

**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 \(on page xxix\)](#).

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. System Requirements.....	5
Chapter 2. Overview.....	6
Chapter 3. Using Refine My results.....	11
Chapter 4. Uploading packages.....	12
Chapter 5. Deploying Latest Antivirus Definitions.....	17
Chapter 6. Viewing Device Details.....	21
Chapter 7. Viewing Fixlets.....	23
Chapter 8. Managing Analyses.....	26
Chapter 9. Exporting Report.....	28
Notices.....	xxix

Chapter 1. System Requirements

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

- Users must have a license for BigFix Compliance. This license can come from Compliance, Workspace, and Enterprise.
- Ensure that the CMEP site is enabled from the License Overview dashboard in Console and subscribed to the devices from Console CMEP site.



Important: CMEP only supports the devices with Mac and Windows platforms. See the BigFix CMEP Support Matrix for latest information on the supported antivirus products and functions at [CMEP Support Matrix](#) .



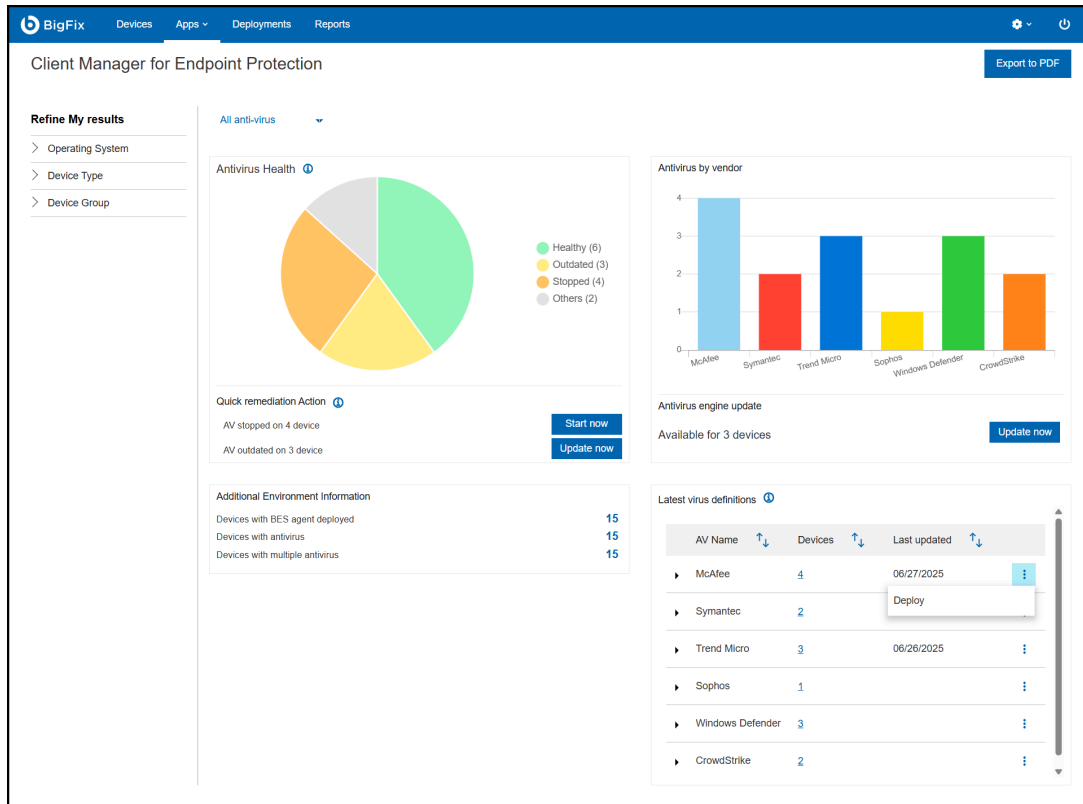
Note: For each supported antivirus product, the CMEP supports all the platforms that are currently supported by the antivirus product, if the platform is also supported by the BigFix agent. To verify the BigFix support scope, see the BigFix system requirement reports at Detailed System Requirement.

Chapter 2. Overview

This task provides a quick status summary of antivirus products deployed on all the devices managed by BigFix.

To navigate to the CMEP Application, log in to WebUI and select **Apps > CMEP** in the top navigation bar.

Figure 1. Overview



The overview page contains four tiles:

1. **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 - **Outdated:** The antivirus definition is out of date and needs to be updated on the device.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.
2. **Antivirus by vendor:** A bar graph, which displays the number of antivirus product installed by an individual vendor.

3. **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).
4. **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 \(on page 17\)](#).

The left panel of the homepage includes a **Device Filter**, which allows you to specify the criteria displayed in the Overview Report.

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

Individual vendor dashboard - Overview

CMEP provides a dashboard for each supported antivirus product.

To view the individual vendor dashboard, click all antivirus dropdown menu in the CMEP application overview page and select the antivirus vendor.



Note: Other antivirus products show the engine and signature version details. CrowdStrike does not show these details; it shows the Falcon Sensor version instead.

