



# FNMS Agent Deployment Guide

## Deployment Guide Document

Version 3.1

May 2018

Prepared By

# Table of Contents

<b>1. DOCUMENT PURPOSE</b>	<b>3</b>
<b>2. INTENDED AUDIENCE</b>	<b>4</b>
<b>3. DOCUMENT MAP</b>	<b>5</b>
3.1. Acronyms/Abbreviations .....	5
3.2. Caveats and Nomenclature .....	5
<b>4. FNMS AGENT SPECIFICATIONS</b>	<b>6</b>
4.1. Technology Overview.....	6
4.2. Hardware Specification .....	6
4.3. Agent Benchmarks.....	6
4.4. Inventory Bandwidth.....	7
4.5. Network Specifications.....	7
4.6. Validate Network Connectivity .....	7
4.7. Account Specifications .....	8
<b>5. INSTALLATION OF THE FNMS AGENT</b>	<b>9</b>
5.1. Agent Installation – Windows .....	9
5.1.1. Windows Agent Information .....	9
5.1.2. Manual Installation .....	9
5.1.3. Packaged Installation .....	10
5.1.4. Log Files .....	10
5.2. Agent Installation – UNIX .....	10
5.2.1. Unix Agent Information.....	10
5.3. HTTPS Certificates .....	11
5.4. FNMS Agent Configuration Settings .....	11
5.5. Manual Installation .....	11
5.6. Installation Verification .....	13
5.7. Log Files.....	14
<b>6. UNINSTALLATION OF THE FNMS AGENT</b>	<b>16</b>
6.1. Agent Uninstallation – Windows .....	16
6.1.1. Manual Uninstallation .....	16
6.1.2. Complete Uninstallation .....	16
6.2. Agent Uninstallation – Unix.....	17
6.2.1. Manual Uninstallation .....	17
<b>7. APPENDIX A: SUPPORTED OPERATING SYSTEMS</b>	<b>19</b>
<b>8. APPENDIX B: TROUBLESHOOTING</b>	<b>21</b>
8.1. I would like to see if the computer has working network connectivity to a beacon. ....	21
8.2. I would like to confirm that the agent was installed correctly on Windows. ....	21
8.3. I would like to confirm that the agent was installed correctly on UNIX. ....	22
8.4. I would like to confirm that the agent is functioning correctly on Windows, by looking at the registry.....	24
8.5. I would like to confirm that the agent is functioning correctly on Windows, by checking the Schedule Agent. ....	25
8.6. I would like to confirm that the agent is functioning correctly on UNIX. ....	27
8.7. I would like to run an inventory process manually on Windows. ....	28
8.8. I would like to run an inventory process manually on unix.....	29
8.9. I would like to run an inventory process manually, on UNIX, but not upload the inventory packet.....	30

8.10. I would like to check agent log files.....	30
8.11. I would like confirm that inventory is uploading to a beacon correctly. ....	31

## 1. Document Purpose

This document has been created to outline the server, storage and network specifications for deploying Flexera's FlexNet Manager Platform Inventory Agent within the STC computer network environment.

The FNMS Inventory Agent performs inventory scans on any computer it is installed. Its main purpose is to provide inventory information for devices that are not covered by other inventory software (ADDM, SCCM, ALTIRIS, LANDesk, etc.), or to enhance the software inventory information already collected by those other products.

## 2. Intended Audience

The intended audience for this document is:

- Windows System Engineers
- UNIX System Engineers
- Network Specialists
- IT Security

## 3. Document Map

### 3.1. Acronyms/Abbreviations

Abbreviation	Description
<b>FNMS</b>	FlexNet Manager Suite
<b>FNMP</b>	Flexera Manager Platform
<b>ADDM</b>	Application Dependency Mapping
<b>SCCM</b>	System Center Configuration Manager

### 3.2. Caveats and Nomenclature

The current release of the Flexera application is named FlexNet Manager Suite (FNMS). Previously, the product is named FlexNet Manager Platform (FNMP). Some diagrams or text in this document may refer to FNMS; unless specified otherwise (such as comparing the various versions of the product), these two names can be used interchangeably.

Additionally, the name “ManageSoft” and “ManageSoft for managed devices” and refers to the older company name and agent name respectively.

## 4. FNMS Agent Specifications

### 4.1. Technology Overview

When the agent connects to the Inventory Manager or FNMS Beacon bootstrap server it is configured for. It then downloads various policies which configure the agent.

On the configured schedule, the agent performs an inventory scan of the computer, capturing hardware information, performing specific checks for certain software, and running a filesystem scan to detect software evidence. This information is then saved to an xml file. The agent then run an algorithm to choose the best Inventory Beacon to upload the inventory packet to.

### 4.2. Hardware Specification

The following are the hardware requirements for the agent to be deployed in any (Mac OS, UNIX, Windows, etc.)

Resource	Recommendation	Comments
Memory	2 Gb	Minimum 512 Mb
OS	Any specified in <a href="#">Appendix A</a>	
Disk Space	25MB installation + 100MB workspace	
Network ports	See <a href="#">Network Specifications</a>	

### 4.3. Agent Benchmarks

Agent Activity	Run Duration	CPU usage (CPU seconds)	CPU usage (% of 1 core)	Memory usage	Network traffic
Inventory Collection	13 to 240 seconds	5 to 130	10% to 50%	4 Mb to 20 Mb	10 Kb to 200 Kb per upload
Usage monitoring.	Ongoing	<1 sec per day	Negligible	4 Mb to 8 Mb	5 Kb to 20 Kb per day
Policy Update (Client Settings, Schedule, and Failover settings)	14 to 33 seconds	<1 sec per policy	Negligible	3 Mb to 5 Mb	10 Kb to 100Kb per policy update

## 4.4. Inventory Bandwidth

Frequency	Data Size	Protocols	Network Configuration
Configurable (e.g. Sundays @ 02:00), at implementation and subsequently.	Typically 100kb (compressed) per managed device.	No proprietary protocols – HTTP and HTTPS.	<b>Reporting Locations:</b> Can be co-located on existing servers. <b>Upload Scheduling:</b> Policy-based schedule (inc. Random). <b>Bandwidth Throttling:</b> Dynamic, algorithm-based restrictions.

