BigFix Compliance
Client Manager for Endpoint Protection App in WebUI User Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page 28)*.

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Welcome to CMEP App in WebUI..... 1

Chapter 2. System requirements..... 2

Chapter 3. CMEP App in WebUI - Overview..... 4

Using Refine My results..... 9

Uploading packages..... 10

Deploying Latest antivirus definitions..... 14

Viewing Device Details..... 19

Viewing Fixlets..... 21

Managing Analyses..... 25

Exporting Report..... 26

Notices..... 28

Chapter 1. Welcome to CMEP App in WebUI

This topic gives an introduction about CMEP App in WebUI and its features.

The CMEP App is an effective tool to monitor the deployment and health status of various Endpoint Protection products and provide quick remediation actions to recover needed endpoint protection. It is now available as a new App in WebUI with enhanced functionality and better user experiences.

The CMEP App in WebUI includes the following functionalities:

- **Consolidated Summary:** Overall deployment and health status across all devices and for each endpoint protection product in various summary graphs.
- **Easy Filtering:** Filtering of all devices based on Operation System, Device Type or Device Group.
- **Quick Action:** A single click to fix frequent deployments issues such as stopped AV agent or outdated virus definition.
- **Report Export:** Exporting reports in PDF including various status summary graphs.
- **Integration with Content App**: Leveraging Content and Take Action app to deploy the antivirus definitions on selected devices.
- **Device list**: See the devices applicable for various reports like health status, deployment stats, and other status. You can check the individual device properties from the device list.
- **Multiple Product Support:** Supporting major antivirus products from vendors such as McAfee, Symantec, Trend Micro, Microsoft (Defender), and Sophos.

Chapter 2. System requirements

This topic describes the requirements before you install and use CMEP App in WebUI.

You must meet the following requirements to use CMEP App in WebUI:

- Any one of the BigFix Compliance Endpoint protection license for using the CMEP App:
  - Security and Compliance
  - Security and Compliance POC
  - Starter Kit for Security and Compliance
  - Starter Kit for Security and Compliance POC
- Ensure that the CMEP site is enabled from the License Overview dashboard in Console and subscribed to the devices from Console CMEP site.
- The process for site subscription depends on the version of the BigFix console that you have. The CMEP site contains tasks, analyses, and Fixlets for protecting your deployment from malware. You must be subscribed to the CMEP site to collect data from the BigFix clients. This data is used for reporting and analysis.
- CMEP App in WebUI must be installed in BigFix Version 9.5.5 and above.

Supported Antivirus products

CMEP offers support for a variety of antivirus products. The following table lists the currently supported antivirus products and product versions:

Important: CMEP only supports the devices with Mac and Windows platforms. See the BigFix CMEP Support Matrix for latest information on the supported AV products and functions at https://bigfix-wiki.hcltechsw.com/wikis/home?lang=en-us#!/wiki/BigFix%20Wiki/page/CMEP%20Support%20Matrix.

Table 1. Supported products

List of supported anti-virus products for CMEP

Vendor	Product	Version
McAfee	Endpoint Security	10.x
	Endpoint Security for Mac	10.x
	VirusScan	8.x
	VirusScan for Mac	9.x
	McAfee Security for Microsoft Exchange	8.5
Microsoft	Windows Defender	All known versions
Symantec	Endpoint Protection	12.1, 14
	Endpoint Protection for Macintosh	12, 14
Sophos	Endpoint Security	9.x, 10.x
	Antivirus for Mac	7.x, 8.x (Audit only)
Trend Micro	OfficeScan	XG
	ServerProtect	5.8
	Trend Micro Security for Mac	1.5, 2.0

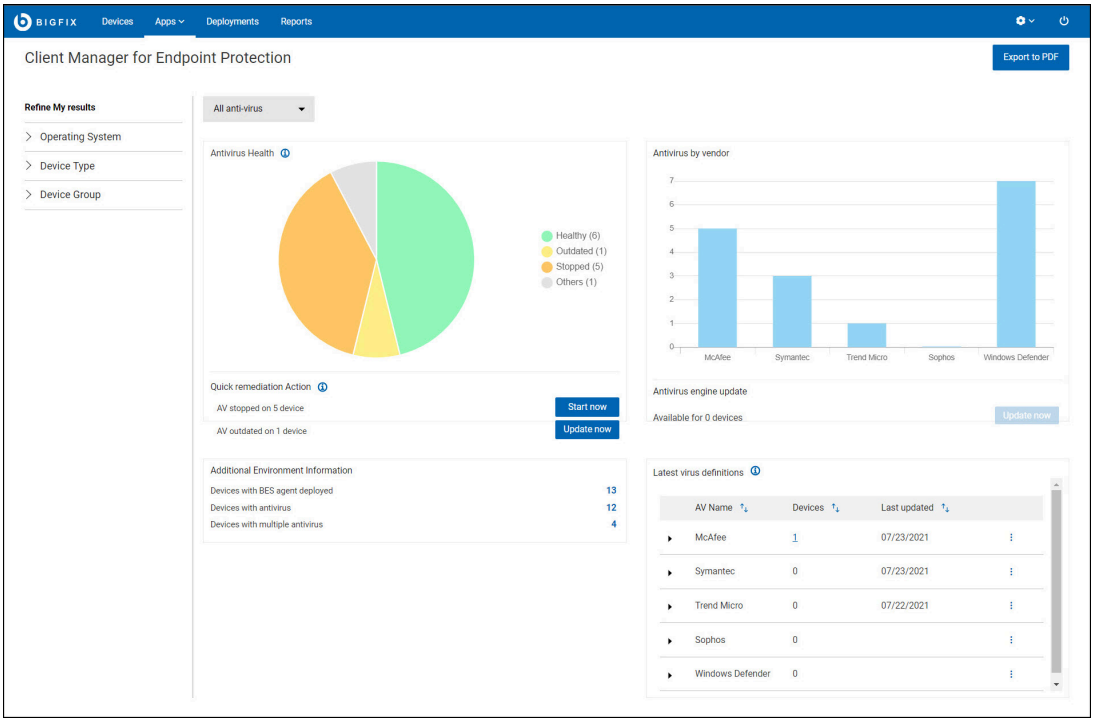
Note: For each supported antivirus product, the CMEP supports all the platforms that are currently supported by the antivirus product, if the platform is also supported by the BigFix agent. To verify the BigFix support scope, see the BigFix system requirement reports at https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Installation/c_spcr_platform.html.

Chapter 3. CMEP App in WebUI - Overview

The CMEP App overview provides a quick status summary of antivirus products deployed on all the devices managed by BigFix.

To navigate to the CMEP App, log in to **WebUI** and select CMEP from the Apps menu.

Figure 1. CMEP App in WebUI - Overview



The overview page contains four tiles:

- **Antivirus Health**: The pie chart in the Antivirus Health window represents the status of the antivirus product installed on the devices. These are the possible statuses:

  Healthy

  Devices with at least one antivirus product installed, updated and running.

  Outdated

The antivirus definition is out of date and needs to be updated on the device.

Stopped

The installed antivirus application is not running.

Others

This device has an antivirus product that is not supported by CMEP, or no antivirus product is installed.

- A status summary with quick remediation action buttons (**Start now** and **Update now**).

  Start now

  Allows you to restart an antivirus product.

  Update now

  Allows you to update an outdated antivirus definition.

- **Antivirus by vendor**: A bar graph, which displays the number of antivirus product installed by an individual vendor.
- **Additional Environment Information**: This tile provides information about the number of devices with BES agent deployed, devices with antivirus, and devices with multiple antivirus (antivirus product installed by vendor and Windows Defender).
- **Latest virus definitions**: This component contains the vendor's product name with the number of installed device and the last updated date. You can also **Deploy** an antivirus definition package by clicking the vertical ellipsis. For more information about uploading a package and deploying it, see Deploying Latest antivirus definitions *(on page 14)*.

The left panel of the homepage has **Device Filter** that you use to set the criteria of what is shown in the Overview Report.

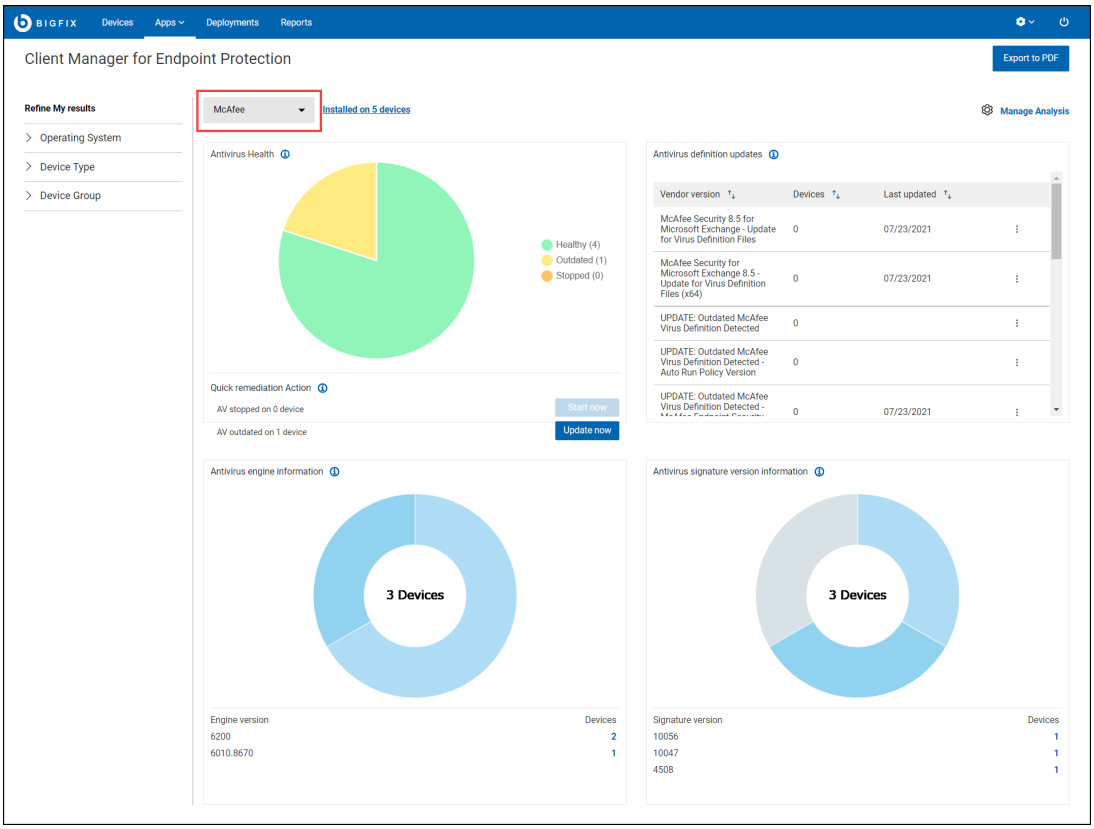
The upper-right corner includes the **Export to PDF** button.