Figure 2. Dashboard-McAFee

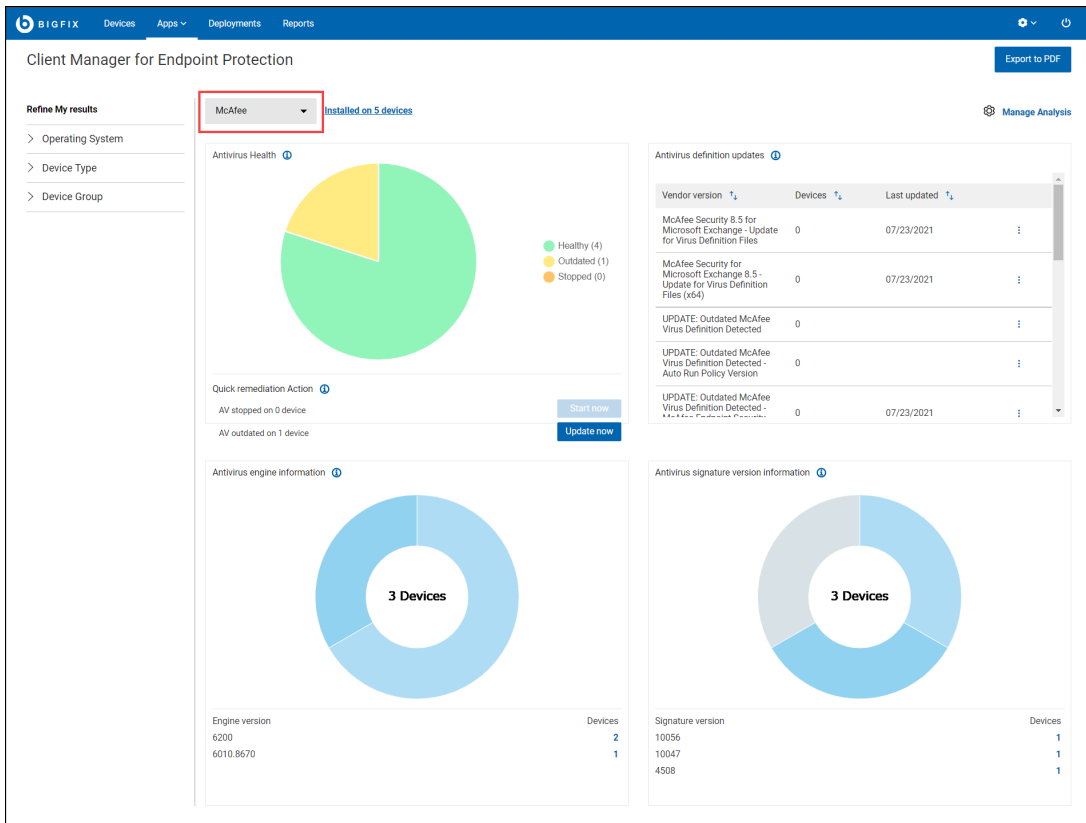
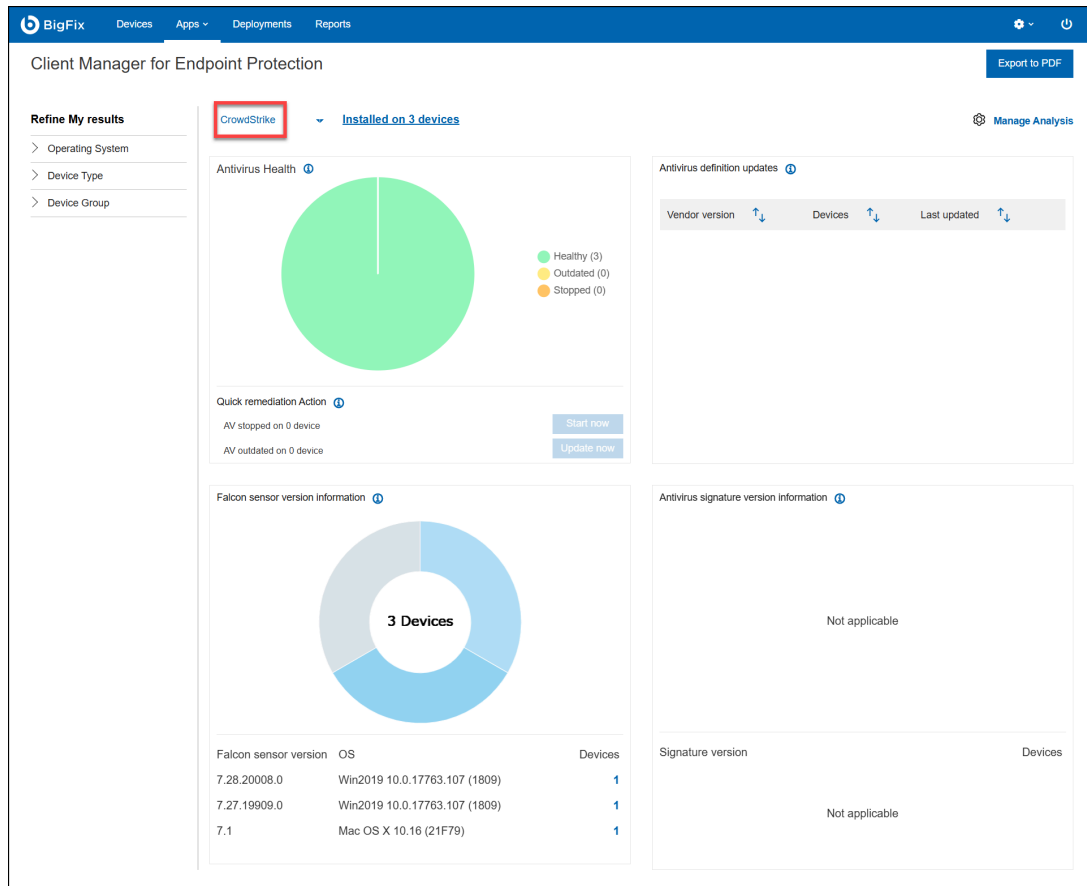


Figure 3. Dashboard-CrowdStrike



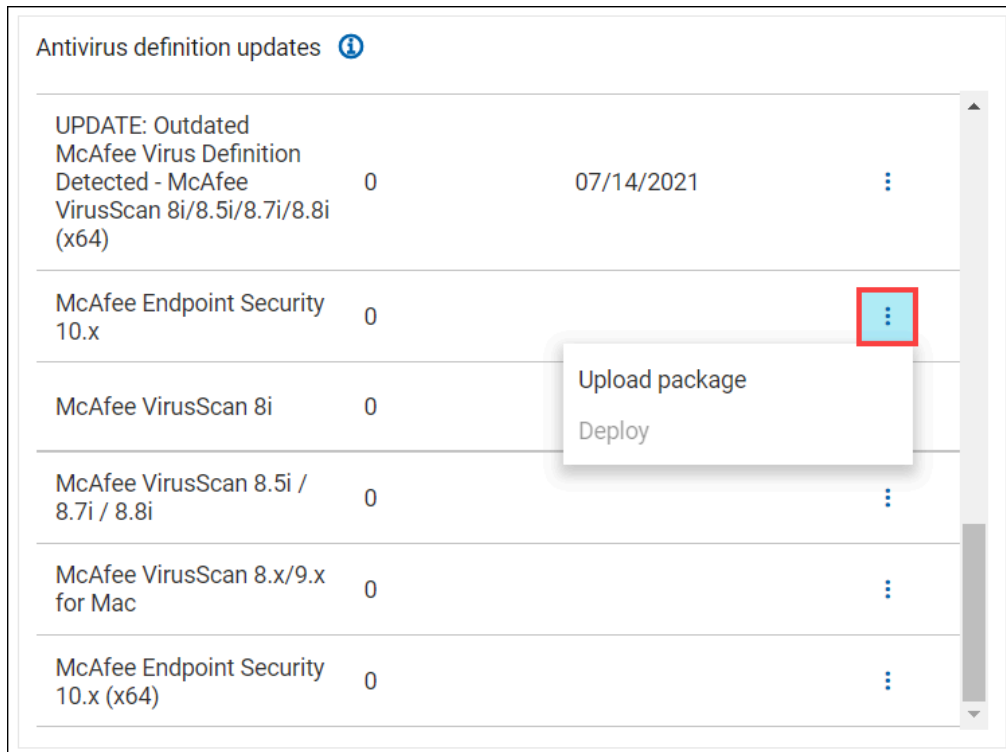
The individual vendor dashboard overview page contains four tiles:

1. **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.
2. **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 \(on page 17\)](#).


Figure 4. Antivirus definition updates



Antivirus definition updates ⓘ			
UPDATE: Outdated McAfee Virus Definition Detected - McAfee VirusScan 8i/8.5i/8.7i/8.8i (x64)	0	07/14/2021	⋮
McAfee Endpoint Security 10.x	0		⋮
McAfee VirusScan 8i	0		
McAfee VirusScan 8.5i / 8.7i / 8.8i	0		⋮
McAfee VirusScan 8.x/9.x for Mac	0		⋮
McAfee Endpoint Security 10.x (x64)	0		⋮

3. **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:** CMEP supports all engine versions of antivirus products. Therefore, the number of devices shown here may differ from the vendor's total device count.

 **Note:** For CrowdStrike, antivirus engine version details are not available; Falcon Sensor version information is provided instead.

4. **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.

