



# Agent Install Guide

Lumension Endpoint Management  
and Security Suite 7.0 SP1



---

# Notices

---

## Version Information

Lumension Endpoint Management and Security Suite Patch Agent Install Guide - Lumension Endpoint Management and Security Suite Version Beta - Released: April 2010

Document Number: 02\_017\_Beta\_101201051

## Copyright Information

Lumension

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255

Phone: +1 888.725.7828

Fax: +1 480.970.6323

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

**Copyright© 1997-2010 Lumension Security, Inc.: ALL RIGHTS RESERVED.** Protected by U.S. Patent nos. 7,278,158, 6,990,660, and 7,487,495 and European Patent nos. EP1745343 and EP1743230; other patents pending. 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® Security, Lumension®, 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.

RSA Secured® is a registered trademark of RSA Security Inc.

Apache is a trademark of the Apache Software Foundation. In addition, any other companies' names and products mentioned in this document may be either registered trademarks or trademarks of their respective owners.



## 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

<b>Preface: About This Document.....</b>	<b>7</b>
Typographical Conventions.....	7
Contacting Lumension.....	7
<b>Chapter 1: Preparing for Agent Installation.....</b>	<b>11</b>
Installation Methods.....	11
Supported Agent Operating Systems.....	12
Supported Languages.....	14
Requirements.....	15
Agent for Windows.....	15
Agent for Linux, UNIX, and Mac.....	16
<b>Chapter 2: Installing Agents.....</b>	<b>19</b>
Installing Agents on Endpoints.....	19
Downloading the Installer.....	19
Installing the Single Agent for Windows 2000.....	21
Installing the Single Agent for Windows XP and Later.....	27
Installing the Single Agent for Mac.....	32
Installing the Command Line Agent for Linux, UNIX, and Mac.....	38
Installing Agents by Agent Management Job.....	39
Upgrading Agents.....	51
Upgrading Agents Locally.....	52
Uninstalling Agents.....	53
Uninstalling Agents by Agent Management Job.....	53
Uninstalling the Agent for Windows 2000 Locally.....	65
Uninstalling the Agent for XP or Later Locally.....	65
Uninstalling the Agent for Linux Locally.....	66
Uninstalling the Agent for Solaris Locally.....	66
Uninstalling the Agent for AIX Locally.....	67
Uninstalling the Agent for HP-UX Locally.....	67
Uninstalling the Command Line Agent for Mac Locally.....	67
<b>Chapter 3: Automating the Agent Installation.....</b>	<b>69</b>
Automating the Windows MSI Installer.....	69



Creating a Network Share.....	70
Modifying the PatchAgent.msi File.....	73
Modifying the LMAgent.msi Installer.....	77
Creating an Organizational Unit.....	82
Performing a Silent Install on Windows.....	86
Command Line Descriptions for Windows 2000.....	87
Command Line Descriptions for Windows XP or Later.....	87
Performing a Silent Install on Linux/UNIX/Mac.....	88
Command Line Descriptions.....	88

**Configuring the Server and Endpoints for Agent Management Jobs.....91**

Configuring the Scanning System.....	91
Configuring Pre-Windows Vista Endpoint for Discovery.....	91
Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista).....	94
Configuring Post-Windows Vista Endpoints for Discovery.....	99
Configuring Endpoints for Agent Management Jobs (Post-Windows Vista).....	103
Resolving Endpoint UAC Issues.....	107
Troubleshooting Agent Management Jobs.....	107
Disabling Password Changes.....	108



---

# Preface

---

## About This Document

---

This Agent Install Guide is a resource written for all users of Lumension Endpoint Management and Security Suite 7.0 SP1. This document defines the concepts and procedures for installing, configuring, implementing, and using Lumension Endpoint Management and Security Suite 7.0 SP1.

**Tip:** Lumension documentation is updated on a regular basis. To acquire the latest version of this or any other published document, please refer to the *Lumension Customer Portal* (<http://portal.lumension.com/>).

---

## Typographical Conventions

---

The following conventions are used throughout this documentation to help you identify various information types.

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

## 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
---	---



<p><b>United Kingdom Office</b></p> <p>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 E-mail: <a href="mailto:patchlink.emea@lumension.com">patchlink.emea@lumension.com</a></p>	<p><b>Lumension Security Ireland Limited</b></p> <p>Galway Technology Centre Unit Number 20 Mervue Industrial Estate County of Galway Ireland Phone: +353 91 730858</p>
<p><b>Germany Office</b></p> <p>Wazmannstrasse 22 82140 Olching (Munich) Germany Phone: +49 (0) 8142 400800 Fax: +49 (0) 8142 400530</p>	<p><b>Spain Office</b></p> <p>Paseo de la Castellana, 141 pt.20 ed. Cuzco IV 28046 Madrid Spain Phone: +34 91 749 80 40 Fax: +34 91 570 71 99 E-mail: <a href="mailto:patchlink.emea@lumension.com">patchlink.emea@lumension.com</a></p>
<p><b>US Federal Solutions Group</b></p> <p>Virginia Office - Federal Solutions Group 13755 Sunrise Valley Drive, Suite 203 Herndon, VA 20171 United States of America Phone: +1 888 725 7828 (option 1) Fax: +1 703 793 7007 E-mail: <a href="mailto:patchlink.federalsales@lumension.com">patchlink.federalsales@lumension.com</a></p>	<p><b>France Office</b></p> <p>Phone: +33 611 821 535</p>
<p><b>Singapore Office</b></p> <p>9 Raffles Place Level 58, Republic Plaza Singapore 048619 Phone: +65 6823 1533 Fax: +65 6823 1377 E-mail: <a href="mailto:patchlink.apac@lumension.com">patchlink.apac@lumension.com</a></p>	<p><b>Australia Office</b></p> <p>Level 20, Tower II, Darling Park 201 Sussex Street Sydney, NSW Australia 2000 Phone: +61 2 9006 1654 Fax: +61 2 9006 1010 E-mail: <a href="mailto:patchlink.apac@lumension.com">patchlink.apac@lumension.com</a></p>



<p><b>North America Sales</b></p> <p>Phone: +1 480 970 1025 (option 1)  E-mail: <a href="mailto:sales@lumension.com">sales@lumension.com</a></p>	<p><b>International Sales</b></p> <p>US Phone: +1 480 970 1025 (option 1)  UK Phone: + 44 (0) 1908 357 897  Luxembourg Phone: + 352 265 364 11  Singapore Phone: + 65 6725 6415  E-mail: <a href="mailto:sales@lumension.com">sales@lumension.com</a> or  <a href="mailto:patchlink.apac@lumension.com">patchlink.apac@lumension.com</a> (APAC) or  <a href="mailto:patchlink.emea@lumension.com">patchlink.emea@lumension.com</a> (EMEA)</p>
<p><b>Lumension Vulnerability Management Technical Support</b></p> <p>Phone: +1 888 725 7828 (Opt 2) (US Toll Free)  +44 800 012 1869 (UK Toll Free)  +353 9142 2999 (EMEA)  +61 (02) 8223 9810 (Australia)  +852 3071 4690 (Hong Kong)  +65 6622 1078 (Singapore)  E-mail: <a href="mailto:patchlink.support@lumension.com">patchlink.support@lumension.com</a> (US)  <a href="mailto:patchlink.apac.support@lumension.com">patchlink.apac.support@lumension.com</a> (APAC)  <a href="mailto:patchlink.emea.support@lumension.com">patchlink.emea.support@lumension.com</a> (EMEA)</p>	<p><b>Lumension Endpoint Security Technical Support</b></p> <p>Phone: +1 877 713 8600 (US Toll Free)  +44 800 012 1869 (UK Toll Free)  +353 9142 2999 (EMEA)  E-mail: <a href="mailto:endpoint.support@lumension.com">endpoint.support@lumension.com</a></p>
<p><b>Note:</b> For additional contact information, please visit the <a href="http://www.lumension.com/contactus.jsp">Contact Lumension</a> page at <a href="http://www.lumension.com/contactus.jsp">http://www.lumension.com/contactus.jsp</a>.</p>	





---

# Chapter

# 1

---

## Preparing for Agent Installation

---

### In this chapter:

- Installation Methods
- Supported Agent Operating Systems
- Supported Languages
- Requirements

Having successfully installed your Lumension Endpoint Management and Security Suite server, you can now proceed to the installation of your agents. Following installation the agent is monitored and maintained by the Lumension Endpoint Management and Security Suite server requiring no additional maintenance.

## Installation Methods

---

Agents can be deployed using any one (or combination) of the following methods:

Table 1: Installation Options

Installation Type	Agent Type	Descriptions
Single agent installer for Windows 2000	Patch 6.4 Agent	Allows you to run the installer, entering the information as prompted. You can also modify the Microsoft Software Installer (MSI) file, using an MSI editor, to include your organization's configuration. The .msi file can be delivered by using a login script, Active Directory Group Policy Object (GPO), or other remote software installation method.
Single agent installer for Windows XP and later	Lumension EMSS 7.0 Agent	Allows you to run the Lumension EMSS (Endpoint Management and Security Suite) agent installer, entering the information as prompted. The Lumension EMSS agent then automatically installs the patch component. You can also modify the Microsoft Software Installer (MSI) file, using an MSI editor, to include your organization's configuration. The .msi file can be delivered by using a login script, Active Directory Group Policy Object (GPO), or other remote software installation method.



Installation Type	Agent Type	Descriptions
Single agent installer for Mac	Lumension EMSS 7.0 Agent	Allows you to run the installer, entering information as prompted.
Single agent installer for Linux/Unix/Mac	Lumension EMSS 7.0 Agent	Allows you to run the installer, entering the information as prompted. You can also perform a silent installation using <code>rsh</code> or <code>SSH</code> .

## Supported Agent Operating Systems

There are multiple versions of the Lumension Endpoint Management and Security Suite (Lumension EMSS) agent to accommodate multiple platforms. In some cases, more than one agent version can be installed on a particular operating system.

The following table lists the supported platforms on which the agent is supported.

Table 2: Supported Operating Systems

Operating System	Version	Edition	Data Width	Proc. Family	Software Prerequisites	Agent Version
Microsoft Windows 2000 SP4	5.0	All <sup>(1)</sup>	32 bit	Intel	Microsoft Windows Installer 2.0+	Patch 6.4 Agent
Microsoft Windows XP SP2+	5.1	Professional <sup>(2)</sup>	32/64 bit	Intel	Microsoft Windows Installer 2.0+	Lumension EMSS 7.0 Agent
Microsoft Windows 2003 SP1+	5.2	Web Standard Enterprise R2	32/64 bit	Intel	Microsoft Windows Installer 2.0+	Lumension EMSS 7.0 Agent
Microsoft Windows Vista	6.0	Business Enterprise Ultimate	32/64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent
Microsoft Windows Server 2008	6.0	Web <sup>(3)</sup> Standard Enterprise	32/64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent



Operating System	Version	Edition	Data Width	Proc. Family	Software Prerequisites	Agent Version
Microsoft Windows 7	7.0	Professional Enterprise Ultimate	32/64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent
Microsoft Windows Server 2008 R2	7.0	Standard Enterprise Web	64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent
Apple Mac OS X	10.3 10.4 10.5 10.6	All	32/64 bit	Intel / PowerPC	Sun Java JRE 1.5.0+	Patch 7.0 Agent
HP-UX	11.11 11.23 11.31	All	64 bit	PA-RISC	Sun Java JRE 1.5.0+	Patch 7.0 Agent
IBM AIX	5.2 5.3 6.1	All	32/64 bit	Power / PowerPC	Sun Java JRE 1.5.0+	Patch 7.0 Agent
Novell SUSE Linux	9 10 11	Enterprise	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
Red Hat Linux	3.0 4.0 5.0	Enterprise AS ES WS	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
Sun Solaris	8 9 10	All	32/64 bit	SPARC / Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent



Operating System	Version	Edition	Data Width	Proc. Family	Software Prerequisites	Agent Version
Oracle Linux	4 5	All	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
CentOS Linux	4 5	All	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
<p>(1) The Datacenter editions of this OS family are not supported.</p> <p>(2) Home, Media Center, and Tablet PC editions are not supported.</p> <p>(3) The Datacenter and Core Editions of this OS family are not supported.</p>						

## Supported Languages

The agent is supported in the following languages:

- en-AU: English (Australia)
- en-BZ: English (Belize)
- en-CA: English (Canada)
- en-JM: English (Jamaica)
- en-NZ: English (New Zealand)
- en-ZA: English (South Africa)
- en-GB: English (United Kingdom)
- en-US: English (United States)
- es-ES: Spanish (Spain)
- fi-FI: Finnish (Finland)
- fr-FR: French (France)
- de-DE: German (Germany)
- it-IT: Italian (Italy)
- ja-JP: Japanese (Japan)
- ko-KR: Korean (Korea)
- nl-NL: Dutch (Netherlands)
- pt-BE: Portuguese (Brazil)
- zh-CN: Chinese (Simplified)
- zh-CHS: Chinese (Simplified)
- zh-TW: Chinese (Traditional)
- zh-CHT: Chinese (Traditional)



## Requirements

The following section lists the hardware and software requirements for the agent.

**Note:** You must disable any virus-scanning software prior to the installation of the Lumension Agent for Windows. Failure to do so may result in an unsuccessful agent installation.

### Agent for Windows

The following minimum requirements must be met in order to install the agent on endpoints running the Microsoft Windows operating system.

The install (and uninstall) must be done by an Administrator or Administrator equivalent.

- 500 MHz processor or higher.
- 256 MB RAM.
- 20 MB of free disk space for agent installation.
- 25 MB of free disk space once the agent is installed
- A single 10 Mbps network connection (with access to the Lumension Endpoint Management and Security Suite server).
- Sufficient free disk space to download and install patches (varies dependent upon size of patch).
- Windows Installer 2.0 or higher.
- Microsoft Internet Explorer 5.01 or higher (Internet Explorer 5.5 or higher if using SSL).
- Network connectivity to your Lumension Endpoint Management and Security Suite server (6.5 or higher).

**Note:** Windows 2000 computers require Service Pack 1.

The following table lists the supported platforms on which the agent is supported.

Table 3: Supported Operating Systems

Operating System	Version	Edition	Data Width	Proc. Family	Software Prerequisites	Agent Version
Microsoft Windows 2000 SP4	5.0	All <sup>(1)</sup>	32 bit	Intel	Microsoft Windows Installer 2.0+	Patch 6.4 Agent
Microsoft Windows XP SP2+	5.1	Professional <sup>(2)</sup>	32/64 bit	Intel	Microsoft Windows Installer 2.0+	Lumension EMSS 7.0 Agent
Microsoft Windows 2003 SP1+	5.2	Web Standard Enterprise R2	32/64 bit	Intel	Microsoft Windows Installer 2.0+	Lumension EMSS 7.0 Agent



Operating System	Version	Edition	Data Width	Proc. Family	Software Prerequisites	Agent Version
Microsoft Windows Vista	6.0	Business Enterprise Ultimate	32/64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent
Microsoft Windows Server 2008	6.0	Web <sup>(3)</sup> Standard Enterprise	32/64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent
Microsoft Windows 7	7	Professional Enterprise Ultimate	32/64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent
Microsoft Windows 2008 R2	7	Standard Enterprise Web	64 bit	Intel	Microsoft .NET Framework 3.0+	Lumension EMSS 7.0 Agent
<p>(1) The Datacenter editions of this OS family are not supported.</p> <p>(2) Home, Media Center, and Tablet PC editions are not supported.</p> <p>(3) The Datacenter and Core Editions of this OS family are not supported.</p>						

## Agent for Linux, UNIX, and Mac

The following minimum requirements must be met in order to install the agent on endpoints running the Linux, UNIX, or Mac operating systems.

The install (and uninstall) must be done by the root user (superuser).

- Presence of `/tmp` directory (`/var/tmp` directory on Solaris) for temporary file storage and processing.
- 105 MB of free disk space for the agent installation. It is recommended that there be 100 MB of free disk space in `/temp` (`/var/tmp` for Solaris) and a separate 50 MB of free disk space in the agent installation directory.
- 500 MHz or greater processor.
- 256 MB RAM.
- 10 Mbps network connection (with access to the Lumension Endpoint Management and Security Suite server).
- Sufficient free disk space to download and install patches.
- Network connectivity to your Lumension Endpoint Management and Security Suite server.

The following table lists the supported platforms on which the agent is supported.



Table 4: Supported Operating Systems

Operating System	Version	Edition	Data Width	Proc. Family	Software Prerequisites	Agent Version
Apple Mac OS X	10.3 10.4 10.5 10.6	All	32/64 bit	Intel / PowerPC	Sun Java JRE 1.5.0+	Lumension EMSS 7.0 Agent
HP-UX	11.11 11.23 11.31	All	64 bit	PA-RISC	Sun Java JRE 1.5.0+	Patch 7.0 Agent
IBM AIX	5.2 5.3 6.1	All	32/64 bit	Power / PowerPC	Sun Java JRE 1.5.0+	Patch 7.0 Agent
Novell SUSE Linux	9 10	Enterprise	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
Red Hat Linux	3.0 4.0 5.0	Enterprise AS ES WS	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
Sun Solaris	8 9 10	All	32/64 bit	SPARC / Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
Oracle Linux	4 5	All	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent
CentOS Linux	4 5	All	32/64 bit	Intel	Sun Java JRE 1.5.0+	Patch 7.0 Agent





---

# Chapter

# 2

---

## Installing Agents

---

### In this chapter:

- Installing Agents on Endpoints
- Upgrading Agents
- Uninstalling Agents

Installing agents on your endpoints allows you to manage the endpoint using Lumension Endpoint Management and Security Suite.

The following section includes instructions for installing the agent. Installation instructions are specific to operating system type and version.

### Installing Agents on Endpoints

---

Running the agent installer on an endpoint connects the endpoint to the Lumension Endpoint Management and Security Suite server.

You can install an agent on an endpoint in either of the following ways:

- Download the appropriate installer to the endpoint that you want to manage, then run the installer locally on the endpoint.
- Create an agent management job to install the agent that targets the endpoint (Windows operating systems only). When the job executes, an agent is installed on the endpoint.

---

**Note:** You should not perform the procedures listed in this section on the Lumension Endpoint Management and Security Suite server. The agent on the Lumension Endpoint Management and Security Suite server is installed and configured during the server installation process.

---

### Downloading the Installer

The standard agent install requires logging in to the Lumension Endpoint Management and Security Suite administration console from the target computer then downloading the installer to that computer.

For some operating systems, you have the option of downloading and installing the command line version of the agent installer or the graphical user interface version of the agent installer. The command line agent is installed and accessed after installation using the command line. The graphical user interface version of the agent is installed using an installation wizard and accessed after installation via the **Control Panel** (Windows) or **System Preferences** (Mac).

1. Log in to the target computer as the local administrator (or a member of the Local Administrators group).
2. Launch your Web browser.



3. Log in to your Lumension Endpoint Management and Security Suite.

**Step Result:** The Lumension Endpoint Management and Security Suite *Home* page opens.

4. Select **Tools** > **Download Agent Installer**.

**Step Result:** The *Download Agent Installers* dialog opens.

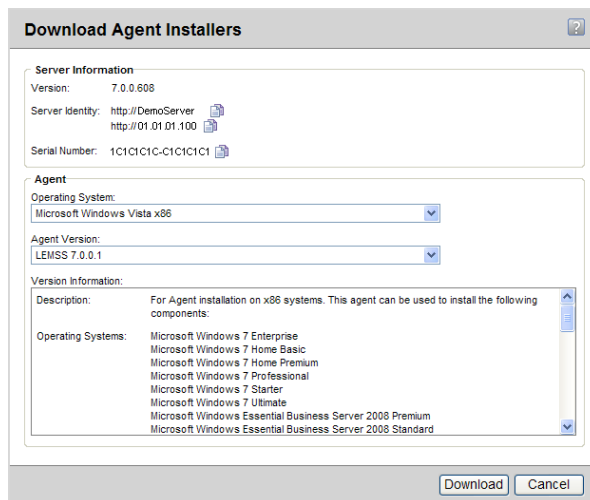


Figure 1: Download Agent Installers Dialog

---

**Note:** You can click **Cancel** at any time to close this page and cancel the download procedure.

---

5. Select the endpoint's operating system from the **Operating System** drop-down list.
6. Select the version of the agent that you want to install from the **Agent Version** drop-down list.
7. Click **Download** to download the installer to the endpoint.

