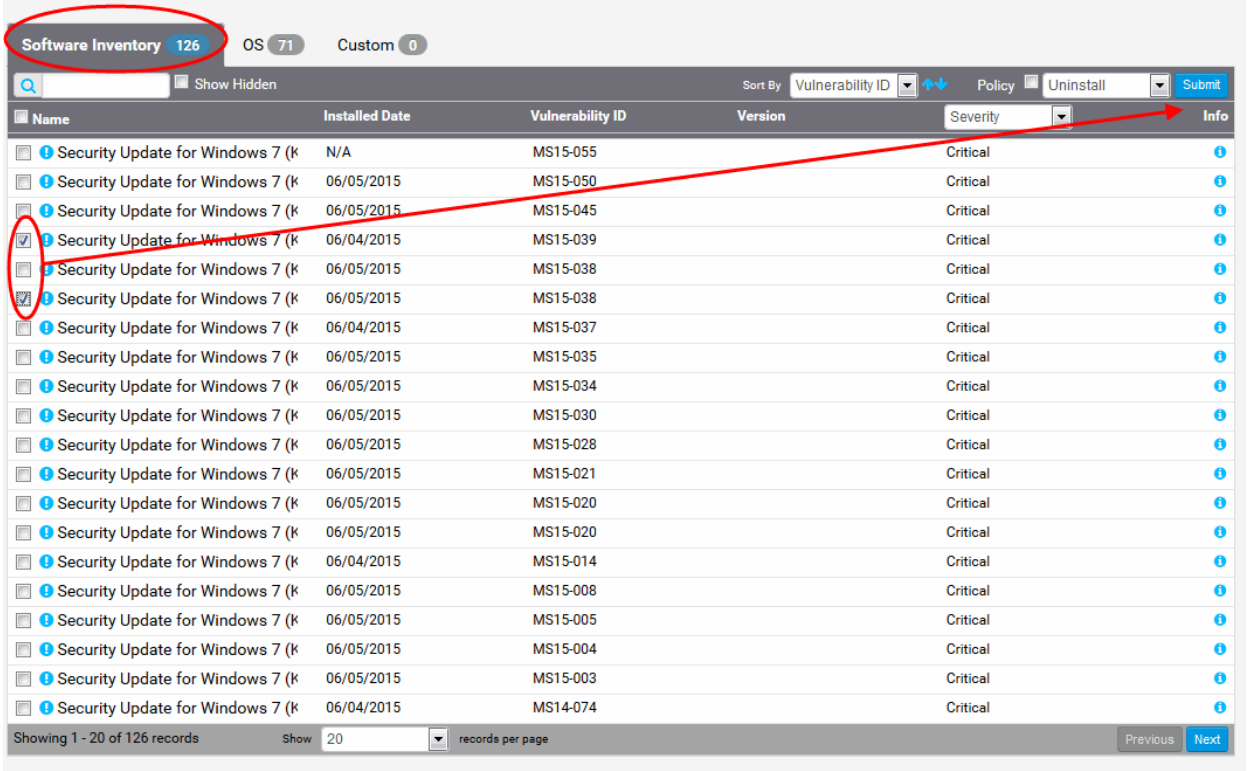
Uninstalling Patches or Update packages from the endpoint

The administrator can instantly uninstall selected OS patches or update packages from the endpoint or create a schedule for the uninstallation.

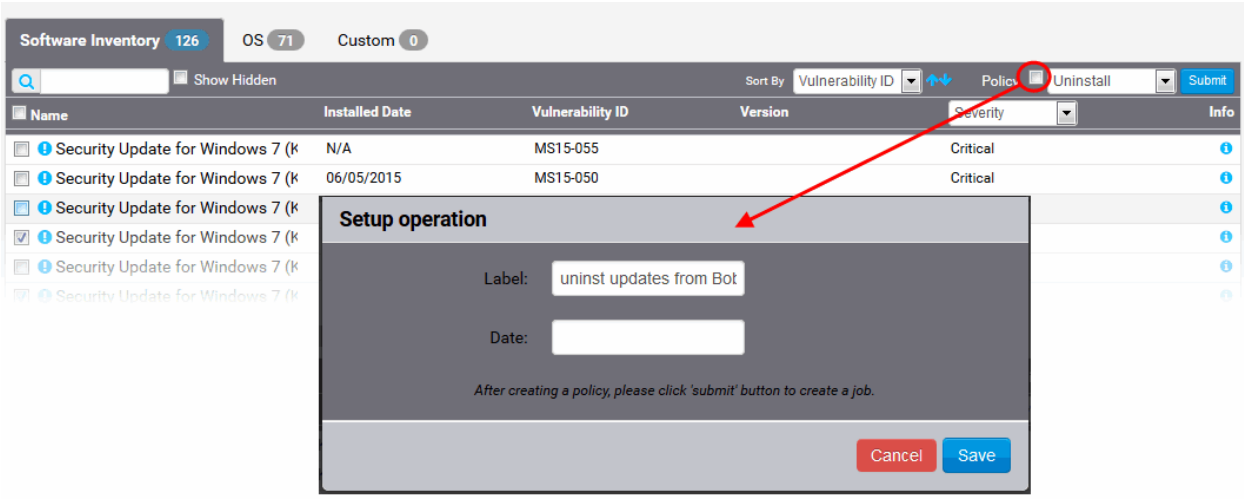
Limitations: The Patch Management module allows you to uninstall only Patches and Updates or third-party applications that were installed from .msi or .msp installation packages, at the endpoint . You cannot uninstall any item installed using .exe installation package.

To uninstall the patches or update packages from an endpoint

- Open the Endpoint Properties interface by clicking the endpoint name from the 'Agents' interface
- Scroll down to the 'Inventory' area and click the 'Software Inventory' tab
- Select the OS patch(es) or OS update(s) to be uninstalled. You can use the search and filter options to search for the specific patch(es)/update(s) to be uninstalled. Refer to the explanation on **Sorting, Filtering and Search Options** in the previous section **Viewing Endpoint Details** for more details
- To uninstall the item(s) instantly, click the 'Submit' button

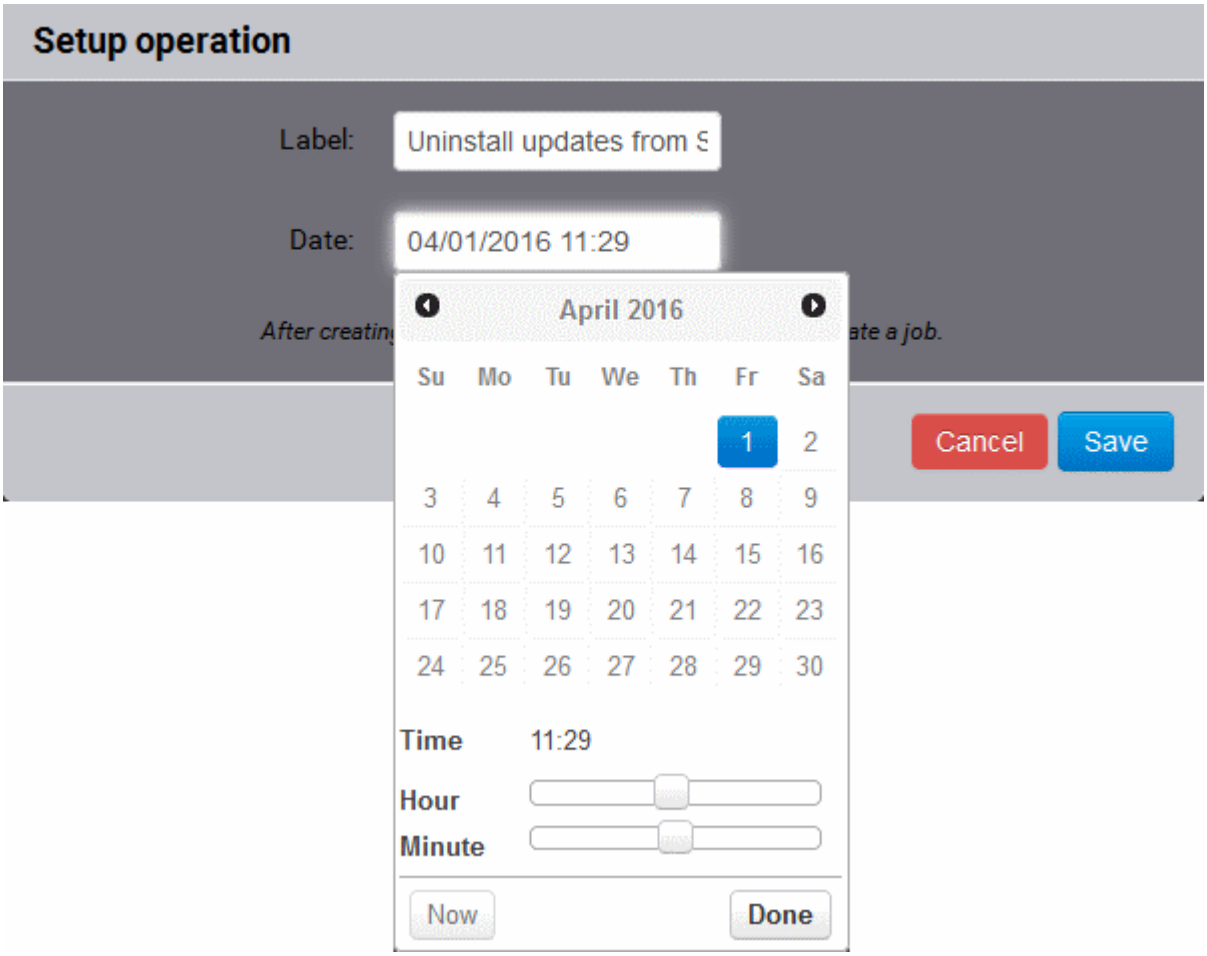


- To uninstall the item(s) at a scheduled time, select the 'Policy' checkbox



The Setup operation dialog will appear to set the schedule.

- Enter a name for the uninstallation operation in the Label text box
- Click the Date text box to enter the time and date at which the selected patch(es) or update(s)are to be uninstalled. A calendar drop-down will appear.



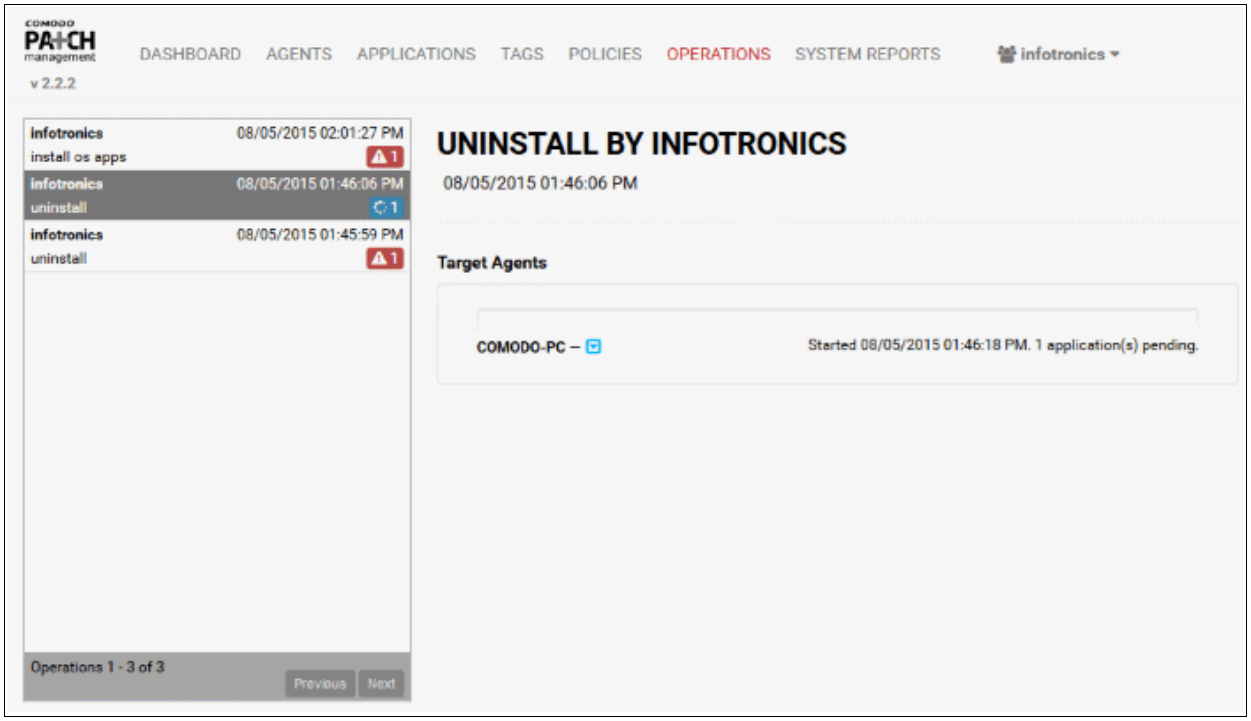
- Select the date from the calendar
- Set the time using the 'Hour' and 'Minute' sliders
- If you want the uninstallation operation to start instantly, click 'Now'
- Click 'Done'
- Click 'Save' from the 'Setup operation' dialog.

- Click 'Submit' from the Inventory area.

The uninstallation operation will be created and executed instantly or at scheduled time as chosen.

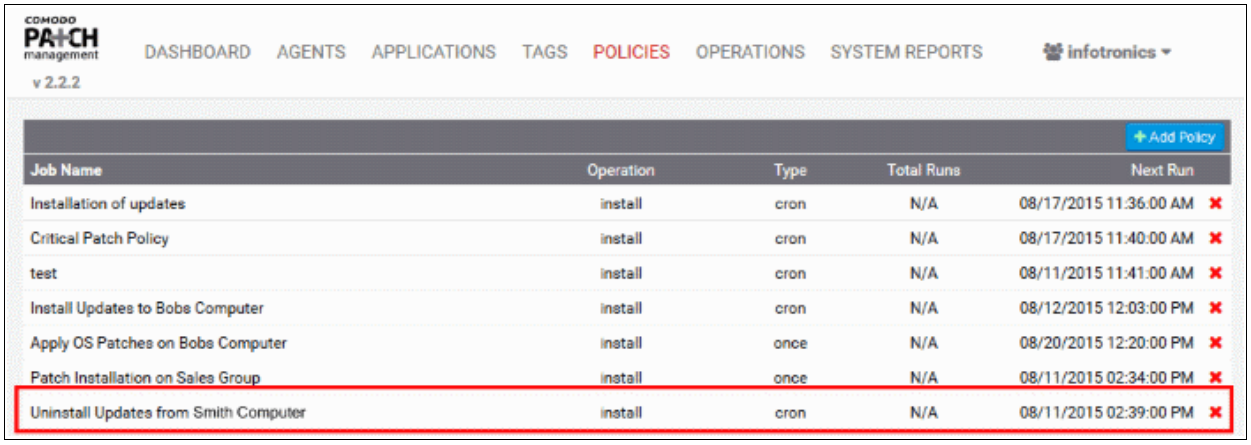
For an instant uninstallation operation, you can view the progress of the operation from the 'Operations' interface.

- Click the 'Operations' tab to open the 'Operations' interface and click on the operation name.



For more details on viewing the details of the operation, refer to the section **Viewing Patch Management Operations**.

For a scheduled uninstallation operation, you can view the schedule displayed under the Policies tab.



The uninstallation operation will commence on the scheduled time.

For more details on managing scheduled operations, refer to the section **Automated Management Policies**.

Installing Patches, OS Updates or third party applications from the server

The administrator can instantly install OS patches/update packages or custom/third-party applications available from the server on to the endpoint or create a schedule for the installation.

Limitations:

- For Security Patches and OS Update packages – The patch management module can install any patch or update which is auto-loaded to the server, on release by the OS vendor.
- For third-party applications and update patches - The patch management module can install any patch or application whose installation package is of the format as given below:
  - Windows - .exe, .msi, .msp, .msu
  - Ubuntu/Debian - .deb

- CentOS - .rpm
- Mac - .dmg

To install OS patches/update packages or an application

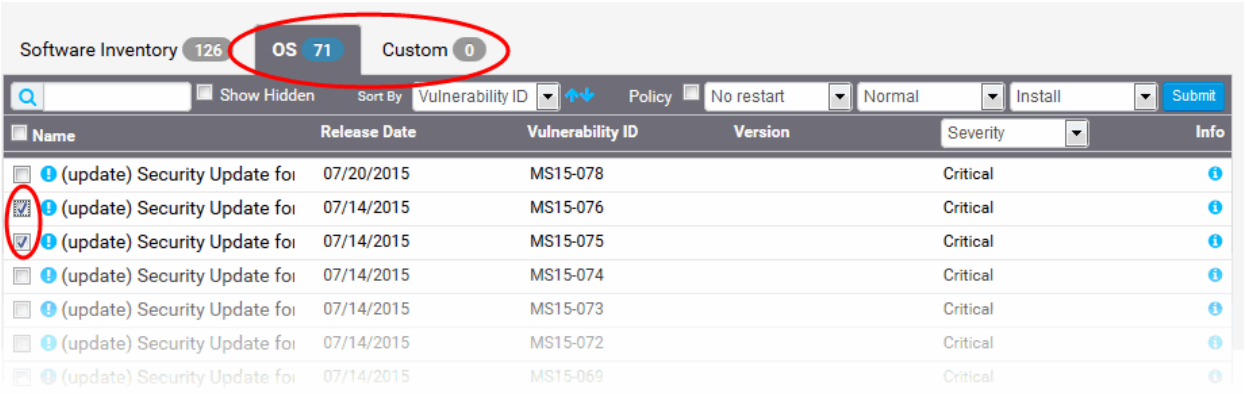
- Open the Endpoint Properties interface by clicking the endpoint name from the 'Agents' interface
- Scroll down to the 'Inventory' area
- Select the items to be installed
  - To install patch(es) or updates, click the 'OS' tab
  - To install custom or third-party applications, select the 'Custom' tab
  - Select the item(s) to be installed. You can use the search and filter options to search for the specific patch(es)/update(s) or applications to be installed. Refer to the explanation on **Sorting, Filtering and Search Options** in the previous section **Viewing Endpoint Details** for more details
- Configure the installation options:

  Restart options – Select whether the endpoint needs to be restarted for the installation to take effect, from the first drop-down at the top right. The options available are:

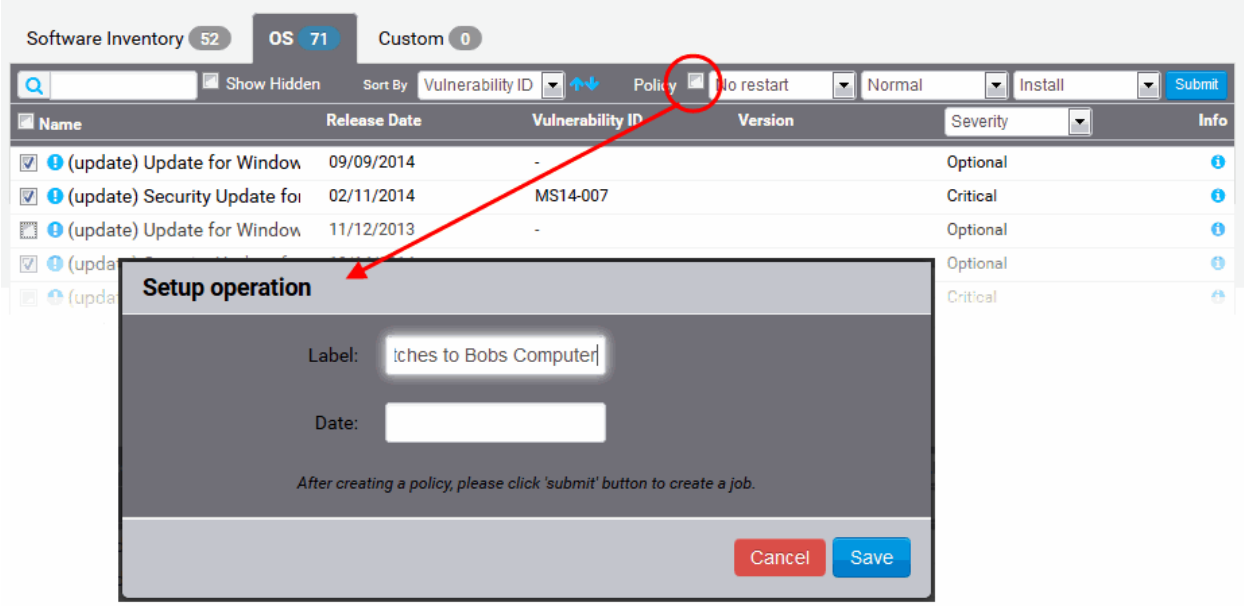
  - **No Restart** – The endpoint will not be restarted on completion of the installation operation. If the item(s) installed require the endpoint to be restarted for the installation to take effect, it will do so, only after the next manual restart of the endpoint by the end user.
  - **Only if needed** – The patch management module will check whether the item(s) installed require(s) the endpoint to be restarted for the installation to take effect. The endpoint will be restarted upon completion of installation only if it is required.
  - **Forced** – The endpoint will be restarted upon completion of installation operation, regardless of whether the items installed requires to do so, for the installation to take effect.

  Priority - Choose the execution priority for the installation operation at the endpoint from the next drop-down. The CPU usage for the installation operation will be set as per the chosen priority. The options available are:

  - Idle
  - Below Normal
  - Normal
  - Above Normal
  - High
- To install the item(s) instantly, click the 'Submit ' button

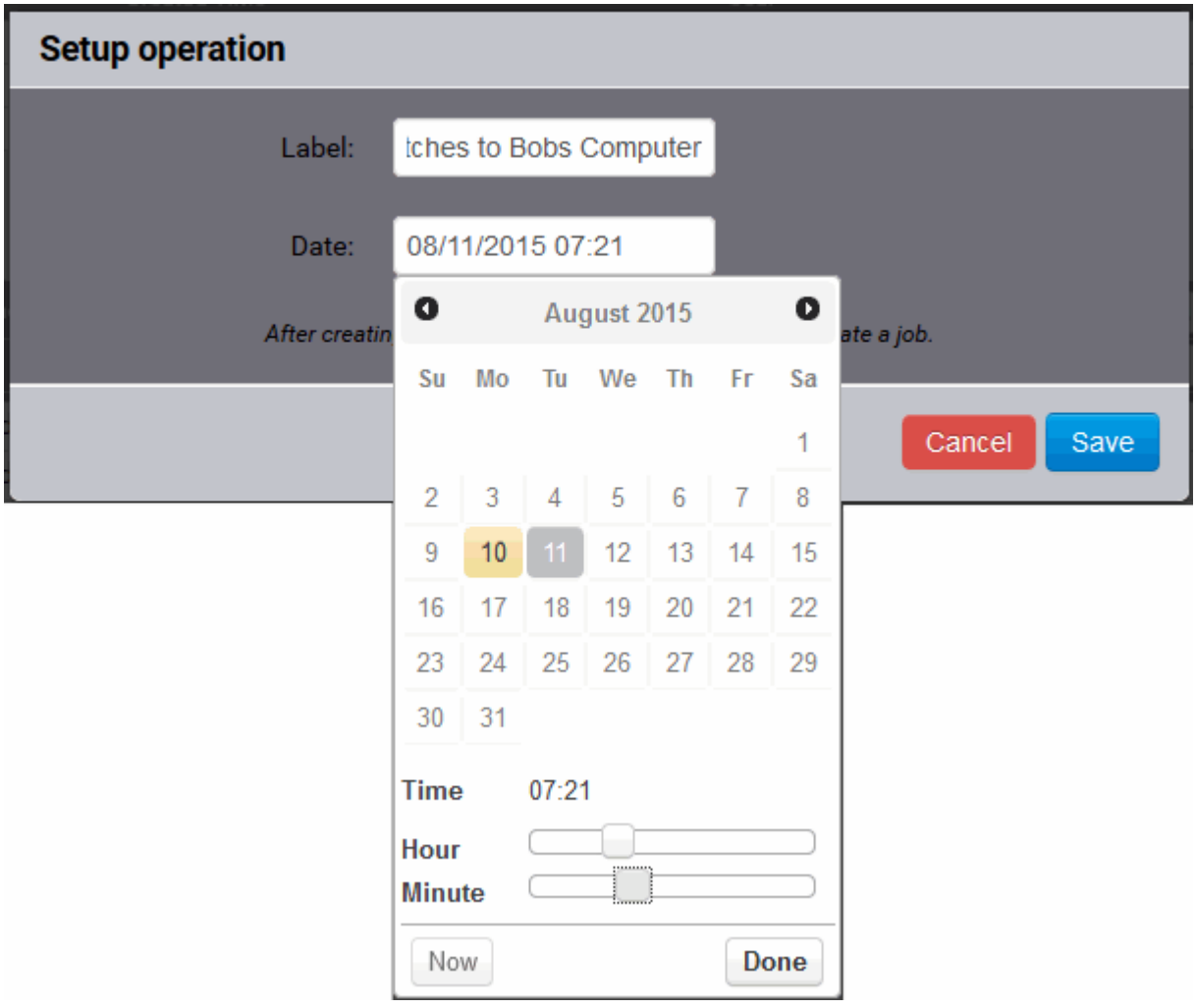


- To install the item(s) at a scheduled time, select the 'Policy' checkbox



The 'Setup operation' dialog will appear to set the schedule.

- Enter a name for the installation operation in the Label text box
- Click the Date text box to enter the time and date at which the selected patch(es) or update(s)are to be installed. A calendar drop-down will appear.



- Select the date from the calendar

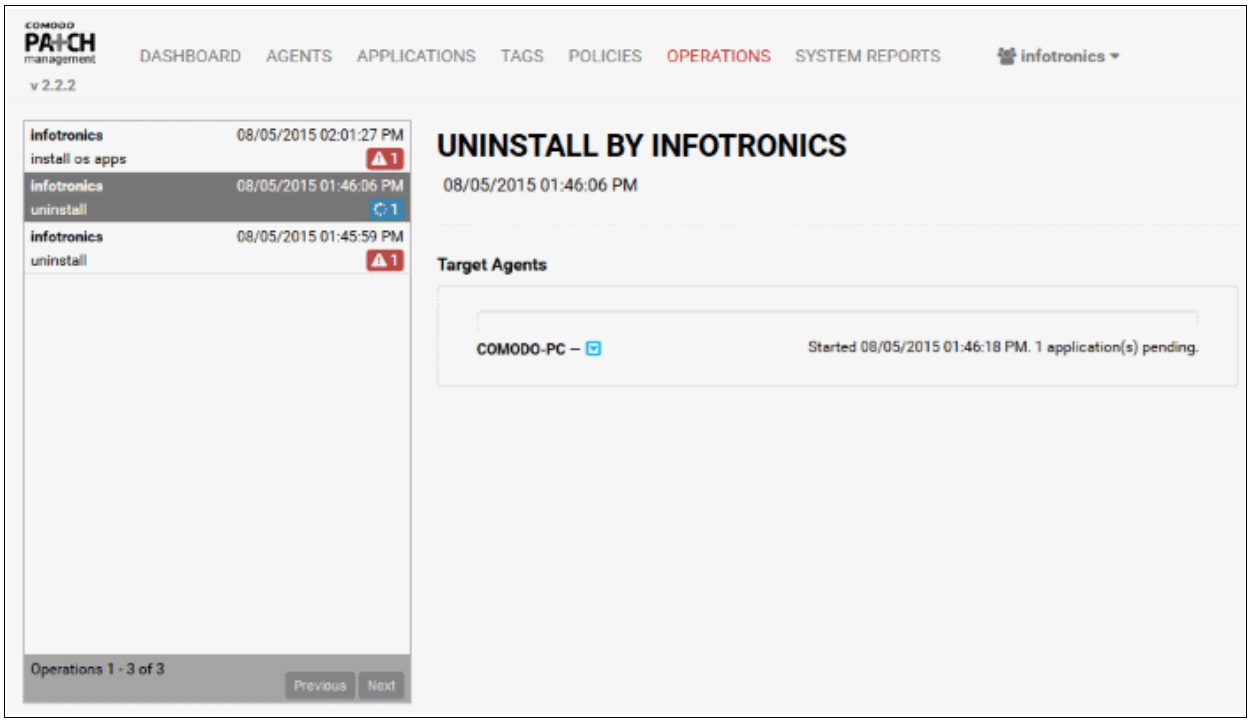
- Set the time using the Hour and Minute sliders
- Click 'Done'
- Click 'Save' from the 'Setup operation' dialog.

- Click 'Submit' from the Inventory area.

The installation operation will be created and executed instantly or at scheduled time as chosen.