 **Note:** The antivirus signature version is not applicable for CrowdStrike.

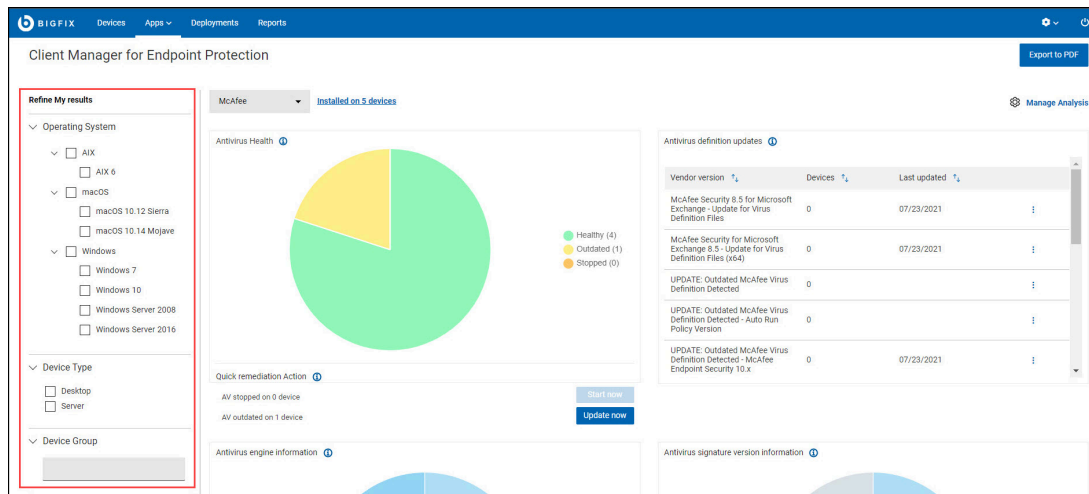
Chapter 3. Using Refine My results

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

Refine My results is located on the left side of the CMEP Application 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 5. Refine My results



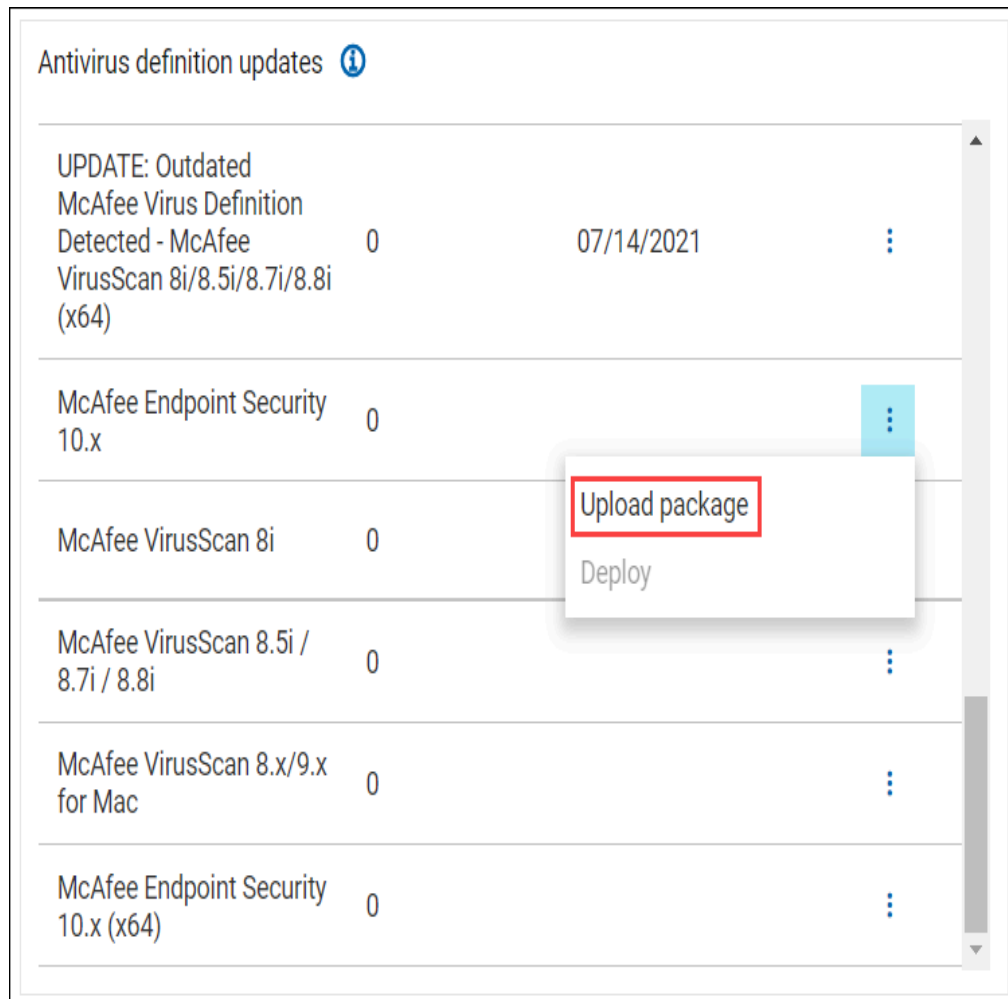
Chapter 4. Uploading packages


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**.

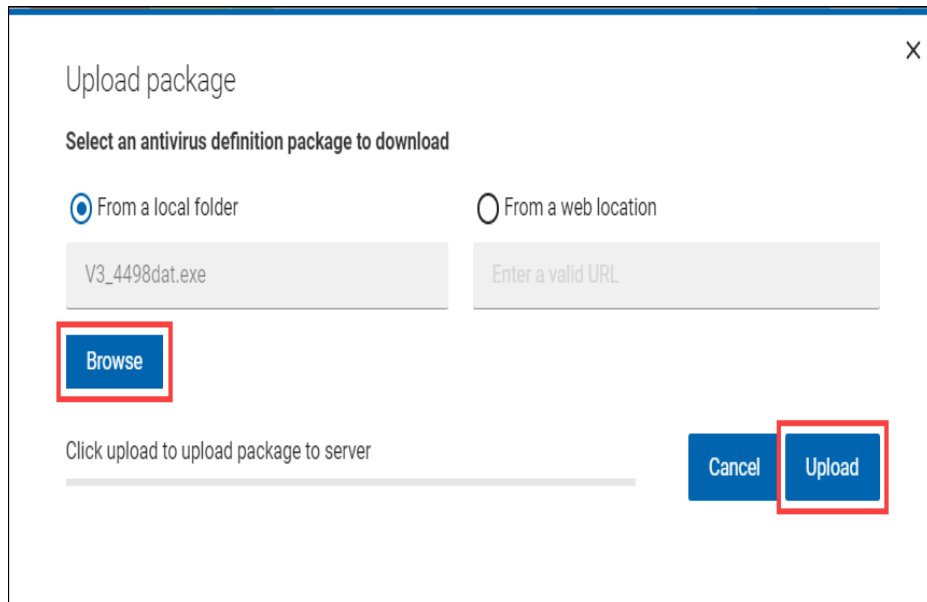
Figure 6. Antivirus definition updates



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

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

Figure 7. Upload package From a local folder



Upload package

Select an antivirus definition package to download

From a local folder From a web location

V3_4498dat.exe Enter a valid URL

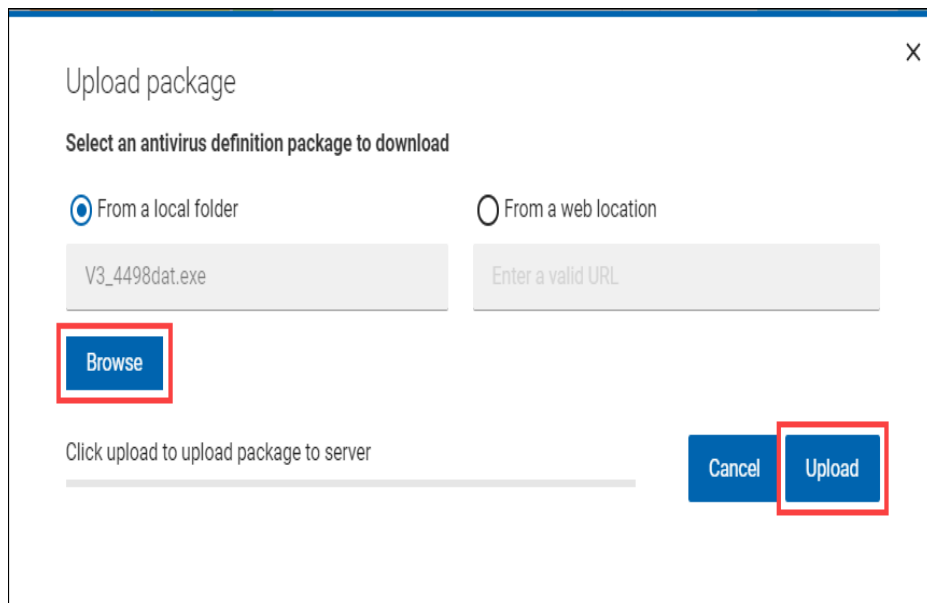
Browse

Click upload to upload package to server

Cancel Upload

- b. 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**.