Individual vendor dashboard - Overview

CMEP provides a consistent dashboard for each supported antivirus product.

To view the individual vendor dashboard, click **All anti-Virus** dropdown menu in the CMEP App overview page and select the antivirus vendor.

Figure 2. McAfee dashboard



The individual vendor dashboard overview page contains four tiles:

- **Antivirus Health**: The pie chart in the Antivirus Health represents the status of the antivirus product installed on the devices. These are the possible statuses:

  Healthy

  Devices with at least one antivirus product installed, updated and running.

Outdated

The antivirus definition is out of date and needs to be updated on the device.

Stopped

The installed antivirus application is not running.

- A status summary with quick remediation action buttons (**Start now** and **Update now**).

  Start now

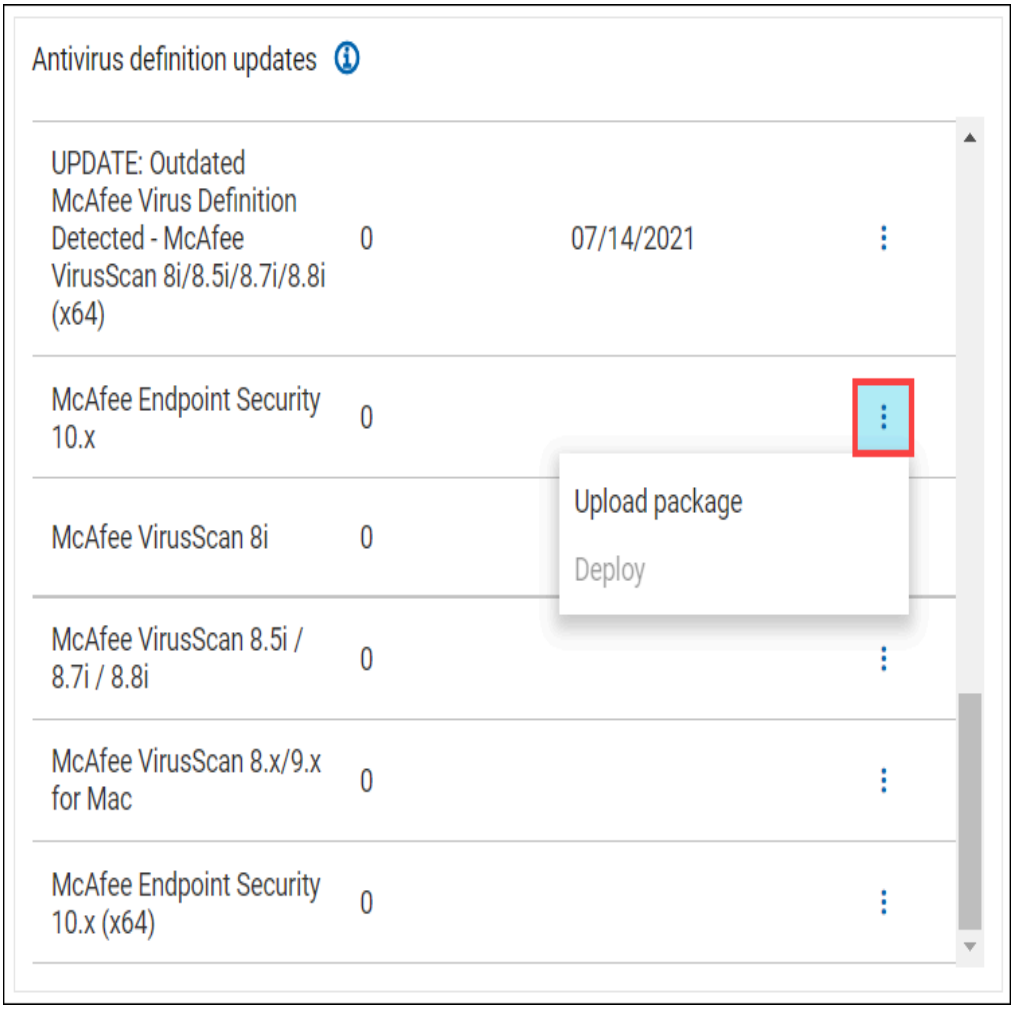
  Allows you to restart an antivirus product.

  Update now

  Allows you to update an outdated antivirus definition.

- **Antivirus definition updates**: This component contains the vendor's product name and version number with the number of installed device and the last updated date. You can also **Upload** or **Deploy** an antivirus definition package by clicking the vertical ellipsis as shown in the following screenshot. For more information about uploading a package and deploying it, see Deploying Latest antivirus definitions *(on page 14)*.

Figure 3. Antivirus definition updates



- **Antivirus engine information**: An antivirus product may have multiple antivirus engine versions. Information about the engine that various antivirus product use (installed on the subscribed device) with the number devices having that engine installed.

Note: All engine versions are currently supported in CMEP App and hence the total number of devices listed here may or may not match the total applicable device count of the vendor.

- **Antivirus signature version information**: An antivirus signature version may not be same for different device. The number of devices that have the signature version or definition version of the antivirus signatures of the antivirus product.

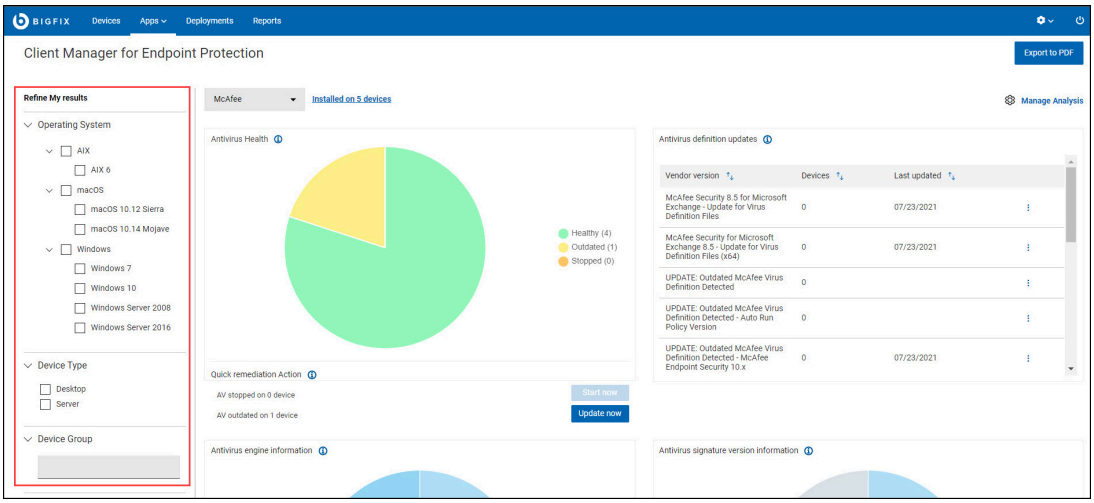
Using Refine My results

This topic gives an overview of Refine My results feature in CMEP App.

Refine My results is located on the left side of the CMEP App overview page. By using **Refine My results**, you can refine the search results based on the following filters:

- **Operating System**: You can filter the information for device health status, deployment stats, vendor installed stats, and so on based on the operating systems that is installed on the devices. If you want to see data only for a particular operating system such as Windows 10, select the same from filters and the reports will show only information about devices have Windows 10 installed.
- **Device Type**: You can filter the information for devices health status, deployment stats, vendor installed stats, and so on.
- **Device Group**: You can group together devices based on their properties in the console. Those groups are available in the WebUI as filters for devices information. You can select group from the **Device Group** filter to view information related only to that device group.

