

# User Guide

*Lumension*® Application Scanner Tool 2.2

December 2011



## Notices

### VERSION INFORMATION

Lumension® Application Scanner Tool 2.2 User Guide

Released: December 2011

### COPYRIGHT INFORMATION

Lumension

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255

Phone: +1 888.725.7828

E-mail: [info@lumension.com](mailto:info@lumension.com)

**Copyright© 2011 Lumension Security, Inc.: ALL RIGHTS RESERVED.**

This manual, as well as the software described in it, is furnished under license. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form - electronic, mechanical, recording, or otherwise - except as permitted by such license.

**LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY:** LUMENSION SECURITY, INC. (LUMENSION) MAKES NO REPRESENTATIONS OR WARRANTIES IN REGARDS TO THE ACCURACY OR COMPLETENESS OF THE INFORMATION PROVIDED IN THIS MANUAL. LUMENSION RESERVES THE RIGHT TO MAKE CHANGES TO THE INFORMATION DESCRIBED IN THIS MANUAL AT ANY TIME WITHOUT NOTICE AND WITHOUT OBLIGATION TO NOTIFY ANY PERSON OF SUCH CHANGES. THE INFORMATION PROVIDED IN THE MANUAL IS NOT GUARANTEED OR WARRANTED TO PRODUCE ANY PARTICULAR RESULT, AND THE ADVICE AND STRATEGIES CONTAINED MAY NOT BE SUITABLE FOR EVERY ORGANIZATION. NO WARRANTY MAY BE CREATED OR EXTENDED WITH RESPECT TO THIS MANUAL BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. LUMENSION SHALL NOT BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER DAMAGES ARISING FROM THE USE OF THIS MANUAL, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

### TRADEMARK INFORMATION

Lumension®, Lumension® Intelligent Whitelisting™, Lumension® Patch and Remediation, Lumension® Enterprise Reporting, Lumension® Security Management Console, Lumension® Content Wizard, Lumension® Scan, Lumension® NAC Integrator, Lumension® Security Configuration Management, Lumension® Application Control, Lumension® Device Control, Lumension® Endpoint Security, Lumension® Endpoint Management and Security Suite, PatchLink®, PatchLink® Update, Sanctuary®, SecureWave®, their associated logos, and all other trademarks and trade names used here are the property of Lumension Security, Inc.

**FEEDBACK**

Your feedback lets us know if we are meeting your documentation needs. E-mail the Lumension Technical Publications department at [techpubs@lumension.com](mailto:techpubs@lumension.com) to tell us what you like best, what you like least, and to report any inaccuracies.

## Table of Contents

User Guide.....	1
<i>Lumension® Application Scanner Tool 2.2</i> .....	1
Notices .....	2
Version Information .....	2
Copyright Information .....	2
Trademark Information .....	2
Feedback .....	3
Table of Contents.....	4
Preface.....	6
About this document.....	6
Typographical Conventions .....	6
Contacting Lumension.....	6
Chapter 1 System Requirements .....	7
Minimum Hardware Requirements.....	7
Supported Operating Systems.....	7
Other Software / Configuration requirements .....	8
Chapter 2 Installation .....	9
Chapter 3 The User Interface.....	14
1) The Main Menu.....	14
2) The Button Bar .....	15
3) The Statistics Pane.....	15
4) The Events View.....	16
5) The Process Indicator Pane.....	16
6) The Status Bar .....	16
7) The Content Pane .....	17
Chapter 4 Using the Application Scanner tool.....	18
Discover.....	18
Assess Applications.....	23
Report.....	25
PDF Reports .....	27
Home .....	29
Chapter 5 File Hash Lookup Utility .....	30
Functional Description.....	30
Modes of Operation.....	30

Chapter 6 Troubleshooting.....33

Chapter 7 Glossary .....34

    Lumension Endpoint Intelligence Center (LEIC).....34

    EIS Cloud Service .....34

    EIS Hash Library .....34

    NSRL Hash Library .....34

    Community Hash Library .....34

    The LEIC Portal.....34

## Preface

### ABOUT THIS DOCUMENT

This User Guide is a resource written for all users of *Lumension®* Application Scanner Tool 2.2. This document defines the concepts and procedures for installing, configuring, implementing, and using the Application Scanner tool.

### TYPOGRAPHICAL CONVENTIONS

Convention	Usage
<b>bold</b>	Buttons, menu items, window and screen objects
<b><i>bold italics</i></b>	Wizard names, window names, page names
<i>italics</i>	New terms, options, variables
UPPERCASE	SQL Commands, keyboard keys
<i>monospace</i>	File names, path names, programs, executables, command syntax

### CONTACTING LUMENSION

<b>Global Headquarters</b> 8660 East Hartford Drive Suite 300 Scottsdale, AZ 85255 United States of America Phone: +1 888 725 7828 Fax: +1 480 970 6323	<b>European Headquarters</b> Atrium Business Park Z.A. Bourmicht 23, rue du Puits Romain L-8070 Bertrange, Luxembourg Phone: +352 265 364 11 Fax: +352 265 364 12	<b>United Kingdom Office</b> Unit C1 Windsor Place Faraday Road, Crawley West Sussex, RH10 9TF United Kingdom Phone: +44 (0) 1908 357 897 Fax: +44 (0) 1908 357 600
<b>North America Sales</b> +1 480 970 1025 (option 1)	<b>International Sales</b> + 44 (0) 1908 357 897 (UK) + 352 265 364 11 (Luxembourg) + 65 6725 6415 (Singapore)	<b>Lumension Endpoint Security Technical Support</b> +1 877 713 8600 (US Toll Free) +44 800 012 1869 (UK Toll Free) +353 9142 2999 (EMEA) E-mail: endpoint.support@lumension.com

**Note:** For additional contact information, please visit the Contact Lumension page at <http://www.lumension.com/contact-us.aspx>.

## Chapter 1 System Requirements

The following sections describe the minimum system requirements necessary for successful installation of *Lumension®* Application Scanner Tool 2.2. The listed specifications are a minimum; larger network environments may require additional hardware and software resources.

### MINIMUM HARDWARE REQUIREMENTS

The hardware requirements for the Application Scanner tool vary depending upon the number of servers and clients you manage. The following minimum hardware requirements will support up to 100 connected Application Scanner tool clients.

Component	Requirement
Server / Management Console	<ul style="list-style-type: none"> <li>• 512 MB RAM (1GB recommended)</li> <li>• Pentium® Dual-Core CPU or AMD equivalent</li> <li>• 3 GB minimum hard disk drive</li> <li>• 100MBit/s NIC</li> <li>• 1024 by 768 pixels for display</li> </ul>
Client	<ul style="list-style-type: none"> <li>• 256 MB RAM (1GB recommended)</li> <li>• 50MB hard disk drive</li> <li>• 100 MBit/s NIC</li> </ul>

### SUPPORTED OPERATING SYSTEMS

Component	Requirement
Server / Management Console	Any one of the following: <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2003 SP2</li> <li>• Microsoft Windows Server 2008 and 2008 R2</li> <li>• Microsoft Windows XP SP2+</li> <li>• Microsoft Windows Vista SP1+</li> <li>• Microsoft Windows 7</li> </ul>
Client	Any one of the following: <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2003 SP2</li> <li>• Microsoft Windows Server 2008 and 2008 R2</li> <li>• Microsoft Windows XP SP2+</li> <li>• Microsoft Windows Vista SP1+</li> </ul>

	<ul style="list-style-type: none"><li>• Microsoft Windows 7</li></ul>
--	---

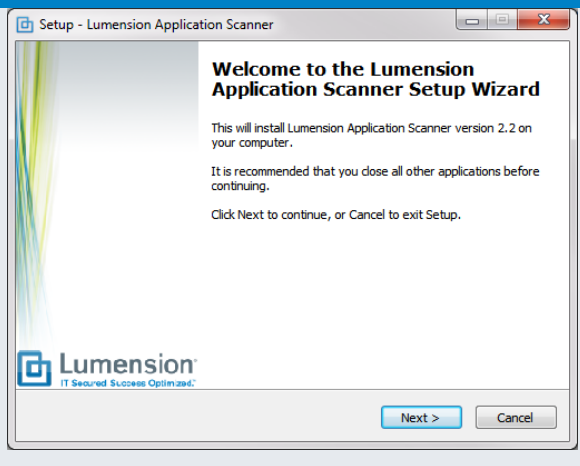
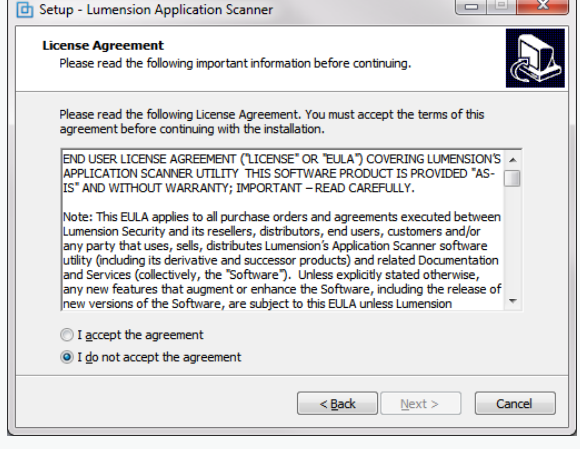
### OTHER SOFTWARE / CONFIGURATION REQUIREMENTS