**Step Result:** The installer downloads to the location you specify on your computer.

---

**Tip:** This dialog stays open during the installer download so that you can copy the server URL and the serial number for use during the agent installation.

---

8. In the *Download Agent Installers* page, click **Close**.

**Step Result:** The *Download Agent Installers* page closes.



## Installing the Single Agent for Windows 2000

### Prerequisites:

Verify that your computer meets the minimum requirements for agent installation. See *Agent for Windows* on page 15 for more information.

Download the appropriate installer for your operating system. See *Downloading the Installer* on page 19 for more information.

**Caution:** The following steps apply to the Lumension Windows 2000 Patch Agent installer. To install the agent for Windows XP or later, refer to *Installing the Single Agent for Windows XP and Later* on page 27.

1. From the downloaded location, open the PatchAgent.msi installer file to extract the Lumension Patch Agent for Windows InstallShield Wizard.

**Step Result:** The *Welcome* dialog opens.

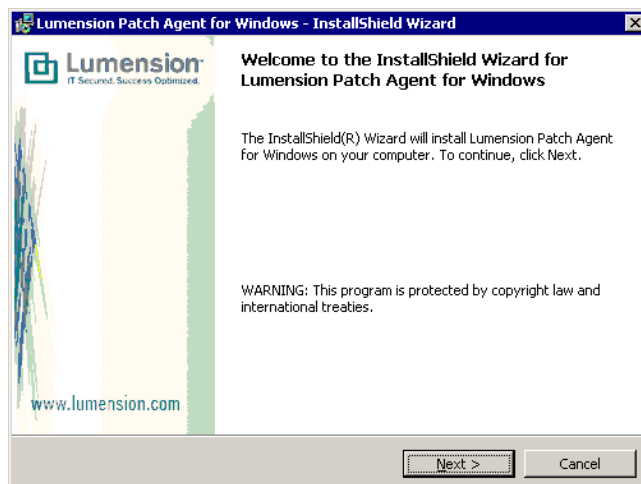


Figure 2: Welcome Dialog



## 2. Click **Next**.

**Step Result:** The *License Agreement* dialog opens.

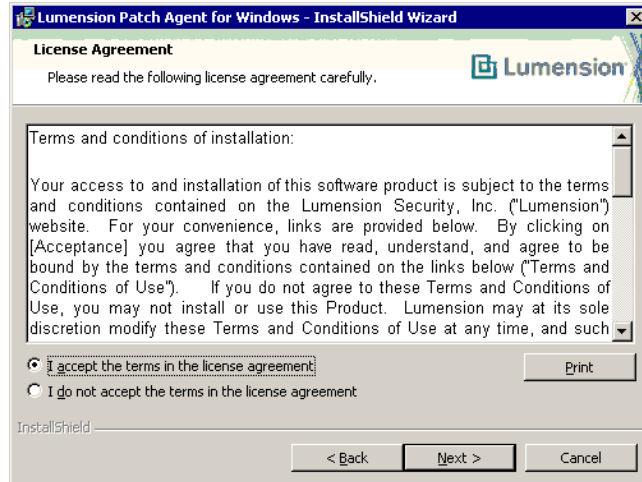


Figure 3: License Agreement Dialog

## 3. If you agree to the license terms select the **I accept the terms in the license agreement** option and click **Next**.

**Step Result:** The *Destination Folder* dialog opens.

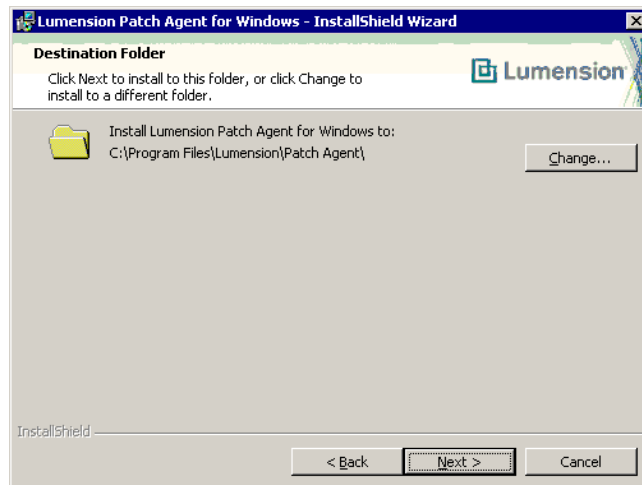


Figure 4: Destination Folder Dialog



4. To change the location of the agent:

a) Click **Change**.

**Step Result:** The *Change Current Destination Folder* dialog opens.

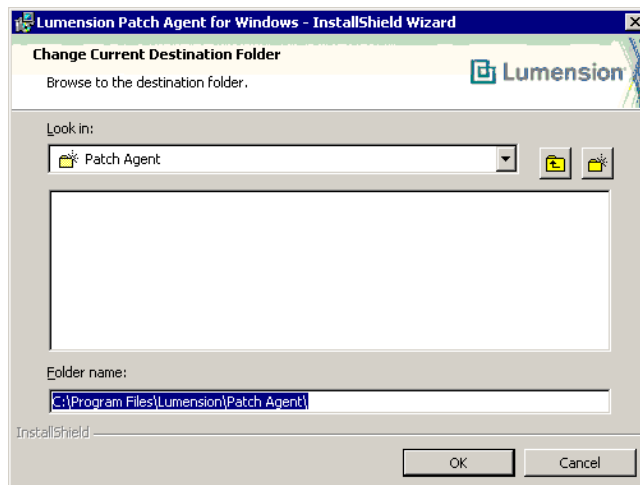


Figure 5: Change Current Destination Folder Dialog

b) Change the installation to the location you want.

c) Click **OK**.

**Step Result:** The *Change Current Destination Folder* dialog closes and the *Destination Folder* dialog reflects the new location.



5. Click **Next**.

**Step Result:** The *Agent Registration* dialog opens.

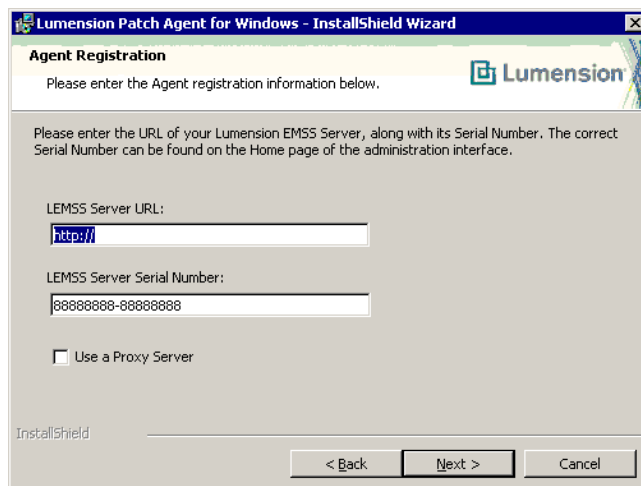


Figure 6: Agent Registration Dialog

6. Type the appropriate IP address or URL in the **LEMSS Server URL** field including the protocol (http://serverAddress or https://ServerAddress for a secure server).
7. Type your serial number in the field. Use the same serial number that was used for the installation of your Lumension Endpoint Management and Security Suite server, otherwise the agent will be unable to communicate with the server.

---

**Tip:** The Lumension Endpoint Management and Security Suite serial number is available on the Lumension Endpoint Management and Security Suite *Home* page.

---



8. If your LAN uses a proxy server:

a) Select **Use a Proxy Server**.

**Step Result:** The *Proxy Information* dialog opens.

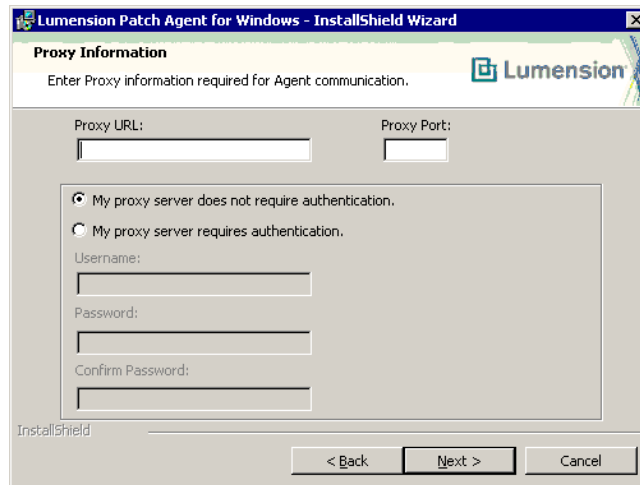


Figure 7: Proxy Information Dialog

- b) In the **Proxy URL** field, enter the URL of your proxy server.
- c) In the **Proxy Port** field, type the proxy port number (if required).
- d) If you are using an authenticated proxy:

1. Select the **My proxy server requires authorization** option.
2. In the **Username** field, type the user name.
3. In the **Password** field, type a new password for the proxy.
4. In the **Confirm Password** field, type the proxy password again.

---

**Note:** In many LAN environments, although a proxy is used for Internet access, a proxy bypass is used to for all access within the corporate network. Therefore, only enter proxy information if your agents will be required to use a proxy to access your Lumension Endpoint Management and Security Suite server.

---



**9. Click Next.**

**Step Result:** The *Ready to Install the Program* dialog opens.

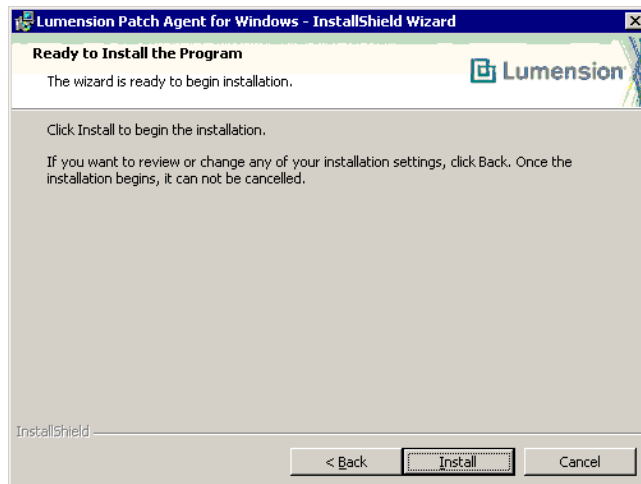


Figure 8: Ready to Install the Program Dialog

**10. Click Install to install the agent.**

**Step Result:** The agent is installed and the *Installation Complete* dialog displays.

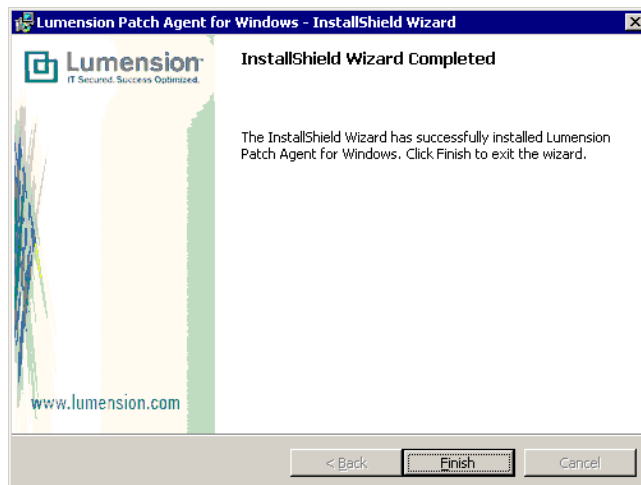


Figure 9: Installation Complete Dialog

**11. Click Finish to exit the wizard.**

**Result:** The agent is installed.



## Installing the Single Agent for Windows XP and Later

### Prerequisites:

Verify that your computer meets the minimum requirements for agent installation. See *Agent for Windows* on page 15 for more information.

Download the appropriate installer for your operating system. See *Downloading the Installer* on page 19 for more information.

The following steps apply to both the single agent for Windows MSI Installer and the single agent for Windows x64 MSI Installer.

**Note:** If you downloaded the 64-bit installer, x64 will be appended to the file name for the installer.

1. From the downloaded location, open the `LMAgent.msi` installer file to extract the agent for Windows Installation Wizard.

**Step Result:** The *Welcome* dialog opens.

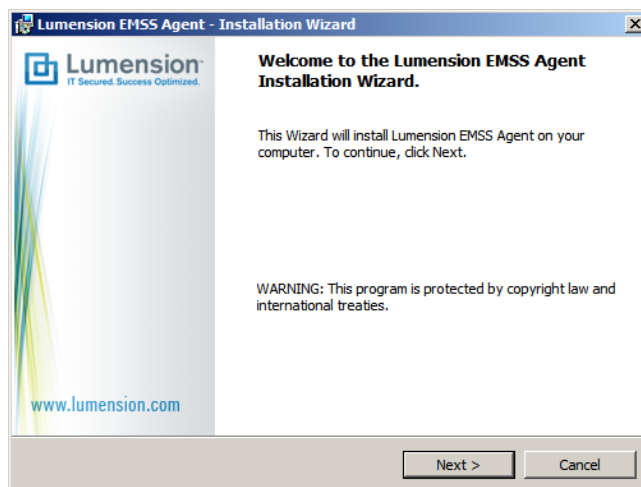


Figure 10: Welcome Dialog



2. Click **Next**.

**Step Result:** The *License Agreement* dialog opens.

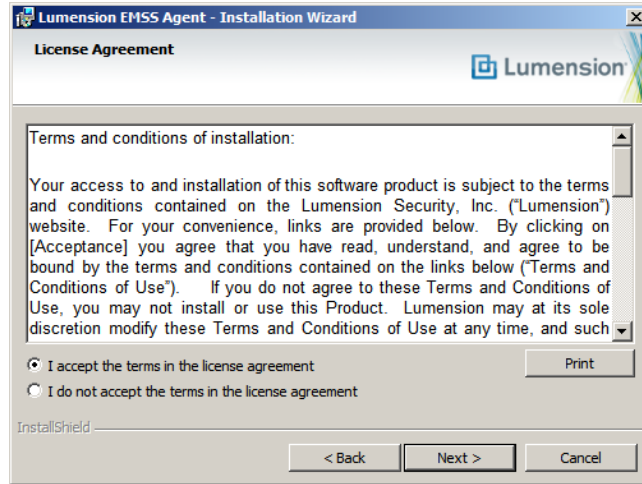


Figure 11: License Agreement Dialog

3. If you agree to the license terms select the **I accept the terms in the license agreement** option and click **Next**.

**Step Result:** The *Destination Folder* dialog opens.

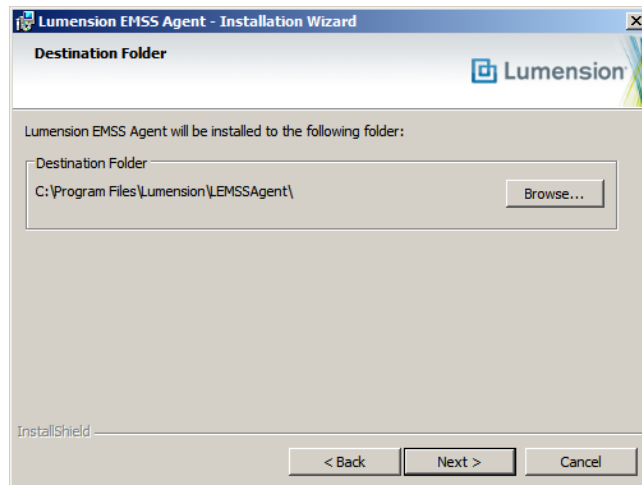


Figure 12: Destination Folder Dialog

4. To change the location of the agent:

a) Click **Change**.

**Step Result:** The *Change Current Destination Folder* dialog opens.

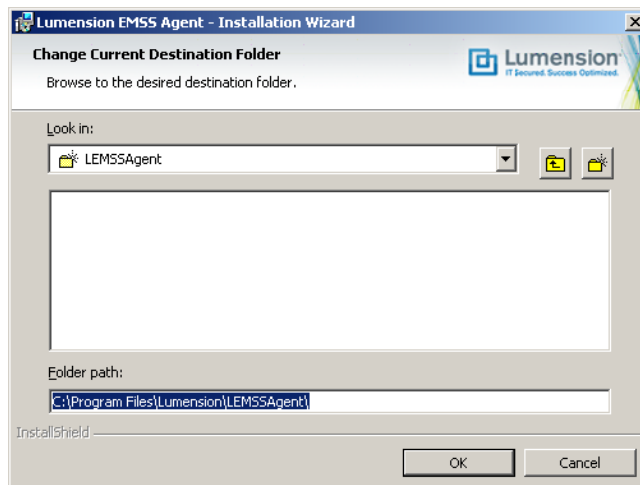


Figure 13: Change Current Destination Folder Dialog

b) Change the installation to the location you want.

c) Click **OK**.

**Step Result:** The *Change Current Destination Folder* dialog closes and the *Destination Folder* dialog reflects the new location.



5. Click **Next**.

**Step Result:** The *Lumension EMSS Server Information* dialog opens.

Figure 14: *Lumension EMSS Server Information* Dialog

6. Type the appropriate IP address or URL in the **Server identity** field including the protocol (http://serverAddress or https://ServerAddress for a secure server).
7. If your LAN uses a proxy server:
  - a) Select **Use a Proxy Server**.

**Step Result:** The *Proxy Information* dialog opens.

Figure 15: Proxy Information Dialog

- b) In the **Proxy URL** field, type the proxy URL.



- c) In the **Port number** field, type the proxy port number (if required).
- d) If you are using an authenticated proxy:
  1. Select the **Authentication is required** check box.
  2. In the **Username** field, type the user name.
  3. In the **Password** field, type a new password for the proxy.
  4. In the **Confirm Password** field, type the proxy password again.

---

**Note:** In many LAN environments, although a proxy is used for Internet access, a proxy bypass is used to for all access within the corporate network. Therefore, only enter proxy information if your agents will be required to use a proxy to access your Lumension Endpoint Management and Security Suite server.

---

8. Click **Next**.

**Step Result:** The *Installation Ready* dialog opens.

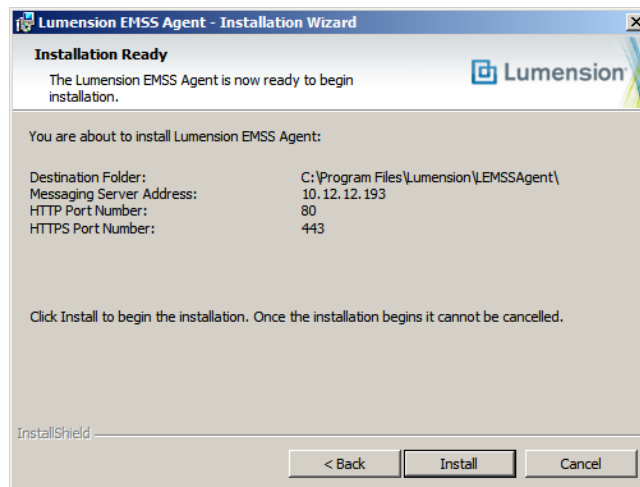


Figure 16: Installation Ready Dialog



9. Click **Install** to install the agent.

**Step Result:** The agent is installed and the *Installation Complete* dialog displays.

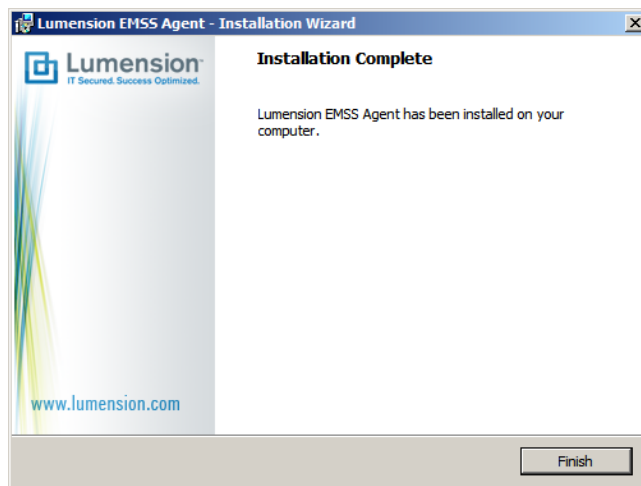


Figure 17: Installation Complete Dialog

10. Click **Finish** to exit the wizard.

**Result:** The agent is installed. The agent's patch component is downloaded automatically to the agent.

## Installing the Single Agent for Mac

Complete the following procedure to install an agent on the Mac.

