BigFix
Asset Discovery User's Guide

Special notice

Before using this information and the product it supports, read the information in Notices (on page 49).

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Chapter 1. Setting up your environment

Learn how BigFix Asset Discovery works.

BigFix Asset Discovery has some key uses in enterprise environments:

- Identification of network assets, including devices such as routers, printers, switches, wireless access points, or anything with an IP address.
- Identification of unmanaged and rogue computers including computers that have had the BigFix agent disabled or rogue computers that are not managed by the company.

With this information, important license inventory questions can be answered regarding what kind of device it is, when it was installed and where it is located. Additionally, security questions and concerns can be answered regarding unauthorized employee computers, wireless units or rogue devices on the network.

The BigFix Asset Discovery solution is unique because the scanning is done by other agents of nearby computers. This is known as distributed scanning. This approach has several key benefits:

- Conserves WAN bandwidth
- Scanning can be done in parallel for much faster results, in minutes instead of weeks
- Can be easily customized to work in complex network configurations, including isolated subnets
- Individual subnets can run customized scan types

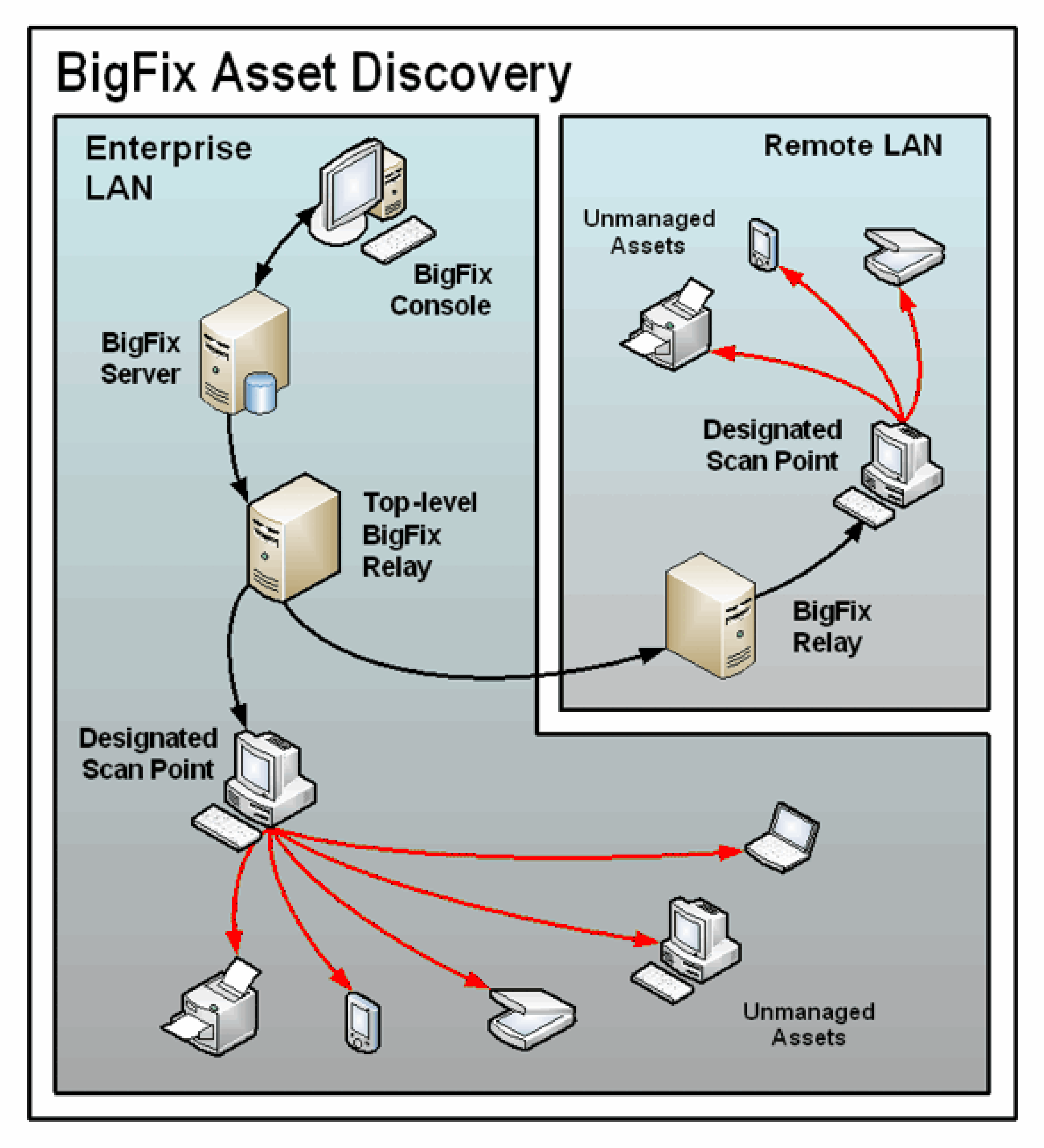
BigFix Asset Discovery works by using Fixlet and Tasks to deploy Scan Points to specified agents in your network. You can then use other Fixlets and Tasks to run Nmap scans at intervals of your choosing. Scan results are automatically sent to the BigFix server, which imports the data into the BigFix database. The scan information can then be viewed in the BigFix console using the *Unmanaged Assets* tab.

Note: On Linux platforms, you must install the BES Server Plugin Service to work with the Asset Discovery Fixlets. This plug-in is available for installation in the BigFix Support site.

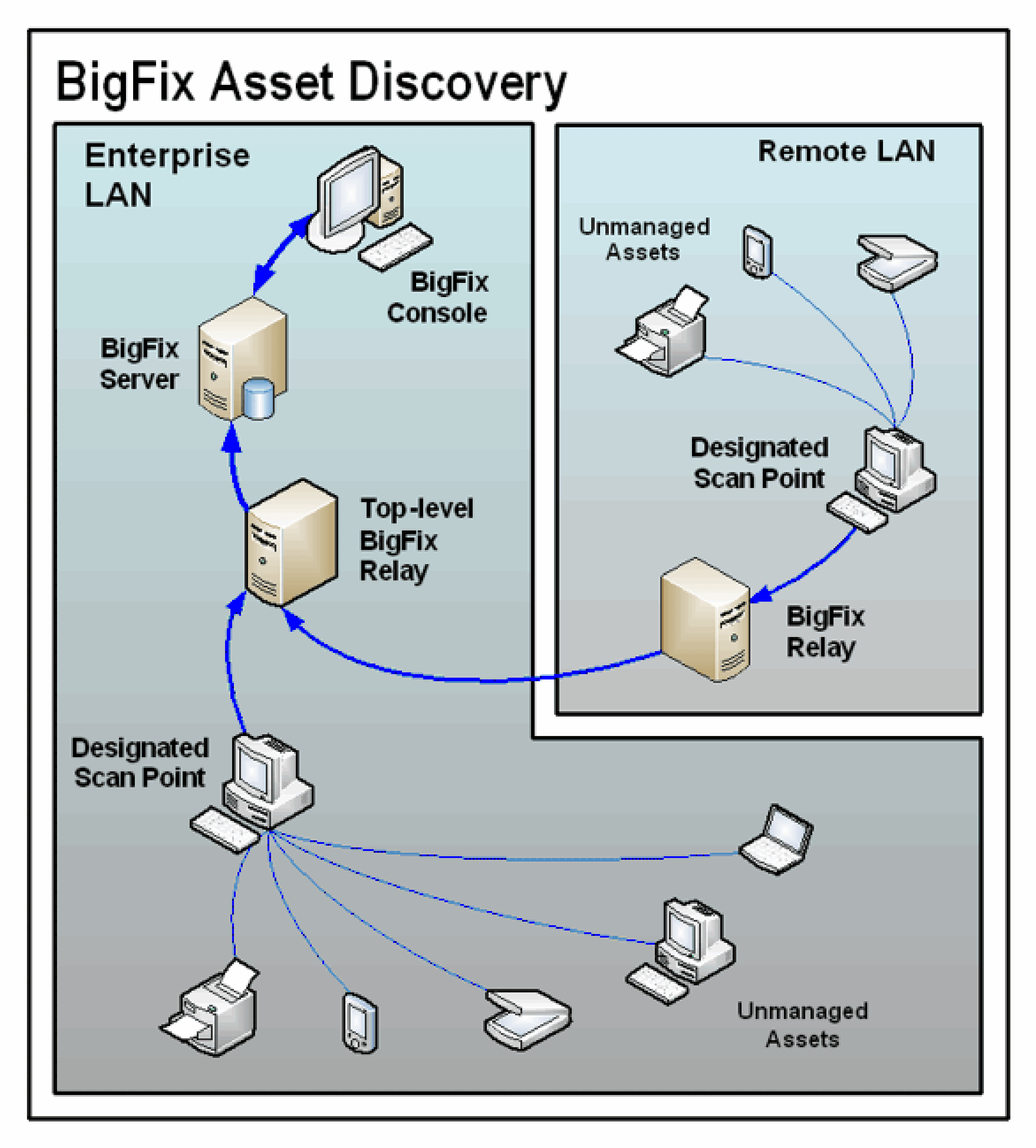
Chapter 2. Overview

A brief overview on how BigFix discovers assets and on what are Scan Points.

BigFix Asset Discovery works by designating certain computers as Scan Points. Any agent can be designated as a Scan Point if it is running a supported operating system. These Scan Points query the unmanaged assets in your network. The following image illustrates this process.



Information is retrieved from these unmanaged assets by the Scan Points and sent back through relays to the database on the BigFix server. From there, you can examine the results on the BigFix console:



Scan Point hardware and software requirements

BigFix Nmap Scan Point runs where BigFix Agent is supported, on all Windows (x86-64), Red Hat Enterprise Linux 7.4 and higher (x86-64), Red Hat Enterprise Linux 8 and higher (x86-64), Red Hat Enterprise Linux 9 and higher (x86-64), CentOS 7,8 (x86-64), Amazon Linux 2 (x86-64), Amazon Linux 2023 (x86-64).

Moreover, with an old Nmap version, BigFix Asset Discovery also supports Red Hat Linux 7 lower than 7.4.

Installation

Tasks to perform to complete a successful installation.

You can perform the following installation tasks in the Asset Discovery site:

- Enable the Unmanaged Asset Importer Service on your BigFix server.
- Designate specific agents as scan points.
- Run the scan.

Note: To view Unmanaged Assets, you must have the proper permissions set through the Administration Tool. To access the tool, click **Start > All Programs > BigFix Enterprise > BES Administration Tool**). A user can be granted permission to view all unmanaged assets or only those connected to the Scan Points that they administer.

Note: On Linux platforms, you must install the BES Server Plugin Service to work with the Asset Discovery Fixlets. This plug-in is available on the BigFix Support site.

Installing the site

Steps to perform to enable and subscribe all the computers to the external site.

