BigFix® Asset Discovery Deployment Guide

BigFix, Inc.
Emeryville, CA

Last Modified: 11/ 8/2007
Version 1.2

Contents

Preface

Audience

This document describes the installation and operation of BigFix Asset Discovery. It is intended for BigFix administrators and operators, as well as people evaluating the product.

Organization of this Guide

This guide is composed of seven major sections:

- **Introduction:** This section introduces BigFix Asset Discovery.
- **Background:** This section gives a large-scale overview of the system operation.
- **Installation:** This section covers the installation process.
- **Operation:** This section covers the operation of the Asset Discovery scanner.
- **Wizard:** This section discusses the Wizard that allows you to customize the Nmap scanner.
- **Warnings:** This section presents some issues to watch out for.
- **FAQ:** This provides answers to some frequently asked questions.

Conventions Used in this Guide

This document makes use of the following conventions and nomenclature:

Convention	Use
Bold Sans	A bold sans-serif font is used for chapter headers.
Bold text	Bold text typically refers to a program or program interface.
Italics	Italics are used for BigFix document titles.
`Mono-space`	A mono-spaced font is used to indicate scripts or code snippets.

Versions

The document describes BigFix Asset Discovery Version 1.2.

Introduction

BigFix Asset Discovery enables you to check on network resources other than computers, potentially discovering problematic or rogue devices in an extended network without needing to implement an expensive Network Access Control system. It uses the well-known Nmap scanner to examine the devices on your network and report back to the BigFix server.

A computer running the BigFix Client is always available for monitoring and remediation from the BigFix Console. There are several ways to install the BigFix Client across your network, including a program called **BigFix Client Deploy.** This program connects to your Active Directory domain and checks to see if the attached computers have the BigFix Client service running. If not, it can then install the program. The **BigFix Installation Generator** automatically installs the Client Deployment software, which in turn can be used to install the BigFix Client on any computers in the Active Directory domain.

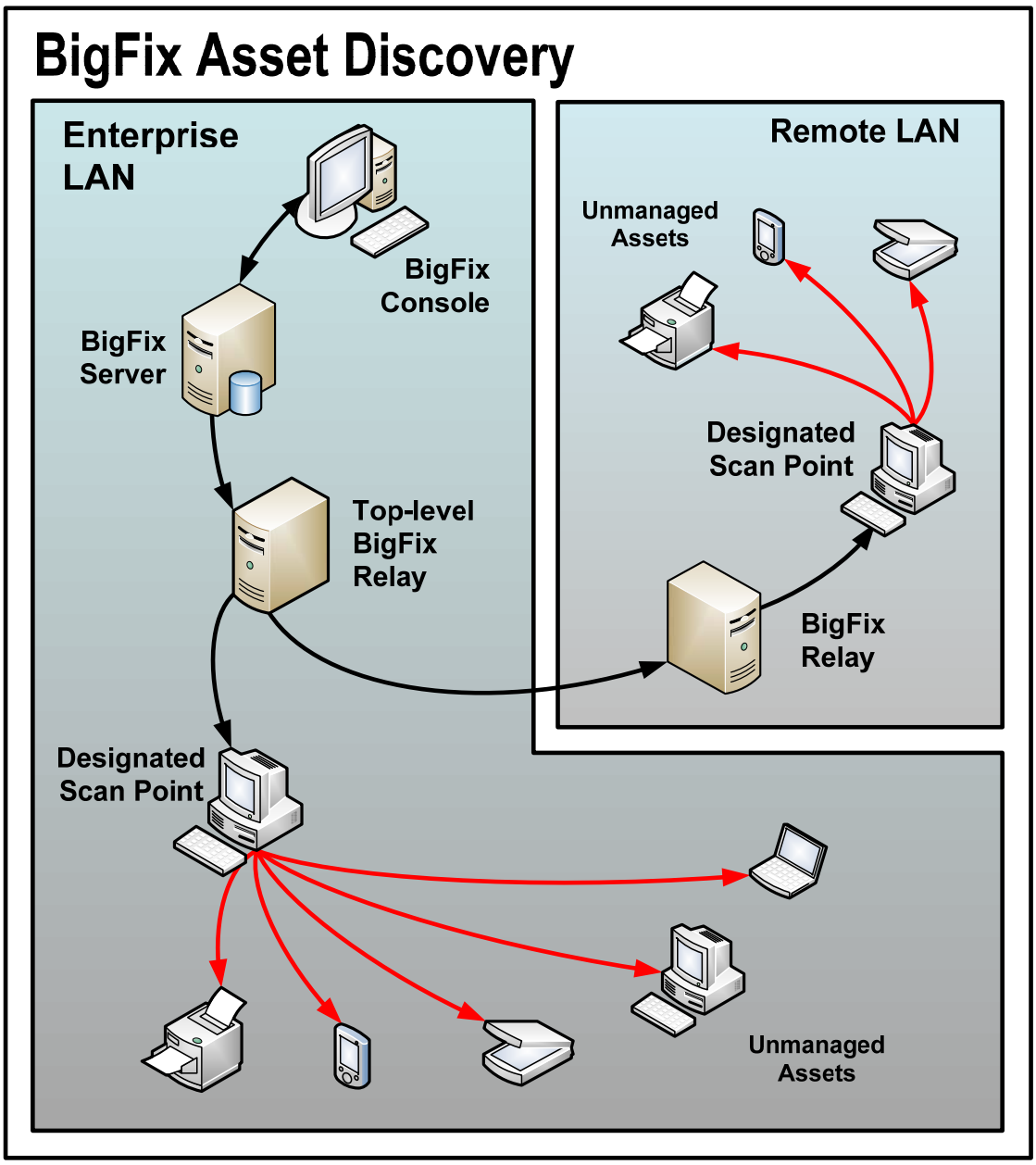
If a computer or other hardware device cannot run the BigFix Client (or if the Client is stopped or disabled), it cannot directly be examined by the BigFix Console. However, it can still be monitored in one of two ways:

- **BigFix Scanner**: This is a standalone tool based on the open-source Nmap Security Scanner. It scans a range of IP addresses, looking for computers and devices that are not running the BigFix Client. The BigFix Scanner is available from the BigFix support site: http://support.bigfix.com/bes/misc/besscanner.html.
- **BigFix Asset Discovery**: This is a Fixlet site that uses Nmap to remotely deploy Scan Points in order to examine remote subnets and then import the data into the BigFix Console. This second technique is the subject of this guide.

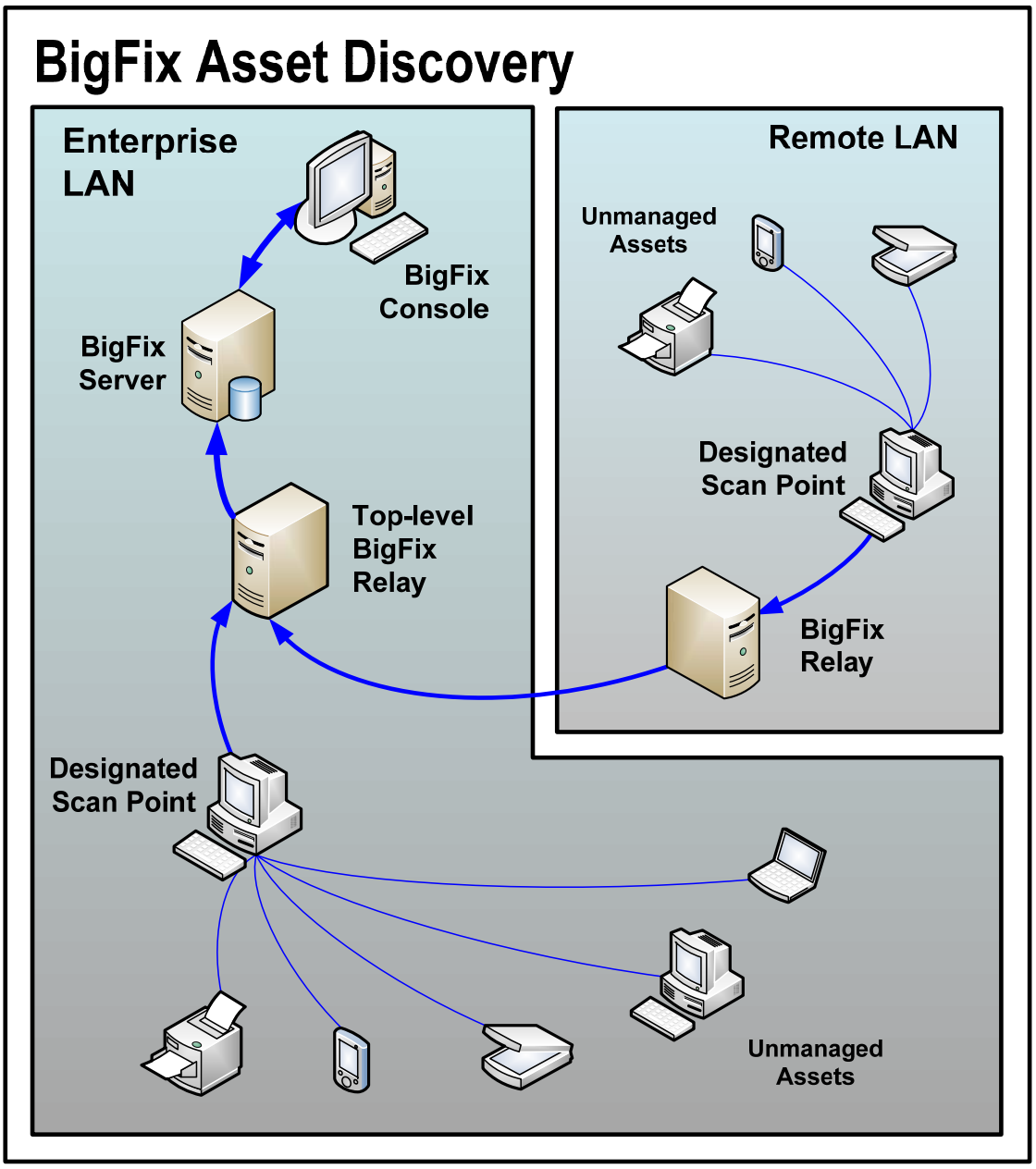
The BigFix Asset Discovery Fixlet site enables you to find unmanaged computers on your network as well as network devices such as routers, printers, and switches which cannot run the BigFix Client. The site uses Fixlet messages and Tasks to deploy Scan Points to specified BigFix Clients in your network. You can then use other Fixlet messages 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.