Figure 4. Refine My results

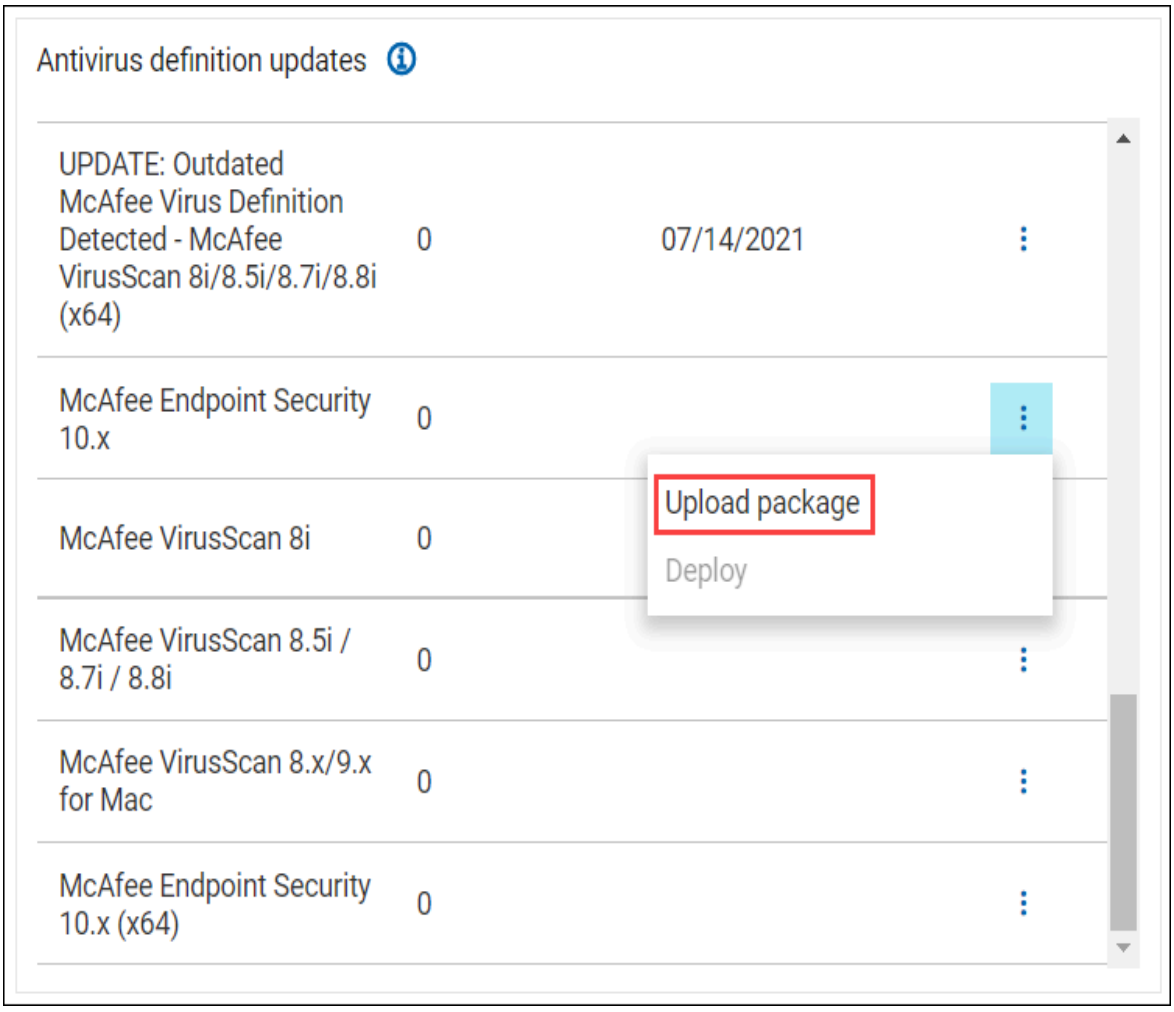


Uploading packages

Use the Upload package function to update the antivirus definition of the antivirus product.

Perform the following steps to upload a package:

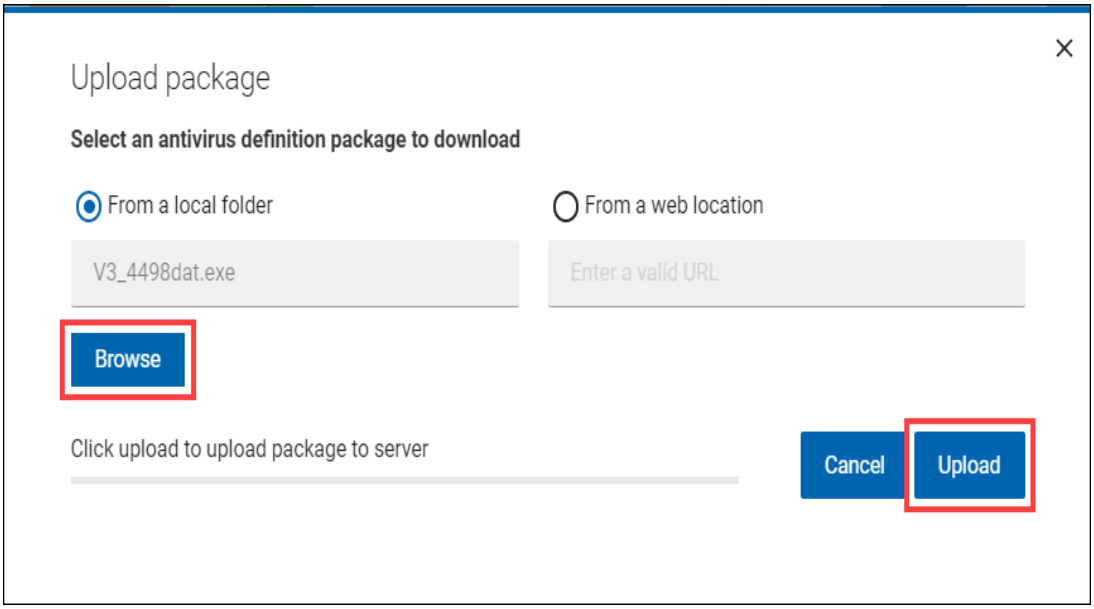
1. In the individual vendor dashboard, click the vertical ellipsis in the **Antivirus definition updates** tile and click **Upload package**.



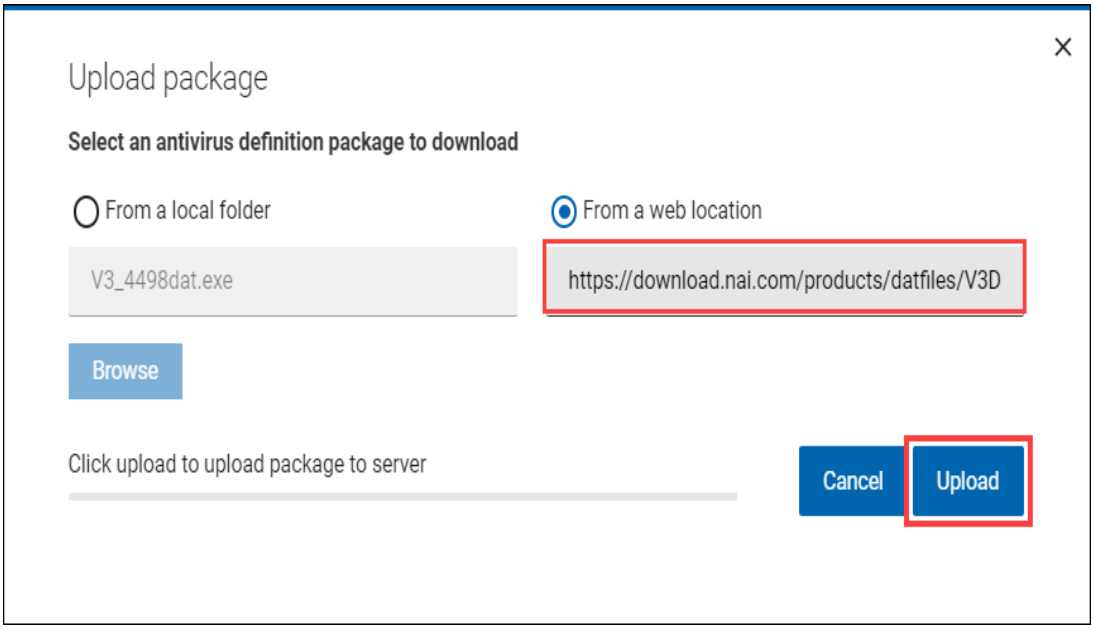
Note: Upload package is available only for a selected antivirus product that is currently in the CMEP App. Also, you must have permission to create custom content.

2. Select one of the following options to download an antivirus definition package:

- From a local folder: Check **From a local folder** and then click **Browse** to select an antivirus definition package from a local folder. Click **Upload**.

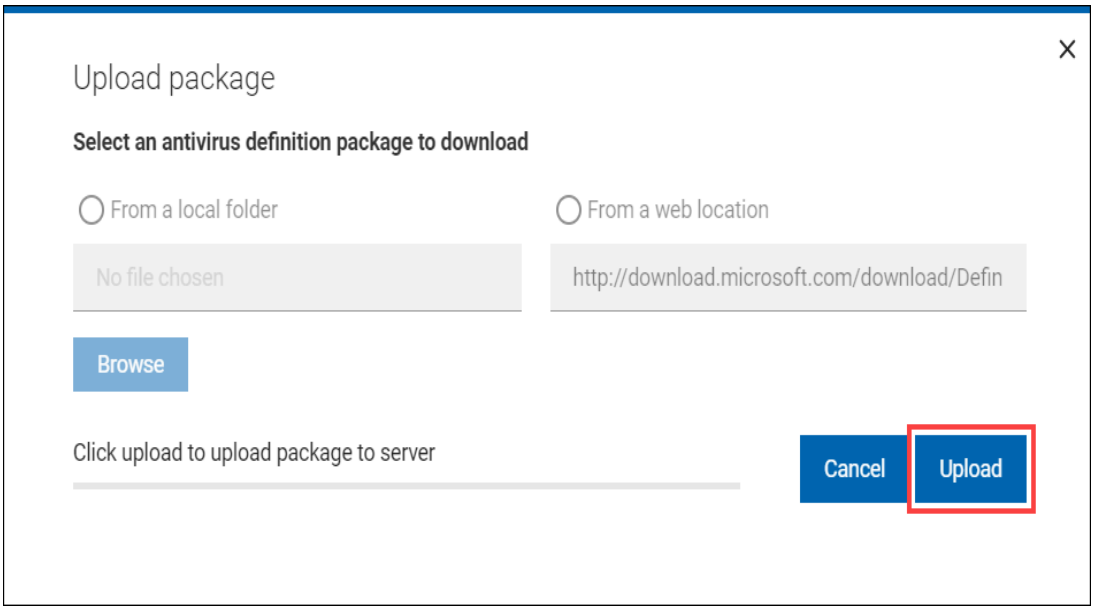


- From a web location: Check **From a web location** and then enter the URL of the antivirus definition package. Click **Upload**.