To enable and subscribe all the computers to the external site using the BigFix Console, perform the following steps:

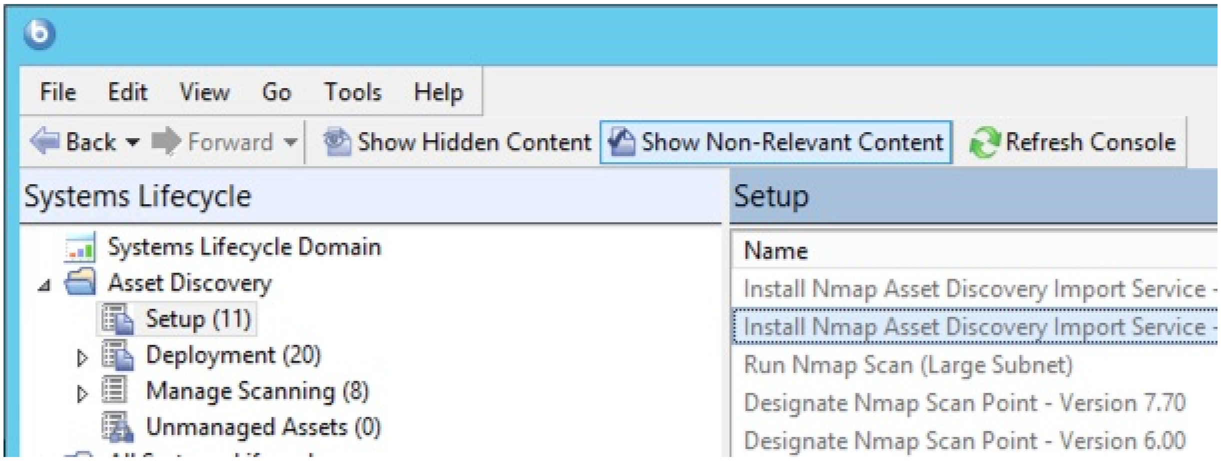
1. Open the BigFix Management domain and scroll to the top to view the associated dashboards.
2. In the Licensing dashboard, click the external site and enable it, if not already enabled, by clicking the name of the site in the list of sites.
3. In the properties panel of the external site, select the **Computer subscriptions** tab and click **All computers** to subscribe all the computers in the BigFix environment to the external site.
4. Click **Save Changes** to save the site subscription settings.

Installing the Import Service task

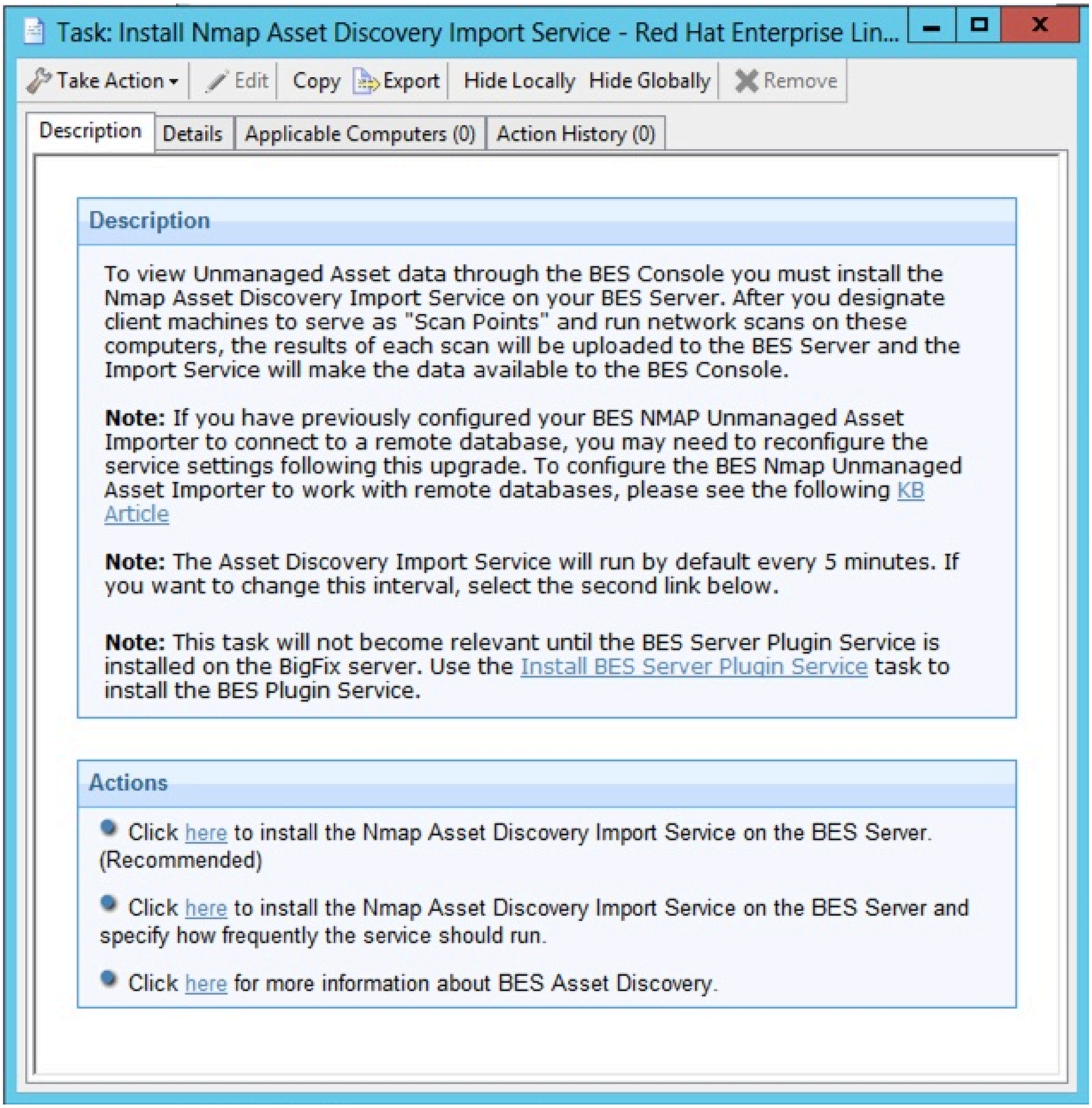
How to install the Nmap Asset Discovery Import Service on the BigFix server.

Note: When accessing a remote database, the NMAP Import Service needs to be run as a domain user, as you cannot use the standard local system to access to the SQL database. This service should be configured like other BigFix services in a remote database environment.

Select the Setup node in the Asset Discovery navigation tree to find the Install Nmap Asset Discovery Import Service Task in the right panel.


File
Edit
View
Go
Tools
Help
Back
Forward
Show Hidden Content
Show Non-Relevant Content
Refresh Console
Systems Lifecycle
Systems Lifecycle Domain
Asset Discovery
Setup (11)
Deployment (20)
Manage Scanning (8)
Unmanaged Assets (0)
Setup
Name
Install Nmap Asset Discovery Import Service -
Install Nmap Asset Discovery Import Service -
Run Nmap Scan (Large Subnet)
Designate Nmap Scan Point - Version 7.70
Designate Nmap Scan Point - Version 6.00

Click the task and view the description in the work area.



Description

To view Unmanaged Asset data through the BES Console you must install the Nmap Asset Discovery Import Service on your BES Server. After you designate client machines to serve as "Scan Points" and run network scans on these computers, the results of each scan will be uploaded to the BES Server and the Import Service will make the data available to the BES Console.

Note: If you have previously configured your BES NMAP Unmanaged Asset Importer to connect to a remote database, you may need to reconfigure the service settings following this upgrade. To configure the BES Nmap Unmanaged Asset Importer to work with remote databases, please see the following KB Article

Note: The Asset Discovery Import Service will run by default every 5 minutes. If you want to change this interval, select the second link below.

Note: This task will not become relevant until the BES Server Plugin Service is installed on the BigFix server. Use the Install BES Server Plugin Service task to install the BES Plugin Service.

Actions

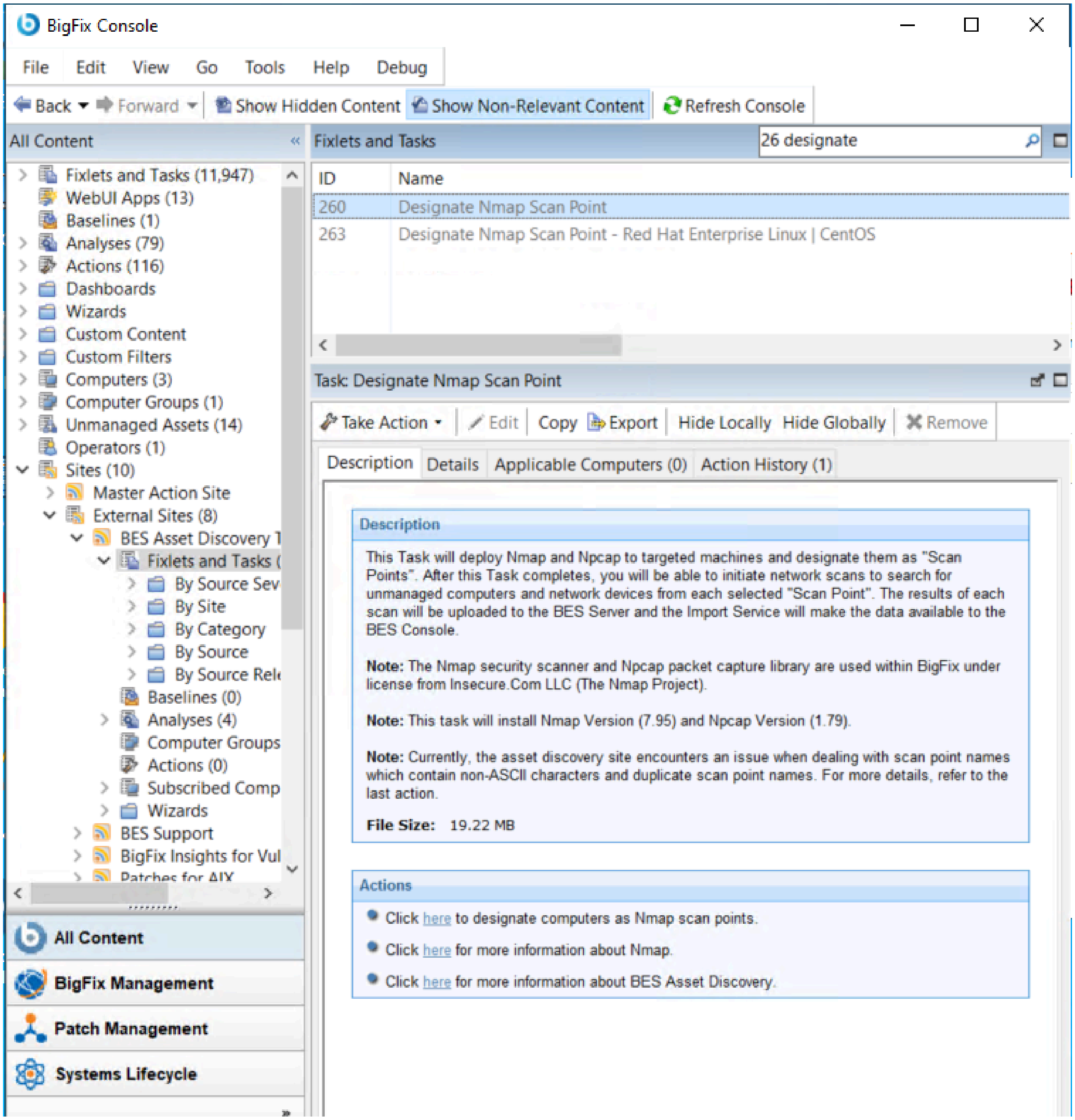
- Click here to install the Nmap Asset Discovery Import Service on the BES Server. (Recommended)
- Click here to install the Nmap Asset Discovery Import Service on the BES Server and specify how frequently the service should run.
- Click here for more information about BES Asset Discovery.