Figure 8. Upload package From a local folder



Upload package

Select an antivirus definition package to download

From a local folder From a web location

V3_4498dat.exe Enter a valid URL

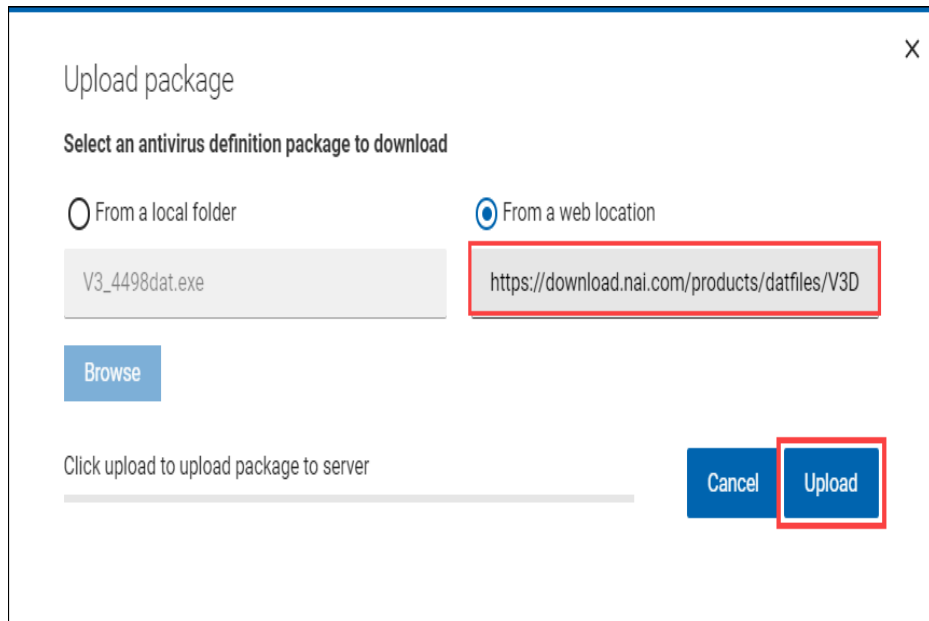
Browse

Click upload to upload package to server

Cancel Upload

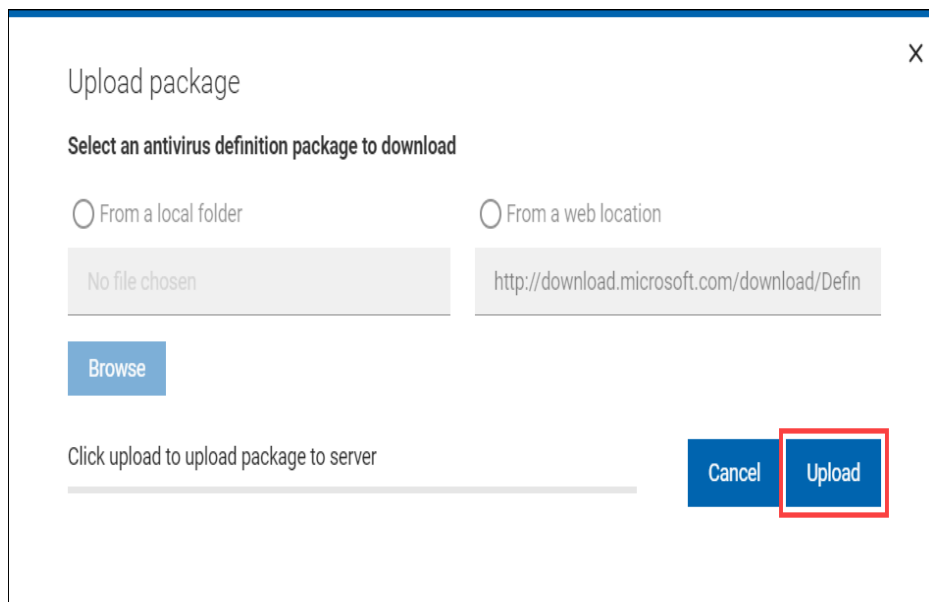
- c. From a web location: Check **From a web location** and then enter the URL of the antivirus definition package. Click **Upload**.

Figure 9. Upload package From a web location



- d. 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.

Figure 10. Windows Defender - Upload package



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


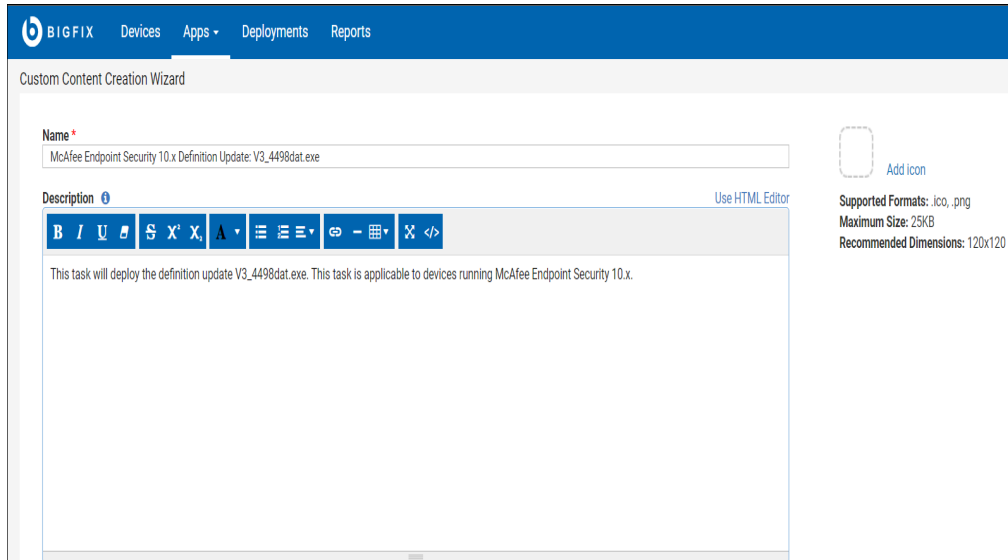
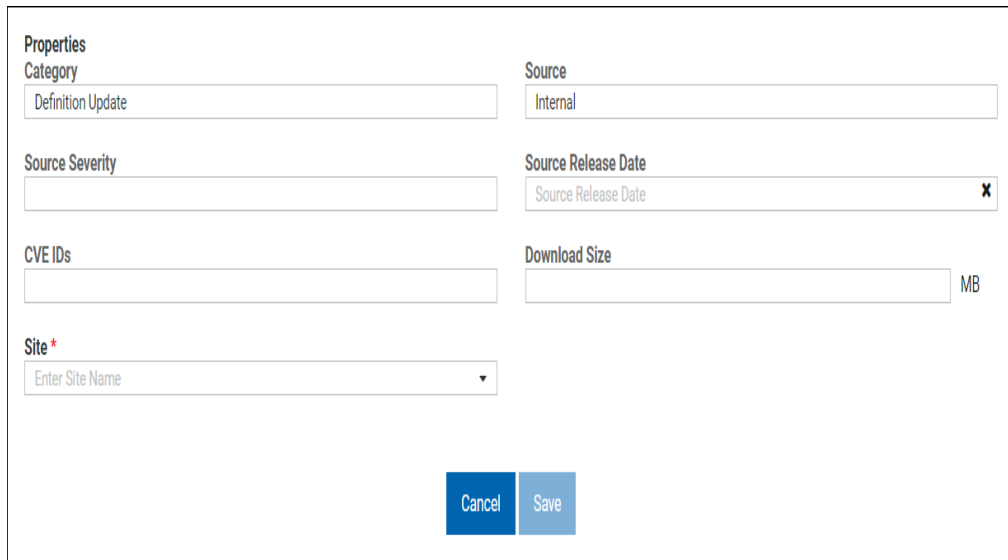
 **Note:** The **Custom Content Creation Wizard** page gives an overview of the Fixlet and its relevance and action.