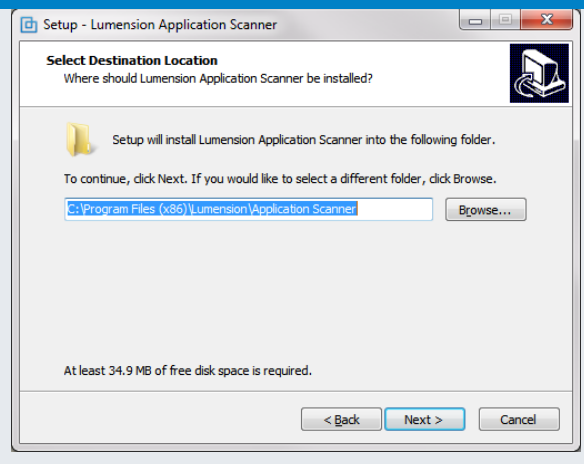
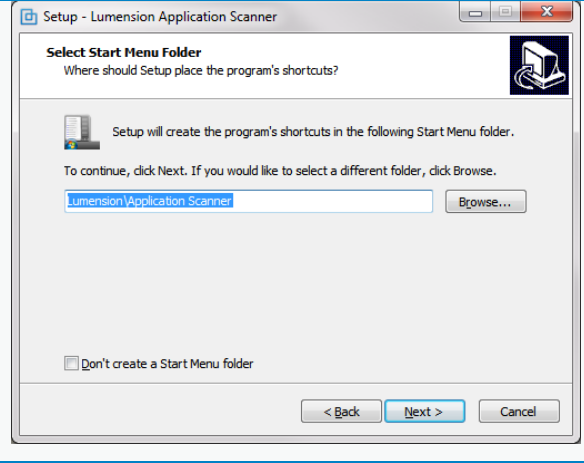
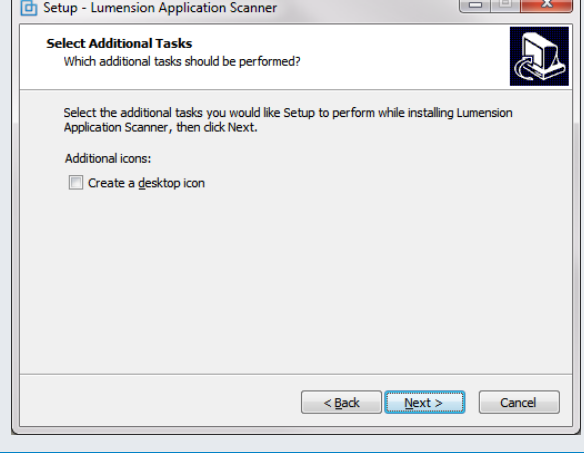
Component	Requirement
Server / Management Console	<ul style="list-style-type: none"><li>• Microsoft .Net v2.0 EN Redistributable Package.</li><li>• The standard FTP port (21) must not be used by another program.</li><li>• The standard HTTP port (80) must be open for outbound internet connections.</li></ul>
Client	<ul style="list-style-type: none"><li>• The WMI service must be up and running and allowed by the local firewall.</li><li>• The “Simple File Sharing” option must be switched off.</li><li>• Outbound FTP to the console must be allowed.</li></ul>

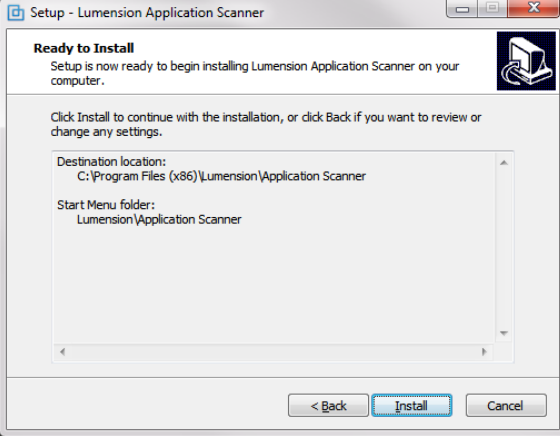
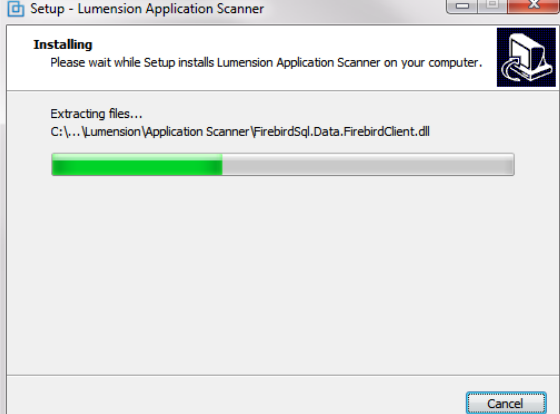
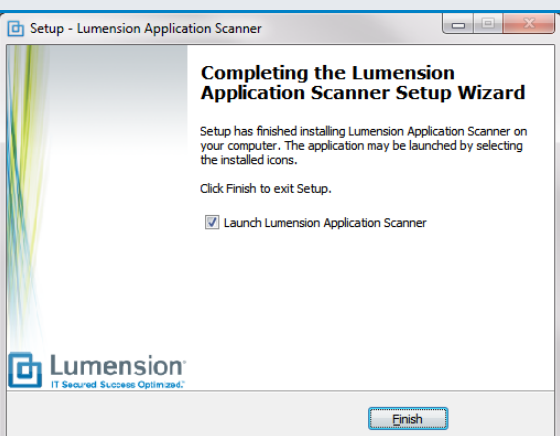
## Chapter 2 Installation

The install *Lumension®* Application Scanner Tool 2.2, double-click on the **appscanner\_setup.2.2.exe** file from the installation media.

Before the Application Scanner tool core components install, the setup procedure will check for additional system requirements (i.e., Microsoft .NET v2.0) and download / install these components. Please make sure to have a valid internet connection during this phase of the installation process.

Installation Screen	Action
	<p>Click on <b>Next &gt;</b> to continue to the next screen</p>
	<p>To accept the EULA, select "I accept the agreement" and click on <b>Next &gt;</b></p>

Installation Screen	Action
	<p>Select the destination folder for the Application Scanner tool server and console and click on <b>Next &gt;</b></p>
	<p>Select the Start Menu Folder Name and click on <b>Next &gt;</b> to continue.</p> <p>Note: it is recommended you create a Start Menu folder for easy access.</p>
	<p>Choose whether you would like to have a desktop icon created and click on <b>Next &gt;</b> to continue.</p> <p>Note: you may create a desktop icon and/or a Quick Launch icon for easy access if desired.</p>

Installation Screen	Action
	<p>Review the installation summary and click on <b>Install</b> to start the installation process.</p>
	<p>Installation in progress.</p>
	<p>Installation complete. Click 'Finish' to launch Lumension Application Scanner immediately.</p>

The Application Scanner tool server and console have been implemented in one executable file: **leics.console.exe**. In addition, there is no separate database to install. The Application Scanner

tool uses an embedded data store, which is automatically created upon first startup of the console.

After the installation process has finished, the installer will suggest launch the Application Scanner tool console. Upon first startup, the console will present a wizard to lead you through the initial configuration of the tool.

To start the Application Scanner tool server and console, simply double-click any of the shortcuts created during installation or **leics.console.exe** in the installation folder. Upon first startup, you will be led through an installation wizard:

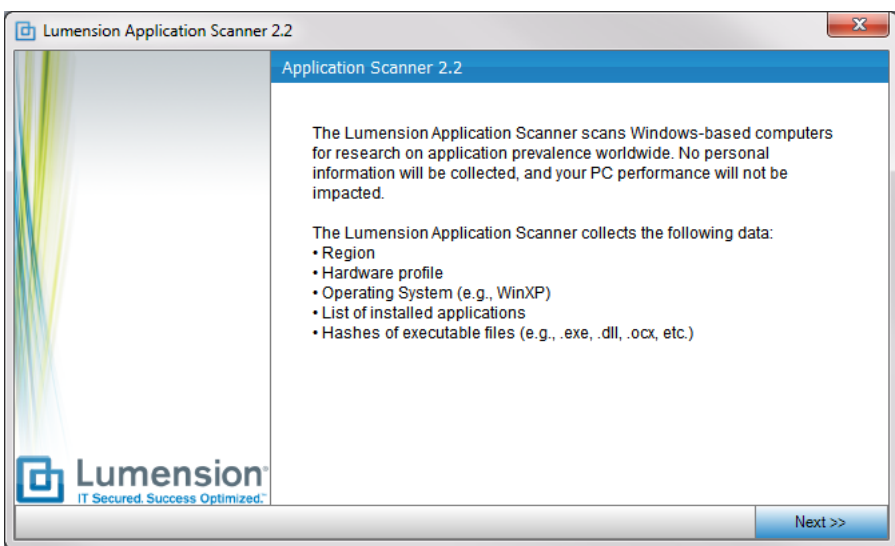


Figure 1: Setup Wizard

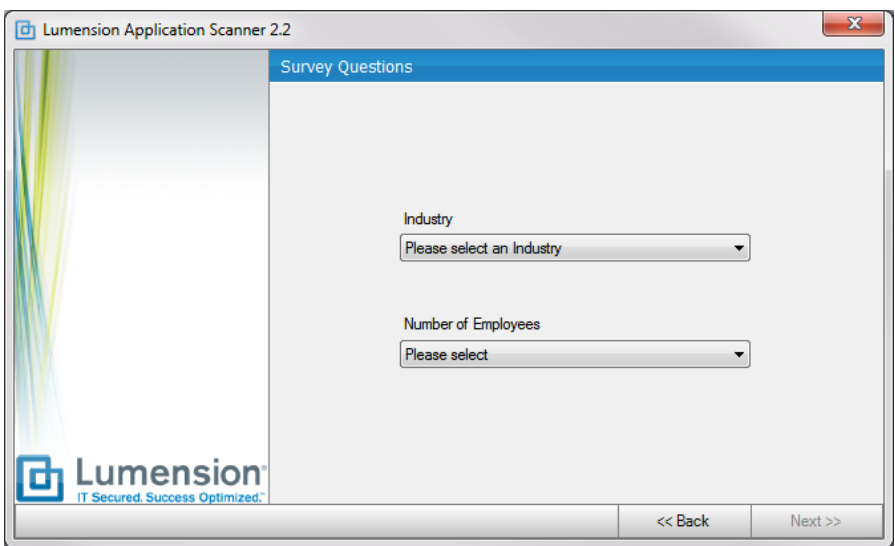


Figure 2: Specify your industry and company size

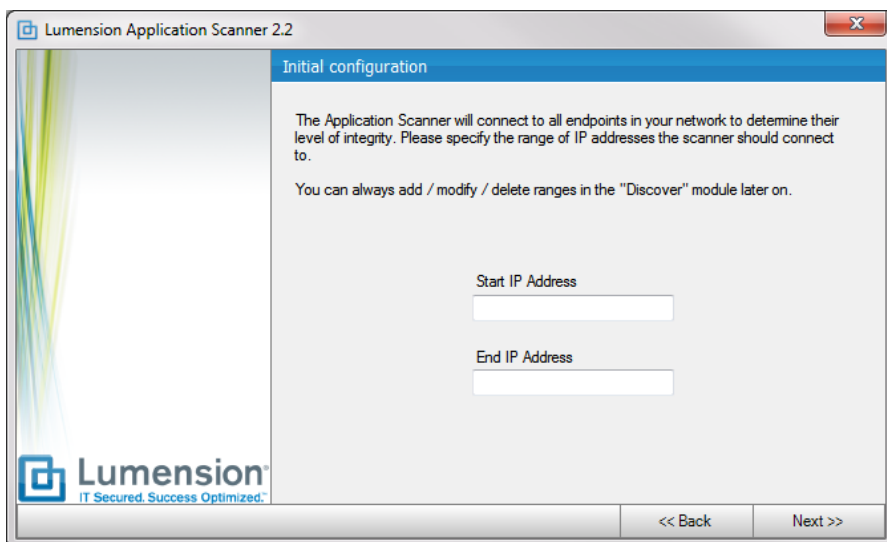


Figure 3: Enter your network's IP address range. You can change this, or add multiple ranges, later on.

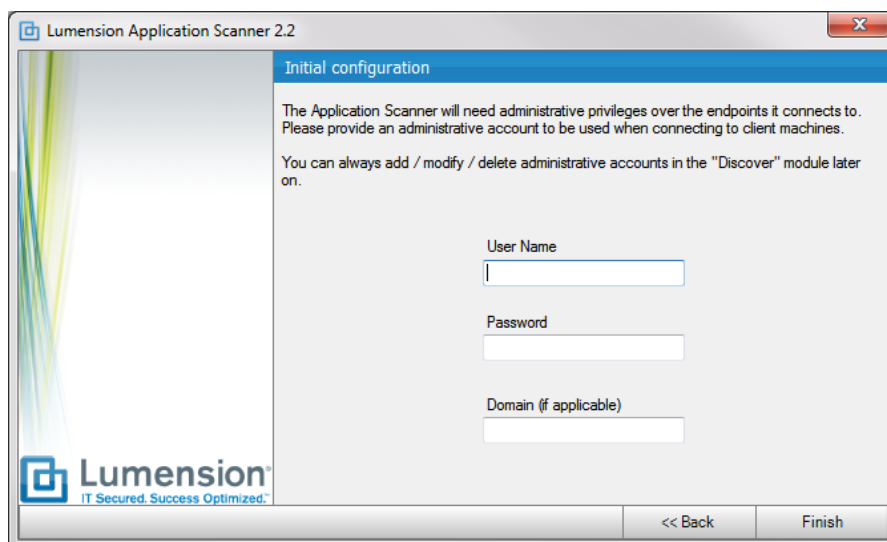


Figure 4: Enter credentials to access endpoints. You can change this, or add multiple credentials, later on.

Once you have completed the wizard, the Application Scanner tool console will load. The console is divided in four (4) modules:

- Discover
- Assess Applications
- Report
- Home

## Chapter 3 The User Interface

The main Lumension® Application Scanner Tool 2.2 user interface is divided in seven (7) panes:

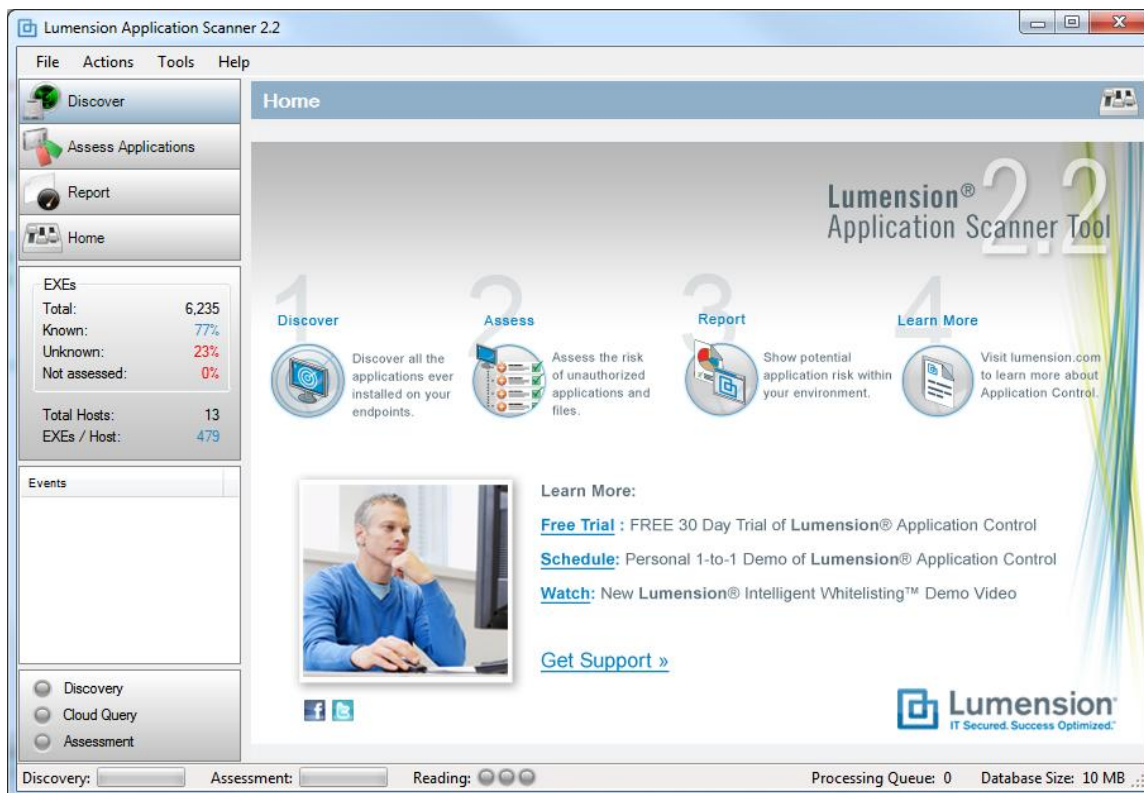




Figure 5: The Main User Interface

### 1) THE MAIN MENU

File Actions Tools Help

#### FILE

**Exit:** Allows you to completely exit the console. **Attention:** if you exit the console, the internal FTP server will be shut down and active scans from endpoints will not be uploaded to the console. If you would like to minimize the console to the system tray, simply click on the upper

right close button . This will minimize the console to the system tray , and with a click on the tray icon, the console is restored again. The FTP server will remain working in the background, as well as all the other Application Scanner tool engines.

#### ACTIONS

The Actions menu item allows you to access the different modules of the Application Scanner tool; it has the same function as the Button Bar (2).