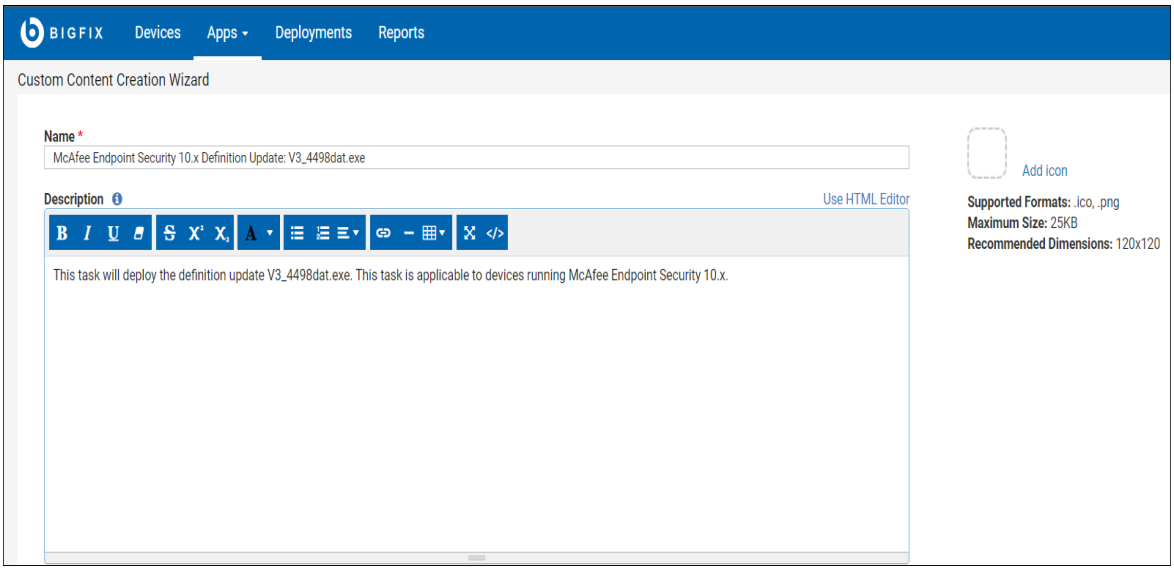
- For Windows Defender x64 and x86 versions, the upload **From a local folder** and **From a web location** feature is disabled. Click **Upload** from the Upload package

window to download the most recently released spyware signature update from Microsoft and then cache the update on the BES Sever for deployment.

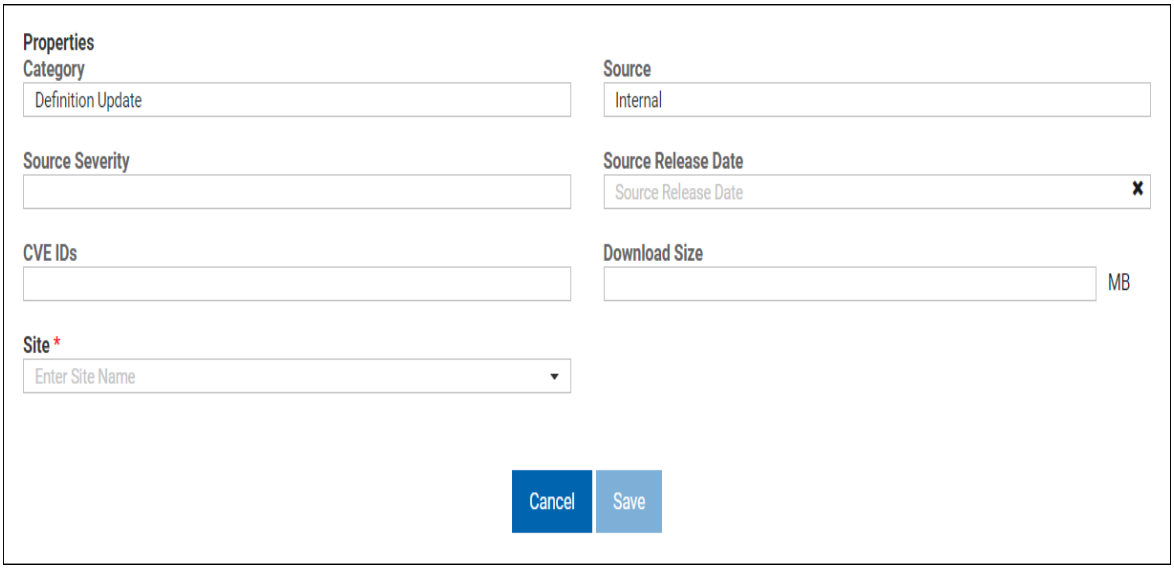


3. When the antivirus definition package is uploaded, you are redirected to the **Custom Content Creation Wizard** page.

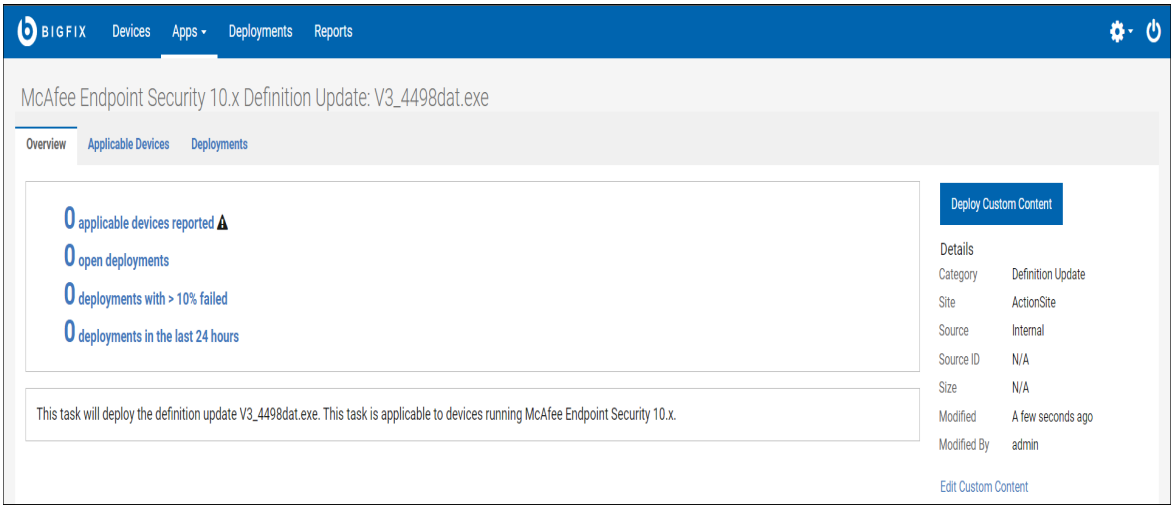
Note: The **Custom Content Creation Wizard** page gives an overview of the Fixlet and its relevance and action.



4. Select **Source Release Date** and the **Site** where you want to save the custom content. Click **Save**.



The Fixlet overview is displayed as shown:



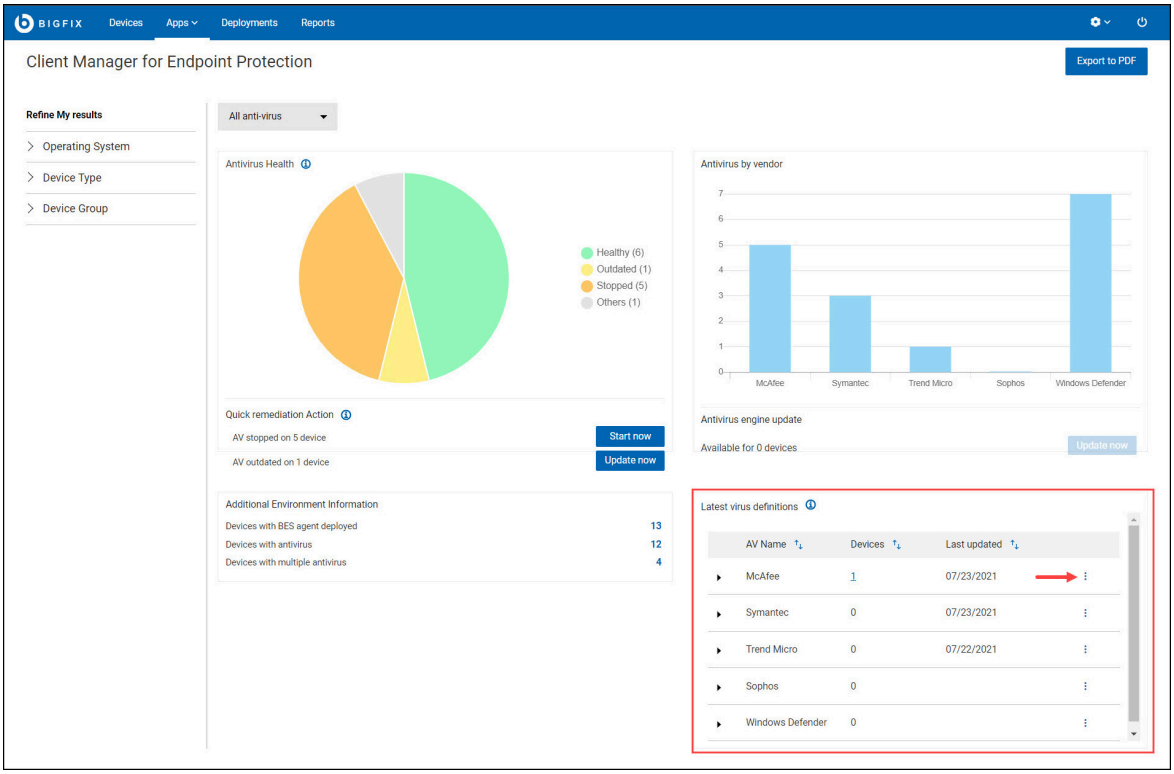
5. To deploy Custom Content, see Deploying Latest antivirus definitions *(on page 14)*.

