



Server Install Guide

Lumension Endpoint Management
and Security Suite 7.0 SP1



Notices

Version Information

Lumension Endpoint Management and Security Suite Server Install Guide - Lumension Endpoint Management and Security Suite Version 7.0SP1 - Released: April 2010

Document Number: 02_202_7.0SP1_101201056

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

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 to tell us what you like best, what you like least, and to report any inaccuracies.



Table of Contents

Preface: About This Document.....	7
Typographical Conventions.....	7
Contacting Lumension.....	7
Chapter 1: System Requirements.....	11
Minimum Hardware Requirements.....	11
Supported Operating Systems.....	12
Supported Database Servers.....	12
Other Software Requirements.....	13
Recommended Configuration.....	13
Lumension Endpoint Management and Security Suite Server Components.....	13
Recommended Server Configuration (Both Components on One Server).....	13
Recommended Server Configuration (Components on Separate Servers).....	14
Recommended Agent Configuration.....	16
Recommended Server Configuration Information.....	17
Server Installation Checklist.....	17
Server Upgrade Checklist.....	18
Chapter 2: Installing Lumension Endpoint Management and Security Suite.....	21
Downloading Lumension Endpoint Management and Security Suite.....	22
About SQL Server Instance Location.....	22
Defining the Web Client Account and Service Account.....	22
Selecting an Installation Method.....	23
Installing Using a New SQL Server Instance.....	24
Installing Using an Existing SQL Server Instance (Either Locally or Remotely).....	33
Installing Using a Remote SQL Server Instance (with no Local Instance).....	46
Installing Lumension Endpoint Management and Security Suite (Separate Lumension EMSS and SQL Server Admins).....	58
Beginning Installation (Part I).....	59
Creating Components on SQL Server (Part II).....	66
Completing Installation (Part III).....	68
Logging In to Lumension Endpoint Management and Security Suite.....	73
Setting Up Lumension Endpoint Management and Security Suite.....	74
Appendix A: Configuring Remote SQL Server Instances.....	79



Creating Remote Accounts.....	79
Configuring SQL Server to Accept Remote Connections.....	82
Configuring Windows Firewall for SQL Server Instance Access.....	84
Appendix B: Configuring Your Server to use SSL.....	85
Configuring Windows Server 2003 for SSL.....	85
Configuring Windows Server 2008 for SSL.....	93
Appendix C: Upgrading from Previous Installations.....	99
Upgrading Lumension Endpoint Management and Security Suite.....	99
Upgrading from Lumension Endpoint Management and Security Suite 7.0.....	101
Upgrading from Lumension Patch and Remediation 6.4 SP2.....	104
Installing Cleanly Over an Existing Installation.....	113
Appendix D: Installation Checklist.....	115
Server Installation Checklist.....	115
Server Upgrade Checklist.....	116



Preface

About This Document

This Server 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
bold	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

<p>Global Headquarters</p> <p>8660 East Hartford Drive Suite 300 Scottsdale, AZ 85255 United States of America Phone: +1 888 725 7828 Fax: +1 480 970 6323</p>	<p>European Headquarters</p> <p>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>
---	---



<p>United Kingdom Office</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: patchlink.emea@lumension.com</p>	<p>Lumension Security Ireland Limited</p> <p>Galway Technology Centre Unit Number 20 Mervue Industrial Estate County of Galway Ireland Phone: +353 91 730858</p>
<p>Germany Office</p> <p>Wazmannstrasse 22 82140 Olching (Munich) Germany Phone: +49 (0) 8142 400800 Fax: +49 (0) 8142 400530</p>	<p>Spain Office</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: patchlink.emea@lumension.com</p>
<p>US Federal Solutions Group</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: patchlink.federalsales@lumension.com</p>	<p>France Office</p> <p>Phone: +33 611 821 535</p>
<p>Singapore Office</p> <p>9 Raffles Place Level 58, Republic Plaza Singapore 048619 Phone: +65 6823 1533 Fax: +65 6823 1377 E-mail: patchlink.apac@lumension.com</p>	<p>Australia Office</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: patchlink.apac@lumension.com</p>



<p>North America Sales</p> <p>Phone: +1 480 970 1025 (option 1) E-mail: sales@lumension.com</p>	<p>International Sales</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: sales@lumension.com or patchlink.apac@lumension.com (APAC) or patchlink.emea@lumension.com (EMEA)</p>
<p>Lumension Vulnerability Management Technical Support</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: patchlink.support@lumension.com (US) patchlink.apac.support@lumension.com (APAC) patchlink.emea.support@lumension.com (EMEA)</p>	<p>Lumension Endpoint Security Technical Support</p> <p>Phone: +1 877 713 8600 (US Toll Free) +44 800 012 1869 (UK Toll Free) +353 9142 2999 (EMEA) E-mail: endpoint.support@lumension.com</p>
<p>Note: For additional contact information, please visit the Contact Lumension page at http://www.lumension.com/contactus.jsp.</p>	





Chapter

1

System Requirements

In this chapter:

- Minimum Hardware Requirements
- Supported Operating Systems
- Supported Database Servers
- Other Software Requirements
- Recommended Configuration
- Server Installation Checklist
- Server Upgrade Checklist

Before installing Lumension Endpoint Management and Security Suite (Lumension EMSS) on a server, ensure that the server meets the minimum system requirements. If your target server does not meet the system requirements, Lumension EMSS will not perform optimally, or may not install.

These requirements are only the minimum. For superior performance, install Lumension EMSS on a server that exceeds the minimum system requirements.

Minimum Hardware Requirements

The Lumension Endpoint Management and Security Suite server must meet or exceed the specified hardware requirements.

- 1.5 GHz multi-core processor
- 1 GB RAM
- 36 GB of available disk space (4 GB for application, 32 GB for storage cache)

Note: Per version of operating systems that are not Windows-based, the storage cache requires an additional 10 GB of disk space.



Supported Operating Systems

The Lumension Endpoint Management and Security Suite server is supported on a number of Microsoft Windows operating systems.

- Windows Server 2003, Web Edition with SP2 or later (x86)
- Windows Server 2003, Standard Edition with SP2 or later (x86)
- Windows Server 2003, Enterprise Edition with SP2 or later (x86)
- Windows Server 2003 R2, Standard Edition with SP2 or later (x86)
- Windows Server 2003 R2, Enterprise Edition with SP2 or later (x86)
- Windows Server 2008, Web Edition with SP2 or later (x86/x64)
- Windows Server 2008, Standard Edition with SP2 or later (x86/x64)
- Windows Server 2008, Enterprise Edition with SP2 or later (x86/x64)
- Windows Server 2008 R2, Standard Edition (with or without Hyper-V)
- Windows Server 2008 R2, Enterprise Edition (with or without Hyper-V)
- Windows Web Server 2008 R2

Important: Lumension Endpoint Management and Security Suite must be installed on an English operating system using an English locale (en-US, en-UK, en-CA, and so on) in its default configuration.

Supported Database Servers

The Lumension Endpoint Management and Security Suite (Lumension EMSS) server is supported by multiple versions of Microsoft SQL Server database.

- SQL Server 2005, Express Edition with SP3 (x86)
- SQL Server 2005, Standard Edition with SP3 (x86)
- SQL Server 2005, Enterprise Edition with SP3 (x86)
- SQL Server 2008, Express Edition (x86)
- SQL Server 2008, Standard Edition (x86/x64)
- SQL Server 2008, Enterprise Edition (x86/x64)

Tip: Lumension recommends using the latest service pack available for your instance of SQL Server.

Note: If an instance of SQL Server is not present on your target server or you do not intend to use a remote SQL Server configuration, SQL Server 2008, Express Edition with SP1 is installed with the Lumension EMSS server. SQL Server 2008 Express Edition is only available in 32-bit architecture. If installing to a 64-bit server, Lumension recommends installing using a supported preexisting instance of SQL Server that supports 64-bit architecture.



Supported database servers can be installed in the following locations relative to the Lumension EMSS server.

- Locally in a named instance installed by the Lumension EMSS installation.
- Locally in a preexisting named or default instance.
- Remotely in a preexisting named or default instance.

Note: When installing Lumension EMSS using an existing SQL Server instance, the instance collation must be set to one of the following values:

- SQL_Latin1_General_CP1_CI_AS
 - Latin1_General_CI_AS
-

Other Software Requirements

The Lumension Endpoint Management and Security Suite server requires additional software.

- Internet Information Services (IIS) 6.0 or later.
- Microsoft Internet Explorer 7.0 or later or Mozilla Firefox 3.0 or later.

Recommended Configuration

Depending on the number of endpoints in your network environment, Lumension recommends different system and bandwidth settings for your Lumension Endpoint Management and Security Suite Server and network. As the number of managed endpoints in your network increases, so do server and network requirements.

Lumension Endpoint Management and Security Suite Server Components

The Lumension Endpoint Management and Security Suite (Lumension EMSS) server contains the following components: the Lumension EMSS Application Server and the Lumension EMSS Database Server.

These components may share a physical server or operate on separate physical servers.

The following list describes each server component.

Lumension EMSS Application Server	This server is responsible for Web site, replication services, and endpoint distribution services.
Lumension EMSS Database Server	This server is responsible for SQL database and stored procedures.

Recommended Server Configuration (Both Components on One Server)

For optimal performance, your Lumension EMSS server should meet the hardware recommendations that increase according to the number of managed endpoints in your network.

The following table lists the recommended server configuration when both components are installed on one physical server.



Table 1: Lumension EMSS Application and Database Server (All Components on One Server)

Endpoint Count		>250	>1,000	>2,500	>5,000	>10,000
Software	Operating Systems	Windows 2003/2008 Web	Windows 2003/2008 Web	Windows 2003/2008 Standard	Windows 2003/2008 Standard	Windows 2003/2008 Standard
	Architecture	x86	x86	x86	x86	x64
	Database Server	SQL 2005/2008 Express	SQL 2005/2008 Express	SQL 2005/2008 Express	SQL 2005/2008 Express	SQL 2005/2008 Standard
Hardware	CPU (Speed)	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Quad Core 2.0 GHz or greater
	# CPU's	1	1	1	1	1
	RAM (GB)	1	1	2	4	8
	HDD Size/Speed	72 GB/7.2K RPM	144 GB/7.2K RPM	250 GB/7.2K RPM	250 GB/7.2K RPM	250 GB/10K RPM
	# Hard Drives	2	2	2	4	4
	Network	100 Mbps	100 Mbps	1000 Mbps	1000 Mbps	1000 Mbps
	Disk Array	RAID 1	RAID 1	RAID 1	RAID 10	RAID 10

Note: If managing more than 10,000 endpoints, contact [Lumension Support \(http://support.lumension.com\)](http://support.lumension.com) for a recommended configuration.

Recommended Server Configuration (Components on Separate Servers)

When the Application Server and Database Server are installed on two physical servers, each server's recommended hardware requirements increase according to the number of managed endpoints in your network.

Review the following information when the components are installed on separate servers.

The following table lists the recommended configuration for the Lumension EMSS Application Server.

Table 2: Lumension EMSS Application Server

Endpoint Count		>250	>1,000	>2,500	>5,000	>10,000
Software	Operating Systems	Windows 2003/2008 Web	Windows 2003/2008 Web	Windows 2003/2008 Standard	Windows 2003/2008 Standard	Windows 2003/2008 Standard
	Architecture	x86	x86	x86	x86	x64

Endpoint Count		>250	>1,000	>2,500	>5,000	>10,000
Hardware	CPU (Speed)	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Quad Core 2.0 GHz or greater
	# CPU's	1	1	1	1	1
	RAM (GB)	1	1	2	2	4
	HDD Size/ Speed	72 GB/7.2K RPM	144 GB/7.2K RPM	250 GB/7.2K RPM	250 GB/7.2K RPM	250 GB/10K RPM
	# Hard Drives	2	2	2	4	4
	Network	100 Mbps	100 Mbps	1000 Mbps	1000 Mbps	1000 Mbps
	Disk Array	RAID 1	RAID 1	RAID 1	RAID 10	RAID 10

The following table lists the recommended configuration for the Lumension EMSS Database Server.

Table 3: Lumension EMSS Database Server

Endpoint Count		>250	>1,000	>2,500	>5,000	>10,000
Software	Architecture	x86	x86	x86	x86	x64
	Database Server	SQL 2005/2008 Express	SQL 2005/2008 Express	SQL 2005/2008 Express	SQL 2005/2008 Express	SQL 2005/2008 Standard
Hardware	CPU (Speed)	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Dual Core 2.0 GHz or greater	Quad Core 2.0 GHz or greater
	# CPU's	1	1	1	1	1
	RAM (GB)	1	1	2	4	8
	HDD Size/ Speed	72 GB/7.2K RPM	144 GB/7.2K RPM	250 GB/7.2K RPM	250 GB/7.2K RPM	250 GB/10K RPM
	# Hard Drives	2	2	2	4	4
	Network	100 Mbps	100 Mbps	1000 Mbps	1000 Mbps	1000 Mbps



Endpoint Count		>250	>1,000	>2,500	>5,000	>10,000
	Disk Array	RAID 1	RAID 1	RAID 1	RAID 10	RAID 10

Note: If managing more than 10,000 endpoints, contact *Lumension Support* (<http://support.lumension.com>) for a recommended configuration.

Recommended Agent Configuration

Lumension recommends configuring server-to-agent communication according to the number of managed endpoints in your network.

Recommended Agent Configurations

After installing Lumension Endpoint Management and Security Suite and agents, Lumension recommends configuring agent settings according to your network size.

Lumension recommends the following settings for the Patch Agent. Agent settings are edited within the Lumension Endpoint Management and Security Suite Web console.

Table 4: Application Settings: Patch Agent

Endpoint Count	>250	>1,000	>2,500	>5,000	>10,000
Communication Interval	30 Min	30 Min	30 Min	60 Min	90 Min
Concurrent Deployment Limit (CDL) - Global	1000	1000	1000	2500	5000
CDL - Reboot	200	200	200	250	500
CDL - DAU	600	600	600	750	800
CDL - MB	600	600	600	750	800

Lumension recommends the following settings for the Lumension EMSS Agent.

Table 5: Application Settings: Lumension EMSS Agent

Endpoint Count	>250	>1,000	>2,500	>5,000	>10,000
Send interval (sec)	2	3	4	5	6
Receive interval (sec)	0	0	0	0	0
Timeout interval	12 hours	12 hours	12 hours	12 hours	12 hours



Endpoint Count	>250	>1,000	>2,500	>5,000	>10,000
Heartbeat interval	30 min	30 min	30 min	60 min	90 min

Note: If managing more than 10,000 endpoints, contact *Lumension Support* (<http://support.lumension.com>) for a recommended configuration.

Recommended Server Configuration Information

Additional server configuration may be needed for physical memory limits, SQL Server system databases, and storage practices.

- For additional information about the physical memory limits for Windows releases, refer to *Memory Limits for Windows Releases* ([http://msdn.microsoft.com/en-us/library/aa366778\(VS.85\).aspx#physical_memory_limits_windows_server_2003](http://msdn.microsoft.com/en-us/library/aa366778(VS.85).aspx#physical_memory_limits_windows_server_2003)).
- For additional information about moving SQL Server 2008 system databases, refer to *Moving System Databases* ([http://msdn.microsoft.com/en-us/library/aa366778\(VS.85\).aspx#physical_memory_limits_windows_server_2003](http://msdn.microsoft.com/en-us/library/aa366778(VS.85).aspx#physical_memory_limits_windows_server_2003)).
- For additional information about Microsoft's top ten best practices for storage, refer to *Storage Top Ten Best Practices* (<http://technet.microsoft.com/en-us/library/cc966534.aspx>).

Server Installation Checklist

This checklist itemizes the information you will need and tasks you will need to complete when installing the Lumension Endpoint Management and Security Suite (Lumension EMSS) server.

Prior to installing Lumension EMSS, you must gather and confirm the following information:

- Your target computer meets or exceeds the requirements defined in *System Requirements* on page 11.
- Your server is *not* a Domain Controller.
- Internet Information Services (IIS) is installed and running. If necessary refer to one of the following links for details about IIS:
 - *How to Configure a Computer Running Windows Server 2003 as a Web Server* (<http://support.microsoft.com/kb/324742>)
 - *Install IIS 7 on Windows Server 2008* (<http://learn.iis.net/page.aspx/29/installing-iis-70-on-windows-server-2008>)
- All required service packs have been installed, as defined in *System Requirements* on page 11.
- If your server is a member of a domain, only the default security policies are in effect.
- Your server DNS host name is: _____



- Your local SMTP mail host name is: _____
- Your Lumension EMSS serial number is: _____ - _____
- Your target system is connected to the Internet.
- If you are using SSL, a valid SSL Web certificate has been obtained.

Note: If you are using SSL, you need to obtain a valid Web certificate, from a trust provider such as Verisign Inc. (www.verisign.com) or Entrust (www.entrust.com), prior to installing Lumension EMSS.

- If you are using SSL, you have started the first portion of one of the following topics based on your operating system (the second portion is completed after installation).
 - [Configuring Windows Server 2003 for SSL](#) on page 85
 - [Configuring Windows Server 2008 for SSL](#) on page 93
- If a proxy server will be used, you know the proxy server's name, IP address, port, user name, and password.
 - Name: _____
 - IP address: ____ - ____ - ____ - ____
 - Port: _____
 - User name: _____
 - Password: _____
- If you are using a preexisting instance of SQL Server, the instance is set to one of the following collation values:
 - SQL_Latin1_General_CP1_CI_AS
 - Latin1_General_CI_AS
- If you are using a remote instance of SQL Server, the server hosting the instance is set to an English locale.
- If you are using a remote SQL instance, the instance is configured to accept remote connections. For additional information refer to [Configuring SQL Server to Accept Remote Connections](#) on page 82.
- If you are using a remote SQL instance, and that instance is behind a firewall, the firewall is configured to allow the Lumension EMSS server access. For additional information, refer to [Configuring Windows Firewall for SQL Server Instance Access](#) on page 84.

Server Upgrade Checklist

This checklist itemizes the information you will need and tasks you will need to complete when upgrading the Lumension Endpoint Management and Security Suite (Lumension EMSS) server. The information you will gather varies according to your upgrade scenario.

Before upgrading Lumension EMSS 7.0 or Lumension Patch and Remediation 6.4 SP2 to Lumension EMSS 7.0 SP1, you must gather and confirm the following information for both upgrade types (upgrade and fresh install):



- Your target computer meets or exceeds the requirements defined in *System Requirements* on page 11.
- Your target server has either Lumension Endpoint Management and Security Suite 7.0 or Lumension Patch and Remediation 6.4 SP2 installed.
- Your server is *not* a Domain Controller.
- Internet Information Services (IIS) is installed and running. If necessary refer to one of the following links for details about IIS:
 - [How to Configure a Computer Running Windows Server 2003 as a Web Server \(http://support.microsoft.com/kb/324742\)](http://support.microsoft.com/kb/324742)
 - [Install IIS 7 on Windows Server 2008 \(http://learn.iis.net/page.aspx/29/installing-iis-70-on-windows-server-2008\)](http://learn.iis.net/page.aspx/29/installing-iis-70-on-windows-server-2008)
- All required service packs have been installed, as defined in *System Requirements* on page 11.
- If your server is a member of a domain, only the default security policies are in effect.
- Your server DNS host name is: _____
- Your local SMTP mail host name is: _____

Prior to upgrading Lumension EMSS 7.0 or Lumension Patch and Remediation 6.4 SP2 to Lumension EMSS 7.0 SP1 via a fresh installation, you must gather and confirm the additional following information.