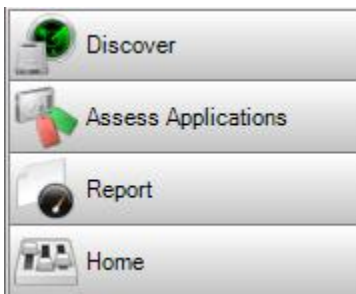
**TOOLS**

The Tools menu allows you to access the Options Dialog (see Scan Options), import L.E.M.S.S endpoints (see L.E.M.S.S Import), as well as to delete all assessments.

**HELP**

The Help menu allows you to visualize this help document, as well as to view the About Dialog which provides version information and lets you check for updates.

**2) THE BUTTON BAR**

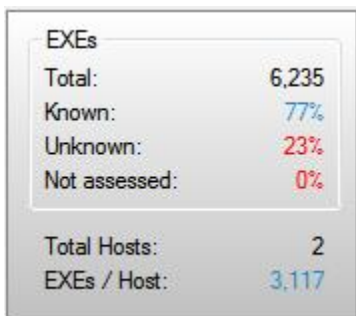


The Button Bar gives you quick access to the four main Application Scanner tool modules:

- Discover
- Assess Applications
- Report
- Home

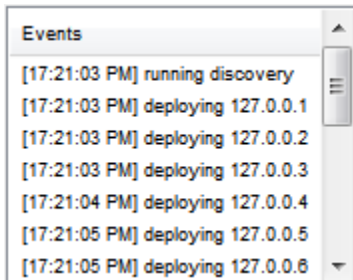
**3) THE STATISTICS PANE**

This view allows you to see the current state of your environment at a glance:



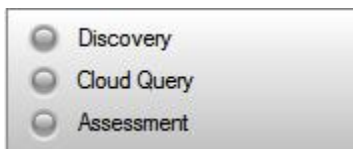
<b>Total</b>	The total number of executables identified in your environment.
<b>Known</b>	The percentage of executables that have known good provenance.
<b>Unknown</b>	The percentage of executables that do not have known good provenance.
<b>Not assessed</b>	The percentage of executables that still need to be assessed.
<b>Total Hosts</b>	The total number of endpoints discovered by the Application Scanner tool.
<b>EXEs / Host</b>	The average number of executables found per endpoint.

#### 4) THE EVENTS VIEW



System events will be shown in this list; that is, you will be notified here when the different engines start working or finish their tasks. Also, all hash files that are uploaded back to the console will show up in this list.

#### 5) THE PROCESS INDICATOR PANE



There are three indicators that show what Application Scanner tool is currently doing in the background:

##### Discovery

Indicates that the Discovery engine is currently scanning IP ranges and hashing executables. You can view the details of the discovery process in the corresponding module.

##### Cloud Query

Indicates that there are outstanding and / or currently processing queries to the cloud regarding hash and application information.

##### Assessment

Indicates that the Assessment procedure is currently running. This procedure will examine executables to determine whether they are of known good provenance and match executables to applications.

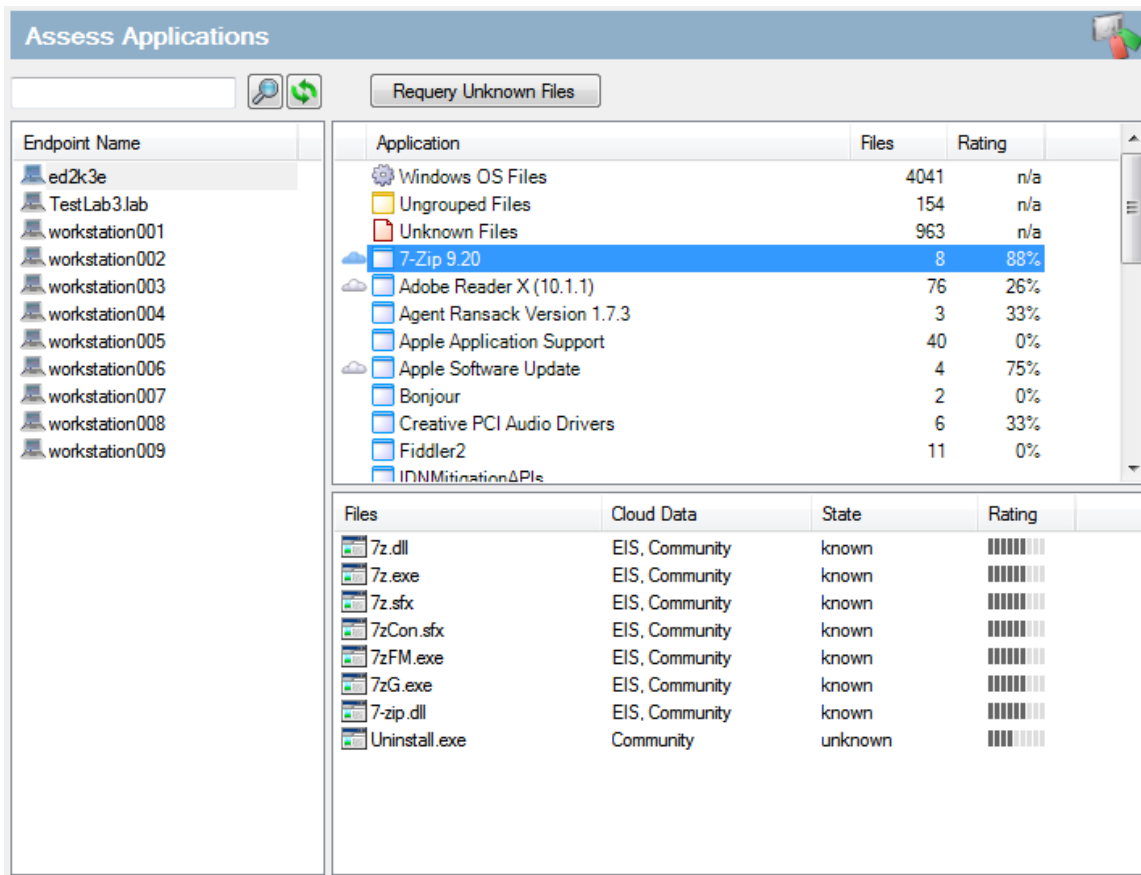
#### 6) THE STATUS BAR



##### Elements of the Status Bar

- Discovery: Progress bar indicating the percentage of completion of the discovery phase.
- Assessment: Progress bar indicating the percentage of completion of the assessment of the current endpoint.
- Matching: LEDs indicating that application matching is currently in progress.
- Processing Queue: Indicates the number of hash files that still need to be processed.
- Database Size: Indicates the size in MB of the internal data storage.

## 7) THE CONTENT PANE



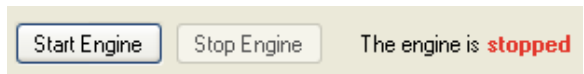
The content pane shows the currently selected module (Discover, Assess Applications, Report, Home) and lets you interact with it. Modules that are not currently shown operate in the background.

## Chapter 4 Using the Application Scanner tool

### DISCOVER

The first task of the Lumension® Application Scanner Tool 2.2 consists of discovering the endpoints within your network environment. As you already have specified an IP range and a set of credentials in the installation wizard, the Application Scanner tool will automatically start scanning. The Discover module allows you to view the current scanning state, as well as to modify scan ranges and credentials and to edit the scan options.

#### Starting / stopping the scan engine



By default, the scan engine will run every 24 hours. You can change this setting in the options popup (see Scan Options). You can also manually start or stop a scanning process by clicking on the corresponding button in the Discover module.

#### Scanning state

Endpoint	Status	Date
192.168.1.1	deployment failure	22.11.2010 14:20
192.168.1.2	no ping reply	22.11.2010 14:20
192.168.1.3	deployment failure	22.11.2010 14:20
192.168.1.4	deployment failure	22.11.2010 14:20
192.168.1.5	deployment failure	22.11.2010 14:20
192.168.1.6	deployment failure	22.11.2010 14:20
192.168.1.7	no ping reply	22.11.2010 14:20
192.168.1.8	deployment failure	22.11.2010 14:20
192.168.1.9	deployment failure	22.11.2010 14:20
192.168.1.10	no ping reply	22.11.2010 14:20
192.168.1.11	deployment failure	22.11.2010 14:20
192.168.1.12	no ping reply	22.11.2010 14:20
192.168.1.13	no ping reply	22.11.2010 14:20
192.168.1.14	deployment failure	22.11.2010 14:20
192.168.1.15	deployment failure	22.11.2010 14:20



The lower panel of the Discover module allows you to see the current state of the machines as defined by your IP range(s). This list is updated automatically as scan results come back from the endpoints. The list will be empty if the scan engine is stopped.

The Discover module can report multiple scanning states:

State	Description
Checking	The endpoint is being pinged to check whether it is up and running.
No ping reply	The endpoint did not reply to a ping request and will not be scanned.