## 4.5. Network Specifications

For the target computer, at least one (but ideally all) Inventory Beacon must:

- 1) Be renderable to an IP address from an FQDN, either by manually editing the target computers hosts file, or by adding an alias in the DNS, and
- 2) Network connectivity as per the following table must be available.

Usage	Source	Destination	Protocol	Port
Communication from agent to Inventory Manager using http	FNMS Agent	FNMS Beacon/Inventory Server	HTTP	TCP:80
Ping tests for Beacon/Inventory Server prioritisation	FNMS Agent	FNMS Beacon/Inventory Server	ICMP PING	

If firewalls and/or restricted VLANs exist between any of the source and destination locations, exemption and routes will need to be configured in order for the FNMS Inventory Agent service to function correctly.

## 4.6. Validate Network Connectivity

Prior to installation, verify that the clients can communicate with the Inventory Beacons. Perform the following tests from the client(s) in a shell window:

**Table 1 - Validate Network Connectivity Steps**

Step	Action	Description	Notes
1)	Test that the beacon's IP address can be resolved	From the command line, run the command: Nslookup C-172-20-151-96.stc.corp	The Inventory Beacon FQDN needs to be able to be resolved to an IP address



Step	Action	Description	Notes
2)	Test that port 80 is open to the beacon	<p>From the command line, run one of the following commands:</p> <ul style="list-style-type: none"> <li>a) telnet C-172-20-151-96.stc.corp 80</li> <li>b) run the PowerShell command: <code>Test-NetConnection -ComputerName C-172-20-151-96.stc.corp -Port 80 -InformationLevel Quiet</code></li> <li>c) open a web browser at attempt to connect to <a href="http://C-172-20-151-96.stc.corp">http://C-172-20-151-96.stc.corp</a></li> </ul>	<p>Standard port used by the agent is port 80.</p> <p>A successful telnet command to port 80 will blank the screen, and not return a "Connect failed" error.</p> <p>For the PowerShell test, a successful test will return "TRUE".</p> <p>Connecting via the web browser should show the IIS server page.</p>
3)	Test that the Inventory Beacon can be pinged.	<p>From the command line, run the command:</p> <p>Ping C-172-20-151-96.stc.corp</p>	<p>The Inventory Beacons need to be able to be pinged, as the agents' algorithm for prioritising which beacon to upload to utilise ping results.</p>

If all commands complete without error the installation can commence. If the commands do not run successfully this most likely indicates a networking issue that will need resolution by the operators of the network. Possible reasons are DNS misconfiguration, restrictive firewall settings and unexpected barriers within the route from the client to the server.

## 4.7. Account Specifications

To install the FNMS Inventory Agent a user with Administrator privileges (Windows) or root privileges (UNIX) to the target computer needs to be pre-configured prior to installation.

Additionally, there can be no group policy or other restrictions denying access privileges.

On Windows based computers, the agent will run as SYSTEM.

On UNIX based computers, the agent will run as root.

## 5. Installation of the FNMS Agent

Links to download the Flexera Installation packages:

<a href="\\C-172-20-151-96\FNMS_Agent2017">\\C-172-20-151-96\FNMS_Agent2017</a>
OR
<a href="http://172.20.151.96:8080/">http://172.20.151.96:8080/</a>

### 5.1. Agent Installation – Windows

#### 5.1.1. Windows Agent Information

Name	FlexNet Inventory Agent
Version	12.4.0
Size	20Mb
Compatibility	Windows XP or better
Source file location	<a href="\\C-172-20-151-96\FNMS_Agent2017">\\C-172-20-151-96\FNMS_Agent2017</a>

#### 5.1.2. Manual Installation

Perform the following steps to install the agent manually:

Step #	Description
1.	Logon to the target computer via RDP, as a local administrator.
2.	Copy the FNMS agent install files from an Inventory Beacon share to a local directory, for example <a href="#">C:\Temp\FNMS_Agent</a> . Refer to section <a href="#">Agent source file locations</a>
3.	Place a copy of the up-to-date mgsetup.ini file in the local directory. Refer to section <a href="#">Mgsetup.ini configuration file</a>
4.	Open a command prompt (cmd) as administrator.
5.	Cd to the local copy of the FNMS agent <a href="#">Cd c:\Temp\FNMS_Agent</a>

Step #	Description
6.	To install manually: <ol style="list-style-type: none"> <li>Execute <b>setup.exe</b></li> <li>Step through the install wizard, accepting the EULA, and selecting a default installation</li> <li>Once complete restart the ndinit service to initiate the bootstrap process.               <ol style="list-style-type: none"> <li>Open a command prompt <b>as administrator</b></li> <li>Run the command "<b>net stop ndinit</b>"</li> <li>Run the command "<b>net start ndinit</b>"</li> </ol> </li> </ol>
7.	To install silently: <ol style="list-style-type: none"> <li>Open a command prompt</li> <li><b>Cd C:\Temp\FNMS_Agent</b></li> <li>Run the following command: <b>msiexec /i "FlexNet Inventory Agent.msi" /qn</b></li> </ol>
8.	Finished.

Refer to [Appendix B: Troubleshooting](#) to verify that the agent was successfully installed.

### 5.1.3. Packaged Installation

Refer to the steps in the [Manual Installation](#) section for any CLI commands to use for a packaged installation.