- Your Lumension EMSS serial number is: _____ - _____
- Your target system is connected to the Internet.
- If you are using SSL, a valid SSL Web certificate has been obtained.

Note: If you are using SSL, you need to obtain a valid Web certificate, from a trust provider such as Verisign Inc. (www.verisign.com) or Entrust (www.entrust.com), prior to installing Lumension EMSS.

- If you are using SSL, you have started the first portion of one of the following topics based on your operating system (the second portion is completed after installation).
 - [Configuring Windows Server 2003 for SSL](#) on page 85
 - [Configuring Windows Server 2008 for SSL](#) on page 93
- If a proxy server will be used, you know the proxy server's name, IP address, port, user name, and password.
 - Name: _____
 - IP address: ____ - ____ - ____ - ____
 - Port: _____
 - User name: _____
 - Password: _____



- If you are using a remote instance of SQL Server, the server hosting the instance is set to an English locale.
- If you are using a preexisting instance of SQL Server, the instance is set to one of the following collation values:
 - SQL_Latin1_General_CP1_CI_AS
 - Latin1_General_CI_AS
- If you are using a remote SQL instance, the instance is configured to accept remote connections. For additional information refer to [Configuring SQL Server to Accept Remote Connections](#) on page 82.
- If you are using a remote SQL instance, and that instance is behind a firewall, the firewall is configured to allow the Lumension EMSS server access. For additional information, refer to [Configuring Windows Firewall for SQL Server Instance Access](#) on page 84.



Chapter

2

Installing Lumension Endpoint Management and Security Suite

In this chapter:

- Downloading Lumension Endpoint Management and Security Suite
- About SQL Server Instance Location
- Defining the Web Client Account and Service Account
- Selecting an Installation Method
- Installing Using a New SQL Server Instance
- Installing Using an Existing SQL Server Instance (Either Locally or Remotely)
- Installing Using a Remote SQL Server Instance (with no Local Instance)
- Installing Lumension Endpoint Management and Security Suite (Separate Lumension EMSS and SQL Server Admins)
- Logging In to Lumension Endpoint Management and Security Suite
- Setting Up Lumension Endpoint Management and Security Suite

Complete the Lumension Endpoint Management and Security Suite (Lumension EMSS) installation method that suits best your network environment.

Before installation, download the latest Lumension Endpoint Management and Security Suite installer.

There is an installation procedure for all Lumension EMSS installation scenarios.

After installation, complete any additional procedures associated with the installation procedure you completed.



Downloading Lumension Endpoint Management and Security Suite

When you purchase Lumension Endpoint Management and Security Suite (Lumension EMSS), you receive no physical media. Rather, you download it from the company Web site.

Download Lumension EMSS from the [Lumension Customer Portal](https://portal.lumension.com) (<https://portal.lumension.com>).

1. Open your Web browser.
2. Browse to the [Lumension Customer Portal](https://portal.lumension.com) (<https://portal.lumension.com>).
3. Browse to and download the most recent version of the Lumension EMSS installer to your desired location.

After Completing This Task:

Complete the installation procedure applicable to your network environment. For additional information refer to [Selecting an Installation Method](#) on page 23.

About SQL Server Instance Location

Lumension Endpoint Management and Security Suite (Lumension EMSS) requires an instance of Microsoft SQL Server to store system data values. You can install this SQL Server instance on your target Lumension EMSS server or a remote server.

Local SQL Server Instance	A SQL Server instance can be installed on the same server as Lumension EMSS. When using a local SQL Server instance, you can use either a named or default instance of SQL Server that is preexisting, or you can use a new instance of SQL Server (which is set up by the Lumension EMSS installer).
Remote SQL Server Instance	A SQL Server instance can be installed on a different server than Lumension EMSS, and Lumension EMSS can then access that remote instance. If you elect to use a remote SQL Server instance, you must direct Lumension EMSS toward the remote instance during Lumension EMSS installation. However, before directing Lumension EMSS to the remote instance, you must configure that instance to accept remote connections. For additional information refer to Configuring SQL Server to Accept Remote Connections on page 82.

Tip: Install Lumension EMSS using a remote SQL Server instance to increase performance.

Defining the Web Client Account and Service Account

Lumension Endpoint Management and Security Suite requires two user accounts to operate critical components: a Web client account and a service account.

Lumension recommends creating new local user accounts to use as Web client and service accounts (as defined in the installation procedures). However, you can also use preexisting local or domain accounts. When using



preexisting local or domain accounts, certain requirements must be fulfilled. Remember the following rules if you use preexisting user accounts when installing Lumension EMSS using a remote instance of SQL Server:

- In cross-domain network configurations, accounts from either domain may be used as the Web client and service accounts, but the domains must have a trust relationship.
- Any install in which either the Lumension EMSS server or the SQL server is in a workgroup must use local accounts as the Web client and service accounts.
- When using local accounts as the Web client and service accounts, there must be a duplicate of each account on each server. For example if the Lumension EMSS server hosts an account named *serviceadmin* with a password of *Password.0*, then the SQL server must host an account called *serviceadmin* with a password of *Password.0*.

Note: You can use existing user accounts as the Web client account and service account. However Lumension recommends creating new accounts specifically for Lumension Endpoint Management and Security Suite via the installer (if using a remote SQL Server instance, manual creation of identical accounts is required). Creating accounts specifically for the product increases security and automates creation of trust relationships.

Selecting an Installation Method

There are multiple methods of installing or upgrading the product. When installing or upgrading, identify the scenario that best suits your network environment, and complete the scenario according to the provided procedures.

For small network environments that do not require complex instances of SQL Server, complete the basic Lumension EMSS installation. This installation includes an installation of Microsoft SQL Server 2008 Express Edition. This installation method is the simplest Lumension Endpoint Management and Security Suite method.

- [Installing Using a New SQL Server Instance](#) on page 24

For larger network environments, the Lumension EMSS installation requires a more sophisticated SQL Server instance that must be installed independently from Lumension EMSS. This instance of SQL Server, which must be installed before Lumension EMSS, can be installed on either the target Lumension EMSS server or a remote server.

- [Installing Using an Existing SQL Server Instance \(Either Locally or Remotely\)](#) on page 33
- [Installing Using a Remote SQL Server Instance \(with no Local Instance\)](#) on page 46

In especially large environments, the SQL Server administrator and the Lumension EMSS administrator may be separate individuals. In this scenario, a special installation procedure is required due to administrator access right limitations.

- [Installing Lumension Endpoint Management and Security Suite \(Separate Lumension EMSS and SQL Server Admins\)](#) on page 58

When upgrading either Lumension Patch and Remediation 6.4 SP2 or Lumension Endpoint Management and Security Suite 7.0 to Lumension Endpoint Management and Security Suite 7.0 SP1, use one of the following upgrade procedures. Use the procedure applicable to your current version. Data from your current install is transferred to your new install.

- [Upgrading from Lumension Patch and Remediation 6.4 SP2](#) on page 104
- [Upgrading from Lumension Endpoint Management and Security Suite 7.0](#) on page 101



When upgrading either Lumension Patch and Remediation 6.4 SP2 or Lumension Endpoint Management and Security Suite 7.0 to Lumension Endpoint Management and Security Suite 7.0 SP1, but do not want to maintain the data from your previous version, use the following upgrade procedure.

- *Installing Cleanly Over an Existing Installation* on page 113

Attention: Complete *Downloading Lumension Endpoint Management and Security Suite* on page 22 before beginning an installation procedure.

Installing Using a New SQL Server Instance

If SQL Server is not installed on your target server, or if you want to use a new instance instead of an existing one, you can create a new SQL Server 2008 Express Edition instance during the Lumension Endpoint Management and Security Suite (Lumension EMSS) installation.

Prerequisites:

- You have completed *Downloading Lumension Endpoint Management and Security Suite* on page 22.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the *Server Installation Checklist* on page 17.

Note: For additional information about using preexisting user accounts to operate critical Lumension EMSS components, refer to *Defining the Web Client Account and Service Account* on page 22.

If you are installing using SSL, complete the first portion of the task applicable to your target server operating system:

- *Configuring Windows Server 2003 for SSL* on page 85
- *Configuring SQL Server to Accept Remote Connections* on page 82

Attention: This installation procedure installs an instance SQL Server 2008 Express Edition for use with Lumension EMSS. SQL Server 2008 Express Edition is only available in 32-bit architecture. If installing to a 64-bit server, Lumension recommends installing using a supported preexisting instance of SQL Server that supports 64-bit architecture:

- *Installing Using an Existing SQL Server Instance (Either Locally or Remotely)* on page 33
- *Installing Using a Remote SQL Server Instance (with no Local Instance)* on page 46

-
1. Log on to the server on which you want to install Lumension EMSS using either a local or domain user account with system administrator privileges.
 2. Double-click the Lumension EMSS installer at the location defined during downloading.

Step Result: The Lumension EMSS *InstallShield Wizard* opens and begins extracting files. This process may take several minutes.

Note: If Windows Installer 4.5 or .NET Framework 3.5 are not installed on your server, you are notified they will be installed. Additionally, if at any time during the installation



procedure you are prompted to reboot, reboot your server. The installer automatically reopens after reboot.

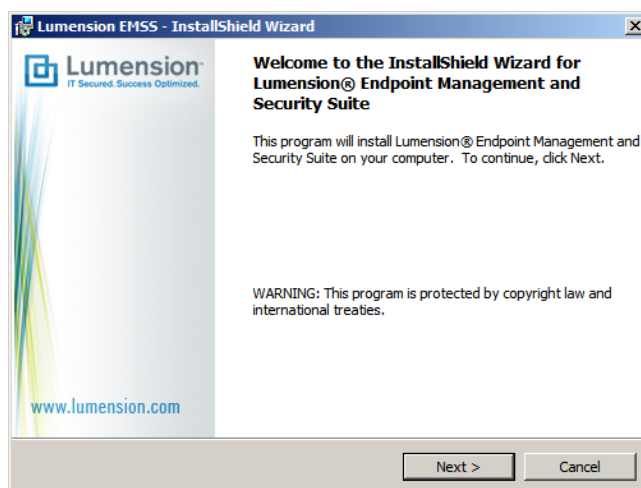


Figure 1: InstallShield Wizard

3. Click **Next**.

Step Result: The *License Agreement* page opens.

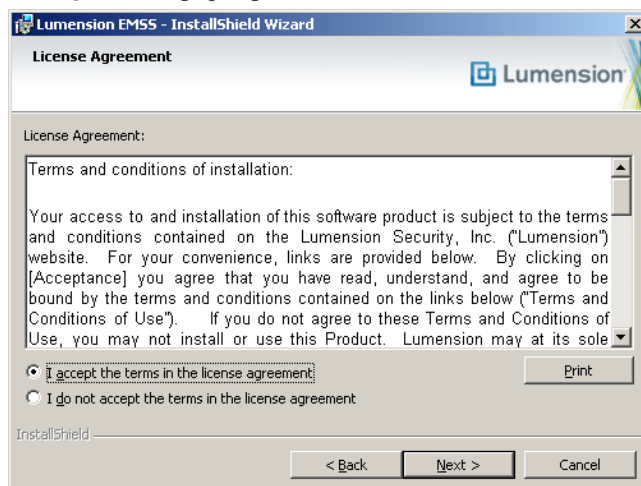


Figure 2: License Agreement Page

Tip: Click **Print** for a hard copy of the license agreement.

4. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.



5. Click **Next**.

Step Result: The *Customer Information* page opens.

Figure 3: Customer Information Page

6. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Lumension EMSS serial number. Note: Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Lumension Sales Support (patchlink.sales@lumension.com) .

Tip: Retain your serial number following installation. It is required for agent registration and Lumension EMSS server reinstallation.

7. Click **Next**.

A new page or dialog opens.

Page/Dialog	Step
If the <i>Question</i> dialog opens:	Click Yes to start network discovery services. These services are necessary to use discovery features within Lumension EMSS.



Page/Dialog	Step
<p>If the <i>Required IIS Features</i> page opens:</p>	<p>Your server does not have the required IIS features installed. Click Next to install the features and proceed.</p> <hr/> <p>Note: On Windows Server 2008, the default installation of IIS lacks components necessary for Lumension EMSS. The Lumension EMSS installer installs the following IIS components if not present:</p> <ul style="list-style-type: none"> • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression <hr/>
<p>If the <i>System Requirements</i> page opens:</p>	<p>Your server does not meet the minimum installation requirements.</p> <ul style="list-style-type: none"> • If you receive only system requirement <i>warnings</i>, you may proceed with installation by clicking Next. Lumension recommends resolving warnings before proceeding with installation. • If you receive any system requirement <i>failures</i>, you must cancel the installation, resolve these failures, and then proceed with installation. <hr/> <p>Tip: Click View all Failures/Warnings for detailed information about prerequisite status deficiencies.</p> <hr/>
<p>If the <i>Service Accounts</i> page opens:</p>	<p>Proceed to the next step.</p>

8. Create or define the Web client account and service account that Lumension EMSS will use.

These accounts are used to operate components critical to Lumension EMSS.



Select from the following options.

Option	Steps
<p>To create new accounts:</p>	<ol style="list-style-type: none"> 1. If desired, edit the Web Client Account Username field. 2. In the Web Client Account Password field, type the desired password. 3. In the Web Client Account Confirm password field, retype the password. 4. If desired, edit the Service Account Username field. 5. In the Service Account Password field, type the desired password. 6. In the Service Account Confirm password field, retype the password. <hr/> <p>Note: If you create new Web Client and Service accounts, Lumension recommends using the default account user names the installation creates.</p> <hr/>
<p>To use preexisting accounts:</p>	<ol style="list-style-type: none"> 1. Type the user name associated with the desired account in the Web Client Account Username field. 2. Type the password associated with the user name in the Web Client Account Password field. 3. Retype the password in the Web Client Account Confirm password field. 4. Type the user name associated with the desired account in the Service Account Username field. 5. Type the password associated with the service account user name in the Service Account Password field. 6. Retype the password in the Service Account Confirm password field. <hr/> <p>Note: Lumension recommends creating new accounts. If using domain accounts, include the domain name as part of the user name (DOMAIN\Username). You may only use preexisting accounts if they meet the requirements defined in Defining the Web Client Account and Service Account on page 22.</p> <hr/>



9. Click **Next**.

If required, acknowledge the creation of new accounts by clicking **OK**.

Step Result: The *SQL Server Instance* page opens.

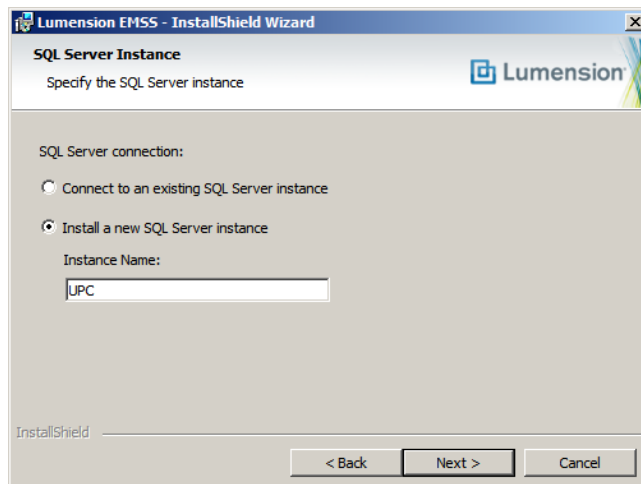


Figure 4: SQL Server Instance Page

10. Select the **Install a new SQL Server instance** option.

11. If desired, type a new instance name in the **Instance Name** field.

12. Click **Next**.

Step Result: The *Destination Location* page opens.

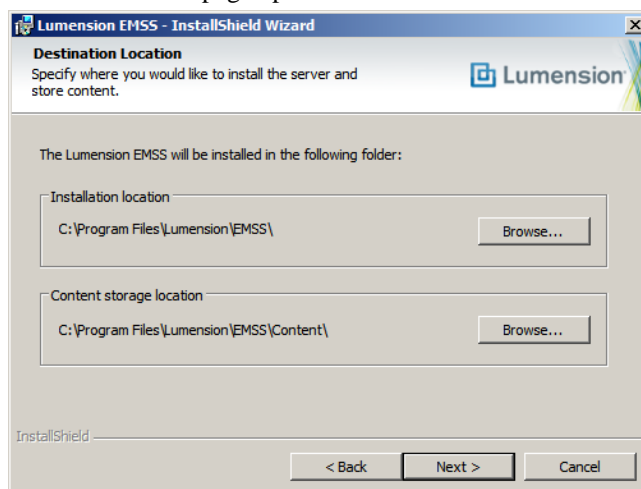


Figure 5: Destination Location Page



13. If desired, change the Lumension EMSS installation location.

- a) Click **Browse**.
- b) Define the desired file path using either the **Look in** lists or the **Folder name** field.
- c) Click **OK**.

Step Result: The **Installation Folder** field reflects your changes.

Note: Although Lumension EMSS can be installed on a 64-bit server, the program itself is not 64-bit. On 64-bit servers, Lumension recommends installing Lumension EMSS at C:\Program Files (x86).

14. If desired, change the Lumension EMSS content storage location.

The content storage location is the location where patches and other content items are downloaded. Lumension recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).

- a) Click **Browse**.
- b) Define the desired file path using either the **Look in** lists or the **Folder name** field.
- c) Click **OK**.

Step Result: The **Content Storage Location** field reflects your changes.

15. Click **Next**.

Step Result: The *Proxy Settings* page opens.

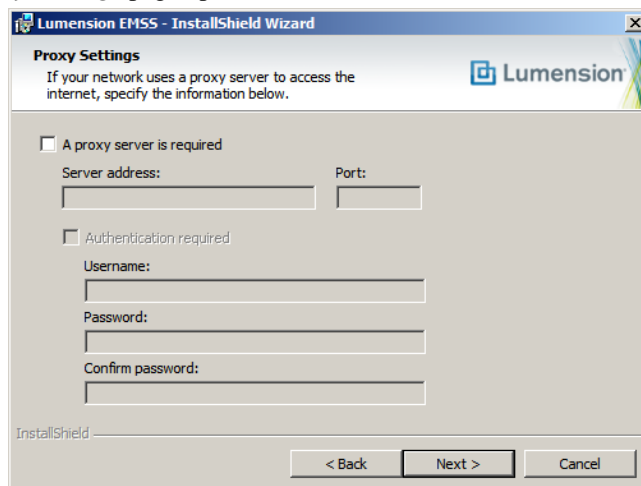
The image shows a screenshot of the 'Lumension EMSS - InstallShield Wizard' window, specifically the 'Proxy Settings' page. The window title bar reads 'Lumension EMSS - InstallShield Wizard'. The main heading is 'Proxy Settings' with a sub-instruction: 'If your network uses a proxy server to access the internet, specify the information below.' There are two checkboxes: 'A proxy server is required' (unchecked) and 'Authentication required' (unchecked). Below the first checkbox are two text input fields labeled 'Server address:' and 'Port:'. Below the second checkbox are three text input fields labeled 'Username:', 'Password:', and 'Confirm password:'. At the bottom left, it says 'InstallShield'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The Lumension logo is visible in the top right corner of the dialog box.