Figure 11. Custom Content Creation Wizard



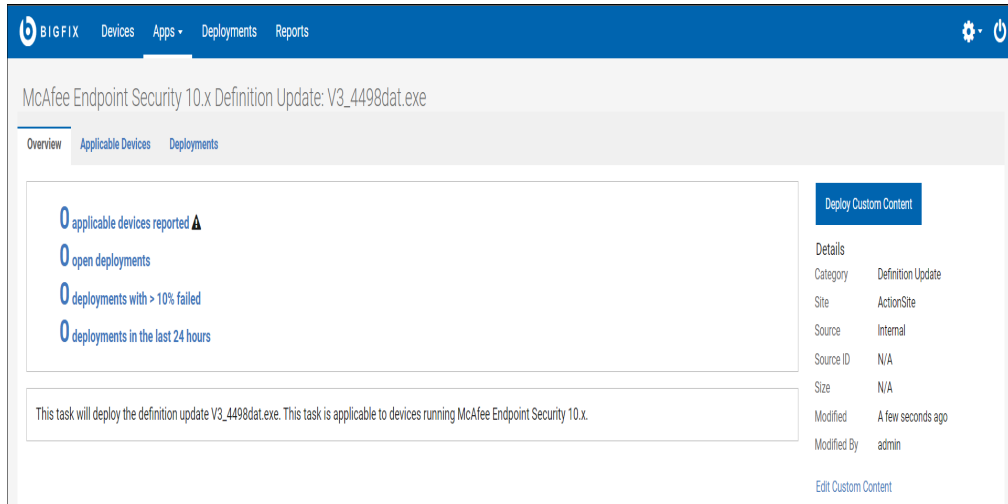
4. Select **Source Release Date** and the **Site** where you want to save the custom content. Click **Save**.

Figure 12. Source Release Date



The Fixlet overview is displayed as shown:

Figure 13. Fixlet overview



5. To deploy Custom Content, see [Deploying Latest Antivirus Definitions \(on page 17\)](#).

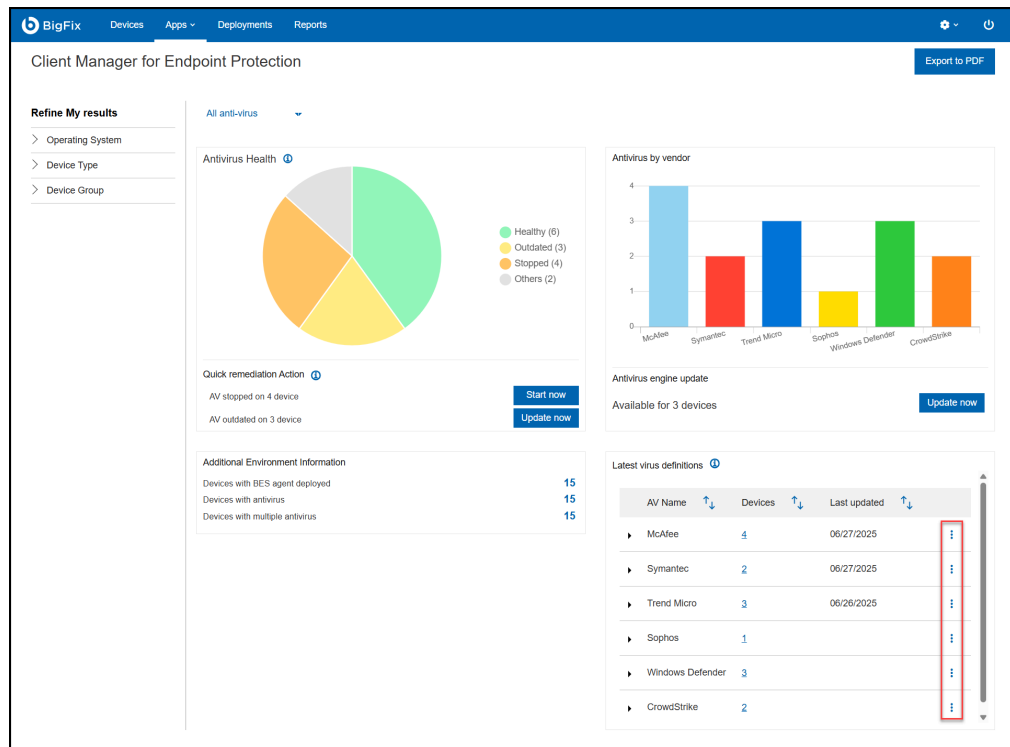
Chapter 5. Deploying Latest Antivirus Definitions

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 Application overview page, click on the vertical **ellipsis** in the **Latest virus definitions** tile.

Figure 14. Latest virus definitions



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 Application 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.

Figure 15. Deploy

AV Name	Devices	Last updated	
McAfee	1	04/14/2021	⋮
Symantec	0	04/13/2021	⋮
Trend Micro	1	04/13/2021	⋮
Sophos	0		⋮

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

Figure 16. Deployment summary

Deploy Content from Client Manager for Anti-Virus

Select content Select action Select targets Configure

1 Task Clear All (1)

UPDATE: Outdated McAfee Virus D... Default: Action1 Click here to initiate the deployment process.

Action Description
NoDescription

Select action
Click here to initiate the deployment process. (Action1)