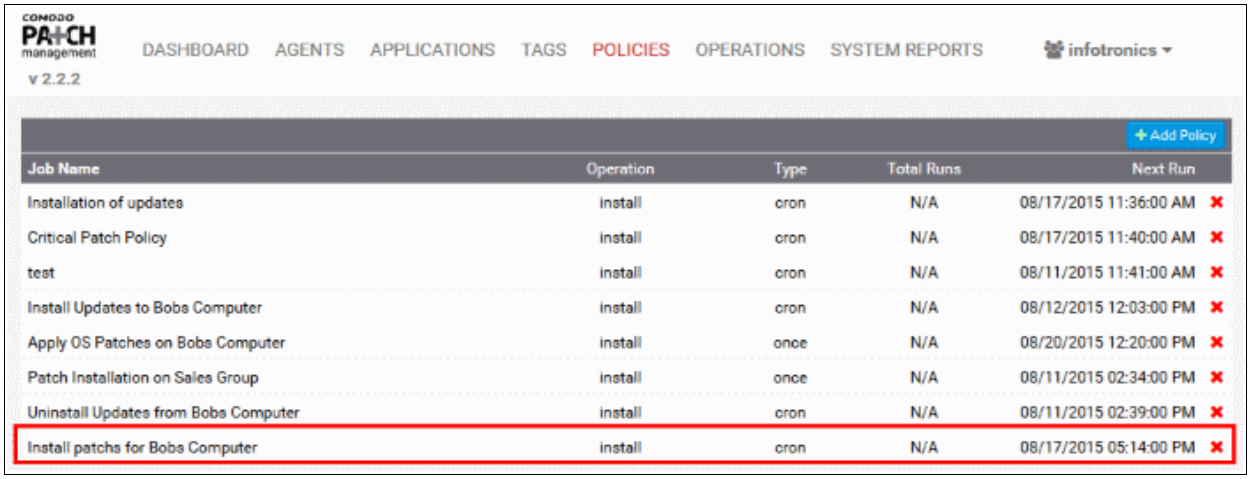
For an instant installation operation, you can view the progress of the operation from the 'Operations' interface.

- Click the 'Operations' tab to open the 'Operations' interface and click on the operation name.



For more details on viewing the details of the operation, refer to the section **Viewing Patch Management Operations**.

For a scheduled installation operation, you can view the schedule displayed under the 'Policies' tab.



Job Name	Operation	Type	Total Runs	Next Run
Installation of updates	install	cron	N/A	08/17/2015 11:36:00 AM
Critical Patch Policy	install	cron	N/A	08/17/2015 11:40:00 AM
test	install	cron	N/A	08/11/2015 11:41:00 AM
Install Updates to Bobs Computer	install	cron	N/A	08/12/2015 12:03:00 PM
Apply OS Patches on Bobs Computer	install	once	N/A	08/20/2015 12:20:00 PM
Patch Installation on Sales Group	install	once	N/A	08/11/2015 02:34:00 PM
Uninstall Updates from Bobs Computer	install	cron	N/A	08/11/2015 02:39:00 PM
Install patchs for Bobs Computer	install	cron	N/A	08/17/2015 05:14:00 PM

The installation operation will commence on the scheduled time.

For more details on managing scheduled operations, refer to the section **Automated Management Policies**.

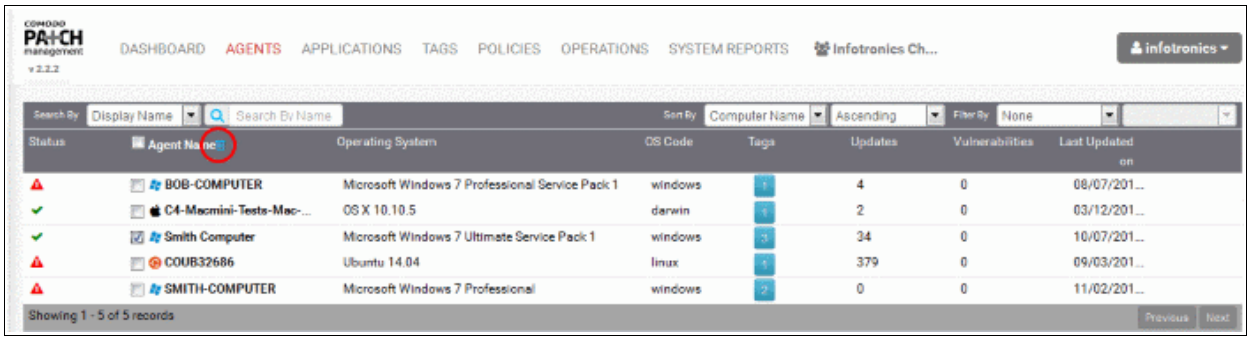
4.3 Remove Selected Endpoint(s)

Endpoints that no longer require management can be removed by simply selecting them and clicking the delete icon at the top or from the endpoint details screen.

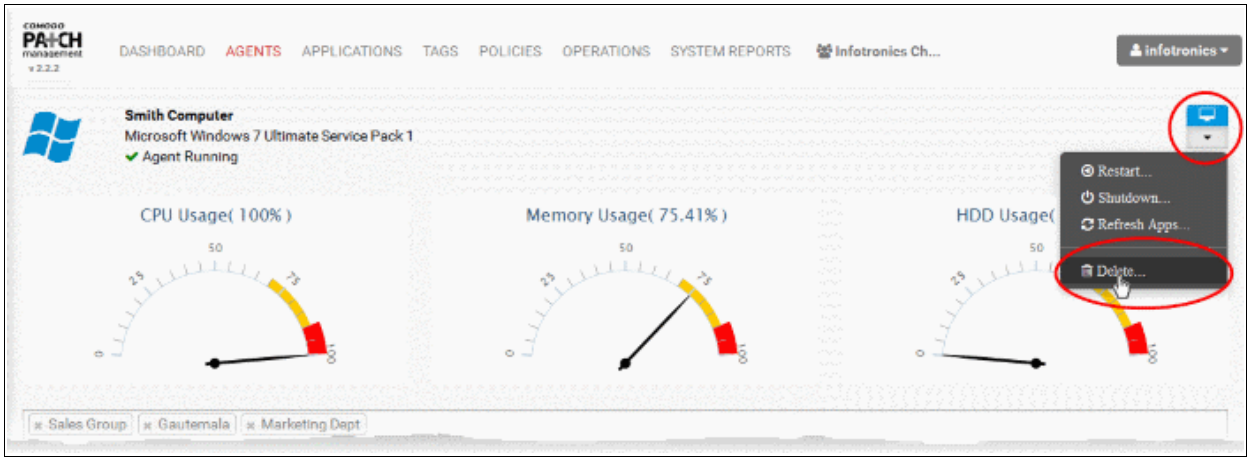
Warning: Once an endpoint is removed, the agent will be automatically uninstalled from the endpoint and all details pertaining to the endpoint will be deleted from the server. If the endpoint needs to be re-enrolled, the agent should be reinstalled on the endpoint.

To remove endpoints

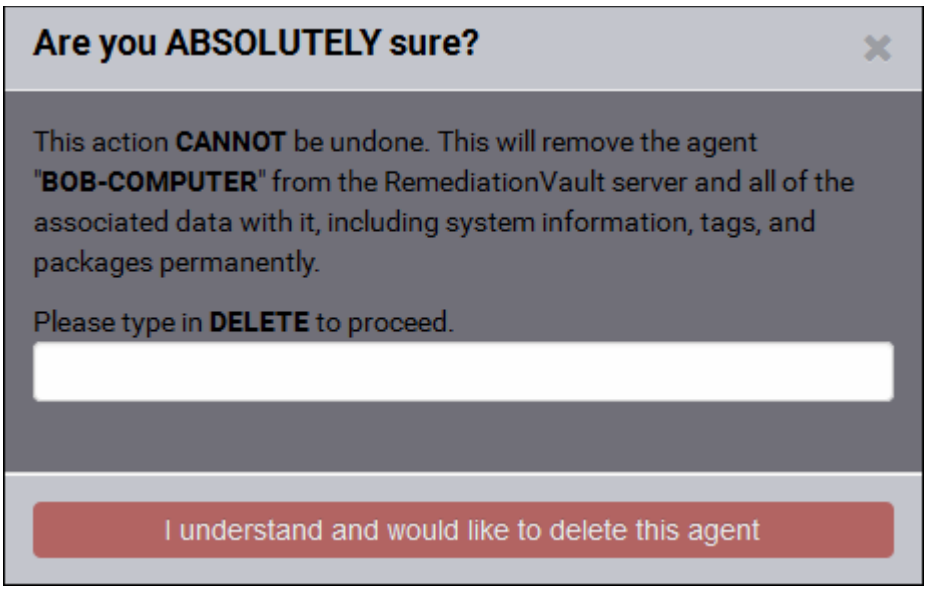
- Open the 'Agents' interface by clicking the 'Agents' tab.
- Select the customer from whose account the endpoints need to be removed from the 'Customer Account' drop-down
- Select the endpoint(s) to be removed
- Click the Trash icon beside “Agent Name” in the table header



Alternatively, click on the name of the endpoint to open its details screen and then click the drop-down at the far end and select 'Delete' from the options.



A confirmation dialog will appear.



- If you are sure on removing the endpoints, type “DELETE” in the text box and click 'I understand and would like to delete this agent'

The agents will be uninstalled from the endpoints and the endpoints will be removed from the patch management module.

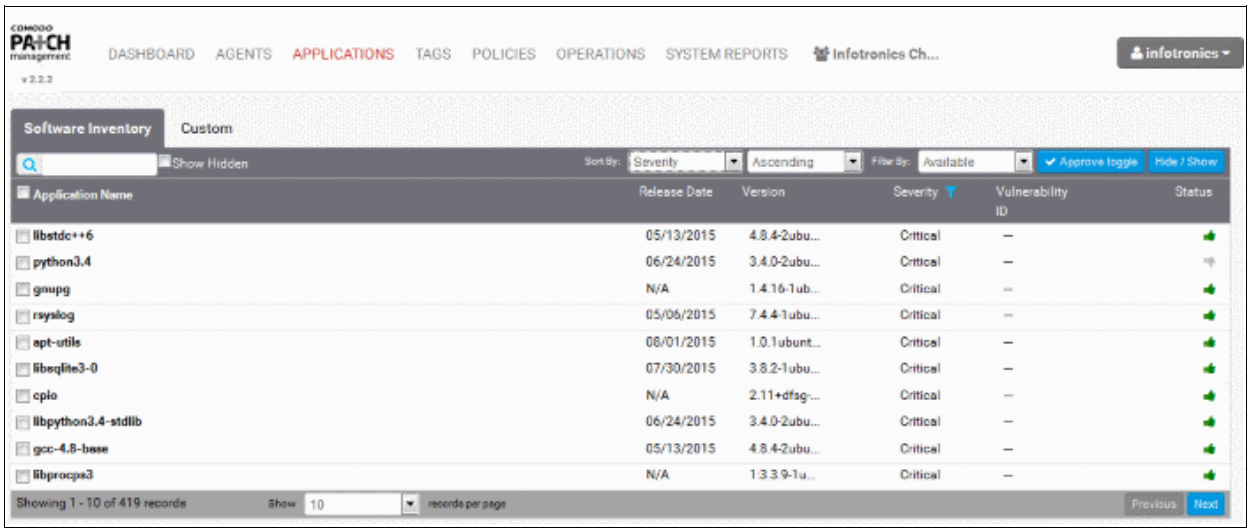
5 Manage OS Updates, Patches and Applications

The 'Applications' interface displays a list of all operating system updates, software patches and custom or third-party applications that are awaiting deployment to endpoints in the selected customer account.

Clicking on any item opens a page which contains complete details about the update, including:

- A description of the update, including severity, vendor and download URL
- A bar chart explaining the quantity of endpoints affected by the update. This includes the number of endpoints for which the update is available (or 'applicable to'), the number on which it has been installed already, and the number of endpoints where installation is pending.
- A table which lists of those endpoints affected by the update. The table has separate tabs for each status ('Available', 'Pending' and 'Installed')

Administrators can use this interface to remotely install patches and/or custom applications to selected endpoint(s) and uninstall an item from the selected endpoint(s).



The interface contains two tabs:

- **Software Inventory** – Displays all the OS patches and update packages that are applicable to the operating systems of the endpoints added to the customer account.
- **Custom** – Displays all the custom and third-party applications that are applicable to the operating systems of the endpoints added to the customer account.

Applications table - Column Descriptions	
Column	**Description**
Application Name	The name of the patch, update package or application
Release Date	The date at which the item was released by the publisher/vendor
Version	The version number of the item
Severity	The severity level of the item. The possible severity levels are: • Critical • Recommended • Optional Clicking filter icon and selecting the Severity level from the drop-down filters the items that fall under the chosen category.
Vulnerability ID	The OS vulnerability addressed by the update or the patch
Status	Indicates the approval status of the item for automated and scheduled patch applications. The approval state of an item can be toggled by selecting it and clicking the 'Approve toggle' button at the table header.

Sorting and Searching Options

Displaying Hidden Items

The patch management module allows the administrator to hide selected OS Update packages, OS patches or custom applications available from the Patch Management server, but are not required or reserved for specific endpoints. More details on hiding the items are available in the section Hiding Unnecessary OS Updates, Patches and Applications.

Such hidden items are not displayed in the inventory lists in the Inventory area. If you want those hidden items to be

displayed in the list, select the 'Show Hidden' checkbox.

Sorting the Entries

You can sort the items in the ascending or descending order of different criteria like application name, release date, severity level, version number and so on.

- Select the criteria from the 'Sort by' drop-down. The available options are:

Criteria	Sorts the entries on...
Name	the alphabetical order of the application names of the OS patch, update package or third-party application
Release Date	the chronological order of the release dates of the items
Severity	the alphabetical order of severity levels of the items
Version	the numerical order of the version number of the items
Vulnerability ID	the numerical order of the identification numbers of vulnerabilities addressed by the item
Hidden	the hidden items. Please note the 'Show Hidden' check box should be selected. If 'Descending' is selected, then the hidden items will be displayed first and if 'Ascending' is selected then the hidden items will be displayed at the last.

- Choose whether the entries are to be sorted on ascending or descending order of the selected criteria from the next drop-down

Filtering the Entries

You can filter the entries based on different criteria like Operating Systems, agent status and more.

- Select the criteria from the 'Filter by' drop-down. The available options are:

Criteria	Displays only ...
None	No filter will be applied.
Available	the items available for installing on to the endpoints pertaining to the customer account
Installed	the items that have been installed on to the endpoints pertaining to the customer account
Pending	the items for which the installation operation has been initiated but pending to be installed on to the endpoints pertaining to the customer account

You can also filter the items based on the severity level by clicking the filter icon and selecting the level from the drop-down.

Searching the patches or applications

You can search for specific items by entering a part of of full application name in the search field and clicking the magnifier icon.

The interface allows the administrator to:

- **View details of a patch, update package or an application**
- **Approve packages for automated and scheduled installations**
- **Install patch or application on to selected endpoints**

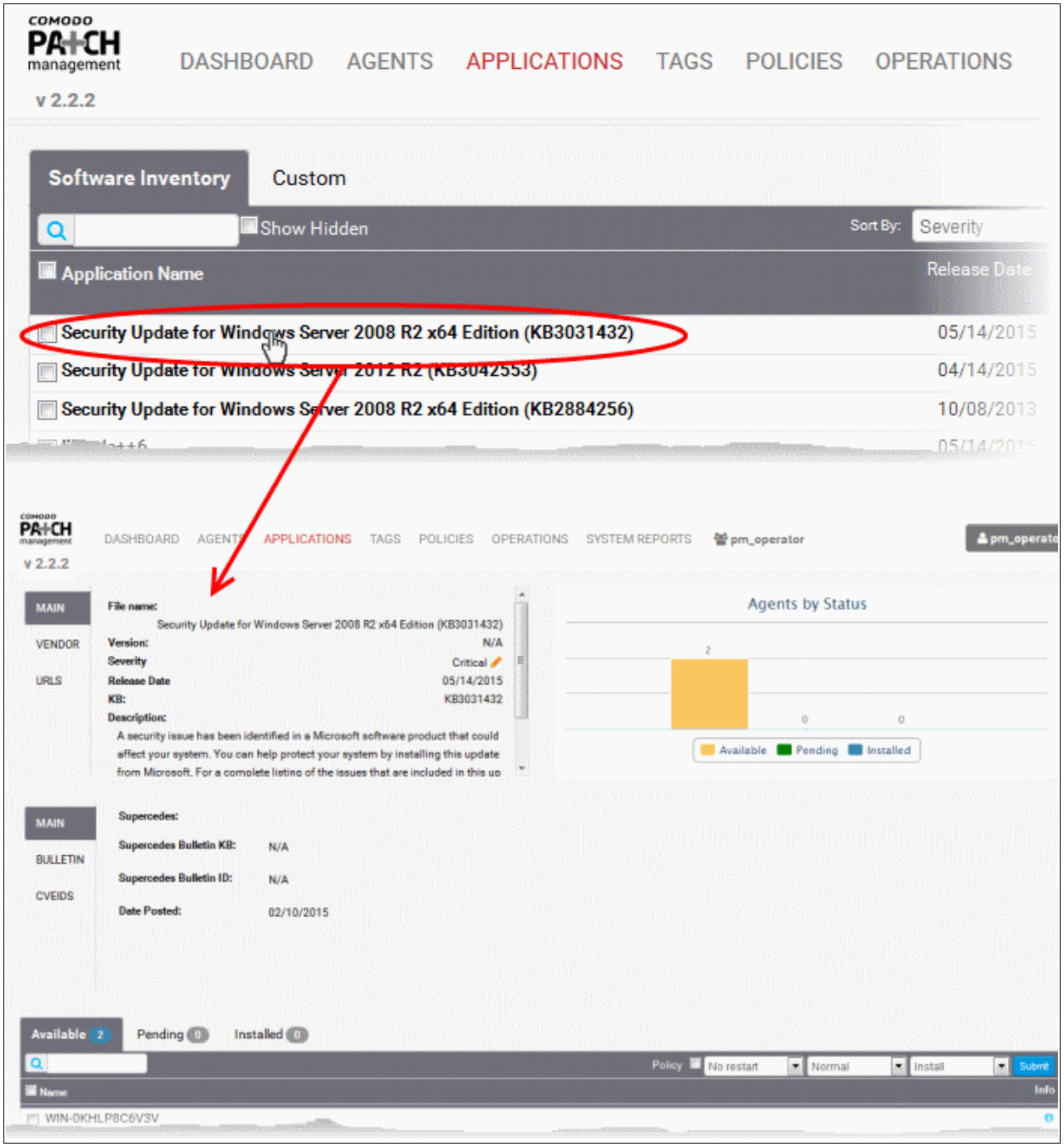
- **Uninstall patch or application from an endpoint**

5.1 View Details of a Patch, Update Package or an Application

The 'Applications' interface allows administrators to view granular details about patches and update packages. This includes patch descriptions, severity and which endpoints the update will affect. In addition, administrators can initiate remote installation of the items onto selected endpoints and uninstall items from endpoints.

To view the details of a Patch, Update Package or an Application

- Open the applications interface by clicking the 'Applications' tab
- Choose the 'Software Inventory' or 'Custom' tab depending on the item
    - **Software Inventory** – Displays all OS patches and update packages
    - **Custom** – Displays all custom and third-party applications
- Click anywhere in the row of item. The Application Details screen will be displayed.

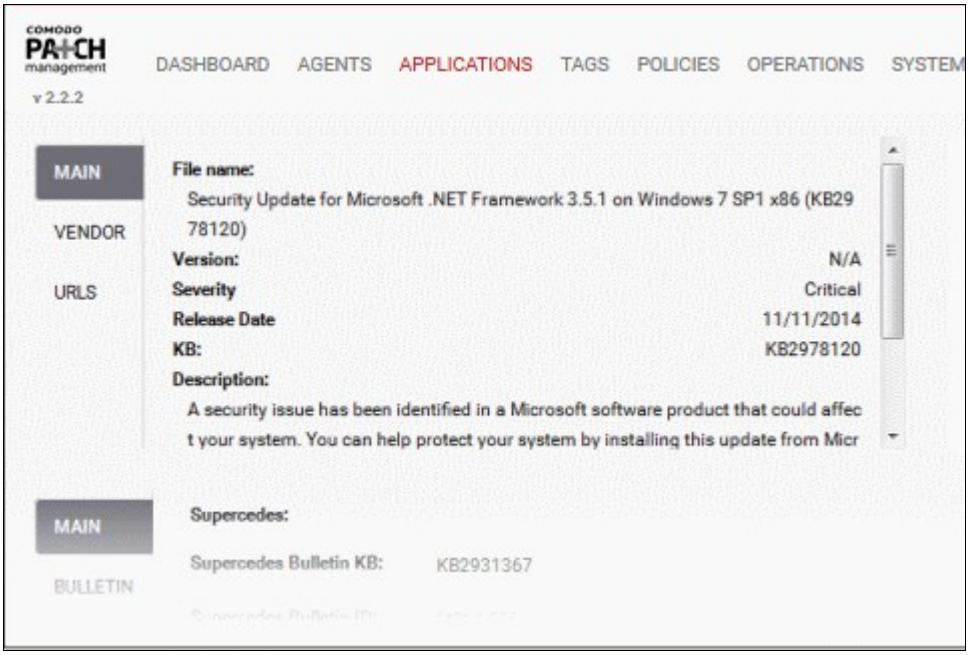


The Application Details screen contains the following areas. Each area is explained in detail after the list.

- Application Information
- Patch Information (Only for Windows Security Patches)
- Graphical Representation of Application Installation Status
- Lists of endpoints on which the items can be installed, the endpoints on which the installation is pending and endpoints on which the item has been installed. You can install the item on to required endpoints or uninstall the item from selected endpoints

Application Information

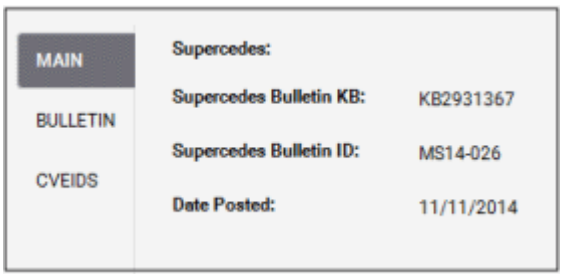
The Application Information area provides a summary of the the update, vendor details and the download URL of the item. Administrators can also edit the severity of the item from here.



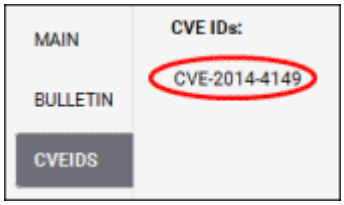
Tab	Details Displayed
Main	General details including name, description, version, severity level, release date and knowledge-base ID. This tab also allows administrators to change the severity level of the update and both severity level and silent installation switch parameters for the applications.
Vendor	Details on vendor or publisher of the application, vendor severity level and the support URL of the application
URL	The download url of the application package and its file hash

Patch Information

For Windows Security Patches, the patch information area displays bulletin information and Common Vulnerabilities and Exposures (CVE) ID under respective tabs.

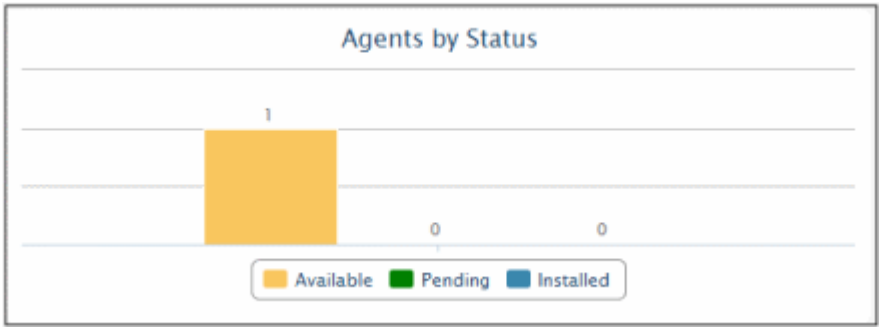


Tab	Details Displayed
Main	Details about the security bulletins and knowledge-base articles superseded by the patch
Bulletin	The ID and description of the security bulletin from Microsoft, relevant to the patch
CVEIDS	The ID of the Common Vulnerabilities and Exposures (CVE) ID of the patch. Clicking the CVE ID opens a new screen displaying the CVE details of the vulnerability addressed by the patch.

Tab	Details Displayed
	

Status Chart

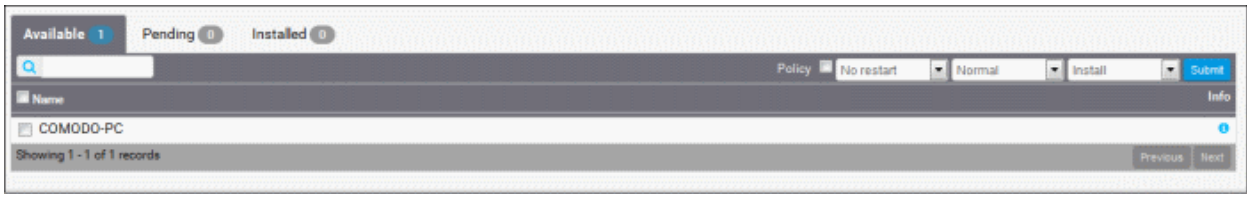
Each update is accompanied by a bar-chart which summarizes which endpoints are affected by the update. The chart displays how many endpoints the item is available for, how many is it already installed on, and how many endpoints it is pending for.



Hovering the mouse cursor over the bars displays the number of endpoints that fall under the selected category.

The Endpoints Details Area

The Endpoints list at the bottom of the screen displays the lists of endpoints under three tabs:



- **Available** – Displays a list of endpoints for which the item is applicable but has not yet been installed. Administrators can remotely install the item on to selected endpoints.
- **Installed** – Displays a list of endpoints which already have the patch installed. Administrators can remotely uninstall the item from selected endpoints.
- **Pending** – Displays a list of endpoints for which the installation operation is in-progress.

The administrator can initiate a manual patch management or remote application installation operation on to selected endpoints from this area. For more details, refer to the section **Install Patch or Application on to Selected Endpoints**.

The Endpoints table - Column Descriptions	
Column	**Description**
Name	The name of the update package/patch/application
Controls	Clicking the info icon ℹ opens the Endpoint Properties interface and displays the

	details of the endpoint. Refer to the section **Viewing Endpoint Details** more details.

Searching patches or applications

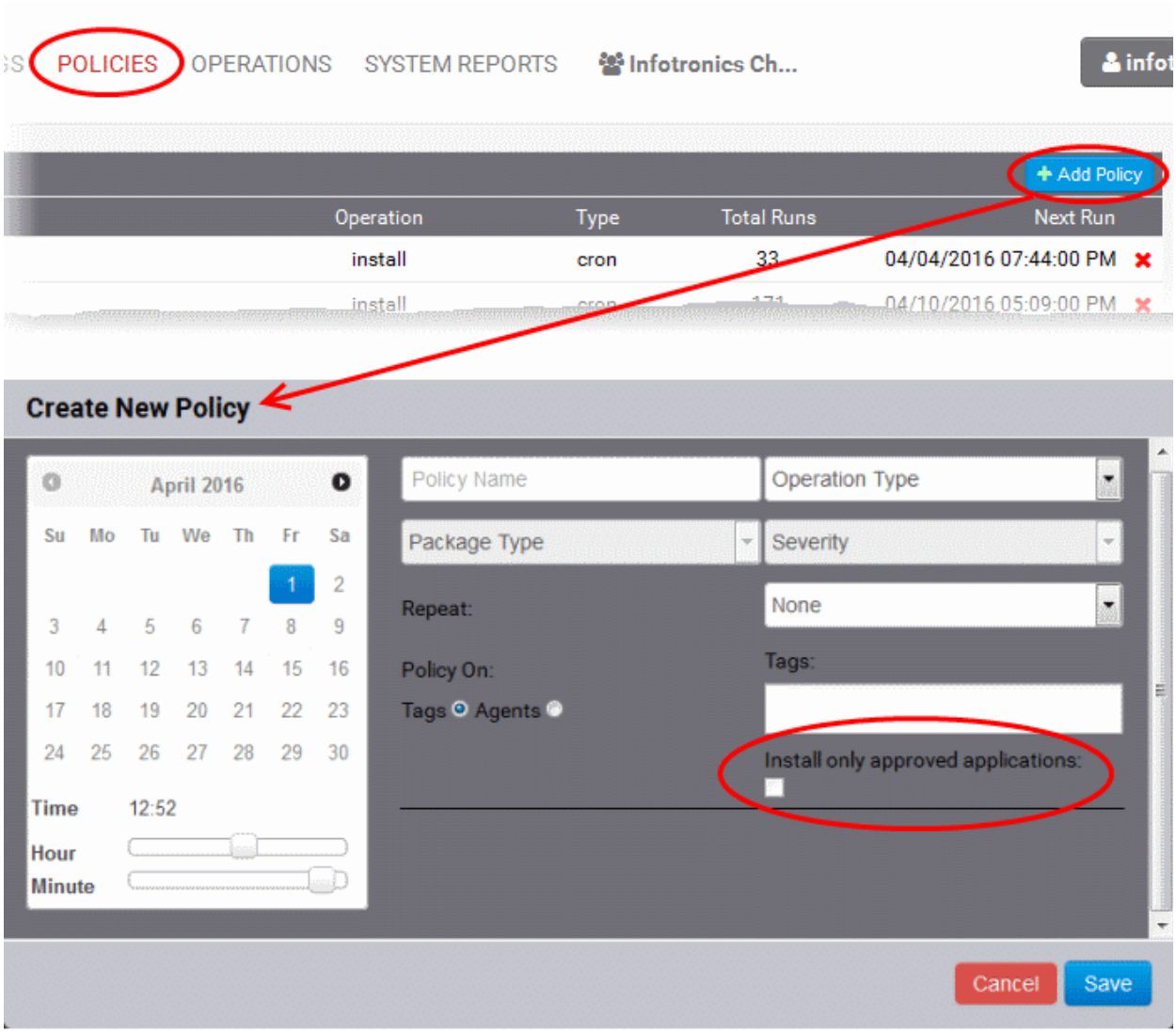
You can search for specific endpoints by entering a part or full display name or hostname in the search field.

5.2 Approve Packages for Automated and Scheduled Installations

The patches and the applications can be approved/unapproved for automated and scheduled installation from the Application Properties interface.