To install the Nmap Asset Discovery Import Service on the BigFix server, click the link in the Actions box. By default, the Import service runs every five minutes and checks for new Nmap scan data that has been delivered to the BigFix server. If you want to establish a different frequency, select the second Action link.

Installing Scan Points

Actions to perform to install Scan Points.

Select the Setup node in the Asset Discovery navigation tree to find the designation tasks on the right panel.



ID	Name
260	Designate Nmap Scan Point
263	Designate Nmap Scan Point - Red Hat Enterprise Linux | CentOS

Description

This Task will deploy Nmap and Npcap to targeted machines and designate them as "Scan Points". After this Task completes, you will be able to initiate network scans to search for unmanaged computers and network devices from each selected "Scan Point". The results of each scan will be uploaded to the BES Server and the Import Service will make the data available to the BES Console.

Note: The Nmap security scanner and Npcap packet capture library are used within BigFix under license from Insecure.Com LLC (The Nmap Project).

Note: This task will install Nmap Version (7.95) and Npcap Version (1.79).

Note: Currently, the asset discovery site encounters an issue when dealing with scan point names which contain non-ASCII characters and duplicate scan point names. For more details, refer to the last action.

File Size: 19.22 MB

Actions

- Click here to designate computers as Nmap scan points.
- Click here for more information about Nmap.
- Click here for more information about BES Asset Discovery.

The computers you designate as Scan Points must be running Windows or Linux. These Scan Points are the hubs from which the local subnet is scanned.

On Windows, click the Designate Nmap Scan Point Task.

Click the first Actions box link to access the Take Action dialog. From the Target tab, select the computers that you want to designate as Scan Points.

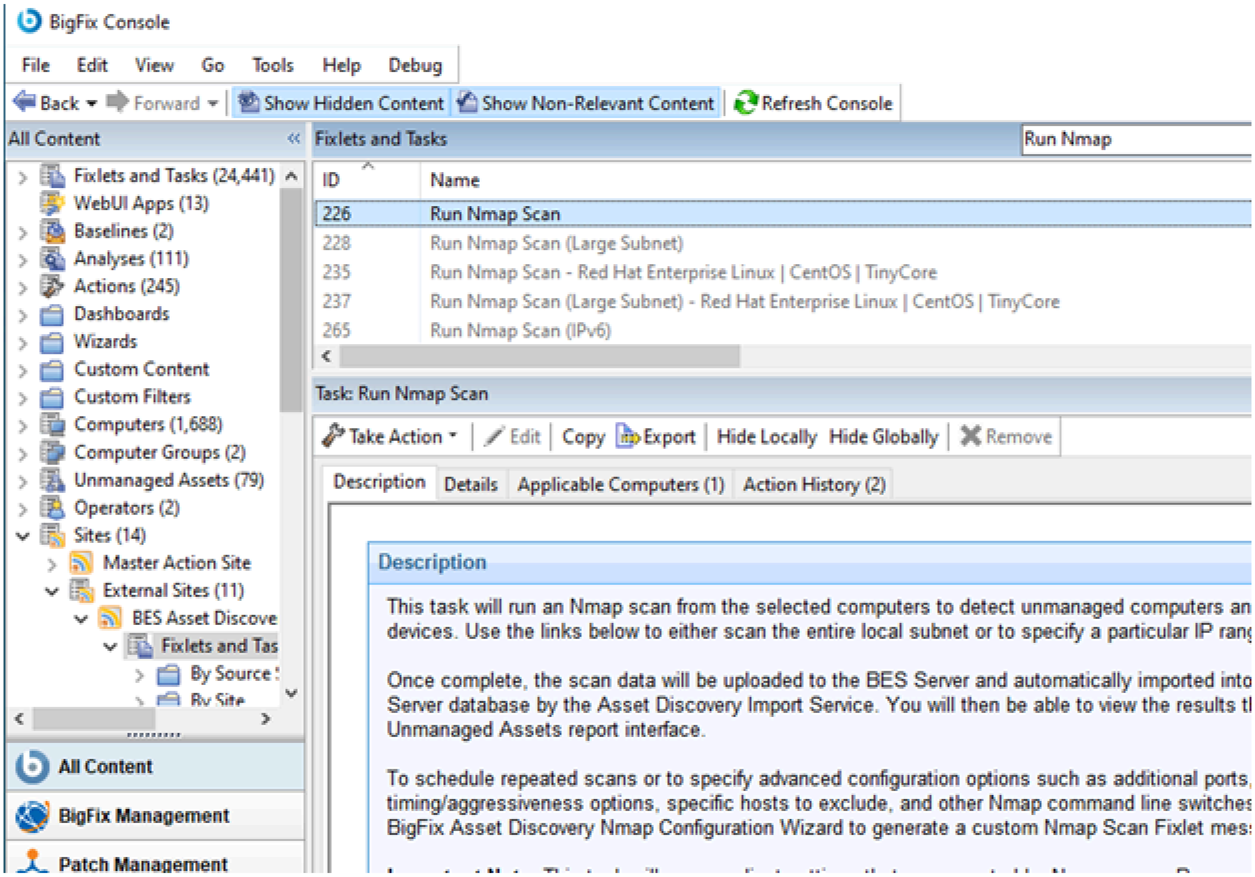
On Linux, click the Designate Nmap Scan Point - Red Hat Enterprise Linux Task.

Click the first Actions box link to designate the Nmap Scan Points.

Running a scan

How to perform a scan to detect unmanaged computers and network devices.

Select the Setup node in the Asset Discovery navigation tree to find all the task available to "Run Nmap Scan".



ID	Name
226	Run Nmap Scan
228	Run Nmap Scan (Large Subnet)
235	Run Nmap Scan - Red Hat Enterprise Linux | CentOS | TinyCore
237	Run Nmap Scan (Large Subnet) - Red Hat Enterprise Linux | CentOS | TinyCore
265	Run Nmap Scan (IPv6)

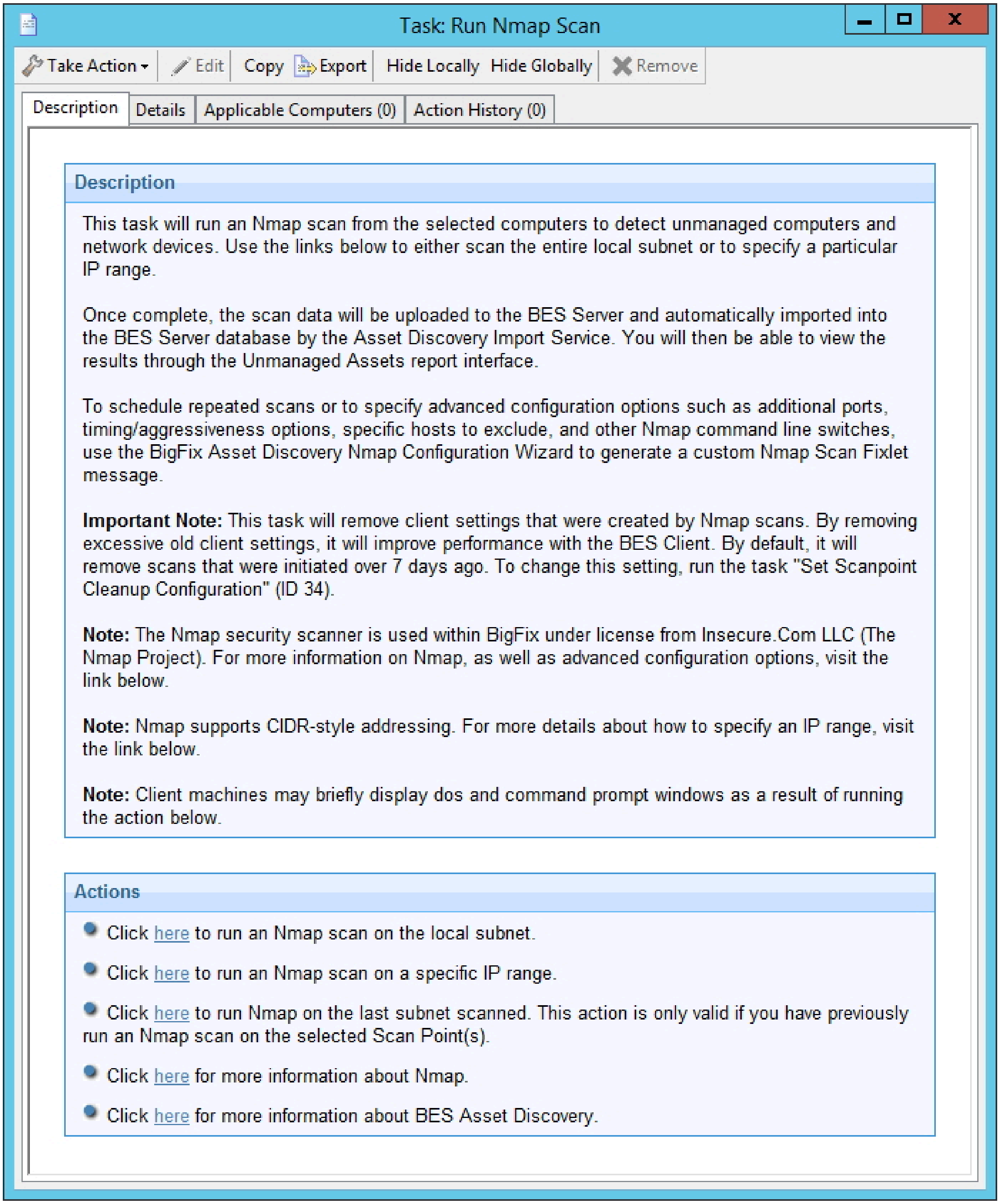
Description

This task will run an Nmap scan from the selected computers to detect unmanaged computers an
devices. Use the links below to either scan the entire local subnet or to specify a particular IP rang

Once complete, the scan data will be uploaded to the BES Server and automatically imported into
Server database by the Asset Discovery Import Service. You will then be able to view the results tl
Unmanaged Assets report interface.