### 5.1.4. Log Files

During installation, some log files are written to %temp%\ManageSoft, the temporary folder of the installing account.

After installation, by default all log files are written to **C:\Windows\Temp\ManageSoft**.

## 5.2. Agent Installation – UNIX

### 5.2.1. Unix Agent Information

Name	FlexNet Inventory Agent
Version	12.4.0
Size	20Mb max (depending on distribution)

Compatibility	See <a href="#">Appendix A: Supported Operating Systems</a>
Source file location	\\C-172-20-151-96\FNMS_Agent2017

### 5.3. HTTPS Certificates

As per the [Agent Configuration Decisions](#), https is not implemented.

### 5.4. FNMS Agent Configuration Settings

A file named **msgft\_rollout\_response** is required to be copied to **/var/tmp** directory. This is mandatory and the location cannot be changed. This file contains the initial configuration settings to install the agent. For Solaris systems, an addition file named admin is required to be placed in to directory containing the installation packages. After installation, additional settings from a file named **client\_config.ini** are merged with the **/var/opt/managesoft/etc/config.ini** file.

### 5.5. Manual Installation

Full instructions for installation of UNIX agents can be found in the Flexera Agent and Managed Devices document. A generic set of instructions is documented here.

Perform the following steps to install the agent manually:

Step#	Description
1)	Logon to the target computer.
2)	Copy the FNMS agent install files from an Inventory Beacon share to a local directory, for example <b>/var/tmp/fnmsagent</b> . Refer to section <a href="#">Unix Agent Information</a> .
3)	Copy the <b>msgft_rollout_response</b> file to <b>/var/tmp</b>
4)	For Solaris platforms only, copy the admin file to the local directory with the install files, in this case <b>/var/tmp/fnmsagent</b>
5)	Copy the <b>client_config.ini</b> file to the local directory with the install files, in this case <b>/var/tmp/fnmsagent</b>
	<b>[this step not applicable]</b>
6)	If using https connectivity with server certificate checking (production environment), copy the <b>msgft_rollout_cert</b> file to <b>/var/tmp</b>

Step#	Description	
7)	As “ <b>sudo</b> ” run the install command (substitute [ <b>PACKAGE PATH</b> ] and [ <b>VERSION</b> ] as appropriate:	
	AIX	<a href="#">Appendix 1</a> installp -aY -d managesoft.[VERSION].bff managesoft.rte
	HP-UX	<a href="#">Appendix 2</a> swinstall -v -x mount_all_filesystems=false -x allow_downdate=true -s [PACKAGE PATH]/managesoft-[VERSION].depot managesoft
	Linux x86	<a href="#">Appendix 3</a> rpm --upgrade --oldpackage --verbose managesoft-[VERSION]-1.i386.rpm
	Linux x86_64	<a href="#">Appendix 4</a> rpm --upgrade --oldpackage --verbose managesoft-[VERSION]-1.x86_64.rpm
	Mac OS X	<a href="#">Appendix 5</a> installer -verbose -pkg ManageSoft.pkg -target
	Solaris SPARC	<a href="#">Appendix 6</a> pkgadd -n -a admin -r /dev/null -d managesoft-[VERSION].sparc.pkg ManageSoft
	Solaris x86	<a href="#">Appendix 7</a> pkgadd -n -a admin -r /dev/null -d managesoft-[VERSION].x86.pkg ManageSoft
8)	Update the config.ini by running the following command: <b>/opt/managesoft/bin/mgsconfig -i /var/tmp/fnmsagent/client_config.ini</b>	

Step#

Description

Execute `/opt/managesoft/bin/managesoft-configure`

Enter the following details

Entry	Production System Value	Notes
Domain Name	STC.corp	Or whatever you know the actual domain of the server is
Bootstrap Download Location	http://C-172-20-151-96.stc.corp/ManageSoftDL	Depending on the location of the target server, you may want to enter a different beacon
9) Bootstrap Upload Location	http://C-172-20-151-96.stc.corp/ManageSoftRL	Depending on the location of the target server, you may want to enter a different beacon
Alternative Machine Identification		LEAVE BLANK
Policy Location Path		LEAVE BLANK
Run Policy	y	Y to confirm
Confirm Options	y	Y to confirm

10) Wait 30 second to one minute for the policy to execute.

Execute `/opt/managesoft/bin/ndschedag -e`

11) And confirm that the ‘Generate Inventory’ event is now seen.

Refer to [Appendix B: Troubleshooting](#)

Run an inventory process by running the following command:

12) `/opt/managesoft/bin/ndtrack -t machine`

## 5.6. Installation Verification

Perform the following steps to verify that agent installed and configured correctly.

Step#	Description	
1.	Run the following command to see the version of the agent installed:	
2.	AIX	lspp -l managesoft.rte
	HP-UX	swlist managesoft
	Linux x86	rpm -q managesoft
	Linux x86_64	rpm -q managesoft
	Mac OS X	
	Solaris SPARC	pkgchk managesoft
	Solaris x86	pkgchk managesoft
3.	Confirm the creation of the following directories: <b>/opt/managesoft</b> <b>/var/opt/managesoft</b>	
4.	View the text file <b>/var/opt/managesoft/etc/config.ini</b> Confirm that the settings from the <b>client_config.ini</b> file were merged into the <b>config.ini</b> , using the <b>mgsconfig</b> command during installation	
5.	Run the command <b>/opt/managesoft/bin/ndschedag -e</b> and confirm that policies have successfully downloaded. Confirm that the "Generate Inventory" event is configured to run within the bounds configured on the Inventory Server. <pre> [ root@ : bin]# /opt/managesoft/bin/ndschedag -e Event                               Next Run Time Generate Inventory                  19/01/16 08:39:00 Update Machine Policy               18/01/16 12:48:00 Update Client Settings              19/01/16 00:17:00 Upload Client Files                 18/01/16 13:04:00 [ root@ : bin]# </pre>	