The patch management module allows you to create policies for automated and scheduled patch management operations to run once or periodically on to selected endpoints or groups of endpoints with specific tags. On creating an installation task, all the OS patches/update packages applicable for the selected endpoints or all the custom third-party applications that fall under the chosen severity level and applicable for the selected endpoints will be installed as per the schedule. Refer to the section **Automated Management Policies** for more details on creating the policies.

The administrator can choose to install only approved patches or applications while creating a schedule, instead of installing all the available patches/applications during a scheduled installation operation.

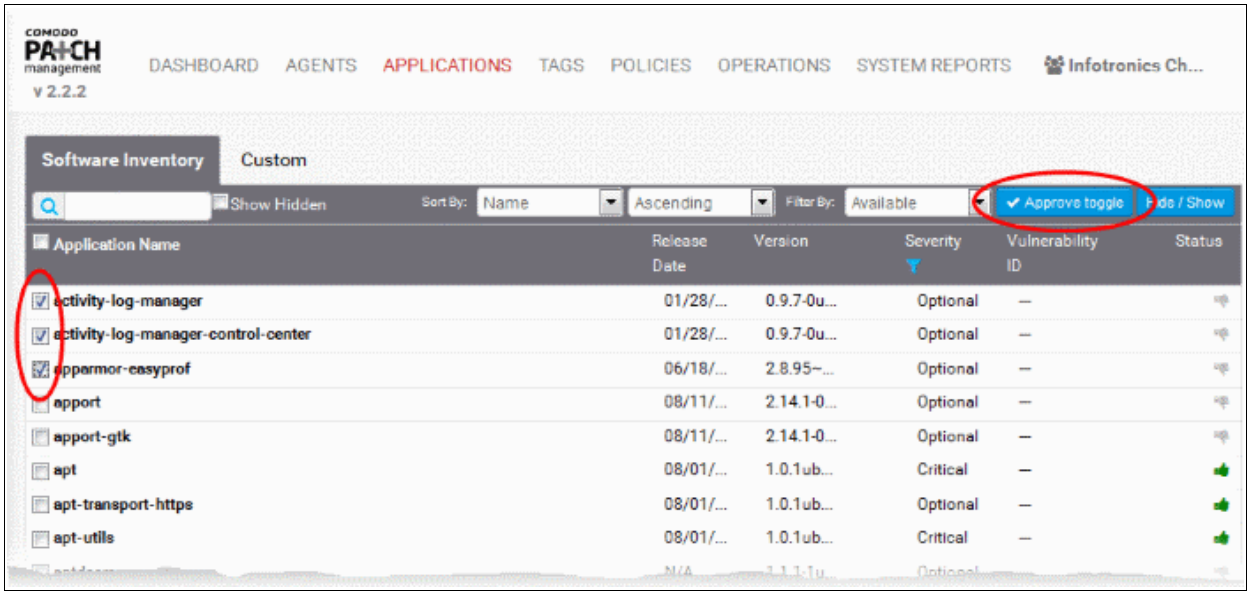


To toggle approval of patches or applications for automated installations

- Open the applications interface by clicking the 'Applications' tab
- Choose the Software Inventory or Custom tab depending on the items to be toggled
  - **Software Inventory** – Displays all OS patches and update packages
  - **Custom** – Displays all custom and third-party applications and third-party patches

The items that are approved are indicated with icon and the items that are not approved are indicated by icon in the 'Status' column.

- Select the items for which the approval is to be switched



- Click the 'Approve toggle' button from the top right

The approval state of the selected items will be toggled for approved to unapproved or vice versa.

5.3 Install a Patch or an Application on to Selected Endpoints

The administrator can instantly install the selected patch/OS update package or custom/third-party application on to selected endpoints or create a schedule for the installation.

Limitations:

- For Security Patches and OS Update packages - The patch management module can install any patch or update which is auto-loaded to the server, on release by the OS vendor.
- For third-party applications and update patches - The patch management module can install any patch or application whose installation package is of the format as given below:
  - Windows - .exe, .msi, .msp, .msu
  - Ubuntu/Debian - .deb
  - CentOS - .rpm
  - Mac - .dmg

To install the item on to selected endpoints

- Open the applications interface by clicking the 'Applications' tab
- Choose the 'Software Inventory' or 'Custom' tab depending on the items to be toggled
    - **Software Inventory** – Displays all OS patches and update packages
    - **Custom** – Displays all custom and third-party applications and third-party patches
- Select the item and click anywhere in the row of item to open the 'Application Properties' interface
- Scroll down to the 'Endpoint Details' area and click the 'Available' tab to view the endpoints that are eligible for installation of the item
- Select the endpoints upon which the item needs to be installed.
    - You can use the search option to search for specific endpoints by entering a part of of full display name or hostname of it in the search field and clicking the magnifier icon.
- Configure the installation options:

Restart options – Select whether the endpoint needs to be restarted for the installation to take effect, from the first drop-down at the top right. The options available are:

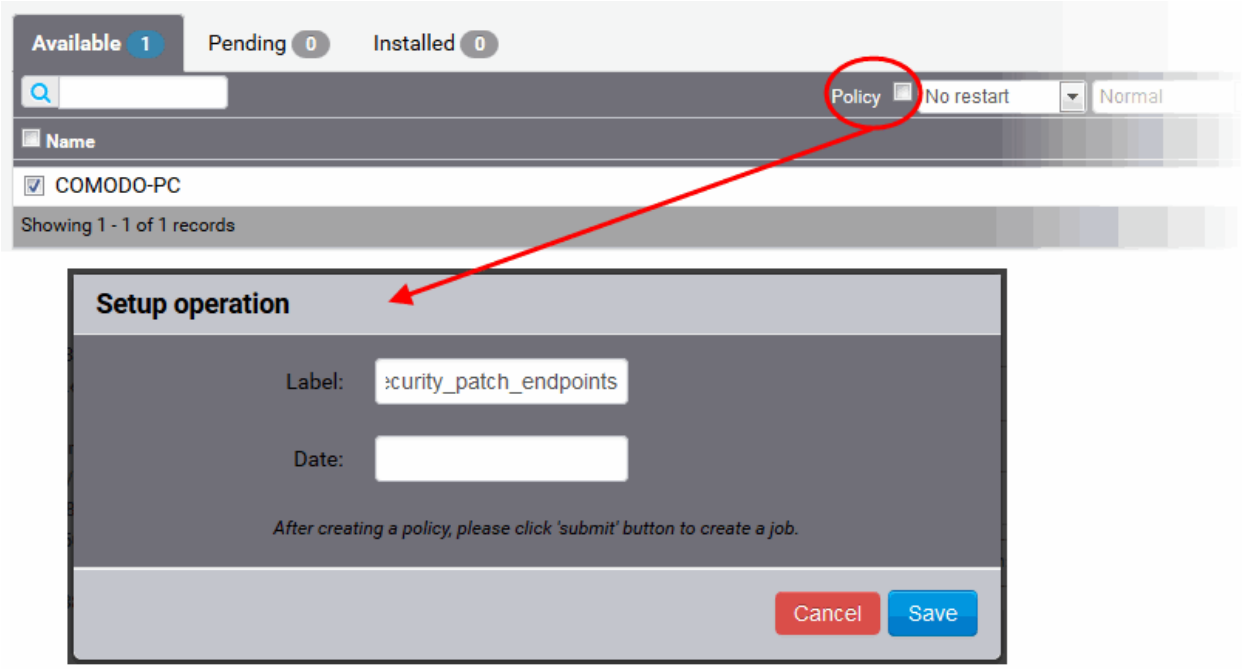
- **No Restart** – The endpoint will not be restarted on completion of the installation operation. If the item(s) installed require the endpoint to be restarted for the installation to take effect, it will do so, only after the next manual restart of the endpoint by the end user.
- **Only if needed** – The patch management module will check whether the item(s) installed require the endpoint requires the endpoint to be restarted for the installation to take effect. The endpoint will be restarted upon completion of installation only if it is required.
- **Forced** – The endpoint will be restarted upon completion of installation operation, regardless of whether the items installed requires to do so, for the installation to take effect.

Priority - Choose the execution priority for the installation operation at the endpoint from the next drop-down. The CPU usage for the installation operation will be set as per the chosen priority. The options available are:

- Idle
- Below Normal
- Normal
- Above Normal
- High

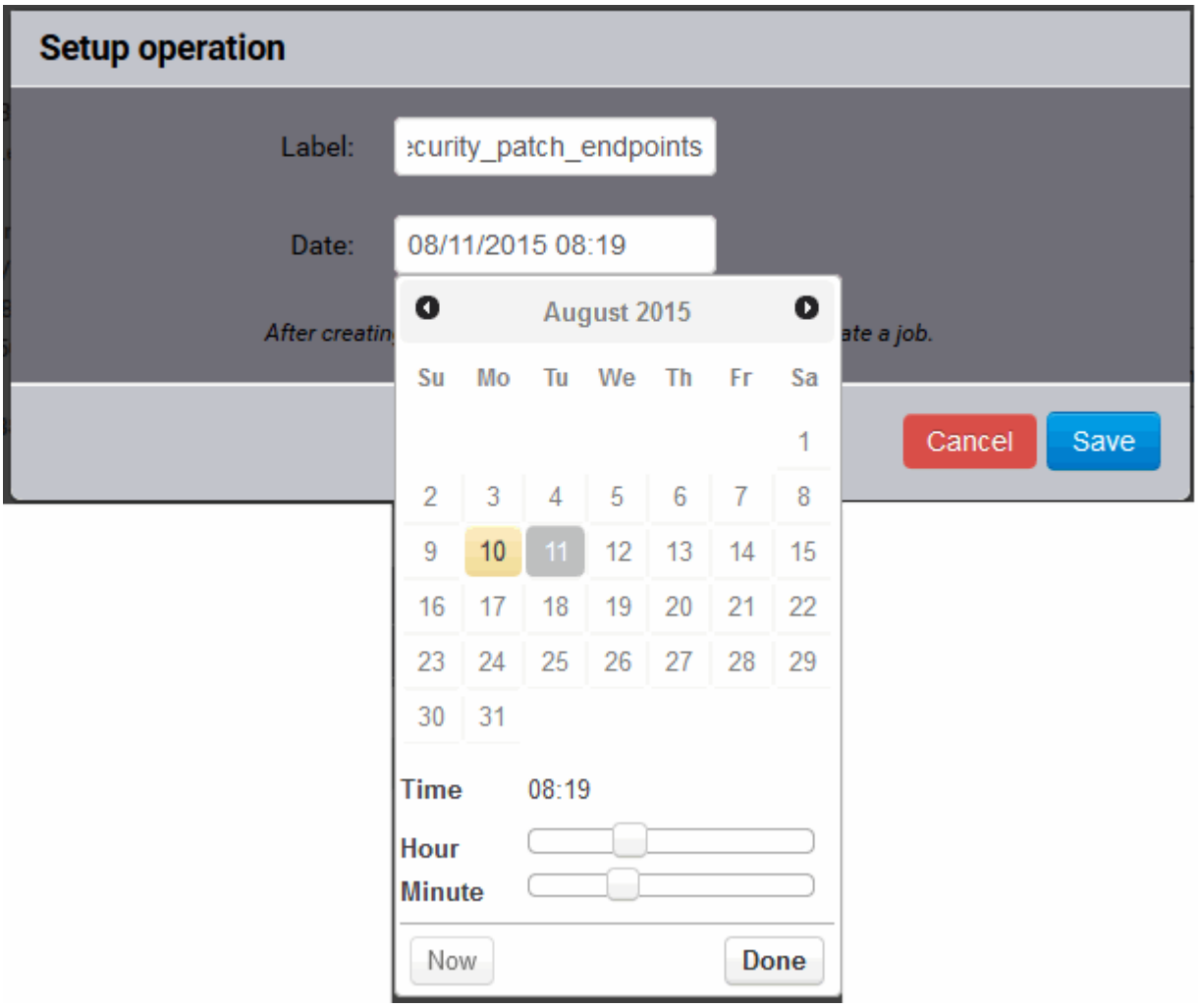
- To install the item instantly, click the 'Submit' button

- To install the item(s) at a scheduled time, select the 'Policy' checkbox



The 'Setup operation' dialog will appear to set the schedule.

- Enter a name for the installation operation in the Label text box
- Click the Date text box to enter the time and date at which the selected patch(es) or update(s)are to be installed. A calendar drop-down will appear.



- Select the date from the calendar
- Set the time using the Hour and Minute sliders
- Click 'Done'
- Click 'Save' from the 'Setup operation' dialog.

- Click 'Submit' from the 'Endpoint Details' area.

The installation operation will be created and executed instantly or at scheduled time as chosen.

For an instant installation operation, you can view the progress of the operation from the 'Operations' interface.

- Click the 'Operations' tab to open the 'Operations' interface and click on the operation name.

For more details on viewing the details of the operation, refer to the section **Viewing Patch Management Operations**.

For a scheduled installation operation, you can view the schedule displayed under the 'Policies' tab.

- Click the 'Policies' tab to open the Polices interface and click on the operation name.

The uninstallation operation will commence on the scheduled time.

For more details on managing scheduled operations, refer to the section **Automated Management Policies**.

5.4 Uninstall a Patch or an Application from Endpoints

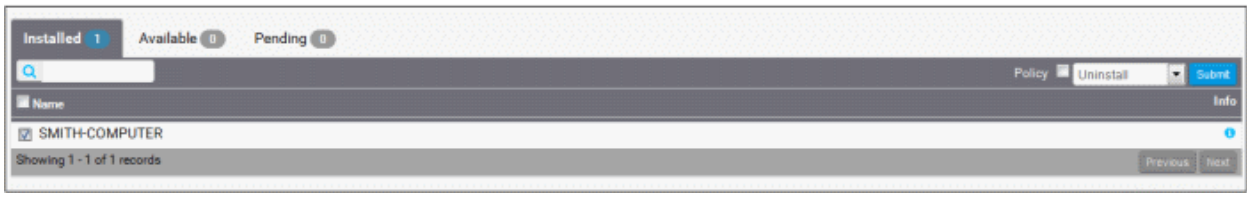
The administrator can instantly uninstall the selected patch/OS update package or custom/third-party application from selected endpoints or create a schedule for the uninstallation.

Limitations:

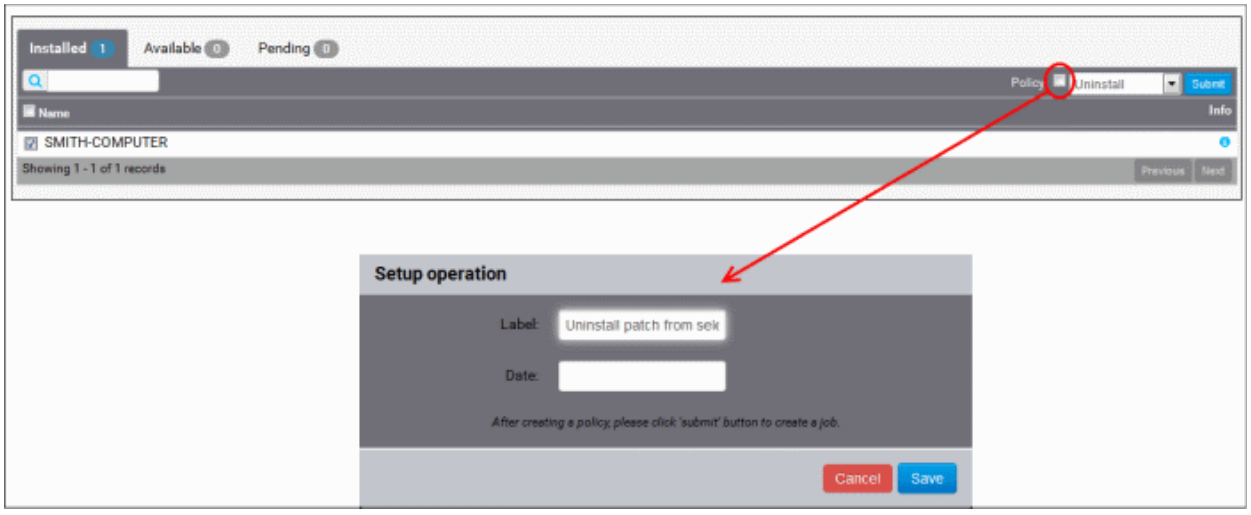
- For Security Patches and OS Update packages - The patch management module cannot uninstall any patch or update which is installed from an installer package of .exe file format.
- For third-party applications and update patches - The patch management module cannot uninstall any application installed from an installer package of .exe file format.

To uninstall an item from selected endpoints

- Open the applications interface by clicking the 'Applications' tab
- Choose the 'Software Inventory' or 'Custom' tab depending on the items to be toggled
  - **Software Inventory** – Displays all OS patches and update packages
  - **Custom** – Displays all custom and third-party applications and third-party patches
- Select the item and click anywhere in the row of item to open the Application Properties interface
- Scroll down to the 'Endpoint Details' area and click the 'Installed' tab to view the list of endpoints upon which the item has been installed
- Select the endpoints from which the item needs to be uninstalled.
  - You can use the search option to search for specific endpoints by entering a part of of full display name or hostname of it in the search field and clicking the magnifier icon.

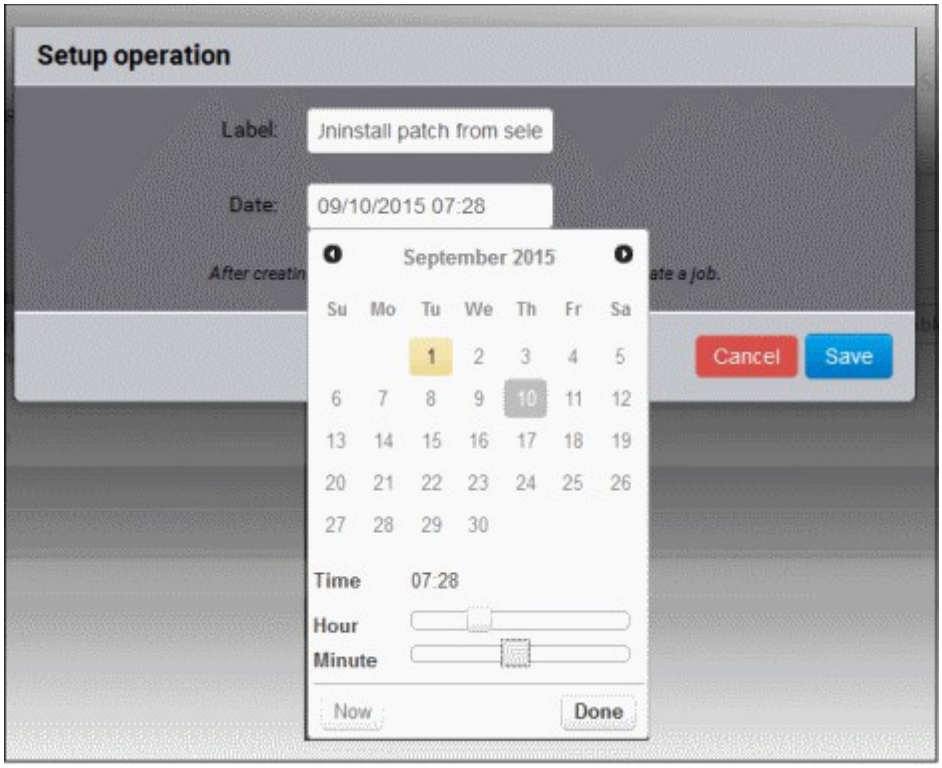


- To install the item instantly, click the 'Submit' button
- To install the item(s) at a scheduled time, select the 'Policy' checkbox



The Setup operation dialog will appear to set the schedule.

- Enter a name for the uninstallation operation in the label text box
- Click the 'Date' text box to enter the time and date at which the selected patch(es) or update(s)are to be uninstalled. A calendar drop-down will appear.



- Select the date from the calendar
- Set the time using the Hour and Minute sliders
- Click 'Done'
- Click 'Save' from the 'Setup operation' dialog.

- Click 'Submit' from the 'Endpoint Details' area.

The uninstallation operation will be created and executed instantly or at scheduled time as chosen.

For an instant installation operation, you can view the progress of the operation from the 'Operations' interface.

- Click the 'Operations' tab to open the 'Operations' interface and click on the operation name.

For more details on viewing the details of the operation, refer to the section **Viewing Patch Management Operations**.

For a scheduled installation operation, you can view the schedule displayed under the 'Policies' tab.

- Click the 'Policies' tab to open the 'Polices' interface and click on the operation name.

The uninstallation operation will commence on the scheduled time.

For more details on managing scheduled operations, refer to the section **Automated Management Policies**.

6 Add Tags and Manage Endpoint Groups

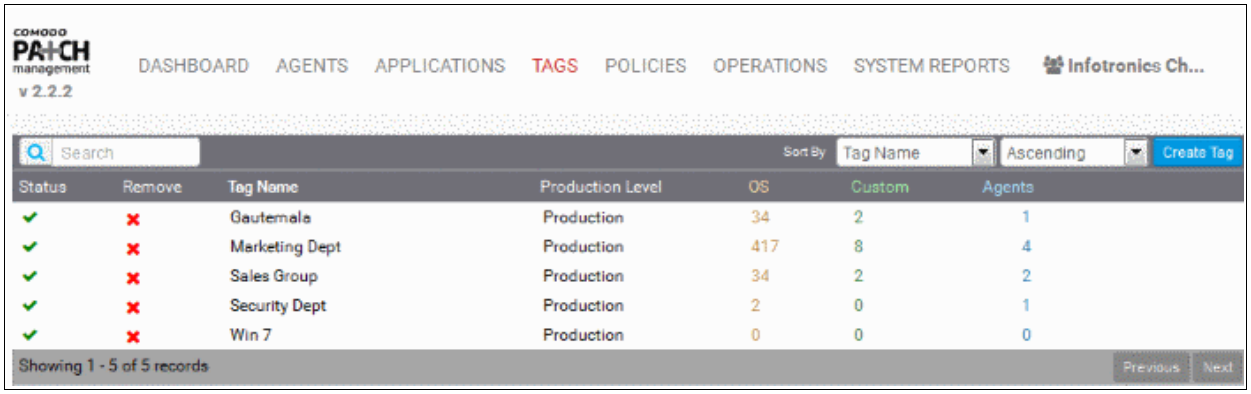
Tags are labels that can be applied to endpoints for creating groups of them. A single endpoint can be applied with any number of tags so that it can be a member of more than one group. Ideally, you should create multiple tags to cover attributes like operating system and department then apply them to particular endpoints as required. For

example, you could create and apply tags called 'Windows XP', 'Windows 7', 'Windows Vista', 'Sales Department', 'IT department', 'DMZ Machines' and 'Accounts' department'.

Applying an action to a tag will apply the action to all endpoints applied with that tag. For example, tags can be selected as a target for any application installation or reboot schedules you deploy in the 'Policies' area. This can save time by allowing you to accurately deploy updates to many endpoints simultaneously.

The Tags interface displays the list of tags for the selected customer account with statistics on the numbers of OS patches/updates and custom applications available from the server for installation onto the endpoints attached with the tag.

Clicking on any row will open a detailed properties page which contains important status information about the tag.



Tags table - Column Descriptions	
Column	**Description**
Status	Indicates whether the tag is active.
Remove	Contains the control button to remove the tag from the patch management module. Removing a tag from the patch management module also removes the same from the endpoints to which it is applied.
Tag Name	The name assigned to the tag, as a short description of category of member endpoints.
Customer	The customer account for which the tag is created.
Production level	The purpose of the endpoints covered by the tag. Refer to the explanation under **Production State** in the section **Viewing Endpoint Details** for more details."
OS	The number of OS patches and OS update packages that are available at the server and eligible for application to the endpoints with the tag
Custom	The number of third-party applications and patches eligible for application to the endpoints with the tag
Agents	The number of endpoints applied with the tag.

Sorting and Searching Options

Sorting the Entries

You can sort the entries in the ascending or descending order of tag name and production level.

- Select the criteria from the 'Sort by' drop-down. The available options are:
  - Tag name
  - Production level

- Choose whether the entries are to be sorted on ascending or descending order of the selected criteria from the next drop-down

Searching the Tags

You can search for specific tags by entering their name in part or full.

- Enter the name of the tag in part or full in the search text box and click the magnifier icon

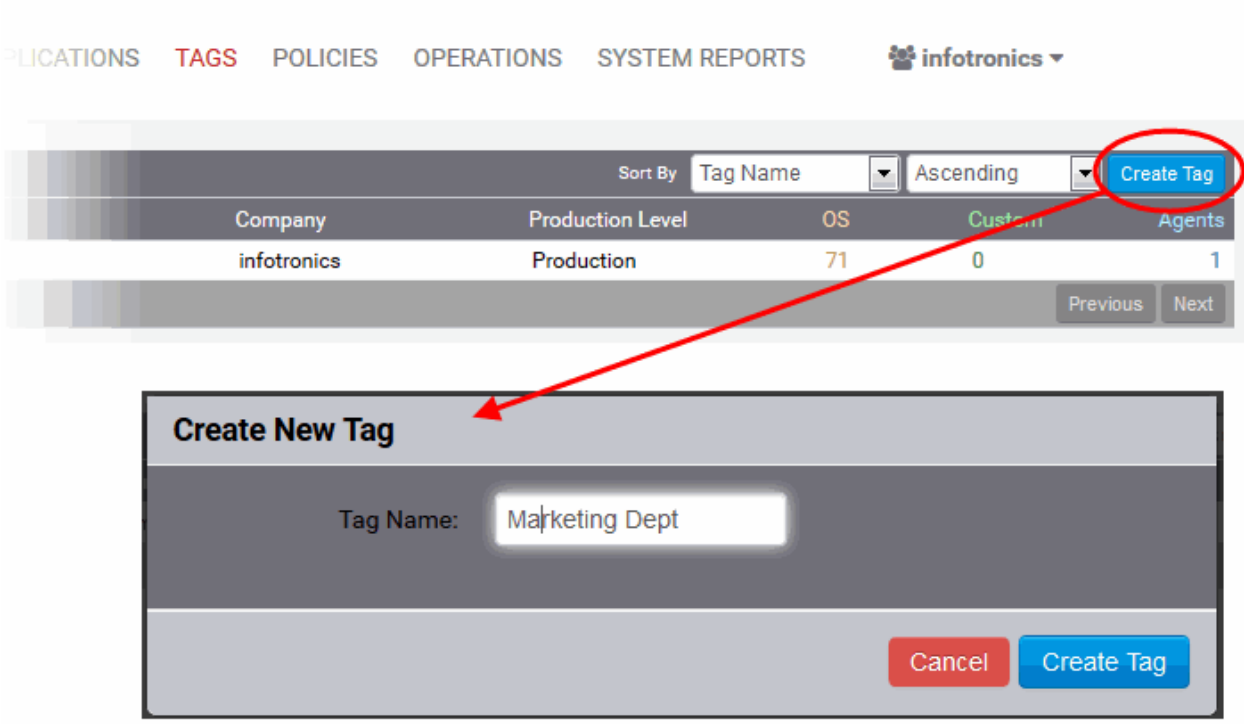
The interface allows the administrator to:

- **Create new tags**
- **View Tag Details**
- **Initiate manual update or patch/application installation operation**

6.1 Create a New Tag

To create a new tag

- Select the customer account from the 'Customer Account' drop-down
- Open the tags interface by clicking the 'Tags' tab
- Click the 'Create Tag' button at the top right. The 'Create New Tag' dialog will open:

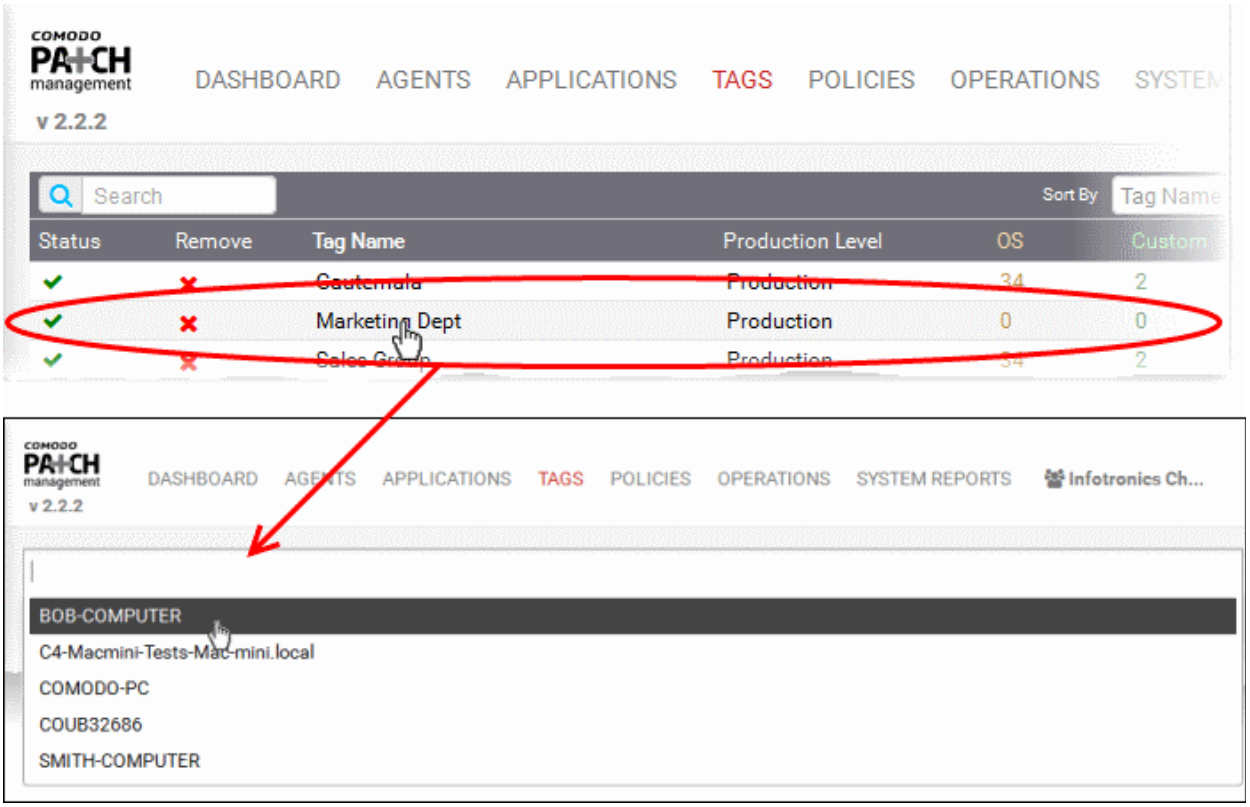


- Enter a short descriptive name to identify endpoints under the tag and click 'Create Tag'.