Background

BigFix Asset Discovery works by designating special computers as Scan Points. These, in turn, query the unmanaged assets in your network:



Information gleaned from these unmanaged assets is retrieved by the Scan Points and then sent back (typically through one or more BigFix Relays) to the database residing on the BigFix Server. From there, you can examine the results on the BigFix Console:



Installation

You install the Asset Discovery service by subscribing to a Fixlet site. This site is available from BigFix and operates on both the Production and Evaluation versions of BigFix. The site contains a set of Tasks that help you to install and run the Nmap scanner. It also includes a Wizard that enables you to configure the Nmap scanner and set a scanning schedule.

Overview

There are four high-level steps you must follow to install and operate the BigFix Asset Discovery service:

1. Download the Nmap software to query your network and the WinPcap software to capture and transmit the resulting data packets.
2. Enable the Nmap Importer Service on your BigFix Server.
3. Designate specific BigFix Clients as Scan Points.
4. Run the Nmap scan.

Note: To view Unmanaged Assets, you must have the proper permissions set through the BigFix Administration program. A user can be granted permission to view all unmanaged assets or only those connected to Scan Points that they administer.

Installation Details

Before setting up the Asset Discovery service, read the Warnings section on page 13. The Asset Discovery service uses Nmap, an open-source utility for network scanning, which may be tagged as problematic by certain firewalls, intrusion detection systems and virus detection programs.

Installing the Site

After reading the warnings and consulting with your network administrators, complete the following steps to begin using the BigFix Asset Discovery Fixlet site:

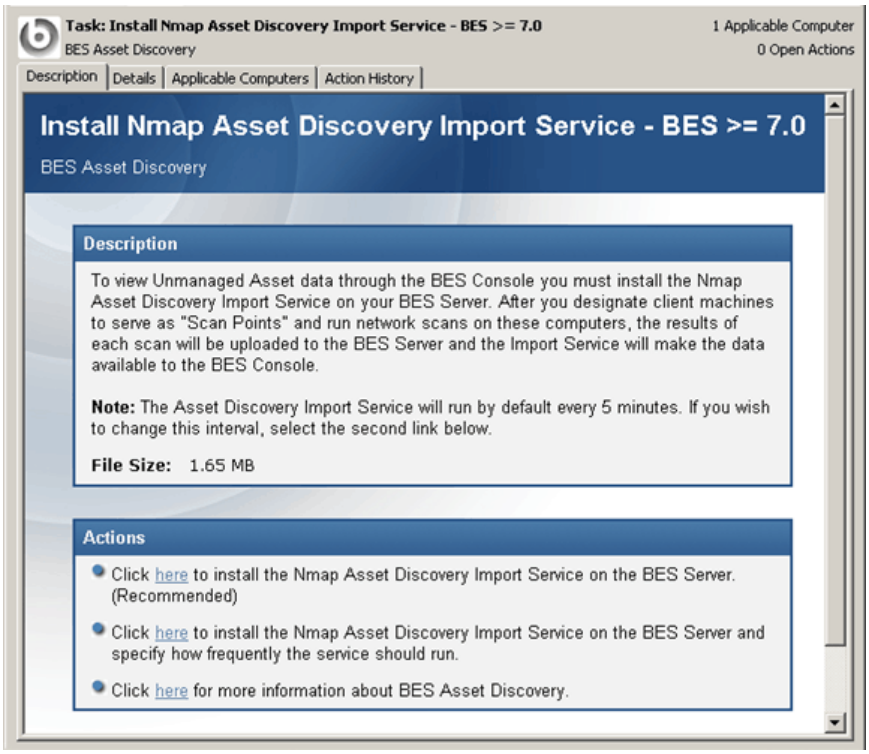
1. Email licensing@bigfix.com to request the masthead for the BigFix Asset Discovery Fixlet site.