To schedule repeated scans or to specify advanced configuration options such as additional ports,
timing/aggressiveness options, specific hosts to exclude, and other Nmap command line switches
BigFix Asset Discovery Nmap Configuration Wizard to generate a custom Nmap Scan Fixlet mes

When the task opens in the work area, select one of the available links in the Actions box to initiate the Nmap scan. You can specify a local subnet:



Description

This task will run an Nmap scan from the selected computers to detect unmanaged computers and network devices. Use the links below to either scan the entire local subnet or to specify a particular IP range.

Once complete, the scan data will be uploaded to the BES Server and automatically imported into the BES Server database by the Asset Discovery Import Service. You will then be able to view the results through the Unmanaged Assets report interface.

To schedule repeated scans or to specify advanced configuration options such as additional ports, timing/aggressiveness options, specific hosts to exclude, and other Nmap command line switches, use the BigFix Asset Discovery Nmap Configuration Wizard to generate a custom Nmap Scan Fixlet message.

Important Note: This task will remove client settings that were created by Nmap scans. By removing excessive old client settings, it will improve performance with the BES Client. By default, it will remove scans that were initiated over 7 days ago. To change this setting, run the task "Set Scanpoint Cleanup Configuration" (ID 34).

Note: The Nmap security scanner is used within BigFix under license from Insecure.Com LLC (The Nmap Project). For more information on Nmap, as well as advanced configuration options, visit the link below.

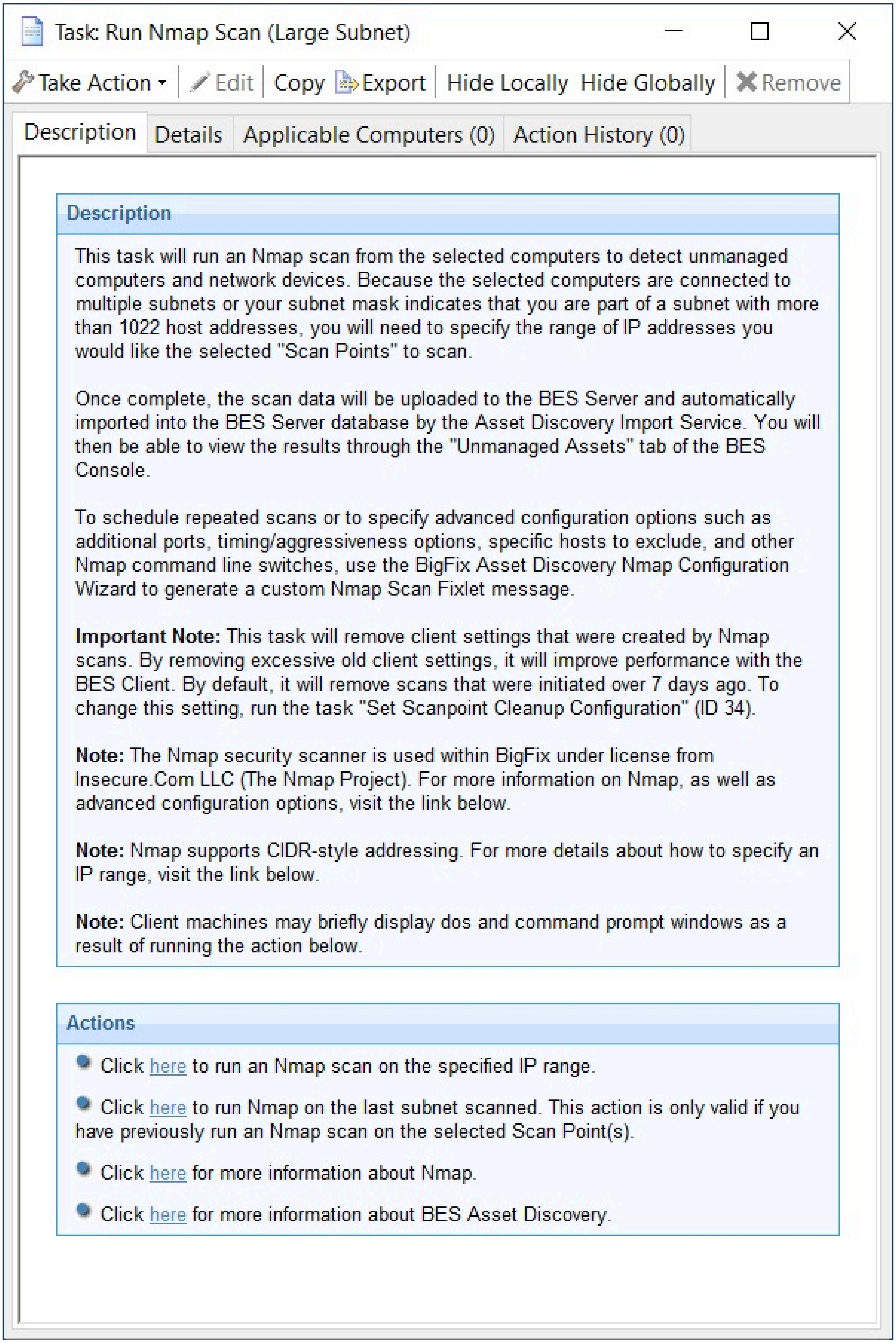
Note: Nmap supports CIDR-style addressing. For more details about how to specify an IP range, visit the link below.

Note: Client machines may briefly display dos and command prompt windows as a result of running the action below.

Actions

- Click here to run an Nmap scan on the local subnet.
- Click here to run an Nmap scan on a specific IP range.
- Click here to run Nmap on the last subnet scanned. This action is only valid if you have previously run an Nmap scan on the selected Scan Point(s).
- Click here for more information about Nmap.
- Click here for more information about BES Asset Discovery.

Or a large subnet:



Description

This task will run an Nmap scan from the selected computers to detect unmanaged computers and network devices. Because the selected computers are connected to multiple subnets or your subnet mask indicates that you are part of a subnet with more than 1022 host addresses, you will need to specify the range of IP addresses you would like the selected "Scan Points" to scan.

Once complete, the scan data will be uploaded to the BES Server and automatically imported into the BES Server database by the Asset Discovery Import Service. You will then be able to view the results through the "Unmanaged Assets" tab of the BES Console.

To schedule repeated scans or to specify advanced configuration options such as additional ports, timing/aggressiveness options, specific hosts to exclude, and other Nmap command line switches, use the BigFix Asset Discovery Nmap Configuration Wizard to generate a custom Nmap Scan Fixlet message.

Important Note: This task will remove client settings that were created by Nmap scans. By removing excessive old client settings, it will improve performance with the BES Client. By default, it will remove scans that were initiated over 7 days ago. To change this setting, run the task "Set Scanpoint Cleanup Configuration" (ID 34).

Note: The Nmap security scanner is used within BigFix under license from Insecure.Com LLC (The Nmap Project). For more information on Nmap, as well as advanced configuration options, visit the link below.

Note: Nmap supports CIDR-style addressing. For more details about how to specify an IP range, visit the link below.

Note: Client machines may briefly display dos and command prompt windows as a result of running the action below.

Actions

- Click here to run an Nmap scan on the specified IP range.
- Click here to run Nmap on the last subnet scanned. This action is only valid if you have previously run an Nmap scan on the selected Scan Point(s).
- Click here for more information about Nmap.
- Click here for more information about BES Asset Discovery.

To execute Nmap scan on IPv6, the tasks like “Run Nmap Scan (IPv6)” will be relevant only on Scan Points where IPv6 protocol is enabled.

Nmap scan does not yet support octet ranges for IPv6 so the target of your Nmap scan can be an IP subset, that is a list of fully qualified IPv6 addresses, in shortened or expanded notation, hostnames and subnets in CIDR-style, all separated by space.

Also, for IPv6, the Nmap Scan on the local subnet is available for subnets of no more than 1022 host addresses.

For IPv4, a scan on a class C network (255 IP addresses) usually takes anywhere from 10-30 minutes, depending on your network. You can also create your own custom Tasks to schedule and configure Nmap scans using the Asset Discovery Nmap Configuration Wizard.

When a Scan Point completes its local scan, the results are uploaded to the BigFix server and imported into the database by the Importer service. The scan results are then visible on the Unmanaged Asset tab in the BigFix console.

This completes the installation of the Asset Discovery service.

Chapter 3. Using Asset Discovery

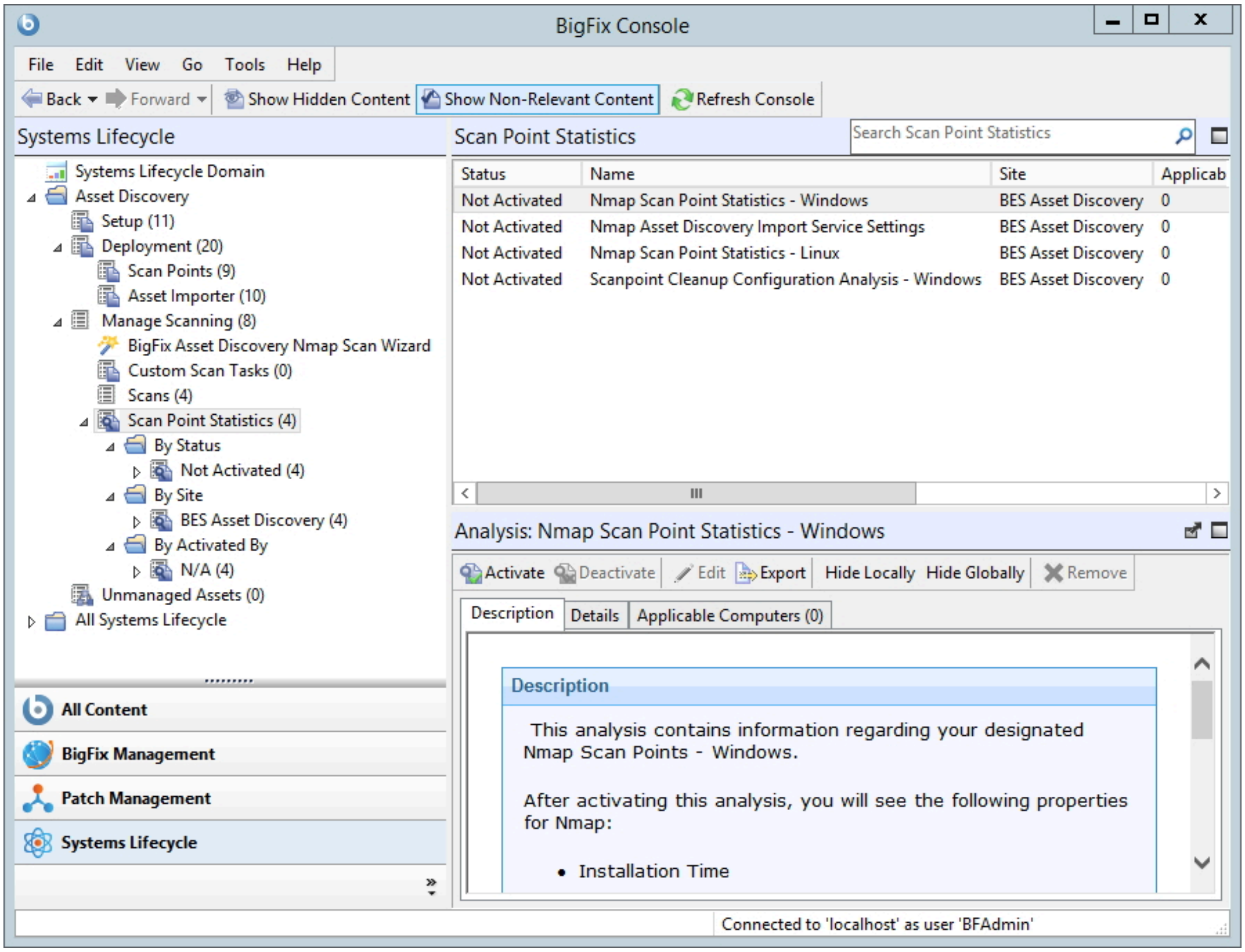
How to operate and things to know about Asset Discovery.