The new tag will be created. The tag can then be applied to endpoints from the 'Tag Properties' screen.

To apply the tag to endpoints

- Click on the row of the tag to open the 'Tag Properties' screen.

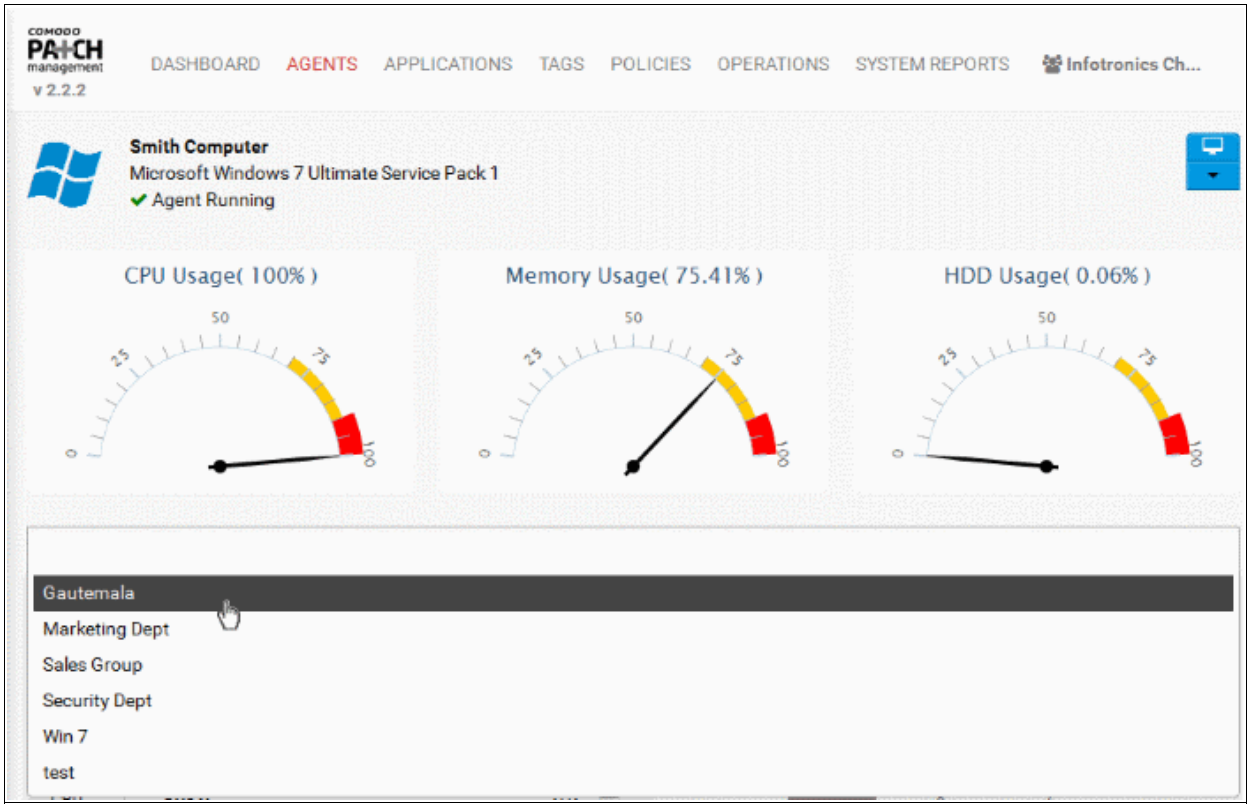


- Click on the 'Select the agent' field. A drop-down with the endpoints registered for the customer account will open.
- Choose the endpoint. The endpoint will be added to the list.

- Repeat the process to add more endpoints.
- To remove an endpoint, click 'X' beside the endpoint name.

Alternatively, you can add the new tag to an endpoint from the 'Endpoint Properties' screen.

- Click 'Agents' tab to open the list of endpoints registered for the customer account.
- Click the endpoint to which the tag is to be applied
- Click on the first text field. A drop-down with all the tags created for the customer account will be displayed.
- Choose the tag to be applied to the endpoint



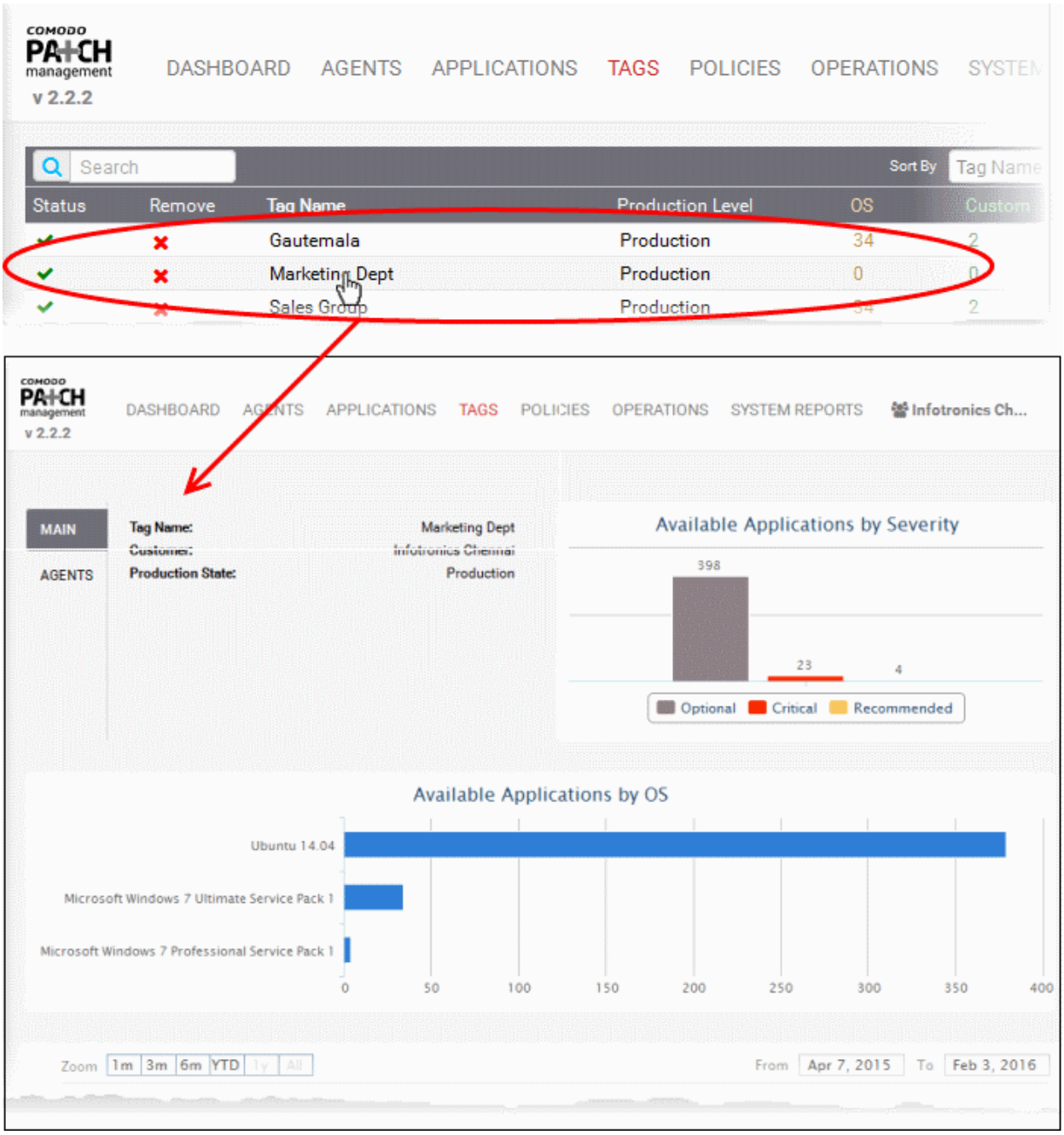
- Repeat the process to add more tags to the endpoint.
- To remove a tag, click 'X' beside the tag name.

For more details on the Endpoint Properties screen, refer to the section **Viewing Endpoint Details**.

6.2 View Details of a Tag

The patch management module can display detailed information about the scope of a tag. This includes the endpoints covered by the tag, a summary of OS and application patches which are available for installation and a time-line showing update history. In addition, administrators can initiate manual patch updates or remotely install/uninstall software for endpoints covered by the tag.

To open the tag detail page, click the name of any tag listed in the 'Tags' interface:



The interface contains the following areas. Each area is explained in detail after the list.

- **The Endpoints covered by the tag. If required, you can add more endpoints to the tag-group by placing your mouse-cursor anywhere in the endpoint details area at the top of the interface**.
- **The General Details of the tag and list of endpoints. You can restart endpoints from this area**.
- **Graphical Summaries of patches and applications available at the server for installation on to the group of endpoints**
- **List of OS updates, patches and third-party applications installed on the endpoints and the lists of OS patches, updates and custom third-party applications that are available for installation on to the endpoints by the patch management module.**

Endpoint Details Area

The text box at the top shows the member endpoints applied with the tag and form the group.

The administrator can add more endpoints to the group or remove the endpoints.

To add new endpoints to the group

- Click inside the endpoints text box
- A drop-down with the list of existing endpoints registered for the customer account will be displayed

- Choose the endpoint for adding it to the group
- Repeat the process for adding more endpoints

To remove the endpoint from a group

- Click the 'X' mark at the left of the group name

Tag Details Area

The Tag Details area provides the general details of the tag and the list of endpoints covered by the tag under respective tags. The administrator can restart individual endpoints or all the endpoints covered by the tag at once from this area.

Tab	Details Displayed
Main	The general details of the tag like the name, the customer account to which the tag pertains and the production level of the endpoints covered by the tag.
Agents	A list of endpoints covered by the tag. You can restart selected endpoints or all endpoints from this area. Refer to the **explanation below** for more details.

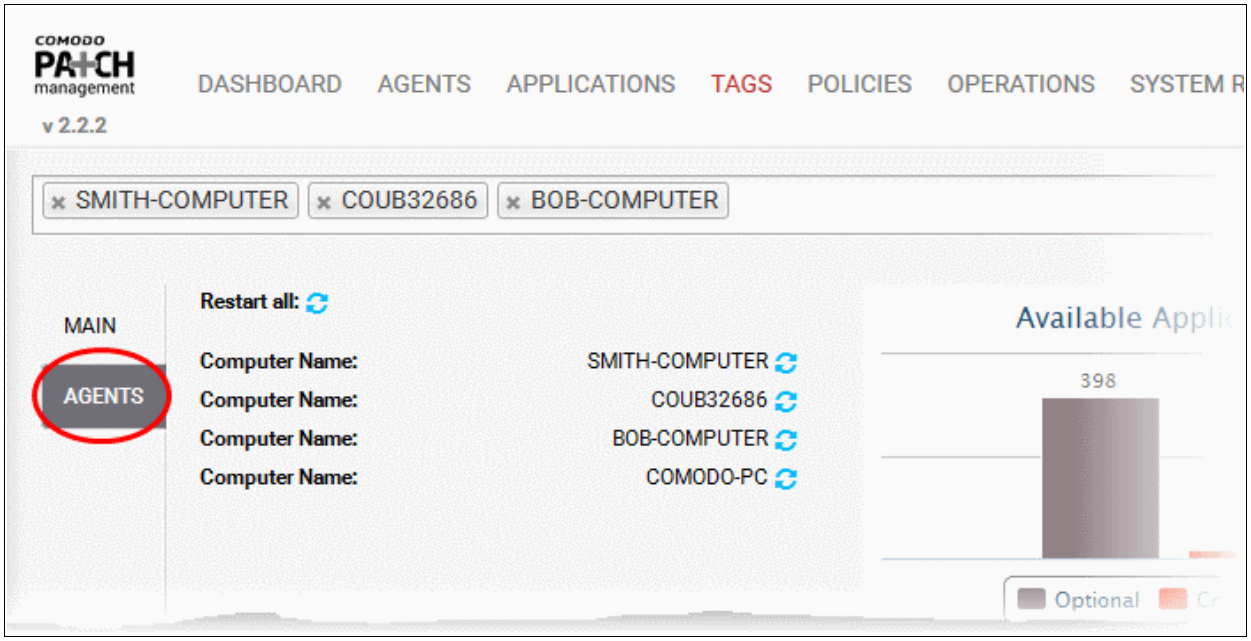
Restarting Endpoints

The Agents tab in the Tag details area allows the administrator to remotely restart the endpoints covered by a

specific tag. This is useful if you have installed a patch, an update or an application that takes effect after a manual restart of the endpoints. The endpoints will be restarted with a delay of one minute after confirmation.

To remotely restart the endpoint(s)

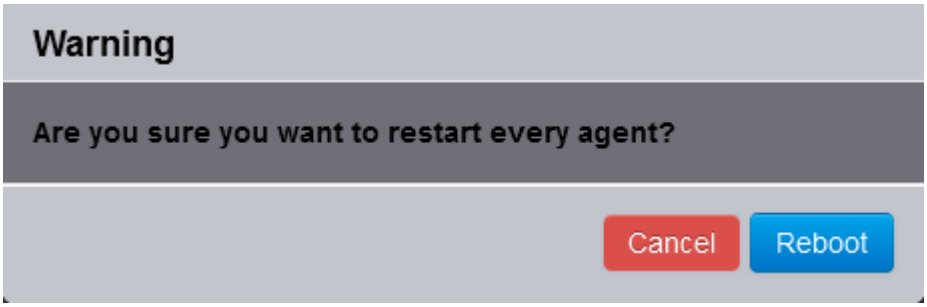
- Open the 'Tags' interface by clicking the 'Tags' tab
- Open the Tag Details interface for the selected tag by clicking on it from the 'Tags' interface.
- Select the 'Agents' tab at the 'Tag Details' area



The list of endpoints covered by the tag will be displayed.

- To restart selected endpoints click the icon beside the respective computer name
- To restart all the endpoints at once, click the icon beside 'Restart all'.

A confirmation dialog will appear, depending on whether you have chosen to restart a single or all endpoints.



- Click 'Reboot' in the confirmation dialog.

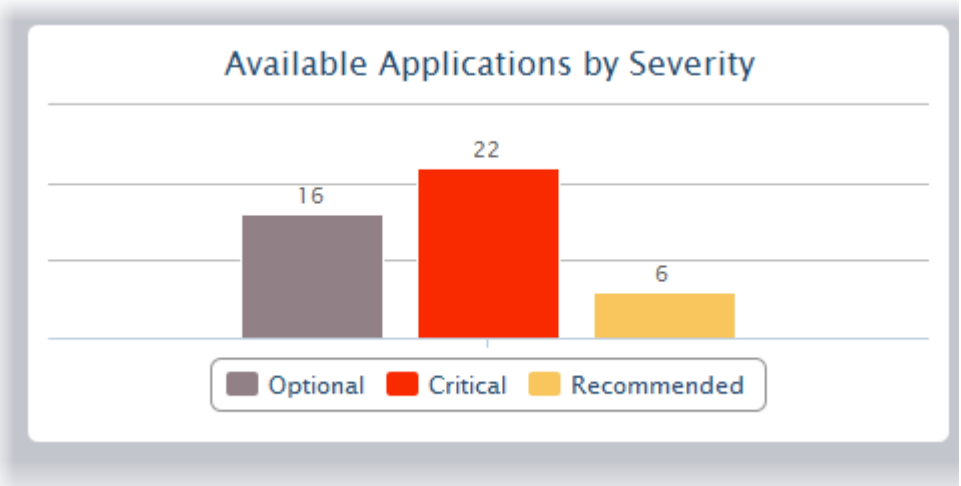
A message will be displayed to endpoint end-users asking them to save any work in progress as the machine will restart in 60 seconds.

Graphical Summary of Available Applications

The Tag Details interface displays the statistics of OS patches, updates and third-party applications that are available in the patch management server and are eligible for installation onto the endpoints covered by the tag, as bar charts.

Available Applications by Severity

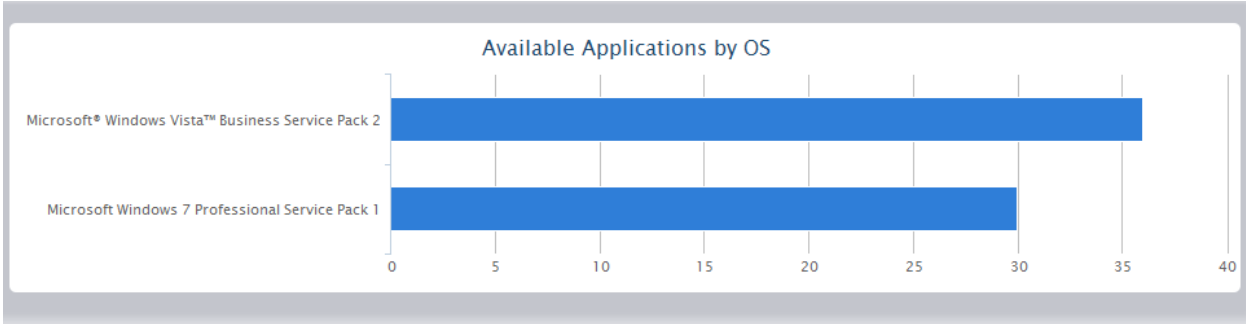
The bar chart displays the numbers of OS patches, updates and third-party applications based on their severity.



Hovering the mouse cursor over the bars displays the number of applications that fall under the selected severity level.

Available Applications by OS

The bar graph shows the consolidated number of items, applicable for the endpoints, based on their operating systems

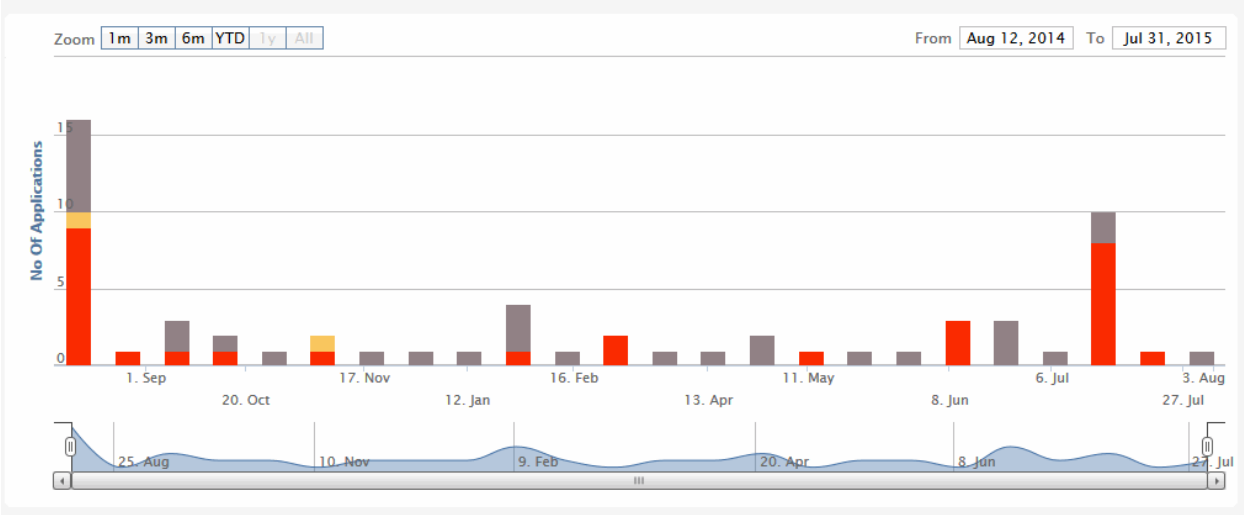


Hovering the mouse cursor over the bars displays the number of items applicable for the operating system.

Upload History

The Tag Details interface also displays a time-line chart showing the upload history of patches, updates and applications that are eligible for the endpoints. The bars are color coded to indicate the numbers of items of different severity levels.

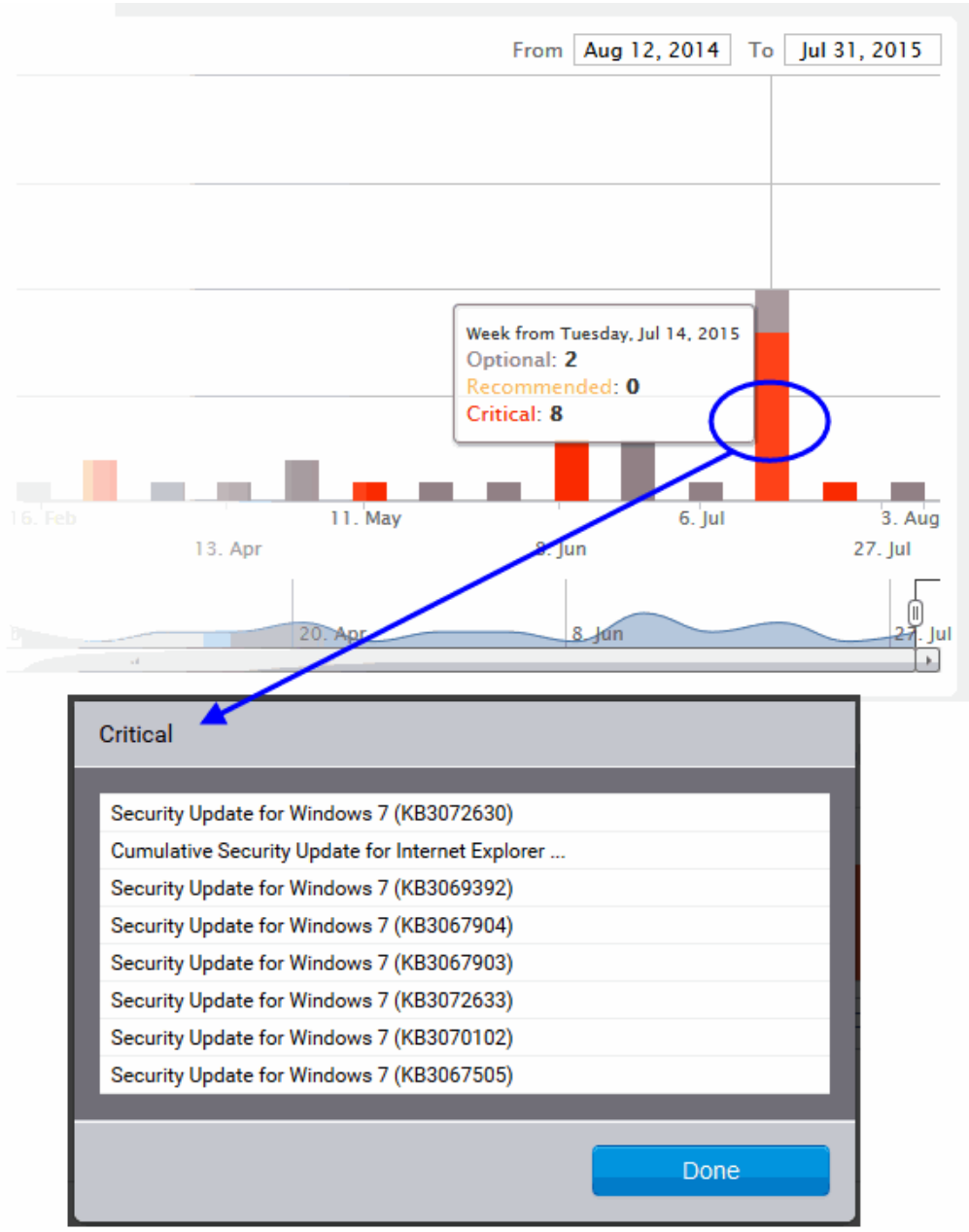
Red	-	Indicates the number of items of 'Critical' severity uploaded on that day
Yellow	-	Indicates the number of items of 'Recommended' severity uploaded on that day
Gray	-	Indicates the number of optional items uploaded on that day



The chart can be re-scaled to display the history for selected period by choosing the preset period options at the top left and further customized using the slider pointers at the bottom.

Hovering the mouse cursor over a bar displays the number of items uploaded on the selected day.

Clicking on a specific colored portion of the bar displays the list of items falling under the severity level, uploaded on that day.



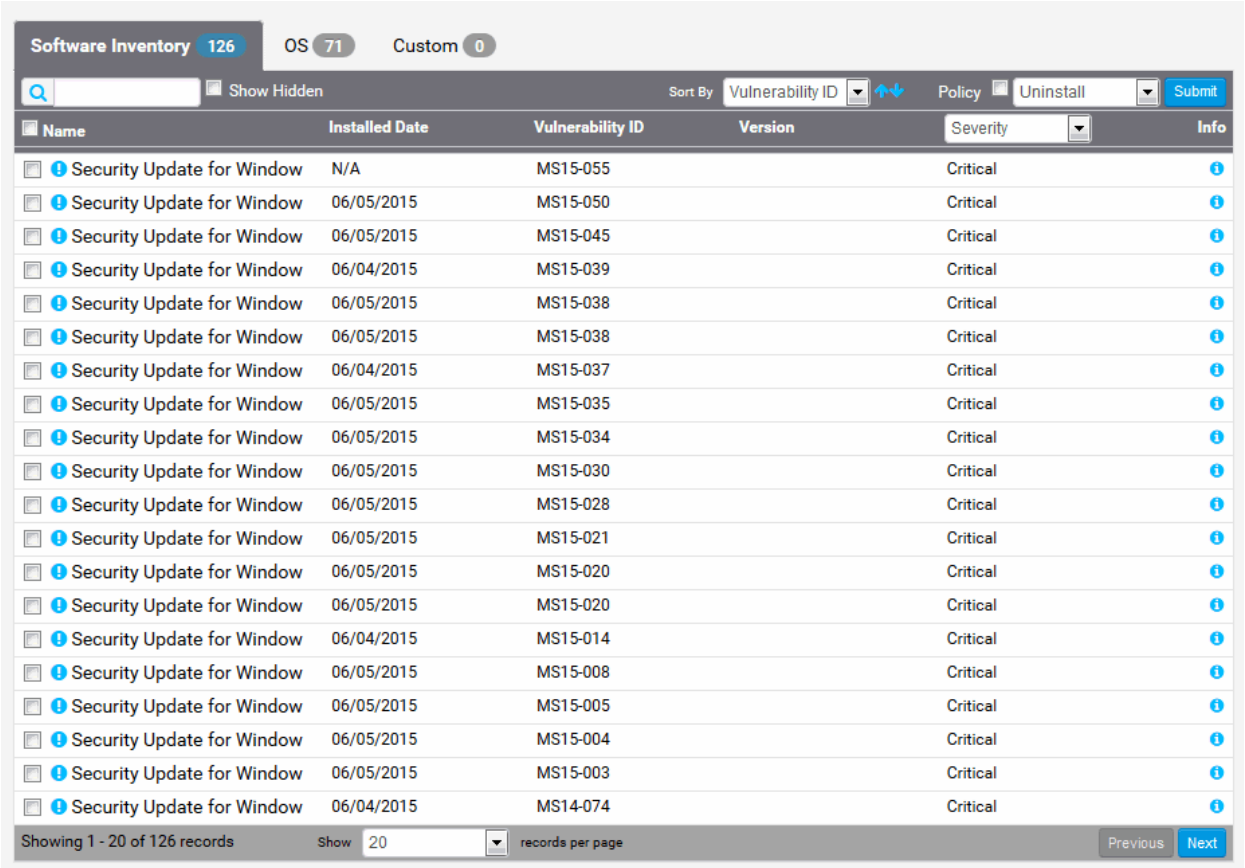
Clicking on an item name opens the 'Applications' interface displaying the complete details of the item, which also allows the administrator to install the item to selected endpoints. For more details on the Application Details interface, refer to the section **Viewing Details of a Patch, Update Package or an Application**.

The Inventory Area

The inventory list at the bottom of the interface displays:

- The list of OS update packages, patches and third-party applications that are installed at the endpoints covered by the tag
- The lists of OS updates, OS security patches and custom third-party applications that are available in the server for installation on to the endpoints.

The administrator can initiate a manual patch management or remote application installation/uninstallation operation on to all the endpoints covered by the tag at-once, from this area. For more details on remote patch management or application installation, refer to the section **Initiating Manual Update or Installation Operation for Group of Endpoints**.



The inventory area contains the following tabs:

- **Software Inventory** – Displays the consolidated list of all OS patches, OS updates, service packs and third-party applications that **have** been installed at the endpoints covered by the tag. The number at the tab indicates the total number of items listed. The administrator can remotely uninstall unwanted patches or OS update packages from the endpoints.