Figure 6: Proxy Settings Page

Note: If one or both of the storage directories defined on the *Destination Location* page does not contain the recommended disk space available, the *Proxy Settings* page does not open. Rather, a dialog opens that lets you redefine the storage directories.

16. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

Field	Type
Server Address	The IP address of the applicable proxy server.
Port	The port number used for communication.

Note: You can also configure Lumension EMSS to use a proxy following installation.

17. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the **Authentication required** check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.

18. Click **Next**.

Step Result: The *Agent to Server Communication* page opens.

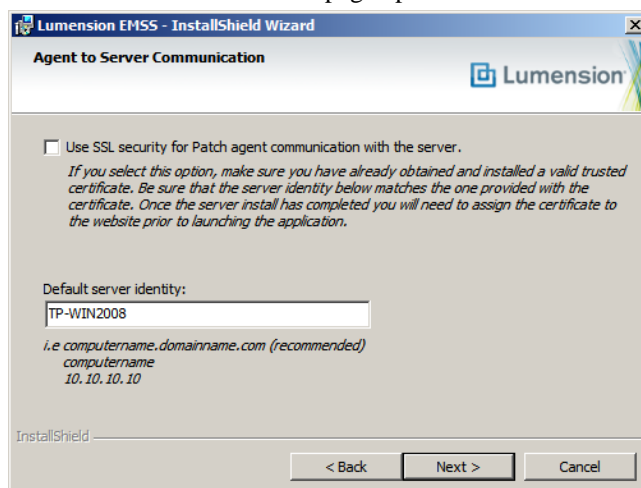


Figure 7: Agent to Server Communication Page

19. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server** check box.

Note: You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.



20. In the **Default server identity** field, type the name of your server in one of the following formats:

- DNS name (*computername.domainname.com*)
- Computer name (*computername*)
- IP address (*10.10.10.10*)

During agent registration, the Lumension EMSS agents use this name to identify the server.

Note: If using SSL, the server name that you type in the field must match the server named on your certificate.

21. Click **Next**.

Step Result: The *Installation Ready* page opens.

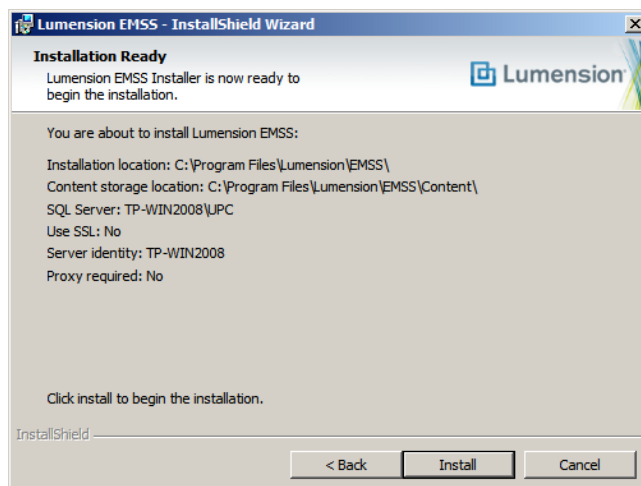


Figure 8: Installation Ready Page

22. Review the installation information and click **Install** to begin the installation of Lumension EMSS.

Important: During installation, do not attempt to access the Lumension EMSS Web site. Accessing the Web site during installation can cause installation errors.

23. After installation completes, click **Finish**.



24. Acknowledge the notification that appears by clicking **OK**.

The credentials you will use to log in to the Lumension EMSS Web site for the first time are the credentials that you used during installation.

Result: Lumension EMSS is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish either *Configuring Windows Server 2003 for SSL* on page 85 or *Configuring Windows Server 2008 for SSL* on page 93.
 - If your server will not use SSL, proceed to *Logging In to Lumension Endpoint Management and Security Suite* on page 73.
-

Installing Using an Existing SQL Server Instance (Either Locally or Remotely)

You can configure your Lumension Endpoint Management and Security Suite (Lumension EMSS) installation to use a SQL Server instance that exists either locally or remotely.

Prerequisites:

- Complete *Downloading Lumension Endpoint Management and Security Suite* on page 22.
 - As applicable to your network environment, you have gathered the information and completed the tasks itemized in the *Server Installation Checklist* on page 17.
-

Note: For additional information about using preexisting user accounts to operate critical Lumension EMSS components, refer to *Defining the Web Client Account and Service Account* on page 22.

If you are installing using SSL, complete the first portion of the task applicable to your target server operating system:

- *Configuring Windows Server 2003 for SSL* on page 85
- *Configuring SQL Server to Accept Remote Connections* on page 82

Additionally, if you are installing using a remote instance of SQL Server, and no instances of SQL Server exist locally, complete *Installing Using a Remote SQL Server Instance (with no Local Instance)* on page 46 rather than this procedure.

1. If installing using a remote instance of SQL Server, complete *Creating Remote Accounts* on page 79.

Note: If using preexisting accounts, you may skip completion of this step.

2. Using either a local or domain account with system administrator privileges, log on to the server on which you will install Lumension EMSS.



3. Double-click the Lumension EMSS installer at the location defined during downloading.

Step Result: The Lumension EMSS *InstallShield Wizard* opens and begins extracting files. This process may take several minutes.

Note: If Windows Installer 4.5 or .NET Framework 3.5 are not installed on your server, you are notified they will be installed. Additionally, if at any time during the installation procedure you are prompted to reboot, reboot your server. The installer automatically reopens after reboot.



Figure 9: InstallShield Wizard

4. Click **Next**.

Step Result: The *License Agreement* page opens.

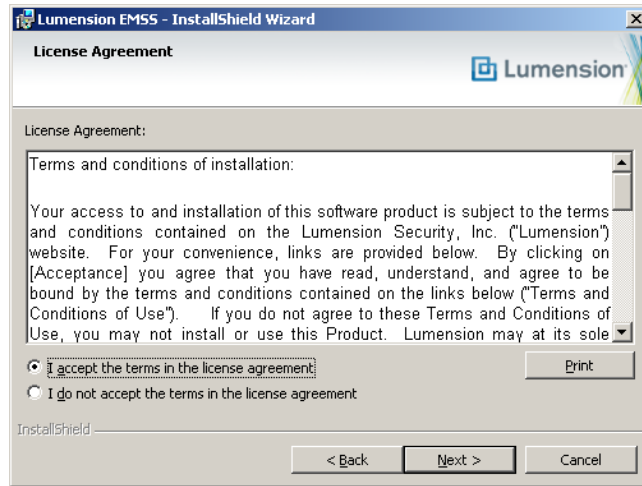


Figure 10: License Agreement Page

Tip: Click **Print** for a hard copy of the license agreement.

5. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.6. Click **Next**.

Step Result: The *Customer Information* page opens.

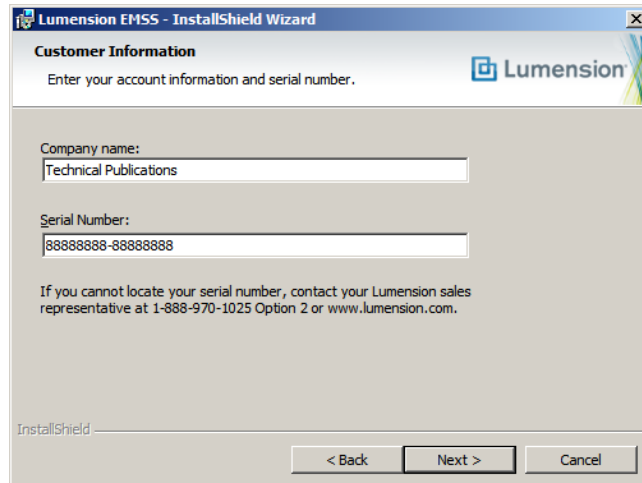


Figure 11: Customer Information Page



7. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Lumension EMSS serial number. Note: Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Lumension Sales Support (patchlink.sales@lumension.com) .

Tip: Retain your serial number following installation. It is required for agent registration and Lumension EMSS server reinstallation.

8. Click **Next**.

A new page or dialog opens.

Page/Dialog	Step
If the <i>Question</i> dialog opens:	Click Yes to start network discovery services. These services are necessary to use discovery features within Lumension EMSS.
If the <i>Required IIS Features</i> page opens:	Your server does not have the required IIS features installed. Click Next to install the features and proceed. Note: On Windows Server 2008, the default installation of IIS lacks components necessary for Lumension EMSS. The Lumension EMSS installer installs the following IIS components if not present: <ul style="list-style-type: none"> • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression



Page/Dialog	Step
If the <i>System Requirements</i> page opens:	<p>Your server does not meet the minimum installation requirements.</p> <ul style="list-style-type: none"> • If you receive only system requirement <i>warnings</i>, you may proceed with installation by clicking Next. Lumension recommends resolving warnings before proceeding with installation. • If you receive any system requirement <i>failures</i>, you must cancel the installation, resolve these failures, and then proceed with installation. <hr/> <p>Tip: Click View all Failures/Warnings for detailed information about prerequisite status deficiencies.</p>
If the <i>Service Accounts</i> page opens:	Proceed to the next step.

9. Define the Web client account and service account that Lumension EMSS will use.

Define these accounts based on how you are configuring your Lumension EMSS server.

Option	Steps
If your install will use a local SQL Server instance:	<p>Define the credentials for two new user accounts (which are created by the installer).</p> <ol style="list-style-type: none"> 1. In the Web Client Account Username field, edit the user name if desired. 2. In the Web Client Account Password field, type a password. 3. In the Web Client Account Confirm password field, retype the password. 4. In the Service Account Username field, edit the user name if desired. 5. In the Service Account Password field, type a password. 6. In the Service Account Confirm password field, retype the password.



Option	Steps
<p>If your install will use a remote SQL Server instance:</p>	<p>Define the credentials for the two user accounts created while completing Creating Remote Accounts on page 79.</p> <ol style="list-style-type: none"> 1. In the Web Client Account Username field, type the user name of the Web client account on your SQL Server. 2. In the Web Client Account Password field, type the password of the Web client account on your SQL Server. 3. In the Web Client Confirm password field, retype the password. 4. In the Service Account Username field, type the user name of the service account on your SQL Server. 5. In the Service Account Password field, type the password of the service account on your SQL Server. 6. In the Service Account Confirm password field, retype the password. <hr/> <p>Important: The Web client account and the service account credentials must be identical on both the SQL Server and the Lumension EMSS server. If they are not, you cannot access the Lumension EMSS Web site.</p> <hr/>
<p>If your install will use a local or remote SQL Server instance that uses preexisting accounts as the Web Client and Service Accounts:</p>	<p>Define the credentials for the preexisting accounts.</p> <ol style="list-style-type: none"> 1. Type the user name associated with the desired account in the Web Client Account Username field. 2. Type the password associated with the user name in the Web Client Account Password field. 3. Retype the password in the Web Client Account Confirm password field. 4. Type the user name associated with the desired account in the Service Account Username field. 5. Type the password associated with the service account user name in the Service Account Password field. 6. Retype the password in the Service Account Confirm password field. <hr/> <p>Important: You can use either local or domain accounts. If using domain accounts, include the domain name as part of the user name (DOMAIN\username). Additionally, preexisting accounts may only be used if they meet the requirements listed in Defining the Web Client Account and Service Account on page 22.</p> <hr/>



10. Click Next.

If required, acknowledge the creation of new accounts by clicking **OK**.

Step Result: The *SQL Server Instance* page opens.

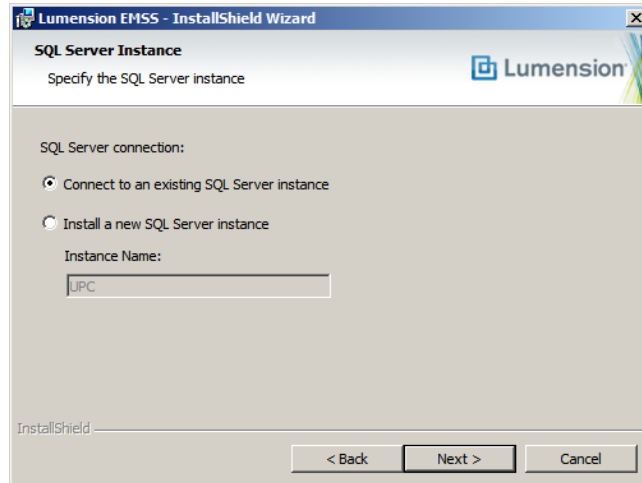


Figure 12: SQL Server Instance Page

11. Ensure the *Connect to an existing SQL Server instance* option is selected.**12. Click Next.**

Step Result: The *SQL Server and Instance* page opens. Use this page to define the SQL Server instance you will use with Lumension EMSS.

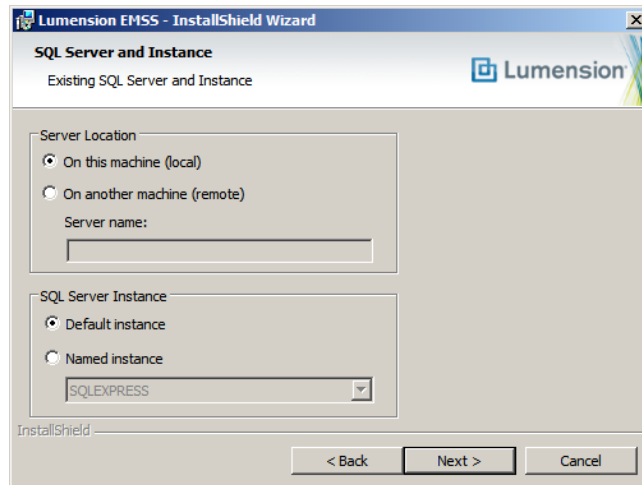


Figure 13: SQL Server and Instance Page



13. Select a Server Location.

Select one of the following options.

Option	Steps
To use a locally installed existing SQL Server instance:	Select the On this machine (local) option.
To use a remotely installed existing SQL Server instance:	<ol style="list-style-type: none"> 1. Select the On another machine (remote) option. 2. Type the server name (<i>not</i> the IP address) in the Server name field. <p>Note: If you must define an IP address, either map the IP address to the server name in the hosts file or create an alias using SQL Server Configuration Manager.</p>

14. Select a SQL Server Instance.

Select one of the following options:

Option	Steps
To use a default instance of SQL Server:	Select the Default instance option.
To use a named instance of SQL Server:	<ol style="list-style-type: none"> 1. Select the Named instance option. 2. If the SQL Server instance is local, select it from the list. If the SQL Server instance is remote, type its name in the field.



15. Click **Next**.

Step Result: The *SQL Server Authentication* page opens.

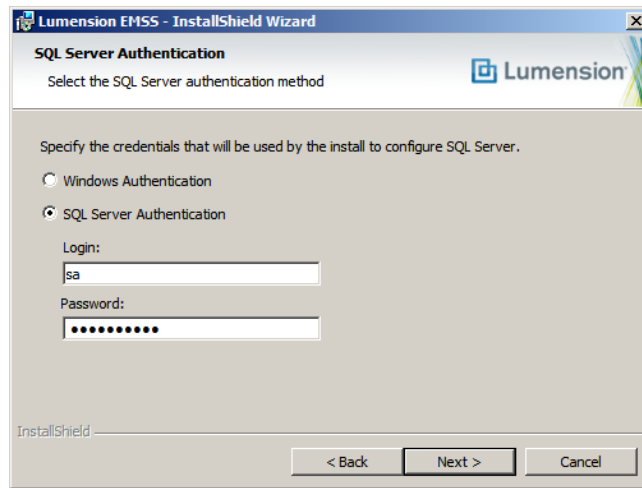


Figure 14: SQL Server Authentication Page

16. Define the credentials that will be used to access the SQL Server instance (based upon its authentication mode).

Select from the following options:

Option	Steps
To use Windows authentication:	Select the Windows Authentication option.
To use SQL Server authentication:	<ol style="list-style-type: none"> 1. Select the SQL Server Authentication option. 2. Type a user name that will validate with the SQL Server instance in the Login field. 3. Type the password associated with the user in the Password field.

Note: The credentials used to access the SQL Server instance must be assigned the **sysadmin** system role within *Microsoft SQL Server Management Studio*. If the user account defined is not assigned this role, the *The credentials provided do not have sufficient privileges to continue* dialog opens after clicking **Next**. You must define a user account assigned this role before you can continue.

If you cannot be assigned this role due to network security policies and procedures that split administrative duties between a Lumension EMSS administrator and a SQL Server administrator, refer to [Installing Lumension Endpoint Management and Security Suite \(Separate Lumension EMSS and SQL Server Admins\)](#) on page 58.



17. Click Next.

A new page opens.

Page	Steps
If the <i>Destination Location</i> page opens:	Proceed to the next step.
If the <i>SQL Server Configuration Requirements</i> page opens:	<p>The pre-installed instance of SQL Server is not configured to work with Lumension EMSS.</p> <ul style="list-style-type: none"> • If you only receive SQL Server configuration requirement <i>informationals</i> or <i>warnings</i>, click Next to continue (the Lumension EMSS installation will automatically reconfigure SQL Server). Proceed to the next step. • If you receive any SQL Server configuration requirement <i>failures</i>, you must cancel the installation, resolve the failures, and then proceed with the installation. <hr/> <p>Tip: Click View all Features/Warnings for detailed information about SQL Server configuration status requirements.</p> <hr/>

18. If desired, change the Lumension EMSS installation location.

- Click **Browse**.
- Define the desired file path using either the **Look in** lists or the **Folder name** field.
- Click **OK**.

Step Result: The **Installation Folder** field reflects your changes.

Note: Although Lumension EMSS can be installed on a 64-bit server, the program itself is not 64-bit. On 64-bit servers, Lumension recommends installing Lumension EMSS at C:\Program Files (x86).

19. If desired, change the Lumension EMSS content storage location.

The content storage location is the location where patches and other content items are downloaded. Lumension recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).

- Click **Browse**.
- Define the desired file path using either the **Look in** lists or the **Folder name** field.
- Click **OK**.

Step Result: The **Content Storage Location** field reflects your changes.



20. Click **Next**.

Step Result: The *Proxy Settings* page opens.

Figure 15: Proxy Settings Page

Note: If one or both of the storage directories defined on the *Destination Location* page does not contain the recommended disk space available, the *Proxy Settings* page does not open. Rather, a dialog opens that lets you redefine the storage directories.

21. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

Field	Type
Server Address	The IP address of the applicable proxy server.
Port	The port number used for communication.

Note: You can also configure Lumension EMSS to use a proxy following installation.

22. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the **Authentication required** check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.



23. Click Next.

Step Result: The *Agent to Server Communication* page opens.