Operation

Actions that you can perform on unmanaged assets retrieved by your Scan Point computers.

Once installed, you can view all unmanaged asset information that was retrieved by your Scan Point computers.

At any point, you can activate the Scan Point Statistics to view information about designated Nmap Scan Points. Click Scan Point Statistics under the Manage Scanning node of the navigation tree. You can view statistics By Status, By Site or By Activation.



Status	Name	Site	Applicab
Not Activated	Nmap Scan Point Statistics - Windows	BES Asset Discovery	0
Not Activated	Nmap Asset Discovery Import Service Settings	BES Asset Discovery	0
Not Activated	Nmap Scan Point Statistics - Linux	BES Asset Discovery	0
Not Activated	Scanpoint Cleanup Configuration Analysis - Windows	BES Asset Discovery	0

Description

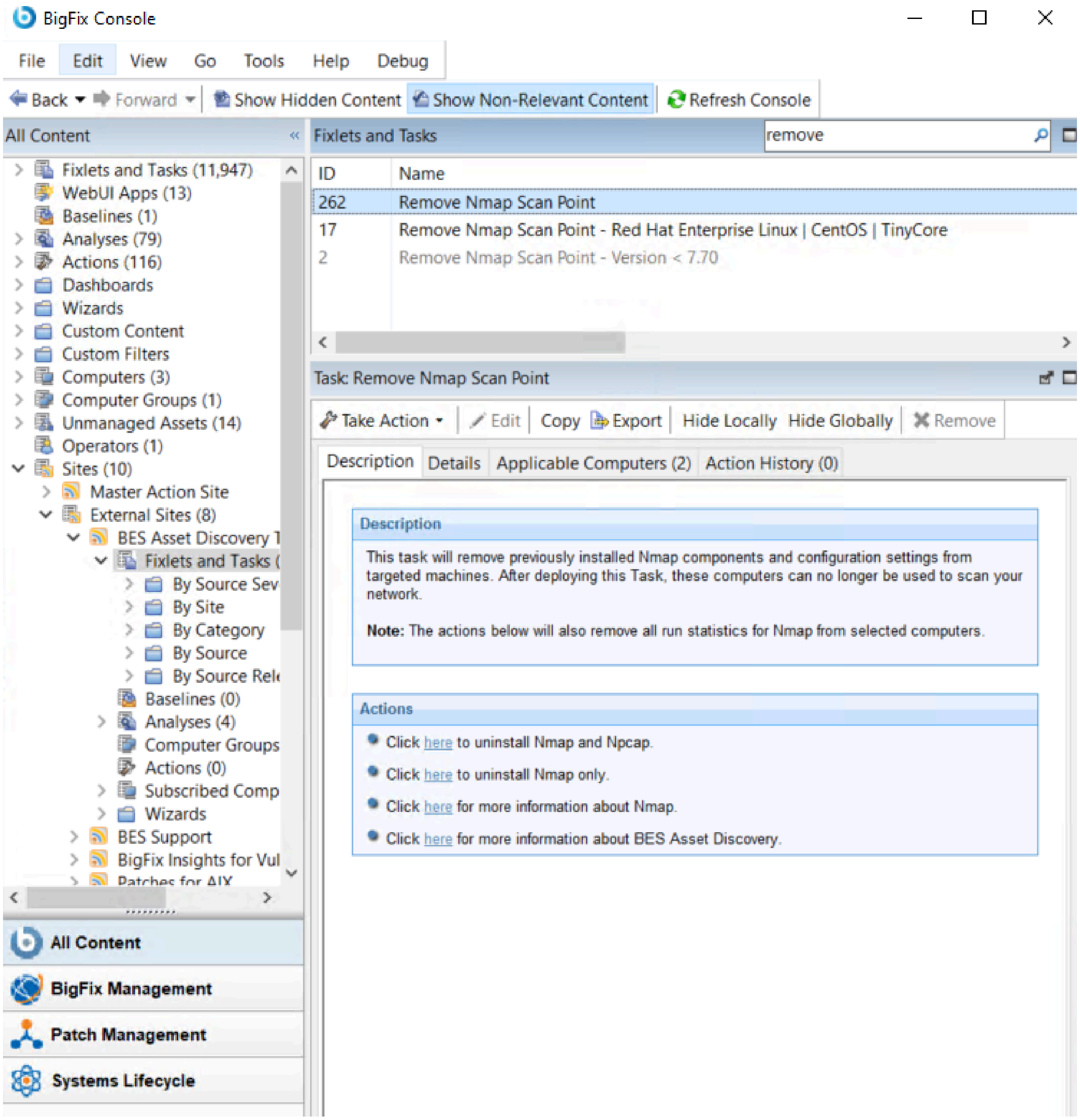
This analysis contains information regarding your designated Nmap Scan Points - Windows.

After activating this analysis, you will see the following properties for Nmap:

- Installation Time

Connected to 'localhost' as user 'BFAdmin'

To decommission a Scan Point computer, use the Remove Nmap Scan Point task in the Deployment node. To access the Remove Nmap Scan Point tasks, click Scan Points under the Deployment node.



ID	Name
262	Remove Nmap Scan Point
17	Remove Nmap Scan Point - Red Hat Enterprise Linux | CentOS | TinyCore
2	Remove Nmap Scan Point - Version < 7.70

Description

This task will remove previously installed Nmap components and configuration settings from targeted machines. After deploying this Task, these computers can no longer be used to scan your network.

Note: The actions below will also remove all run statistics for Nmap from selected computers.

Actions

- Click here to uninstall Nmap and Npcap.
- Click here to uninstall Nmap only.
- Click here for more information about Nmap.
- Click here for more information about BES Asset Discovery.

This removes Nmap from the specified Scan Point and can also remove WinPcap or Npcap for the latest Nmap version. Click the Actions box to access the Take Action dialog and select the Scan Point computers that you want to decommission. To delete an unmanaged asset, click Unmanaged Assets at the bottom of the navigation tree.

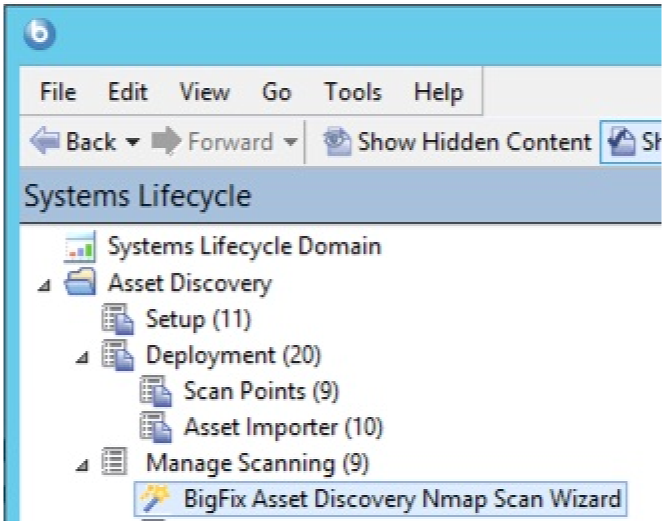
Using the Nmap Scan Wizard

How to customize the Nmap scanner to best suit your needs.

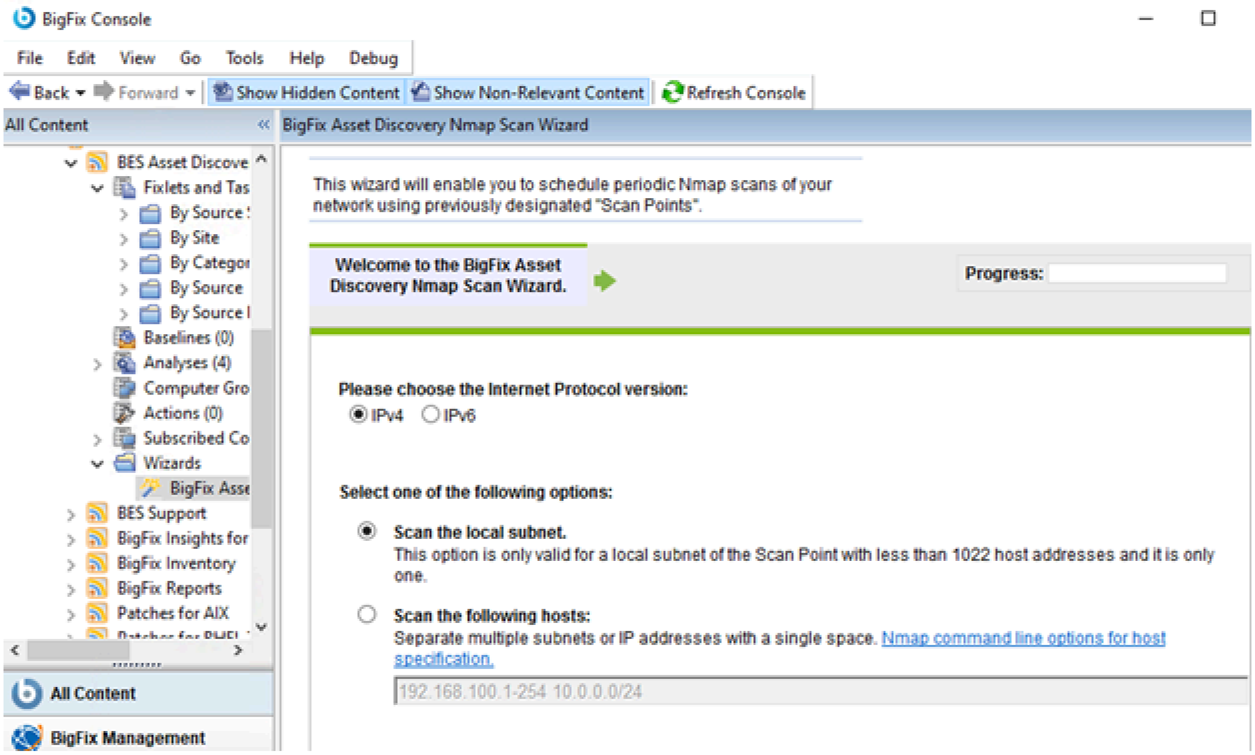
You can change various aspects of the Nmap scanner by using the Asset Discovery Nmap Scan Wizard. You can schedule periodic Nmap scans of your network using previously designated Scan Points.