   If you are using an evaluation copy of BigFix, the evaluation installer will allow you to install the BigFix Asset Discovery site. If you have the BigFix Advanced Edition, you already have the site, and you can skip this step.

2. From **Tools > Manage Sites**, click the **Add External Site** button.
3. Browse to the masthead you received from BigFix and then click on it to subscribe to the site.

   Alternatively, you can double-click on the masthead to automatically invoke it as a new subscription site within the Console.

4. Select the **Task** tab and double-click the **Install Nmap Asset Discovery Import Service** Task to view it in the workspace window:



5. Click on one of the **Action** links to install the **Nmap Asset Discovery Import Service** on the BigFix Server.

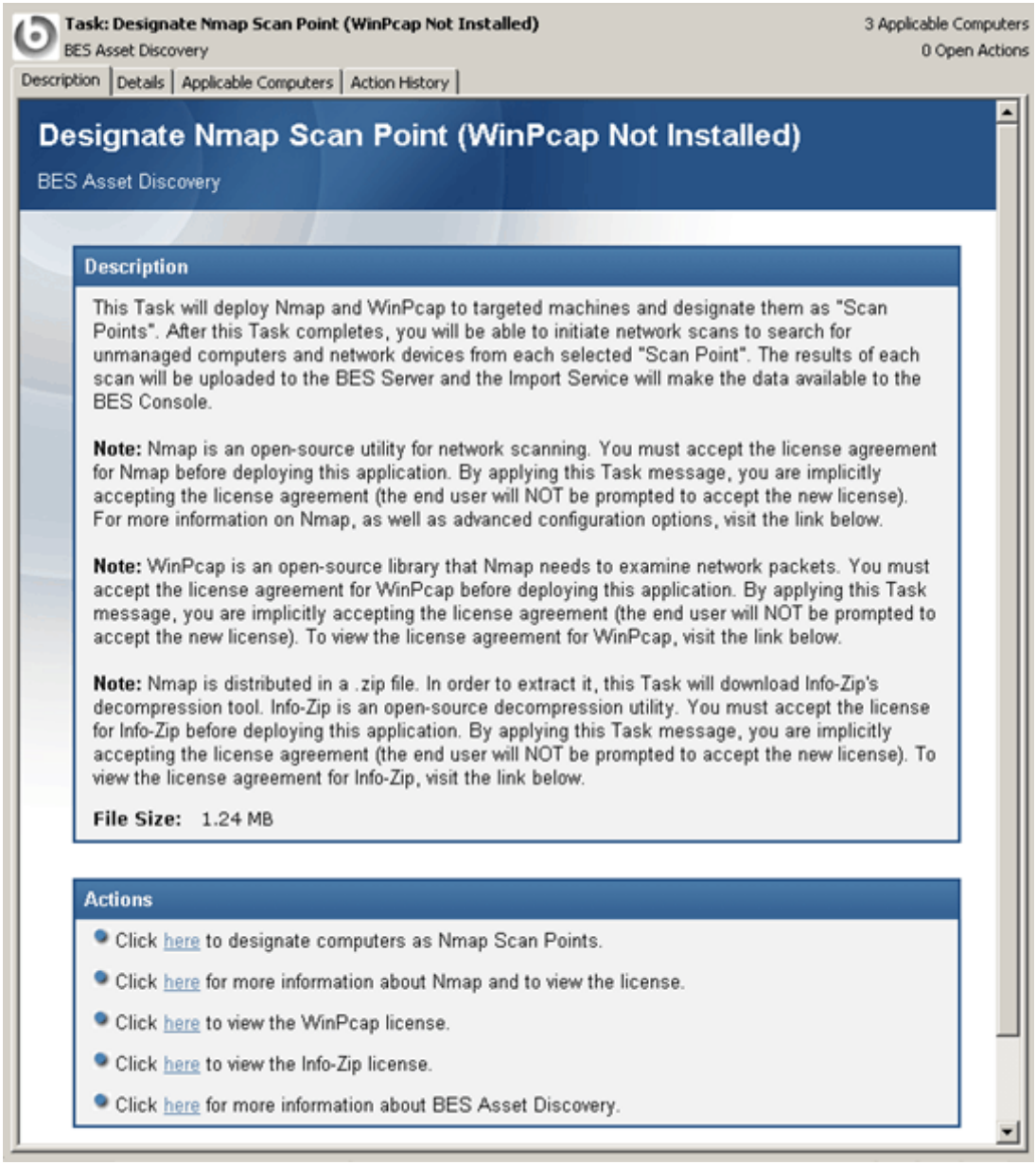
   The Import service will run periodically (by default, every 5 minutes) and check for new Nmap scan data that has been delivered to the BigFix Server. If you want to establish a different frequency, select the second Action link.

   Once you have set up the Nmap service, the **Unmanaged Assets** tab will be added to the Console interface (it may take a few minutes to appear).