State	Description
Could not connect	<p>The connection to this endpoint has failed. This can have multiple reasons:</p> <ul style="list-style-type: none"> <li>• The endpoint is down</li> <li>• The endpoint runs an unsupported OS</li> <li>• The endpoint's firewall is preventing access</li> <li>• The provided credentials are not valid</li> <li>• The endpoint is configured for simple file sharing</li> <li>• The WMI service is not running</li> </ul> <p>To see why a particular endpoint could not be scanned, please check the console logs.</p>
Could not execute Application Inspector	The console was able to connect to the endpoint and successfully pushed the scanning process (Application Inspector) to the endpoint, but it failed to remotely execute the Application Inspector.
Could not execute ftp commands	The console was able to connect to the endpoint through WMI, but the remote commands to download the Application Inspector failed.
Success	The endpoint scanning process was successfully initiated. Scanning can take 30 minutes (or longer if the user is actively using the endpoint) and will automatically be processed by the console once completed.
Already scanning	There is a scanning process actively running on the endpoint.
Already scanned	The endpoint has already been scanned successfully and will be rescanned after a certain period only (see Scan Options for details).

**The Discovery workflow**

 <p><b>Console</b></p>	 <p><b>Endpoints</b></p>
1) The console starts its internal FTP server.	
2) The console creates a WMI session on each endpoint to be scanned.	
3) The console instructs each endpoint to download the scanning engine (Application Inspector) from its FTP repository.	4) The endpoints download the Application Inspector into a temporary folder.
5) The console instructs each endpoint to execute the downloaded Application Inspector.	6) The endpoints execute the Application inspector in a background process.
	7) Once the Application Inspector has finished its hashing process, hashes are packed and uploaded to the Console FTP server.
8) The console unpacks the uploaded files and inserts the hashes into the internal storage.	
9) The newly inserted hashes are assessed for known provenance.	

**Scan Targets**

The Scan Targets button allows you to enter the target endpoint IP ranges as well as the corresponding credentials. Multiple ranges and multiple credentials can be entered. For each IP address in the range, the Application Scanner tool will try to connect with each provided username / password combination until a successful connection is established.

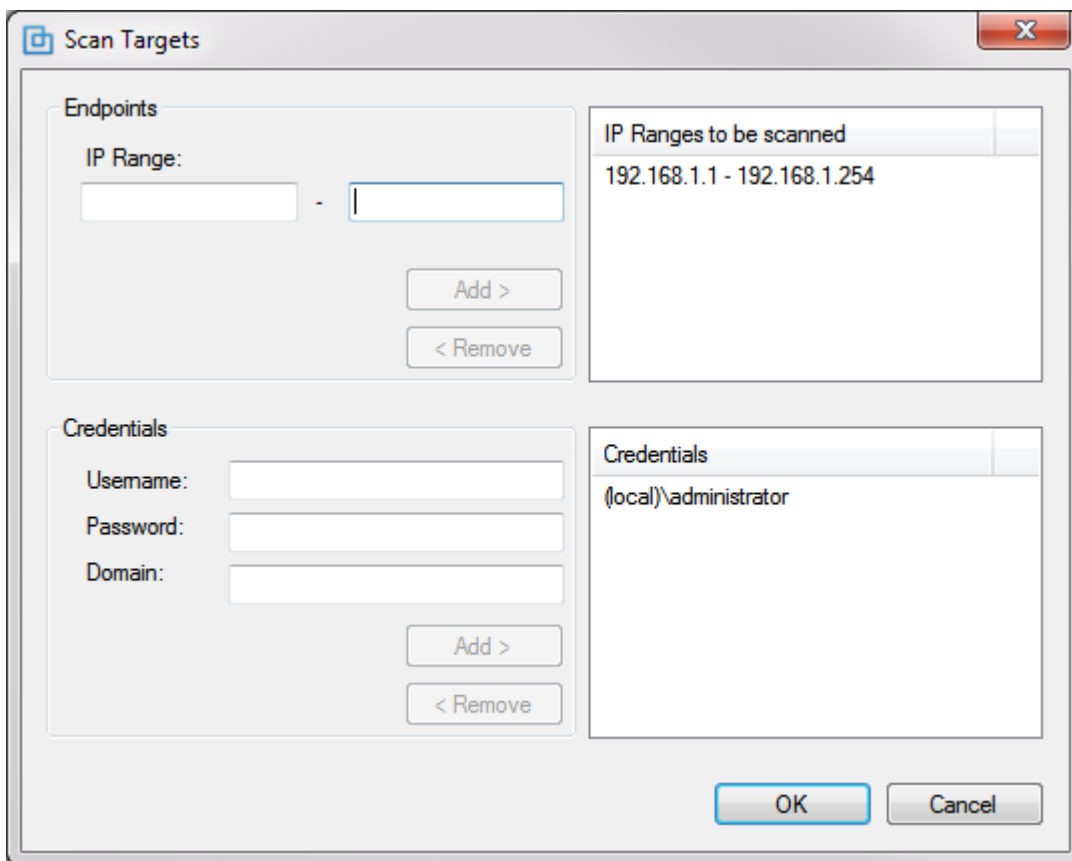


Figure 6: Scan Targets

### Scan Options

The scan options dialog allows you to modify the following settings:

Setting	Description
Endpoint scanning	<p>This determines the extent of the scan on the endpoints.</p> <ul style="list-style-type: none"> <li>• Full - scan all files on all non-removable hard drives</li> <li>• Standard (the default) - scan all files in the program files and Windows directories</li> <li>• Quick - only scan files that are currently loaded in memory</li> </ul>
Automatically start assessment after data processing	<p>If checked, the file provenance assessment will start automatically after data has been gathered from at least one endpoint. If unchecked, you will need to start the assessment manually from the Assess module.</p>

Setting	Description
Start discovery every <h> hours	If checked, the discovery workflow will execute automatically after the specified period of time.
Rescan machines after <d> days	Specifies the period of time after which an endpoint will be rescanned for new executables.
Ping endpoints before scanning	If checked, endpoints will be pinged and scanned only upon successful ping reply. If unchecked, the Application Scanner tool will attempt to scan all endpoints specified in the IP ranges.
Check for updates on startup	If checked, the Application Scanner tool will check whether an update is available online upon startup. To manually check for updates, click on “Check for Updates” in the About dialog.

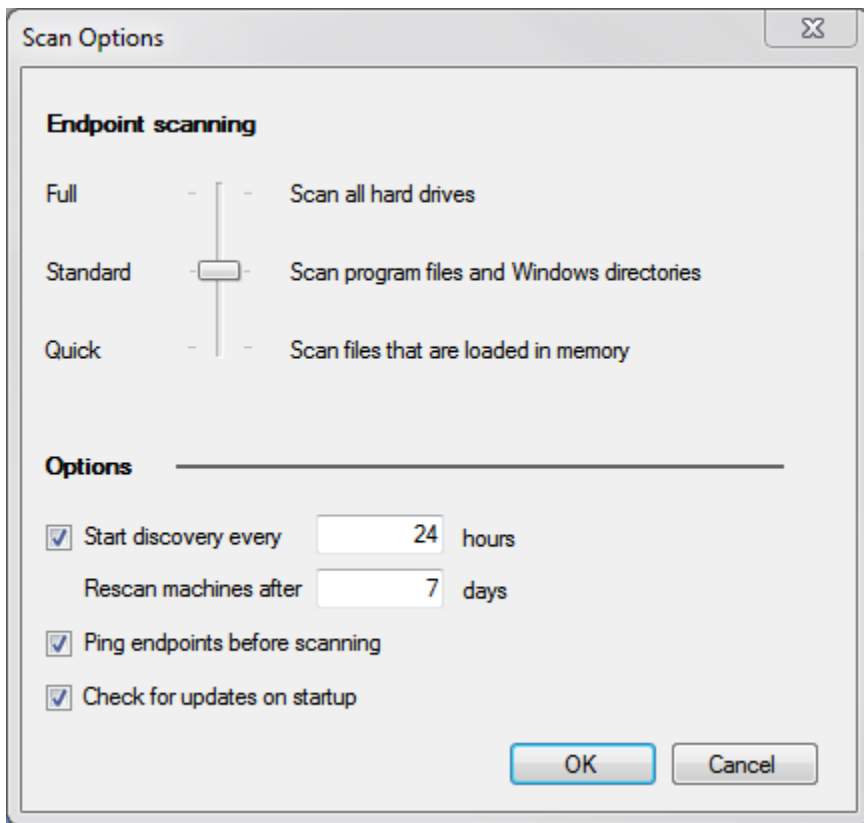


Figure 7: Scan Options

### L.E.M.S.S Import

Endpoint file data can also be directly imported from Lumension® Endpoint Management and Security Suite (L.E.M.S.S). Select "Tools | Import..." and fill out the L.E.M.S.S Server field. Choose between Windows and SQL Authentication. Click Connect to verify the connection then click Import. Endpoints will appear in the Assess Applications module with a Lumension icon.