Note: The Nmap scanner requires that the `UnmanagedAssetImporter -NMAP` service is running on the server.

Click Scan Wizard under the Manage Scanning node in the navigation tree.



The wizard is displayed on the right.



This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard.

Progress:

Please choose the Internet Protocol version:

● IPv4 ○ IPv6

Select one of the following options:

● **Scan the local subnet.**
This option is only valid for a local subnet of the Scan Point with less than 1022 host addresses and it is only one.

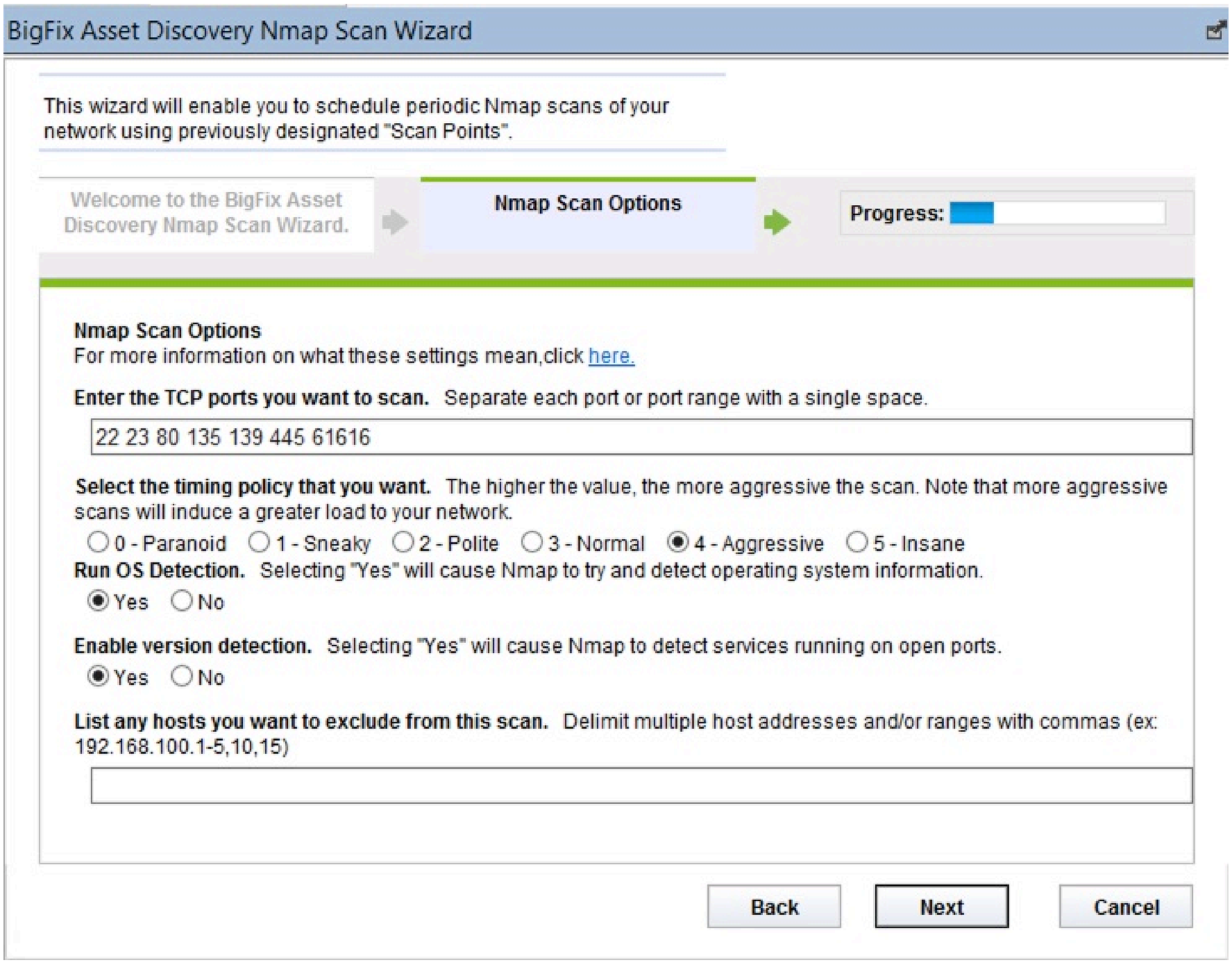
○ **Scan the following hosts:**
Separate multiple subnets or IP addresses with a single space. Nmap command line options for host specification.

192.168.100.1-254 10.0.0.0/24

Begin by selecting the type of protocol and a type of scan.

You can scan the local subnet or scan a particular host. Click Next.

If you select Scan the local subnet, you set specific parameters of the scan in the next screen. Check the Progress bar at the top of the window.



BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Nmap Scan Options
For more information on what these settings mean,click here.

Enter the TCP ports you want to scan. Separate each port or port range with a single space.

22 23 80 135 139 445 61616

Select the timing policy that you want. The higher the value, the more aggressive the scan. Note that more aggressive scans will induce a greater load to your network.

○ 0 - Paranoid ○ 1 - Sneaky ○ 2 - Polite ○ 3 - Normal ● 4 - Aggressive ○ 5 - Insane

Run OS Detection. Selecting "Yes" will cause Nmap to try and detect operating system information.

● Yes ○ No

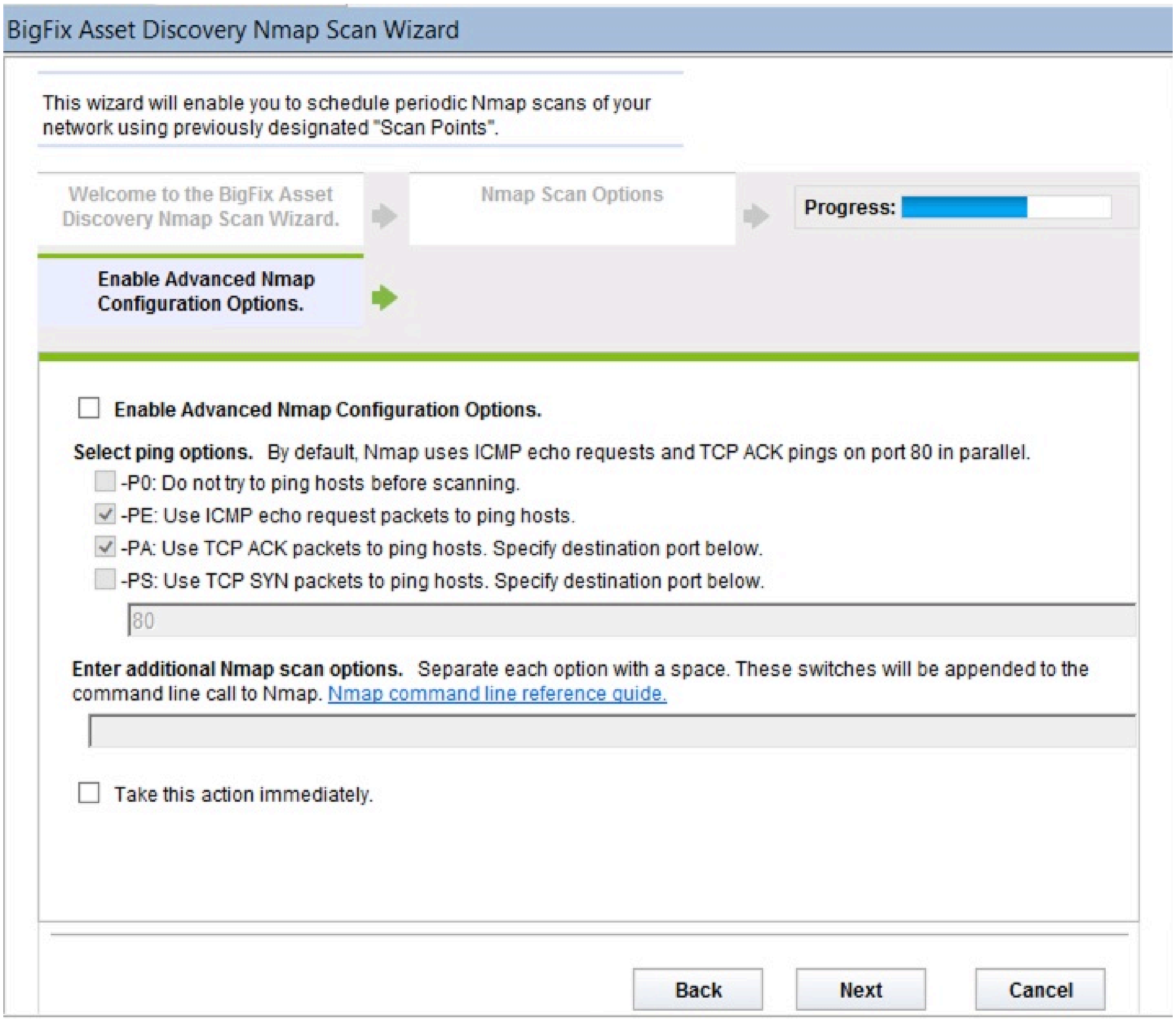
Enable version detection. Selecting "Yes" will cause Nmap to detect services running on open ports.

● Yes ○ No

List any hosts you want to exclude from this scan. Delimit multiple host addresses and/or ranges with commas (ex: 192.168.100.1-5,10,15)

On this screen, you scan ports, run operating system detection, enable version detection, and list hosts to exclude. Make your selections and click Next.

On the next screen, you can enable Advanced Nmap configuration options, select Ping Options, and additional Nmap scan options. Make your selections and click Next.



BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard.
Nmap Scan Options
Progress:
Enable Advanced Nmap Configuration Options.

☐ Enable Advanced Nmap Configuration Options.

Select ping options. By default, Nmap uses ICMP echo requests and TCP ACK pings on port 80 in parallel.