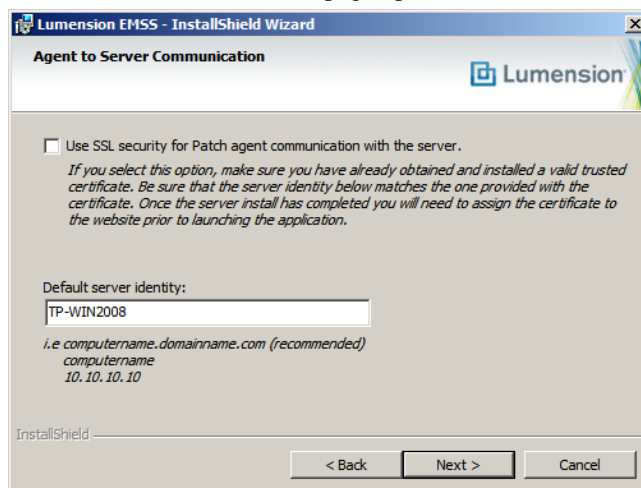


Figure 16: Agent to Server Communication Page

24. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server check box.**

Note: You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.

25. In the **Default server identity field, type the name of your server in one of the following formats:**

- DNS name (*computername.domainname.com*)
- Computer name (*computername*)
- IP address (*10.10.10.10*)

During agent registration, the Lumension EMSS agents use this name to identify the server.

Note: If using SSL, the server name that you type in the field must match the server named on your certificate.



26. Click Next.

Step Result: The *Installation Ready* page opens.

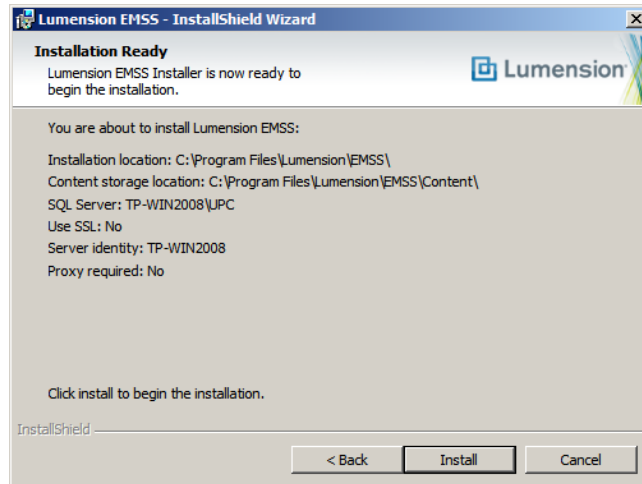


Figure 17: Installation Ready Page

27. Review the installation information and click **Install to begin the installation of Lumension EMSS.**

Important: During installation, do not attempt to access the Lumension EMSS Web site. Accessing the Web site during installation can cause installation errors.

28. After installation completes, click **Finish.****29. Acknowledge the notification that appears by clicking **OK**.**

The credentials you will use to log in to the Lumension EMSS Web site for the first time are the credentials that you used during installation.

Result: Lumension EMSS is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish either *Configuring Windows Server 2003 for SSL* on page 85 or *Configuring Windows Server 2008 for SSL* on page 93.
 - If your server will not use SSL, proceed to *Logging In to Lumension Endpoint Management and Security Suite* on page 73.
-



Installing Using a Remote SQL Server Instance (with no Local Instance)

Installing Lumension Endpoint Management and Security Suite (Lumension EMSS) using an existing remote SQL Server instance differs slightly when no SQL Server instance exists locally.

Prerequisites:

- Complete *Downloading Lumension Endpoint Management and Security Suite* on page 22.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the *Server Installation Checklist* on page 17.

Note: For additional information about using preexisting user accounts to operate critical Lumension EMSS components, refer to *Defining the Web Client Account and Service Account* on page 22.

If you are installing using SSL, complete the first portion of the task applicable to your target server operating system:

- *Configuring Windows Server 2003 for SSL* on page 85
- *Configuring SQL Server to Accept Remote Connections* on page 82

-
1. Complete *Creating Remote Accounts* on page 79.

Note: If using preexisting accounts, you may skip completion of this procedure.

2. Using either a local or domain account with system administrator privileges, log on to the server on which you will install Lumension EMSS.
3. Double-click the Lumension EMSS installer at the location defined during downloading.

Step Result: The Lumension EMSS *InstallShield Wizard* opens and begins extracting files. This process may take several minutes.

Note: If Windows Installer 4.5 or .NET Framework 3.5 are not installed on your server, you are notified they will be installed. Additionally, if at any time during the installation



procedure you are prompted to reboot, reboot your server. The installer automatically reopens after reboot.



Figure 18: InstallShield Wizard

4. Click **Next**.

Step Result: The *License Agreement* page opens.

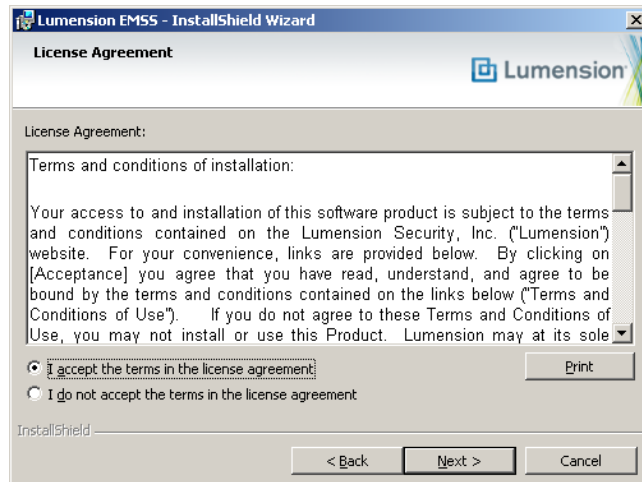


Figure 19: License Agreement Page

Tip: Click **Print** for a hard copy of the license agreement.

5. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.



6. Click **Next**.

Step Result: The *Customer Information* page opens.

Figure 20: Customer Information Page

7. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Lumension EMSS serial number. Note: Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Lumension Sales Support (patchlink.sales@lumension.com) .

Tip: Retain your serial number following installation. It is required for agent registration and Lumension EMSS server reinstallation.

8. Click **Next**.

A new page or dialog opens.

Page/Dialog	Step
If the <i>Question</i> dialog opens:	Click Yes to start network discovery services. These services are necessary to use discovery features within Lumension EMSS.



Page/Dialog	Step
<p>If the <i>Required IIS Features</i> page opens:</p>	<p>Your server does not have the required IIS features installed. Click Next to install the features and proceed.</p> <hr/> <p>Note: On Windows Server 2008, the default installation of IIS lacks components necessary for Lumension EMSS. The Lumension EMSS installer installs the following IIS components if not present:</p> <ul style="list-style-type: none"> • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression <hr/>
<p>If the <i>System Requirements</i> page opens:</p>	<p>Your server does not meet the minimum installation requirements.</p> <ul style="list-style-type: none"> • If you receive only system requirement <i>warnings</i>, you may proceed with installation by clicking Next. Lumension recommends resolving warnings before proceeding with installation. • If you receive any system requirement <i>failures</i>, you must cancel the installation, resolve these failures, and then proceed with installation. <hr/> <p>Tip: Click View all Failures/Warnings for detailed information about prerequisite status deficiencies.</p> <hr/>
<p>If the <i>Service Accounts</i> page opens:</p>	<p>Proceed to the next step.</p>



9. Define the Web client account and service account that your Lumension EMSS server will use.

Select from the following options.

Option	Steps
<p>To duplicate the accounts on your SQL Server:</p>	<ol style="list-style-type: none"> 1. In the Web Client Account Username field, type the user name of the Web client account on your SQL Server. 2. In the Web Client Account Password field, type the password of the Web client account on your SQL Server. 3. In the Web Client Account Confirm password field, retype the password. 4. In the Service Account Username field, type the user name of the service account on your SQL Server. 5. In the Service Account Password field, type the password of the service account on your SQL Server. 6. In the Service Account Confirm password field, retype the password. <hr/> <p>Important: The Web client account and the server account credentials must be identical on both the SQL Server and the Lumension EMSS server. If they are not, you cannot access the Lumension EMSS Web site.</p>
<p>To use preexisting accounts:</p>	<ol style="list-style-type: none"> 1. Type the user name associated with the desired account in the Web Client Account Username field. 2. Type the password associated with the user name in the Web Client Account Password field. 3. Retype the password in the Web Client Account Confirm password field. 4. Type the user name associated with the desired account in the Service Account Username field. 5. Type the password associated with the service account user name in the Service Account Password field. 6. Retype the password in the Service Account Confirm password field. <hr/> <p>Important: You can use either local or domain accounts. If using domain accounts, include the domain name as part of the user name (DOMAIN\username). Additionally, preexisting accounts may only be used if they meet the requirements listed in Defining the Web Client Account and Service Account on page 22.</p>



10. Click Next.

If required, acknowledge the creation of new accounts by clicking **OK**.

Step Result: The *SQL Server Instance* Page opens.

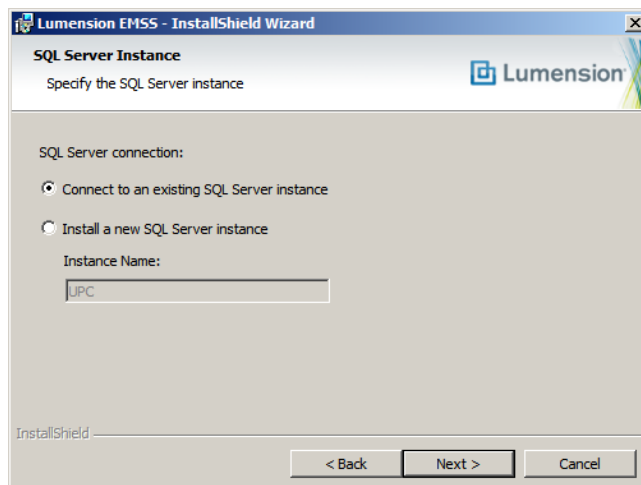


Figure 21: SQL Server Instance Page

11. Ensure the *Connect to an existing SQL Server instance* option is selected.

12. Click Next.

Step Result: The *SQL Server and Instance* page opens.

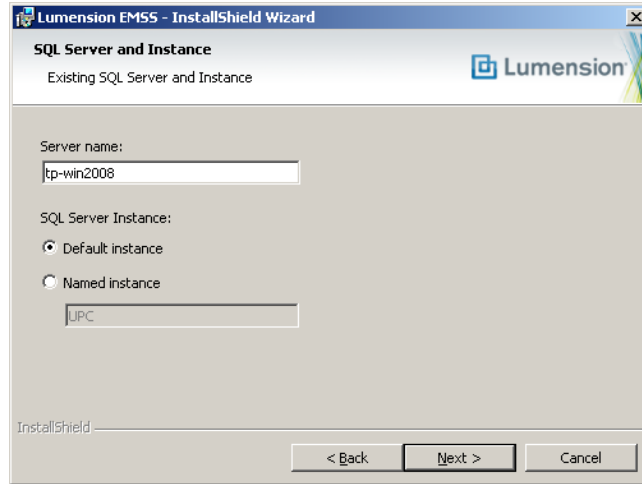


Figure 22: SQL Server and Instance Page (No Local Options)

Note: If **Server Location** options are available from this page, you are performing the wrong procedure. Instead, perform *Installing Using an Existing SQL Server Instance (Either Locally or Remotely)* on page 33.

13. Type the name (*not* the IP address) of the server hosting the remote SQL Server instance in the **Server name** field.

14. Based on the SQL Server instance you are using, select a **SQL Server Instance** option.

Select one of the following options.

Option	Steps
To use a default SQL Server instance:	Select the Default instance option.
To use a named SQL Server instance:	<ol style="list-style-type: none"> 1. Select the Named instance option. 2. Type the instance name in the Named instance field.



15. Click **Next**.

Step Result: The *SQL Server Authentication* page opens.

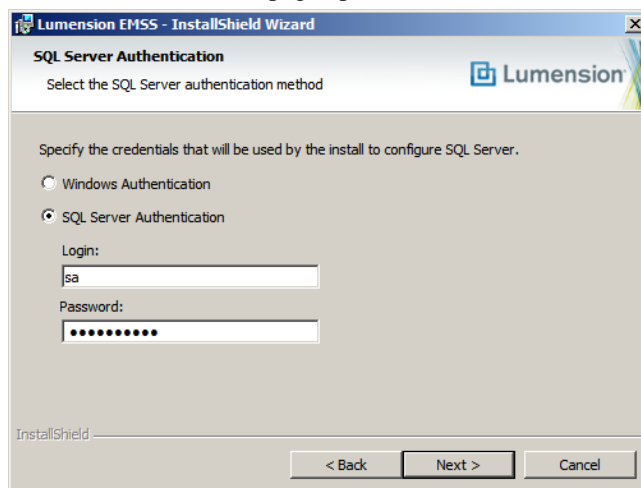


Figure 23: SQL Server Authentication Page

16. Define the credentials that will be used to access the SQL Server instance (based upon its authentication mode).

Select from the following options:

Option	Steps
To use Windows authentication:	Select the Windows Authentication option.
To use SQL Server authentication:	<ol style="list-style-type: none"> 1. Select the SQL Server Authentication option. 2. Type a user name that will validate with the SQL Server instance in the Login field. 3. Type the password associated with the user in the Password field.

Note: The credentials used to access the SQL Server instance must be assigned the **sysadmin** system role within *Microsoft SQL Server Management Studio*. If the user account defined is not assigned this role, the *The credentials provided do not have sufficient privileges to continue* dialog opens after clicking **Next**. You must define a user account assigned this role before you can continue.

If you cannot be assigned this role due to network security policies and procedures that split administrative duties between a Lumension EMSS administrator and a SQL Server administrator, refer to *Installing Lumension Endpoint Management and Security Suite (Separate Lumension EMSS and SQL Server Admins)* on page 58.



17. Click Next.

A new page opens.

Page	Steps
If the <i>Destination Location</i> page opens:	Proceed to the next step.
If the <i>SQL Server Configuration Requirements</i> page opens:	<p>The pre-installed instance of SQL Server is not configured to work with Lumension EMSS.</p> <ul style="list-style-type: none"> • If you only receive SQL Server configuration requirement <i>informationals</i> or <i>warnings</i>, click Next to continue (the Lumension EMSS installation will automatically reconfigure SQL Server). Proceed to the next step. • If you receive any SQL Server configuration requirement <i>failures</i>, you must cancel the installation, resolve the failures, and then proceed with the installation. <hr/> <p>Tip: Click View all Features/Warnings for detailed information about SQL Server configuration status requirements.</p> <hr/>

18. If desired, change the Lumension EMSS installation location.

- a) Click **Browse**.
- b) Define the desired file path using either the **Look in** lists or the **Folder name** field.
- c) Click **OK**.

Step Result: The **Installation Folder** field reflects your changes.

Note: Although Lumension EMSS can be installed on a 64-bit server, the program itself is not 64-bit. On 64-bit servers, Lumension recommends installing Lumension EMSS at C:\Program Files (x86).

19. If desired, change the Lumension EMSS content storage location.

The content storage location is the location where patches and other content items are downloaded. Lumension recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).

- a) Click **Browse**.
- b) Define the desired file path using either the **Look in** lists or the **Folder name** field.
- c) Click **OK**.

Step Result: The **Content Storage Location** field reflects your changes.



20. Click **Next**.

Step Result: The *Proxy Settings* page opens.

Figure 24: Proxy Settings Page

Note: If one or both of the storage directories defined on the *Destination Location* page does not contain the recommended disk space available, the *Proxy Settings* page does not open. Rather, a dialog opens that lets you redefine the storage directories.

21. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

Field	Type
Server Address	The IP address of the applicable proxy server.
Port	The port number used for communication.

Note: You can also configure Lumension EMSS to use a proxy following installation.

22. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the **Authentication required** check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.



23. Click Next.

Step Result: The *Agent to Server Communication* page opens.

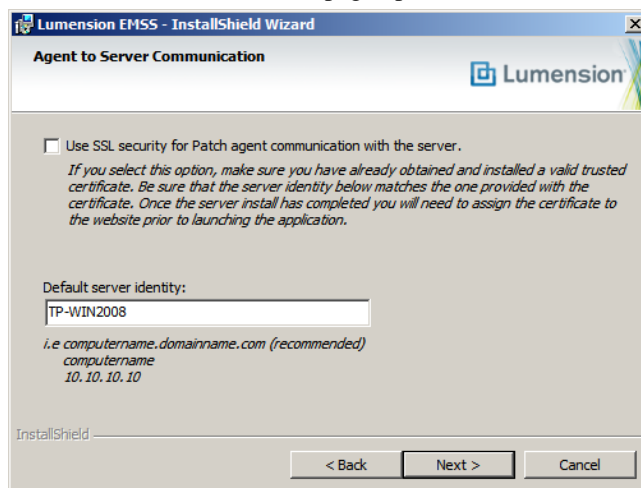


Figure 25: Agent to Server Communication Page

24. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server check box.**

Note: You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.

25. In the **Default server identity field, type the name of your server in one of the following formats:**

- DNS name (*computername.domainname.com*)
- Computer name (*computername*)
- IP address (*10.10.10.10*)

During agent registration, the Lumension EMSS agents use this name to identify the server.

Note: If using SSL, the server name that you type in the field must match the server named on your certificate.



26. Click Next.

Step Result: The *Installation Ready* page opens.

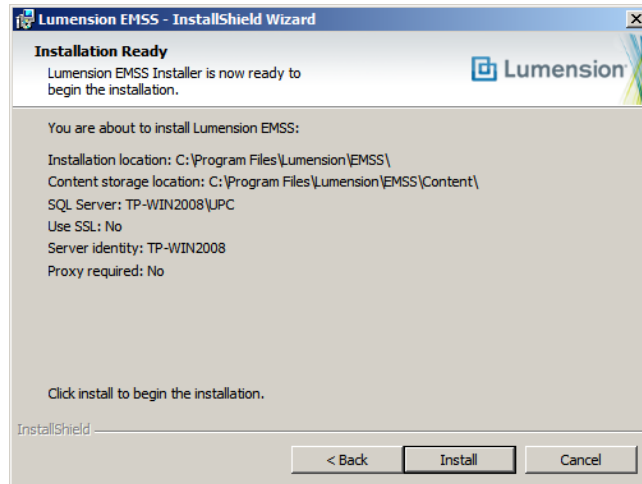


Figure 26: Installation Ready Page

27. Review the installation information and click **Install to begin the installation of Lumension EMSS.**

Important: During installation, do not attempt to access the Lumension EMSS Web site. Accessing the Web site during installation can cause installation errors.

28. After installation completes, click **Finish.****29. Acknowledge the notification that appears by clicking **OK**.**

The credentials you will use to log in to the Lumension EMSS Web site for the first time are the credentials that you used during installation.

Result: Lumension EMSS is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish either *Configuring Windows Server 2003 for SSL* on page 85 or *Configuring Windows Server 2008 for SSL* on page 93.
 - If your server will not use SSL, proceed to *Logging In to Lumension Endpoint Management and Security Suite* on page 73.
-



Installing Lumension Endpoint Management and Security Suite (Separate Lumension EMSS and SQL Server Admins)

When installing Lumension Endpoint Management and Security Suite (Lumension EMSS) using a remote SQL Server instance in a large network environment, a special installation procedure that splits install duties between the Lumension EMSS and the SQL Server administrator may be necessary.