Deploying Latest antivirus definitions

This task helps you to deploy latest antivirus definitions to the devices.

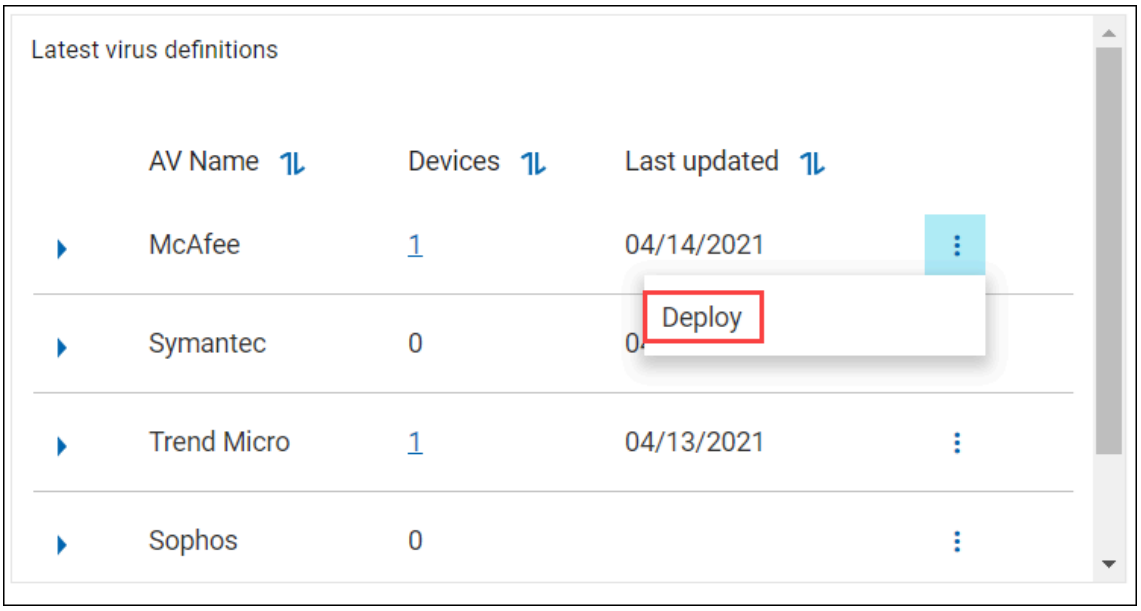
Perform the following steps to deploy the latest virus definitions for your antivirus products:

1. In the CMEP App overview page, click on the vertical **ellipsis** in the **Latest virus definitions** tile.

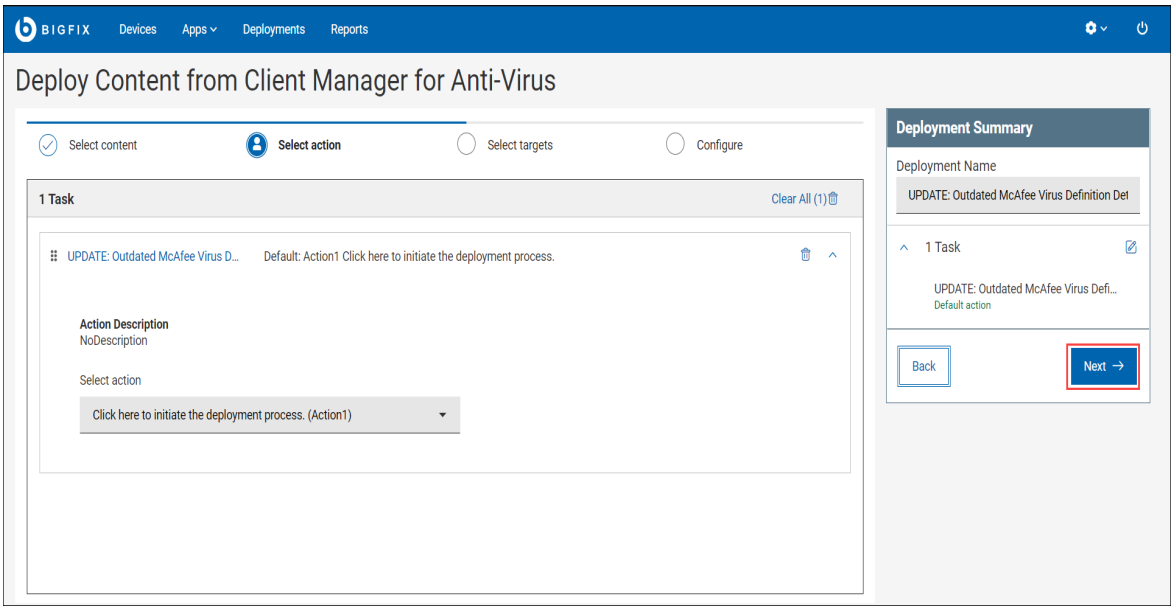


2. Click **Deploy**.

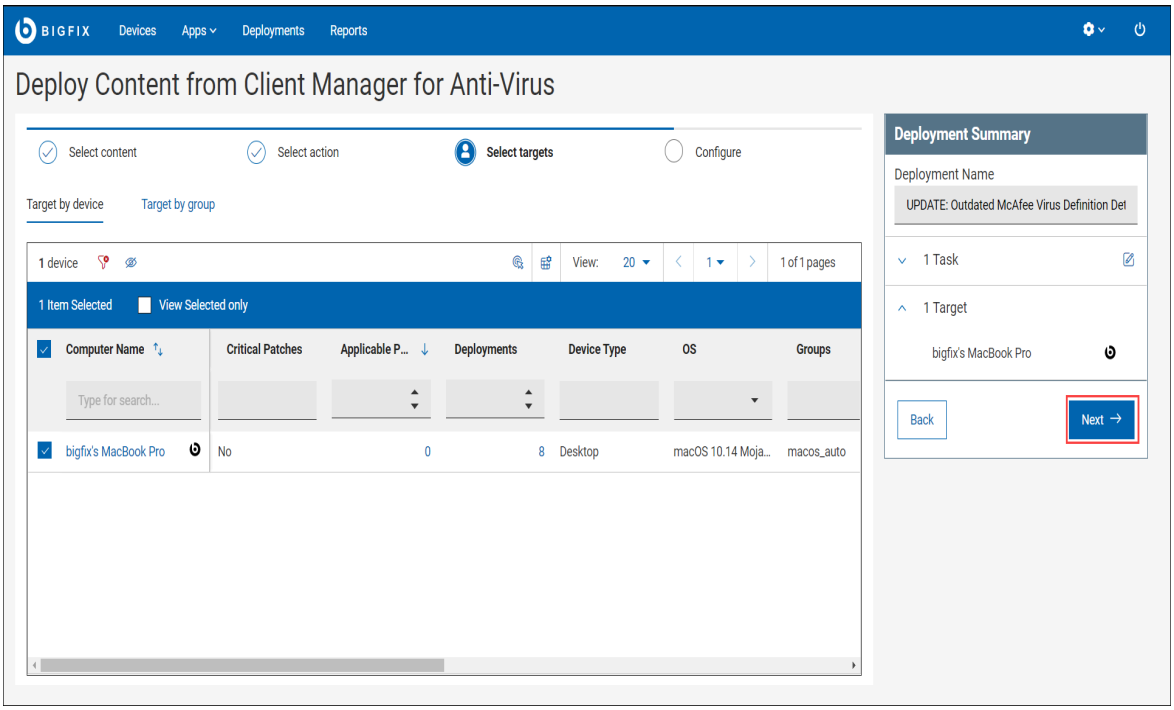
Note: The **Deploy** option is available if for any antivirus or if the version number of outdated devices is greater than 0. The CMEP App has predefined fixlets for certain antivirus versions, which can update the definition package of the product with those devices. With this option, you can deploy those fixlets for those devices and update the definition packages.