## 5.7. Log Files

The directory **/var/opt/managesoft/log** contains all log files created by the FNMS agent. With successful installation and configuration of the agent as per Unix [Manual Installation](#), the following log files will be created:

- **installation.log**
- **policy.log**
- **schedule.log**

- `tracker.log`
- `uploader.log`
- `usageagent.log`



## 6. Uninstallation of the FNMS Agent

### 6.1. Agent Uninstallation – Windows

#### 6.1.1. Manual Uninstallation

Perform the following steps to uninstall the Windows agent manually:

Step#	Description
1.	Logon to the target computer via RDP, as a local administrator.
2.	Using the task manager, kill all ndtask.exe processes (This stop the uninstall process from asking to reboot the computer)
3.	Open “Add/Remove Programs” (or Control Panel->”Programs and Features”, and uninstall “Flexera Inventory Agent”, or “ManageSoft for managed devices” for older versions of the FNMS agent.


#### 6.1.2. Complete Uninstallation

A manual uninstallation will legacy registry entries and files in “\ProgramData” and “\Program Files (x86)”.

The script CleanAgentUninstall.cmd is provided to completely remove all trace of the agent, with the exception of log files in \Windows\Temp\ManageSoft.

The CLI script calls a vbscript that searches for version of the FNMS Agent (named “Flexera Inventory Agent” or “ManageSoft for managed devices”), performs a silent uninstall using msixec.exe. The CLI script then deletes registry and folder locations.

This script should NOT be run on FNMP/FNMS infrastructure, such as inventory servers or beacons.

CleanAgentUninstall script	 CleanAgentUninstall v1 1.zip
----------------------------	--

Perform the following steps to run the script.

Step#	Description
1.	Logon to the target computer via RDP, as a local administrator.

2. Extract the contents of CleanAgentUninstall.zip to a temporary folder, for example C:\Temp\CleanAgentUninstall.
3. Open a command prompt “as Administrator”
4. Change directory to C:\Temp\CleanAgentUninstall, and run CleanAgentUninstall.cmd  
The installation will take approximately 1 minute to run.

## 6.2. Agent Uninstallation – Unix

### 6.2.1. Manual Uninstallation

Perform the following steps to uninstall the UNIX agent manually:

Step#	Description														
1.	Logon to the target computer.														
2.	As “superuser” run the uninstall command: <table border="1"> <tr> <td><b>AIX</b></td><td>installp -u managesoft.rte</td></tr> <tr> <td><b>HP-UX</b></td><td>swremove managesoft</td></tr> <tr> <td><b>Linux x86</b></td><td>rpm --erase --verbose managesoft</td></tr> <tr> <td><b>Linux x86_64</b></td><td>rpm --erase --verbose managesoft</td></tr> <tr> <td><b>Mac OS X</b></td><td>/opt/managesoft/bin/uninstall-managesoft.command -force</td></tr> <tr> <td><b>Solaris SPARC</b></td><td>echo action=nocheck &gt; admin.mgs pkgrm -n -a admin.mgs managesoft rm -f admin.mgs</td></tr> <tr> <td><b>Solaris x86</b></td><td>echo action=nocheck &gt; admin.mgs pkgrm -n -a admin.mgs managesoft rm -f admin.mgs</td></tr> </table>	<b>AIX</b>	installp -u managesoft.rte	<b>HP-UX</b>	swremove managesoft	<b>Linux x86</b>	rpm --erase --verbose managesoft	<b>Linux x86_64</b>	rpm --erase --verbose managesoft	<b>Mac OS X</b>	/opt/managesoft/bin/uninstall-managesoft.command -force	<b>Solaris SPARC</b>	echo action=nocheck > admin.mgs pkgrm -n -a admin.mgs managesoft rm -f admin.mgs	<b>Solaris x86</b>	echo action=nocheck > admin.mgs pkgrm -n -a admin.mgs managesoft rm -f admin.mgs
<b>AIX</b>	installp -u managesoft.rte														
<b>HP-UX</b>	swremove managesoft														
<b>Linux x86</b>	rpm --erase --verbose managesoft														
<b>Linux x86_64</b>	rpm --erase --verbose managesoft														
<b>Mac OS X</b>	/opt/managesoft/bin/uninstall-managesoft.command -force														
<b>Solaris SPARC</b>	echo action=nocheck > admin.mgs pkgrm -n -a admin.mgs managesoft rm -f admin.mgs														
<b>Solaris x86</b>	echo action=nocheck > admin.mgs pkgrm -n -a admin.mgs managesoft rm -f admin.mgs														
3.	Verify the existence of the <b>managesoft</b> folder in <b>/var/opt</b> . If this folder exists then remove it using the following command <b>rm -rf ./managesoft</b> from the <b>/var/opt</b> folder.														
4.	Verify the existence of the <b>managesoft</b> folder in <b>/var/tmp</b> . If this folder exists then remove it using the following command <b>rm rf ./managesoft</b> from the <b>/var/tmp</b> folder.														