When installing Lumension EMSS using a remote SQL Server instance, the user account you use to access the SQL server instance must be assigned the *sysadmin* role within *Microsoft SQL Server Management Studio*. However, Lumension recognizes that in larger network environments, the administrator installing Lumension EMSS may not be able to obtain this role due to IT policies and procedures; only the SQL Server administrator can access the applicable SQL instance.

Therefore, under these circumstances, the network administrator and SQL Server administrator must cooperate to complete Lumension EMSS installation. To install Lumension EMSS in this type of environment, the installation is broken in to three separate procedures.

Procedure Portion	Description
<i>Beginning Installation (Part I)</i> on page 59	Performed by the Lumension EMSS administrator on the target Lumension EMSS server, this procedure begins the product installation. During this procedure, the Lumension EMSS administrator reviews a licence agreement, defines registration information, defines the remote SQL Server location, and creates a script to modify the SQL Server instance.
<i>Creating Components on SQL Server (Part II)</i> on page 66	Performed by the SQL Server administrator on the server hosting the applicable SQL instance, this procedure creates the user accounts necessary to operate Lumension EMSS and then runs the script created in part I. This script modifies the SQL Server instance to accommodate Lumension EMSS installation for an administrator without <i>sysadmin</i> rights within Microsoft SQL Server.
<i>Completing Installation (Part III)</i> on page 68	Performed by the Lumension EMSS administrator on the target Lumension EMSS server, this procedure completes Lumension EMSS installation. This procedure defines where the Lumension EMSS server and its content will be stored, whether the server will use a proxy server, and whether the server will use SSL.



Beginning Installation (Part I)

The Lumension Endpoint Management and Security Suite (Lumension EMSS) administrator performs the first portion of the install procedure. At the end of this portion, the installer creates a script that you deliver to the SQL Server administrator.

Prerequisites:

- Complete *Downloading Lumension Endpoint Management and Security Suite* on page 22.
- As applicable to your network environment, you have gathered the information and completed the tasks itemized in the *Server Installation Checklist* on page 17.

This first portion of this installation procedure is performed by the Lumension EMSS administrator on the target Lumension EMSS server.

1. Using either a local or domain account with system administrator privileges, log on to the server on which you will install Lumension EMSS.
2. Double-click the Lumension EMSS installer at the location defined during downloading.

Step Result: The Lumension EMSS *InstallShield Wizard* opens and begins extracting files. This process may take several minutes.

Note: If Windows Installer 4.5 or .NET Framework 3.5 are not installed on your server, you are notified they will be installed. Additionally, if at any time during the installation procedure you are prompted to reboot, reboot your server. The installer automatically reopens after reboot.

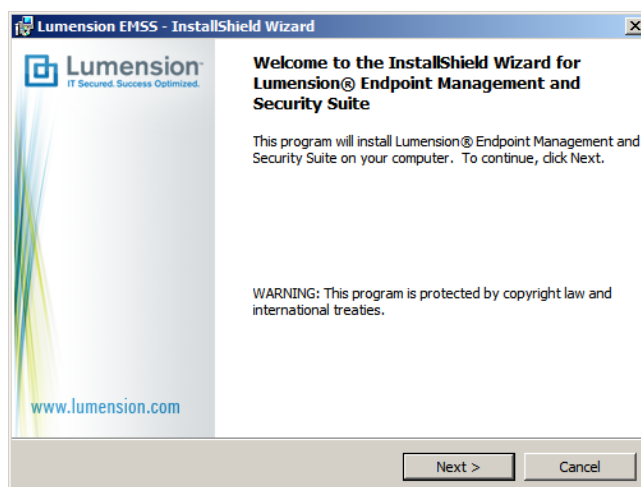


Figure 27: InstallShield Wizard



3. Click **Next**.

Step Result: The *License Agreement* page opens.

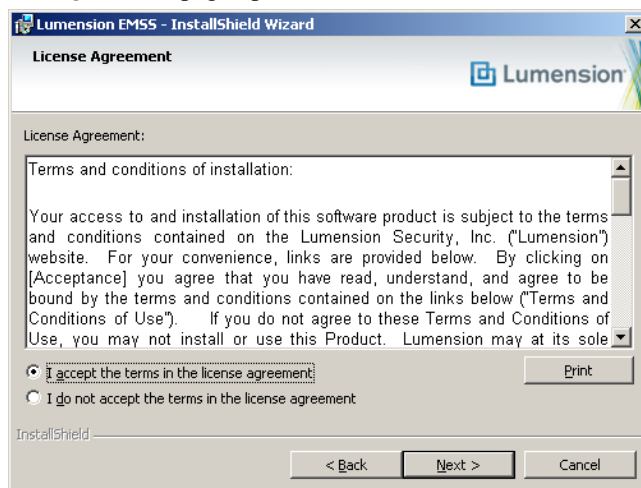


Figure 28: License Agreement Page

Tip: Click **Print** for a hard copy of the license agreement.

4. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.

5. Click **Next**.

Step Result: The *Customer Information* page opens.

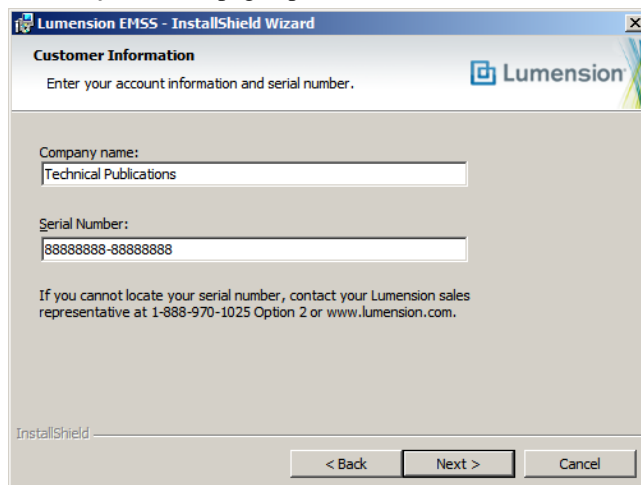


Figure 29: Customer Information Page



6. Type the applicable information in the following fields:

Field	Description
Company Name	Your company name.
Serial Number	Your Lumension EMSS serial number. Note: Your serial number is two groups of eight alphanumeric characters. Letters are not case sensitive. If you cannot locate your serial number, obtain it by contacting the Lumension Sales Support (patchlink.sales@lumension.com) .

Tip: Retain your serial number following installation. It is required for agent registration and Lumension EMSS server reinstallation.

7. Click **Next**.

A new page or dialog opens.

Page/Dialog	Step
If the <i>Question</i> dialog opens:	Click Yes to start network discovery services. These services are necessary to use discovery features within Lumension EMSS.
If the <i>Required IIS Features</i> page opens:	Your server does not have the required IIS features installed. Click Next to install the features and proceed. Note: On Windows Server 2008, the default installation of IIS lacks components necessary for Lumension EMSS. The Lumension EMSS installer installs the following IIS components if not present: <ul style="list-style-type: none"> • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression



Page/Dialog	Step
If the <i>System Requirements</i> page opens:	<p>Your server does not meet the minimum installation requirements.</p> <ul style="list-style-type: none"> • If you receive only system requirement <i>warnings</i>, you may proceed with installation by clicking Next. Lumension recommends resolving warnings before proceeding with installation. • If you receive any system requirement <i>failures</i>, you must cancel the installation, resolve these failures, and then proceed with installation. <hr/> <p>Tip: Click View all Failures/Warnings for detailed information about prerequisite status deficiencies.</p>
If the <i>Service Accounts</i> page opens:	Proceed to the next step.

8. Create the Web client account and server accounts that Lumension EMSS will use.

Important: Preexisting accounts or domain accounts cannot be used for this installation procedure.

- If desired, edit the **Web Client Account Username** field.
- In the **Web Client Account Password** field, type the desired password.
- In the **Web Client Account Confirm password** field, retype the password.
- If desired, edit the **Service Account Username** field.
- In the **Service Account Password** field, type the desired password.
- In the **Service Account Confirm password** field, retype the password.

Note: Lumension recommends using the default account user names the installation creates.



9. Click **Next**.

If required, acknowledge the creation of new accounts by clicking **OK**.

Step Result: The *SQL Server Instance* Page opens.

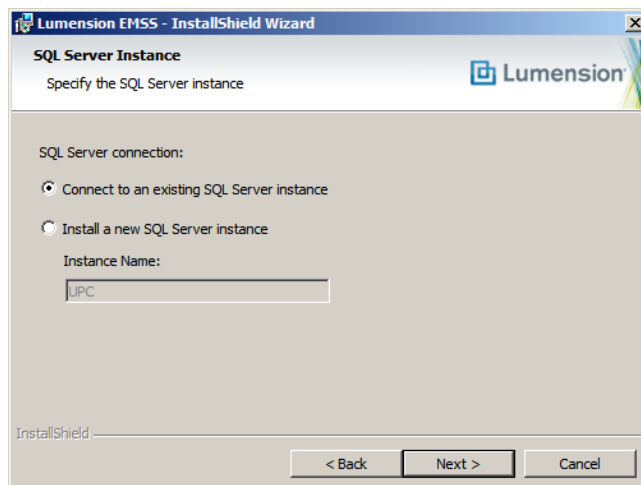


Figure 30: SQL Server Instance Page

10. Ensure the **Connect to an existing SQL Server instance** option is selected.



11. Click Next.

Step Result: The *SQL Server and Instance* page opens.

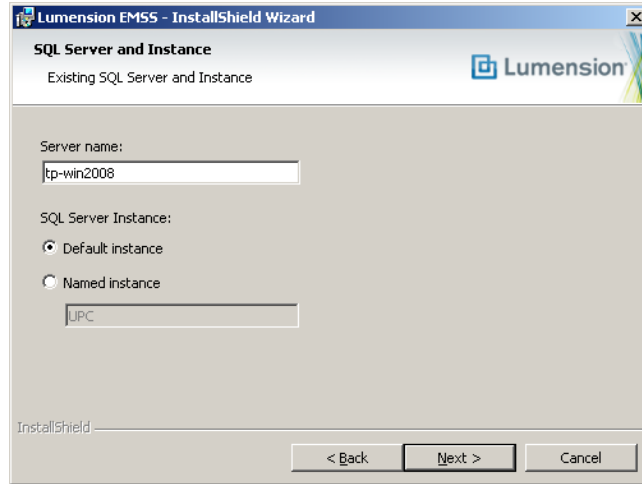


Figure 31: SQL Server and Instance Page (No Local Options)

Note: If **Server Location** options are available from this page, you are performing the wrong procedure. Instead, perform *Installing Using an Existing SQL Server Instance (Either Locally or Remotely)* on page 33.

12. Type the name (*not* the IP address) of the server hosting the remote SQL Server instance in the **Server name** field.

13. Based on the SQL Server instance you are using, select a **SQL Server Instance** option.

Select one of the following options.

Option	Steps
To use a default SQL Server instance:	Select the Default instance option.
To use a named SQL Server instance:	<ol style="list-style-type: none"> 1. Select the Named instance option. 2. Type the instance name in the Named instance field.



14. Click Next.

Step Result: The *SQL Server Authentication* page opens.

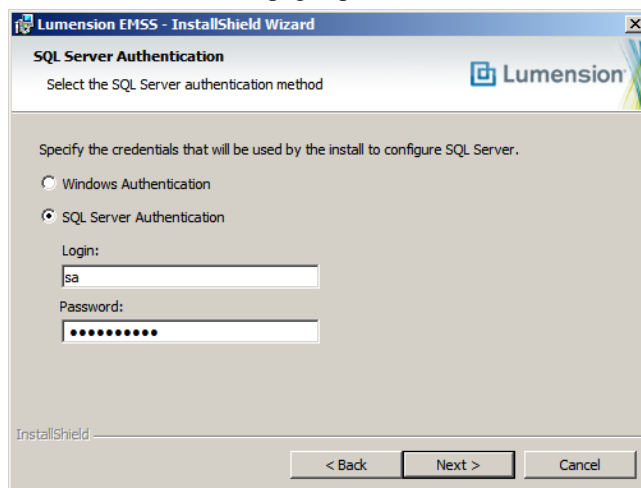


Figure 32: SQL Server Authentication Page

15. Click Next.

Step Result: *The credentials provided do not have sufficient privileges to continue* dialog opens.

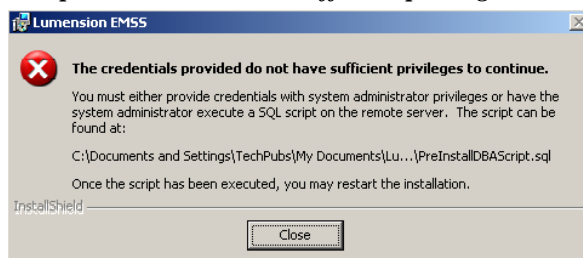


Figure 33: Insufficient Credentials Dialog

16. Note where the script is located and click **Close**.

17. Leave the installer open on its current page.

You will continue from this point during the last portion of the procedure.

18. Deliver the script to your SQL Server administrator.

After Completing This Task:

Have your SQL Server administrator complete *Creating Components on SQL Server (Part II)* on page 66.



Creating Components on SQL Server (Part II)

The SQL Server administrator performs this portion of the install procedure, which installs components on the SQL Server instance necessary for Lumension Endpoint Management and Security Suite (Lumension EMSS) to function. These components are installed via the script your Lumension EMSS administrator delivers.

Prerequisites:

- Complete *Configuring SQL Server to Accept Remote Connections* on page 82.
- Complete *Configuring Windows Firewall for SQL Server Instance Access* on page 84.
- Obtain the script created by the Lumension EMSS installation from your network Lumension EMSS administrator and ensure it is on your SQL Server.
- Review the script to ensure it coincides with your IT department's policies and procedures.

This second portion of the installation procedure is performed by the SQL Server administrator on your existing remote instance of SQL Server.

Tip: If you have any questions and/or require additional assistance, contact Lumension support at *Lumension Support* (<http://www.lumension.com/support.jsp>).

1. Log on to your SQL Server using an account with administrative privileges. This account should also be assigned the *sysadmin* server role within *Microsoft SQL Server Management Studio*.
2. Create three user accounts.

Important: Preexisting accounts or domain accounts cannot be used for this installation procedure.

The first account you will create is identical to the user account used to begin the installation of Lumension EMSS. This account will be granted a login to the Lumension EMSS databases and assigned the *db_owner* role within *Microsoft SQL Server Management Studio*.

The second and third accounts created are the Web client account and the service account. These accounts are used to operate components critical to Lumension EMSS.

Important: The credentials for each of these accounts must match their respective accounts on the Lumension EMSS target server. Consult your network administrator for the credentials for each account. If these accounts are not identical, Lumension EMSS will not function correctly.

Complete the following substeps to create the account:

- a) Select **Start > Administrative Tools > Computer Management**.

Step Result: The *Computer Management* dialog opens.

- b) Expand the directory tree structure to **Users (Computer Management [local] > System Tools > Local Users and Groups > Users)**.



- c) Right-click **Users** and select **New User**.

Step Result: The *New User* dialog opens.

Figure 34: New User Dialog

- d) Create a user account identical to the user account used to begin installation of Lumension EMSS.
- In the **User name** field, type the applicable user name.
 - In the **Password** field, type the applicable password.
 - In the **Confirm password** field, retype the password.

Note: Consult your Lumension EMSS administrator to obtain these credentials.

- e) Clear the *User must change password at next logon* check box.
 f) Select the *Password never expires* check box.
 g) Click **Create**.

Step Result: The user account is created.

- h) Repeat substeps d through g to create the Web client account.
 i) Repeat substeps d through g to create the service account.
 j) Click **Close**.

3. Select **Start > Run**.

4. In the field, type `cmd`.



5. Click **OK**.

Step Result: A command prompt opens.

6. From the command prompt, type `sqlcmd -SSERVERNAME\INSTANCENAME -E -ifilepath \PreInstallDBAScript.sql -kl>c:\PreInstallDBAScript_out.txt`.

Note: Remember the following information when entering this command at the prompt:

- All characters in the command are case sensitive.
- When typing `SERVERNAME\INSTANCENAME`, the slash and instance name are not necessary if the applicable instance is a default instance.
- The `-E` command instructs sqlcmd to connect to the SQL Server using a trusted connection.
- The `-i` command defines where to locate the script to execute. If this command is executed from the directory where `PreInstallDBAScript.sql` is located, then the file path is not necessary; otherwise, the full file path must be defined.
- The `-kl` command instructs sqlcmd to remove any control characters found in the input file.

Result: The following databases are created:

PLUS	Patch Management Database
PLUS_Staging	Content Replication Database
SCM	Security Configuration Management Database
STAT_Guardian	Network Discovery/Agent Deployment Database
UPCCommon	Endpoint Management Platform Database

The modifications necessary for your Lumension EMSS administrator to complete installation of Lumension EMSS are finished.

After Completing This Task:

Have your Lumension EMSS administrator complete *Completing Installation (Part III)* on page 68.

Completing Installation (Part III)

The Lumension Endpoint Management and Security Suite (Lumension EMSS) administrator performs this portion of the install procedure, which completes installation of Lumension EMSS.

The final portion of the installation procedure is performed by the Lumension EMSS administrator on your target Lumension Endpoint Management and Security Suite server.

Tip: If you have any questions and/or require additional assistance, contact Lumension support at [Lumension Support \(http://www.lumension.com/support.jsp\)](http://www.lumension.com/support.jsp).

1. Ensure **Windows Authentication** is selected.



2. Click **Next**.

A new page opens.

Page	Steps
If the <i>Destination Location</i> page opens:	Proceed to the next step.
If the <i>SQL Server Configuration Requirements</i> page opens:	<p>The pre-installed instance of SQL Server is not configured to work with Lumension EMSS.</p> <ul style="list-style-type: none"> If you only receive SQL Server configuration requirement <i>informationals</i> or <i>warnings</i>, click Next to continue (the Lumension EMSS installation will automatically reconfigure SQL Server). Proceed to the next step. If you receive any SQL Server configuration requirement <i>failures</i>, you must cancel the installation, resolve the failures, and then proceed with the installation. <p>Tip: Click View all Features/Warnings for detailed information about SQL Server configuration status requirements.</p>

3. Click **Next**.

Step Result: The *Destination Location* page opens.

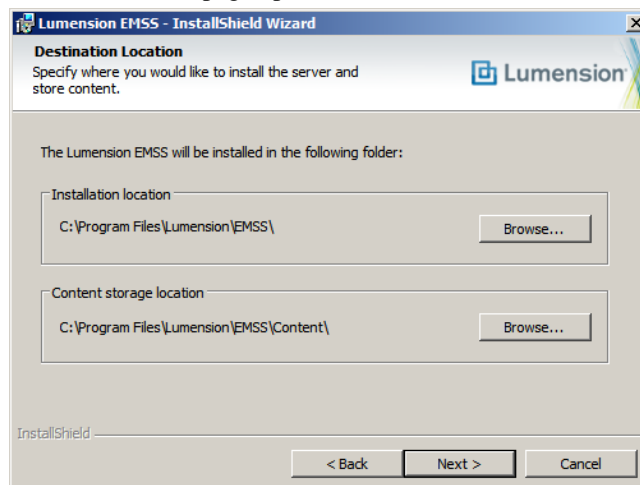


Figure 35: Destination Location Page

4. If desired, change the Lumension EMSS installation location.

- Click **Browse**.
- Define the desired file path using either the **Look in** lists or the **Folder name** field.



c) Click **OK**.