---

### Prerequisites:

Verify that your computer meets the minimum requirements for agent installation. See [Agent for Linux, UNIX, and Mac](#) on page 16 for more information.

Download the appropriate installer for your operating system. See [Downloading the Installer](#) on page 19 for more information.

---

1. Verify that your computer meets the minimum requirements for agent installation.
2. From the downloaded location, select the `updateagentformac.dmg` to extract the *Patch Agent for Mac Installer*.
3. Open the installer.



4. Enter your system password.

**Step Result:** The *Introduction* dialog displays.

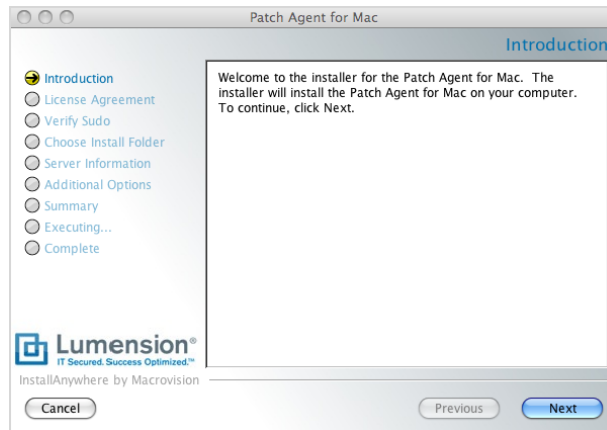


Figure 18: Introduction Dialog

5. Click **Next**.

**Step Result:** The *License Agreement* dialog displays.

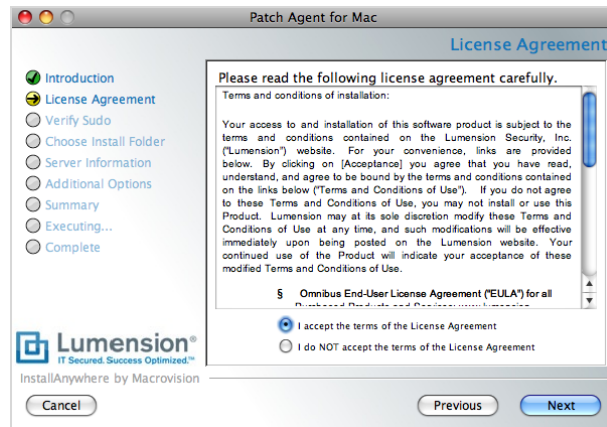


Figure 19: License Agreement Dialog



- If you agree to the license terms select the **I Accept the terms of the License Agreement** option and click **Next**.

**Step Result:** The *Verify Sudo Password* dialog opens.

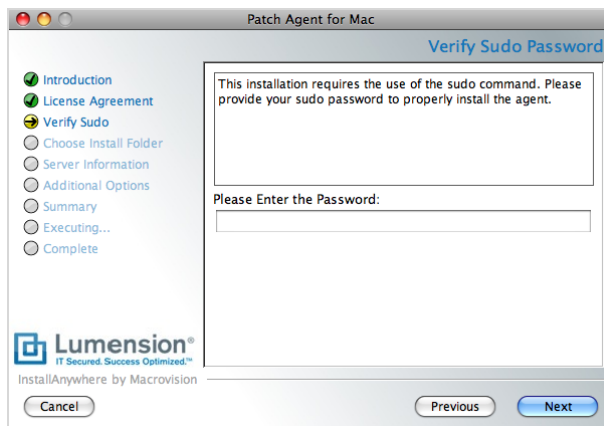


Figure 20: Verify Sudo Password Dialog

- Enter your system password in the **Please Enter the Password** field. This is the same password that you entered in step previously.
- Click **Next**.

**Step Result:** The *Choose Install Folder* dialog displays.

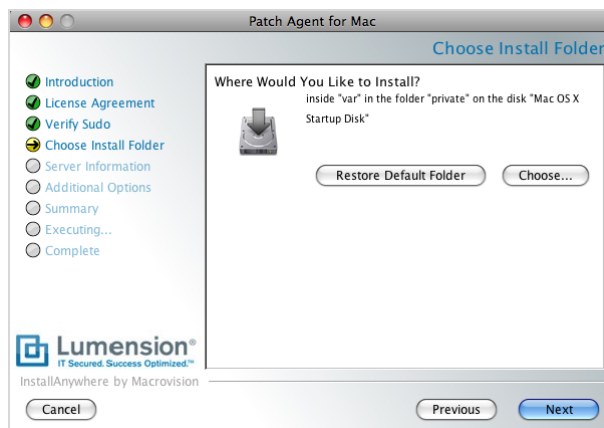


Figure 21: Choose Install Folder Dialog



9. To change the location of the agent:

a) Click **Choose**.

**Step Result:** The Finder window opens.

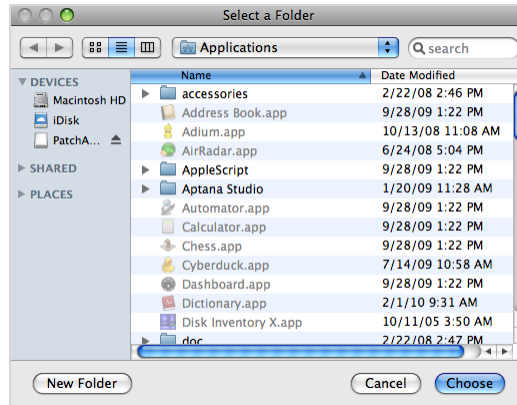


Figure 22: Finder window

b) Change the installation to the location you need.

c) Select **Open**.

d) Optionally, you can click **Restore Default Folder** to restore the default installation location.

10. Select **Next**.

**Step Result:** The **Server Information** dialog displays.

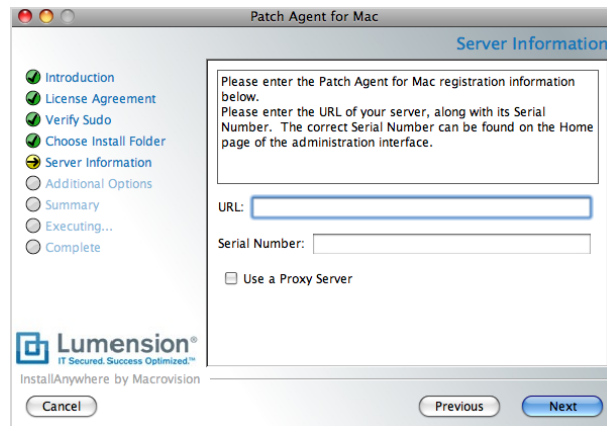


Figure 23: The Server Information Dialog

11. Type the appropriate URL in the **URL** field including the protocol (http://serverAddress or https://serverAddress for a secure server).



12. Type your serial number in the **Serial Number** field. Use the same serial number that was used for the installation of your Lumension Endpoint Management and Security Suite otherwise the agent will be unable to communicate with the server.

---

**Tip:** The Lumension Endpoint Management and Security Suite serial number is available on the Lumension Endpoint Management and Security Suite *Home* page.

---

13. If your LAN uses a proxy server:
- Select the **Use a Proxy Server** check box.
  - Click **Next**.

**Step Result:** The *Proxy Configuration* dialog displays.

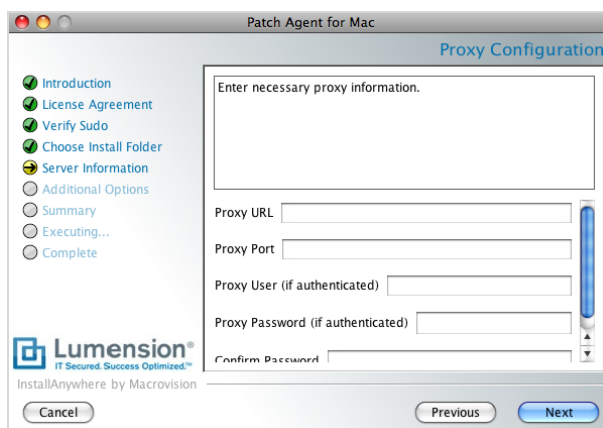


Figure 24: Proxy Configuration Dialog

- In the **Proxy URL** field, type the proxy URL.
- In the **Proxy Port** field, type the proxy port (if required).
- If you are using an authenticated proxy:
  - Enter the proxy server user name in the **Proxy User (if authenticated)** field.
  - Enter the proxy server password in the **Proxy Password (if authenticated)** field.
  - Enter the proxy server password a second time in the **Confirm Password** field.

---

**Note:** In many LAN environments, although a proxy is used for Internet access, a proxy bypass is used for all access within the corporate network. Therefore, only enter proxy information if your agents will be required to use a proxy to access your Lumension Endpoint Management and Security Suite.

---



**14. Click Next.**

**Step Result:** The *Additional Options* dialog displays.

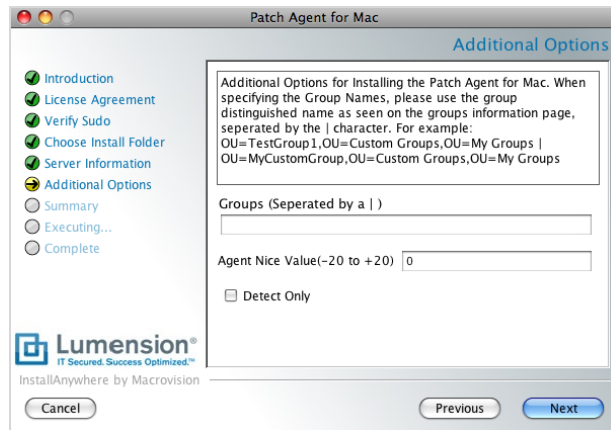


Figure 25: Additional Options Dialog

**15.** To optionally add the agent to specific device groups, enter these names of the groups in the **Groups** field. Values should be separated by a (|) symbol.

**16.** To optionally set the operating system's prioritization value for the agent, enter a value in the **Agent Nice Value** field. A value of -20 in this field gives the agent the highest priority and 20 is the lowest priority

**17.** To optionally configure the agent so that it's detectable but cannot have packages deployed to it, select the **Detect Only** check box.

**18. Click Next.**

**Step Result:** The *Pre-Installation Summary* dialog box displays.

**19.** Verify the agent pre-installation summary information is accurate.



20. Click **Next** to begin the installation.

**Step Result:** The *Install Complete Success* dialog displays when the installation process is finished.

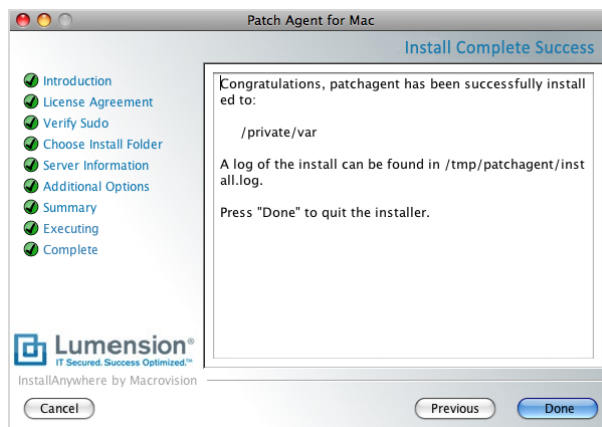


Figure 26: Install Complete Success Dialog

21. Click **Done** to complete the installation and close the installer.

## Installing the Command Line Agent for Linux, UNIX, and Mac

### Prerequisites:

Ensure that the currently installed Java version meets the requirements defined under *Supported Agent Operating Systems* on page 12.

Verify that your computer meets the minimum requirements for agent installation. See *Agent for Linux, UNIX, and Mac* on page 16 for more information.

Download the appropriate installer for your operating system. See *Downloading the Installer* on page 19 for more information.

After ensuring the endpoint meets the minimum system requirements, complete the following steps to install the command line agent.

1. In the `/root` directory, create an `UnixUpdateAgent` directory.
2. From the downloaded location select the `UnixUpdateAgent.tar` file, and extract the file's contents to: `/root/UnixUpdateAgent`.
3. Open a Terminal window.
4. Navigate to the `/root/UnixUpdateAgent/` directory.
5. Type `./install` to start the installation process.
6. At the Enter the Directory where the Agent should be installed `[/usr/local]:` prompt, type the desired installation path or press ENTER to accept the default path of `/usr/local`.
7. At the Enter your Lumension Endpoint Management and Security Suite address prompt, type the URL or IP of the Lumension Endpoint Management and Security Suite, to which the agent will be communicating, in the format of `http://ServerAddress` or `https://ServerAddress`.

8. At the Enter the product serial number that appears as xxxxxxxx-xxxxxxx: prompt, type your serial number.

---

**Tip:** You must enter your serial number in the xxxxxxxx-xxxxxxx format. You can copy the serial number from the Lumension Endpoint Management and Security Suite *Home* page or the *Download Agent Installers* page.

---

9. At the Do you have a Proxy [Y/N]: prompt; type y to configure a proxy, or press ENTER to continue without configuring a proxy server.
10. At the Do you wish to add this agent to existing groups on Lumension Endpoint Management and Security Suite? [Y/N]: prompt, type y to add the agent to a group or n to continue.

**Result:** The installation completes and the terminal link can be disconnected.

---

**Note:** Some issues when installing the Agent for Linux/Unix/Mac may include:

- An incorrect Lumension Endpoint Management and Security Suite address (if using SSL, the URL starts with https://).
  - An incorrect serial number.
  - Networking problems.
  - An incorrect proxy address or port.
- 

## Installing Agents by Agent Management Job

You can install agents upon network endpoints remotely by using agent management jobs. Installing agents remotely substantially eases an administrator's workload, since they do not have to install agents locally.

---

### Prerequisites:

- Agent management jobs can only manage Windows-based endpoints. Unix-based endpoints are not agent management job-compatible.
- When configuring the job, you must enter credentials that authenticate with target endpoints for a successful job outcome.
- Windows Vista, Windows Server 2008, and Windows 7 targets must have **Network discovery** and **File sharing** enabled to be discovered by the agent management job. For additional information refer to [Configuring Post-Windows Vista Endpoints for Discovery](#) on page 99.
- Your server must be configured to allow agent management. For additional information, refer to [Configuring the Scanning System](#) on page 91.
- Targets must be configured to allow agent management. For additional information, refer to [Configuring Endpoints for Agent Management Jobs \(Pre-Windows Vista\)](#) on page 94 or [Configuring Endpoints for Agent Management Jobs \(Post-Windows Vista\)](#) on page 103.

Verify that your computer meets the minimum requirements for agent installation. See [Agent for Linux, UNIX, and Mac](#) on page 16 for more information.

---



Configuration of agent management jobs is similar to configuration of an ad hoc discovery scan job. Configuration occurs in the *Schedule Agent Management Job - Install Wizard*.

**Note:** Agent management jobs can only manage Windows-based endpoints. Unix-based endpoints are not agent management job-compatible.

1. Select **Discover > Assets and Manage Agents > Install Agents**.

**Step Result:** The *Schedule Agent Management Job - Install* wizard opens to the *Job Name and Scheduling* page.

Figure 27: Job Name and Scheduling Page

2. If desired, type a new name in the **Scan job name** field.

**Note:** By default, new agent management jobs for installation are named `New Agent Install Management Job`, followed by the server's date and time, which is formatted according to your browser's locale setting.

3. Schedule the job.

Use one of the following methods.

Method	Steps
<b>To schedule an immediate job:</b>	Select the <b>Immediate</b> option.



Method	Steps
<p><b>To schedule a one-time job:</b></p>	<ol style="list-style-type: none"> <li>1. Ensure the <b>Once</b> option is selected.</li> <li>2. Define a start date. Complete one of the following sub step sets. <ul style="list-style-type: none"> <li>To define a start date manually:</li> <li>You can also select the start date by clicking the <b>Calender</b> icon.</li> <li>a. Type the start date in the <b>Start date</b> field using a mm/dd/yyyy format.</li> <li>To define a start date using the UI:</li> <li>a. Click the <b>Menu</b> icon.</li> <li>b. Select a date from the calender. If necessary, use the arrow icons to open change months.</li> </ul> </li> <li>3. Define a start time. Complete one of the following sub step sets. <ul style="list-style-type: none"> <li>To define a start time manually:</li> <li>a. Type the start time in the <b>Start time</b> field using a hh:mm format followed by AM or PM. The <b>Start time</b> field supports both 12- and 24-hour time.</li> <li>To define a start time using the UI:</li> <li>a. Click the <b>Clock</b> icon.</li> <li>b. Select a time from the menu.</li> </ul> </li> </ol> <hr/> <p><b>Note:</b> Scheduling a one-time job for a past date and time will launch the job immediately.</p> <hr/>



Method	Steps
<b>To schedule a recurring weekly job:</b>	<ol style="list-style-type: none"><li>1. Select the <b>Weekly</b> option.</li><li>2. Define a start date. Complete one of the following sub step sets.  To define a start date manually:  You can also select the start date by clicking the <b>Calender</b> icon.<ol style="list-style-type: none"><li>a. Type the start date in the <b>Start date</b> field using a mm/dd/yyyy format.</li></ol> To define a start date using the UI:<ol style="list-style-type: none"><li>a. Click the <b>Menu</b> icon.</li><li>b. Select a date from the calender. If necessary, use the arrow icons to open change months.</li></ol></li><li>3. Define a start time. Complete one of the following sub step sets.  To define a start time manually:<ol style="list-style-type: none"><li>a. Type the start time in the <b>Start time</b> field using a hh:mm format followed by AM or PM. The <b>Start time</b> field supports both 12- and 24-hour time.</li></ol> To define a start time using the UI:<ol style="list-style-type: none"><li>a. Click the <b>Clock</b> icon.</li><li>b. Select a time from the menu.</li></ol></li></ol>



Method	Steps
<p><b>To schedule a recurring monthly job:</b></p>	<ol style="list-style-type: none"> <li>1. Select the <b>Monthly</b> option.</li> <li>2. Define a start date. Complete one of the following sub step sets. <p>To define a start date manually:</p> <p>You can also select the start date by clicking the <b>Calender</b> icon.</p> <ol style="list-style-type: none"> <li>a. Type the start date in the <b>Start date</b> field using a mm/dd/yyyy format.</li> </ol> <p>To define a start date using the UI:</p> <ol style="list-style-type: none"> <li>a. Click the <b>Menu</b> icon.</li> <li>b. Select a date from the calender. If necessary, use the arrow icons to open change months.</li> </ol> </li> <li>3. Define a start time. Complete one of the following sub step sets. <p>To define a start time manually:</p> <ol style="list-style-type: none"> <li>a. Type the start time in the <b>Start time</b> field using a hh:mm format followed by AM or PM. The <b>Start time</b> field supports both 12- and 24-hour time.</li> </ol> <p>To define a start time using the UI:</p> <ol style="list-style-type: none"> <li>a. Click the <b>Clock</b> icon.</li> <li>b. Select a time from the menu.</li> </ol> </li> </ol>

---

**Note:** One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

---



#### 4. Click **Next**.

**Step Result:** The *Targets* page opens.

Figure 28: Targets Page

#### 5. Define targets (endpoints) for the job to locate.

Use one or more of the following discovery methods.