Note: For Windows computers, the patch management agent uses Windows API to query the OS database for the applications installed on it. Hence only those applications installed through the Windows installer will be listed in the 'Software Inventory' column. Applications that were installed using custom installers or using unconventional installation processes will not be displayed in the list.

- **OS** - Displays the list of OS update packages and security patches that are available at the patch management server and eligible for installation on to the endpoints depending on the operating systems of them. The number at the tab indicates the total number of items available. The administrator can remotely install these updates and patches on to the endpoint.
- **Custom** - Displays the list of custom and third-party applications that are available at the patch management server and compatible for installation on to the endpoints. The number at the tab indicates the number of applications available. The administrator can remotely install these applications on to the endpoint.

The Inventory table - Column Descriptions	
Column	**Description**
Name	The name of the update package/patch/application
Installed Date/Release Date	For Software Inventory - The date at which the item was installed at the endpoint For OS and Custom tabs - The date at which the item was released by the vendor

Vulnerability ID	The OS vulnerability addressed by the update or the patch
Version	The version number of the item
Severity	The severity level of the item. The possible severity levels are: • Critical • Recommended • Optional Selecting the Severity level from the drop-down filters the items that fall under the chosen category.
Info	Clicking the info icon opens the Applications interface and displays the details of the item. Refer to the section **Viewing Details of a Patch, Update Package or an Application** for more details.

Sorting, Filtering and Search options

Displaying Hidden Items

The patch management module allows the administrator to hide selected OS Update packages, OS patches or custom applications available from the Patch Management server, but are not required or reserved for specific endpoints. More details on hiding the items are available in the section **Managing OS Updates, Patches and Applications**.

Such hidden items are not displayed in the inventory lists in the Inventory area. If you want those hidden items to be displayed in the list, select the 'Show Hidden' checkbox.

Searching OS Updates or custom application

You can search for a specific OS Update package, OS patch or a custom application from the lists under the Inventory area.

- Switch to the respective tab
- Enter the name of the item in part or full in the Search text box and click the magnifier icon

Sorting the Items

You can sort the items in the ascending or descending order of different criteria like Application Name, Vulnerability ID or the Installed/Release Date.

- Switch to the respective tab
- Select the criteria from the 'Sort by' drop-down. The available options are:
  - Application Name
  - Installed/Release Date
  - Vulnerability ID
- Choose whether the entries are to be sorted on ascending or descending order by clicking the blue UP or Down blue arrow next to the drop-down

Filtering the Entries

You can filter the items based on the severity level.

- Switch to the respective tab
- Select the severity level from the drop-down at the 'Severity Level' column

Only the items that fall under the selected severity level will be displayed.

6.3 Initiate Manual Update or Installation Operation for Group of Endpoints

The 'Inventory' area at the bottom of the Tag Details interface displays lists of:

- OS Update packages, OS security patches, third-party update patches and custom third-party applications that have been installed at the endpoint
- OS Update packages, OS security patches, third-party update patches and custom third-party applications that are available at the Patch Management server and applicable for installation on to the endpoint.

The items are also indicated as Critical, Recommended or Optional based on their severity level.

The administrator can initiate a manual instant or scheduled patch uninstallation and patch/application installation operations on to the batch of endpoints covered by the tag from this area.

The following sections explain more on:

- **Uninstalling Security Patches, Updates or third party applications from the endpoints**
- **Installing Security Patches, Updates or third party applications from the server**

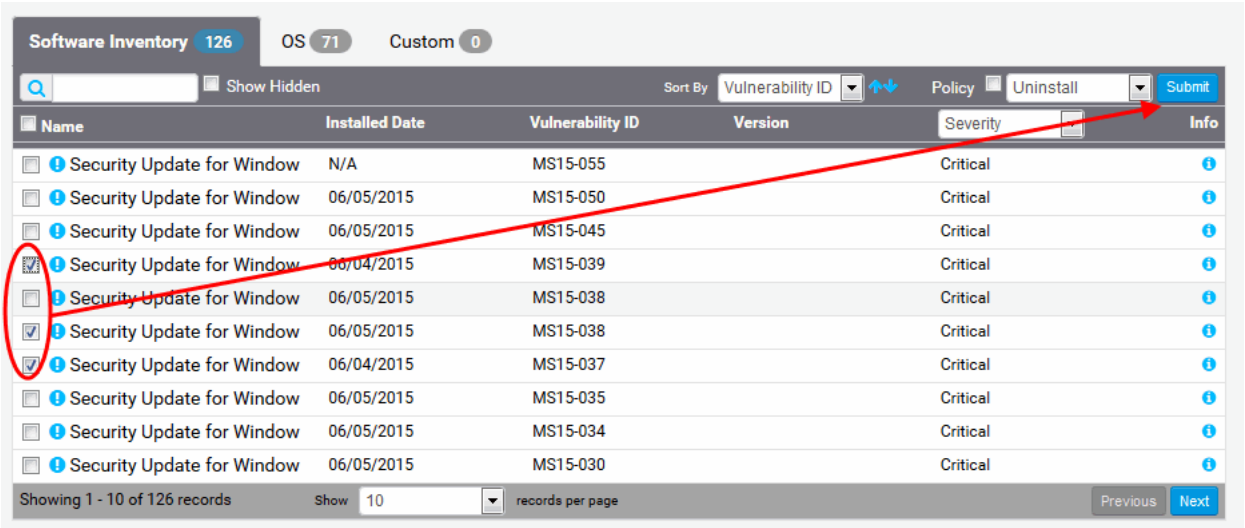
Uninstalling Patches or Update packages from the endpoints

The administrator can instantly uninstall selected OS patches or update packages or applications from the endpoints or create a schedule for the uninstallation.

Limitations: The Patch Management module allows you to uninstall only Patches and Updates or third-party applications that were installed from .msi or .msp installation packages, at the endpoint . You cannot uninstall any item installed using .exe installation package.

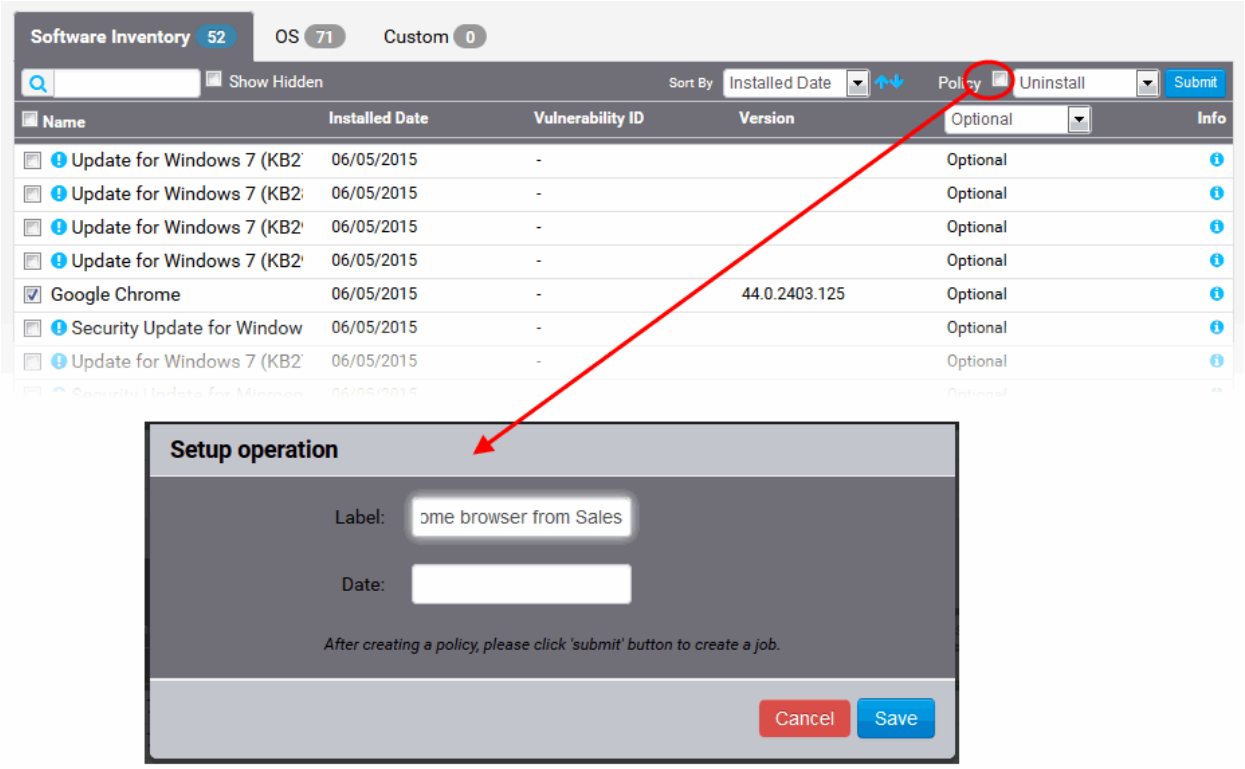
To uninstall the patches or update packages from the batch of endpoints

- Open the Tags interface by clicking the Tags tab
- Click on the selected tag from the list to open the Tag Details interface.
- Scroll down to the Inventory area and click the 'Software Inventory' tab
- Select the OS patch(es) or OS update(s) to be uninstalled. You can use the search and filter options to search for the specific patch(es)/update(s) to be uninstalled. Refer to the explanation on **Sorting, Filtering and Search Options** in the previous section **Viewing Details of a Tag** for more details
- To uninstall the item(s) instantly from all the endpoints covered by the tag, click the 'Submit' button



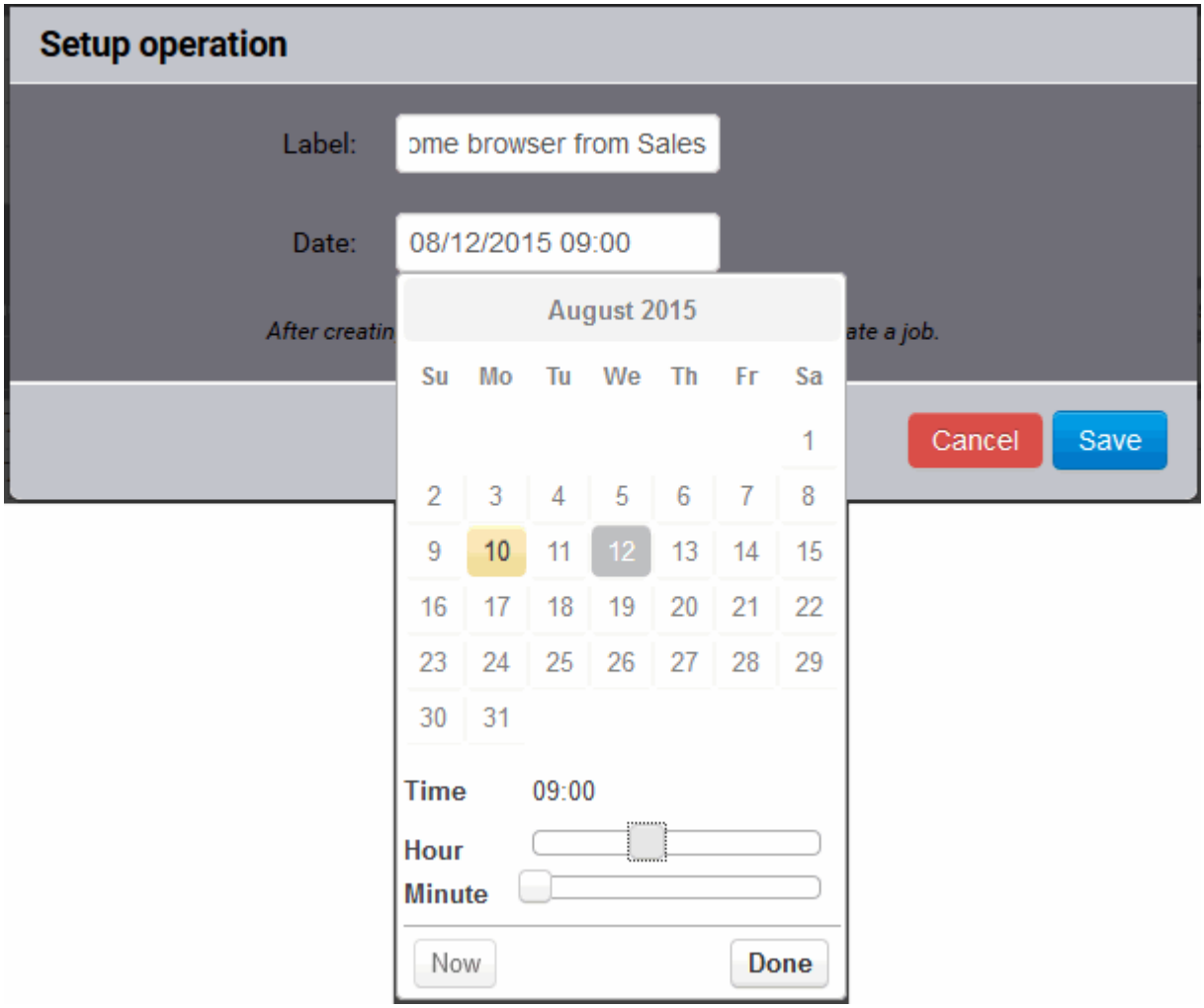
The uninstall operation command will be sent to the agents at the respective endpoints on which the item has been installed, from the group of them formed by the tag.

- To uninstall the item(s) at a scheduled time, select the 'Policy' checkbox



The 'Setup operation' dialog will appear to set the schedule.

- Enter a name for the uninstallation operation in the 'Label' text box
- Click the 'Date' text box to enter the time and date at which the selected patch(es) or update(s)are to be uninstalled. A calendar drop-down will appear.



- Select the date from the calendar
- Set the time using the Hour and Minute sliders
- Click 'Done'
- Click 'Save' from the 'Setup operation' dialog.

- Click 'Submit' from the Inventory area.

The uninstallation operation command will be sent to the agents at the respective endpoints on which the selected item has been installed at the scheduled time as chosen.

For an instant uninstallation operation, you can view the progress of the operation from the Operations interface.

- Click the Operations tab to open the Operations interface and click on the operation name.

For more details on viewing the details of the operation, refer to the section **Viewing Patch Management Operations**.

For a scheduled uninstallation operation, you can view the schedule displayed under the Policies tab.

The uninstallation operation will commence on the scheduled time.

For more details on managing scheduled operations, refer to the section **Automated Management Policies**.

Installing Patches, OS Updates or third party applications from the server

The administrator can instantly install OS patches/update packages or custom/third-party applications available from the server on to the batch of all the endpoints covered by the tag or create a schedule for the installation.

Limitations:

- For Security Patches and OS Update packages – The patch management module can install any patch or update which is auto-loaded to the server, on release by the OS vendor.
- For third-party applications and update patches - The patch management module can install any patch or application whose installation package is of the format as given below:
  - Windows - .exe, .msi, .msp, .msu
  - Ubuntu/Debian - .deb
  - CentOS - .rpm
  - Mac - .dmg

To install OS patches/update packages or an application

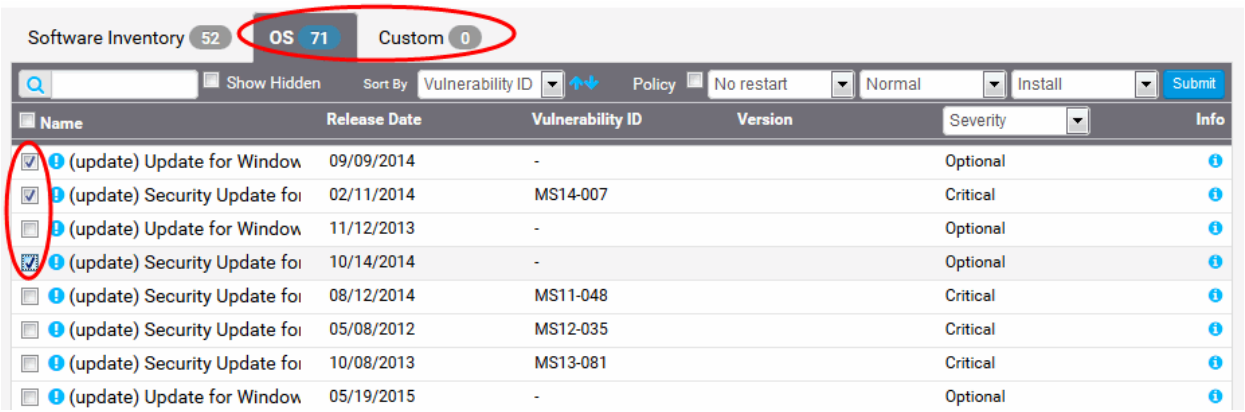
- Open the Tags interface by clicking the 'Tags' tab
- Click on the selected tag from the list to open the Tag Details interface.
- Select the items to be installed
  - To install OS patch(es) or updates, click the 'OS' tab
  - To install custom or third-party applications, select the 'Custom' tab
  - Select the item(s) to be installed. You can use the search and filter options to search for the specific patch(es)/update(s) or applications to be installed. Refer to the explanation on **Sorting, Filtering and Search Options** in the previous section **Viewing Details of a Tag** for more details
- Configure the installation options:

  Restart options – Select whether the endpoints need to be restarted for the installation to take effect, from the first drop-down at the top right. The options available are:

  - **No Restart** – The endpoints will not be restarted on completion of the installation operation. If the item(s) installed require the endpoint to be restarted for the installation to take effect, it will do so, only after the next manual restart of the respective endpoint by the end user.
  - **Only if needed** – The patch management module will check whether the item(s) installed require(s) the endpoint to be restarted for the installation to take effect. The endpoints will be restarted upon completion of installation only if it is required.
  - **Forced** – The endpoints will be restarted upon completion of installation operation, regardless of whether the items installed require(s) to do so, for the installation to take effect.

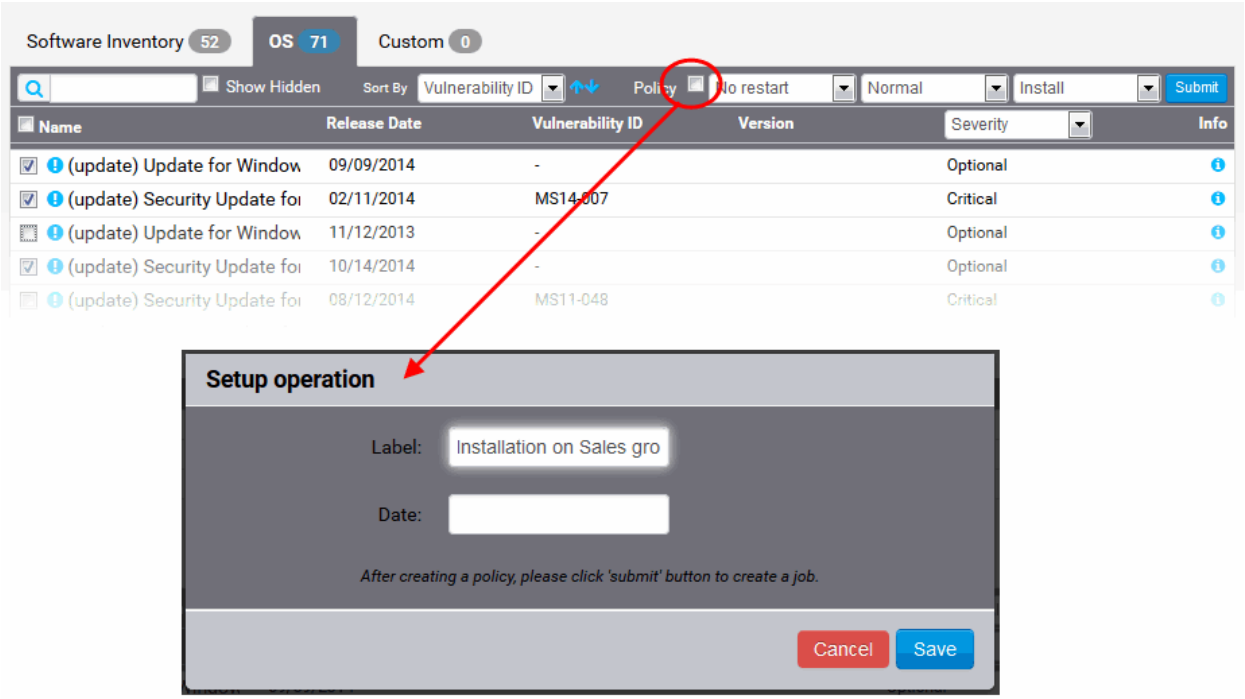
  Priority - Configure the execution priority for the installation operation at the endpoint from the next drop-down. The CPU usage for the installation operation will be set as per the chosen priority. The options available are:

  - Idle
  - Below Normal
  - Normal
  - Above Normal
  - High
- To install the item(s) instantly, click the 'Submit' button



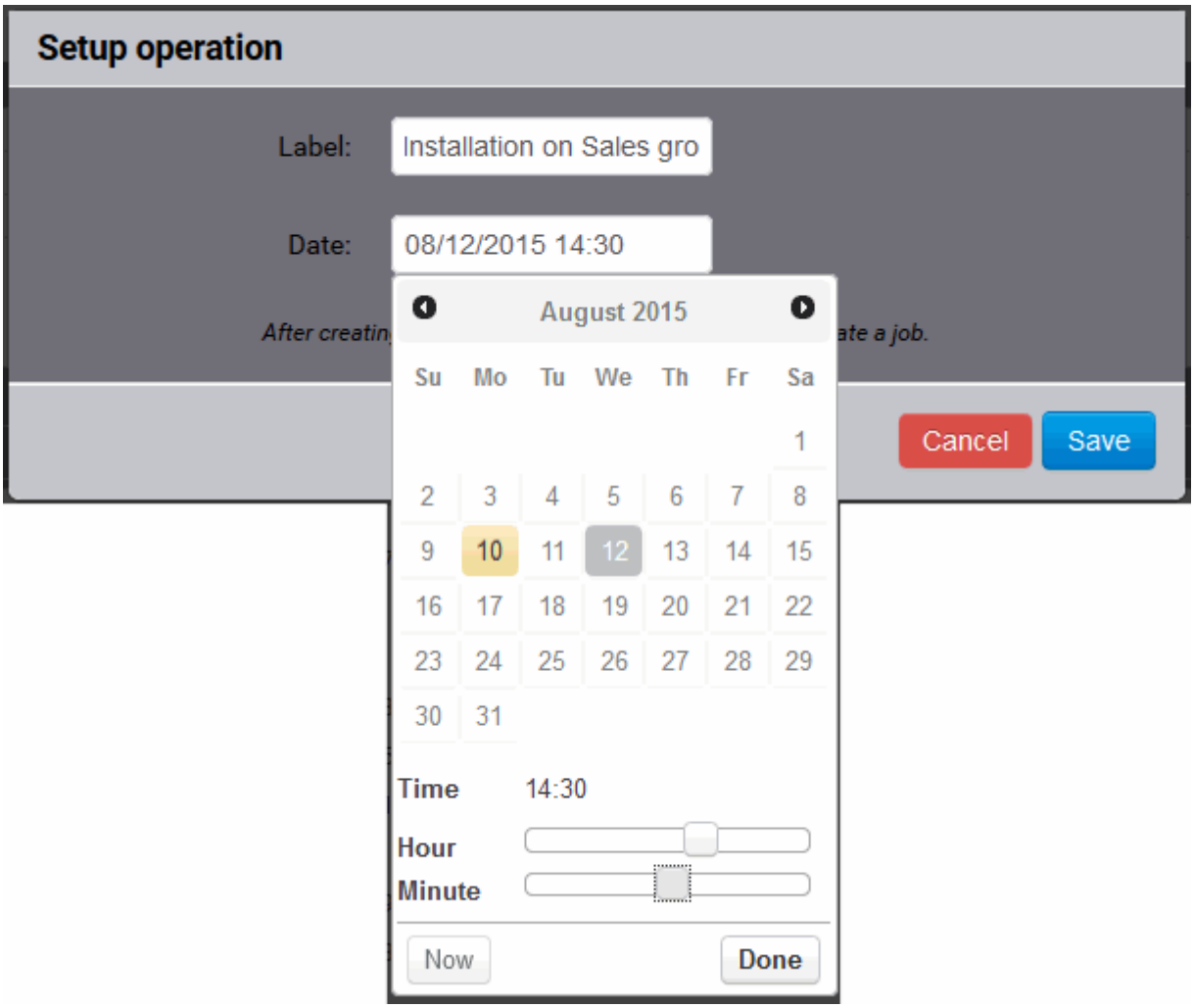
The installation operation command will be sent to the endpoints with operating systems and system requirements satisfying those of the item to be installed and covered by the tag.

- To install the item(s) at a scheduled time, select the 'Policy' checkbox



The 'Setup operation' dialog will appear to set the schedule.

- Enter a name for the installation operation in the Label text box
- Click the Date text box to enter the time and date at which the selected patch(es) or update(s)are to be installed. A calendar drop-down will appear.



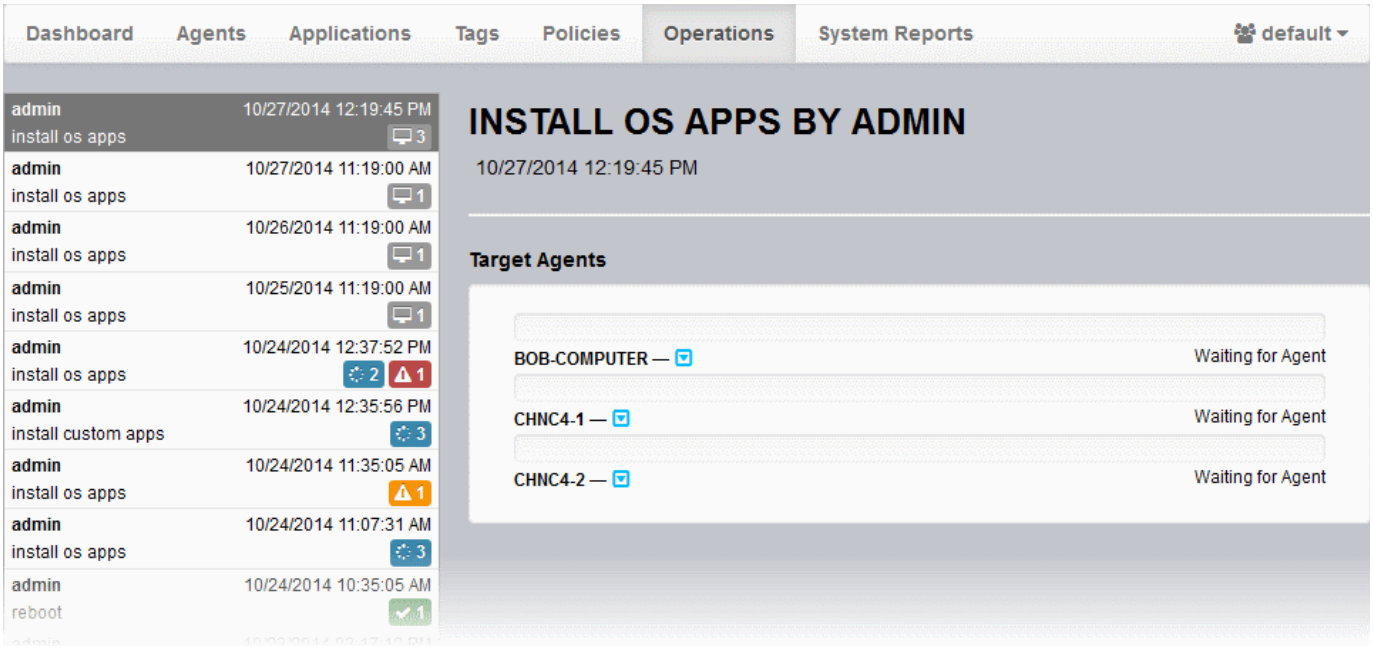
- Select the date from the calendar
- Set the time using the Hour and Minute sliders
- Click 'Done'
- Click 'Save' from the 'Setup operation' dialog.

- Click 'Submit' from the Inventory area.

The installation operation command will be sent to the endpoints with operating systems and system requirements satisfying those of the item to be installed and covered by the tag, at the time as specified in the schedule.

For an instant installation operation, you can view the progress of the operation from the 'Operations' interface.

- Click the 'Operations' tab to open the 'Operations' interface and click on the operation name.



For more details on viewing the details of the operation, refer to the section **Viewing Patch Management Operations**.

For a scheduled installation operation, you can view the schedule displayed under the 'Policies' tab.

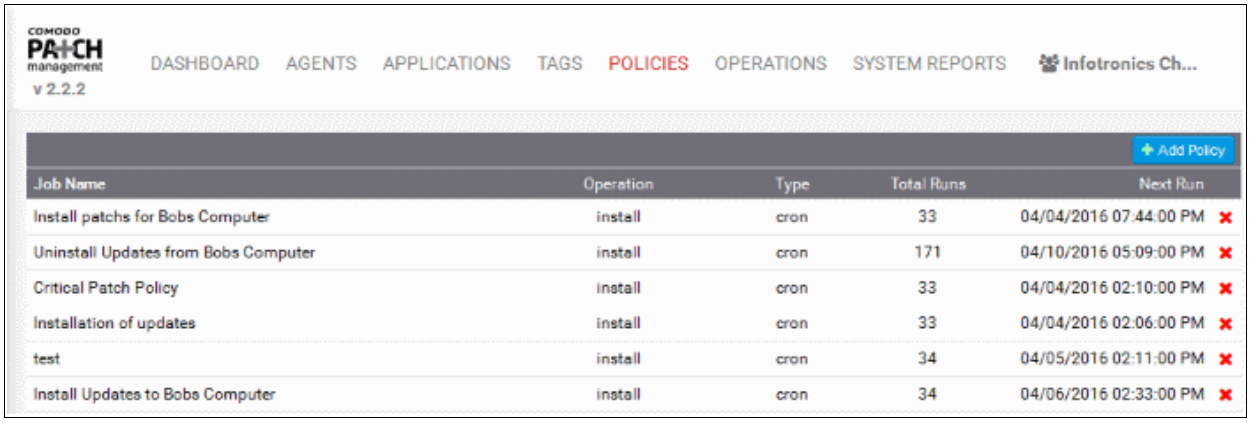
For more details on managing scheduled operations, refer to the section **Automated Patch Management Policies**.