- |    |  |
|----|--|
| 5. | Verify the existence of the <b>managesoft</b> folder in <b>/opt</b> . If this folder exists then remove it using the following command <b>rm -rf ./managesoft</b> from the <b>/opt</b> folder. |
| 6. | Verify the existence of the <b>managsoft.ini</b> file in <b>/etc</b> . If this file exists then remove it using the following command <b>rm ./managesoft.ini</b> from the <b>/etc</b> folder.  |

## 7. Appendix A: Supported Operating Systems

Supported Operating Systems for the current FNMS Agent's installation

Operating System
<b>Windows</b>
Windows Server 2016
Windows Server 2012 R2 SP1
Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2 x64 Server Core
Windows Server 2008 R2 x64
Windows Server 2008 Server Core
Windows Server 2008 Server Core
Windows Server 2008 x64 Server Core
Windows Server 2008 x64
Windows Server 2003 R2
Windows Server 2003 R2 x64
Windows Server 2003
Windows Server 2003 x64
Windows XP Professional
Windows XP Professional x64
Windows XP Home
Windows Vista
Windows Vista x64
Windows 7
Windows 7 x64
Windows 8
Windows 8 x64
Windows 10
Windows 10 x64

**Linux**

Ubuntu 12 - 15 (x86-64 only)

Debian 6, 7 (x86-64 only)

RedHat Linux 8 and 9 (x86-64 only)

RedHat Enterprise Linux 3, 4, 5, 6, 7 (x86-64 only)

CentOS 4 – 7 (x86-64 only)

Fedora 6 – 11 &amp; 18 – 23 (x86-64 only)

Oracle Linux 4.5 – 7.0 (x86-64 only)

SuSE Professional 12, 13 (x86-64 only)

SuSE Enterprise Server 11 &amp; 12 (x86-64 only)

**Solaris**

Solaris 9, 10, 11 (Intel), Zones for versions 10 &amp; 11

Solaris 8, 9, 10, 11 (SPARC), Zones for versions 10 &amp; 11

**Mac OS**

Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10, 10.11

**AIX**

AIX 5.2, 5.3, 6.1, 7.1, LPARs

**HP-UX**

HP-UX 11.00, 11i, 11i v2, 11i v3, vPars/nPars

For Windows 2000 servers, a legacy agent (Version 8.4) can be used.

## 8. Appendix B: Troubleshooting

### 8.1. I would like to see if the computer has working network connectivity to a beacon.

Refer to section [Validate Network Connectivity](#) in this document.

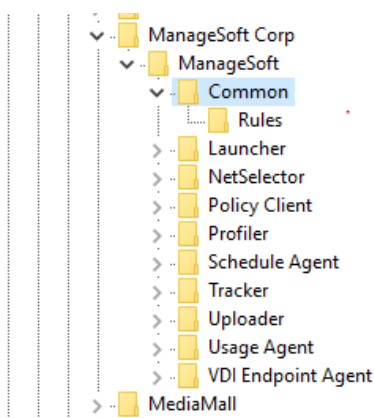
### 8.2. I would like to confirm that the agent was installed correctly on Windows.

Check that the agent was installed correctly, with the configuration file (mgssetup.ini) placed in the install folder. Perform the following steps:

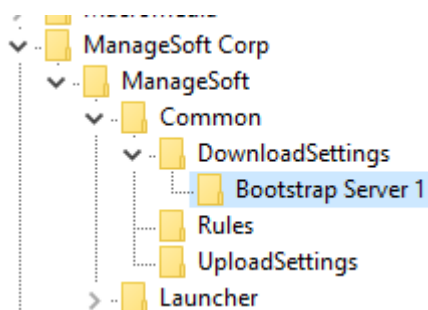
**Table 2: Check for Bootstrap Server key.**

Step	Description
1)	<p>For Windows, open regedit.exe</p> <p>For 64bit systems go to the following node:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ManageSoft Corp\ManageSoft\Common</p> <p>For 32 bit systems go to the following node:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ManageSoft\Common</p>
2)	Expand the DownloadSettings key.
3)	Confirm that in the DownloadSettings key there is a 'Bootstrap Server' key.

If this Bootstrap Server key is not there, it means that the agent was installed without putting the mgssetup.ini file in the install folder before installing.



**Figure 1: In correctly installed agent, with no Bootstrap key.**



**Figure 2: A correctly configured agent, with Bootstrap key.**

To remediate this, perform the following steps:

**Table 3: Remediate incorrectly installed Windows agent.**

Step	Description
1)	Perform a <a href="#">Manual Uninstallation</a> of the agent
2)	Perform a <a href="#">Manual Installation</a> of the agent, ensuring that the mgssetup.ini file is placed in with the install media BEFORE installing, as per the instructions.

### 8.3. I would like to confirm that the agent was installed correctly on UNIX.

Check that the agent was installed correctly, with response file in place, and managesoft-config command executed correctly.

Perform the following steps:

**Table 4: Check for Bootstrap Server setting in config.ini on UNIX.**

Step	Description
1)	Logon to the target computer
2)	Using a text editor, open the file /var/opt/managesoft/etc/config.ini
3)	Confirm that in data exists in the following section  [ManageSoft\Common\UploadSettings\Bootstrap Server 1]  [ManageSoft\Common\DownloadSettings\Bootstrap Server 2]

If the Bootstrap Server entries do not exist, it means that the agent was installed executing the managesoft-config.

To remediate, refer to the [Manual Installation](#) section, and perform the step to execute the command managesoft-config.

**Table 5: The config.ini file must show the bootstrap server settings.**

```
[ManageSoft\Tracker\CurrentVersion\Linux\Hardware\MGSVM_VMComputerSystem]
provider=LinuxVMComputerSystem

[ManageSoft\Common\UploadSettings\Bootstrap Server 1]
Protocol=http
Priority=100
AutoPriority=False
Host=tmgwinapp03.corp.tmg100.com
Port=80
User=
Password=
Directory=/ManageSoftRL

[ManageSoft\Common\DownloadSettings\Bootstrap Server 1]
Protocol=http
Priority=100
AutoPriority=False
Host=tmgwinapp03.corp.tmg100.com
Port=80
User=
Password=
Directory=/ManageSoftDL/

[ManageSoft\Common\UploadSettings\{1B3E9499-704A-43A0-898D-918A71B47FDE}]
```



## 8.4. I would like to confirm that the agent is functioning correctly on Windows, by looking at the registry.

If you have confirmed that the agent was installed correctly, you can check that the agent is functioning correctly by looking at the registry.