Deployment Summary

Deployment Name
UPDATE: Outdated McAfee Virus Definition Def

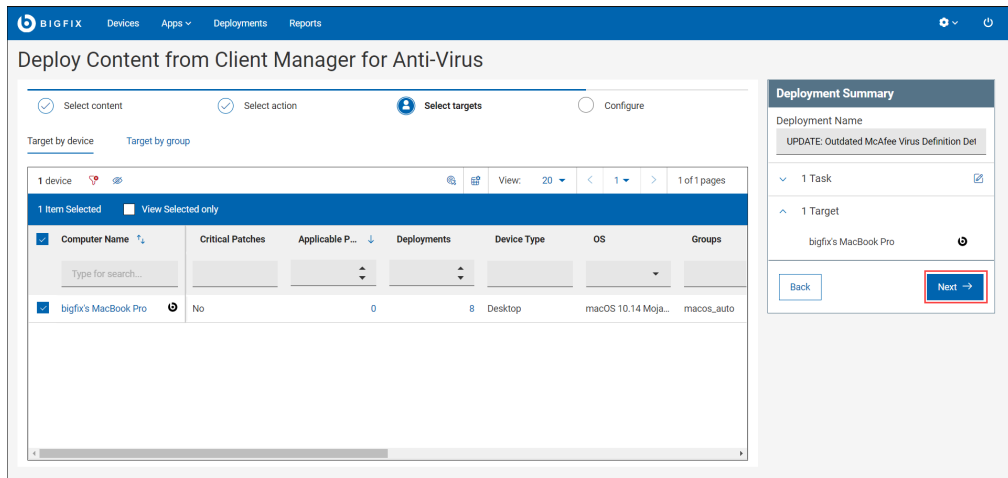
1 Task ⊕

UPDATE: Outdated McAfee Virus Def...
Default action

Back Next →

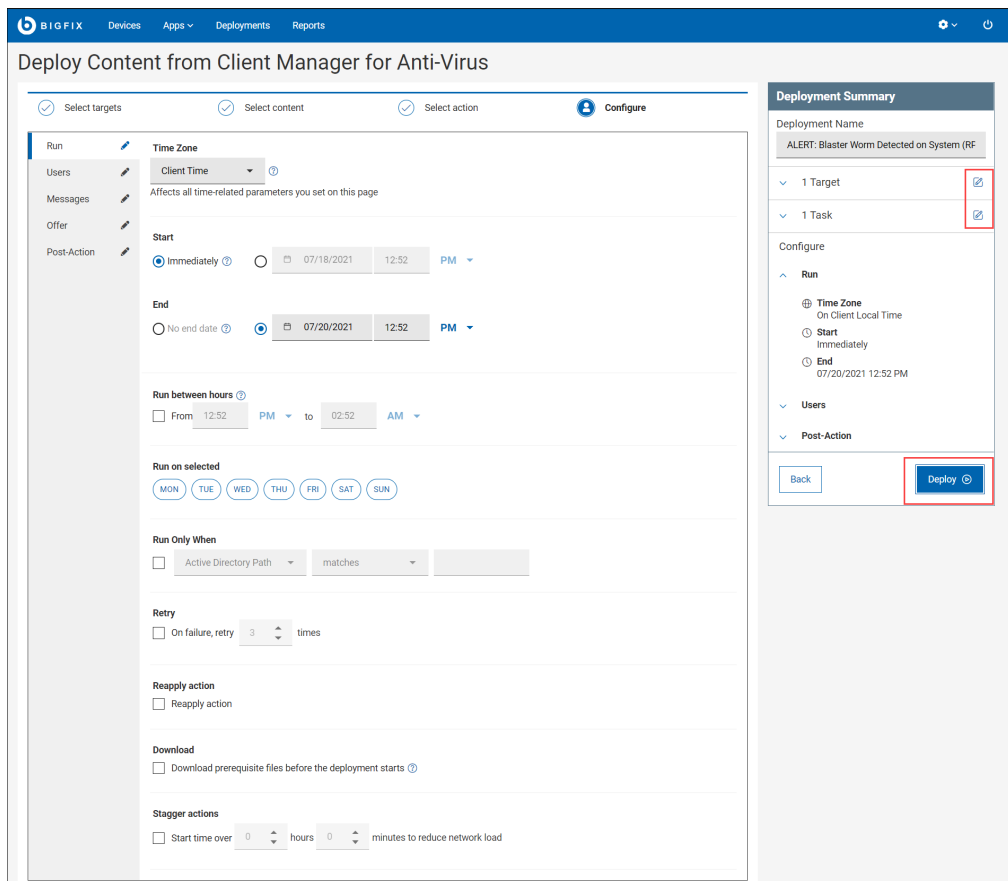
4. The **Select targets** tab, select the targets and click **Next**.

Figure 17. Select targets



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

Figure 18. Deploy content from client manager for Anti-virus



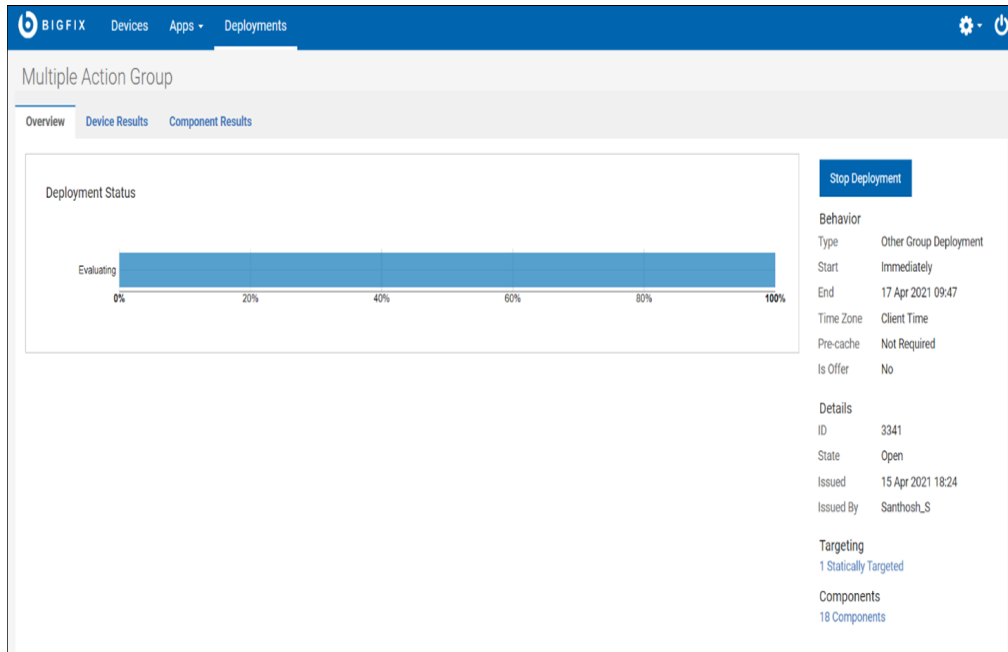
 **Note:**



- 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, End date, and so on.

The deployment status is displayed as shown.

Figure 19. Stop Deployment



Click **Stop Deployment** to stop the deployment on the endpoints.

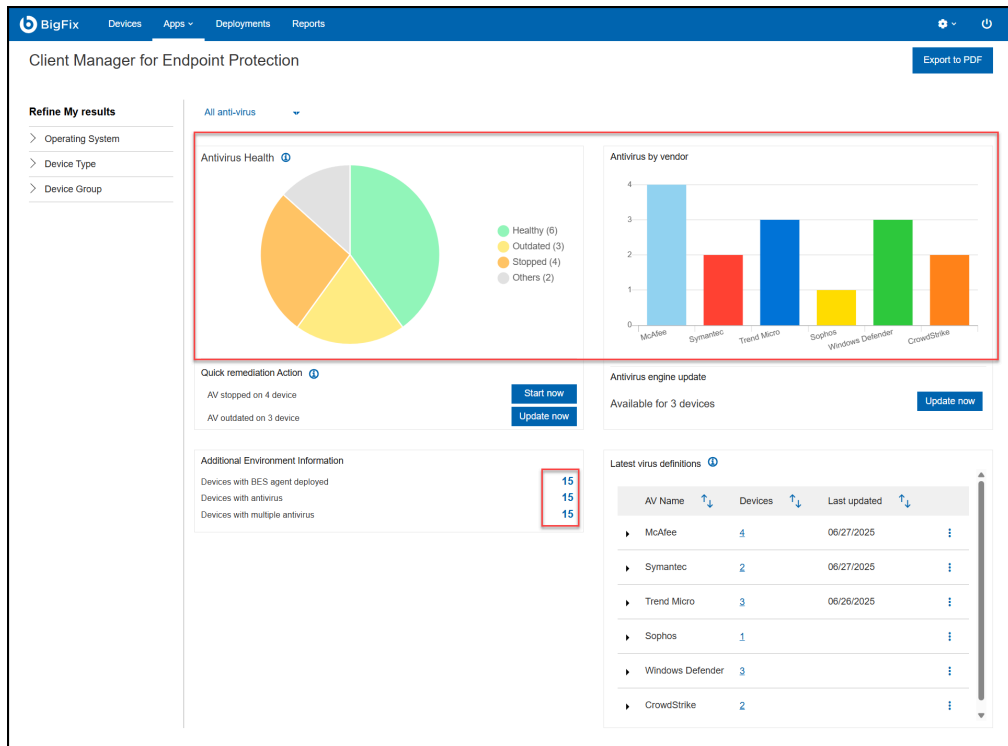
Chapter 6. Viewing Device Details

This task 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 Application 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.