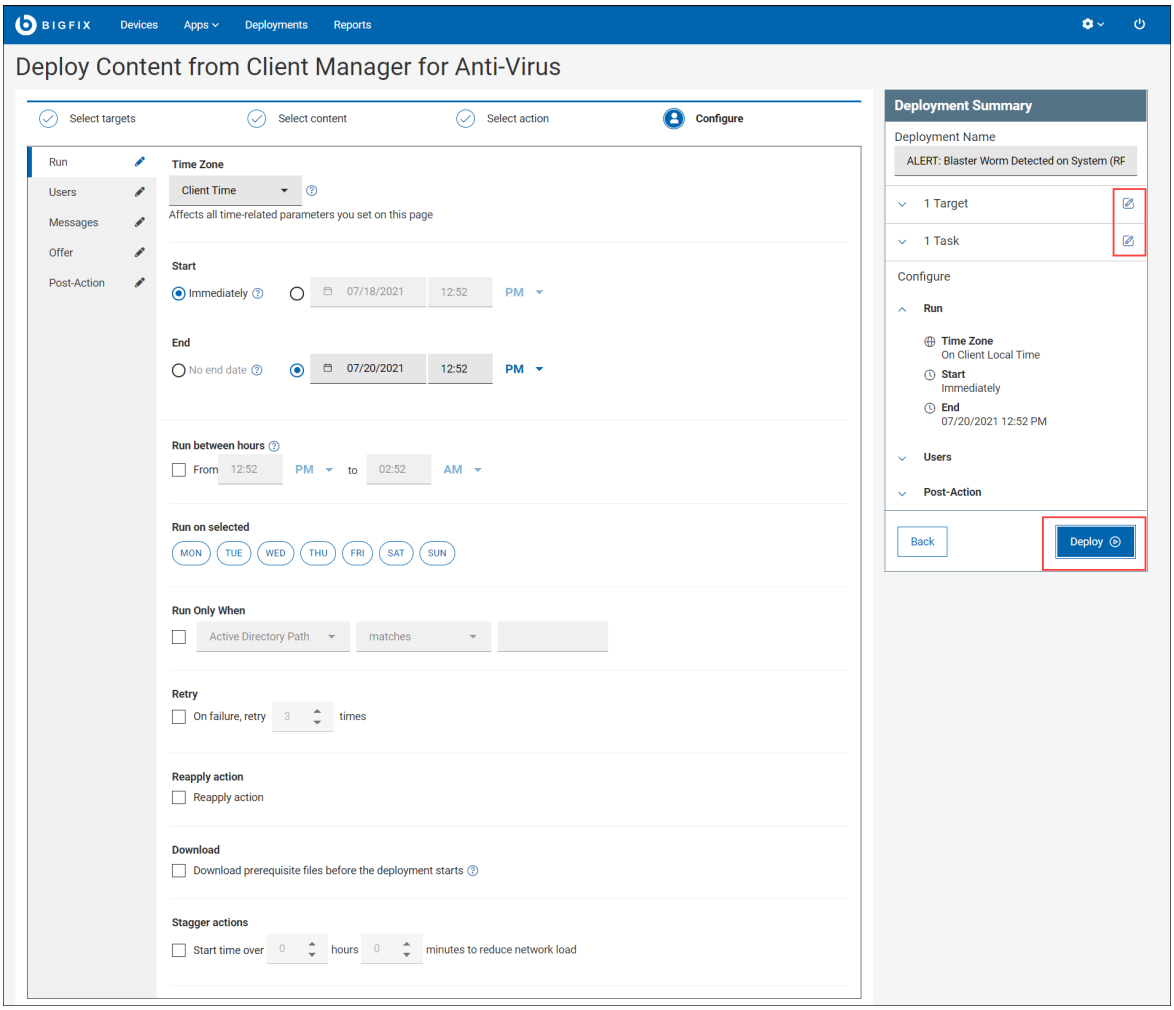
3. In the **Select action** tab, click **Next**.



4. The **Select targets** tab, select the targets and click **Next**.



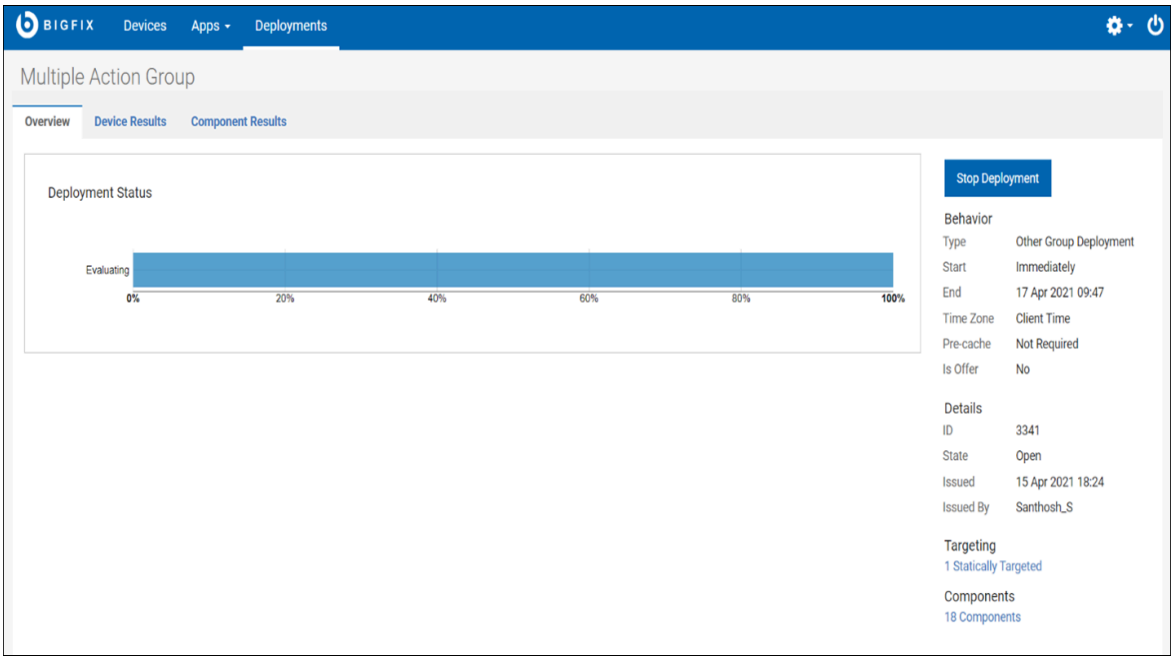
5. On the **Configure** tab, click **Deploy**.



Note:

- In the **Deployment Summary**, use the **edit** icon to edit the task, and target.
- You can change the parameters in the **Configure** tab as required, the parameter includes Time Zone, Start and End date, and so on.

The Deployment Status is displayed as shown.



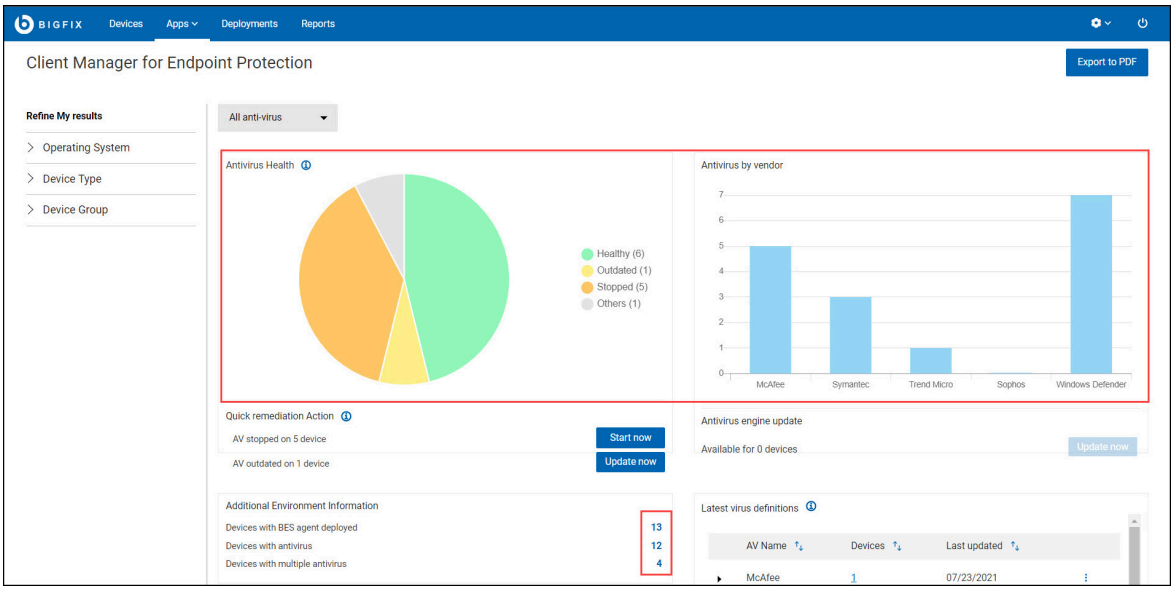
Click **Stop Deployment** to pause the deployment.

Viewing Device Details

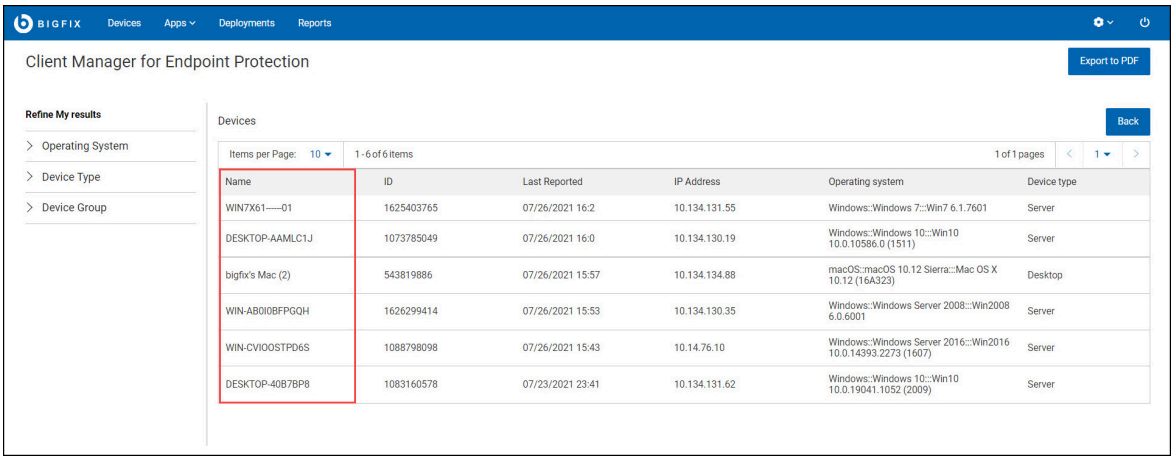
This topic helps you to learn more about the device details.