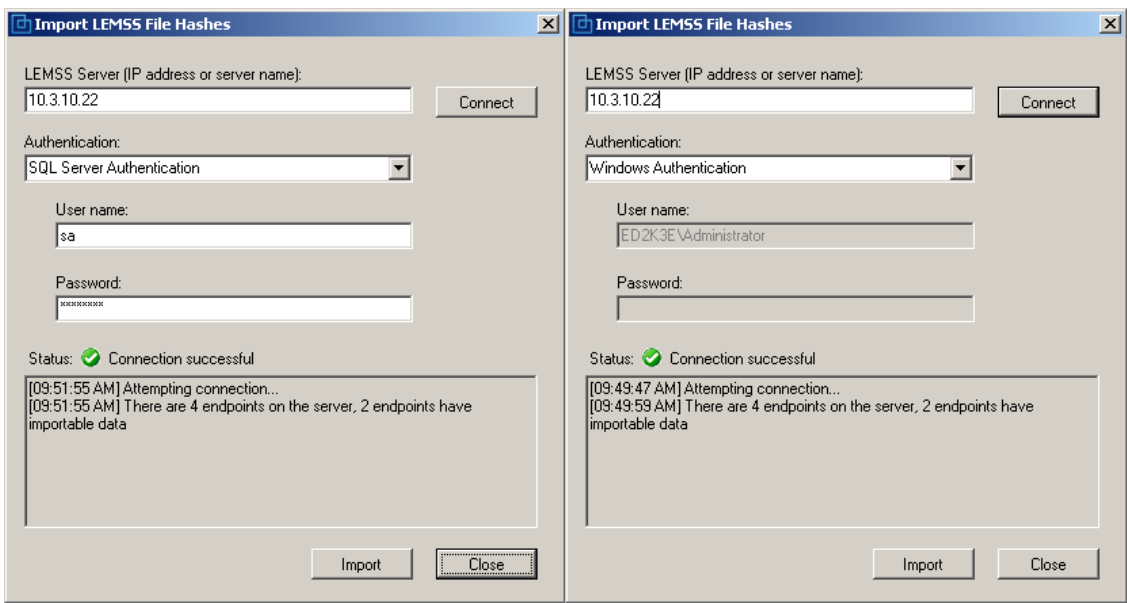


Figure 8: Import L.E.M.S.S File Hashes

## ASSESS APPLICATIONS

The Assess Applications module allows you to identify the software that has been installed on the scanned endpoints and view the prevalence of those applications. It will also report all executable files and the corresponding hashes it has found on all scanned endpoints.

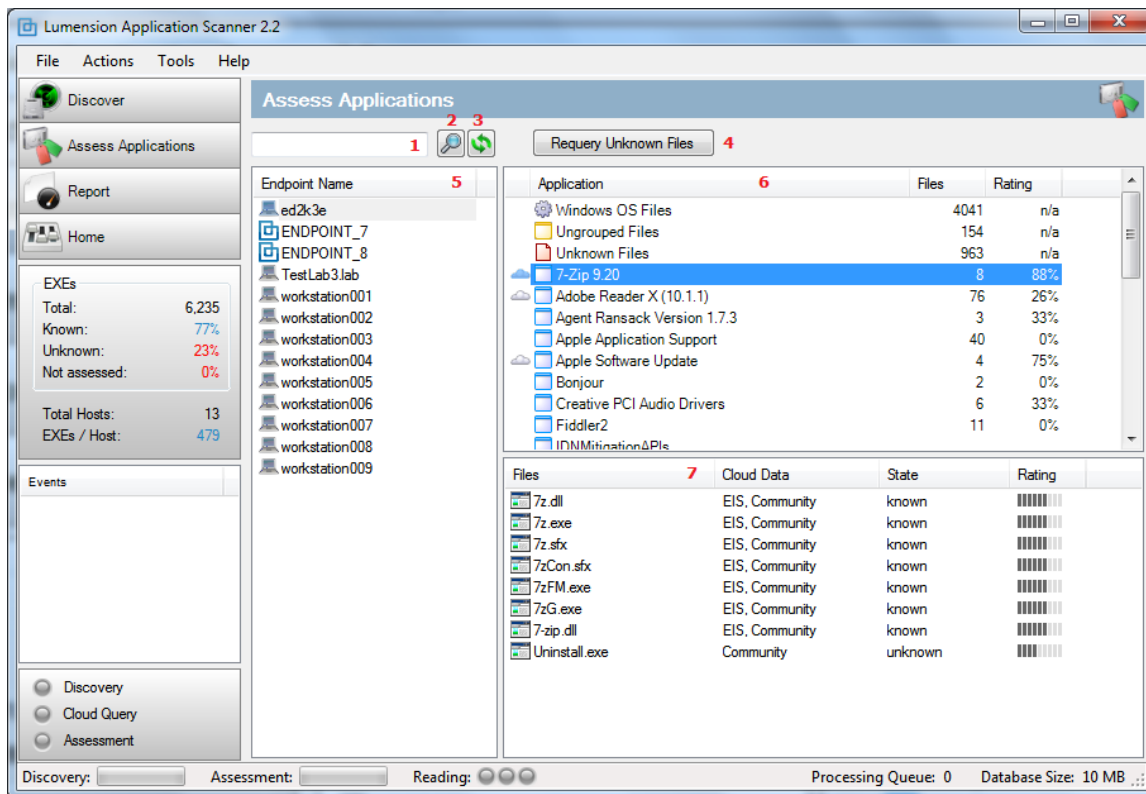


Figure 10: Assess Applications

1. Endpoint search box: Type in a part of the name of an endpoint and click on the search button (2) to find a specific computer.
2. The search button: used to trigger the endpoint search.
3. The refresh button: refreshes the content of the Assess module.
4. Reassess button: Instantly starts an assessment job for executables that have not yet been assessed.
5. Endpoint list box: shows all endpoints known to the system – can be filtered by the search box (1). Endpoints scanned through the Discover module have a generic computer icon while endpoints imported through the L.E.M.S.S Import function have Lumension icon.
6. The application list box shows a list of applications present on a selected endpoint.
  - a. "Windows OS Files" - these files are part of the operating system
  - b. "Ungrouped Files" - these files are of known good provenance but cannot be associated with an application
  - c. "Unknown Files" - these files have not been hashed by Lumension
  - d. Applications
    - i. Cloud icon - indicates that this application is known to Lumension - the tooltip text displays the associated CPE code

- ii. Rating - this is the percentage of files associated with the application that are of good provenance
- 7. Executables list box: shows a list of executables that are part of the selected application on the selected endpoint.
  - a. The State column specifies whether an executable has a known good provenance (“known”), whether it has an unknown provenance (“unknown”) or whether it has not yet been assessed (blank).
  - b. The Cloud Data column details information about the file found in the following databases: Community (data collected from the Lumension community of users), EIS (data collected by Lumension directly from vendors and other known, trusted sources), and NSRL (data collected from the [National Software Reference Library](#), and hosted by NIST).
  - c. The Rating column shows an evaluation of the provenance and prevalence of the file hash.

N.B.: A given endpoint may not have all of the executable files for a specific application installed on it; for example, some files may be OS-specific.

All elements in the endpoint, application and executable list boxes can be double-clicked to present a detail popup.

## REPORT

The report module contains four graphs that visualize the current state of your environment. The graphs can be printed using the corresponding context menu item.

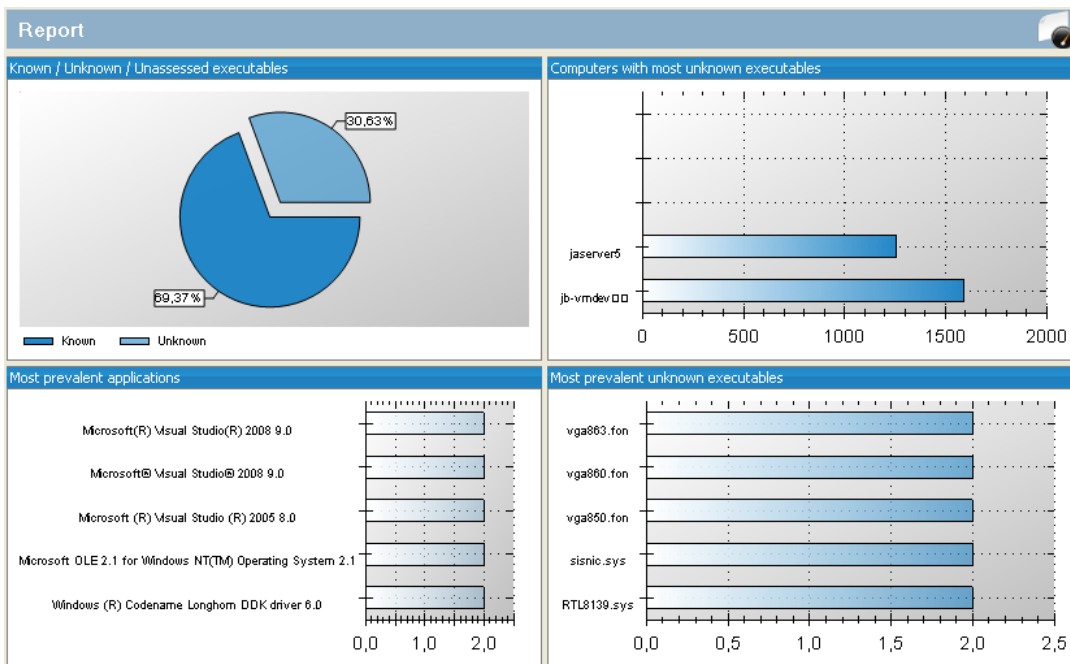


Figure 11: Report Module

**Known / Unknown / Unassessed executables**

Pie chart representing the total amount of executables, split into the ones that have a known good provenance, unknown provenance and executables that still need assessment.