Figure 20. Antivirus Health



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

Figure 21. Available devices

The screenshot shows the BigFix Client Manager for Endpoint Protection interface displaying a list of available devices. The table below shows the details for 6 items.

Name	ID	Last Reported	IP Address	Operating system	Device type
WIN7X61-01	1625403765	07/26/2021 16:2	10.134.131.55	Windows:Windows 7--Win7 6.1.7601	Server
DESKTOP-AAML1C1J	1073785049	07/26/2021 16:0	10.134.130.19	Windows:Windows 10--Win10 10.0.10586.0 (1511)	Server
bigfix's Mac (2)	543819886	07/26/2021 15:57	10.134.134.88	macOS:macOS 10.12 Sierra--Mac OS X 10.12 (16A323)	Desktop
WIN-AB010BFPGGH	1626299414	07/26/2021 15:53	10.134.130.35	Windows:Windows Server 2008--Win2008 6.0.6001	Server
WIN-CV100STPD6S	1088798098	07/26/2021 15:43	10.14.76.10	Windows:Windows Server 2016--Win2016 10.0.14393.2273 (1607)	Server
DESKTOP-40B7BP8	1083160578	07/23/2021 23:41	10.134.131.62	Windows:Windows 10--Win10 10.0.19041.1052 (2009)	Server

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

Figure 22. Device Properties

The screenshot shows the BIGFIX web interface for a device named DESKTOP-AAMLC1J. The interface is divided into several sections:

- Navigation Bar:** Contains the BIGFIX logo and menu items: Devices, Apps, Deployments, Reports.
- Device Name:** DESKTOP-AAMLC1J
- Summary Cards:**
 - 0 Critical Vulnerabilities
 - 0 Failed Deployments
 - Last Reported: 9 minutes ago (26 Jul 2021 16:00)
 - OS: Win10 10.0.10586.0 (1511)
 - User: bigfix
 - 28.30 GB Free Disk Space
- System Details Table:**

CPU	2400 MHz Xeon Gold 6148	DNS Name	DESKTOP-AAMLC1J
Active Directory Path	<Not specified>	IP Address	10.134.130.19
IPv6 Address	fe80:0:0:91a7:d124:2e03:d942	Device Type	Server
ID	1073785049	RAM	8192 MB
Total Size of System Drive	81417 MB	BIOS	12/12/2018
Subnet Address	10.134.130.0		
- Details Sidebar:**
 - IPs: 10.134.130.19
 - OS: Win10 10.0.10586.0 (1511)
 - DNS: DESKTOP-AAMLC1J
 - Device Type: Server
 - Groups: win10
 - Locked: No
 - Last Seen: 9 minutes ago
 - Last User: bigfix
- Buttons:** Deploy, More, Add Property Group.



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

Chapter 7. Viewing Fixlets

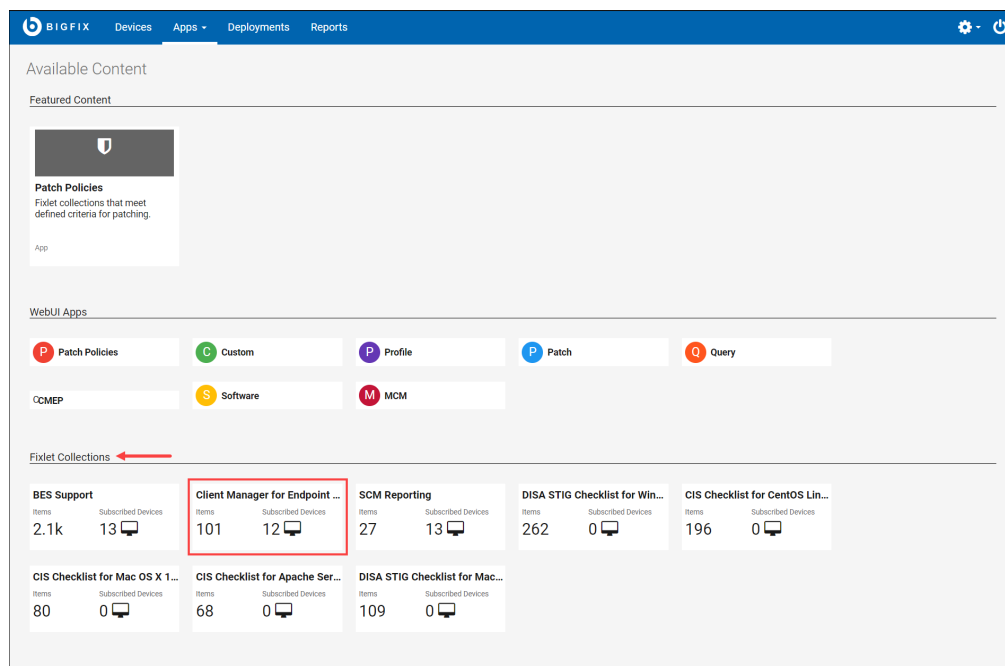
This topic describes how to view the CMEP Application Fixlets.

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

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

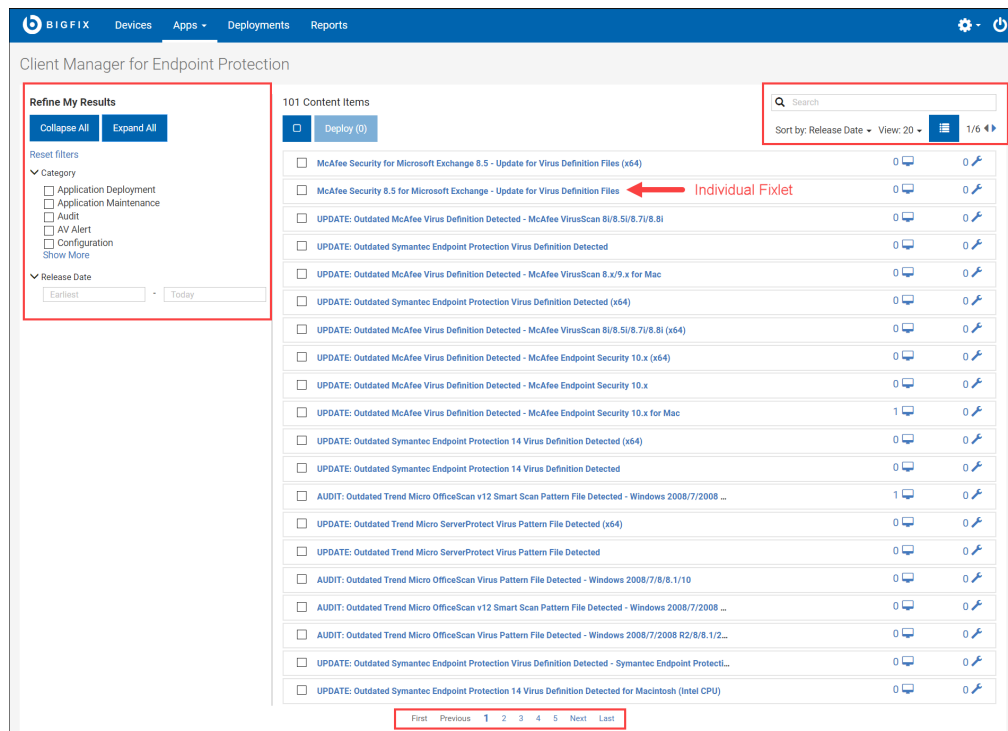
1. Log in to **WebUI** and select **Content** from the Application menu.
2. Click **Client Manager for Endpoint Protection** in the Fixlet Collections module.