Method	Steps
<p><b>To define targets using a single IP address:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Single IP Address</b>.</li> <li>2. Type an IP address in the empty field. Wildcards are supported. For additional information refer to <i>Defining Targets Within an Imported File</i> in the <i>Lumension Endpoint Management and Security Suite 7.0 User Guide</i> (<a href="http://portal.lumension.com">http://portal.lumension.com</a>).</li> <li>3. If necessary, edit the <b>Timeout</b> list. The <b>Timeout</b> list defines the number of seconds before a scan fails due to inactivity for a particular target. Under most network conditions, the <b>Timeout</b> field does not require editing.</li> <li>4. If necessary, edit the <b>Number of retries</b> list. The <b>Number of retries</b> list defines the number of times a scan retries on that target if the scan times out.</li> </ol>



Method	Steps
<p><b>To define targets using an IP range:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>IP Range</b>.</li> <li>2. In the first empty field, type the beginning of IP range. Wildcards are supported. For additional information refer to <i>Defining Targets Within an Imported File</i> in the <i>Lumension Endpoint Management and Security Suite 7.0 User Guide</i> (<a href="http://portal.lumension.com">http://portal.lumension.com</a>).</li> <li>3. In the second empty field, type the ending of the IP range.</li> <li>4. If necessary, edit the <b>Timeout</b> list. The <b>Timeout</b> list defines the number of seconds before a scan fails due to inactivity for that particular target. Under most network conditions, the <b>Timeout</b> field does not require editing.</li> <li>5. If necessary, edit the <b>Number of retries</b> list. The <b>Number of retries</b> list defines the number of times a scan retries on that target if the scan times out.</li> </ol>
<p><b>To define targets using a computer name:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Computer name</b>.</li> <li>2. In the empty field, type an endpoint name in one of the following formats: endpointname or domain\endpointname.</li> </ol>
<p><b>To define targets using network neighborhood:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Network Neighborhood</b>.</li> <li>2. From the second list, select the desired network neighborhood.</li> </ol>
<p><b>To define targets using active directory:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Active Directory</b>.</li> <li>2. In the <b>Fully-qualified domain name</b> field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller's DNS name was <i>box.domain.company.local</i>, you would type <i>domain.company.local</i> in this field.</li> <li>3. In the <b>Organizational Unit</b> field, type the active directory's organizational unit string from specific to broad (optional). The omission of this field returns job results containing the full contents of <i>all</i> the active directory's organizational units.</li> <li>4. In the <b>Domain controller</b> field, type the domain controller's IP address.</li> <li>5. In the <b>Username</b> field, type the user name that will authenticate with the domain controller. Type the user name in one of the following format: domainname\username or username.</li> <li>6. In the <b>Password</b> field, type the password associated with the user name.</li> </ol>



Method	Steps
<b>To define targets using an imported file:</b>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Import file</b>.</li> <li>2. Click <b>Browse</b>.</li> <li>3. Browse to the file you want to use for target discovery. The following file types are supported: .txt and .csv.</li> <li>4. Click <b>Open</b>.</li> </ol>

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

Use one of the following methods.

Method	Steps
<b>To include defined targets in the job:</b>	Click <b>Add to Scan</b> .
<b>To exclude defined targets from the job:</b>	Click <b>Exclude from Scan</b> .

**Note:** You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

7. If desired, define additional targets and add them to the list. For more information, see *Editing Targets* in the *Lumension Endpoint Management and Security Suite 7.0 User Guide* (<http://portal.lumension.com>).
8. Click **Next**.

**Step Result:** The *Options* page opens.

**Options**

---

**Scan Options**

<input checked="" type="checkbox"/> Verify With Ping <input checked="" type="checkbox"/> ICMP Discovery <input type="checkbox"/> Port Scan Discovery <input checked="" type="checkbox"/> SNMP Discovery	<input checked="" type="checkbox"/> Windows Version Discovery <input checked="" type="checkbox"/> Resolve DNS Names <input checked="" type="checkbox"/> Resolve MAC Addresses <input checked="" type="checkbox"/> Resolve NetBIOS Names
--	--

---

**Agent Options**

Windows XP and newer agent version: <input type="text" value="LEMSS 7.0.0.1"/>	Windows 2000 agent version: <input type="text" value="Patch 6.4.0.490"/>
Upgrade/Repair: <input type="checkbox"/> Overwrite existing agents	

Figure 29: Options Page



9. Select or clear the desired **Scan Options**.

The following table defines each **Scan Option**.

Option	Description
<b>Verify With Ping</b>	<p>Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to <b>Verify With Ping</b> are not scanned by other selected discovery options.</p> <hr/> <p><b>Note:</b> Anti-virus software and host firewalls may block <b>Verify With Ping</b>. If necessary, adjust anti-virus and firewall configurations to permit ping requests.</p>
<b>ICMP Discovery</b>	<p>Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems.</p> <hr/> <p><b>Note:</b> <b>ICMP Discovery</b> is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with <b>Windows Version Discovery</b>.</p>
<b>Port Scan Discovery</b>	<p>Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified.</p> <hr/> <p><b>Note:</b> For best results in identifying Windows operating systems, use this option in conjunction with <b>Windows Version Discovery</b>.</p>
<b>SNMP Discovery</b>	<p>Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified.</p> <hr/> <p><b>Note:</b> Without authenticated credentials, SNMP devices ignore <b>SNMP Discovery</b> requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the <i>public</i> credential by default.</p>



Option	Description
<b>Windows Version Discovery</b>	<p>Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during <b>ICMP</b> or <b>Port Scan Discovery</b>.</p> <hr/> <p><b>Note:</b> Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either <b>ICMP</b> or <b>Port Scan Discovery</b>.</p>
<b>Resolve DNS Names</b>	<p>Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification.</p>
<b>Resolve MAC Addresses</b>	<p>Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification.</p> <hr/> <p><b>Note:</b> Monitor network inventory reports to prevent MAC address spoofing that may alter the <b>Resolve MAC Addresses</b> results.</p>
<b>Resolve NetBIOS Names</b>	<p>Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.</p> <hr/> <p><b>Note:</b> Security-hardened networks running Windows 2000, Windows 2003, or Windows XP may require enablement of NetBIOS over TCP/IP for <b>Resolve NetBIOS Names</b> to acquire NetBIOS names. Additionally, firewalls protecting endpoints using Windows XP Professional SP2 may require adjustment to permit NetBIOS communication.</p>

#### 10. Select the desired **Agent Options**.

These options control which version of the agent are installed on Windows endpoints.

- For endpoints running Windows XP or a newer Windows operating system, select an agent version from the **Windows XP and newer agent versions** list.
- For endpoints running Windows 2000, select an agent version from the **Windows 2000 agent version** list.

---

**Note:** The availability of different agents in these lists is determined by the Lumension Endpoint Management and Security Suite server settings. For more information, see *Agent Versions* in the [Lumension Endpoint Management and Security Suite 7.0 User Guide \(http://portal.lumension.com\)](http://portal.lumension.com).

- If desired, select the **Overwrite existing agents** check box.

This option controls whether the agent management job re-installs the agent on targets that already have agents installed. If the a Windows XP or later endpoint has a version 6.3 or 6.4 agent on it, the agent will be overwritten with a version 7.0 agent. If the endpoint has a version 6.2 agent on it, it will not be overwritten and the agent management job will show as Incomplete.



**11. Click Next.**

**Step Result:** The *Credentials* page opens.

The screenshot shows a web form titled "Credentials" with the subtitle "Providing credentials can help the scan identify OSs with greater accuracy." The form is divided into three sections:

- Windows:** Contains three input fields labeled "Username:", "Password:", and "Confirm password:". Below the Username field is a small text example: "e.g. username or domain\username".
- POSIX:** Contains three input fields labeled "Username:", "Password:", and "Confirm password:". Below the Username field is a small text example: "e.g. login@domain". Below these fields is a "Private key:" label followed by a text input field and a "Browse..." button.
- SNMP:** Contains a single input field labeled "Community string:".

Figure 30: Credentials Page

**12. Define Windows credentials for the target.**

Type the applicable information in the following fields.

**Note:** When configuring an agent management job, you must define valid Windows credentials.

Field	Description
<b>Username</b>	A user name that authenticates with Windows-based endpoints. Type the user name in a local format (username) or a domain format (domain/username).
<b>Password</b>	The password associated with the <b>Username</b> .
<b>Confirm password</b>	The <b>Password</b> retyped.



**13. Click Next.**

**Step Result:** The *Agent Settings* page opens.

Figure 31: Agent Settings Page

**14. Define the **Distribution** drop-down lists.**

The following table describes each list their available values.

List	Description
<b>Timeout</b>	Defines the number of minutes before the agent management job terminates due to a non-responsive agent installation or removal (0-30).
<b>Number of retries</b>	Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10).
<b>Number of simultaneous installs</b>	Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of 1 indicates that serial installs or removals should occur.

**15. Define how the endpoints that are having agents installed will name the Lumension Endpoint Management and Security Suite server within their registries by selecting a **Server identity** option.**

The following table describes each option.

Method	Steps
<b>To have agents list the Lumension Endpoint Management and Security Suite server by its default name:</b>	Do not edit the <b>Server identity</b> field. The server will be identified on the agent according to the value set in the <b>Agent Installation</b> section of the <i>Agents</i> tab located on the <i>Options</i> page. For more information, see <i>Agent Installation</i> in the <a href="http://portal.lumension.com">Lumension Endpoint Management and Security Suite 7.0 User Guide</a> ( <a href="http://portal.lumension.com">http://portal.lumension.com</a> ) .



Method	Steps
<b>To have agent list the Lumension Endpoint Management and Security Suite server by a user-defined name:</b>	Type address information for your Lumension EMSS server in the <b>Server identity</b> field. Information must be entered in one of the following formats: <ul style="list-style-type: none"> <li>• endpointname.domainname.com</li> <li>• computername</li> <li>• 10.10.10.10</li> </ul>

16. If using a proxy during agent management, and that proxy requires authentication, select the **Authentication required** check box and define the following fields.

Field	Description
<b>Username</b>	A user name that authenticates with the proxy.
<b>Password</b>	The password associated with the <b>Username</b> .
<b>Confirm password</b>	The <b>Password</b> retyped.

17. Click **Finish**.

**Result:** The *Schedule Agent Management Job - Install* wizard closes. Depending on how you configured the job, it moves to either the *Scheduled* tab or *Active* tab on the *Job Results* page. The job will run at the applicable time, installing agents on the defined targets, and move to *Completed* tab when finished.

## Upgrading Agents

Endpoints running Windows XP or later operating systems are upgraded regularly when they connect to the Lumension Endpoint Management and Security Suite server due to the presence of the Lumension EMSS Agent. Endpoints running Windows 2000 or a version of the Linux, Unix, or Mac operating systems must be upgraded manually. In all cases, you should verify that your agents are being upgraded on your endpoints regularly.



## Upgrading Agents Locally

Upgrading the agent replaces the version of the agent running on the endpoint with the most recent version of the agent.

1. Click **Tools > Download Agent Installer**.

**Step Result:** The *Download Agent Installers* page opens.

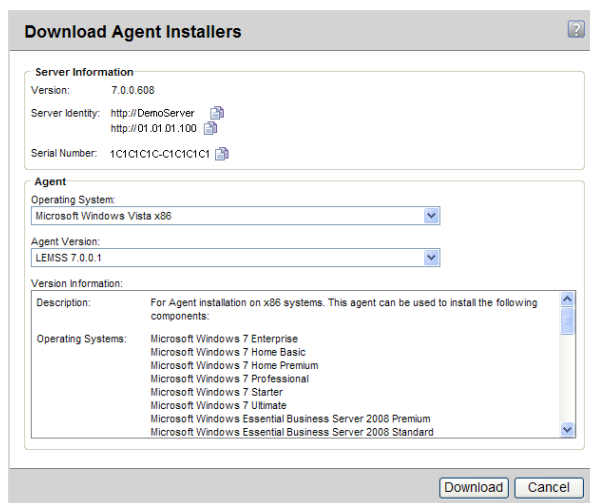


Figure 32: Download Agent Installers

---

**Note:** You can click **Cancel** at any time to close this page and cancel the download procedure.

---

**Tip:** Click the **copy** icon to copy the version, URL, or serial number information to the clipboard.

---

2. Select the endpoint's operating system from the **Operating System** drop-down list.
3. Select the version of the agent that you want to install from the **Agent Version** drop-down list.
4. Click **Download** to download the installer to the endpoint.

**Step Result:** The installer downloads to the location you specify on your computer.

5. In the *Download Agent Installers* page, click **Close**.

**Result:** The *Download Agent Installers* page closes.



---

## Uninstalling Agents

---

Uninstalling an agent from an endpoint removes the agent from the endpoint. The endpoint can still be detected by the Lumension Endpoint Management and Security Suite server, but will no longer receive security content from the Lumension Endpoint Management and Security Suite server.

You can uninstall an agent on an endpoint in either of the following ways:

- Uninstall the agent locally on the endpoint.
- Create an agent management job to uninstall the agent that targets the endpoint. When the job executes, an agent is uninstalled on the endpoint.

### Uninstalling Agents by Agent Management Job

You can remotely uninstall agents from endpoints in your network using an agent management job. These jobs prevent administrators from having to uninstall agents locally.

---

#### Prerequisites:

- Agent management jobs can only manage Windows-based endpoints. Unix-based endpoints are not agent management job-compatible.
- When configuring the job, you must enter credentials that authenticate with target endpoints for a successful job outcome.
- Windows Vista, Windows Server 2008, and Windows 7 targets must have **Network discovery** and **File sharing** enabled to be discovered by the agent management job. For additional information refer to [Configuring Post-Windows Vista Endpoints for Discovery](#) on page 99.
- Your server must be configured to allow agent management. For additional information, refer to [Configuring the Scanning System](#) on page 91.
- Targets must be configured to allow agent management. For additional information, refer to [Configuring Endpoints for Agent Management Jobs \(Pre-Windows Vista\)](#) on page 94 or [Configuring Endpoints for Agent Management Jobs \(Post-Windows Vista\)](#) on page 103.

---

Configuration of agent management is similar to an ad hoc discovery scan. Configuration occurs in the **Schedule Agent Management Job - Uninstall** wizard.

---

**Note:** Agent management jobs can only manage Windows-based endpoints. Unix-based endpoints are not agent management job-compatible.

---



1. Select **Discover > Assets and Manage Agents > Uninstall Agents**.

**Step Result:** The *Schedule Agent Management Job - Uninstall* wizard opens to the *Job Name and Scheduling* page.

Figure 33: Job Name and Scheduling Page

2. If desired, type a new name in the **Scan job name** field.

**Note:** By default, new agent management jobs for uninstallation are named `New Agent Uninstall Management Job`, followed by the server's date and time, which is formatted according to your browser's locale setting.

3. Schedule the job.

Use one of the following methods.

Method	Steps
To schedule an immediate job:	Select the <b>Immediate</b> option.



Method	Steps
<p><b>To schedule a one-time job:</b></p>	<ol style="list-style-type: none"> <li>1. Ensure the <b>Once</b> option is selected.</li> <li>2. Define a start date. Complete one of the following sub step sets. <ul style="list-style-type: none"> <li>To define a start date manually:</li> <li>You can also select the start date by clicking the <b>Calender</b> icon.</li> <li>a. Type the start date in the <b>Start date</b> field using a mm/dd/yyyy format.</li> <li>To define a start date using the UI:</li> <li>a. Click the <b>Menu</b> icon.</li> <li>b. Select a date from the calender. If necessary, use the arrow icons to open change months.</li> </ul> </li> <li>3. Define a start time. Complete one of the following sub step sets. <ul style="list-style-type: none"> <li>To define a start time manually:</li> <li>a. Type the start time in the <b>Start time</b> field using a hh:mm format followed by AM or PM. The <b>Start time</b> field supports both 12- and 24-hour time.</li> <li>To define a start time using the UI:</li> <li>a. Click the <b>Clock</b> icon.</li> <li>b. Select a time from the menu.</li> </ul> </li> </ol> <hr/> <p><b>Note:</b> Scheduling a one-time job for a past date and time will launch the job immediately.</p> <hr/>



Method	Steps
<b>To schedule a recurring weekly job:</b>	<ol style="list-style-type: none"><li>1. Select the <b>Weekly</b> option.</li><li>2. Define a start date. Complete one of the following sub step sets.  To define a start date manually:  You can also select the start date by clicking the <b>Calender</b> icon.<ol style="list-style-type: none"><li>a. Type the start date in the <b>Start date</b> field using a mm/dd/yyyy format.</li></ol> To define a start date using the UI:<ol style="list-style-type: none"><li>a. Click the <b>Menu</b> icon.</li><li>b. Select a date from the calender. If necessary, use the arrow icons to open change months.</li></ol></li><li>3. Define a start time. Complete one of the following sub step sets.  To define a start time manually:<ol style="list-style-type: none"><li>a. Type the start time in the <b>Start time</b> field using a hh:mm format followed by AM or PM. The <b>Start time</b> field supports both 12- and 24-hour time.</li></ol> To define a start time using the UI:<ol style="list-style-type: none"><li>a. Click the <b>Clock</b> icon.</li><li>b. Select a time from the menu.</li></ol></li></ol>



Method	Steps
<p><b>To schedule a recurring monthly job:</b></p>	<ol style="list-style-type: none"> <li>1. Select the <b>Monthly</b> option.</li> <li>2. Define a start date. Complete one of the following sub step sets. <p>To define a start date manually:</p> <p>You can also select the start date by clicking the <b>Calender</b> icon.</p> <ol style="list-style-type: none"> <li>a. Type the start date in the <b>Start date</b> field using a mm/dd/yyyy format.</li> </ol> <p>To define a start date using the UI:</p> <ol style="list-style-type: none"> <li>a. Click the <b>Menu</b> icon.</li> <li>b. Select a date from the calender. If necessary, use the arrow icons to open change months.</li> </ol> </li> <li>3. Define a start time. Complete one of the following sub step sets. <p>To define a start time manually:</p> <ol style="list-style-type: none"> <li>a. Type the start time in the <b>Start time</b> field using a hh:mm format followed by AM or PM. The <b>Start time</b> field supports both 12- and 24-hour time.</li> </ol> <p>To define a start time using the UI:</p> <ol style="list-style-type: none"> <li>a. Click the <b>Clock</b> icon.</li> <li>b. Select a time from the menu.</li> </ol> </li> </ol>

---

**Note:** One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

---



4. Click **Next**.

**Step Result:** The *Targets* page opens.

Figure 34: Targets Page

## 5. Define targets (endpoints) for the job to locate.

Use one or more of the following discovery methods.

Method	Steps
<b>To define targets using a single IP address:</b>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Single IP Address</b>.</li> <li>2. Type an IP address in the empty field. Wildcards are supported. For additional information refer to <i>Defining Targets Within an Imported File</i> in the <i>Lumension Endpoint Management and Security Suite 7.0 User Guide</i> (<a href="http://portal.lumension.com">http://portal.lumension.com</a>).</li> <li>3. If necessary, edit the <b>Timeout</b> list. The <b>Timeout</b> list defines the number of seconds before a scan fails due to inactivity for a particular target. Under most network conditions, the <b>Timeout</b> field does not require editing.</li> <li>4. If necessary, edit the <b>Number of retries</b> list. The <b>Number of retries</b> list defines the number of times a scan retries on that target if the scan times out.</li> </ol>



Method	Steps
<p><b>To define targets using an IP range:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>IP Range</b>.</li> <li>2. In the first empty field, type the beginning of IP range. Wildcards are supported. For additional information refer to <i>Defining Targets Within an Imported File</i> in the <i>Lumension Endpoint Management and Security Suite 7.0 User Guide</i> (<a href="http://portal.lumension.com">http://portal.lumension.com</a>).</li> <li>3. In the second empty field, type the ending of the IP range.</li> <li>4. If necessary, edit the <b>Timeout</b> list. The <b>Timeout</b> list defines the number of seconds before a scan fails due to inactivity for that particular target. Under most network conditions, the <b>Timeout</b> field does not require editing.</li> <li>5. If necessary, edit the <b>Number of retries</b> list. The <b>Number of retries</b> list defines the number of times a scan retries on that target if the scan times out.</li> </ol>
<p><b>To define targets using a computer name:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Computer name</b>.</li> <li>2. In the empty field, type an endpoint name in one of the following formats: endpointname or domain\endpointname.</li> </ol>
<p><b>To define targets using network neighborhood:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Network Neighborhood</b>.</li> <li>2. From the second list, select the desired network neighborhood.</li> </ol>
<p><b>To define targets using active directory:</b></p>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Active Directory</b>.</li> <li>2. In the <b>Fully-qualified domain name</b> field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller's DNS name was <i>box.domain.company.local</i>, you would type <i>domain.company.local</i> in this field.</li> <li>3. In the <b>Organizational Unit</b> field, type the active directory's organizational unit string from specific to broad (optional). The omission of this field returns job results containing the full contents of <i>all</i> the active directory's organizational units.</li> <li>4. In the <b>Domain controller</b> field, type the domain controller's IP address.</li> <li>5. In the <b>Username</b> field, type the user name that will authenticate with the domain controller. Type the user name in one of the following format: domainname\username or username.</li> <li>6. In the <b>Password</b> field, type the password associated with the user name.</li> </ol>



Method	Steps
<b>To define targets using an imported file:</b>	<ol style="list-style-type: none"> <li>1. From the <b>Scan for</b> list, select <b>Import file</b>.</li> <li>2. Click <b>Browse</b>.</li> <li>3. Browse to the file you want to use for target discovery. The following file types are supported: .txt and .csv.</li> <li>4. Click <b>Open</b>.</li> </ol>

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

Use one of the following methods.