Note that this check can be performed remote from the computer, if the required permissions and connectivity to see the computer's registry are available.

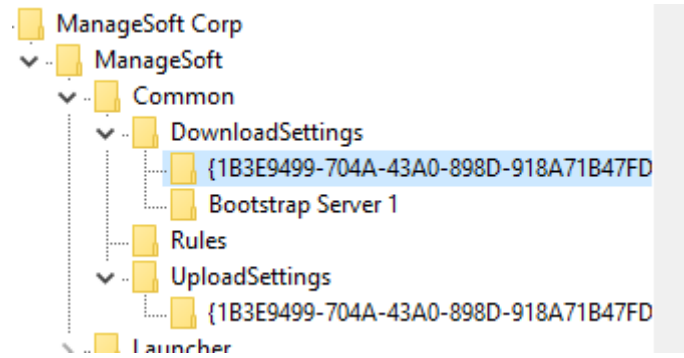
Perform the following steps:

**Table 6: Check to GUID keys in registry on Windows.**

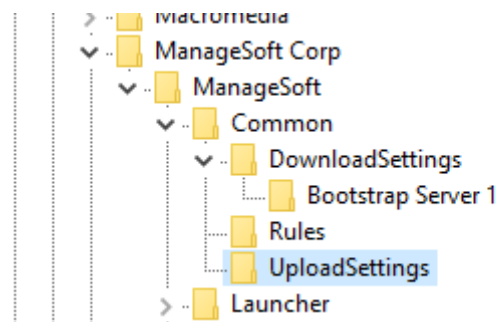
Step	Description
1)	<p>For Windows, open regedit.exe and go to the node</p> <p>For 64bit systems:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ManageSoft Corp\ManageSoft\Common</p> <p>For 32 bit systems:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ManageSoft\Common</p>
2)	Open the DownloadSettings and UploadSettings keys.
3)	In the DownloadSettings and UploadSettings keys, confirm that there are keys named as GUIDS. These represent each of the <a href="#">Beacon Servers</a> in the FNMS implementation.

If these keys do not exist, it means that the agent may have been installed correctly, and that network connectivity issues are possibly stopping the download of the policy.

Refer to section [Validate Network Connectivity](#).



**Figure 3: Correctly installed and functioning agent, GUID registry keys exist.**



**Figure 4: Missing GUID keys indicate that the agent is installed, but is not functioning correctly.**

### 8.5. I would like to confirm that the agent is functioning correctly on Windows, by checking the Schedule Agent.

If you have confirmed that the agent was installed correctly, you can check that the agent is functioning correctly by looking checking the Schedule Agent dialog box.

For Windows platforms, perform the following steps:

**Table 7: Open the Schedule Agent dialog box.**

Step	Description
1)	Logon to the target computer.
2)	Open an "As Administrator" command prompt.
3)	Cd C:\Program Files (x86)\ManageSoft\Schedule Agent\

Step	Description
4)	Execute either:  ndschedag.exe -o scheduletype=machine  or  ndschedag.exe -t machine

If no Events are found, check that you are executing ndschedag “As Administrator”.

If no Events are found even after checking that ndschedag is executed correctly, [Validate Network Connectivity](#), and confirm that the agent was installed correctly.