7 Automated Patch Management Policies

The Patch Management module allows administrators to create policies to automatically apply patches to endpoints according to a specific schedule. Creating a policy will keeps selected endpoints up-to-date without the administrator intervention. Policies are constructed by specifying the type of patch (operating system or third-party), the schedule for the operation, the target endpoints and various other criteria such as patch severity. The patch management module uses 'Cron' to execute the policy commands.

Install and uninstall schedules which were created in the 'Endpoint Details' and 'Tag Details' interfaces will also be displayed in this interface as policies if the 'Policy' check-box was enabled.

The 'Policies' interface displays the list of current policies and allows you to create new policies:



Policies table - Column Descriptions	
Column	**Description**
Job Name	The name assigned o the policy, shortly describing the operation to be executed.
Operation	Indicates the type of operation carried out as per the schedule. The possible values are: • Install • Uninstall • Reboot
Type	Indicates whether the operation is executed to run periodically or one time. The possible values are: • Cron - The operation is executed repeatedly at periodical intervals as per the schedule. • Once - The operation is scheduled to be executed only once.
Total Runs	Indicates the number of times the operation has been executed so far, as per the schedule.
Next Run	Indicates the precise date and time of next execution of the operation.
Controls	Clicking the ✖ icon removes the policy from the patch management module.

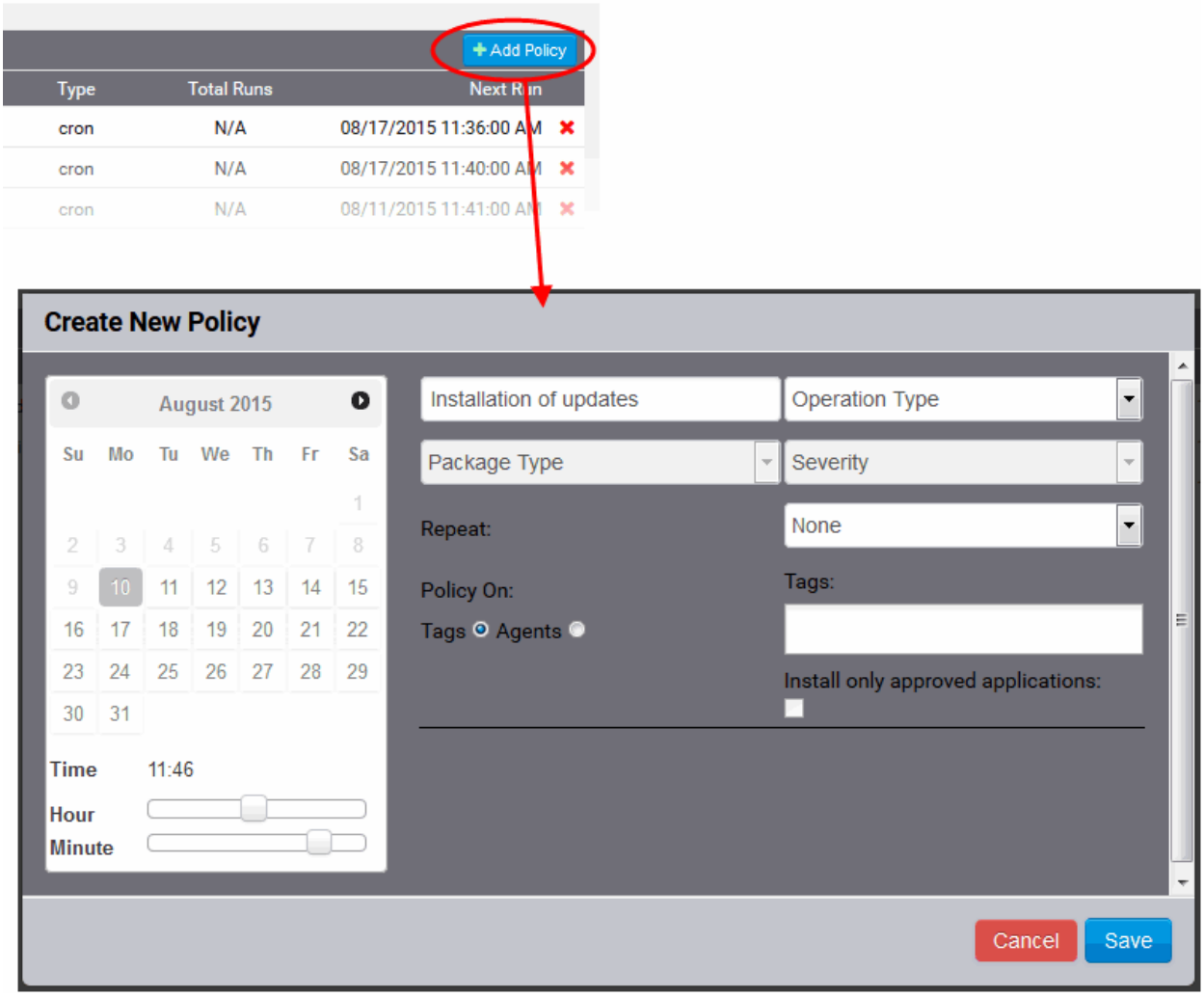
Refer to the following section **Creating a New Patch Management Policy** for more details.

7.1 Create a New Patch Management Policy

The administrator can create new patch management policies from the Policies interface for automatically and periodically install the patches and updates or third-party applications available from the patch management server on to individual endpoints or groups of endpoints covered by specific tags, registered for the selected customer account.

To add a new policy

- Select the customer account from the 'Customer Account' drop-down
- Open the policies interface by clicking the 'Policies' tab
- Click the 'Add Policy' button at the top right. The 'Create New Policy' dialog will open:



- Configure the parameters as shown below:

Create New Policy Dialog – Table of Parameters	
Parameter	**Description**
Policy Name	Enter a name shortly describing the operation to be executed as per the schedule.
Operation Type	Select the operation to be executed from the drop-down: • Install - Installs the OS patches/updates or third-party applications available from the server at the time of execution on to the selected endpoint(s), appropriate to their respective operating systems. • Reboot – Restarts the selected endpoints.
Package Type	Select the type of items to be installed from the drop-down, if you have chosen 'Install' as operation type: • OS - Installs the OS patches and update packages available from the server at the time of execution on to the selected endpoint(s), appropriate to their respective operating systems. • Custom - Installs the third-party applications available from the server at the time of execution on to the selected endpoint(s), appropriate to their respective operating systems.

	You can filter the items to be installed by choosing the severity level of them.
Severity	Select the severity level of items to be installed from the drop-down. • Any – Instals all the items • Optional – Installs only the optional items • Recommended – Installs only the recommended items • Critical - Installs only the items with 'Critical' severity level
Repeat	Choose the frequency at which the operation is to be performed: None – The operation will be executed only once on the date and time chosen from the calendar at the left. Choose the date from the calendar and time from the Hour and Minute sliders. Every day – The operation will be executed daily at the set time, starting from the date and time chosen from the calendar. Every week - The operation will be repeated weekly once on the day of the week same as that of the date chosen from the calendar, at the set time for the first execution . Every Month - The operation will be repeated monthly once on the day of the month same as that of the date and time chosen from the calendar for the first execution. Every Year - The operation will be repeated yearly once on the day of the year same as that of the date and time chosen from the calendar for the first execution. Custom – Repeats the operation at custom intervals. Refer to the **section below, explaining setting up the custom intervals**.
Policy On	Choose whether the operation is to be executed on selected endpoint(s) or group(s) of endpoints covered by specified tag(s). • Tags – On choosing Tags, click inside the Tags field at the right and select the tags that cover the endpoints upon which the items are to be installed from the drop-down. • Agents - On choosing Agents, click inside the Agents field at the right and select the Endpoints upon which the items are to be installed from the drop-down.
Install only approved applications	Selecting the checkbox installs only those items that are approved for automated installation from the 'Applications' interface. For more details on approving the items, refer the section **Approving Packages for Automated and Scheduled Installations**.

Setting Custom Intervals for Scheduled Patch Management Operation

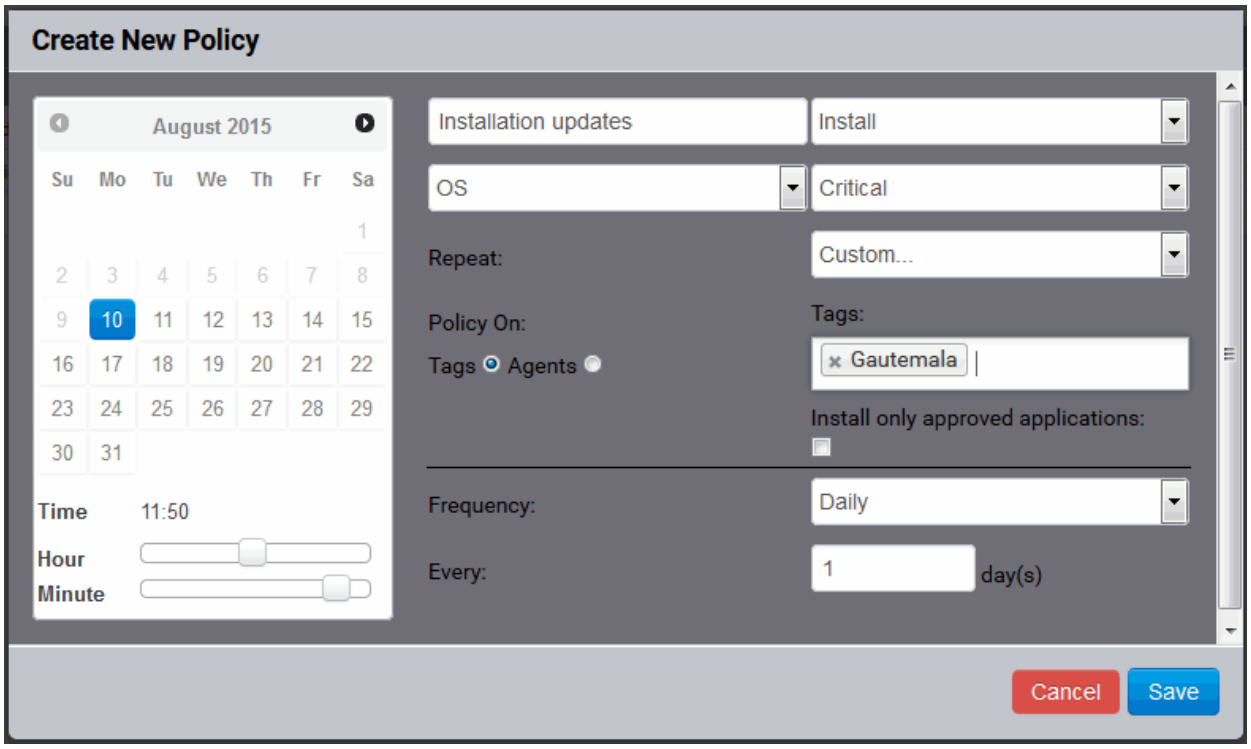
The administrator can also configure the policies to execute the operation repeatedly at custom time points. The schedule can be set to run the operation once in every:

- **'N' number of days** – The operation will be run once in on every N number of days at the set time
- **'N' number of weeks** - The operation will be run once in on every N number of weeks on the set weekdays at the set time.
- **'N' number of months** - The operation will be run once in on every N number of months on the set days at the set time.
- **'N' number of years** - - The operation will be run once in on every N number of years on the set dates at

the set time.

To set a schedule for the operation to run every 'N' number of days

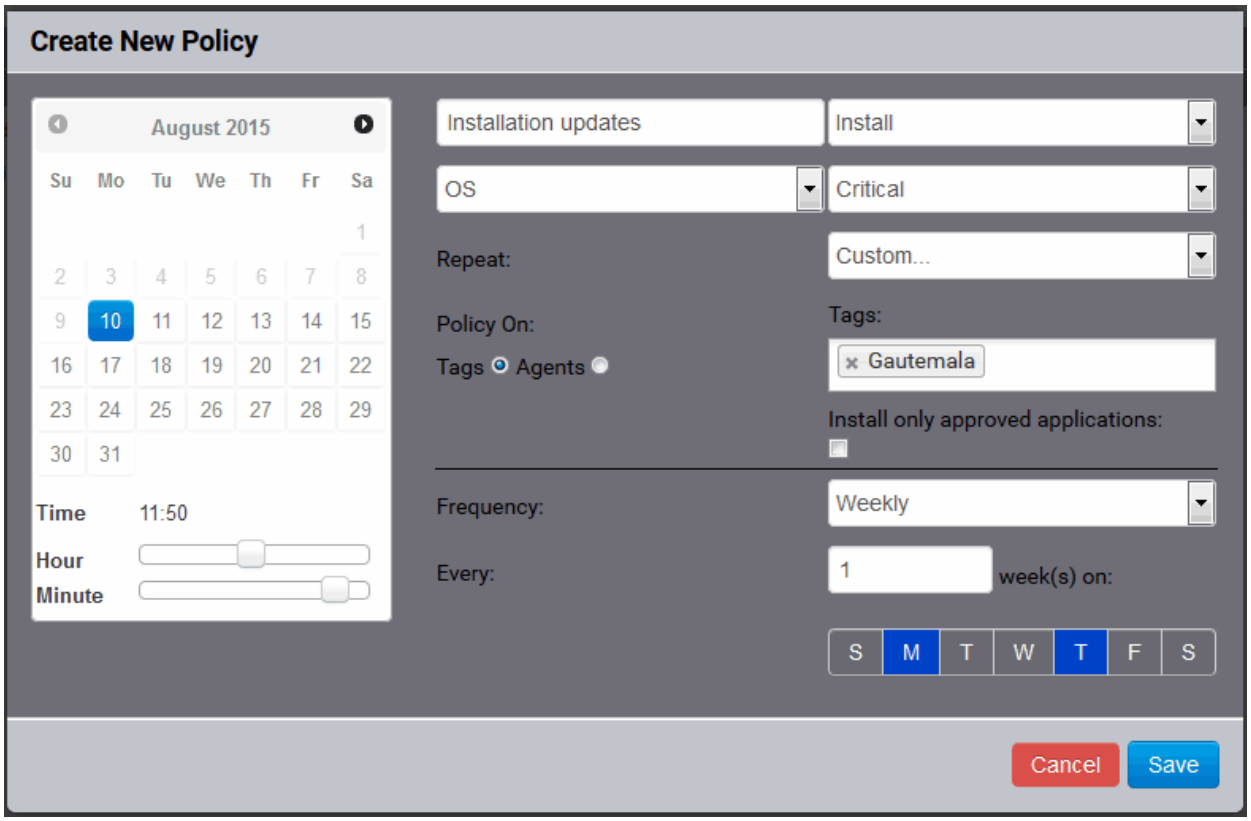
- Choose 'Custom' from the Repeat drop-down.



- Select 'Daily' from the 'Frequency' drop-down.
- Choose the number of days to be set as the interval from the Every drop-down.
- Set the time at which the operation is to be executed from the time slider at the left
- Click 'Save' from the 'Create New Policy' dialog

To set a schedule for the operation to run every 'N' number of weeks

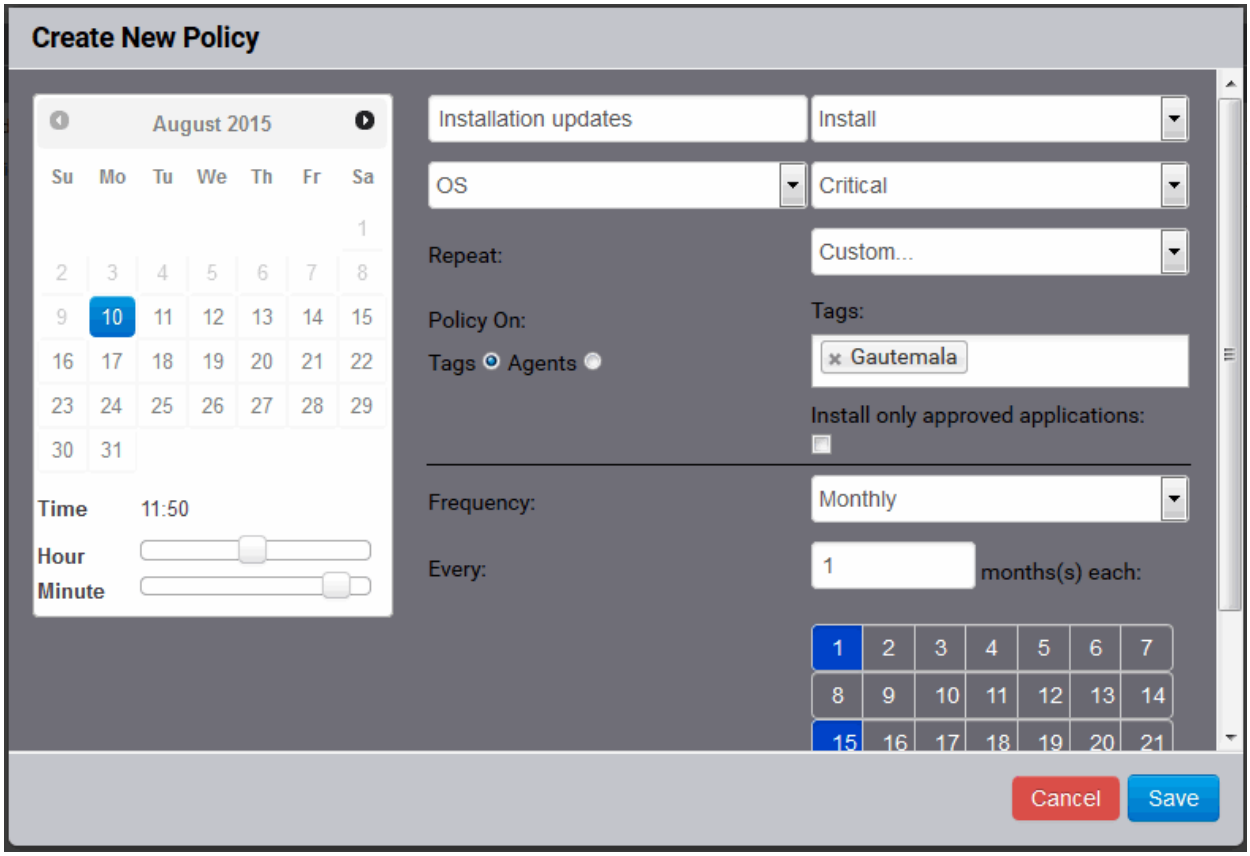
- Choose 'Custom' from the Repeat drop-down.
- Select 'Weekly' from the 'Frequency' drop-down.



- Choose the number of weeks to be set as the interval from the 'Every' drop-down.
- Select the days of the week from the days displayed below 'Every' drop-down.
- Set the time at which the operation is to be executed from the time slider at the left.
- Click 'Save' from the 'Create New Policy' dialog

To set a schedule for the operation to run every 'N' number of months

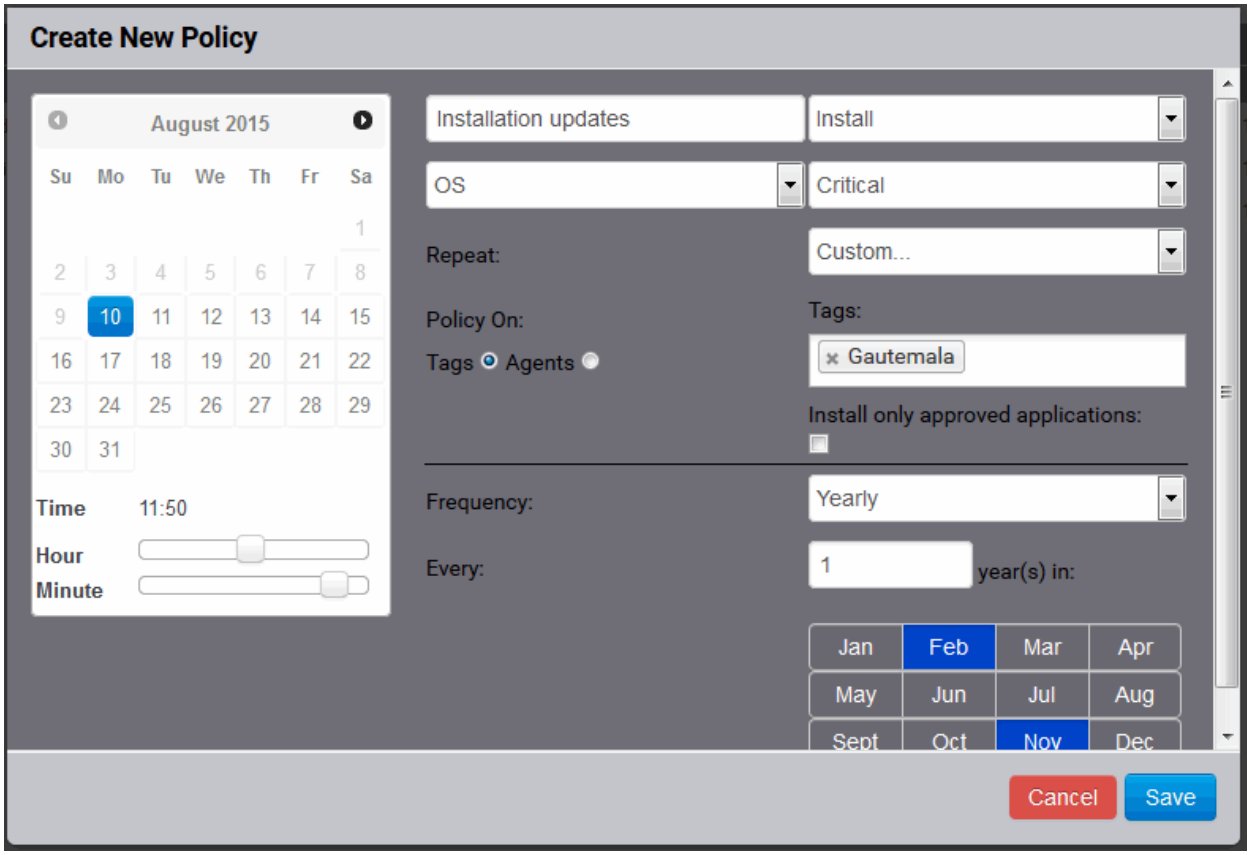
- Choose 'Custom' from the Repeat drop-down.
- Select 'Monthly' from the 'Frequency' drop-down.



- Choose the number of months to be set as the interval from the 'Every' drop-down.
- Select the days of the month from the month calendar displayed below 'Every' drop-down.
- Set the time at which the operation is to be executed from the time slider at the left.
- Click 'Save' from the 'Create New Policy' dialog

To set a schedule for the operation to run every 'N' number of years

- Choose 'Custom' from the Repeat drop-down.
- Select 'Yearly' from the 'Frequency' drop-down.

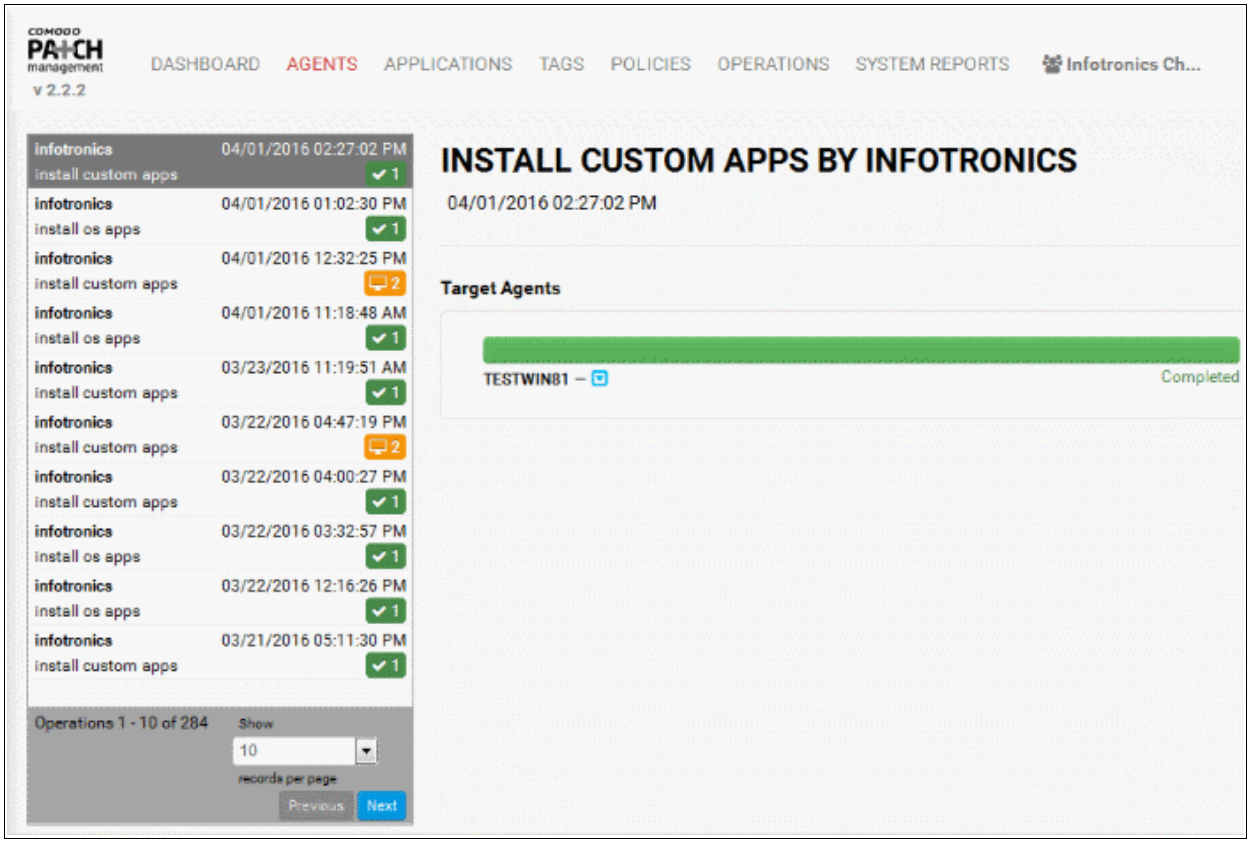


- Choose the number of years to be set as the interval from the 'Every' drop-down.
- Select the months from the months displayed below 'Every' drop-down.
- Set the day of the month(s) and the time at which the operation is to be executed from the calendar at the left.
- Click 'Save' from the 'Create New Policy' dialog

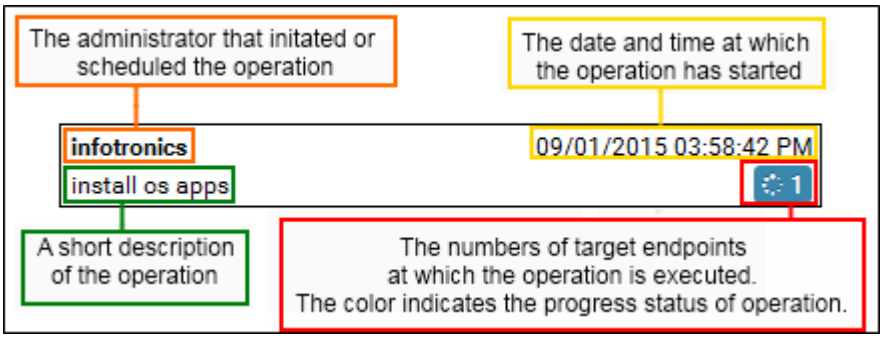
The schedule will be saved and the operation will be executed as per the schedule.

8 View Patch Management Operations

The Operations interface displays a list of currently running and completed operations initiated for the selected customer account. The list contains both manually initiated and scheduled operations. Administrators can also view details like the status of the operation on the target endpoints, items installed or uninstalled and more.



The left hand pane displays the list operations. The right hand side pane displays the details of the operation selected from the list.



Each item in the list has the following details:

- The username of the administrator that has manually initiated the operation or created the schedule for the operation
- The precise details of date and time at which the operation has started
- A short description of the operation. The possible values are:
  - Install OS apps
  - Install Custom apps
  - Uninstall
  - Reboot
- The numbers of target endpoints at which the operation is completed or being currently executed. The status of the operation is indicated by the background patch color of the number: The possible stages are:

✔ 3 - The operation is completed successfully.