Method	Steps
<b>To include defined targets in the job:</b>	Click <b>Add to Scan</b> .
<b>To exclude defined targets from the job:</b>	Click <b>Exclude from Scan</b> .

**Note:** You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

7. If desired, define additional targets and add them to the list. For more information, see *Editing Targets* in the *Lumension Endpoint Management and Security Suite 7.0 User Guide* (<http://portal.lumension.com>).
8. Click **Next**.

**Step Result:** The *Options* page opens.

The screenshot shows a window titled "Options" with a section for "Scan Options". The following checkboxes are checked:

- Verify With Ping
- ICMP Discovery
- Port Scan Discovery
- SNMP Discovery
- Windows Version Discovery
- Resolve DNS Names
- Resolve MAC Addresses
- Resolve NetBIOS Names

Figure 35: Options Page

9. Select or clear the desired **Scan Options**.

The following table defines each **Scan Option**.

Option	Description
<b>Verify With Ping</b>	<p>Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to <b>Verify With Ping</b> are not scanned by other selected discovery options.</p> <hr/> <p><b>Note:</b> Anti-virus software and host firewalls may block <b>Verify With Ping</b>. If necessary, adjust anti-virus and firewall configurations to permit ping requests.</p>
<b>ICMP Discovery</b>	<p>Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems.</p> <hr/> <p><b>Note:</b> <b>ICMP Discovery</b> is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with <b>Windows Version Discovery</b>.</p>
<b>Port Scan Discovery</b>	<p>Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified.</p> <hr/> <p><b>Note:</b> For best results in identifying Windows operating systems, use this option in conjunction with <b>Windows Version Discovery</b>.</p>
<b>SNMP Discovery</b>	<p>Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified.</p> <hr/> <p><b>Note:</b> Without authenticated credentials, SNMP devices ignore <b>SNMP Discovery</b> requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the <i>public</i> credential by default.</p>



Option	Description
<b>Windows Version Discovery</b>	<p>Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during <b>ICMP</b> or <b>Port Scan Discovery</b>.</p> <hr/> <p><b>Note:</b> Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either <b>ICMP</b> or <b>Port Scan Discovery</b>.</p> <hr/>
<b>Resolve DNS Names</b>	<p>Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification.</p>
<b>Resolve MAC Addresses</b>	<p>Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification.</p> <hr/> <p><b>Note:</b> Monitor network inventory reports to prevent MAC address spoofing that may alter the <b>Resolve MAC Addresses</b> results.</p> <hr/>
<b>Resolve NetBIOS Names</b>	<p>Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.</p> <hr/> <p><b>Note:</b> Security-hardened networks running Windows 2000, Windows 2003, or Windows XP may require enablement of NetBIOS over TCP/IP for <b>Resolve NetBIOS Names</b> to acquire NetBIOS names. Additionally, firewalls protecting endpoints using Windows XP Professional SP2 may require adjustment to permit NetBIOS communication.</p> <hr/>



**10. Click Next.**

**Step Result:** The *Credentials* page opens.

The screenshot shows a web form titled "Credentials" with the following sections:

- Windows:** Username (administrator), Password (masked with dots), Confirm password (masked with dots). Example: e.g. username or domain\username.
- POSIX:** Username, Password, Confirm password, Private key (with a Browse... button). Example: e.g. login@domain.
- SNMP:** Community string.

Figure 36: Credentials Page

**11. Define Windows credentials.**

Type the applicable information in the following fields.

**Note:** When configuring an agent management job, you must define valid Windows credentials.

Field	Description
<b>Username</b>	A user name that authenticates with Windows endpoints. Type the user name in a local format (username) or a domain format (domain/username).
<b>Password</b>	The password associated with the <b>Username</b> .
<b>Confirm password</b>	The <b>Password</b> retyped.



**12. Click Next.**

**Step Result:** The *Agent Settings* page opens.

Figure 37: Agent Settings Page

**13. Define the **Distribution** drop-down lists.**

The following table describes each list their available values.

List	Description
<b>Timeout</b>	Defines the number of minutes before the agent management job terminates due to a non-responsive agent installation or removal (0-30).
<b>Number of retries</b>	Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10).
<b>Number of simultaneous installs</b>	Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of 1 indicates that serial installs or removals should occur.

**14. Define the **Reboot** option.**

Select one of the following options:

- **Suppress the reboot**
- **Force a reboot (does not prompt the user)**

**Note:** If the agent being uninstalled resides on the Lumension Endpoint Management and Security Suite server, the reboot is automatically suppressed regardless of this setting.

**15. Click **Finish**.**

**Result:** The *Schedule Agent Management Job - Uninstall* wizard closes. Depending on how you configured the job, it moves to either the *Scheduled* tab or *Active* tab on the *Job Results* page.



The job will run at the applicable time, uninstalling agents on the defined targets, and move to the *Completed* tab when finished.

## Uninstalling the Agent for Windows 2000 Locally

You can uninstall agents locally on managed endpoints running the pre-Windows Vista operating system.

### Prerequisites:

In order to uninstall an agent from an endpoint, you must provide the uninstall password. See [Lumension Endpoint Management and Security Suite 7.0 User Guide \(http://portal.lumension.com\)](http://portal.lumension.com) for more information.

1. Select **Start** > **Control Panel** from the Windows menu bar.
2. Double-click **Add/Remove Programs**.
3. Select **Patch Agent** from the list of installed programs.
4. Click **Change**.

**Step Result:** The Patch Agent installer displays.

5. Click **Next**.
6. Enter the uninstall password for the endpoint in the **Global or uninstall password** field.  
The uninstall password is set in the Global Agent Policy Set. For more information on agent policy sets, see *The Policies View* in the [Lumension Endpoint Management and Security Suite 7.0 User Guide \(http://portal.lumension.com\)](http://portal.lumension.com).
7. Click **Next**.
8. Click **Remove**.
9. Click **Finish**.

**Result:** The agent is uninstalled.

## Uninstalling the Agent for XP or Later Locally

You can uninstall Patch Agents locally on managed endpoints running the Windows XP (or later) operating system.

### Prerequisites:

In order to uninstall an agent from an endpoint, you must provide the uninstall password. See [Lumension Endpoint Management and Security Suite 7.0 User Guide \(http://portal.lumension.com\)](http://portal.lumension.com) for more information.

1. Select **Start** > **Control Panel** from the Windows menu bar.
2. Double-click **Programs and Features**.
3. Select **LM Agent** from the list of installed programs.
4. Click **Change**.

**Step Result:** The Patch Agent installer displays.

5. Click **Next**.



6. Enter the uninstall password for the endpoint in the **Global or uninstall password** field.  
The uninstall password is set in the Global Agent Policy Set. For more information on agent policy sets, see *The Policies View* in the *Lumension Endpoint Management and Security Suite 7.0 User Guide* (<http://portal.lumension.com>).
7. Click **Next**.
8. Click **Remove**.
9. Click **Finish**.

**Result:** The agent is uninstalled.

## Uninstalling the Agent for Linux Locally

Perform the following procedure to uninstall the Linux agent locally.

1. Navigate to the agent installation directory. By default, this is `/usr/local/patchagent`.
2. Type `./uninstall` at the command prompt.
3. Press `ENTER`.

**Step Result:** The Linux agent is uninstalled.

4. Type `cd /usr/local` to navigate to the parent directory of the installation directory. If you installed the agent to a directory other than the default directory, navigate to the parent directory of the agent installation directory.
5. Press `ENTER`.
6. Type `rm -rf patchagent`.
7. Press `ENTER`.

**Result:** The Linux agent installation directory is deleted.

## Uninstalling the Agent for Solaris Locally

Perform the following procedure to uninstall the Solaris agent locally.

1. Navigate to the agent installation directory. By default, this is `/export/home/patchagent`.
2. Type `./uninstall` at the command prompt.
3. Press `ENTER`.

**Step Result:** The Solaris agent is uninstalled.

4. Type `cd /export/home` to navigate to the parent directory of the installation directory. If you installed the agent to a directory other than the default directory, navigate to the parent directory of the agent installation directory.
5. Press `ENTER`.
6. Type `rm -rf patchagent`.
7. Press `ENTER`.

**Result:** The Solaris agent installation directory is deleted.



## Uninstalling the Agent for AIX Locally

Perform the following procedure to uninstall the AIX agent locally.

1. Navigate to the agent installation directory. By default, this is `/usr/local/patchagent`.
2. Type `./uninstall` at the command prompt.
3. Press `ENTER`.

**Step Result:** The AIX agent is uninstalled.

4. Type `cd /usr/local` to navigate to the parent directory of the installation directory. If you installed the agent to a directory other than the default directory, navigate to the parent directory of the agent installation directory.
5. Press `ENTER`.
6. Type `rm -rf patchagent`.
7. Press `ENTER`.

**Result:** The AIX agent installation directory is deleted.

## Uninstalling the Agent for HP-UX Locally

Perform the following procedure to uninstall the HP-UX agent locally.

1. Navigate to the agent installation directory. By default, this is `/usr/local/patchagent`.
2. Type `./uninstall` at the command prompt.
3. Press `ENTER`.

**Step Result:** The HP-UX agent is uninstalled.

4. Type `cd /usr/local` to navigate to the parent directory of the installation directory. If you installed the agent to a directory other than the default directory, navigate to the parent directory of the agent installation directory.
5. Press `ENTER`.
6. Type `rm -rf patchagent`.
7. Press `ENTER`.

**Result:** The HP-UX agent installation directory is deleted.

## Uninstalling the Command Line Agent for Mac Locally

Perform the following procedure to uninstall the Mac command line agent locally.

1. Navigate to the agent installation directory. By default, this is `/private/var/patchagent`.
2. Type `./uninstall` at the command prompt.
3. Press `ENTER`.

**Step Result:** The Mac agent is uninstalled.



4. Type `cd /private/var` to navigate to the parent directory of the installation directory. If you installed the agent to a directory other than the default directory, navigate to the parent directory of the agent installation directory.
5. Press `ENTER`.
6. Type `rm -rf patchagent`.
7. Press `ENTER`.

**Result:** The Mac command line agent installation directory is deleted.



---

# Chapter

# 3

---

## Automating the Agent Installation

---

### In this chapter:

- Automating the Windows MSI Installer
- Performing a Silent Install on Windows
- Performing a Silent Install on Linux/UNIX/Mac

The following section includes instructions for automating the installation of the agent to a device. Instructions include the following:

- Automation of the `PatchAgent.msi` installer. This is the agent installer for the Windows 2000 operation system.
- Automation of the `LMAgent.msi` installer. This is the agent installer for the Windows XP, Windows Vista, Windows 7, Windows 2008, and Windows 2008 R2 operating systems.
- Command line options for installing the Windows 2000 agent automatically.
- Command line options for installing the Windows XP or later agent automatically.
- Command line options for installing the Linux/Unix/Mac agent automatically.

## Automating the Windows MSI Installer

---

The Lumension Patch Agent (Patch Agent) and the Lumension Endpoint Management and Security Suite (LEMSS) Agent for Windows MSI Installers can be used to perform a single installation on the current computer or, through the use of the Windows MSI Installer, Group Policy Objects (GPOs), and the Orca package editor, on multiple computers. Using these tools you can install the agent on all windows computers within your domain.

1. Create a network share as defined in [Creating a Network Share](#) on page 70.
2. Modify the Lumension Patch Agent or LEMSS Agent for Windows MSI Installer (`.msi`) file as defined in [Modifying the PatchAgent.msi File](#) on page 73.
3. Create an organizational unit as defined in [Creating an Organizational Unit](#) on page 82.

---

**Note:** Microsoft Group Policy Object (GPO) allows for mandatory software distribution to computers under control of a particular organizational unit (OU) and can be used to distribute the agent. However, the GPO installation does not check for an existing installation of the agent on the target computer and will reinstall the agent on any computers in the OU. In order to avoid potential problems caused by reinstalling the agent ensure that computers with existing agents are NOT members of the OU which contains the Lumension software GPO.

---



## Creating a Network Share

Create a network share (with read-only access) from which all users can access and install the agent using the Windows MSI installer.

1. Create the `Agent MSI` folder on a network computer.
2. Right-click the `Agent MSI` folder and select **Properties**.
3. Select the **Sharing** tab.
4. Select the **Share this folder** option. If needed, change the **Share name**.

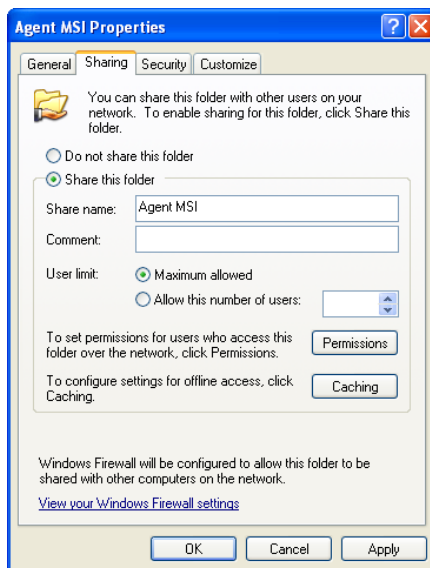


Figure 38: Sharing Tab



## 5. Click **Permissions**.

**Step Result:** The *Permissions for Agent MSI* dialog opens.

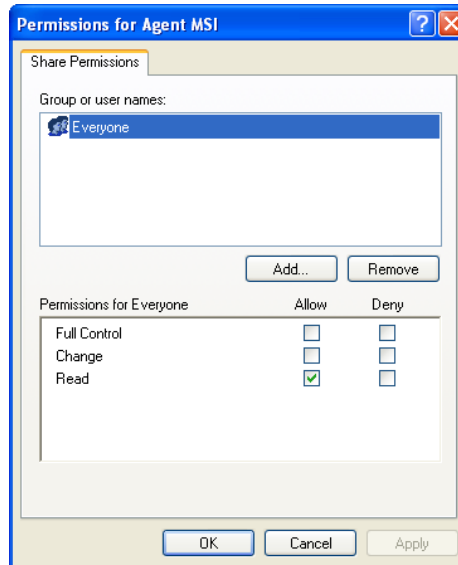


Figure 39: Permissions Dialog

## 6. Click **Add**.

**Step Result:** The *Select Users, Computers, or Groups* dialog opens.

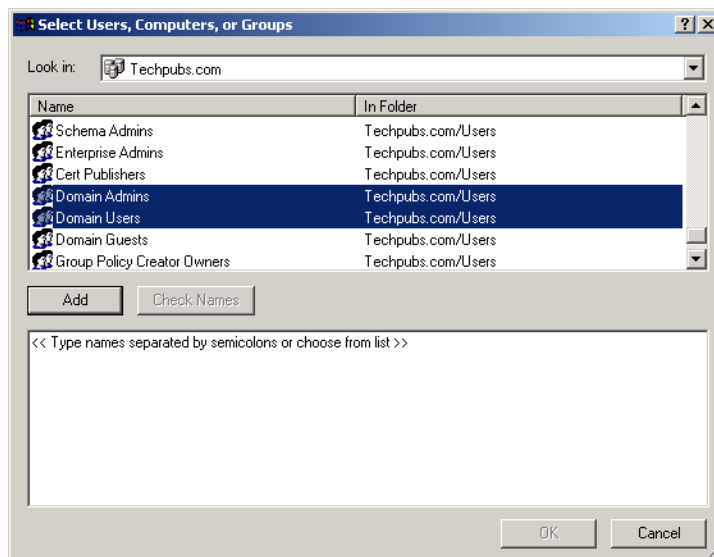


Figure 40: Select Users, Computers, or Groups Dialog



7. In the **Domain Users** and **Domain Admins** groups, select the **Domain Users** group. If you cannot locate the groups, type the names in the **Enter the object names to select** field and click **Check Names**.

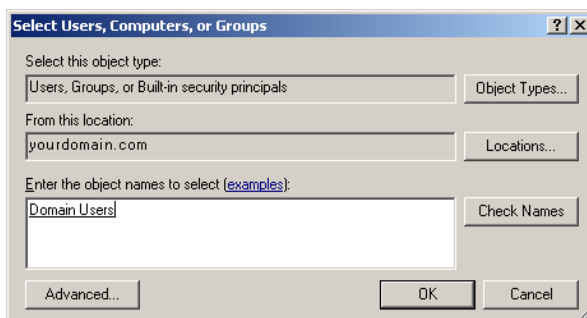


Figure 41: Group Search Dialog

8. Click **OK**.

**Step Result:** The *Select Users, Computers, or Groups* dialog closes and displays the *Permissions for Agent MSI* dialog.

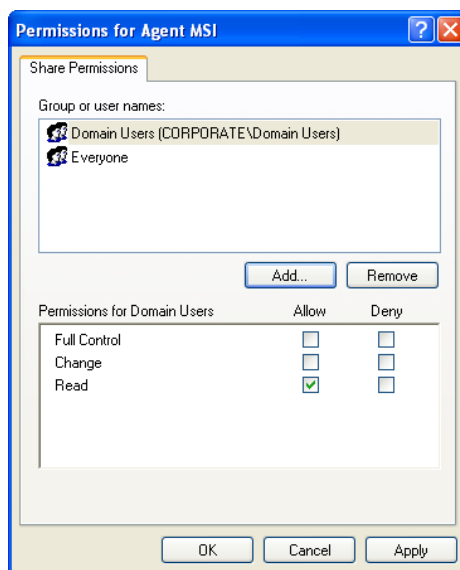


Figure 42: Permissions for Agent MSI Dialog

9. Select the **Everyone** group and choose **Deny Change** and **Allow Read** access.
10. Select the **Domain Admins** group, and choose **Allow Full Control** access.
11. Click **OK**.

**Step Result:** The *Permissions* dialog closes and displays the *Properties* window.

12. Select the *Security* tab.



13. Add the **Domain Users**, **Domain Admins**, and **Everyone** groups (refer to steps 6 through 8) applying **Allow Read** and **Deny Execute** permissions to the **Everyone** and **Domain Users** groups.
14. Add the **Allow Full Control** to the **Domain Admins** group.
15. Click **OK** to close the *Agent MSI Properties* dialog.
16. Download the agent installer that you want to share on your network. For more information, see [Downloading the Installer](#).
17. Copy the installer that you downloaded to the Agent MSI folder you created.

## Modifying the PatchAgent.msi File

To fully automate the agent installation you must modify the `PatchAgent.msi` file to include your host name and serial number. Microsoft Orca allows you to make changes to the application so your users will not have to manually enter their name and serial number for their installs. This also allows the application to be installed remotely.

The user-customized installer properties are defined in the following table:

Table 5: Description of PatchAgent.msi Installation Properties

Property	Description
HOST	The URL (or IP) of your Lumension Endpoint Management and Security Suite.
SERIAL	The serial number of your Lumension Endpoint Management and Security Suite.
USEPROXY	Whether or not a proxy is used. 0=No, 1=Yes.
PROXYURL	The URL (or IP) of your proxy.
PROXYUSER	Login user for an authenticated proxy.
PROXYPASS	Login password for an authenticated proxy.
GROUPLIST	Automatically add the agent to the defined group(s). Either the group name or distinguished name can be used. If the group name is used, the agent will be added to all of the groups with that name.

**Note:** Modifying the digitally signed MSI file will invalidate the digital signature assigned by Lumension. Depending upon your security settings, this may introduce security warnings and restrictions during agent installation.

### To Modify the PatchAgent.msi File Using Microsoft Orca

This procedure explains how to modify the MSI file using Microsoft Orca.

#### Prerequisites:

You must download Microsoft Orca before you can complete this procedure. Orca is installed from the Microsoft Windows Installer SDK which can be downloaded from [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca\\_exe.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp).



Complete this procedure to modify the MSI file using Microsoft Orca.