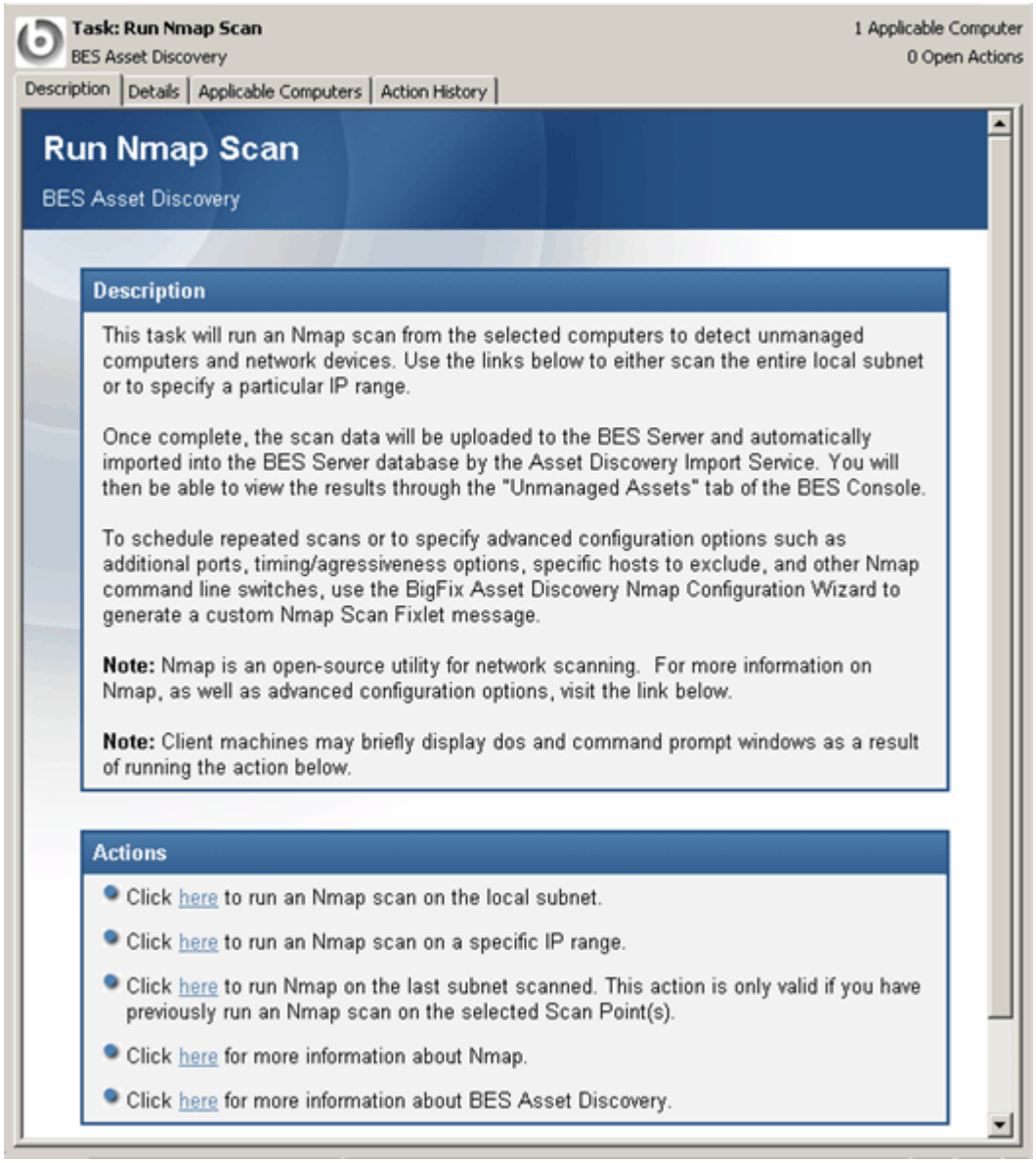
Establishing Scan Points

After the Unmanaged Assets tab appears in the BigFix Console, establish Scan Points throughout your network. The computers you designate as Scan Points must be running Windows. These Scan Points will be the hubs from which the local subnet will be scanned. This task also allows you to view the license agreements for Nmap, WinPcap and Info-zip. In executing this Action, you are implicitly accepting these license agreements.

1. From the Tasks tab, select the Designate Nmap Scan Point.



2. Click the first Action link to bring up the **Take Action** dialog.
3. From the **Target** tab, select the computer(s) you want to designate as Scan Points.
4. From the **Tasks** tab, select the **Run Nmap Scan** task to initiate the scanning process.



5. Select one of the Action links to start the Nmap scan.

   You can choose to scan the local subnet or you may want to specify a range of IP addresses. If you have used Nmap before, you can accept the previously selected subnet. This completes the installation of the Asset Discovery service.