**Computers with most unknown executables**

Shows the top-5 endpoints that have the most executables of unknown provenance.

**Most prevalent applications**

Shows the top-5 most prevalent applications in your environment.

**Most prevalent unknown executables**

Shows the top-5 most prevalent executable files of unknown provenance in your environment.

### PDF REPORTS

The Application Scanner tool allows the creation of PDF reports corresponding to the four graphs. To produce a PDF report, right-click on the graph of interest and select “Generate PDF Report” from the menu. The report will then be generated and shown in your default PDF reader.

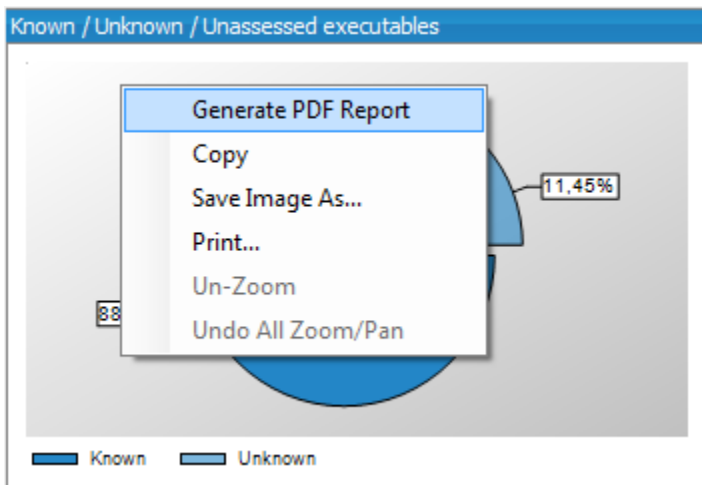
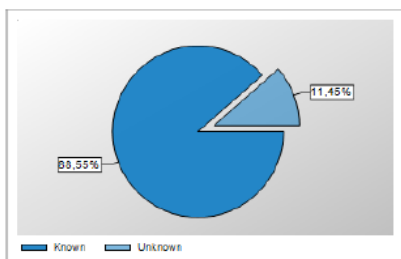


Figure 12: Generating a PDF Report

Generating a PDF report can take a few minutes depending on the number of endpoints that reside in the database. Reports will be stored in your application startup folder, in the “reports” sub-folder. The following PDF reports are available:

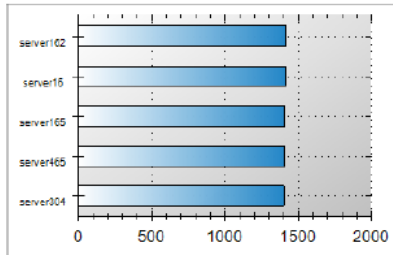
### Lumension Application Scanner 2.2 Report Known / Unknown / Unassessed Executables



Endpoint Name	Total EXEs	Known EXEs	Unknown EXEs	Unassessed EXEs	System Integrity
machine323	6.688	6.386	302	0	95%
machine425	5.794	5.491	303	0	94%
machine426	5.167	4.911	256	0	95%
machine427	7.115	6.772	343	0	95%
machine428	5.254	4.998	256	0	95%
machine429	604	569	35	0	94%
machine430	6.295	5.976	319	0	94%

Figure 13: Report 1 - Known / Unknown / Unassessed Executables

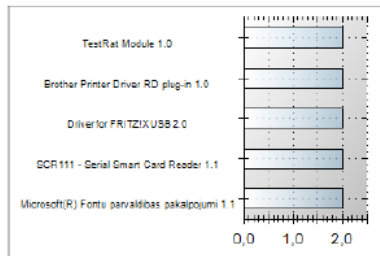
### Lumension Application Scanner 2.2 Report Endpoints With Most Unknown Executables



	Endpoint Name	Unknown EXEs
1	server162	1,419
2	server16	1,419
3	server165	1,414

Figure 14: Report 2 - Endpoints With Most Unknown Executables

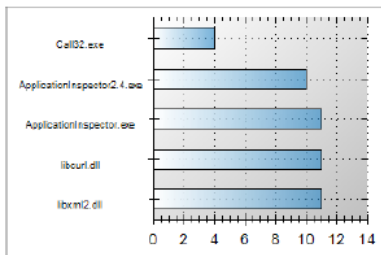
### Lumension Application Scanner 2.2 Report Most Prevalent Applications (>1)



Application Name	Version	Prevalence
Canon Render DLL	1.0	2
Canon Extraui DLL	1.0	2
Canon Inkjet Printer Driver	1.0	2
Microsoft .NET Framework	1.0	2

Figure 15: Report 3 - Most Prevalent Applications

### Lumension Application Scanner 2.2 Report Top 10 Unknown Executables



Executable Name	Prevalence	Found on Endpoints (showing 10 max)
libxml2.dll	11	server01 server02 workstation002 workstation003 workstation004 workstation005 workstation006 workstation007 workstation008 workstation009
libcurl.dll	11	server01 server02 workstation002 workstation003 workstation004 workstation005 workstation006 workstation007 workstation008 workstation009

Figure 16: Report 4 - Top 10 Unknown Executables

### HOME

The Application Scanner tool gives you full visibility over all applications and files resident on your endpoints and the level of integrity of your environment. Please contact Lumension to learn how our solutions can help you to regain control your environment.

### Free 30 Day Trial

<http://www.lumension.com/Products/Evaluation-Request.aspx>

### Personal Demo

<http://www.lumension.com/Products/Request-a-Product-Demonstration.aspx>

### Contact

<http://www.lumension.com/contact-us.aspx>

### Support

<http://www.lumension.com/Services/technical-support-services.aspx>

## Chapter 5

### File Hash Lookup Utility

#### FUNCTIONAL DESCRIPTION

The File Hash Lookup utility lets you look up relevant information on Microsoft Windows executable files using the [Lumension® Endpoint Intelligence Center](#) portal.

The portal takes advantage of the Lumension® Endpoint Integrity Cloud service to deliver the following information on windows executable files:

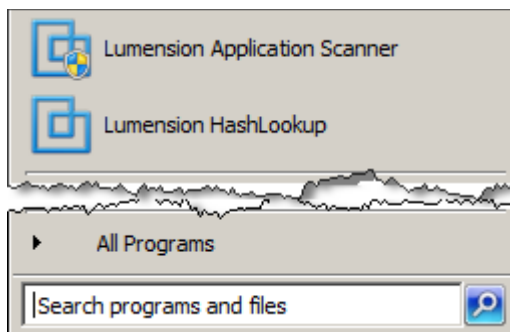
- File hash (MD5, SHA-1, SHA-256)
- Basic File Information: Manufacturer, File Name(s), File Type, Architecture, Version
- Product Information: Vendor, Product Name, Product Version, Product Type
- File Sources: Community (data collected from the Lumension® community of users), EIS Cloud Service (data collected by Lumension directly from vendors and other known, trusted sources), and NSRL (data collected from the [National Software Reference Library](#), and hosted by NIST).

#### MODES OF OPERATION

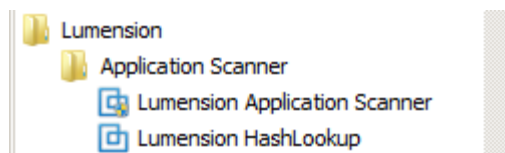
The File Hash Lookup utility can be used in two (2) different ways:

##### Standalone Execution

To launch the File Hash Lookup utility in standalone mode, select the corresponding menu item from your Start menu, or click on the File Hash Lookup utility desktop icon.