1. Install Microsoft Orca (or a similar MSI editor tool) to your management workstation.
2. Select **Start > Programs > Orca** to open Microsoft Orca.
3. Open the PatchAgent.msi file that you copied to the network share you created.

**Step Result:** Orca displays the PatchAgent.msi file.

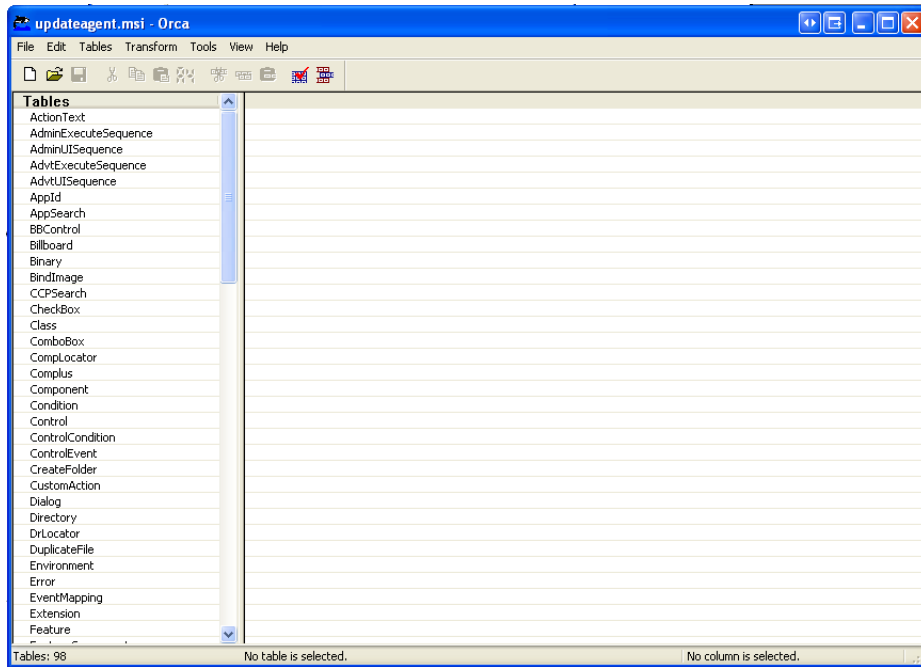


Figure 43: Orca Initial Display

4. Scroll through the **Tables** list and select the **Property** table.

**Step Result:** The **Rows** field populates with the rows associated with the Property table.

5. Locate the **Host** row, and click the **Value** field.

**Step Result:** The **Value** field is activated and can be edited.

6. Type the Lumension Endpoint Management and Security Suite URL in the format: `http://ServerName` (or `https://ServerName` for a secure server) in the **Value** field.

7. Locate the **Serial** row, and click the **Value** field.

**Step Result:** The **Value** field is activated and can be edited.



8. Type your Lumension Endpoint Management and Security Suite serial number in the **Value** field.

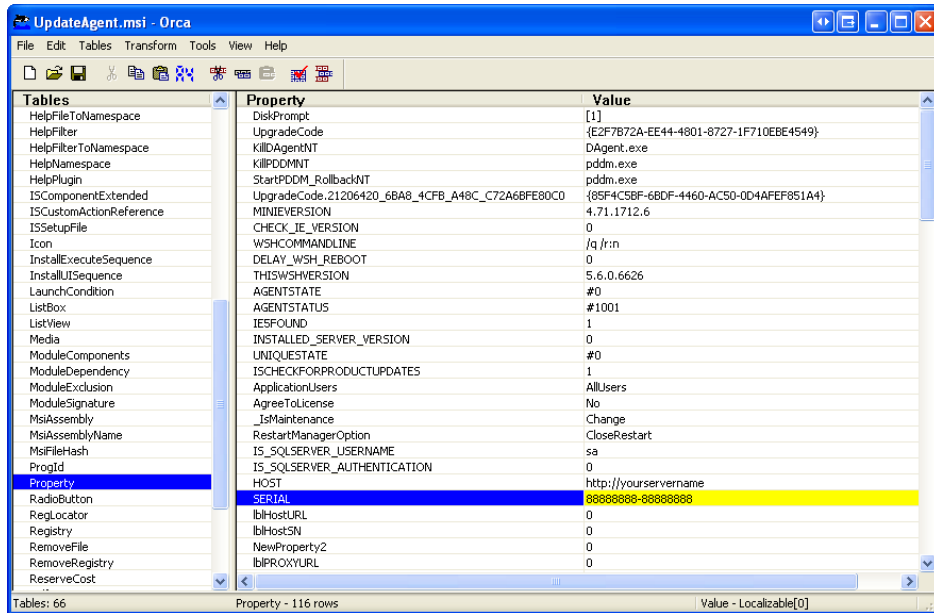


Figure 44: Enter Serial Number

9. If you are using a Proxy Server, add the necessary proxy entries as follows:

- a) Right-click in the right window pane and select **Add Row**.

**Step Result:** The **Add Row** dialog box opens.

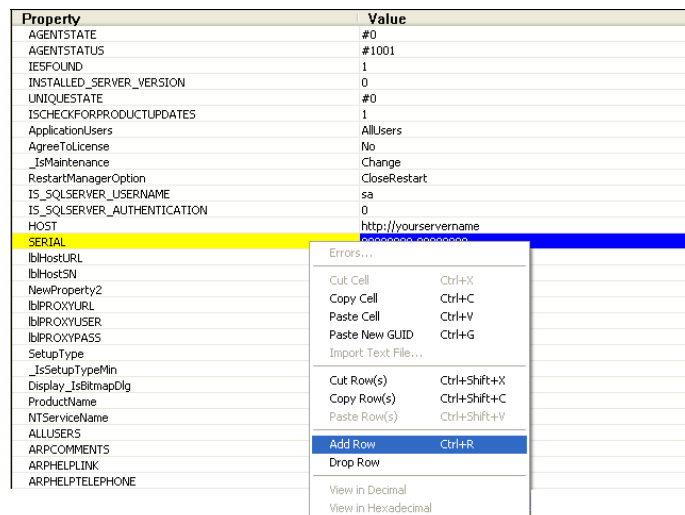


Figure 45: The Add Row dialog box



- b) Enter USEPROXY as the **Property Column** field.

Figure 46: Add Row Property

- c) Select **Value** and type 1 to indicate that proxy is enabled.

Figure 47: Add Row Value

- d) Click **OK**.

**Step Result:** The **USEPROXY** row is added to the Property table.

- e) Add additional rows as needed for the following proxy entries:

Table 6: Proxy specific entries

Property	Value
USEPROXY	1
PROXYURL	http://yourproxyserver:port
PROXYUSER (optional)	Authenticated proxy login user.



Property	Value
PROXYPASS (optional)	Authenticated proxy login user's password.

10. To automatically add the agent to an existing group, add the following entry:

- a) Right-click in the right window pane and select **Add Row**.

**Step Result:** The *Add Row* dialog box opens.

- b) Enter GROUPLIST as the **Property Column** field.
- c) Select **Value** and enter the Group Names in the format: "GroupName1 | GroupName2 | GroupNameN"

**Step Result:** The GROUPLIST row is added to the Property table.

11. Click **Save**.

**Step Result:** Orca saves the changes to the PatchAgent.msi file.

12. Close Microsoft Orca.

**Result:** You can now use the PatchAgent.msi file to manually install the agent by browsing, from the target computer, to the network share you created and manually opening the PatchAgent.msi file.

## Modifying the LMAgent.msi Installer

To fully automate the agent installation you must modify the file to include your server IP address (or fully qualified domain name), group information, and the agent global uninstall password. Microsoft Orca allows you to make changes to the application so your users will not have to manually enter this information for their installs. This also allows the application to be installed remotely.

The user-customized installer properties are defined in the following table:

Table 7: Description of LMAgent.msi Installation Properties

Property	Description
SERVERIPADDRESS	The URL (or IP) of your Lumension Endpoint Management and Security Suite server. You can also use your server's fully qualified domain name as the value for this property.
SERVERPORT	The HTTP port used by the agent. The default value for this property is 80.
SECUREPORT	The HTTPS port used by the agent. The default value for this property is 443.
STANDDOWNPASSWORD	The global uninstall password. This is required if you want to uninstall the agent.
PROXYADDRESS	The URL (or IP) of your proxy.
PROXYPORT	The port used by the proxy.
PROXYUSERNAME	Login user for an authenticated proxy.



Property	Description
PROXYPASSWORD	Login password for an authenticated proxy.
GROUPLIST	Automatically add the agent to the defined group(s). Either the group name or distinguished name can be used. If the group name is used, the agent will be added to all of the groups with that name.

**Note:** Modifying the digitally signed MSI file will invalidate the digital signature assigned by Lumension. Depending upon your security settings, this may introduce security warnings and restrictions during agent installation.

## To Modify the LMAgent.msi File Using Microsoft Orca

### Prerequisites:

You must download Microsoft Orca before you can complete this procedure. Orca is installed from the Microsoft Windows Installer SDK which can be downloaded from [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca\\_exe.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp).

Complete this procedure to modify the MSI file using Microsoft Orca.

1. Install Microsoft Orca (or a similar MSI editor tool) to your management workstation.
2. Select **Start > Programs > Orca** to open Microsoft Orca.
3. Open the LMAgent.msi file that you copied to the network share you created.

**Step Result:** Orca displays the LMAgent.msi file.

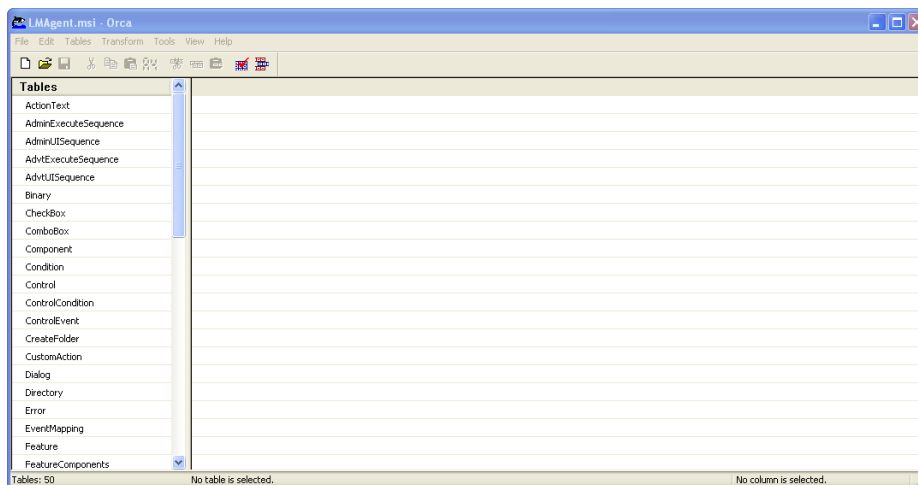


Figure 48: Orca Initial Display

4. Scroll through the **Tables** list and select the **Property** table.

**Step Result:** The **Rows** field populates with the rows associated with the Property table.



5. Right-click in the right window pane and select **Add Row**.

**Step Result:** The *Add Row* dialog box opens.

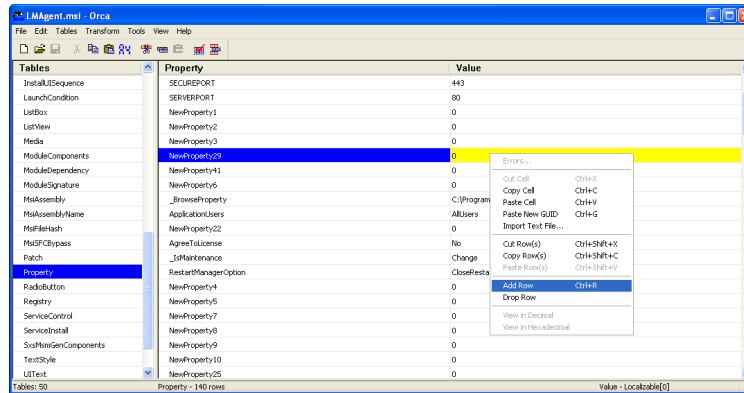


Figure 49: The Add Row dialog box

6. Enter `SERVERIPADDRESS` as the **Property Column** field.

7. Select **Value** and type your server IP address or the server's fully qualified domain name.

8. Click **OK**.

**Step Result:** The `SERVERIPADDRESS` row is added to the Property table.

9. To change the default a value for the `SERVERPORT` property (80) to another value, perform the following steps:

- a) Double click in the **Value** column of the `SERVERPORT` property in the Property table.

**Step Result:** The **Value** column for the `SERVERPORT` property becomes editable.

- b) Enter the value that you want to use for the `SERVERPORT` property.

- c) Press Enter.

**Step Result:** The value for the `SERVERPORT` property is changed in the Property table.

10. To change the default value for the `SECUREPORT` property (443) to another value, perform the following steps:

- a) Double click in the **Value** column of the `SECUREPORT` property in the Property table.

**Step Result:** The **Value** column for the `SECUREPORT` property becomes editable.

- b) Enter the value that you want to use for the `SECUREPORT` property.

- c) Press Enter.

**Step Result:** The value for the `SECUREPORT` property is changed in the Property table.

11. Right-click in the right window pane and select **Add Row**.

**Step Result:** The *Add Row* dialog box opens.

12. Enter `STANDDOWNPASSWORD` as the **Property Column** field.



13. Select **Value** and type the global agent uninstall password.

14. Click **OK**.

**Step Result:** The **STANDDOWNPASSWORD** row is added to the Property table.

15. If you are using a Proxy Server, add the necessary proxy entries as follows:

a) Right-click in the right window pane and select **Add Row**.

**Step Result:** The **Add Row** dialog box opens.

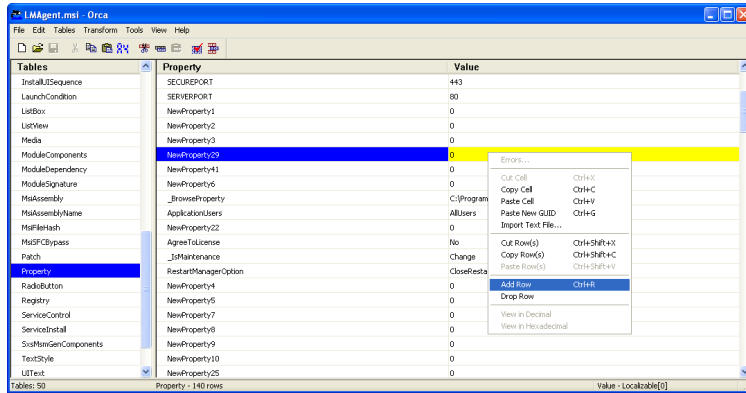


Figure 50: The Add Row dialog box

b) Enter PROXYADDRESS as the **Property Column** field.

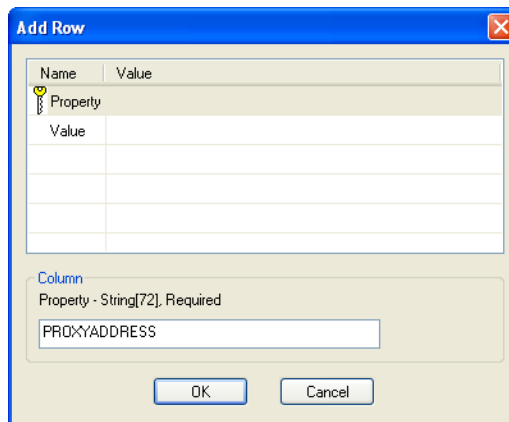


Figure 51: Add Row Property



- c) Select **Value** and type the URL or IP address of your proxy.

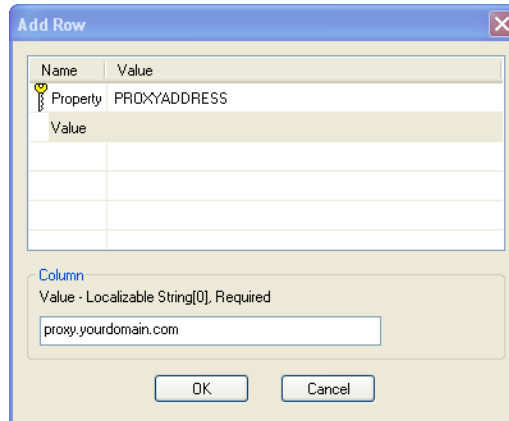


Figure 52: Add Row Value

- d) Click **OK**.

**Step Result:** The **PROXYADDRESS** row is added to the Property table.

- e) Add additional rows as needed for the following proxy entries:

Table 8: Proxy specific entries

Property	Value
PROXYPORT	The port used by the proxy.
PROXYUSERNAME (optional)	Authenticated proxy login user.
PROXYPASSWORD (optional)	Authenticated proxy login user's password.

16. To automatically add the agent to an existing group, add the following entry:

- a) Right-click in the right window pane and select **Add Row**.

**Step Result:** The **Add Row** dialog box opens.

- b) Enter **GROUPLIST** as the **Property Column** field.

- c) Select **Value** and enter the Group Names in the format: "GroupName1 | GroupName2 | GroupNameN".

**Step Result:** The **GROUPLIST** row is added to the Property table.

17. Click **Save**.

**Step Result:** Orca saves the changes to the **LMagent.msi** file.

18. Close Microsoft Orca.

**Result:** You can now use the **LMagent.msi** file to manually install the agent by browsing, from the target computer, to the network share you created and manually opening the **LMagent.msi** file.



## Creating an Organizational Unit

This procedure explains how to create an organizational unit.

Complete the following procedure to use organizational units classify and differentiate between installer files.

1. Click **Start > Administrative Tools > Active Directory Users and Computers**.

**Step Result:** The *Active Directory Users and Computers* management console opens.

2. Right-click the domain tree (mydomain.com) and select **New > Organizational Unit**.

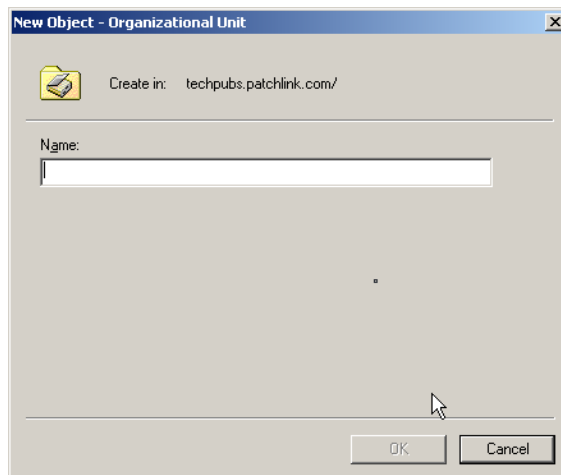


Figure 53: Create New OU

3. Assign a name (LumensionMSI) to your Organizational Unit (OU) and click **OK**.
4. Right-click the new OU and select **Properties**.

5. In the **Group Policy** tab, click **New** and assign a name (Install Windows Agent) to the new Group Policy.

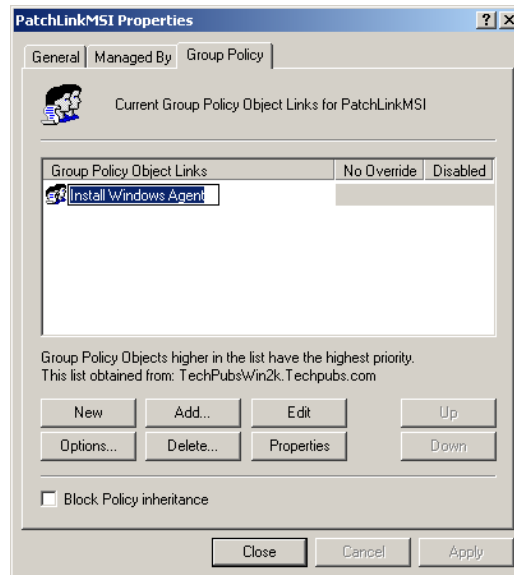


Figure 54: OU Group Policy tab

6. Select your new Group Policy and click **Edit**.  
**Step Result:** The *Group Policy Editor* opens.
7. Expand the **Software Settings** sub-branch of the **Computer Configuration** branch.