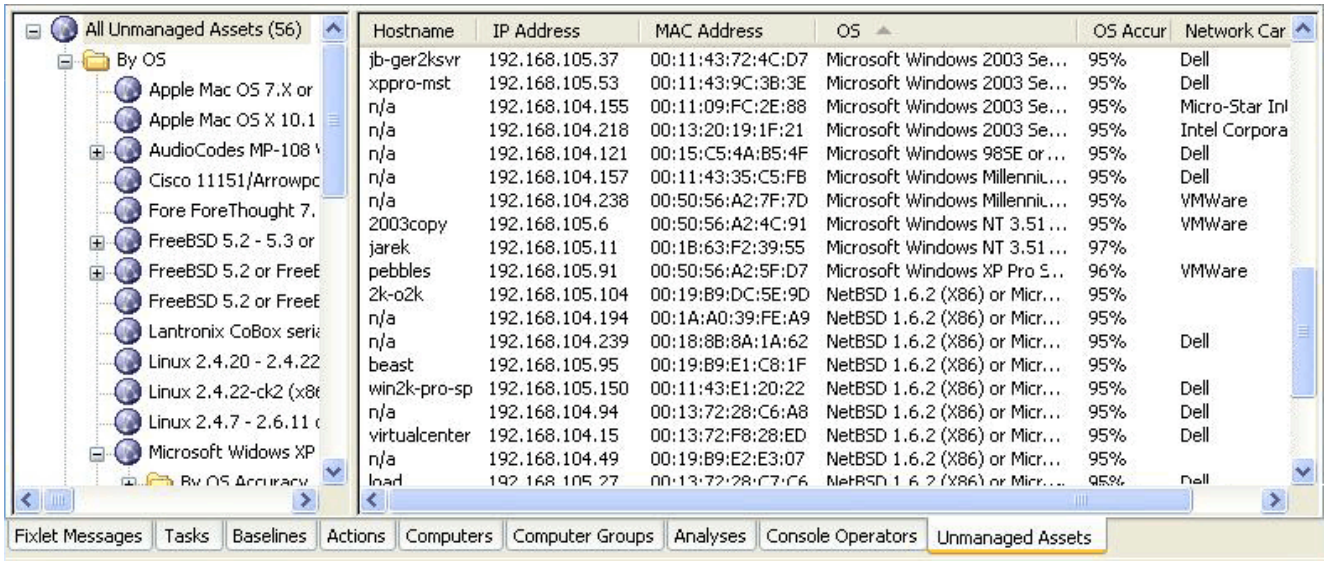
A scan on a class C network usually takes about 20-30 minutes. You can also create your own schedule and configure Nmap scans using the **Asset Discovery Nmap Configuration Wizard** (see page 10).
When a Scan Point has finished its local scan, the results will be uploaded to the BigFix Server and imported into the database by the Importer service. The scan results will then be visible on the **Unmanaged Asset** tab in the BigFix Console.

Operation

Once installed, you can view all the unmanaged asset information that has been retrieved by your various Scan Point computers. There are several properties that you can use to filter the list of assets, including:

- **Last Scan Time:** The scan time as determined by the BigFix server.
- **First Scan Time:** This is the time (as determined by the BigFix server) that the asset was first scanned.
- **Addresses:** These include the IP and MAC addresses of the specified asset.
- **OS:** Nmap uses various techniques, including TCP/IP stack fingerprinting, to try to determine the OS of the unmanaged asset.
- **OS Accuracy:** This is a measure of confidence that the Nmap scan has deduced the correct OS based on the analyzed data.
- **Device Type:** Returns the device type as determined by Nmap.
- **Scan Point:** Returns the Scan Point computer that this device is connected to.

You can use these properties to sort or filter your list of unmanaged assets. Click on the appropriate column header in the Unmanaged Assets list to sort it. Click on items in the filter panel to narrow down the viewable list.



Double-click on any item in the list to bring up in-depth information about the specified asset:

At any point, you can activate the **Nmap Scan Point Statistics** Analysis to view information about designated Nmap Scan Points. Double-click to select it from the Analyses tab, and then click on the **Results** tab to view the Scan Point computers. Click on a column header to sort the list by that field value. You can also view the data in a summary form by using the pull-down menu directly above the computer list.

To decommission a Scan Point computer, use the **Remove Nmap Scan Point** task. This will remove Nmap from the specified Scan Point and optionally remove WinPcap as well. Click on an Action link to bring up the Take Action dialog and select the Scan Point computer(s) you wish to decommission.