Figure 23. Fixlet Collections



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

Figure 24. 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, antivirus 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 \(on page 17\)](#).
- 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.

Figure 25. Fixlet properties page



BigFix

Devices Apps Deployments Reports

McAfee Security for Microsoft Exchange 8.5 - Update for Virus Definition Files (x64)

Overview Applicable Devices Deployments

0 applicable devices reported

0 open deployments

0 deployments with > 10% failed

0 deployments in the last 24 hours

Deploy Content

Details

Category	Definition Update
Site	Client Manager for Anti-Virus
Source	McAfee
Source ID	N/A
Size	143.43 MB
Released	8/11/21
Modified	4 months ago

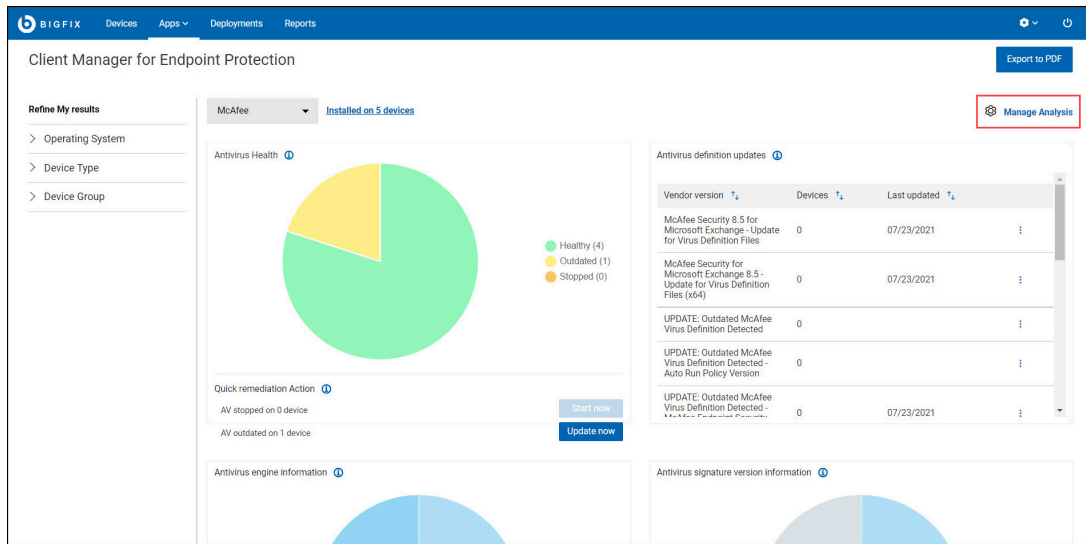
BigFix has detected that McAfee Security for Microsoft Exchange 8.5 is using an outdated virus definition file to scan affected computers. To ensure that your anti-virus software can protect against the latest threats, McAfee recommends immediately upgrading to the latest virus definition file.

Chapter 8. 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 26. McAfee dashboard - Manage Analysis



Manage analysis provides a mechanism for activating or deactivating the CMEP Application 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 Application 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 27. Analyses slider

Analyses ✕

Analyses help you collect information about your devices in terms of the status of antivirus and their versions and their versions. You can also generate reports by activating analyses

McAfee VirusScan Enterprise 8.7/8.8 - Client Information	Activate
McAfee VirusScan: On-Demand Scan - Configuration Information (Part 1)	De-activate
McAfee VirusScan: On-Demand Scan - Configuration Information (Part 2)	Activate
McAfee Security for Microsoft Exchange v8.5 - Client Information	De-activate
McAfee VirusScan Enterprise 8.7/8.8 - Virus Information	De-activate
McAfee VirusScan 9.x for Mac - Client Information	De-activate
McAfee Endpoint Security 10.x for Mac - Client Information	De-activate
McAfee Endpoint Security 10.x for Windows - Client Information	De-activate

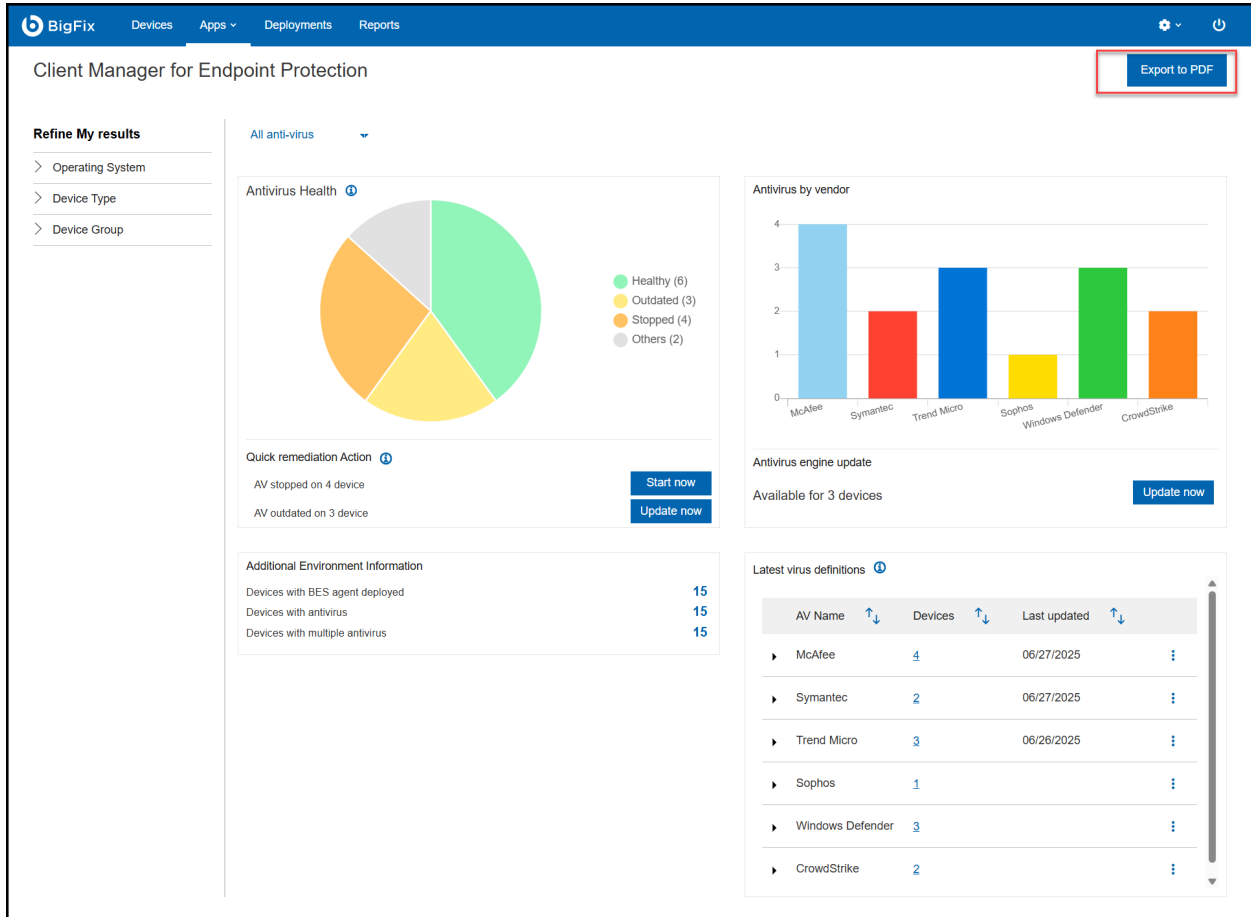
Chapter 9. Exporting Report

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

You can export any dashboard reports to PDF format:

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

Figure 28. Exporting Report



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.