Step Result: The **Installation Folder** field reflects your changes.

Note: Although Lumension EMSS can be installed on a 64-bit server, the program itself is not 64-bit. On 64-bit servers, Lumension recommends installing Lumension EMSS at C:\Program Files (x86).

5. If desired, change the Lumension EMSS content storage location.

The content storage location is the location where patches and other content items are downloaded.

Lumension recommends allocating at least 32 GB of storage space to content (plus an additional 10 GB if managing non-Windows endpoints).

a) Click **Browse**.

b) Define the desired file path using either the **Look in** lists or the **Folder name** field.

c) Click **OK**.

Step Result: The **Content Storage Location** field reflects your changes.

6. Click **Next**.

Step Result: The *Proxy Settings* page opens.

Figure 36: Proxy Settings Page

Note: If one or both of the storage directories defined on the *Destination Location* page does not contain the recommended disk space available, the *Proxy Settings* page does not open. Rather, a dialog opens that lets you redefine the storage directories.

7. If your network uses a proxy server to access the Internet, select the **A proxy server is required** check box and type the applicable information in the following fields.

Field	Type
Server Address	The IP address of the applicable proxy server.



Field	Type
Port	The port number used for communication.

Note: You can also configure Lumension EMSS to use a proxy following installation.

8. If your network uses a proxy server to access the Internet, and that proxy requires authentication, select the **Authentication required** check box and type the applicable information in the following fields.

Field	Type
Username	A user name that authenticates with the proxy.
Password	The password associated with the user name.
Confirm Password	The password retyped.

9. Click **Next**.

Step Result: The *Agent to Server Communication* page opens.

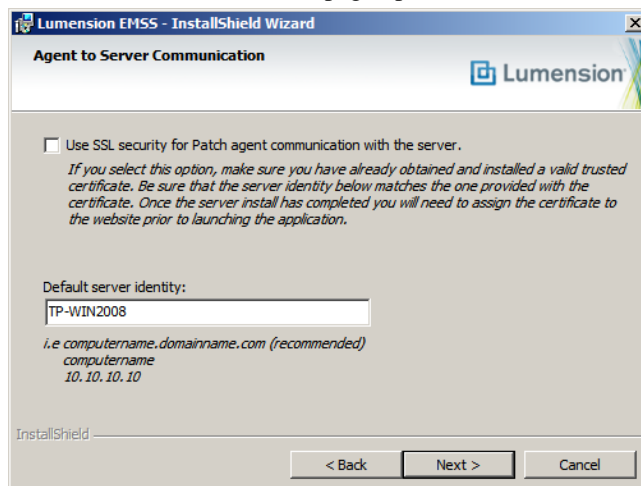


Figure 37: Agent to Server Communication Page

10. If you are using SSL for server and agent communication, select the **Use SSL security for Patch agent communication with the server** check box.

Note: You must possess an SSL certificate to implement SSL communication. Implementation of SSL communication during installation is optional. This feature can be implemented following installation.



11. In the **Default server identity** field, type the name of your server in one of the following formats:

- DNS name (*computername.domainname.com*)
- Computer name (*computername*)
- IP address (*10.10.10.10*)

During agent registration, the Lumension EMSS agents use this name to identify the server.

Note: If using SSL, the server name that you type in the field must match the server named on your certificate.

12. Click **Next**.

Step Result: The *Installation Ready* page opens.

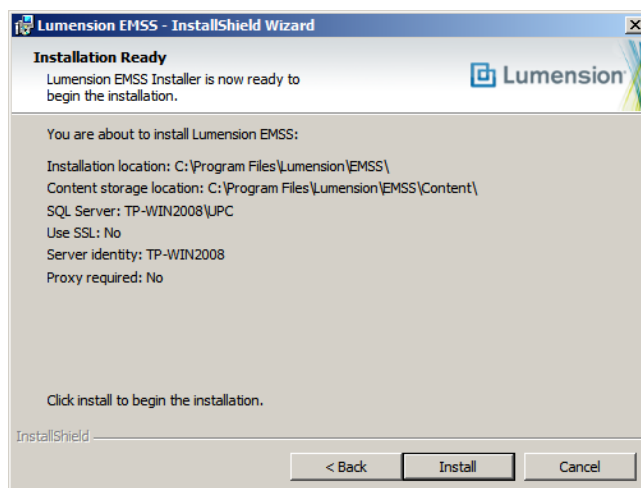


Figure 38: Installation Ready Page

13. Review the installation information and click **Install** to begin the installation of Lumension EMSS.

Important: During installation, do not attempt to access the Lumension EMSS Web site. Accessing the Web site during installation can cause installation errors.

14. After installation completes, click **Finish**.

Result: Lumension EMSS is installed and can now be accessed.

After Completing This Task:

Proceed to one of the following procedures based on selections made during installation.

- If your server will use SSL, finish either *Configuring Windows Server 2003 for SSL* on page 85 or *Configuring Windows Server 2008 for SSL* on page 93.
 - If your server will not use SSL, proceed to *Logging In to Lumension Endpoint Management and Security Suite* on page 73.
-



Logging In to Lumension Endpoint Management and Security Suite

After installing Lumension Endpoint Management and Security Suite (Lumension EMSS), log in to begin configuring the system.

You can log into the system from the server itself or any other endpoint within your network.

1. Open your Web browser.
2. In your browser's address bar, type the Lumension Endpoint Management and Security Suite URL.
3. Press ENTER.

Step Result: The *Connect to* dialog opens.



Figure 39: Connect to Dialog

Note: If using Mozilla Firefox, the dialog appears differently.

4. Type your user name in the **User name** field.
When logging in for the first time, type the user name of the Windows user account used to install Lumension EMSS. You can use additional user names after adding new user profiles to Lumension EMSS. If logging in using a domain account, type the name in the following format: DOMAIN\Username.
5. Type your password in the **Password** field.
6. Click **OK**.

Result: Lumension Endpoint Management and Security Suite opens to the *Home* page and launches the *Application Setup Manager*.

After Completing This Task:

Complete *Setting Up Lumension Endpoint Management and Security Suite* on page 74.



Setting Up Lumension Endpoint Management and Security Suite

Following installation and initial log in, the **Application Setup Manager** opens. Use this dialog to configure basic options within the system. This dialog appears only the first time you log in to Lumension Endpoint Management and Security Suite (Lumension EMSS).

Prerequisites:

Complete Lumension EMSS installation and open the Web console in your browser.

You cannot reopen this dialog following its completion. However, you can access these settings from various Lumension EMSS pages.

1. Log in to Lumension EMSS. For additional information refer to [Logging In to Lumension Endpoint Management and Security Suite](#) on page 73.

Step Result: Lumension EMSS opens and the **Application Setup Manager** displays. This dialog only appears the first time Lumension EMSS is opened.

Figure 40: Application Setup Manager

2. Ensure the **Customer Info** tab is selected.
3. Type the applicable information in the following fields.

Field	Description
First name	Your first name.



Field	Description
Last name	Your last name.
Company name	Your company name. The company name specified during installation appears by default but can be edited.

4. Select the *Languages* tab.

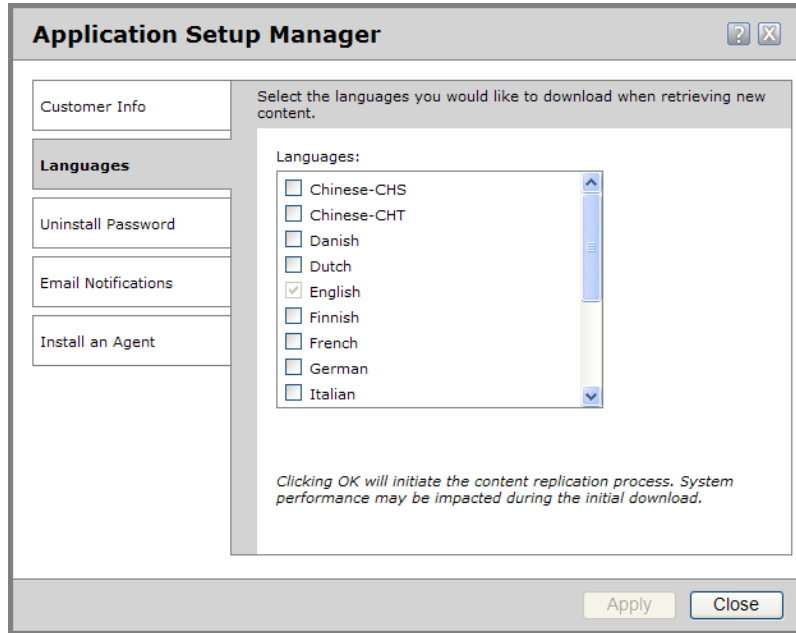


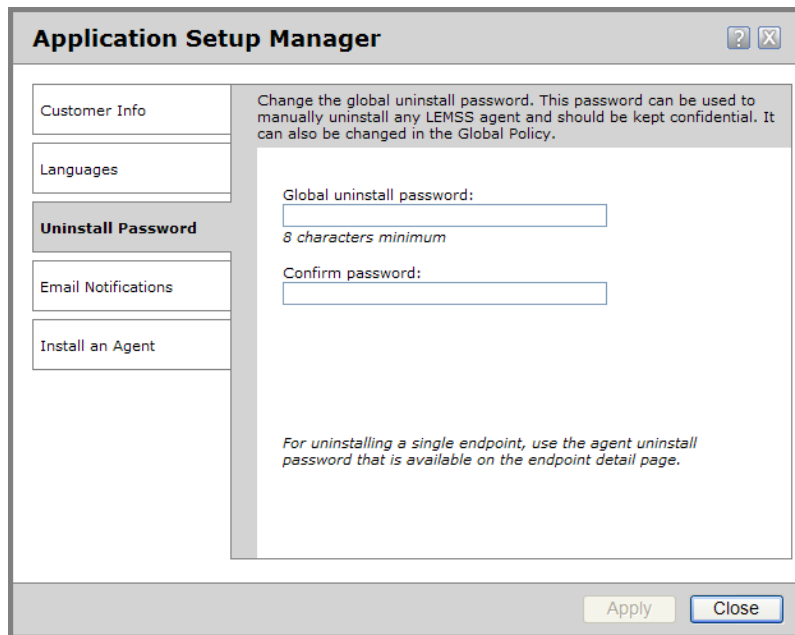
Figure 41: Languages

5. Select the check boxes associated with the languages you want to receive content in.

Each content item available in Lumension EMSS may be available in multiple versions for different languages.



6. Select the *Uninstall Password* tab.



Application Setup Manager [?] [X]

Customer Info

Languages

Uninstall Password

Email Notifications

Install an Agent

Change the global uninstall password. This password can be used to manually uninstall any LEMSS agent and should be kept confidential. It can also be changed in the Global Policy.

Global uninstall password:

8 characters minimum

Confirm password:

For uninstalling a single endpoint, use the agent uninstall password that is available on the endpoint detail page.

Apply Close

Figure 42: Uninstall Password

7. Define the global agent uninstall password.

This password can be used to manually uninstall Lumension EMSS agents and should be kept confidential.



8. Select the *Email Notifications* tab.

Application Setup Manager [?] [X]

Customer Info

Languages

Uninstall Password

Email Notifications

Install an Agent

The SMTP Host and 'From' address are used when the system sends email notifications. You may also specify an email address for receiving system notifications.

SMTP Host:

'From' email address:

'To' email address:

To configure the types of email notifications the system sends go to Tools > Email Notifications.

Apply Close

Figure 43: Email Notifications

9. Define the email information used for email notifications.

Email notifications are alerts sent by Lumension EMSS when certain system events occur.

Type the applicable information in the following fields.

Field	Description
SMTP Host	The local SMTP mail host name. Lumension EMSS uses your corporate Internet (SMTP) mail server.
'From' email address	The email address used when the system sends email notifications.
'To' email address	An email address you use to receive system notifications.



10. Select the ***Install an Agent*** tab.

Note: If upgrading or overwriting a previous installation, the ***Install an Agent*** tab is unavailable. Proceed to step 12.

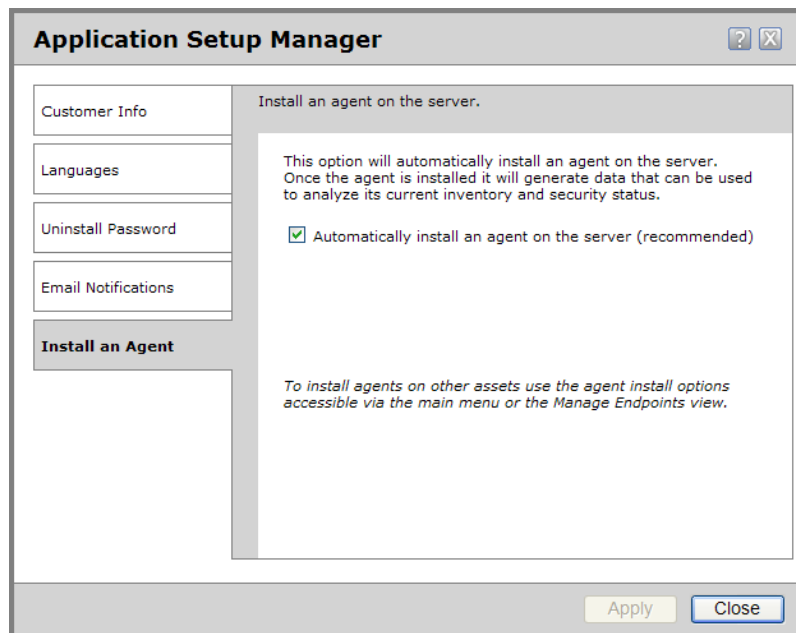


Figure 44: Install an Agent

11. If desired, select the **Automatically install an agent on the server** check box to install an agent on the server.

12. Click **Apply**.

Step Result: Your initial settings are applied.

13. Click **Close**.

Result: Initial configuration is complete. You are now ready to begin monitoring your network with Lumension EMSS.



Appendix

A

Configuring Remote SQL Server Instances

In this appendix:

- Creating Remote Accounts
- Configuring SQL Server to Accept Remote Connections
- Configuring Windows Firewall for SQL Server Instance Access

If you elect to install Lumension Endpoint Management and Security Suite using a remote instance of SQL Server, you must first create two user accounts on the server hosting the instance (provided you are not using preexisting accounts for your installation).

Additionally, you must also configure your instance (and, if in place, its Windows Firewall) to accept remote connections from the server that will host Lumension Endpoint Management and Security Suite.

Procedures to configure remote instances of SQL Server 2008 and SQL Server 2005 are provided, as well as a procedure to create the necessary user accounts.

Creating Remote Accounts

When installing Lumension Endpoint Management and Security Suite using a remote instance of SQL server, you must first create two user accounts on the server hosting your instance: a Web client account and a service account. Lumension Endpoint Management and Security Suite uses these accounts to operate components critical to the system. Without these accounts, Lumension Endpoint Management and Security Suite will be unable to access the remote SQL Server.

Create these accounts on the server hosting your SQL Server instance.

Note: If using domain accounts, these accounts do not have to be created locally. However, any domain account used as the service account must be added to the database server's administrators group. To use a domain account as a service account, complete this task, skipping steps 3-13.

1. Log on to the server hosting your SQL Server instance using either a local or domain user account with system administrator privileges.

If your SQL Server instance uses mixed mode authentication, ensure that the user account you log in with supports SQL Server login.

2. Select **Start > Administrative Tools > Computer Management**.

Step Result: The *Computer Management* dialog opens.

3. Expand the directory tree structure to the **Users** folder (**System Tools > Local Users and Groups > Users**).



4. Right-click the **Users** folder.
5. Select **New User**.

Step Result: The *New User* dialog opens.

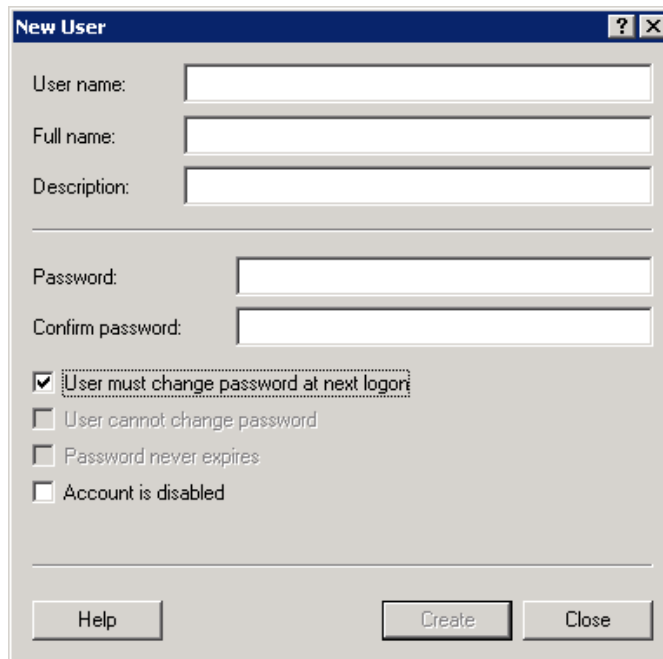


Figure 45: New User Dialog

6. In the **User name** field, type the desired Web client account name (or service account name).
Lumension recommends *clientadmin* for the Web client account, and *serviceadmin* for the service account.
7. In the **Password** field, type the desired password.
8. In the **Confirm Password** field, retype the **Password**.
9. Ensure the **User must change password at next logon** check box is cleared.

Important: When creating these accounts, failure to clear the **User must change password at next logon** will deny you access to the Lumension EMSS Web site following installation.

10. Select the **Password never expires** check box.
11. Click **Create**.
Step Result: The Web client account is created.
12. Repeat steps 6 through 11 to create the service account.
Step Result: The service account is created.
13. Click **Close**.



14. Expand the directory tree structure to the **Groups** folder (**System Tools > Local Users and Groups > Groups**).

15. In the main pane, double-click **Administrators**.

Step Result: The *Administrators Properties* dialog opens.