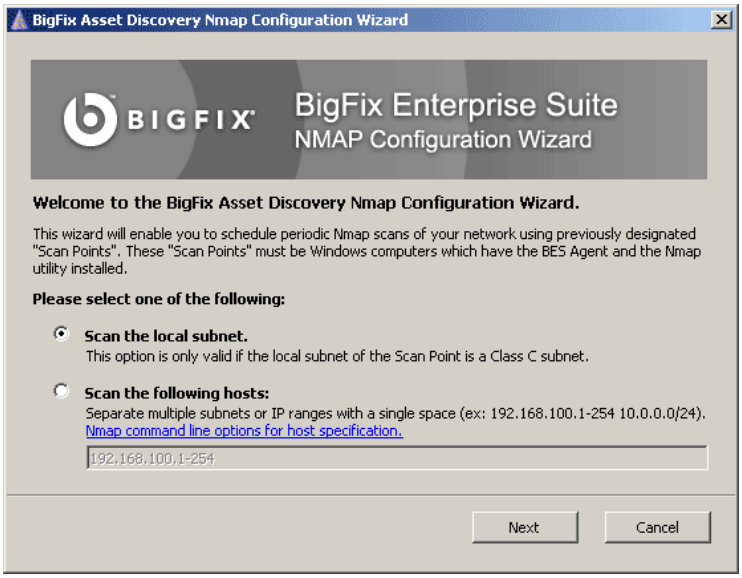
To delete an unmanaged asset, right-click on it from the Unmanaged Assets tab and select **Delete** from the context menu.

To completely remove the Asset Discovery Service from your network, use the **Uninstall Nmap Asset Discovery Import Service** Task. This will stop Nmap scans, but will still retain any data that you have already accumulated. To delete this data as well, first run the **Delete Nmap Discovery Data** task.

Using the Asset Discovery Nmap Configuration Wizard

You can change various aspect of the Nmap scanner by using the Wizard included with the Asset Discovery Fixlet site. It enables you to create an Action for immediate execution, or a Fixlet message that can be used to deploy the Action at a later time. To use the Wizard, follow these steps:

1. Choose Wizards > BigFix Asset Discovery Nmap Configuration Wizard. The Wizard opens.



2. Select whether you want to scan the local subnet of a Scan Point or to Scan specific hosts. Click **Next**.

   The **Nmap Scan Options** page opens.

3. On this page:

a. Enter the TCP ports you want to scan, separating them by spaces.

   You can use ports like this to help determine what kind of computer or device is connected to the Scan Point. The lower numbers include things like SSH and HTML ports which would be expected to be open on a computer and the higher-numbered ports would be expected to be closed.

b. Select the timing using one of five pre-defined Nmap timing policies.

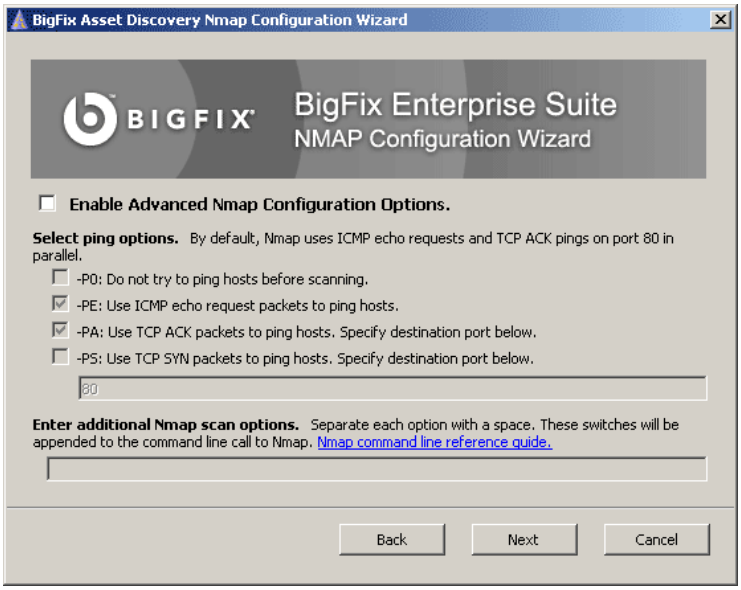
   Paranoid delays 5 minutes to avoid being tagged as an intruder. **Sneaky** waits 15 seconds between sending packets. **Polite** delays for about half a second, but keeps the probes serialized to ease the load on the network. **Normal** is the default Nmap mode, which runs as quickly as possible in parallel. **Aggressive** expedites SYN scans against heavily filtered hosts on a fast network. **Insane** is suitable only for very high-speed networks.

c. Select whether or not you want Nmap to try to detect OS information.

d. Select whether or not you want Nmap to check for services running on open ports.

e. You can also specify IP Addresses and ranges to exclude from Nmap scanning.

Click **Next**.