Follow the steps to view the devices details in the Antivirus Health, Antivirus by vendor and Additional Environmental Information tiles. You can view the device details for All anti-virus and individual vendor dashboard.

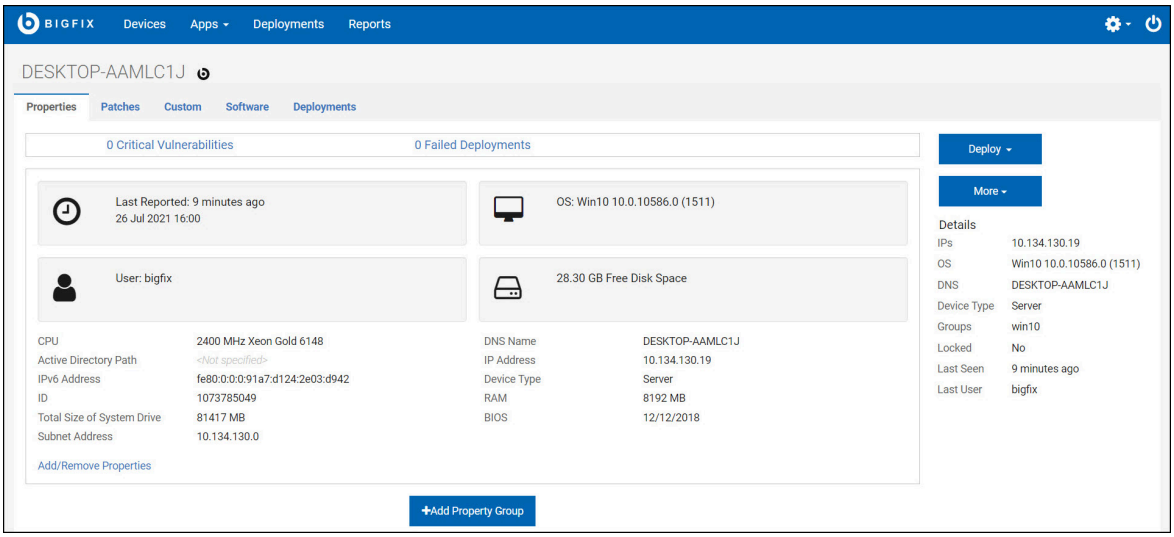
1. Navigate to CMEP App overview or individual vendor dashboard page.
2. **Click** the piechart, bar graph, or numbers to view the list of available devices for that particular selection.



3. From the list of available devices, **click** the device name.



You are redirected to the device properties page, which contains Last Reported, OS, User, Disk Space and other details of the device.



Note: You can also view the patches, custom, software, and deployments available for the individual device.

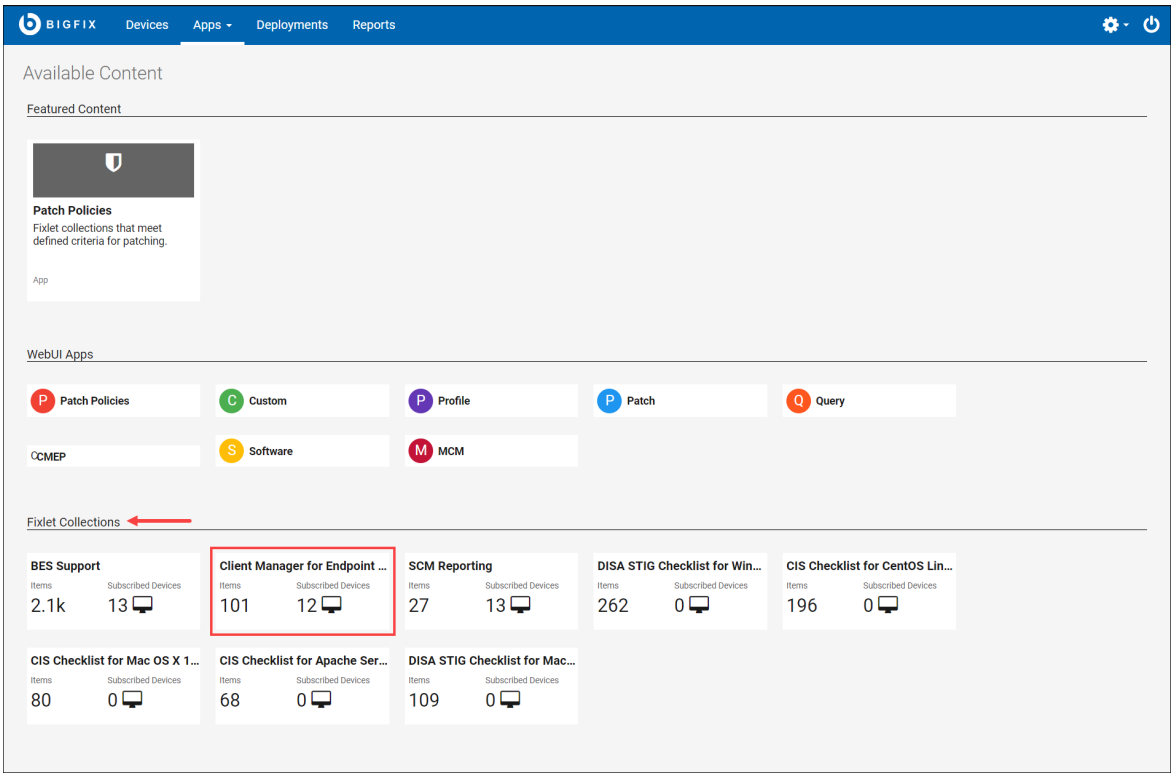
Viewing Fixlets

This topic describes how to view the CMEP App's Fixlets.

The Content App allows you to view all the Fixlets available for CMEP App and provides various information about the Fixlet such as overview, applicable devices, and deployment. You can also deploy the Fixlets from the Content App.

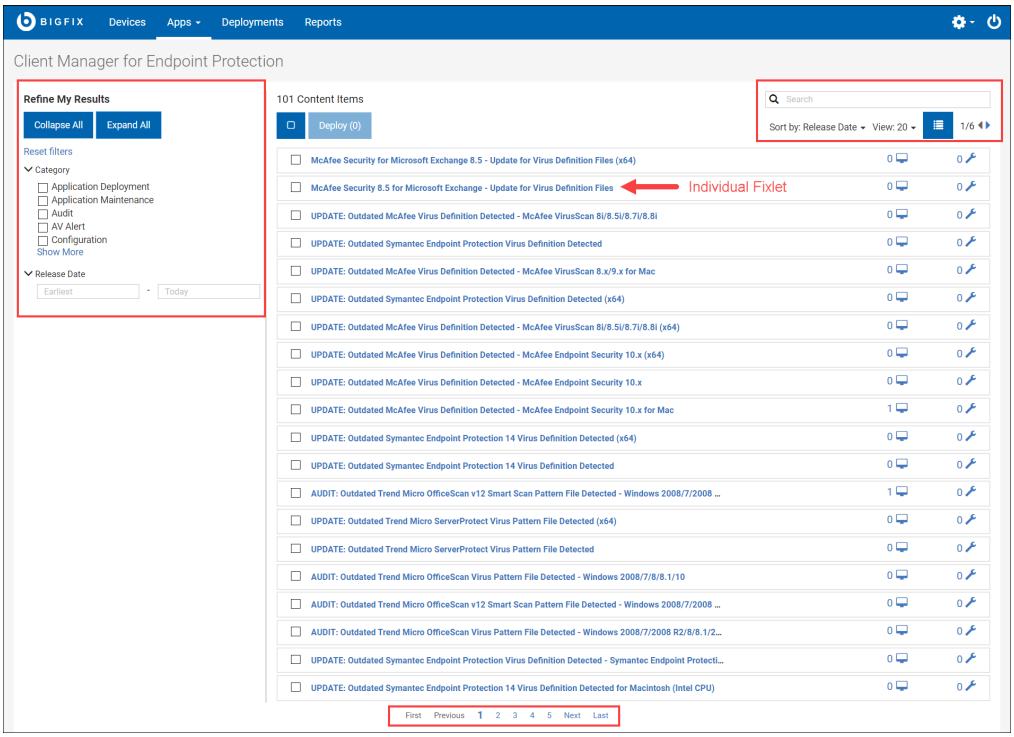
Follow the steps to view the Fixlets available for CMEP App in WebUI.

1. Log in to **WebUI** and select **Content** from the Apps menu.
2. Click **Client Manager for Endpoint Protection** in the Fixlet Collections module.



Note: Ensure that you have subscribed to CMEP App in WebUI. If not, the **Client Manager for Endpoint Protection** tile will not be listed in Fixlet Collections module.

Figure 5. Fixlets page - Overview



3. You are redirected to the Fixlets overview page. The Fixlets overview page contains the following:
    - **Refine My Results** is located on the left side of the Fixlets page. Use **Refine My Results**, to refine the search results based on the following filters:
        - **Category**: You can filter the Fixlets based on Application Deployment, Application Maintenance, Audit, AV Alert and Configuration. Clicking **Show More** opens a dialog box, which contains additional filters and search bar.
        - **Release Date**: Filters the Fixlets based on the release date.

        Note:

        Use **Collapse All** and **Expand All** button to expand and collapse the filters in Refine My Results.