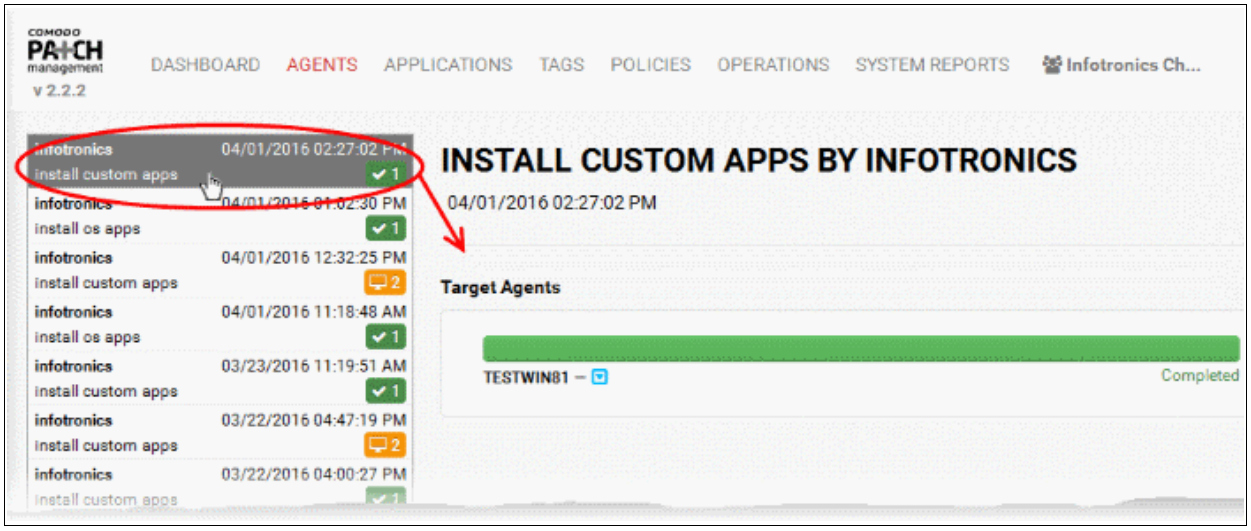
- The operation is completed but with some errors. You can view the list of errors from the details at the right hand side pane. Refer to the explanation under **Viewing Details of an Operation** for more details.
- The operation is not completed. You can view the error message from the details at the right hand side pane. Refer to the explanation under **Viewing Details of an Operation** for more details.
- The operation is under progress. You can view the progress bar at the details at the right hand side pane. Refer to the explanation under **Viewing Details of an Operation** for more details.
- Waiting for the agent to receive the operation command.

Viewing Details of an Operation

Clicking an operation in the list on the left will display operation details on the right. The details pane lists the target endpoints and the progress status of the operation. The administrator can also view the list of items being installed at any endpoint.

To view the details of an operation

- Select the customer account from the 'Customer Account' drop-down
- Open the operations interface by clicking the 'Operations' tab
- Click on the selected operation from the list at the left hand side. The details pane will open in the right hand side:



The details pane displays a list of target endpoints and the status of the operation at each endpoint.

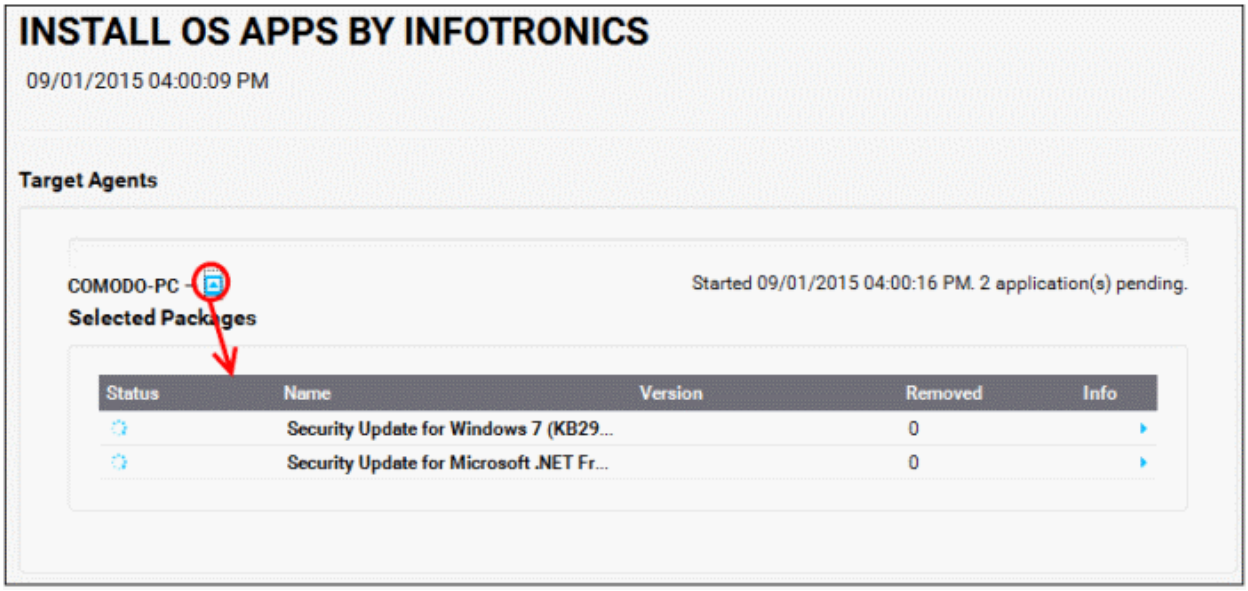
Clicking an endpoint name opens the Endpoint Details interface for that endpoint. For more details on the interface, refer to the section **Viewing Endpoint Details**.

This interface allows you to:

- **View the list of packages being installed and their status**
- **View the error messages for operations not completed successfully**
- **View the error messages for operations that are completed, but with errors**

To view the list of packages being installed on an endpoint and their status

- Click the blue drop-down beside the endpoint name. The list of items selected for installation on to the endpoint, based on the OS of it, will be displayed:

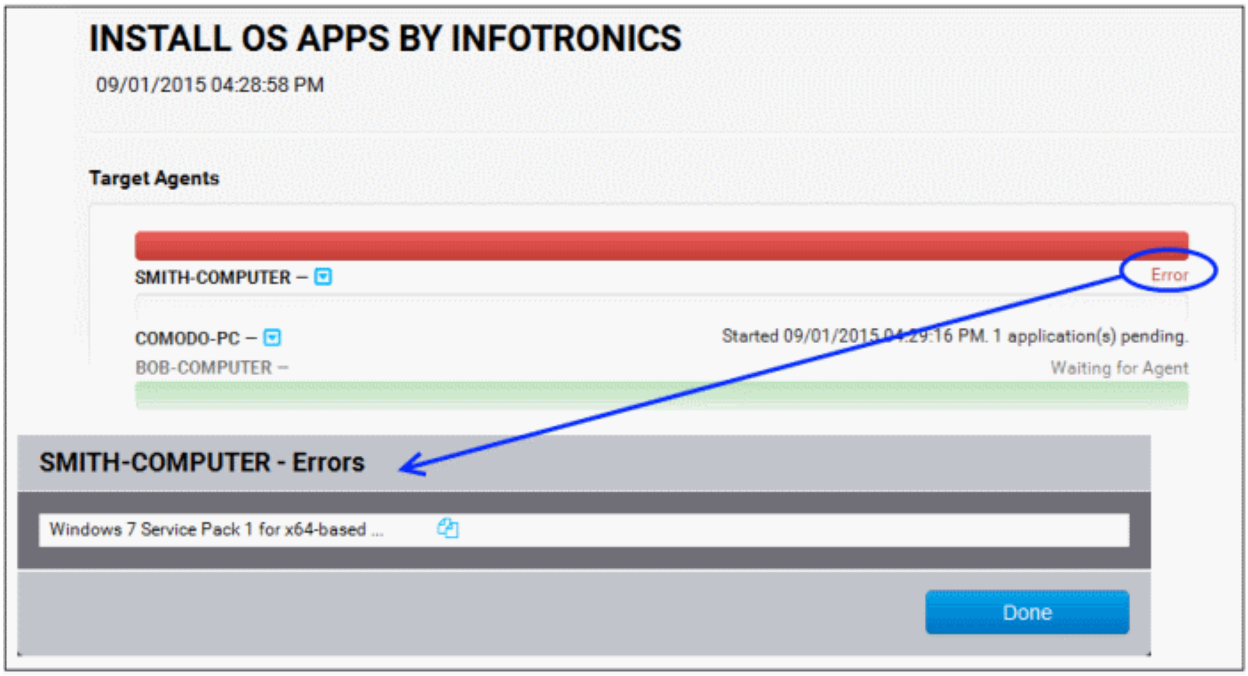


- Clicking a package name opens the Application Details interface, displaying the details of the OS patch/update package or the application. For more details on the application details interface, refer to the section **Viewing Details of a Patch, Update Package or an Application**.

Note: The blue-drop down will appear only for endpoints that is eligible for the packages installed. If you are installing a package by selecting a tag, the package will be installed only on to the applicable endpoints covered by the tag and the drop-down will appear only for those endpoints.

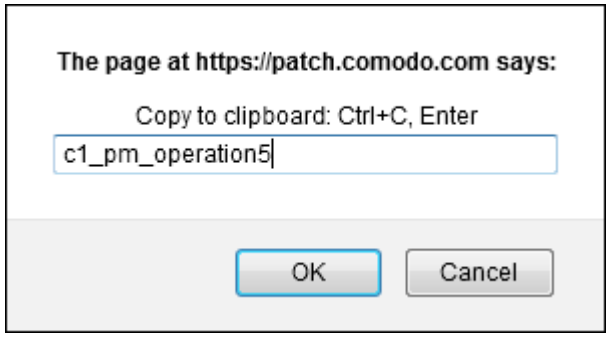
To view the error messages for operations not completed successfully

- Open the Operation Details pane of the operation not completed successfully by clicking on it from the list
- Click on the 'Error' link at the right end, for the endpoint you wish to see the error details.



The list of applications that failed to install and the reasons for failure is displayed.

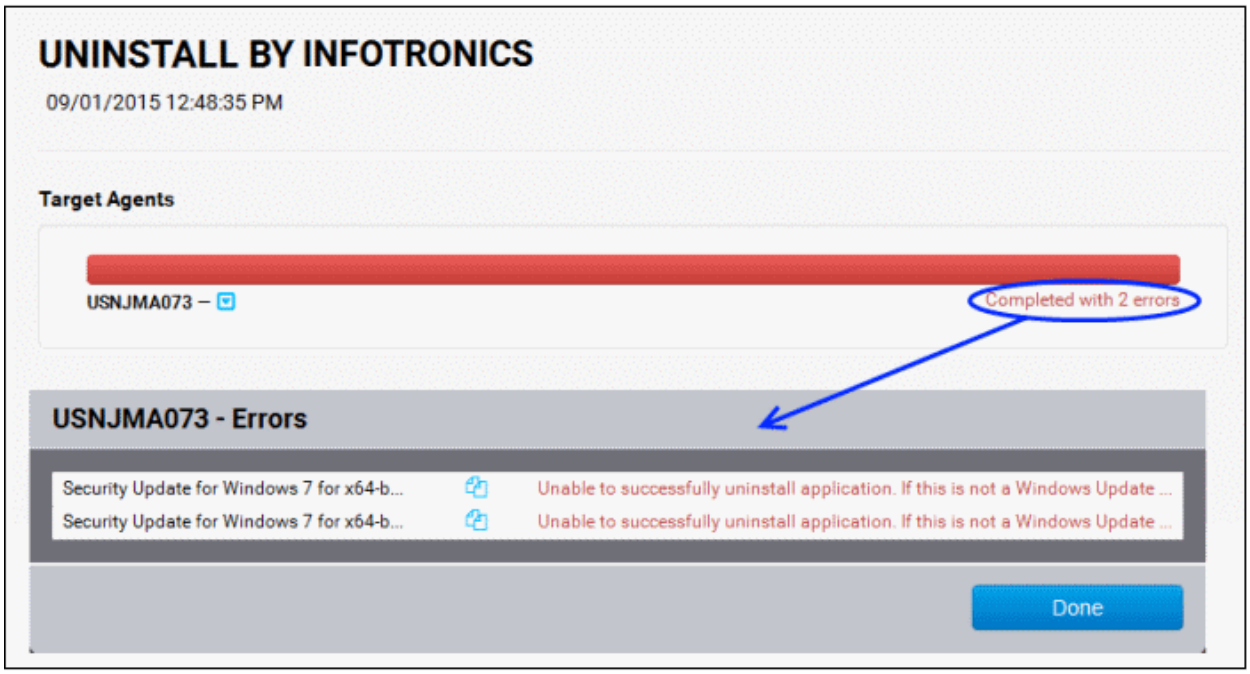
Clicking the copy icon opens a dialog that enables you to copy the error message to your clipboard for pasting to your document or text files.



- Press CTRL+C from the keyboard or right click inside the text box and choose 'Copy' from the context sensitive menu to copy the error message to the clipboard.

To view the error messages for operations that are completed with errors

- Open the Operation Details pane of the operation completed but with errors (indicated by yellow triangle) by clicking on it from the list
- Click on the 'Completed with 'N' errors' link at the right end, for the endpoint you wish to see the error details.



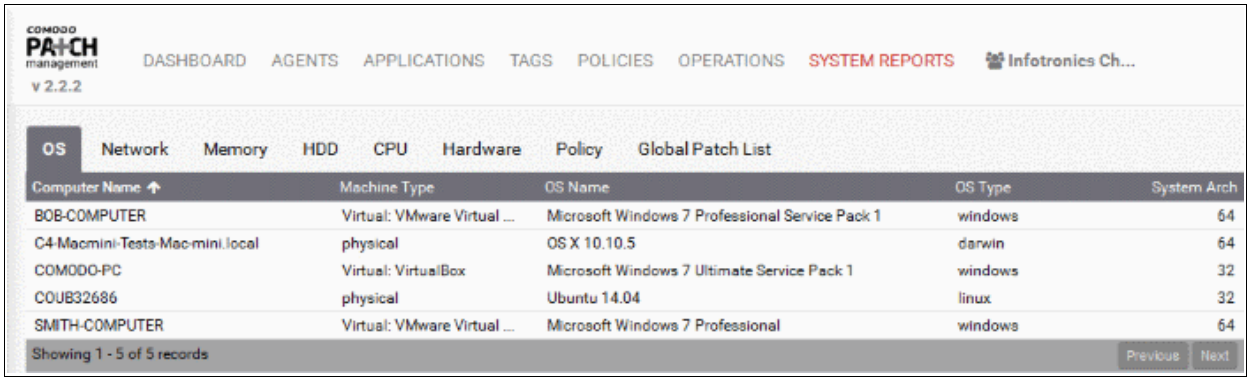
The list of applications that failed to uninstall and the reasons for failure is displayed.

Clicking the copy icon opens a dialog that enables you to copy the error message to your clipboard for pasting to your document or text files.

- Press Ctrl+C from the keyboard or right click inside the text box and choose 'Copy' from the context sensitive menu to copy the error message to the clipboard.

9 View Endpoint Report Summaries

The 'System Reports' interface displays summaries of hardware/software/network details for each endpoint registered for the customer account. It also displays the patch management policies active for the customer and an exhaustive list of available OS patches and updates with details of endpoints affected by them.



The Interface contains the following tabs:

- **OS**
- **Network**
- **Memory**
- **HDD**
- **CPU**
- **Hardware**
- **Policy**
- **Global Patch List**

Operating System

The OS tab displays the details of operating system of each endpoint added to the customer account.

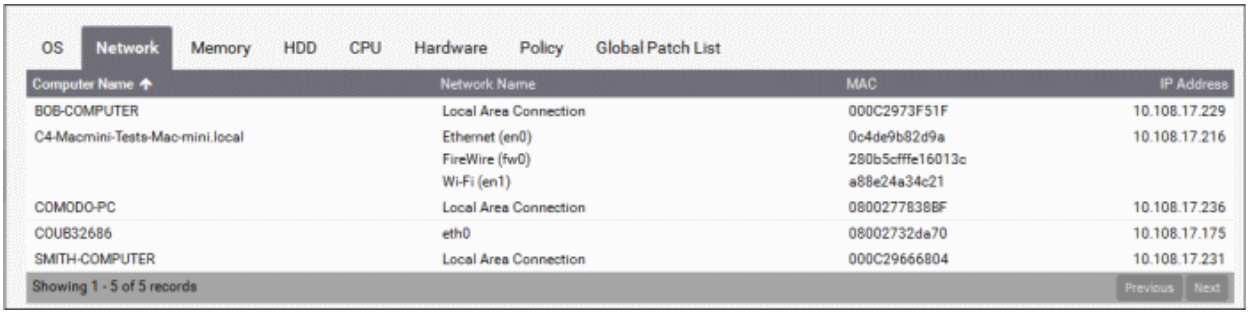
OS table - Column Descriptions	
Column	**Description**
Computer Name	The 'Display name' of the endpoint. If a display name is not assigned for the endpoint, its host name is displayed. Refer to the explanation of **editing display name of an endpoint** in the section **Viewing Endpoint Details** for more details on assigning the display names.
Machine Type	Indicates whether the endpoint is a physical computer or a virtual machine.
OS Name	Displays the OS installed on the endpoint with its version number and service pack details.
OS Type	Displays the base code of the OS.
System Arch	Indicates the bit architecture of the endpoint, whether the system is 64-bit or 32-bit based.

Sorting Options:

You can sort alphabetically in ascending or descending order by clicking the arrow next to 'Computer Name' in the table header.

Network Details

The Network tab displays information about the networks to which each endpoints is connected. This includes the type of network and the MAC and IP addresses of the endpoint.



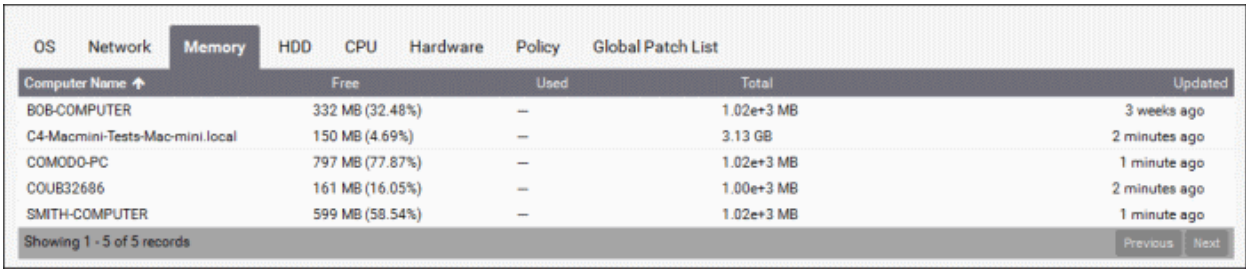
Network table - Column Descriptions	
Column	**Description**
Computer Name	The 'Display name' of the endpoint. If a display name is not assigned for the endpoint, its host name is displayed. Refer to the explanation of **editing display name of an endpoint** in the section **Viewing Endpoint Details** for more details on assigning the display names.
Network Name	Displays the network(s) to which the endpoint is connected.
MAC	Displays the MAC address of the endpoint.
IP Address	Displays the IP address of the endpoint with respect to each network..

Sorting Options:

You can sort alphabetically in ascending or descending order by clicking the arrow next to 'Computer Name' in the table header.

Memory Details

The Memory tab displays the size of the system memory (RAM) mounted on each endpoint and the current usage statistics of it.



Memory Details table - Column Descriptions	
Column	**Description**
Computer Name	The 'Display name' of the endpoint. If a display name is not assigned for the endpoint, its host name is displayed. Refer to the explanation of **editing display name of an**

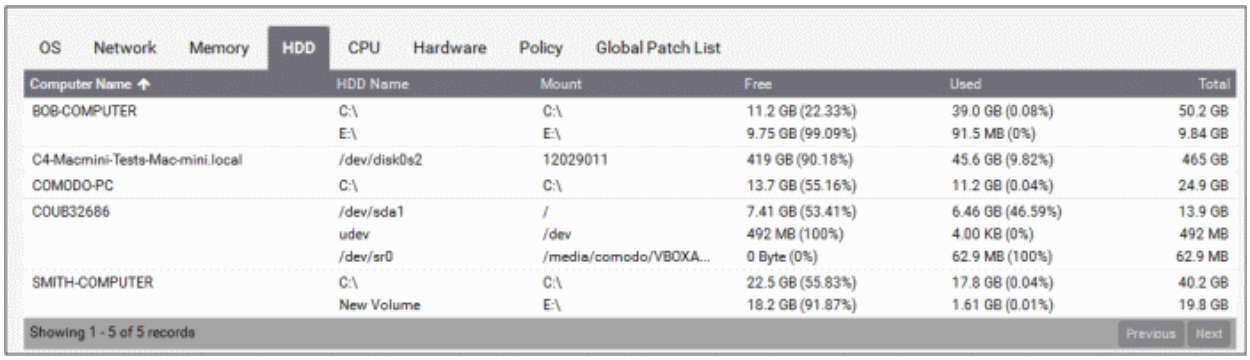
	endpoint in the section **Viewing Endpoint Details** for more details on assigning the display names.
Free	Displays the size of free memory available at the endpoint.
Used	Displays the size of memory used at the endpoint.
Total	Displays the total size of system memory mounted in the endpoint.
Updated	Indicates the last update time of the memory usage statistics.

Sorting Options:

You can sort alphabetically in ascending or descending order by clicking the arrow next to 'Computer Name' in the table header.

Storage Details

The HDD tab displays the details of the hard disk drive mounted on each endpoint and the current usage statistics of it.



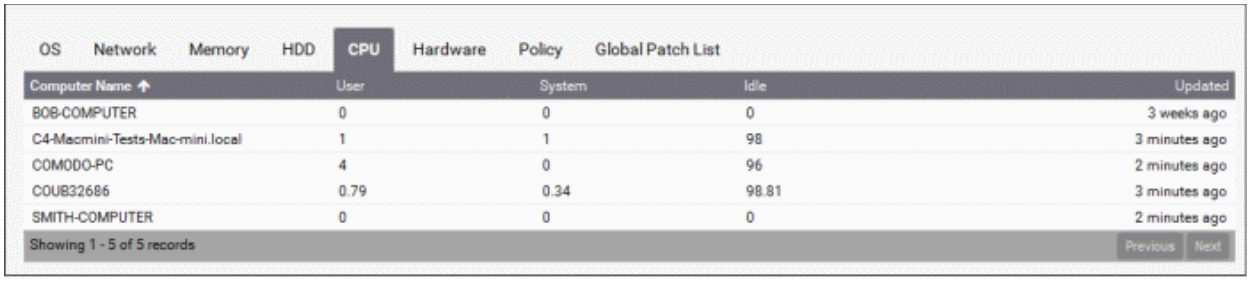
HDD Details table - Column Descriptions	
Column	**Description**
Computer Name	The 'Display name' of the endpoint. If a display name is not assigned for the endpoint, its host name is displayed. Refer to the explanation of **editing display name of an endpoint** in the section **Viewing Endpoint Details** for more details on assigning the display names.
HDD Name	Displays the details of hard disk drive partitions at the endpoint.
Mount	Displays all the drive partitions, including network drives mounted on the endpoint.
Free	Displays the size of free HDD space available at the endpoint
Used	Displays the size of used HDD space
Total	Displays the total size of HDD mounted on the endpoint.

Sorting Options:

You can sort alphabetically in ascending or descending order by clicking the arrow next to 'Computer Name' in the table header.

CPU Details

The CPU tab displays the details of the CPU usage (in percentage), by user initiated and system initiated processes.



CPU Details table - Column Descriptions	
Column	**Description**
Computer Name	The 'Display name' of the endpoint. If a display name is not assigned for the endpoint, its host name is displayed. Refer to the explanation of **editing display name of an endpoint** in the section **Viewing Endpoint Details** for more details on assigning the display names.
User	Displays the CPU usage (in percentage) by user initiated processes, running in the user space.
System	Displays the CPU usage (in percentage) by system initiated processes, running in the kernel space.
Free	Displays the unused CPU capacity.
Updated	Indicates the last update time of the CPU usage statistics.

Sorting Options:

You can sort alphabetically in ascending or descending order by clicking the arrow next to 'Computer Name' in the table header.

Hardware Details

The Hardware tab displays information on basic hardware components like HDD, CPU, Display and RAM in each endpoint.

OS | Network | Memory | HDD | CPU | Hardware | Policy | Global Patch List

Computer Name	Component	Name	Size	File System/Cores	Speed (Mhz)/Free size	Arch
BOB-COMPUTER	Disk	E:	9.84 GB	NTFS	9.75 GB	
	CPU	Intel(R) Core(TM) i3 CPU ...	256 kb	2	3059	64
	Display	Standard VGA Graphics ...	NaN und...			
	RAM		1.00 GB			
C4-Macmini-Tests-Mac-m...	Disk	/dev/disk0s2	465 GB	hfs	419 GB	
	CPU	Intel Core i5	3072 kb	2	2560	
	Display	No CPU info available				
	RAM		4.00 GB			
COMODO-PC	Disk	C:	24.9 GB	NTFS	13.8 GB	
	CPU	Intel(R) Core(TM) i3-2120...	null kb	1	3281	32
	Display	Standard VGA Graphics ...	NaN und...			
	RAM		0 Byte			
COUB32686	Disk	/dev/sda1 udev /dev/sr0	13.9 GB 492 MB 62.9 MB	ext4 devtmpfs iso9660	7.10 GB 492 MB 0 Byte	
	CPU	Intel(R) Core(TM) i3-2120...	6144 kb	1	3294.403	32
	Display	InnoTek Systemberatung...	16.0 MB		0	
	RAM		1.00e+3 MB			
SMITH-COMPUTER	Disk	New Volume	19.8 GB	NTFS	18.2 GB	
	CPU	Intel(R) Core(TM) i3 CPU ...	256 kb	1	3059	64
	Display	Standard VGA Graphics ...	NaN und...			
	RAM		1.00 GB			

Showing 1 - 5 of 5 records | Previous | Next

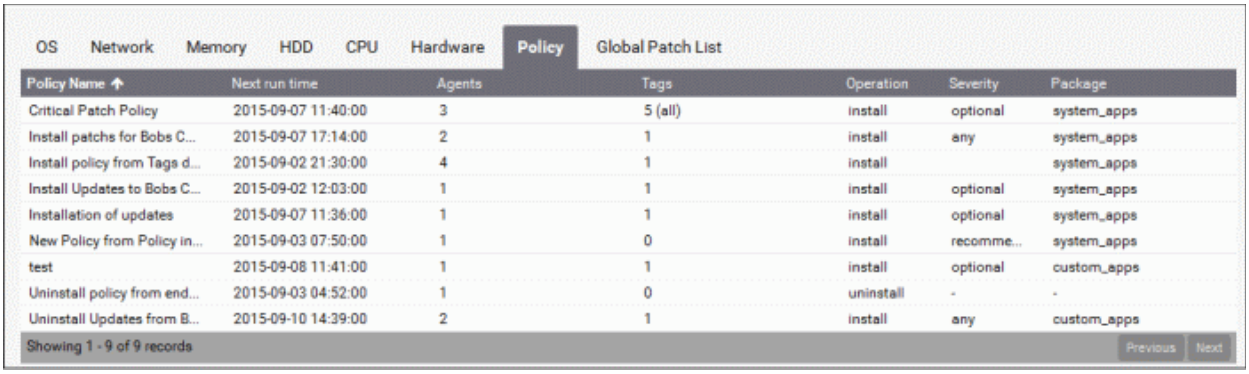
Hardware Details table - Column Descriptions	
Column	**Description**
Computer Name	The 'Display name' of the endpoint. If a display name is not assigned for the endpoint, its host name is displayed. Refer to the explanation of **editing display name of an endpoint** in the section **Viewing Endpoint Details** for more details on assigning the display names.
Component	Displays the list of basic hardware components of the endpoint, whose detail are displayed in the columns at right.
Name	Displays the name, brand and/or model of the component
Size	Displays the memory capacity of the component. For HDD - The size of hard disk drive mounted on the endpoint For CPU - The size of internal cache memory of the processor at the endpoint For Display – The memory size of the graphics card For RAM - The size of RAM mounted on the endpoint
File System/Cores	Displays the file system information of HDD and other memory devices mounted and number of cores in the processor.
Speed/Free Size	For HDD - Displays the size of free HDD space available at the endpoint For CPU – Displays the processing speed (clock frequency) of the processor in MHz For Display – Displays the size of free space in memory of the graphics card
Arch	Indicates the bit architecture of the endpoint, whether the system is 64-bit or 32-bit based.

Sorting Options:

You can sort alphabetically in ascending or descending order by clicking the arrow next to 'Computer Name' in the table header.

Active Policies

The Policy tab displays the policies for automated and scheduled patch management, active for the customer account.



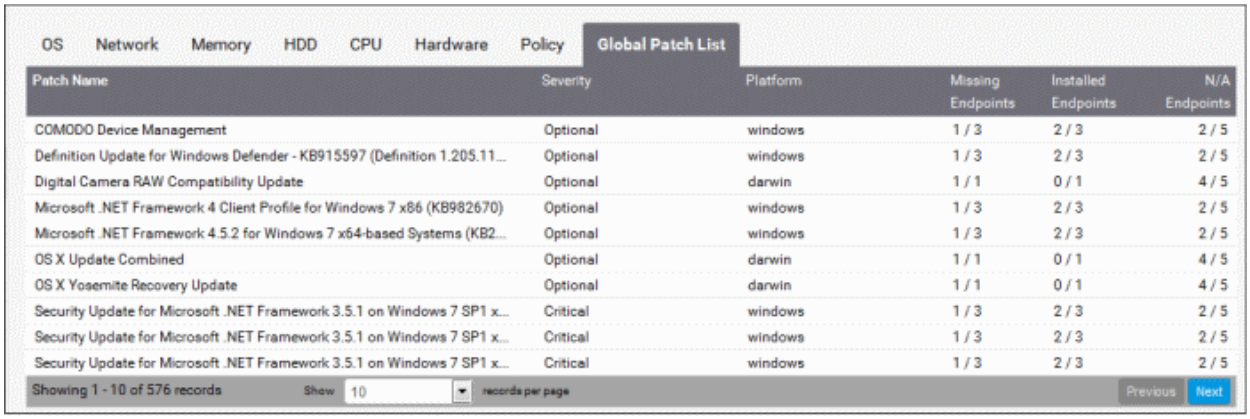
Policy Details table - Column Descriptions	
Column	**Description**
Policy Name	The name of the policy.
Next run time	Indicates the date and time of next execution of the operation as per the policy schedule.
Agents	Indicates the number of endpoints upon which the operation will be executed
Tags	Indicates the number of groups of endpoints upon which the operation will be executed, based on the tags covering them.
Operation	Indicates the type of operation, whether it is installation, uninstallation or reboot.
Severity	Indicates the severity level of the packages to be installed for installation operation.
Package	Indicates the type of packages that will be installed during the installation operation. The possible values are: • system_apps – All the missing OS patches and update packages will be installed according to the OS of each endpoint, from the packages available from the patch management server. • custom_apps - All the missing custom applications will be installed according to the OS of each endpoint, from the packages available from the patch management server.