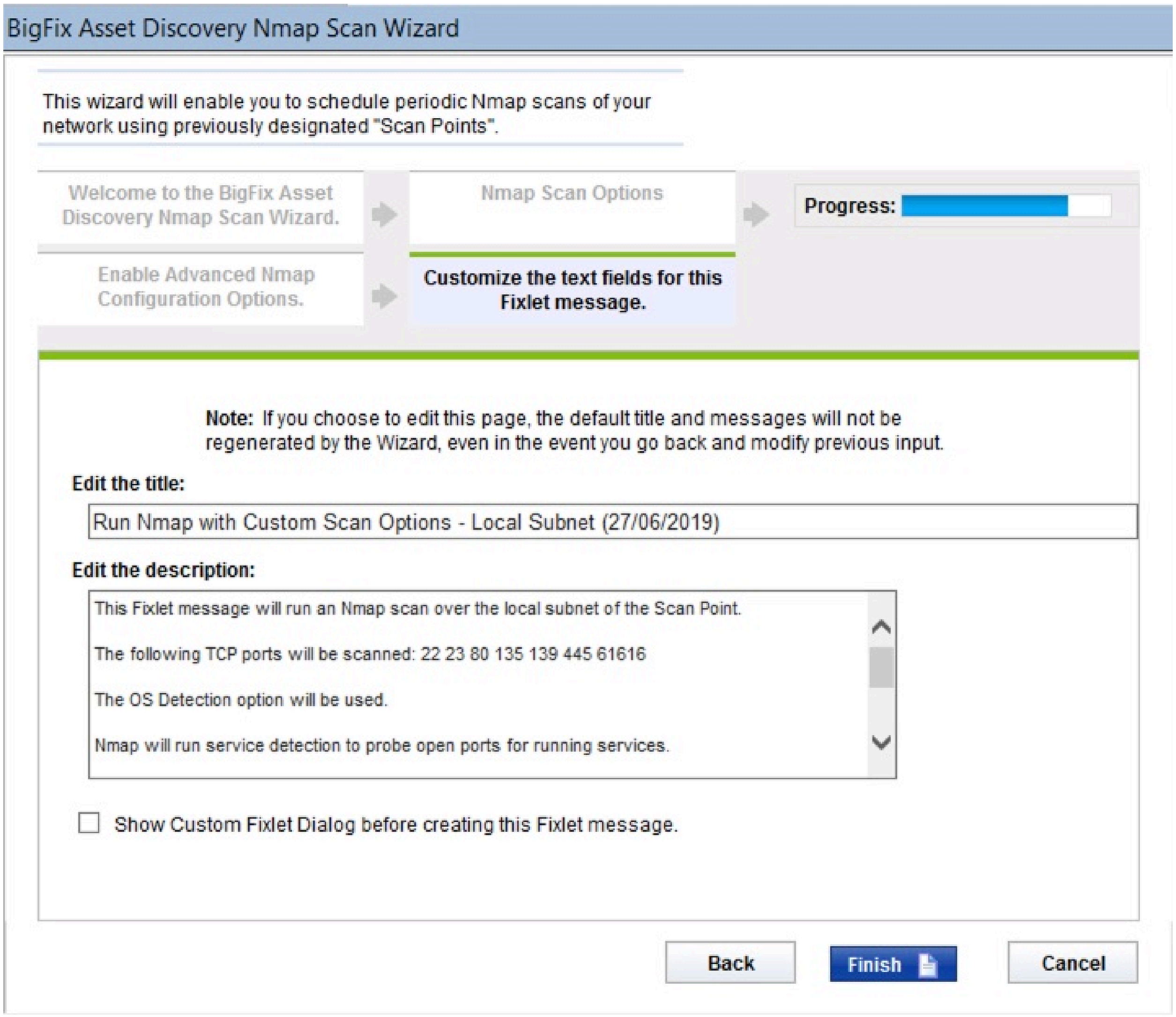
☐ -P0: Do not try to ping hosts before scanning.
☑ -PE: Use ICMP echo request packets to ping hosts.
☑ -PA: Use TCP ACK packets to ping hosts. Specify destination port below.
☐ -PS: Use TCP SYN packets to ping hosts. Specify destination port below.

80

Enter additional Nmap scan options. Separate each option with a space. These switches will be appended to the command line call to Nmap. Nmap command line reference guide.

☐ Take this action immediately.

In the next screen, you can customize the text fields for the Fixlet. You can edit the title and the description of the Fixlet. When you have customized all text fields, click Finish and enter your Private Key Password.



BigFix Asset Discovery Nmap Scan Wizard

This wizard will enable you to schedule periodic Nmap scans of your network using previously designated "Scan Points".

Welcome to the BigFix Asset Discovery Nmap Scan Wizard.
Nmap Scan Options
Progress:
Enable Advanced Nmap Configuration Options.
Customize the text fields for this Fixlet message.

Note: If you choose to edit this page, the default title and messages will not be regenerated by the Wizard, even in the event you go back and modify previous input.

Edit the title:

Run Nmap with Custom Scan Options - Local Subnet (27/06/2019)

Edit the description:

This Fixlet message will run an Nmap scan over the local subnet of the Scan Point.

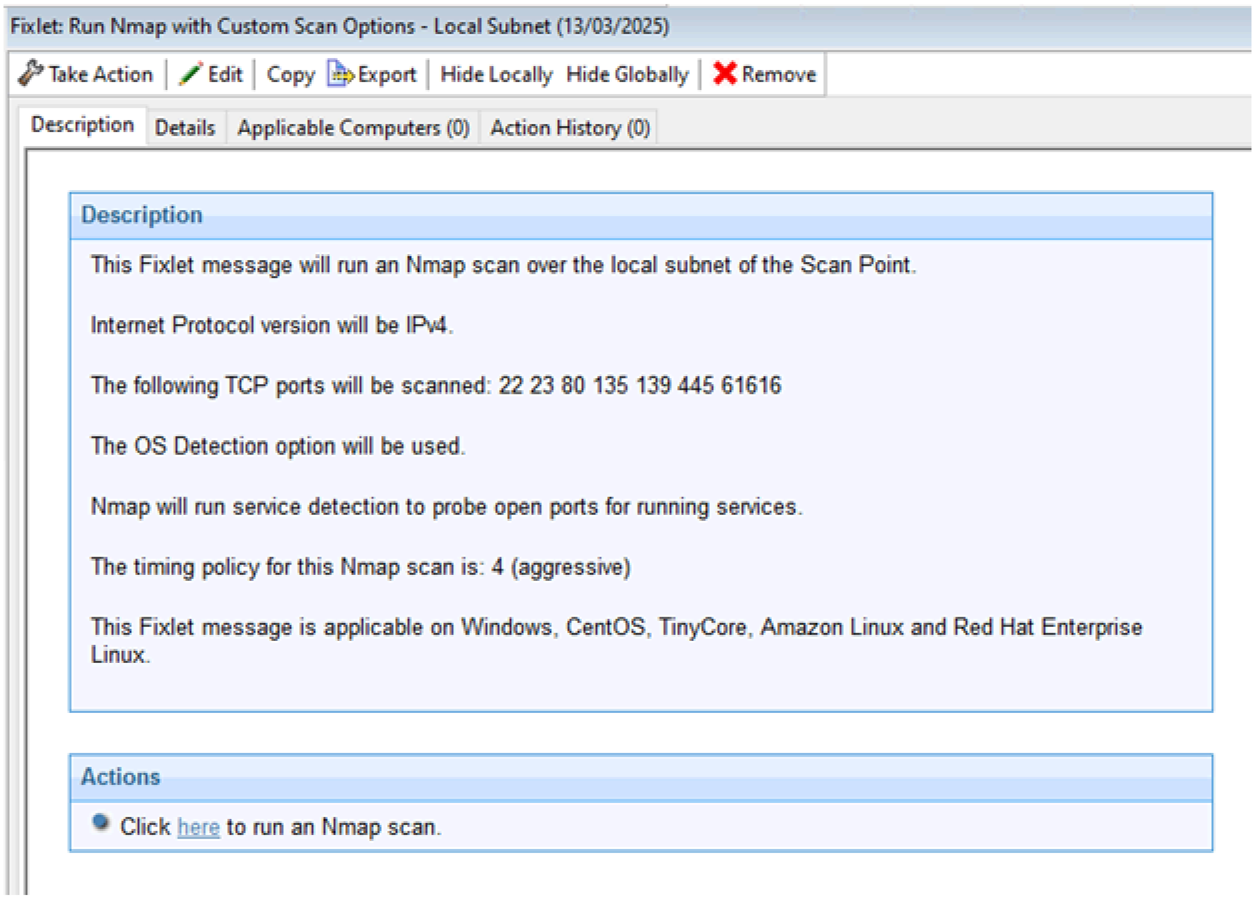
The following TCP ports will be scanned: 22 23 80 135 139 445 61616

The OS Detection option will be used.

Nmap will run service detection to probe open ports for running services.

□ Show Custom Fixlet Dialog before creating this Fixlet message.

You now see the Fixlet that includes the specific parameters and customizations you entered in the wizard. Review the text in the Description field, and click in the Actions box to run an Nmap scan.



Description

This Fixlet message will run an Nmap scan over the local subnet of the Scan Point.

Internet Protocol version will be IPv4.

The following TCP ports will be scanned: 22 23 80 135 139 445 61616

The OS Detection option will be used.

Nmap will run service detection to probe open ports for running services.

The timing policy for this Nmap scan is: 4 (aggressive)

This Fixlet message is applicable on Windows, CentOS, TinyCore, Amazon Linux and Red Hat Enterprise Linux.

Actions

- Click here to run an Nmap scan.

Considerations

Things to know about licensing and potential scanning issues.

Licensing

- When you designate Scan Points, you are installing Nmap and Npcap. The Nmap security scanner and Npcap packet capture library are used within BigFix under license from Insecure.Com LLC (The Nmap Project).

Potential scanning issues

- Network scans might trigger Intrusion Detection Systems. To minimize this possibility, set the Nmap scanning mode to 0 ('Paranoid'), or modify your IDS to allow Nmap scans. This might cause scans to take longer.
- Network scans might cause certain legacy network devices, such as old network printer devices, to fail if scanned.
- Network scans might cause personal firewalls to advise you that a computer is scanning the local computer. Modify your firewall to allow Nmap scans.
- Nmap is sometimes flagged by virus scanners as a potentially harmful tool. Ensure that your virus scanner is not set to block Nmap from running.
- If you set Nmap to scan a very large network, it might take several hours and consume significant bandwidth during the scan. The default scan is the local Class C network, which is usually a fast LAN. It is not recommended that you scan large networks across the WAN with this tool.
- Using Nmap to scan is typically a very safe operation, but there may be issues specific to your organization that must be addressed. Obtain the appropriate authorization from your network team before proceeding.
- The scan point name cannot include any non-ASCII characters. Any non-ASCII character might result in unmanaged assets not being found when a non master operator runs "By Scan Point", or it fails to upload the scanning report to the BigFix server.