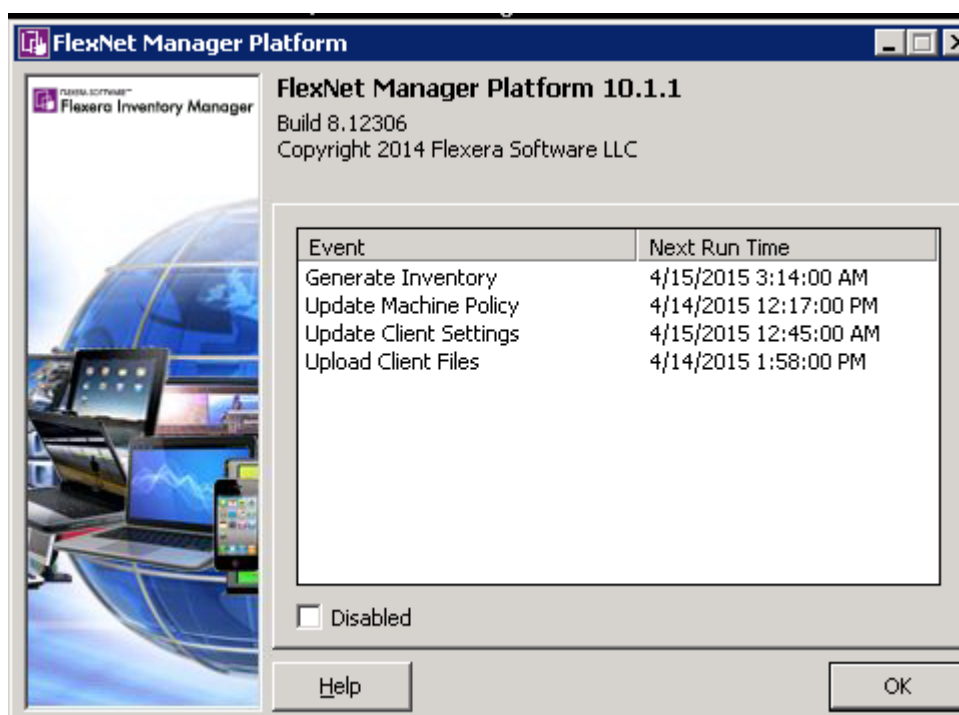


Figure 5: ndschedag.exe showing a correctly configured Agent

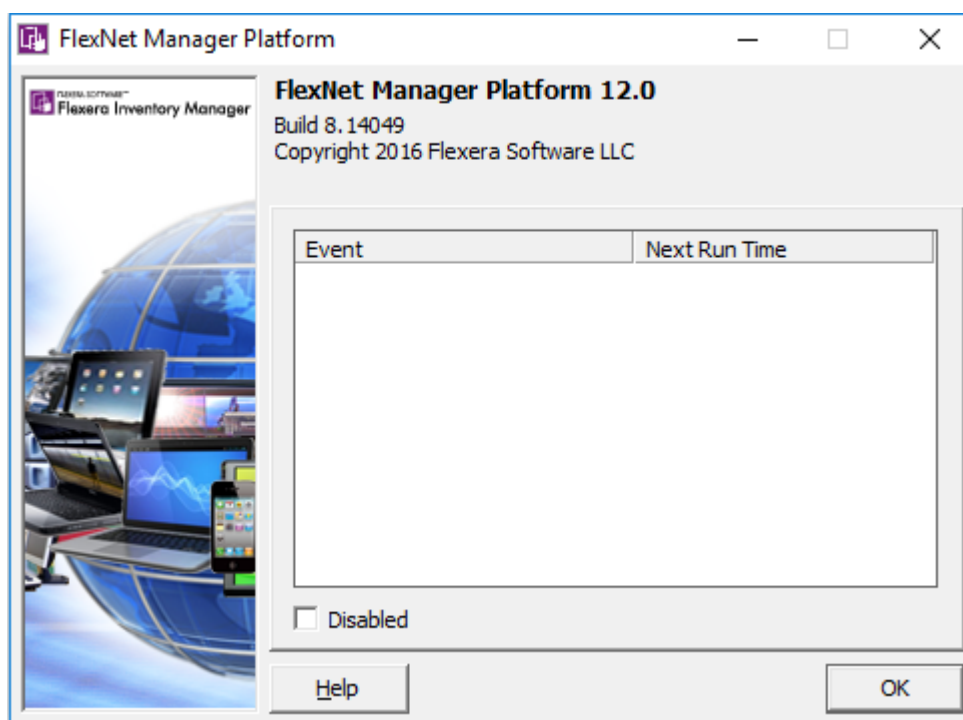


Figure 6: Missing Event information, possibly run "As Administrator"

## 8.6. I would like to confirm that the agent is functioning correctly on UNIX.

For UNIX platforms, perform the following steps:

Table 8: Run the Schedule Agent command on UNIX.

Step	Description
1)	Logon to the target computer
2)	Open a sudo command prompt
3)	Execute the following command: /opt/managesoft/bin/ndschedag -e
4)	Confirm that a number of events are visible, namely Generate Inventory, Update Machine Policy, Update Client Settings, Upload Client Files.

If no Events are found, check that you are executing ndschedag as sudo.

If no Events are found even after checking that ndschedag is executed correctly, [Validate Network Connectivity](#), and confirm that the agent was installed correctly.

**Table 9: A correctly functioning agent on UNIX shows all Events.**

```
[root@j1ufedora bin]# ./ndschedag -e

Event                               Next Run Time
Generate Inventory                  16/02/17 00:31:00
Update Machine Policy               16/02/17 00:36:00
Update Client Settings              16/02/17 00:42:00
Upload Client Files                 16/02/17 14:23:00

[root@j1ufedora bin]#
```

## 8.7. I would like to run an inventory process manually on Windows.

Perform the following steps:

**Table 10: Run the inventory process manually, using the Schedule Agent dialog.**

Step	Description
1)	Logon to the target computer.
2)	Open an "As Administrator" command prompt.
3)	Cd C:\Program Files (x86)\ManageSoft\Schedule Agent\
4)	Execute either: ndschedag.exe -o scheduletype=machine or ndschedag.exe -t machine
5)	Right-Click on "Generate Inventory" and select run.

Ndtrack.exe will execute.

Run time will depend on the performance of the computer and the size of its file system.

When complete, ndtrack will terminate. The following logs will be updated

- C:\Windows\Temp\ManageSoft\schedule.log
- C:\Windows\Temp\ManageSoft\tracker.log

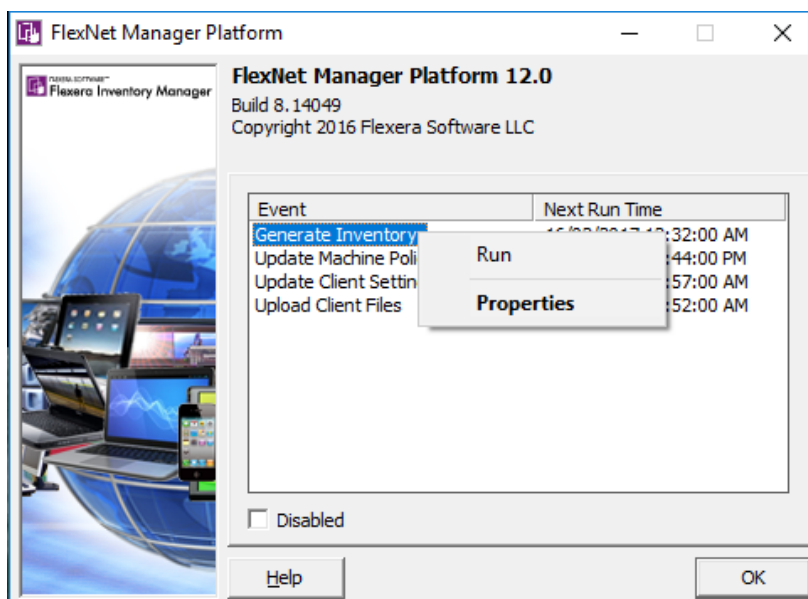


Figure 7: Right-Click on the Generate Inventory Event.

ndinit.exe	5556	Running	SYSTEM	00	668 K	N
ndschedag.exe	8200	Running	SYSTEM	00	2,784 K	S
ndschedag.exe	6136	Running	jlu	00	2,976 K	S
ndtask.exe	512	Running	SYSTEM	00	824 K	N
ndtask.exe	5184	Running	jlu	00	528 K	N
ndtrack.exe	7708	Running	SYSTEM	00	3,440 K	Ir
MirSrv.exe	4660	Running	LOCAL SE	00	8,512 K	N

Figure 8: Ntrack.exe executing as seen in Task Manager

## 8.8. I would like to run an inventory process manually on unix.

Perform the following steps:

Table 11: Run the inventory process manual by running ndtrack.