8. Right-click Software Installation and select **Properties** opening the *Software Installation Properties* window.

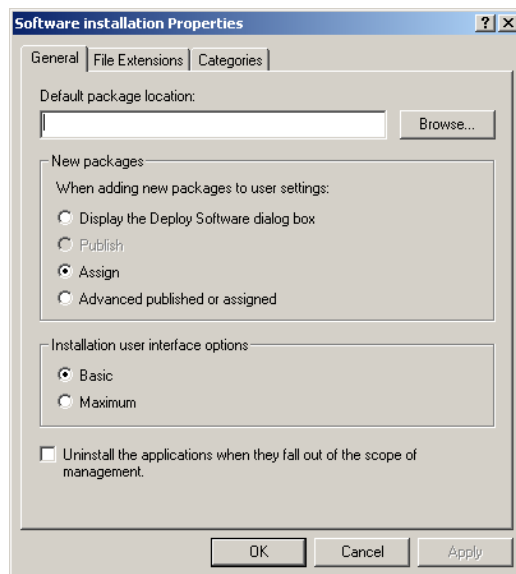


Figure 55: General tab

9. In the *General* tab, select the **Assign** radio button.
10. Select the **Uninstall the applications when they fall out of the scope of management** check box in the *General* tab (in the *Advanced* tab in Windows 2003).
11. Click **OK**.
12. Right-click **Software Installation** and select **New > Package**.



13. Browse to the shared folder you created and select the modified `PatchAgent.msi` or `LMAgent.msi` package.

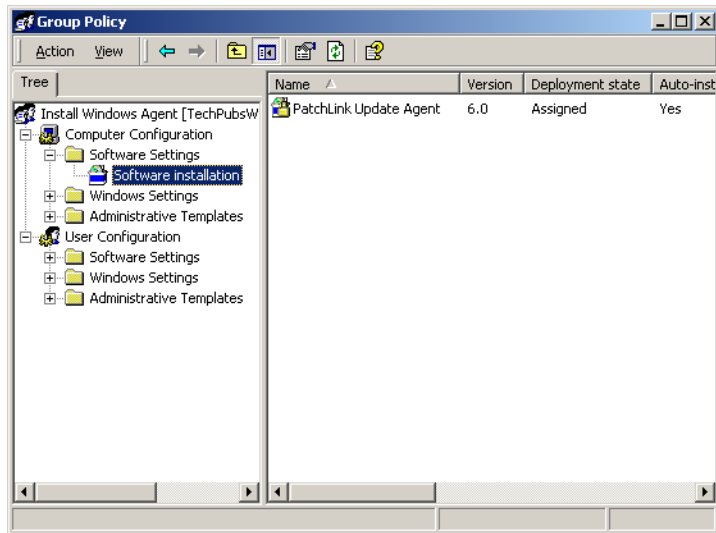


Figure 56: Group Policy

14. Close the *Group Policy* editor and click **Close**.

15. In the *Active Directory Users and Computers* management console, select the **Computers** branch of your domain tree (mydomain.com).



16. Select the computers to be added to the new OU.

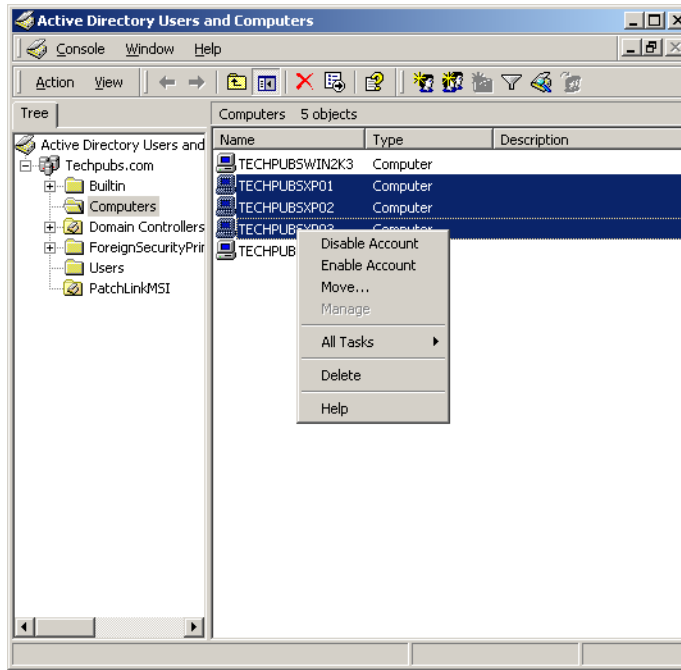


Figure 57: Add Computers to the OU

17. Right-click and select **Move** to add them to the OU.

18. Select your OU (LumensionMSI) from the *Move* window.

19. Close the *Active Directory Users and Computers* management console.

## Performing a Silent Install on Windows

In addition to the Lumension Patch and Remediation Server URL (or IP) and Serial Number, you can define a Proxy and Auto-Assign groups when performing a silent install using the Single Agent Windows MSI Installer:

1. Open a command prompt.
2. Define the host/server location and other settings using the following syntax:

To perform an install on a Windows 2000 endpoint with a proxy:

```
msiexec /i "C:\PatchAgent.msi" /qn HOST="http://myServer" SERIAL="88888888-88888888"
USEPROXY="1" PROXYURL="http://xxx.xxx.xxx" PROXYPORT="xxxx" PROXYUSER="ProxyUser"
PROXYPASS="ProxyPassword" GROUPLIST="GroupName1 | GroupName2 | GroupNameN"
```



To perform an install on a Windows 2000 endpoint without a proxy:

```
msiexec /i "C:\PatchAgent.msi" /qn HOST="http://myServer" SERIAL="88888888-88888888"
USEPROXY="0" GROUPLIST="GroupName1 | GroupName2 | GroupNameN"
```

**Note:** When performing a silent install on a Windows 2000 endpoint, the Patch Agent is installed.

To perform an install on a Windows XP or later endpoint with a proxy:

```
msiexec /i "C:\LMAgent.msi" /qn SERVERIPADDRESS="xxx.xxx.xxx.xxx" SERVERPORT="xxxx"
SECUREPORT="xxxx" PROXYADDRESS="xxx.xxx.xxx" PROXYPORT="xxxx" PROXYUSERNAME="ProxyUser"
PROXYPASSWORD="ProxyPassword" GROUPLIST="GroupName1 | GroupName2 | GroupNameN"
```

To perform an install on a Windows XP or later endpoint without a proxy:

```
msiexec /i "C:\LMAgent.msi" /qn SERVERIPADDRESS="xxx.xxx.xxx.xxx" SERVERPORT="xxxx"
SECUREPORT="xxxx" GROUPLIST="GroupName1 | GroupName2 | GroupNameN"
```

**Note:** When performing a silent install on a Windows XP or later endpoint, the Lumension Agent is installed.

## Command Line Descriptions for Windows 2000

The following commands can be used to perform a silent installation on endpoints running Windows 2000.

The user customized installer properties are defined in the following table:

Table 9: Description of Installation Properties

Property	Description
HOST	The URL (or IP address) of your Lumension Endpoint Management and Security Suite.
SERIAL	The serial number for your Lumension Endpoint Management and Security Suite.
USEPROXY	Indicates whether or not a proxy is used. 0=No, 1=Yes.
PROXYURL	The URL (or IP address) for your proxy.
PROXYPORT	The port your proxy server is using.
PROXYUSER	Login user for an authenticated proxy.
PROXYPASS	Login password for an authenticated proxy.
GROUPLIST	Automatically add the Agent to the defined group(s). Either the group name or distinguished name can be used. If the group name is used, the agent will be added to all of the groups with that name.

## Command Line Descriptions for Windows XP or Later

The following commands can be used to perform a silent installation on endpoints running Windows XP or later.

The user customized installer properties are defined in the following table:



Table 10: Description of Installation Properties

Property	Description
SERVERIPADDRESS	The IP address of your Lumension Endpoint Management and Security Suite.
SERVERPORT	The HTTP port for your Lumension Endpoint Management and Security Suite. If no value is specified, the default value (80) is used.
SECUREPORT	The SSL port for your Lumension Endpoint Management and Security Suite. If no value is specified, the default value (443) is used.
PROXYADDRESS	The IP address for your proxy server.
PROXYPORT	The port your proxy server is using.
PROXYUSERNAME	Login user for an authenticated proxy.
PROXYPASSWORD	Login password for an authenticated proxy.
GROUPLIST	Automatically add the Agent to the defined group(s). Either the group name or distinguished name can be used. If the group name is used, the agent will be added to all of the groups with that name.

## Performing a Silent Install on Linux/UNIX/Mac

In addition to the Lumension Endpoint Management and Security Suite URL (or IP) and Serial Number, you can define a Proxy and Auto-Assign groups when performing a silent install using the Single Agent Installer for Linux/UNIX/Mac:

1. Open a command prompt.
2. Define the host location, serial number, and other optional settings using the following syntax:

To perform a silent install with a proxy:

```
./install -silent -d "/user/local" -p "http://myServer" -sno "88888888-88888888" -proxy "http://myProxy" -port ## -g "GroupName1|GroupName2|GroupNameN"
```

To perform a silent install without a proxy:

```
./install -silent -d "/user/local" -p "http://myServer" -sno "88888888-88888888" -g "GroupName1|GroupName2|GroupNameN"
```

## Command Line Descriptions

The user customized installer properties are defined in the following table:

Table 11: Command Line Descriptions

Command	Description
-silent	Performs installation silently.



Command	Description
-d	The install directory.
-p	The URL (or IP) of your Lumension Endpoint Management and Security Suite.
-sno	The serial number of your Lumension Endpoint Management and Security Suite.
-proxy	The URL (or IP) of your proxy.
-port	The proxy port.
-g	Automatically add the Agent to the defined group(s). Either the group name or distinguished name can be used. If the group name is used, the agent will be added to all of the groups with that name.





# Configuring the Server and Endpoints for Agent Management Jobs

---

After installing Lumension Endpoint Management and Security Suite on a server, you must perform additional configuration on the endpoints that you want to manage so that agent management jobs will complete successfully.

## Configuring the Scanning System

---

The Lumension Endpoint Management and Security Suite server must be configured in the following manner so that you can run agent management jobs on your managed endpoints.

1. Click **Start > Run**.

2. Enter `regedit` in the **Open** field.

3. Click **OK**.

**Step Result:** The registry editor displays.

4. In the registry editor, navigate to `HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Control\Lsa`.

5. Verify that the value for the `lmcompatibilitylevel` registry key is set to 3.

---

**Note:** Under most network conditions, a setting of 3 is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to <http://support.microsoft.com/kb/239869>.

---

## Configuring Pre-Windows Vista Endpoint for Discovery

---

For pre-Windows Vista endpoints behind local firewalls, certain ports must be opened in order for them to be discovered. Pre-Windows Vista endpoints that do not have local firewalls in place will be discovered without performing this procedure.

Perform this task from the pre-Windows Vista endpoint you are configuring for discovery.

1. Select **Start > Control Panel**.

**Step Result:** *Control Panel* opens.



## 2. Double-click **Windows Firewall**.

**Step Result:** The *Windows Firewall* dialog opens.

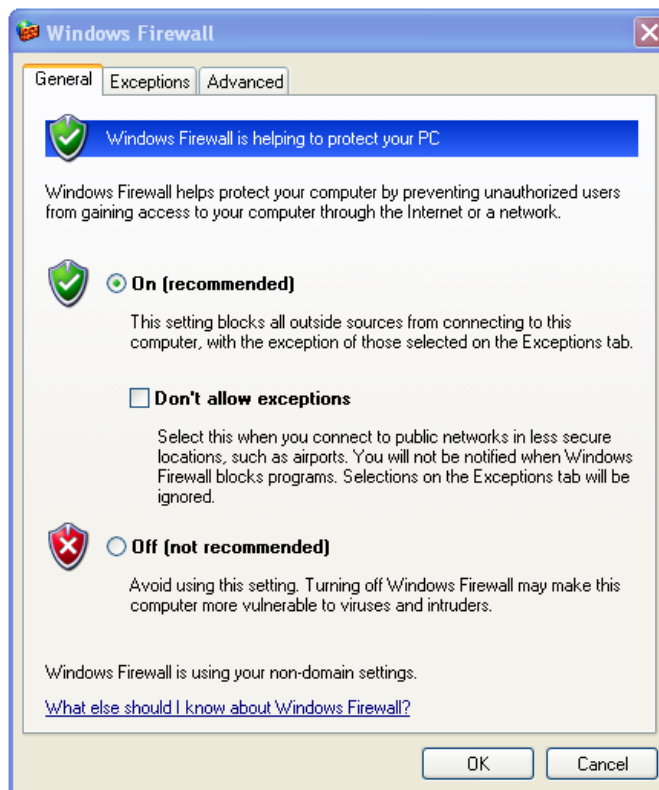


Figure 58: Windows Firewall Dialog



3. Select the *Exceptions* tab.

**Step Result:**

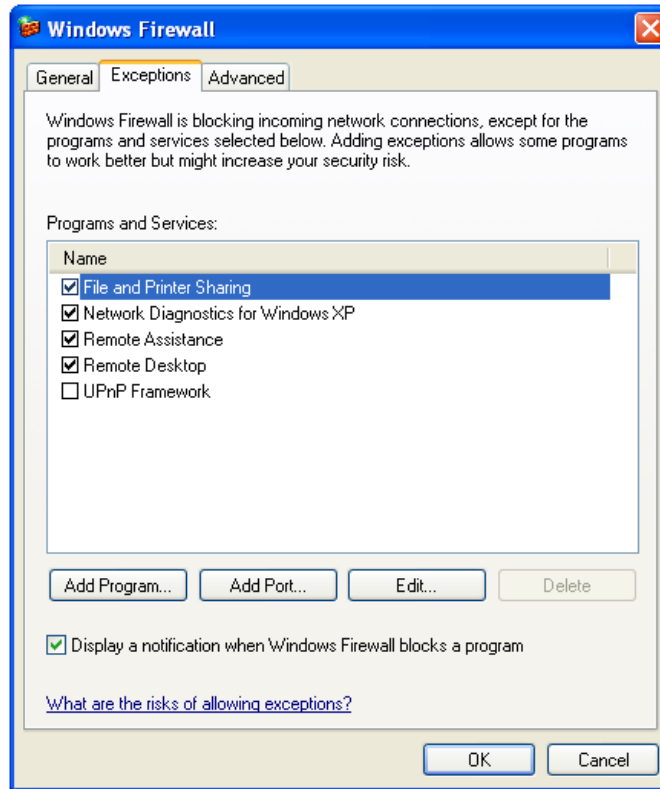


Figure 59: Exceptions Tab

4. Ensure the **File and Printer Sharing** check box is selected.

A **File and Printer Sharing** exception opens the following ports, which are essential for discovery and agent management.

- 445/TCP
- 139/TCP
- 135/UDP
- 137/UDP

5. Click **OK**.

**Result:** The endpoint can now be discovered during discovery scan jobs and agent management jobs.



## Configuring Endpoints for Agent Management Jobs (Pre-Windows Vista)

---

In order to successfully perform network-based assessments, you must complete the following configuration procedure on your managed endpoints after you install the Lumension Agent.

Configure your networked devices running pre-Windows Vista operating systems (Windows 2003, Windows XP, and so on) according the following procedure.

1. Select **Start > Run**.

2. Enter `cmd` in the **Open** field.

3. Click **OK**.

**Step Result:** The command prompt displays.

4. Type `net share` and press ENTER.

5. Verify that `C$` and `ADMIN$` are enabled and appear in the `Share name` column.

If they are not, type the following commands to enable these shares.

- `NET SHARE C$=C`
- `NET SHARE ADMIN$`

These commands enable the shares until the system reboots.

6. Select **Start > Control Panel**.

**Step Result:** *Control Panel* opens.



## 7. Double-click **Administrative Tools**.

**Step Result:** The *Administrative Tools* dialog opens.



Figure 60: Administrative Tools Dialog

## 8. Double-click **Services**.

**Step Result:** The *Services* dialog opens.

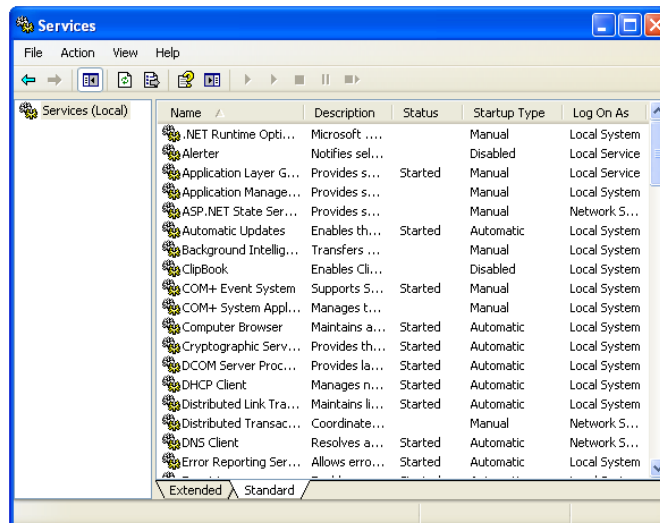


Figure 61: Services Dialog



9. Verify that the following services are running:

- DCOM Server Process Launcher
- Remote Procedure Call (RPC)
- Remote Registry
- Server
- Windows Firewall/Internet Connection Sharing
- Windows Management Instrumentation

If any of these services is not running, start it by completing the following substeps.

- a) Double-click the applicable service.
- b) Ensure the **General** tab is selected.
- c) From the **Startup type** list, select **Automatic**.
- d) Click **Start**.
- e) Click **OK**.

10. Select **Start > Run**.

11. Enter `gpedit.msc` in the **Open** field.

12. Click **OK**.

**Step Result:** The **Group Policy** dialog opens.

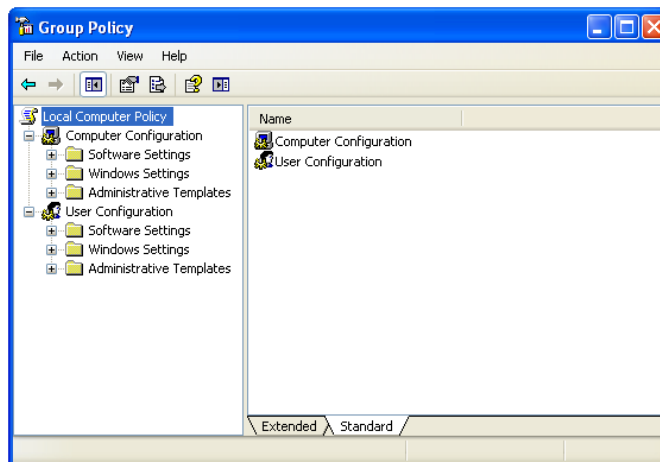


Figure 62: Services Dialog

13. Expand the directory tree structure to **Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile/Standard Profiles**.

The standard profile is enforced for workgroup members, and the domain profile is enforced for domain members. Edit both lists for consistency.



14. Edit the following settings according to the following table.

Value	Setting
Enable	<ul style="list-style-type: none"> <li>• <b>Windows Firewall: Allow file and printer sharing exception</b></li> <li>• <b>Windows Firewall: Allow remote administration exception</b></li> </ul>
Disable	<ul style="list-style-type: none"> <li>• <b>Windows Firewall: Do not allow exceptions</b></li> </ul>

To edit these settings, perform the following substeps.

- Right-click the applicable setting.
- Select **Properties**.
- Select the applicable option (**Enable** or **Disable**).
- If desired, define an IP range in the **Allow unsolicited incoming messages from** field.

**Note:** This substep is only applicable to the **Windows Firewall: Allow file and printer sharing exception** and **Windows Firewall: Allow remote administration exception** settings. To define a range, you may use the following syntax: \* (any IP address), 10.3.2.0/24 (specific Class C subnet), and localsubnet (for local subnetwork access only).

This input is not validated. By default, you should leave the box blank to allow any IP address.

- Click **OK**.