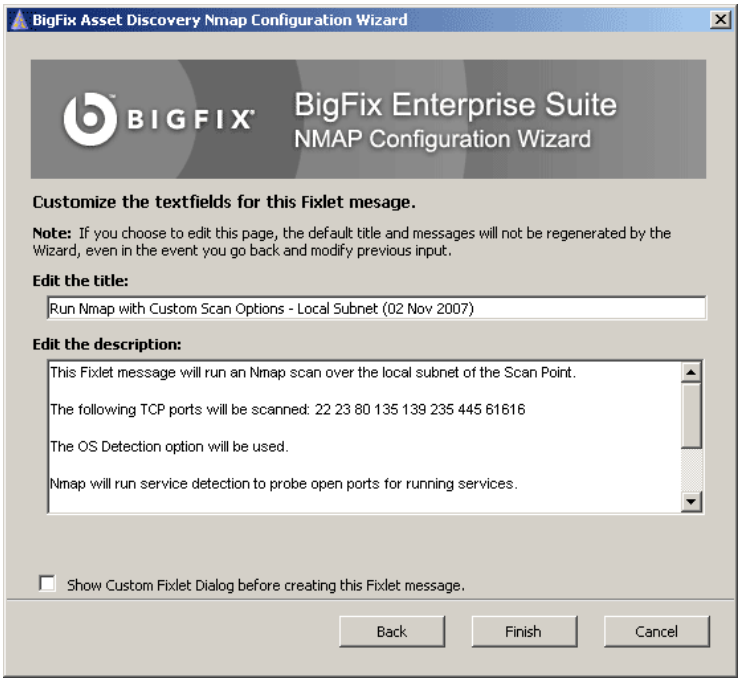
4. Select any of the advanced Nmap configurations you want. Click **Next**.

   For more information about these options, see the Nmap site at http://www.insecure.org/.

   The **Scheduling** page opens.

5. Specify your scheduling options. Click **Next**.

   If you check the box at the bottom to immediately execute the Action, it will execute the Action without creating a Fixlet.



6. Customize the text for your Fixlet.

   It is a good idea to check the box at the bottom to preview the Fixlet before it is deployed. If you want to make any changes, click **Cancel** to edit your message.

   When you are happy with the Fixlet message, click **Finish**.

Warnings

The warnings below are important, please read them before installing the BigFix Asset Discovery Fixlet site.

Licensing

- When you designate Scan Points, you are installing the Nmap scanner application available from http://www.insecure.org/nmap. You must agree to the terms of the Nmap license before designating the Scan Points. As with all the following licenses, your agreement is implied when you activate the task.
- When you designate Scan Points, you will be installing the packet capture library, WinPcap 3.1 (also available at http://winpcap.polito.it/install/default.htm). You must agree to the terms of the WinPcap license before designating the Scan Points.
- Nmap is distributed as a .zip file. In order to extract it, BigFix will temporarily download and use Info-Zip's decompression tool. Info-Zip is an open-source decompression utility. More information on Info-Zip is available at http://www.info-zip.org/. You must agree to the terms of the Info-Zip license before designating the Scan Points.
- BigFix Asset Discovery is included in BigFix Advanced Edition. If you use BigFix Standard Edition, you must license the Asset Discovery Fixlet site separately.

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.
- Network scans may cause certain legacy network devices, such as old network printer devices, to fail if scanned.
- Network scans might cause personal firewalls to advise the user 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 because it is possible to use it for malicious purposes. Ensure your virus scanner is not set to block Nmap from running.
- If you set Nmap to scan a very large network, it may take several hours and consume significant bandwidth during the scan. The default scan is the local Class C network, which usually is a fast LAN. BigFix does not recommend scanning large networks across the WAN with this tool.
- Using Nmap to scan is usually a very safe operation, but there may be issues specific to your organization that you need to address. Please obtain the appropriate authorization from your network team before proceeding.

Frequently Asked Questions

I've started the scan; where are the results?

When first installed, it may 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 or so, press F5 to force a full refresh.

Where is the Unmanaged Assets tab?

The Unmanaged Assets tab will only show up after you have installed the Nmap Asset Discovery Import Service. It might take a few minutes to be added to the interface. When it is added, you can open the tab and click on individual assets to learn more about them.

How long does it take to scan?

The time will vary according to your network. It might take up to 20 minutes on a Class C subnet, but a thorough scan on a Class B network can take several hours to run.

How much memory is required?

A thorough scan of a Class B network can consume over 20 megabytes. Check the upload size limit of your BigFix configuration to make sure you can accommodate a file of this size.

About BigFix, Inc.

Founded in 1997, BigFix is the category leader in security configuration management software, services, and solutions for real-time visibility and control of computers across the distributed enterprise. BigFix solutions are proven in production at more than 500 companies, government agencies and public sector institutions worldwide and currently manage over 5,000,000 desktop and mobile clients, workstations, and servers. The company has received numerous awards and industry recognitions, including the 2005 Codie Award for "Best Security Product" and the SC Magazine "Product of the Year" recognition in 2004 and eWeek's "Analyst's Choice" award in 2006. For more information, visit www.bigfix.com.

BigFix, Inc.
1480 64th Street Suite 200
Emeryville, California 94608
[t] 510 652-6700
[f] 510 652-6742
[e] info@bigfix.com
[e] sales@bigfix.com