        Use **Reset filters** option to clear the applied filter.

- **Select All**: This feature allows you to select all the Fixlets in a page.
- **Deploy**: Use this feature to deploy the Fixlets, the number in parentheses indicates the number of Fixlets selected. Deploying Fixlets is similar to deploying latest antivirus. For more information. see Deploying Latest antivirus definitions *(on page 14)*.
- You can search for Fixlets by using **Search** feature.
- Use **Sort by** to view Fixlets based on Release Date, Open Deployments, and Content Item Name.
- Use **Show/Hide Details** icon to toggle between list and detail view. The detailed view gives more information about the Fixlet such as Fixlet name, Description, ID, CVE IDs, and so on. Whereas list view shows only the Fixlet name, Applicable Devices, and Open Deployment.
- Use **View** feature to increase or decrease the number of Fixlets in a page.
- You have pagination feature at the top-right corner and bottom of the page, use this feature to toggle between the pages.

4. Click **Fixlet** to view the properties of the individual Fixlet.

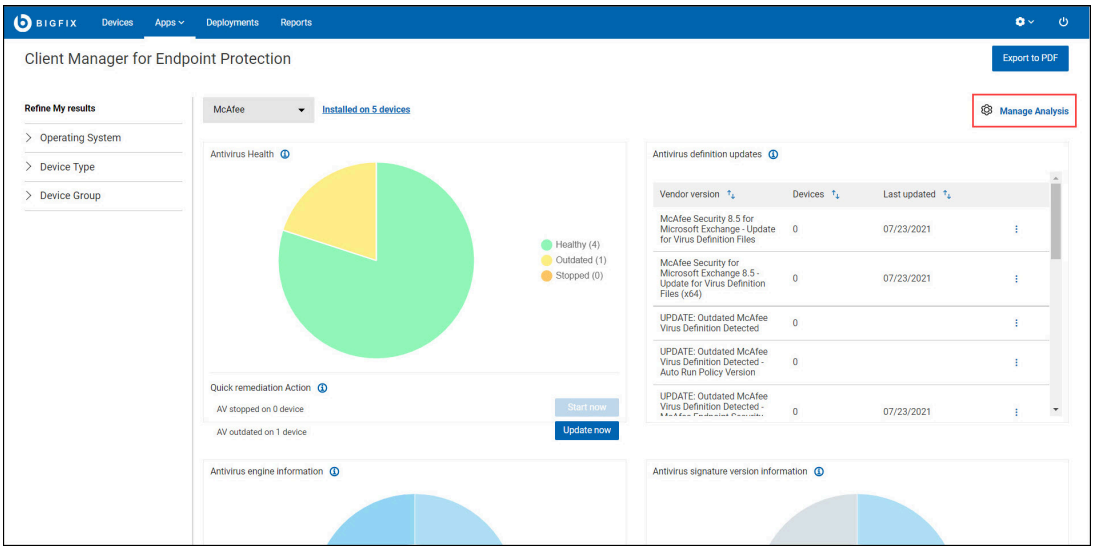
You are redirected to the Fixlet properties page, which contains Overview, Applicable Devices, and Deployments. You can also deploy the Fixlet from the Fixlet properties page.

Managing Analyses

Use Manage Analysis to view the status of the antivirus and their versions and also to generate reports by activating analyses.

With Manage Analyses, you can control what antivirus information and deployment status to collect from your managed devices.

Figure 6. McAfee dashboard - Manage Analysis

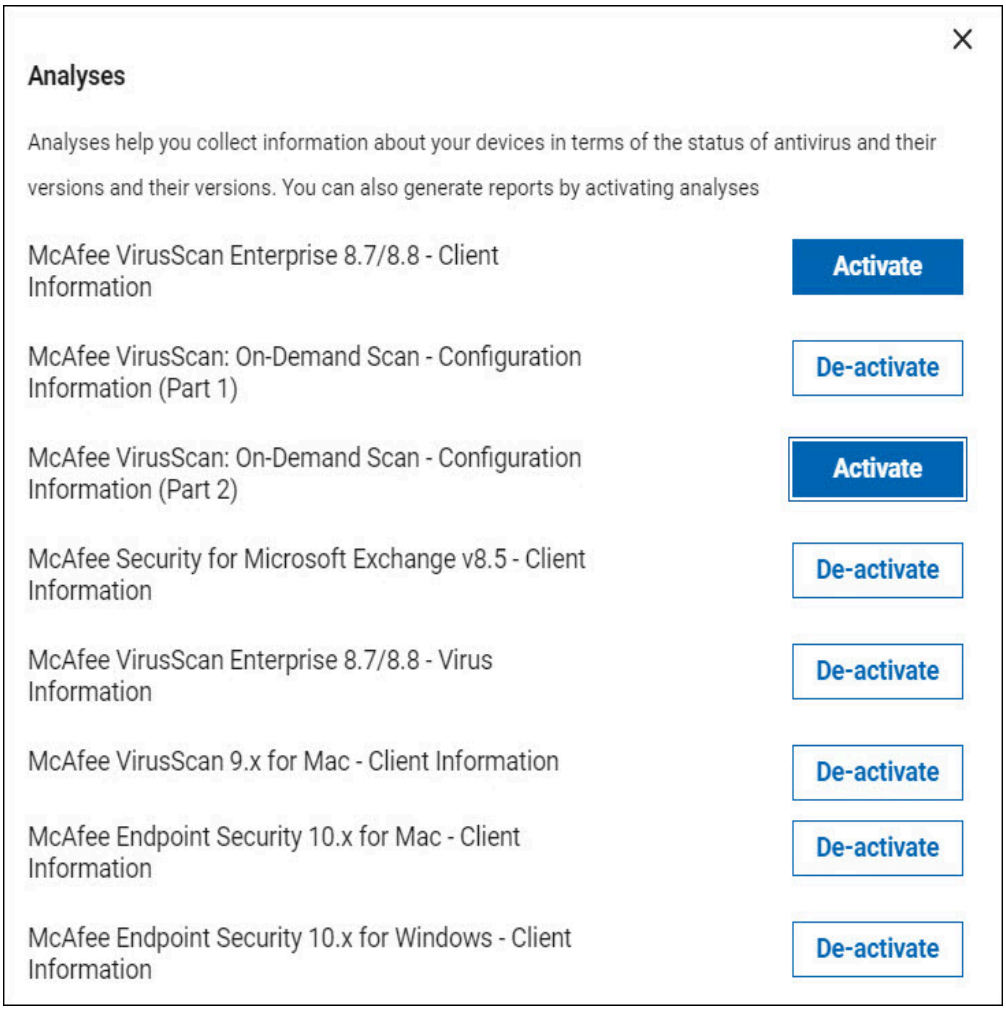


Manage analysis provides a mechanism for activating or deactivating the CMEP App analysis for a particular product.

Note: The total number of installed devices from an antivirus application might not equal the total number of devices with engine information or signature information, because all engine information might not be available through the CMEP App analyses.

- **Activate**: Starts collecting reports for a particular antivirus status and their versions.
- **Deactivate**: Stops collecting reports for a particular antivirus products on the devices.

Figure 7. Analyses slider

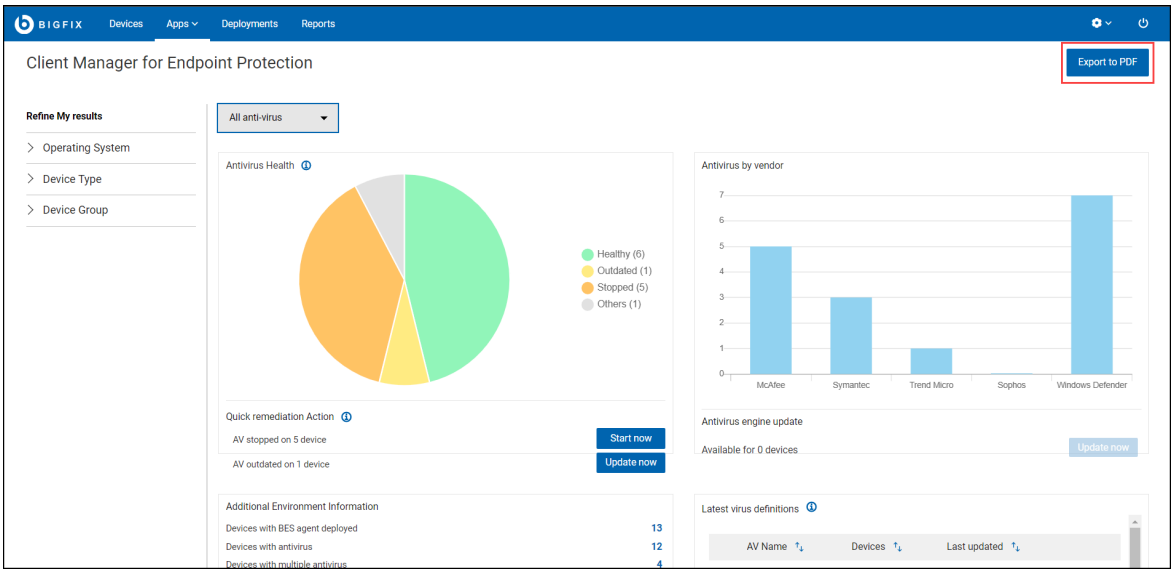


Exporting Report

Use Export to PDF feature to save CMEP App overview or individual vendor dashboard reports.

You can export any dashboard reports to PDF format:

1. In the CMEP App overview or individual vendor dashboard page, click **Export to PDF**.



2. The report is generated in PDF format.

Note: The PDF report will be saved in the default downloads location of the device.

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or

any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.