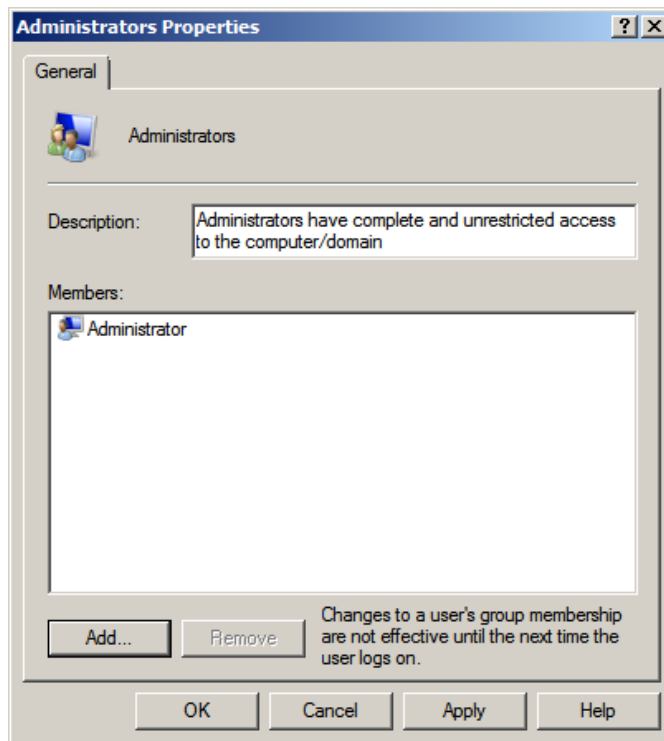


Figure 46: Administrators Properties Dialog



16. Click Add.

Step Result: The *Select Users* dialog opens.

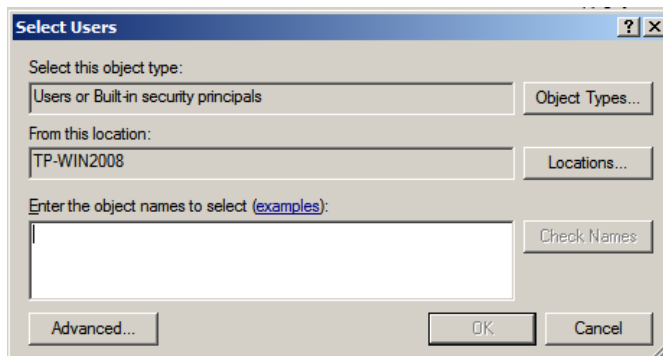


Figure 47: Select Users Dialog

17. In the Enter the object names to select dialog, type your service account name.

18. Click OK.

Step Result: The service account is added to the *Administrators* group.

19. Click OK.

Result: The Web client and service accounts are created.

Configuring SQL Server to Accept Remote Connections

When configuring Lumension Endpoint Management and Security Suite (Lumension EMSS) for use with a remote SQL Server instance, you must configure that instance to accept remote connections.

Perform this task on the server hosting the SQL Server instance you want to use with Lumension EMSS.



1. Open *SQL Server Configuration Manager* (**Start > All Programs > Microsoft SQL Server 2008 [or 2005] > Configuration Tools > SQL Server Configuration Manager**).

Step Result: The *SQL Server Configuration Manager* opens.

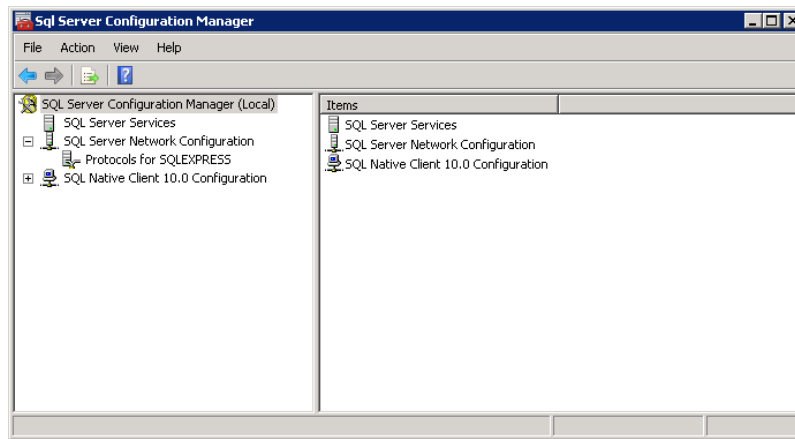


Figure 48: SQL Server Configuration Manager

2. Expand the directory tree structure to the protocols for the instance you are going to use with Lumension EMSS and select it (**SQL Server Network Configuration > Protocols for InstanceName**).
3. Double-click **TCP/IP**.

Step Result: The *TCP/IP Properties* dialog opens.

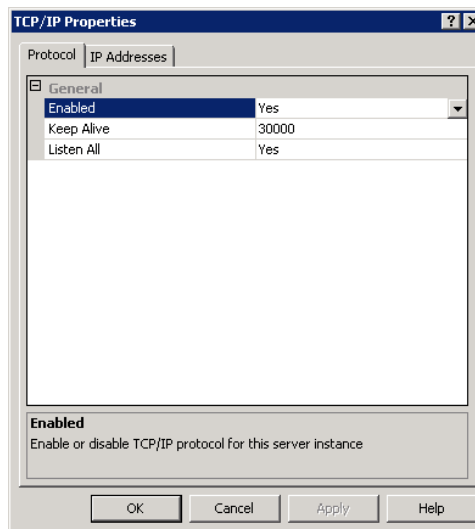


Figure 49: TCP/IP Properties Dialog

4. Ensure the *Protocol* tab is selected.
5. Ensure the **Enabled** list is set to **Yes**.



6. Select the **IP Addresses** tab.
7. Ensure the **Active** list is set to **Yes**.
You can use any desired IP slot (*IP1*, *IP2*, and so on).
8. Ensure the applicable **Enabled** list is set to **Yes**.
9. In the applicable **IP Address** field, type the IP address of the server that will host Lumension EMSS.
10. Click **OK**.
11. Acknowledge the warning by clicking **OK**.
12. If installing Lumension EMSS to a named instance of SQL Server, ensure the SQL Server Browser Service is running.
 - a) From the directory tree structure, select **SQL Server Services**.
 - b) From the main pane, double-click the **SQL Server Browser**.
 - c) Ensure the **Service** tab is selected.
 - d) Ensure that **Automatic** is selected from the **Start Mode** list.
 - e) Click **OK**.
 - f) From the main pane, right-click **SQL Server Browser**.
 - g) Select **Restart** (or **Start** if **Restart** is unavailable).
13. From the main pane, right-click **SQL Server (InstanceName)**.
14. Select **Restart**.

Result: Your SQL Server instance is ready for use with Lumension EMSS. Proceed with the installation procedure (provided your SQL Server instance is not behind Windows Firewall).

After Completing This Task:

If your SQL server instance is behind Windows Firewall, complete *Configuring Windows Firewall for SQL Server Instance Access* on page 84.

Configuring Windows Firewall for SQL Server Instance Access

If you are configuring Lumension Endpoint Management and Security Suite (Lumension EMSS) for use with a remote SQL Server instance, you must configure your SQL Server's Windows Firewall to allow access to Lumension EMSS (if your SQL Server has Windows Firewall enabled).

Configure your SQL Server firewall according to your SQL server instance version. Complete the steps listed in one of the following applicable Microsoft Web sites.

- If you need to configure the Windows firewall on a server hosting a SQL Server 2008 instance, refer to <http://msdn.microsoft.com/en-us/library/ms175043.aspx>.
- If you need to configure the Windows firewall on a server hosting a SQL Server 2005 instance, refer to [http://msdn.microsoft.com/en-us/library/ms175043\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms175043(SQL.90).aspx).

Note: How you edit your Windows Firewall settings changes according to the specific server operating system. The procedures available at the provided links may differ slightly when you edit Windows Firewall settings.



Appendix

B

Configuring Your Server to use SSL

In this appendix:

- Configuring Windows Server 2003 for SSL
- Configuring Windows Server 2008 for SSL

During installation of the Lumension Endpoint Management and Security Suite (Lumension EMSS) server, you can configure Lumension EMSS to use SSL for server to agent communication after obtaining an SSL certificate from a trust provider.

Obtaining a trusted SSL certificate can take several days. Therefore, Lumension recommends obtaining an SSL certificate *before* installing Lumension EMSS. Certificates can be obtained from trust providers such as Verisign Inc. (www.verisign.com) or Entrust (www.entrust.com).

Configuring Windows Server 2003 for SSL

For security purposes, you can configure the Lumension Endpoint Management and Security Suite (Lumension EMSS) server and agent to use SSL communication. To use SSL, assign your certificate to the Lumension EMSS Web site.

Prerequisites:

You must obtain a certificate from a root certificate authority.

Associate your certificate with the Lumension EMSS Web site in your server's *Internet Information Services (IIS) Manager*.

Note: The first portion of this procedure is performed before installation of Lumension EMSS, and the second portion is performed following installation of Lumension EMSS.

Important: If you are installing Lumension EMSS on a server that already hosts a Web site, a different procedure must be used for SSL configuration. For additional information refer to the Knowledge Base at the *Lumension Customer Portal* (<http://portal.lumension.com/>).



1. If necessary, import your certificate.

To import your certificate, complete the following substeps.

- a) Open **Internet Information Services (IIS) Manager** (**Start > Administrative Tools > Internet Information Services [IIS] Manager**).

Step Result: The **Internet Information Services (IIS) Manager** opens.

- b) Expand the directory tree to **Default Web Site** (**Server Name > Web Sites > Default Web Site**).
- c) Right-click **Default Web Site** and select **Properties**.
- d) Select the **Directory Security** tab.
- e) Click **Server Certificate**.

Step Result: The **Web Server Certificate Wizard** opens.



Figure 50: Web Server Certificate Wizard

f) Click **Next**.

Step Result: The *Server Certificate* page opens.

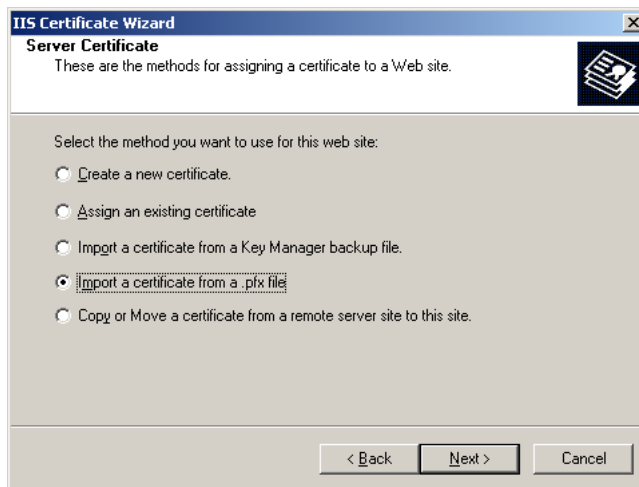


Figure 51: Server Certificate Page

g) Select the **Import a certificate from a .pfx file** option.

h) Click **Next**.

Step Result: The *Import Certificate* page opens.

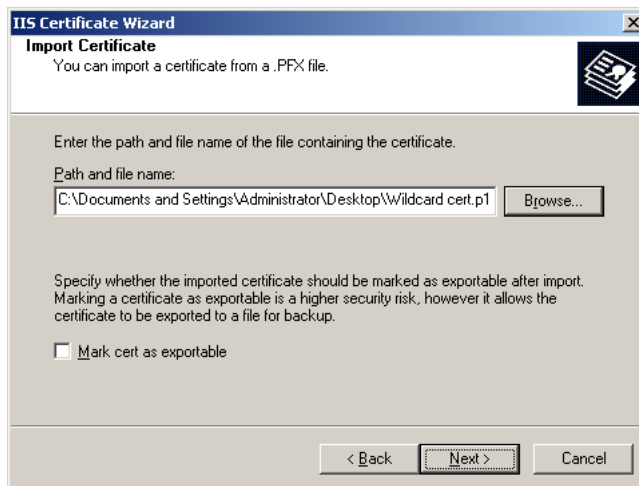


Figure 52: Import Certificate Page

i) Click **Browse**.

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



- j) Browse to and select your certificate.

Note: You may have to select **All Files** from the **Files of type** list to locate your certificate.

- k) Click **Open**.

- l) Click **Next**.

Step Result: The *Import Certificate Password* page opens.

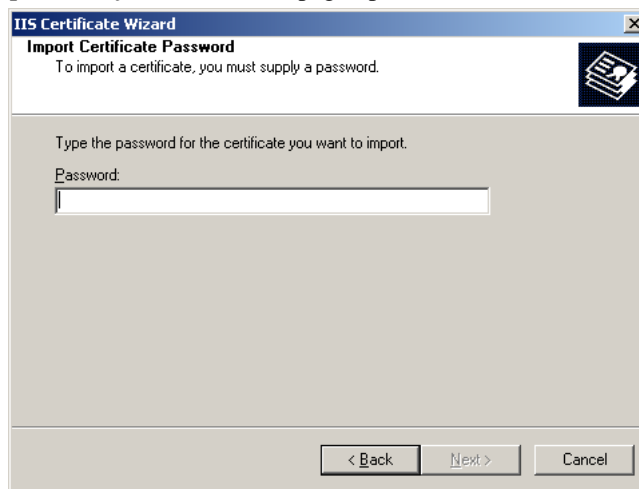


Figure 53: Import Certificate Password Page

- m) Type the certificate's password in the **Password** field.

- n) Click **Next**.

Step Result: The *SSL Port* page opens.

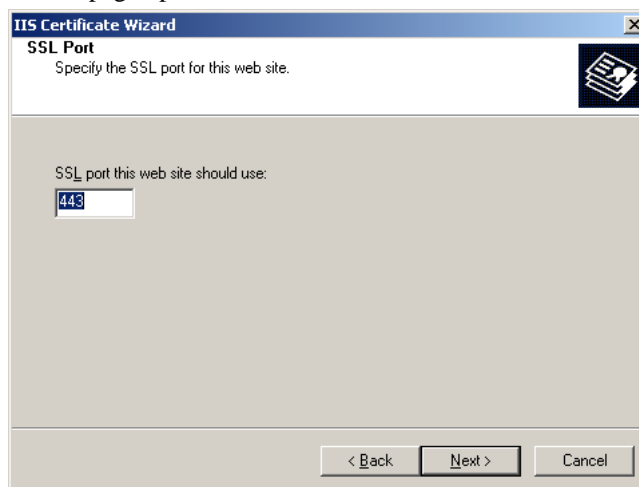


Figure 54: Web Server Certificate Wizard



- o) Type the applicable port number in the *SSL port this Web site should use* field (443 by default).
- p) Click **Next**.

Step Result: The *Imported Certificate Summary* page opens.

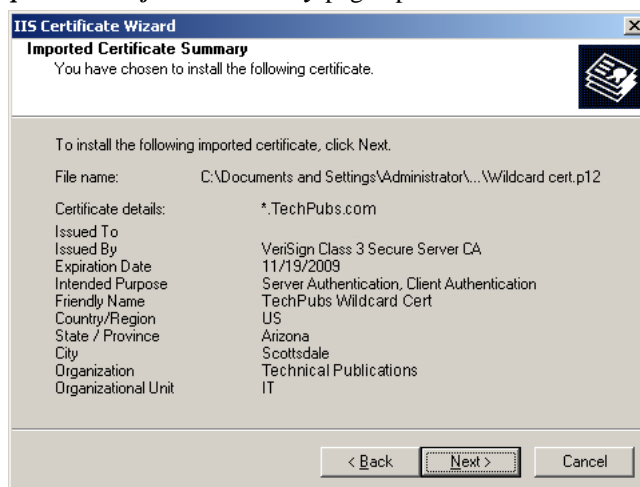


Figure 55: Import Certificate Summary Page

- q) Review the summary and click **Next**.
 - r) Click **Finish**.
2. Complete one of the following Lumension EMSS installation procedures listed in [Selecting an Installation Method](#) on page 23.

While installing Lumension EMSS, select the **Use SSL security for Patch agent communication with the server** check box.

Note: Name resolution of the server, endpoints, and the root certificate authority is required to use SSL.



3. Assign the certificate to the Lumension EMSS Web site.

To assign the certificate, complete the following substeps.

- a) Open **Internet Information Services (IIS) Manager** (Start > Administrative Tools > Internet Information Services [IIS] Manager).

Step Result: The **Internet Information Services (IIS) Manager** opens.

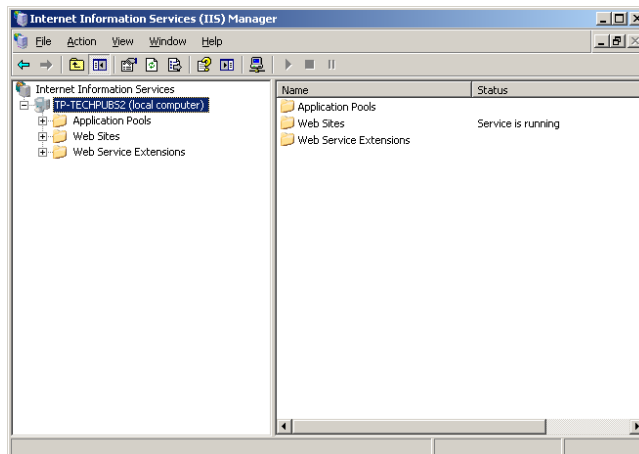


Figure 56: Internet Information Services (IIS) Manager

- b) Expand the directory tree to the **Lumension Web site** (*Server Name* > **Web Sites** > **Lumension**).
- c) Right-click **Lumension** and select **Properties**.
- d) Select the **Directory Security** tab.
- e) Click **Server Certificate**.

Step Result: The **Web Server Certificate Wizard** opens.



Figure 57: Web Server Certificate Wizard

f) Click **Next**.

Step Result: The *Server Certificate* page opens.

g) Select the **Assign an existing certificate** option.

Step Result:

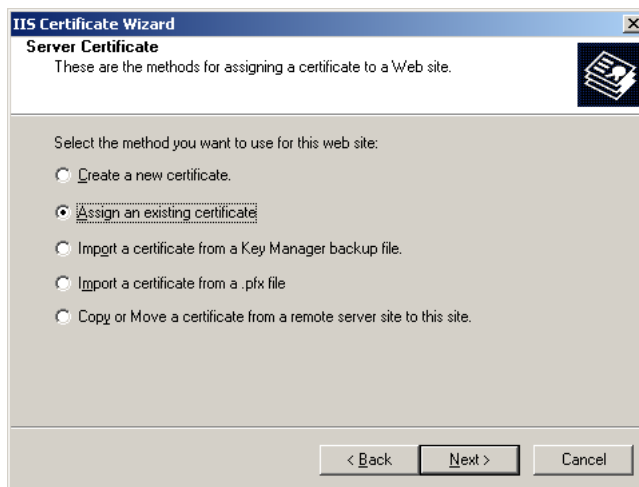


Figure 58: Server Certificate Page

h) Click **Next**.

Step Result: The *Available Certificates* page opens.

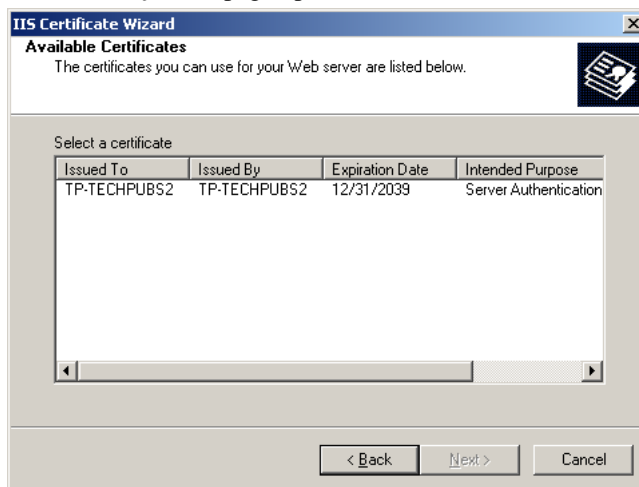


Figure 59: Web Server Certificate Wizard

i) Select your certificate.



j) Click **Next**.