15. Select **Start > Run**.

16. Enter `regedit` in the **Open** field.

17. Click **OK**.

**Step Result:** The *Registry Editor* opens.

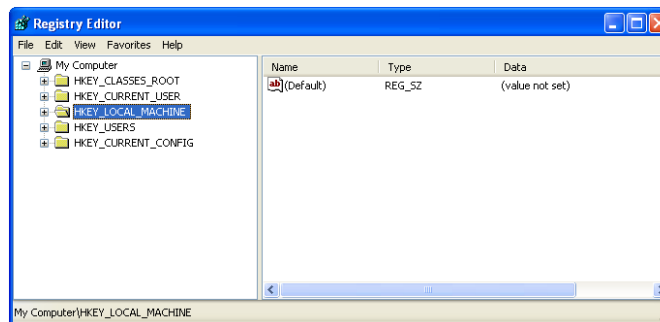


Figure 63: Services Dialog

18. From the directory tree structure, expand to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.



19. Verify that the value for the `lmcompatibilitylevel` registry key is set to 3 or 5.

If the key is not set to one of the following values, complete the following substeps.

---

**Note:** Under most network conditions, a setting of 3 or 5 is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to <http://support.microsoft.com/kb/239869>.

---

a) Double-click **lmcompatibilitylevel**.

**Step Result:** The *Edit DWORD Value* dialog opens.

b) In the **Value data** field, type 3 or 5 (unless another value is required).

c) Click **OK**.

20. Select **Start > Run**.

21. Enter `cmd` in the **Open** field.

22. Click **OK**.

**Step Result:** A command prompt displays.

23. Type `gpupdate /force` and press ENTER.

24. Select **Start > Control Panel**.

**Step Result:** *Control Panel* opens.

25. Double-click **Network Connections**.

**Step Result:** The *Network Connections* dialog opens.

26. Right-click your local area connection.



## 27. Select **Properties**.

**Step Result:** The *Local Area Connection Properties* dialog opens.

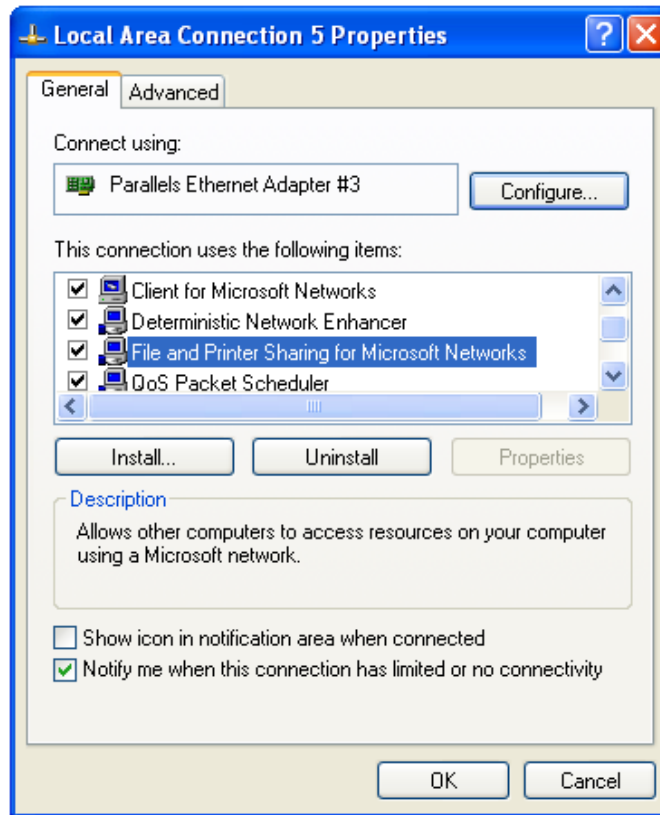


Figure 64: Local Area Connection Properties Dialog

28. Ensure the **File and Printer Sharing for Microsoft Networks** check box is selected.

29. Click **OK**.

## Configuring Post-Windows Vista Endpoints for Discovery

For Lumension Patch and Remediation to discover Windows Vista, Windows Server 2008, and Windows 7 endpoints during discovery scan jobs and agent management jobs, they must have both network discovery and file sharing enabled. Target endpoints without these features enabled will not be discovered.

Perform these steps on the applicable post-Windows Vista endpoint.

1. Select **Start > Control Panel**.

**Step Result:** *Control Panel* opens.



## 2. Open **Network and Sharing Center**.

**Step Result:** The *Network and Sharing Center* opens.

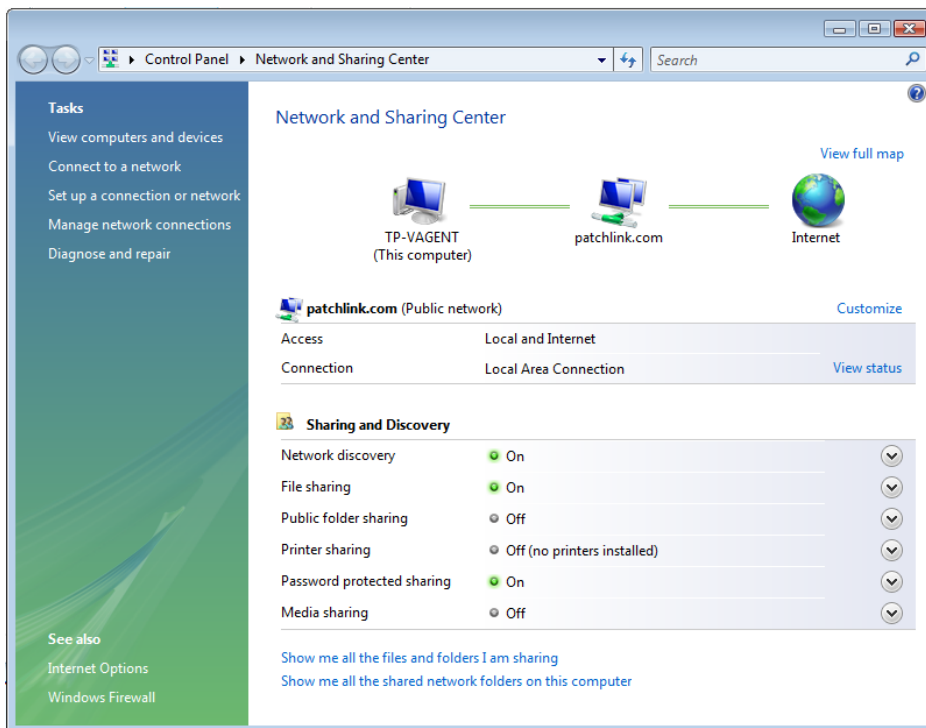


Figure 65: Network and Sharing Center

## 3. Ensure **Network discovery** is enabled.

## 4. Select **Start > Control Panel**.

**Step Result:** *Control Panel* opens.

## 5. Double-click **Windows Firewall**.

**Step Result:** The *Windows Firewall* dialog opens.



6. Click the **Change Settings** link.

**Step Result:** The *Windows Firewall Settings* dialog opens.

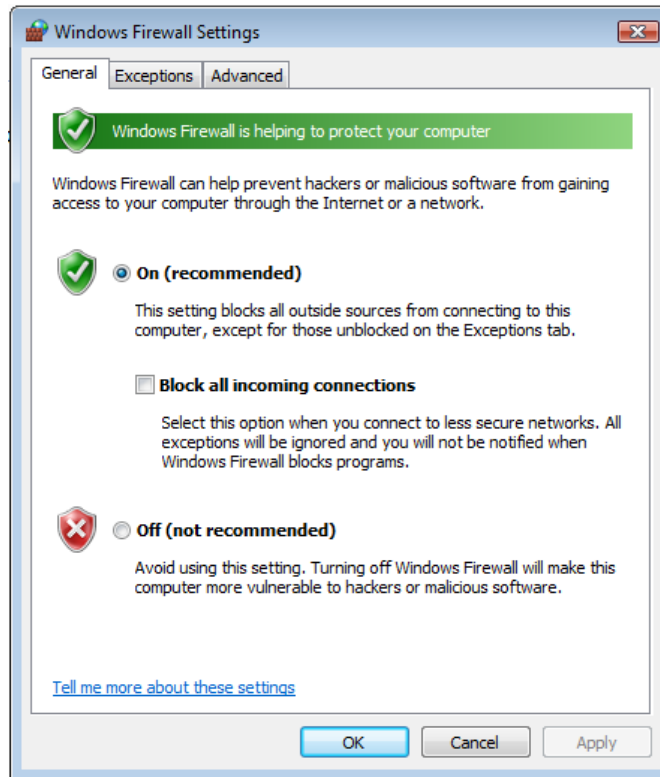


Figure 66: Windows Firewall Settings Dialog



7. Select the *Exceptions* tab.

**Step Result:**

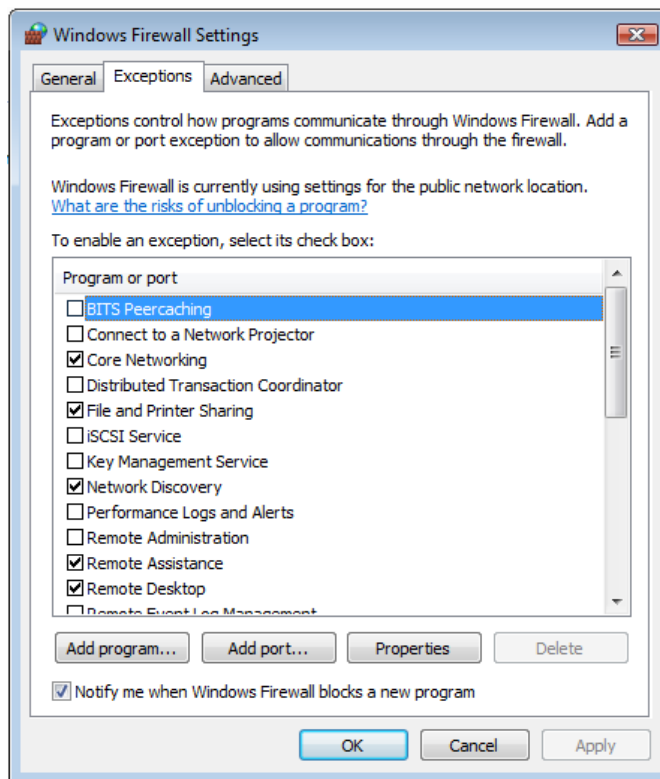


Figure 67: Exceptions Tab

8. Ensure the **File and Printer Sharing** check box is selected.

A **File and Printer Sharing** exception opens the following ports, which are essential for discovery and agent management.

- 445/TCP
- 139/TCP
- 135/UDP
- 137/UDP

9. Click **OK**.

**Result:** **Network discovery** and **File sharing** are enabled, and the ports are opened. The endpoint can now be discovered during discovery scan jobs and agent management jobs.



## Configuring Endpoints for Agent Management Jobs (Post-Windows Vista)

---

In order to successfully perform network-based assessments, you must complete the following configuration procedure on your managed endpoints before you install the agent.

### Prerequisites:

Complete *Configuring Post-Windows Vista Endpoints for Discovery* on page 99.

---

Configure your networked endpoints running Windows Vista, Windows Server 2008, or Windows 7 according to the following procedure.

**Note:** While executing some of the following steps, a *User Account Control* dialog may appear, to verify permission to continue with the requested action. Click **Continue** and proceed to the next step.

---

1. Select **Start > Run**.
2. Enter `cmd` in the **Open** field.
3. Click **OK**.

**Step Result:** The command prompt displays.

4. Type `net share` and press ENTER.
5. Verify that C\$ and ADMIN\$ are enabled and appear in the `Share name` column.

If they are not, type the following commands to enable these shares.

- `NET SHARE C$=C`
- `NET SHARE ADMIN$`

These commands enable the shares until the system reboots.

6. Select **Start > Control Panel**.

**Step Result:** *Control Panel* opens.



## 7. Double-click **Administrative Tools**.

**Step Result:** The *Administrative Tools* dialog opens.

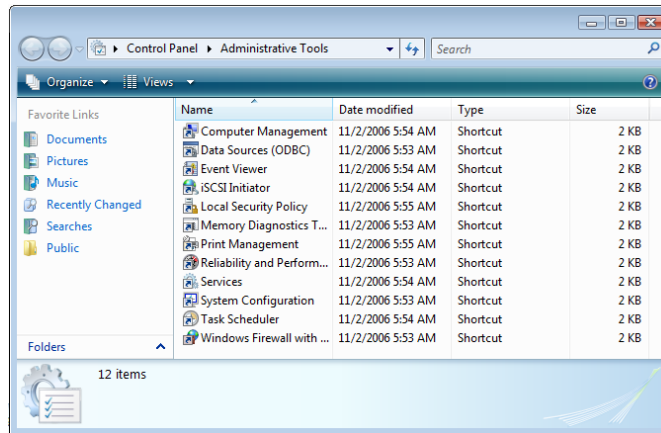


Figure 68: Administrative Tools Dialog

## 8. Double-click **Services**.

**Step Result:** The *Services* dialog opens.

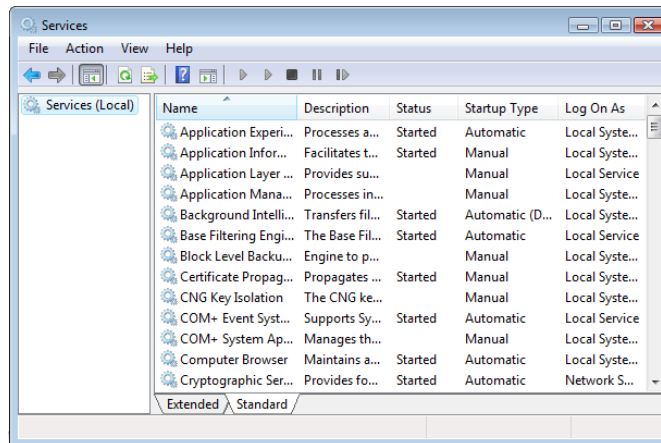


Figure 69: Services Dialog

9. Verify that the following services are running:

- DCOM Server Process Launcher
- Remote Procedure Call (RPC)
- Remote Registry
- Server
- Windows Firewall/Internet Connection Sharing
- Windows Management Instrumentation

If any of these services is not running, start it by completing the following substeps.

- a) Double-click the applicable service.
- b) Ensure the **General** tab is selected.
- c) From the **Startup type** list, select **Automatic**.
- d) Click **Start**.
- e) Click **OK**.

10. Select **Start > Run**.

11. Enter `gpedit.msc` in the **Open** field.

12. Click **OK**.

**Step Result:** The *Group Policy Object Editor* opens.

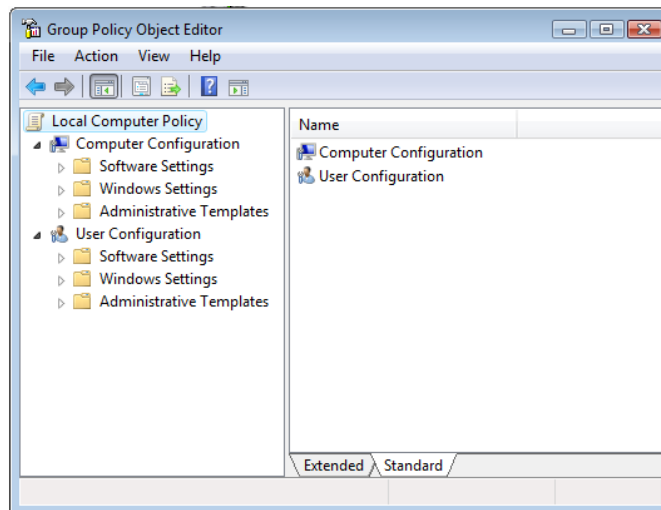


Figure 70: Group Policy Object Editor

13. Expand the directory tree structure to **Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile/Standard Profiles**.

The standard profile is enforced for workgroup members, and the domain profile is enforced for domain members. Edit both lists for consistency.



14. Edit the following settings according to the following table.

Value	Setting
Enable	<ul style="list-style-type: none"> <li>• <b>Windows Firewall: Allow file and printer sharing exception</b></li> <li>• <b>Windows Firewall: Allow remote administration exception</b></li> <li>• <b>Windows Firewall: Allow ICMP exceptions</b></li> </ul>
Disable	<ul style="list-style-type: none"> <li>• <b>Windows Firewall: Do not allow exceptions</b></li> </ul>

To edit these settings, perform the following substeps.

- Right-click the applicable setting.
- Select **Properties**.
- Select the applicable option (**Enable** or **Disable**).

---

**Note:** After enabling the **Windows Firewall: Allow ICMP exceptions** setting, select the **Allow inbound echo request** check box. Ensure all other check boxes are clear.

---

- If desired, define an IP range in the **Allow unsolicited incoming messages from** field.

---

**Note:** This substep is only applicable to the **Windows Firewall: Allow file and printer sharing exception** and **Windows Firewall: Allow remote administration exception** settings. To define a range, you may use the following syntax: \* (any IP address), 10.3.2.0/24 (specific Class C subnet), and localsubnet (for local subnetwork access only).

This input is not validated. By default, you should leave the box blank to allow any IP address.

---

- Click **OK**.

15. Select **Start > Run**.

16. Enter `regedit` in the **Open** field.

17. Click **OK**.

**Step Result:** The *Registry Editor* displays.

18. From the directory tree structure, expand to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.

19. Verify that the value for the `lmcompatibilitylevel` registry key is set to 3 or 5.

If the key is not set to one of the following values, complete the following substeps.

---

**Note:** Under most network conditions, a setting of 3 or 5 is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to <http://support.microsoft.com/kb/239869>.

---

- Double-click **lmcompatibilitylevel**.

**Step Result:** The *Edit DWORD Value* dialog opens.



- b) In the **Value data** field, type 3 or 5 (unless another value is required).
- c) Click **OK**.

20. Select **Start > Run**.

21. Enter `cmd` in the **Open** field.

22. Click **OK**.

**Step Result:** A command prompt displays.

23. Type `gpupdate /force` and press ENTER.

## Resolving Endpoint UAC Issues

On endpoints running Windows Vista or later operating systems, UAC security features are set to highly restrictive levels by default. These settings must be configured properly to ensure agent management job success.

When a post-Windows Vista endpoint is in this default UAC configuration, agent management jobs fail with an `access denied` error.

Use one of two methods to resolve this issue:

### Add a domain account

Adding a domain account to the applicable endpoint's local administrator's group will typically resolve the issue. To use this method, add the endpoint to a domain (provided it isn't already added), and then add a domain user to the endpoint's local administrator group. Running an agent management job configured to use this domain account's credentials will allow the job to complete successfully.

**Note:** The domain account added to the local administrator's group *must* be an individual domain account; you cannot add a domain group.

### Set a Registry Value

If the user of a local administrative account is desired or required, you can set a registry value to resolve this issue.

Create a `DWORD` registry value named *LocalAccountTokenFilterPolicy* in the `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` registry hive. Set its value to *1*.

No reboot is required. This method allows a local administrative account to successfully run agent management jobs.

**Note:** For additional information about this method, refer to <http://support.microsoft.com/kb/942817>.

## Troubleshooting Agent Management Jobs

If agent managements are not completing successfully, additional configuration may be required.

If the Lumension Endpoint Management and Security Suite server or an applicable network endpoint has lost its trust relationship with the domain, agent management jobs will fail with an error of `access denied`.



To verify if this issue is causing agent management job failure, ensure that the Lumension EMSS server can connect to the applicable endpoints C\$, and that the applicable endpoints can connect to the server's C\$.

To verify these connections, type the following command from the applicable endpoint or server prompt: `\EndpointIPAddress\C$`.

If the following system output results from the command, your endpoint or server has lost its trust relationship with the domain: `The trust relationship between this workstation and the primary domain failed.`

To resolve this issue, remove the applicable server or endpoint from the domain, and then add it back. This process forces the domain to refresh the endpoint password. The endpoint password prompts users for resetting at scheduled intervals according to its security settings.

To disable password changes, complete [Disabling Password Changes](#) on page 108.

## Disabling Password Changes

To disable password changes, create a registry key for the applicable endpoint.

Perform this task from the applicable endpoint.

1. Select **Start > Run**.

**Step Result:** The *Run* dialog opens.

2. Type `regedit` in the **Open** field.

3. Click **OK**.

**Step Result:** The *Registry Editor* opens.

4. Expand the directory tree structure to `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`.

5. Right-click `DisablePasswordChange`.

6. Select **Modify**.

**Step Result:** The *Edit DWORD Value* dialog opens.

7. In the **Value data** field, type `1`.

8. Click **OK**.

**Result:** The key value is updated. User profile passwords can no longer be edited on the applicable endpoint.