Step	Description
1)	Logon to the target computer
2)	Open a sudo command prompt
3)	Execute the following command: /opt/managesoft/bin/ndtrack -t machine

Once complete, check the log file

/var/opt/managesoft/log/tracker.log

The end of the file will show where the NDI inventory file was written to.

## 8.9. I would like to run an inventory process manually, on UNIX, but not upload the inventory packet.

Perform the following steps:

Step	Description
1)	Logon to the target computer.
2)	Open a sudo command prompt.
3)	Execute the following command: <code>/opt/managesoft/bin/ndtrack -t machine -o Upload=False</code>

Once complete, check the log file

`/var/opt/managesoft/log/tracker.log`

The end of the file will show where the NDI inventory file was written to.

## 8.10. I would like to check agent log files.

On installation, some log files are saved to %TEMP%\ManageSoft

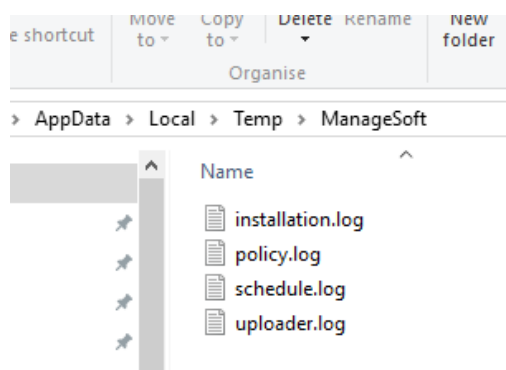


Figure 9: installation log files in %TEMP%

Once the installation is complete, by default all logs are written to C:\Windows\Temp\Managesoft

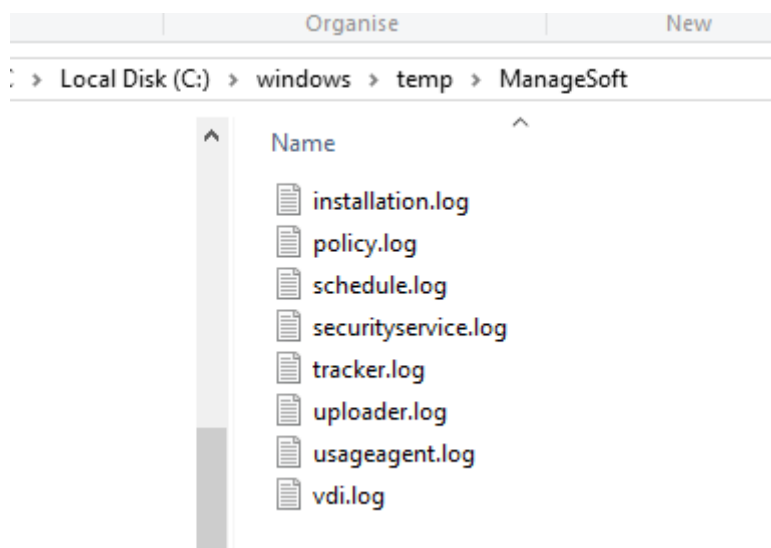


Figure 10: Log files in C:\Windows\Temp\ManageSoft

For UNIX distributions of the agent, logs are written to /var/opt/managesoft/log

### 8.11. I would like confirm that inventory is uploading to a beacon correctly.

Check the tracker.log log file

Search for the words 'upload' or 'uploading'

At the end of the file, there should be a section stating if the NDI packet was uploaded, and to which beacon.

```
[14/02/2017 3:09:38 PM (G, 0)] [9724] Upload directory is 'C:\ProgramData\ManageSoft Corp\ManageSoft\Common\Uploads\Inventories'
[14/02/2017 3:09:38 PM (G, 0)] [9724] Will attempt to upload file(s) '*.ndi.gz'
[14/02/2017 3:09:38 PM (G, 0)] [9724] Upload rule is 'Inventory'
[14/02/2017 3:09:38 PM (G, 0)] [9724] Connecting to upload location 'http://tmgwinapp15/ManageSoftRI/Inventories'
[14/02/2017 3:09:38 PM (G, 0)] [9724] Upload username is ''
[14/02/2017 3:09:38 PM (G, 0)] [9724] Upload proxy is ''
[14/02/2017 3:09:39 PM (G, 0)] [9724] Uploading file 'system on tmgwinlpt12 at 20170214T150603 (Full).ndi.gz' to '
http://tmgwinapp15/ManageSoftRI/Inventories'
[14/02/2017 3:09:39 PM (G, 0)] [9724] File 'system on tmgwinlpt12 at 20170214T150603 (Full).ndi.gz' removed from upload directory
[14/02/2017 3:09:39 PM (G, 0)] [9724] Upload successful
[14/02/2017 3:09:39 PM (G, 0)] [9724] Uploading finished
[14/02/2017 3:09:39 PM (G, 0)] [9724] .....
```

Figure 11: tracker.log showing a successful upload of inventory.