Sorting Options:

You can sort alphabetically in ascending or descending order by clicking the arrow next to 'Policy Name' in the table header.

Global Patch List

The Global Patch List tab displays an exhaustive list of available OS patches and updates with details of endpoints affected by them.

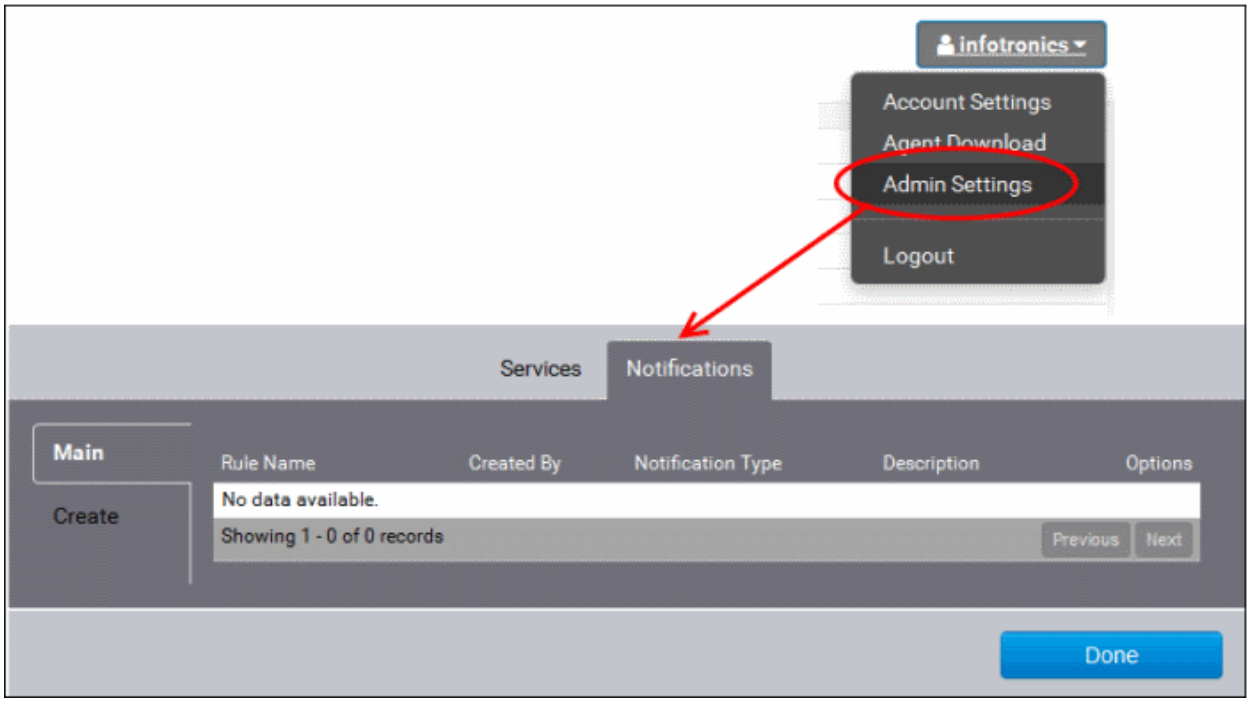


Global Patch List table - Column Descriptions	
Column	**Description**
Patch Name	The name of the patch or the update package
Severity	The severity level of the package
Platform	The base code of the OS to which the patch/update is applicable
Missing Endpoints	Indicates the number of endpoints from which the package was not found installed, out of total number or endpoints upon which the package is applicable.
Installed Endpoints	Indicates the number of endpoints upon which the package has been found installed out of total number or endpoints upon which the package is applicable.
N/A Endpoints	Indicates the number of endpoints for which the package is not applicable out of total number or endpoints.

10 Admin Management

The administrator can configure Log settings and email server settings and automated notification settings from the administrator management interface.

To open the customer and administrator management interface, click your login name displayed at the top right and choose Admin Settings from the drop-down.



The following sections explain in detail about:

- **Configuring log settings and email settings for notifications**
- **Configuring automated notifications for administrators**

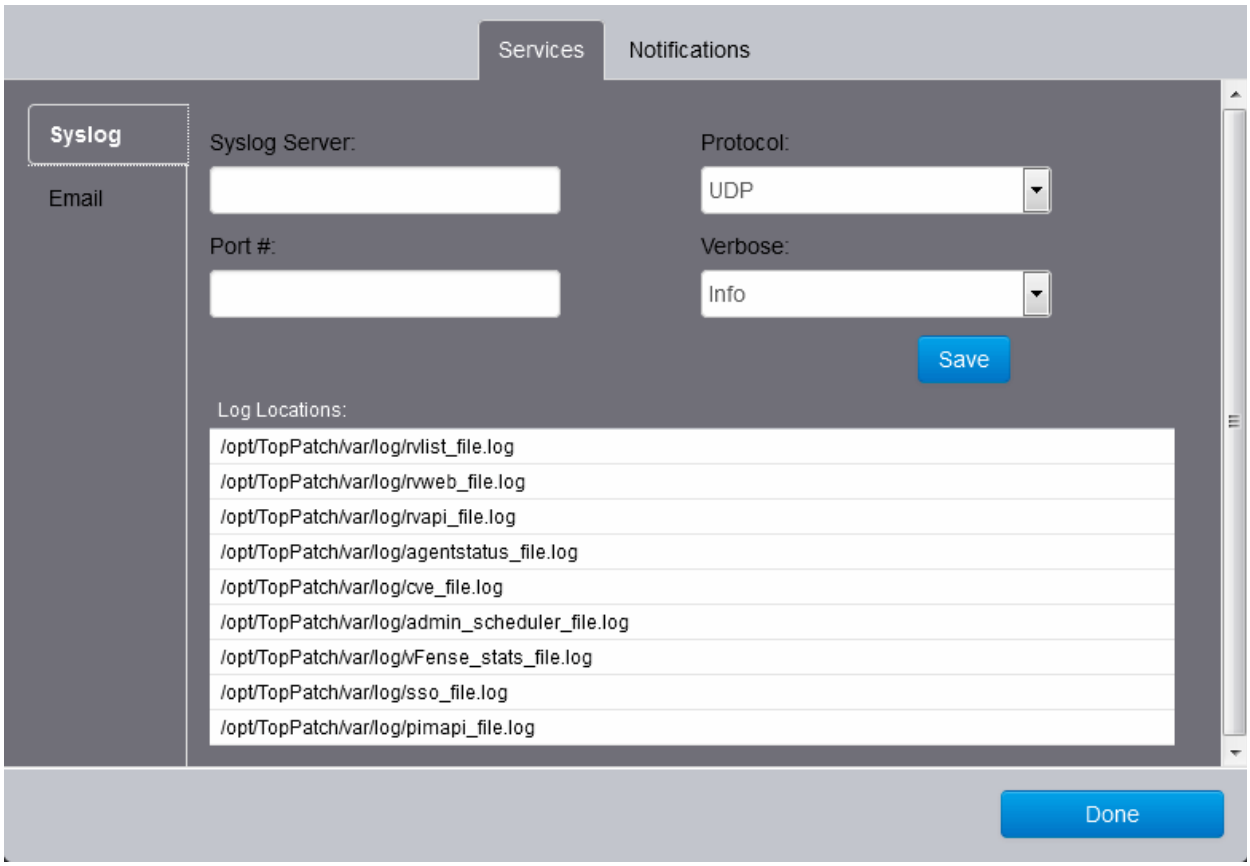
10.1 Manage Log Settings and Email Settings

The Services tab in the administrative interface allows the administrator to configure the following:

- **Syslog Server** - The patch management module has the ability to forward the logs pertaining to various operations and configuration changes to a remote Syslog server. The administrator can integrate the module with the remote Syslog server used by the organization to maintain the logs in it, for easy analysis of the logs and conserving disk space in the patch management server.
- **Email** - The patch management module can send automated notification emails, as configured under the Notifications tab in the administrative interface. The email accounts and the addresses to be used for the notifications can be configured under the Services tab.

To access the services settings interface

- Select the customer account from the right end of the title bar in the main interface
- Open the Administrative Settings interface by clicking your login name at the top right and choosing 'Admin Settings' from the drop-down.
- Click the 'Services' tab.



The following sections explain more on the settings made through this interface.

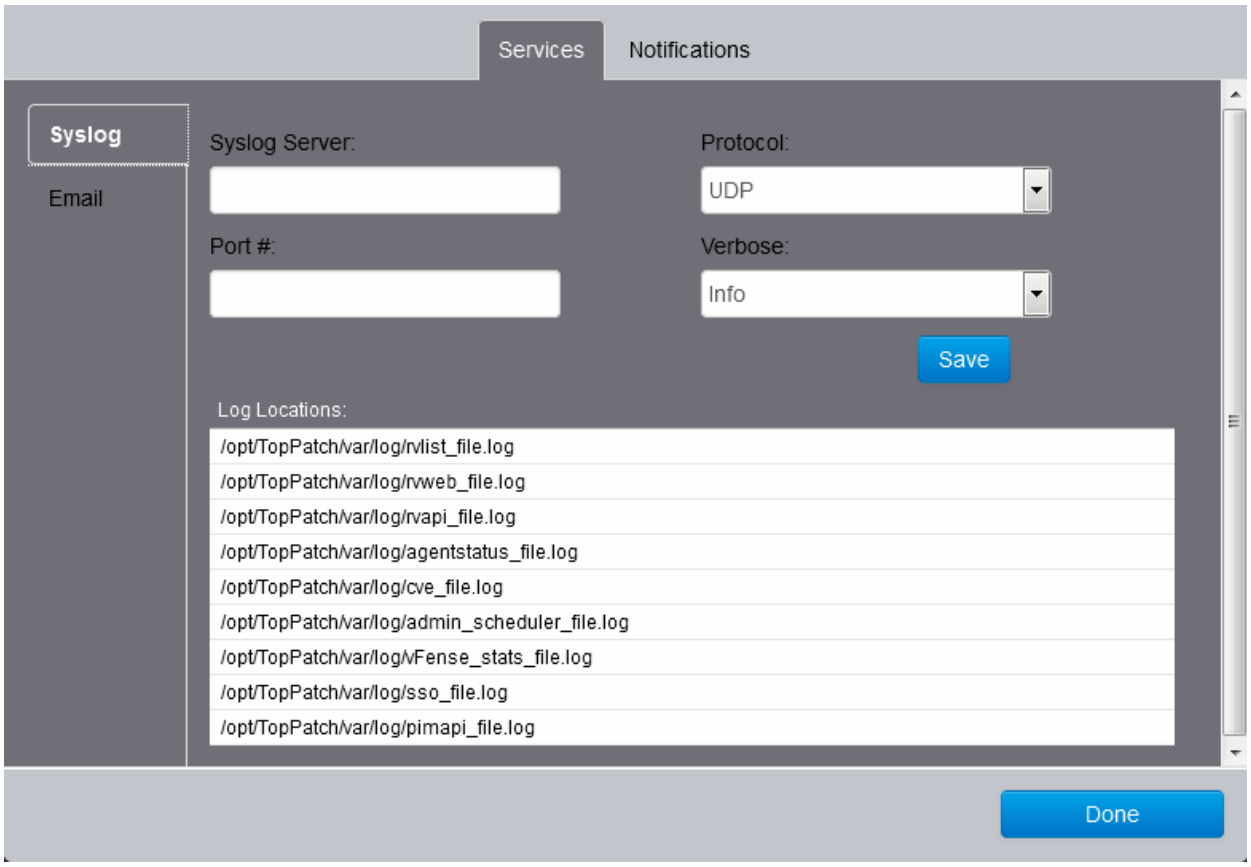
- **Configuring connection to remote Syslog Server**
- **Configuring email account**

Configuring connection to remote Syslog Server

The Syslog tab in the Service settings interface allows the administrator to specify the syslog server and the connection parameters for the selected customer account.

To configure syslog connection settings

- Open the service settings interface as explained **above**.
- Click the Syslog tab from the left hand side navigation.



The upper pane displays the connection parameters for the syslog server and the lower pane shows the paths of different types of log files in the syslog server.

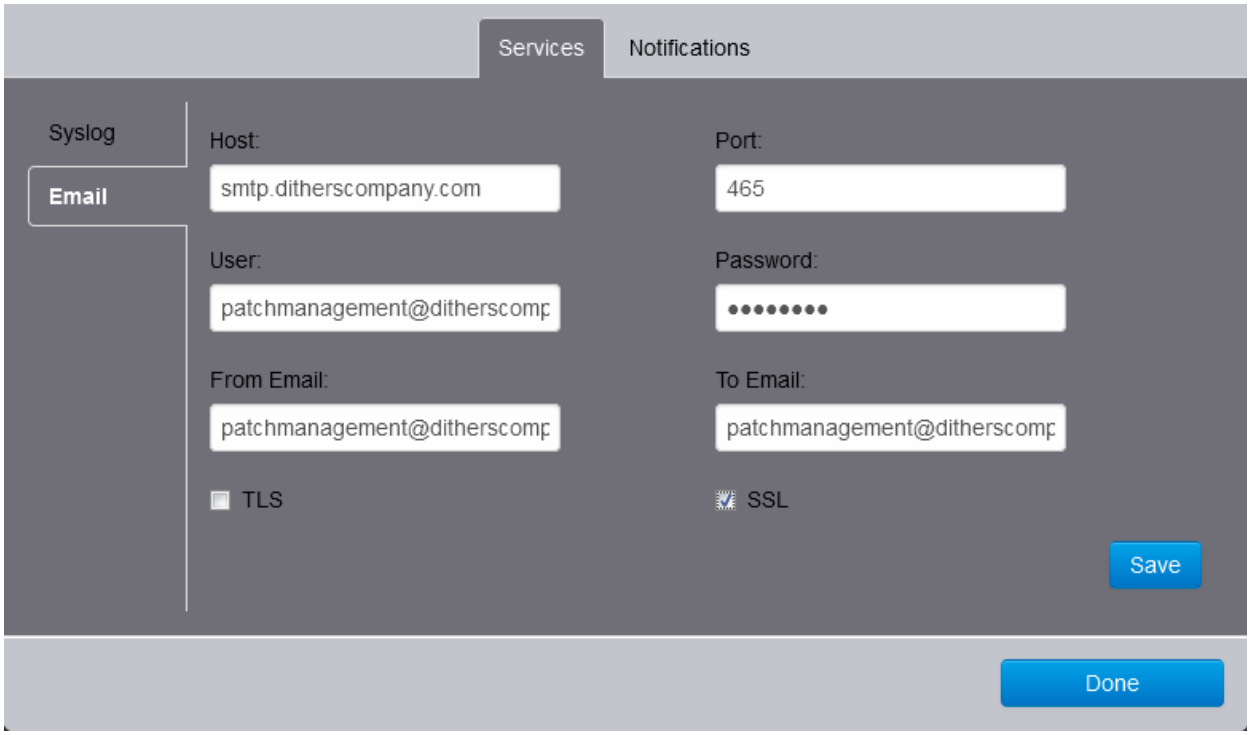
- Configure the connection parameters as shown below:
  - Syslog Server - Enter the host name or the IP address of the remote logging server to which the logs are to be passed.
  - Protocol – Choose the protocol used for the transfer of logs
  - Port – Enter the port number of the UDP listening port through which the server receives the logs. Default is 514.
  - Verbose – Choose the log level from the drop-down depending on the space allotted in the remote server.
- Click 'Save' to save your changes.
- Click 'Done' in the Administrative interface

Configuring Email Account

The email tab in the service settings interface allows the administrator to specify the SMTP server and the email account to be used for sending the automated notification emails from the patch management module.

To configure Email server settings

- Open the service settings interface as explained **above**.
- Click the Email tab from the left hand side navigation



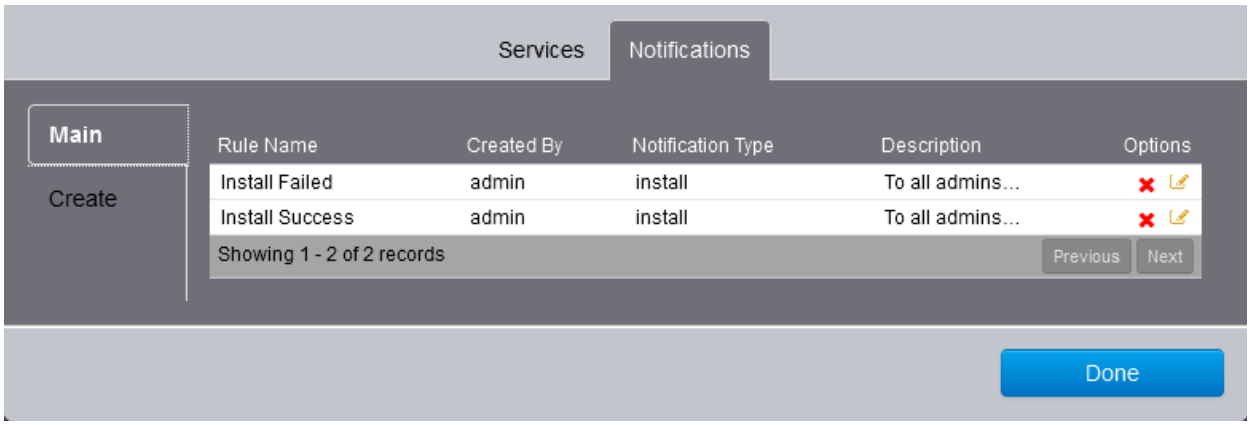
- Configure the email settings as shown below:
  - Host - Enter the SMTP server to be used for sending the notification emails.
  - Port – Enter the SMTP port number of the email server, based on the encryption protocols to be used. (***Default = 465 for SSL/TLS encryption, 25 for plain emails***)
  - User - Enter the username or email address of the email account to be used by the patch management server to send the notification emails. Preferably you can create a new account for the patch management module in your mail server and enter its username in this field.
  - Password – Enter the password for the dedicated account.
  - From Email – Enter the email address to be displayed in the 'From:' field of the notification emails. Usually this will be same as the address entered in the 'User' field.
  - To Email – Enter the default email address to which all the notifications need to be sent.
- Click 'Save' to save your changes.
- Click 'Done' in the Administrative interface.

10.2 Configure and Manage Notifications

The patch management module can send automated notification emails for the specified events to administrative users of the selected customer account, as configured under the 'Notifications' tab in the Administrative Settings interface.

To access the Notifications interface

- Select the customer account from the right end of the title bar in the main interface
- Open the Administrative Settings interface by clicking your login name at the top right and choosing 'Admin Settings' from the drop-down.
- Click the 'Notifications' tab.

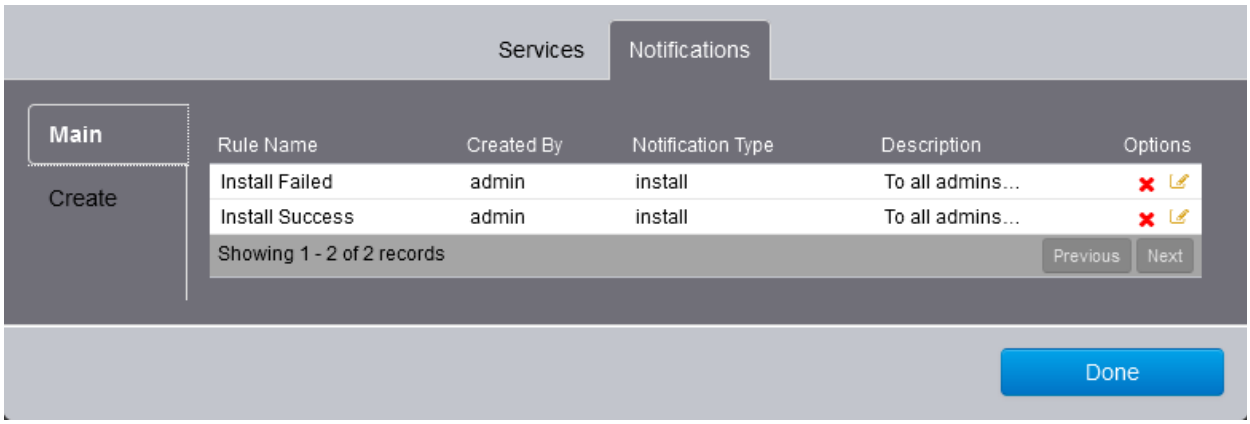


The interface contains two tabs:

- **Main** – Displays a list of notification settings in action. Refer to the section **Viewing Notifications** for more details
- **Create** – Enables you to create new notifications. Refer to the section **Creating New Notifications** for more details

Viewing Notifications

The Main tab in the Notifications interface displays a list of pre-configured notifications for various events an allows you to edit or remove them.



Notifications table - Column Descriptions	
Column	**Description**
Rule Name	The name of the rule created for sending the notification, shortly describing the purpose of the notification.
Created by	The administrator that created the rule.
Notification Type	The event for which the notification is to be sent. The possible values are: • Install • Uninstall • Reboot • Shutdown
Description	The description of the notification entered during its creation

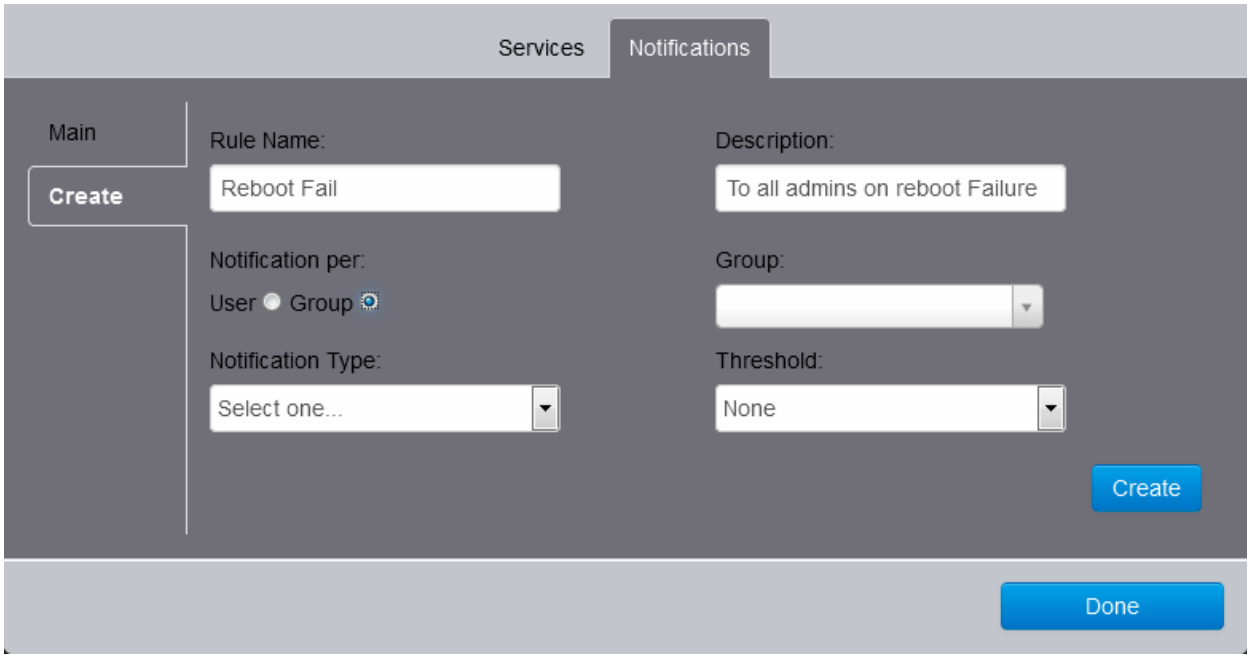
Options	Contains control buttons to edit and remove the rule. - Clicking the pencil icon opens the edit interface to edit the notification settings. The edit interface is similar to the 'Create' interface. Refer to the section **Creating New Notifications** for explanations on parameters configured through this interface. - Enables you to remove the notification rule after confirmation.

Creating New Notifications

The 'Create' interface allows you to add new notification rules for automated emails to be sent for different events to specified administrative users or user groups.

To create a new notification rule

- Open the Notifications settings interface as explained **above**.
- Click the 'Create' tab from the left hand side navigation.



- Configure the notification parameters as shown below:
  - Rule Name – Enter a name for the notification rule, shortly describing the purpose of the rule
  - Description – Enter a description for the notification rule
  - Notifications per – Choose whether the notification is to be sent to a single administrative user or a user group.
    - User – The notification will be sent to a single administrative user.. Choose the user form the 'User' drop-down at the right.
    - Group - The notification will be sent to all administrative users in a user group. Choose the group from the 'Group' drop-down at the right.
  - Notification Type – Choose the operation type from the drop-down. The possible values are:
    - Install
    - Uninstall
    - Reboot
    - Shutdown

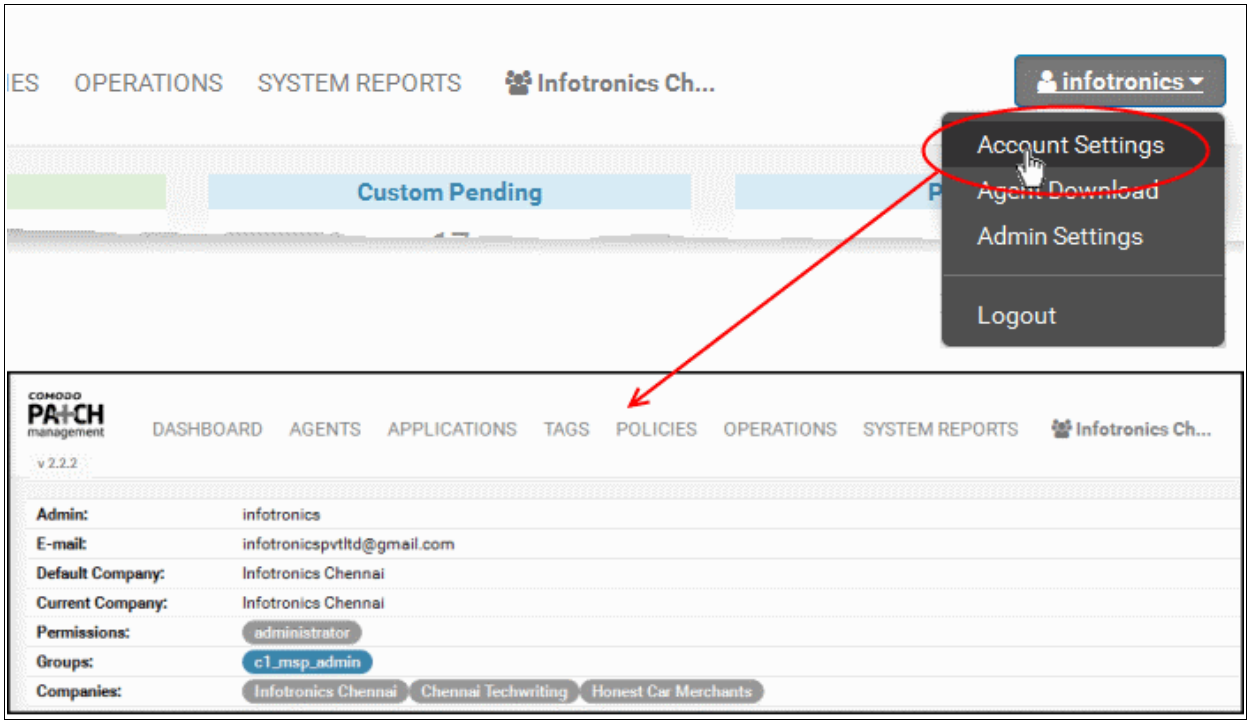
- Threshold – Choose the event for the operation on the occurrence of which the notification should be sent. The possible values are:
  - Pass
  - Fail
  - Both

- Click 'Create'. The rule will be added to the list of notification rules in the 'Main' interface.
- Repeat the process for adding more rules
- Click 'Done' in the 'Administrative Settings' interface.

10.3 View Administrator Account Settings

The 'Account settings' screen contains a details summary for the Administrator that is currently logged into the patch management module. Administrators can view their login name, full name, the email address that is associated with their account, the user group(s) to which the they are members, the permissions assigned by the groups and the customer accounts managed by them.

To view the 'Account Settings' screen, click your login name at the top right and choose 'Account Settings' from the drop-down.



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 : +1.888.266.636

Tel : +1.703.581.6361

https://www.comodo.com

Email**: EnterpriseSolutions@Comodo.com**