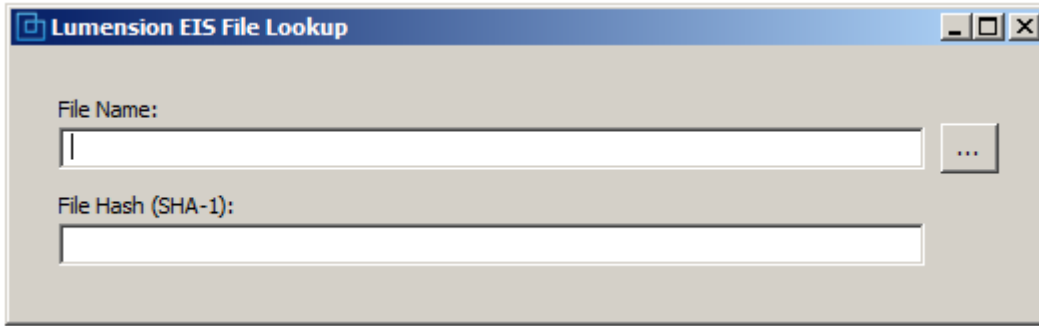



Pinned to Start Menu



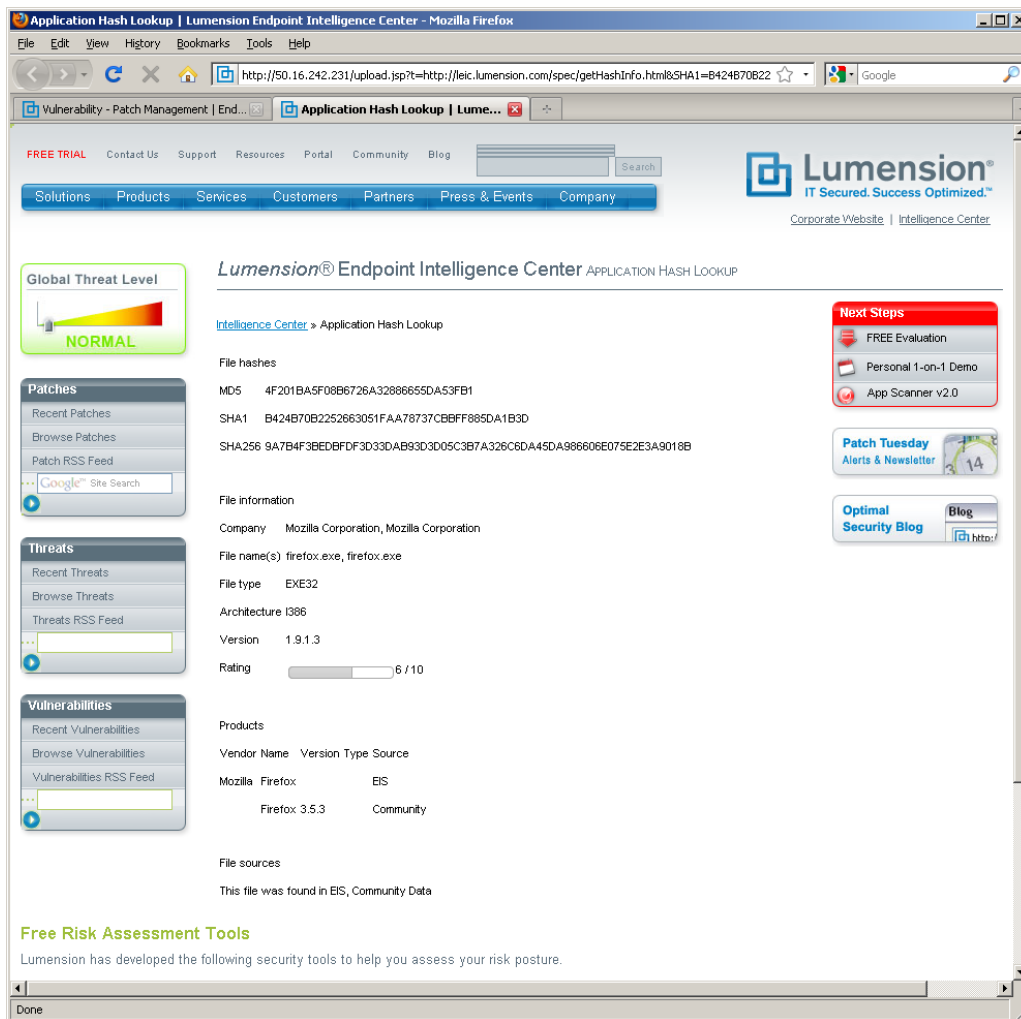
In Start Menu Structure

The main user interface lets you enter a Windows executable file name to be checked by the Lumension Endpoint Integrity Cloud service.



To select a file, click on the  icon and choose a file from the subsequent dialog. The selected file will then be hashed by the utility; a SHA-1 hash will be produced and displayed in the “File Hash” text box. Please note that not all file types are supported.

The file hash will then be sent to the EIS Cloud service and the result will be displayed in your default web browser:



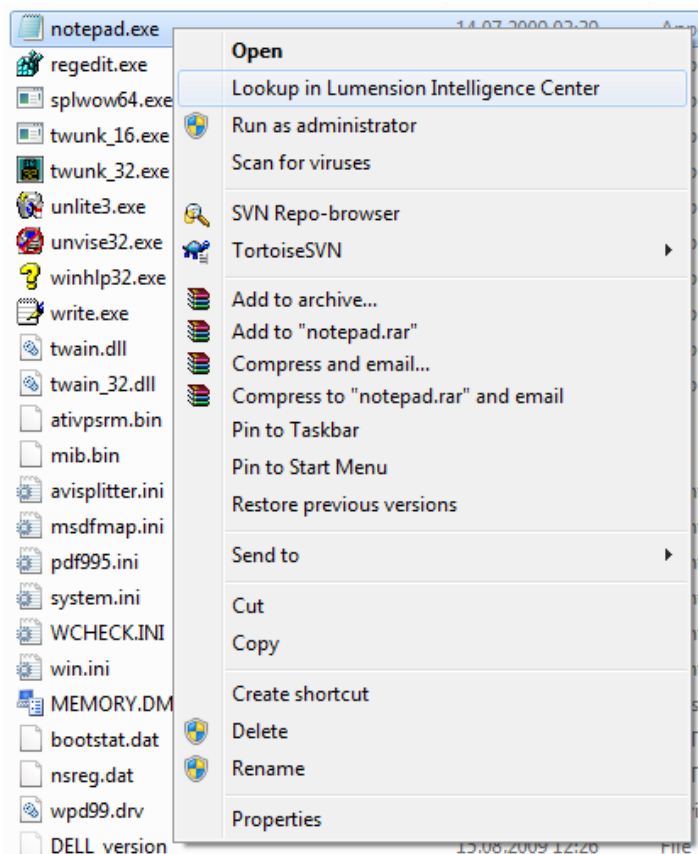
### Context Menu Execution

After the File Hash Lookup utility has been run for the first time, it will register itself as shell extension for the following file types:

- DLL
- EXE
- CPL
- COM\*
- SYS\*

\* Not all COM and SYS files are supported by this utility

An additional context menu item will appear if you right-click on one of these types of files: "Lookup in Lumension Intelligence Center".



Clicking on this context menu will launch the EIS File Lookup utility, automatically produce the SHA-1 hash of the file, and open the resulting web page in your default browser.

## Chapter 6 Troubleshooting

Problem	Cause	Action
The Discovery module reports "Could not connect" on a specific IP address.	The endpoint is down.	Start the endpoint.
	The endpoint runs an unsupported OS.	Exclude the endpoint from the scan range.
	The endpoint's firewall prevented access.	Allow WMI inbound and FTP inbound and outbound on the endpoint's firewall.
	The provided credentials are not valid.	Add a valid set of credentials in the scan targets dialog.
	The endpoint is configured for simple file sharing.	Remove simple file sharing (Open Windows Explorer > Menu "Tools" > Folder Options > View > uncheck "Simple File Sharing").
	The WMI / RPC service(s) is/are not running.	Activate the corresponding services on the endpoint.
The Discovery module reports "success" on an endpoint, but it does not show up in the Assessment module.	The endpoint is still scanning.	Check whether there is an active process named "ApplicationInspector" running on the endpoint. It can take 30 minutes or longer (depending on user activity) for the process to complete.
	The endpoint was shut down during scan.	Start the endpoint and rescan it.
The console takes 100% CPU cycles.	During the data collection phase, tens of thousands of database inserts are being processed. This will use CPU cycles and the console could become unresponsive during peaks.	Minimize the console until the data processing phase is completed.

## Chapter 7 Glossary

### LUMENSION ENDPOINT INTELLIGENCE CENTER (LEIC)

The Lumension Endpoint Intelligence Center – a service that integrates threat, exploit, vulnerability, patching and whitelisting research information into a single security feed that can be used by both Lumension customers and IT professionals at large.

### EIS CLOUD SERVICE

The Lumension Endpoint Integrity service – a web based cloud service within LEIC that provides a trust rating and allows the assessment of binary files. The service allows to retrieve meta-information on software products and the related binary files, including a product categorization and tags.

### EIS HASH LIBRARY

The EIS Cloud service binary file hash database – a database which contains hashes and meta-information to known good binary files, including file provenance. It is used by the EIS Cloud Service.

### NSRL HASH LIBRARY

The [National Software Reference Library](#) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS is a collection of digital signatures of known, traceable software applications. There are application hash values in the hash set which may be considered malicious, i.e. steganography tools and hacking scripts. There are no hash values of illicit data, i.e. child abuse images. The NSRL Hash Library is used by the EIS Cloud Service.

### COMMUNITY HASH LIBRARY

A database maintained by Lumension containing binary file hashes provided by the Lumension Application Scanner community. The library does not contain a trust rating mechanism, as the files are not provided by a trusted source; instead, it contains prevalence information for files and software products (by geography, by industry, by company size). The Community Hash Library is used by the EIS Cloud Service.

### THE LEIC PORTAL

A Web based portal (<http://leic.lumension.com>) that allows all users to browse and search the feeds provided by the EIS Cloud Service. It also allows any user to upload binary files and receive an assessment and the meta-information to those files.