Chapter 4. Unmanaged Asset Importer - NMAP

The following options will work as command line arguments to run the importer on its own. For example "UAImporter-NMAP -debugout output.txt -file testfile.xml".

Note: The argument specified in the command line is considered only if the same argument is not already defined as a client setting. Otherwise, the client setting is used.

Windows BigFix server

These options are under `HKLM\Software\BigFix\Enterprise Server \AssetDiscover\NMAP`.

- "DSN"[REG_SZ]

  DSN to use for remote databases. Default is bes_bfenterprise.
- "username"[REG_SZ]

  SQL user name. Default is nt authentication.
- "password"[REG_SZ]

  SQL password. Default is nt authentication.
- "file"[REG_SZ]

  Just import this file into the database. The file must be in the format "nmap-NameOfYourChoice-1570442924" where, "nmap" is the prefix and "1570442924" is a timestamp. In the middle, the name you choose.
- "filedirectory"[REG_SZ]

  Just import all the files in this directory into the database.
- "port"[REG_SZ]

  BigFix port number to use when filtering out assets running the BigFix Client.
- "filteroutclients"[REG_SZ]

  Set to 1 to filter out BigFix Clients, 0 to include BigFix Clients. Default is 1.

- "serviceinterval"[REG_SZ]

  How many seconds the service should sleep between attempting to import a batch of assets. Default is 300.
- "osfamilyclientexemptions"[REG_SZ]

  String of os families; if nmap reports that an asset has one of these families, it will be assumed to not have a client. This is useful if the importer assumes the client is installed because it appears the device is listening on port 52311, but we know for certain the client is not running because it is a printer or some other device type that we do not have a client for. Default is "embedded;IOS;DYNIX".
- "usegmt"[REG_SZ]

  Set to 0 for "Scan Time" and "Import Time" to be in terms of server time, 1 for GMT. Default is 0.
- "debugout"[REG_SZ]

  If this key points to a file, then the UnmanagedAssetImporter-NMAP will print debug output to that file. The default path to the debug output file is "".
- "filteroutdownhosts"[REG_SZ]

  If set to 1, we will not import assets whose state is "down". Default is 1.
- "ignoredeletedassets"[REG_SZ]

  If 1, then deleted assets are ignored and do not return on subsequent scans. If 0, deleted assets are restored on re-scan. Default is 1.

Linux BigFix server

These options are in the besclient.config file. For the option definitions, see the section above.

- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_debugout]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_file]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_filedirectory]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_port]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_filteroutclients]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_serviceinterval]

- [Software\BigFix\EnterpriseClient\Settings\Client _AssetDiscovery_osfamilyclientexemptions]
- [Software\BigFix\EnterpriseClient\Settings\Client_AssetDiscovery_usgmt]
- [Software\BigFix\EnterpriseClient\Settings\Client _AssetDiscovery_filteroutdownhosts]
- [Software\BigFix\EnterpriseClient\Settings\Client _AssetDiscovery_ignoredeletedassets]

Appendix A. Frequently asked questions

A list of the most frequently asked questions.

How is an Unmanaged Asset identified?

Two Unmanaged Assets, where MAC addresses are known, match if they have the same MAC, otherwise they do not. Two Unmanaged assets, where one of the MAC addresses is not known but their hostnames are known, match if they have the same hostname, otherwise they do not. If both Unmanaged assets do not have a MAC address nor a hostname, they match if they have the same IP address, otherwise they do not.

If two Unmanaged Assets match by MAC address or hostname and they do not match by IP address, the IP address is the one of the last asset discovered. So, if the last Nmap scan uses IPv6 protocol, the IP address is the last discovered IPv6 address.

I started a scan - where are the results?

When first installed, Asset Discovery might take several minutes to initially scan the system and report on your unmanaged assets. If you still do not see anything in the BigFix console after 20 minutes, press F5 on your keyboard to force a full refresh.

Where is the Unmanaged Assets tab?

The Unmanaged Assets tab is only visible after you install the Nmap Asset Discovery Import Service. It might take a few minutes to display in the interface. When it is displayed, you can open the tab and click the individual assets to learn more about them.

How long does a typical scan take?

Scanning a Class C subnet typically takes 10-30 minutes, but this can vary based on your specific network. On bigger networks, the scans may take several hours to run.

What are the bandwidth requirements?

The Nmap scanner sends small packets that are unlikely to cause any bandwidth concerns, especially because it is designed to scan nearby computers on fast networks. Once the scan is finished, the scan results are uploaded to the BigFix server. Normally this is a relatively small file - generally 10-200 KB - depending on the number of endpoints scanned.

Scanning large networks with a single Scan Point can result in bigger files, but these scans are only run periodically.

How often can I run a scan?

When Asset Discovery is set up correctly, there is very little network impact and it can be run fairly often without issues. Scans can be run as often as several times a day to find unauthorized network devices, or less often to maintain accurate network inventory information.

Can the Nmap scan settings be changed?

Yes. The default Nmap scan settings enable fast and thorough scanning. The settings can be changed as necessary using the Nmap Configuration Wizard and support any possible Nmap configuration.

Which data can the Importer read from the XML ouput of the Nmap utility?

The BigFix Asset Discovery Importer reads from the Nmap results the following data (XML attributes):

```
host: starttime=

host:status: state= reason=

host:hostnames:hostname: name=

host:address: addr= addrtype= vendor=

host:os:osmatch: name= accuracy=

host:os:osmatch:osclass: accuracy= vendor= osfamily= osgen= type=

host:ports:port: protocol= portid=

host:ports:port:state: state=

host:ports:port:service: name= product= version= extrainfo=

runstats:finished: time=
```

Appendix B. Glossary

This glossary provides terms and definitions for the BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

A *(on page 33)* B *(on page 34)* C *(on page 35)* D *(on page 37)* E *(on page 39)* F *(on page 39)* G *(on page 39)* L *(on page 40)* M *(on page 40)* N *(on page 41)* O *(on page 41)* P *(on page 42)* R *(on page 42)* S *(on page 43)* T *(on page 45)* U *(on page 45)* V *(on page 46)* W *(on page 46)*

A

action

1. See Fixlet *(on page 39)*.
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

Action Script

Language used to perform an action on an endpoint.

agent

See BigFix agent *(on page 34)*.

ambiguous software

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

audit patch

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

automatic computer group

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also computer group *(on page 35)*.

B

baseline

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also deployment group *(on page 37)*.

BigFix agent

The BigFix code on an endpoint that enables management and monitoring by BigFix.

BigFix client

See BigFix agent *(on page 34)*.

BigFix console

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

BYOD

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

C

client

A software program or computer that requests services from a server. See also server *(on page 44)*.

client time

The local time on a BigFix client device.

Cloud

A set of compute and storage instances or services that are running in containers or on virtual machines.

Common Vulnerabilities and Exposures Identification Number (CVE ID)

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also National Vulnerability Database *(on page 41)*.

Common Vulnerabilities and Exposures system (CVE)

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

component

An individual action within a deployment that has more than one action. See also deployment group *(on page 37)*.

computer group

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also automatic computer group *(on page 34)* and manual computer group *(on page 40)*.

console

See BigFix console *(on page 34)*.

content

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

content relevance

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also device relevance *(on page 38)*.

Coordinated Universal Time (UTC)

The international standard of time that is kept by atomic clocks around the world.

corrupt patch

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

custom content

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

CVE

See Common Vulnerabilities and Exposures system *(on page 35)*.

CVE ID

See Common Vulnerabilities and Exposures Identification Number *(on page 35)*.

D

data stream

A string of information that serves as a source of package data.

default action

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

definitive package

A string of data that serves as the primary method for identifying the presence of software on a computer.

deploy

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

deployment

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

deployment group

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also baseline *(on page 34)*, component *(on page 35)*, deployment window *(on page 38)*, and multiple action group *(on page 41)*.

deployment state

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

deployment status

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

deployment type

An indication of whether a deployment involved one action or multiple actions.

deployment window

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the 3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also deployment group *(on page 37)*.

device

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

device holder

The person using a BigFix-managed computer.

device property

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

device relevance

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also content relevance *(on page 36)*.

device result

The state of a deployment, including the result, on a particular endpoint.

Disaster Server Architecture (DSA)

An architecture that links multiple servers to provide full redundancy in case of failure.

DSA

See Disaster Server Architecture *(on page 38)*.

dynamically targeted

Pertaining to using a computer group to target a deployment.

E

endpoint

A networked device running the BigFix agent.

F

filter

To reduce a list of items to those that share specific attributes.

Fixlet

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

Full Disk Encryption

To reduce a list of items to those that share specific attributes.

G

group deployment

A type of deployment in which multiple actions were deployed to one or more devices.

H

Hybrid cloud

The utilization of distinct sets of cloud services (typically public and private) with integration and/or orchestration across them.

L

locked

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

M

MAG

See multiple action group *(on page 41)*.

management rights

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

manual computer group

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also computer group *(on page 35)*.

master operator

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

masthead

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

MCM and BigFix Mobile

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

mirror server

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

Multicloud

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

multiple action group (MAG)

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also deployment group *(on page 37)*.

N

National Vulnerability Database (NVD)

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also Common Vulnerabilities and Exposures Identification Number *(on page 35)*.

NVD

See National Vulnerability Database *(on page 41)*.

O

offer

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device holder can decide whether to install a software application, and whether to run the installation at night or during the day.

open-ended deployment

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

operator

A person who uses the BigFix WebUI, or portions of the BigFix console.

P

patch

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

patch category

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

patch severity

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

R

relay

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

Relevance

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether an action can or should be applied. Relevance is paired with Action Script in Fixlets.

S

SCAP

See Security Content Automation Protocol *(on page 43)*.

SCAP check

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP checklist

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

SCAP content

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP enumeration

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

SCAP mapping

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

Security Content Automation Protocol (SCAP)

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

server

A software program or a computer that provides services to other software programs or other computers. See also client *(on page 35)*.

signing password

A password that is used by a console operator to sign an action for deployment.

single deployment

A type of deployment where a single action was deployed to one or more devices.

site

A collection of BigFix content. A site organizes similar content together.

site administrator

The person who is in charge of installing BigFix and authorizing and creating new console operators.

software package

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

SQL Server

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

standard deployment

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

statistically targeted

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

superseded patch

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

system power state

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

T

target

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

targeting

The method used to specify the endpoints in a deployment.

task

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

U

UTC

See Coordinated Universal Time *(on page 36)*.

V

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

VPN

See virtual private network *(on page 46)*.

vulnerability

A security exposure in an operating system, system software, or application software component.

W

Wake-from-Standby

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

Wake on LAN

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

WAN

See wide area network *(on page 46)*.

wide area network (WAN)

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

Appendix C. Support

For more information about this product, see the following resources:

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

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.