Step Result: The *SSL Port* page opens.

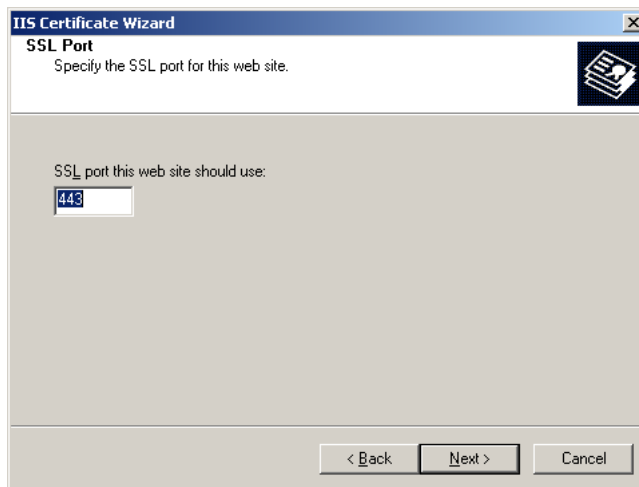


Figure 60: SSL Port Page

k) Type the applicable port number in the **SSL port this Web site should use** field (443 by default).

l) Click **Next**.

Step Result: The *Certificate Summary* page opens.

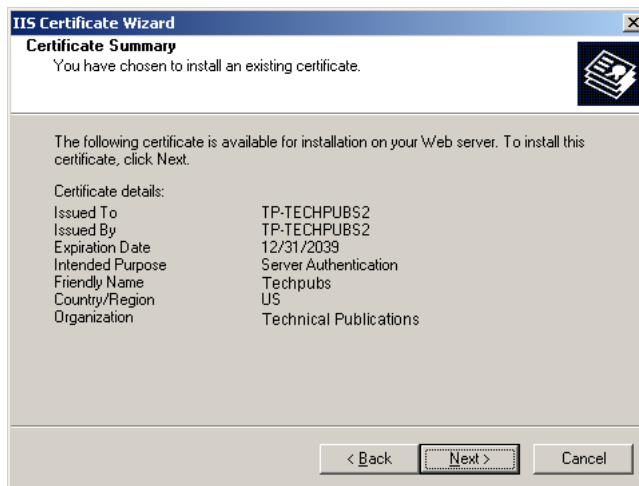


Figure 61: Certificate Summary Page

m) Review the summary and click **Next**.

n) Click **Finish**.



4. Configure the Web site to accept only SSL connections.
 - a) From the *Directory Security* tab, click **Edit**.

Step Result: The *Secure Communications* dialog opens.
 - b) Select the **Require secure channel (SSL)** check box.
 - c) Click **OK**.

Result: Your server is now configured for SSL communication.

After Completing This Task:

- Complete *Logging In to Lumension Endpoint Management and Security Suite* on page 73.
 - Complete *Setting Up Lumension Endpoint Management and Security Suite* on page 74.
 - After you have completed setup, edit your global configuration policy set and set **Use SSL for agent to server communication to True**. For additional information refer to the *Lumension Endpoint Management and Security Suite 7.0 User Guide* (<http://portal.lumension.com>).
-

Configuring Windows Server 2008 for SSL

For security purposes, you can configure the Lumension Endpoint Management and Security Suite (Lumension EMSS) server and agent to use SSL communication. To use SSL, assign your certificate to the Lumension EMSS Web site.

Prerequisites:

You must obtain a certificate from a root certificate authority.

Associate your certificate with the Lumension EMSS Web site in your server's *Internet Information Services (IIS) Manager*.

Note: The first portion of this procedure is performed before installation of Lumension EMSS, and the second portion is performed following installation of Lumension EMSS.

Important: If you are installing Lumension EMSS on a server that already hosts a Web site, a different procedure must be used for SSL configuration. For additional information refer to the Knowledge Base at the *Lumension Customer Portal* (<http://portal.lumension.com/>).

1. If necessary, import your certificate.

To import your certificate, complete the following substeps.

 - a) Open *Internet Information Services (IIS) Manager* (**Start > Administrative Tools > Internet Information Services [IIS] Manager**).

Step Result: The *Internet Information Services (IIS) Manager* opens.



- b) From the directory tree, select your Lumension Endpoint Management and Security Suite server.

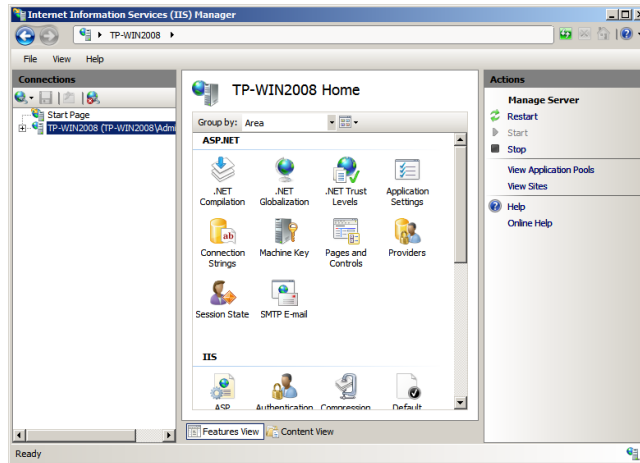


Figure 62: Internet Information Services (IIS) Manager

- c) In the main pane, scroll to the **IIS** section and double-click **Server Certificates**.

Step Result: The *Server Certificates* page opens.

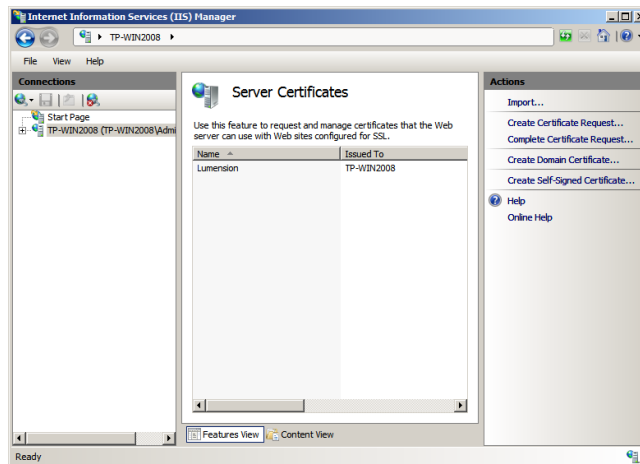


Figure 63: Server Certificates Page



d) Click the **Import** link.

Step Result: The **Import Certificate** dialog opens.

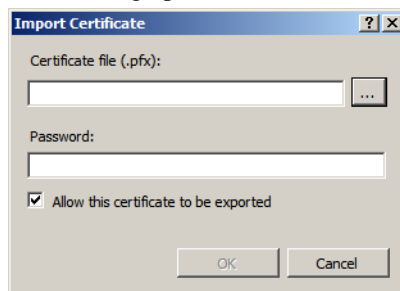


Figure 64: Import Certificate Dialog

e) Click the **Elipses** button (...), browse to your certificate, and click **Open**.

You may have to edit the **File name type** list to see your certificate.

f) Type the applicable password in the **Password** field.

g) Click **OK**.

2. Assign the certificate to the default Web site.

To assign the certificate, complete the following substeps.

a) From the directory tree, expand to **Default Web Site** (*Server Name* > **Sites** > **Default Web Site**).

b) Click the **Bindings** link.

Step Result: The **Site Bindings** dialog opens.

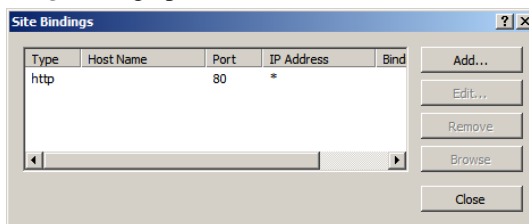


Figure 65: Site Bindings Dialog



c) Click **Add**.

Step Result: The *Add Site Binding* dialog opens.

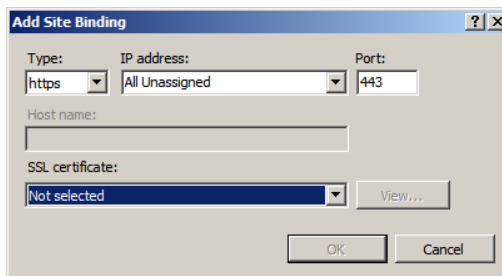


Figure 66: Add Site Bindings Dialog

d) From the **Type** list, select **https**.

e) From the **SSL certificate** list, select your certificate.

f) Click **OK**.

g) Click **Close**.

3. Complete one of the following Lumension EMSS installation procedures listed in *Selecting an Installation Method* on page 23.

While installing Lumension EMSS, select the **Use SSL security for Patch agent communication with the server** check box.

Note: Name resolution of the server, endpoints, and the root certificate authority is required to use SSL.

4. Assign the certificate to the Lumension EMSS Web site.

Complete the following substeps to assign the certificate.

- a) Open *Internet Information Services (IIS) Manager* (**Start > Administrative Tools > Internet Information Services [IIS] Manager**).

Step Result: The *Internet Information Services (IIS) Manager* opens.

- b) From the directory structure, select **Lumension** Web site (*Server Name > Sites > Lumension*).

- c) Click the **Bindings** link.

Step Result: The *Site Bindings* dialog opens.

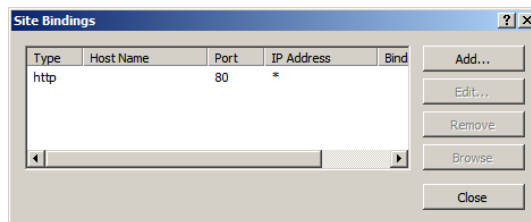


Figure 67: Site Bindings Dialog

d) Click **Add**.

Step Result: The *Add Site Binding* dialog opens.

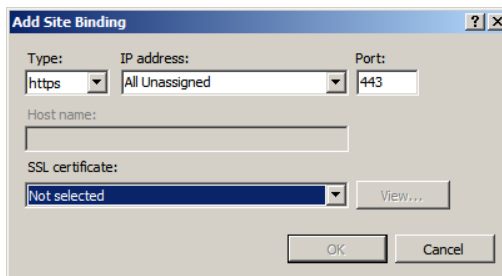


Figure 68: Add Site Bindings Dialog

e) From the **Type** list, select **https**.

f) From the **SSL certificate** list, select your certificate.

g) Click **OK**.

h) Click **Close**.

5. Configure the Web site to accept only SSL connections.

a) In the main pane, scroll to the **IIS** section.

b) Double-click **SSL Settings**.

c) Select the **Require SSL** check box.

d) Click **Apply**.

Result: Your server is now configured for SSL communication.

After Completing This Task:

- Complete *Logging In to Lumension Endpoint Management and Security Suite* on page 73.
- Complete *Setting Up Lumension Endpoint Management and Security Suite* on page 74.
- After you have completed setup, edit your global configuration policy set and set **Use SSL for agent to server communication** to **True**. For additional information refer to the *Lumension Endpoint Management and Security Suite 7.0 User Guide* (<http://portal.lumension.com>).





Appendix

C

Upgrading from Previous Installations

In this appendix:

- Upgrading Lumension Endpoint Management and Security Suite

Lumension routinely releases service packs that upgrade previous product installations. Install these new versions to take advantage of new features.

Rather than deleting the previous product installation, you can upgrade or overwrite the existing installation to the new version by using the latest Lumension Endpoint Management and Security Suite installer.

Upgrading Lumension Endpoint Management and Security Suite

Lumension routinely releases service packs to update Lumension Endpoint Management and Security Suite (Lumension EMSS).

Important: Only Lumension EMSS or Lumension Patch and Remediation 6.4 SP2 or later can be upgraded to Lumension EMSS 7.0 SP1.

When installing Lumension EMSS on a target server that has a previous product version installed, the installer offers two installation scenarios. The following lists describe each installation scenario and important notes to remember when following the applicable scenario.

Scenario	Description
Fresh Install	This option will uninstall any previous product installation and then reinstall the latest version of Lumension EMSS.



Scenario	Description
Upgrade	<p>This option will upgrade your server to the latest version of Lumension EMSS while retaining the data from your previous installation. You may use this option when upgrading from either a previous version of Lumension EMSS or Lumension Patch and Remediation 6.4 SP2 or later. When upgrading from a previous version of Lumension EMSS 7.0, the old version is overwritten by the new install and the database is saved. When upgrading from Patch and Remediation 6.4 SP2, the databases are renamed and saved, the old version is deleted, the new version is written, and then data from the old version is transferred to the new one.</p> <p>The following list itemizes the data retained for each Lumension EMSS feature.</p> <ul style="list-style-type: none"> • Agent policy sets (communication interval, deployment options, SCM policies) • Custom content • Deployment history • Discovery and agent management jobs • Email notification settings • Enhanced content settings • Group settings (system groups, directory services, IP groups, agent-to-group assignments, and other group settings) • Mandatory Baselines • NCA vendor credential information • Server logs • Subscription service communication history • System settings • Users and roles (Windows users, non-deleted system users, and user roles) <hr/> <p>Important: Due to architectural changes from Patch and Remediation 6.4 SP2 to Lumension EMSS 7.0 SP1, certain data cannot be retained when upgrading Patch and Remediation 6.4 SP2. This data includes:</p> <ul style="list-style-type: none"> • Deployment history • Mandatory Baselines • Server logs • System group settings • Subscription history • Content cache status <p>For your convenience, the installation procedure archives this 6.4 SP2 data at <Installation Directory>\Lumension\EMSS\Archive. This data is archived only for reference purposes.</p> <hr/>



Upgrading from Lumension Endpoint Management and Security Suite 7.0

The Lumension Endpoint Management and Security Suite (Lumension EMSS) SP1 installer automatically recognizes any previous versions of the product and then guides you through the upgrade procedure.

Prerequisites:

- Complete *Downloading Lumension Endpoint Management and Security Suite* on page 22.
- As applicable to your network environment, you have gathered the information and completed the tasks defined in the *Server Upgrade Checklist* on page 18.

To initiate the upgrade procedure, open the Lumension EMSS SP1 installer.

1. Log on to the server where you want to install Lumension EMSS using either a local or domain user account with system administrator privileges.
2. Double-click the Lumension EMSS installer at the location defined during downloading.

Step Result: The installer opens to the *Installation Method* page.

Note: If Windows Installer 4.5 or .NET Framework 3.5 are not present on your server, you are notified they will be installed. Additionally, if at any time during the installation procedure you are prompted to reboot, reboot your server. The installer automatically reopens.

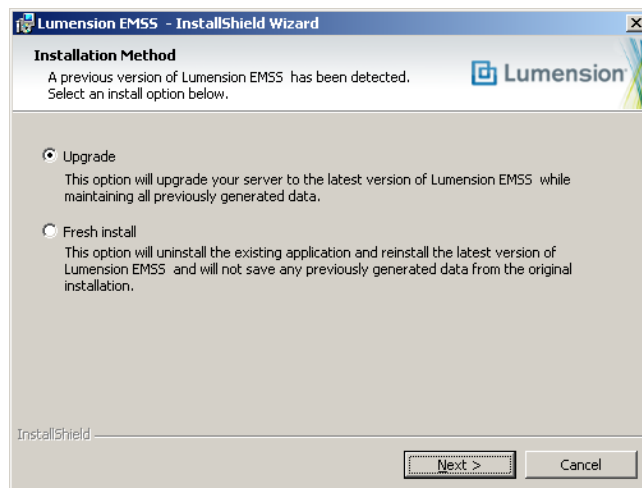


Figure 69: Installation Method Page

3. Ensure the **Upgrade** option is selected.



4. Click **Next**.

Step Result: The *License Agreement* page opens.

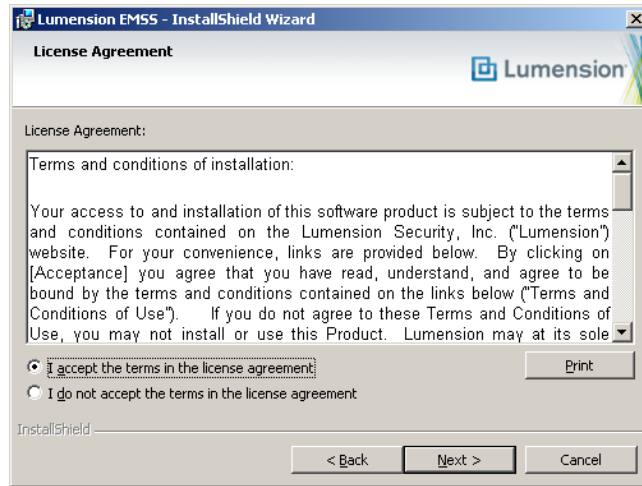


Figure 70: License Agreement Page

Tip: Click **Print** for a hard copy of the license agreement.

5. Review the **License Agreement** and select the **I accept the terms of the license agreement** option.6. Click **Next**.

A new page or dialog opens.

Page/Dialog	Step
If the <i>Question</i> dialog opens:	Click Yes to start network discovery services. These services are necessary to use discovery features within Lumension EMSS.



Page/Dialog	Step
<p>If the <i>Required IIS Features</i> page opens:</p>	<p>Your server does not have the required IIS features installed. Click Next to install the features and proceed.</p> <hr/> <p>Note: On Windows Server 2008, the default installation of IIS lacks components necessary for Lumension EMSS. The Lumension EMSS installer installs the following IIS components if not present:</p> <ul style="list-style-type: none"> • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression <hr/>
<p>If the <i>System Requirements</i> page opens:</p>	<p>Your server does not meet the minimum installation requirements.</p> <ul style="list-style-type: none"> • If you receive only system requirement <i>warnings</i>, you may proceed with installation by clicking Next. Lumension recommends resolving warnings before proceeding with installation. • If you receive any system requirement <i>failures</i>, you must cancel the installation, resolve these failures, and then proceed with installation. <hr/> <p>Tip: Click View all Failures/Warnings for detailed information about prerequisite status deficiencies.</p> <hr/>



Page/Dialog	Step
If the <i>SQL Server Configuration Requirements</i> page opens:	<p>The pre-installed instance of SQL Server is not configured to work with Lumension EMSS.</p> <ul style="list-style-type: none"> If you only receive SQL Server configuration requirement <i>informationals</i> or <i>warnings</i>, click Next to continue (the Lumension EMSS installation will automatically reconfigure SQL Server). Proceed to the next step. If you receive any SQL Server configuration requirement <i>failures</i>, you must cancel the installation, resolve the failures, and then proceed with the installation. <hr/> <p>Tip: Click View all Features/Warnings for detailed information about SQL Server configuration status requirements.</p>
If the <i>Installation Ready</i> page opens:	Proceed to the next step.

7. Click **Install**.

Step Result: The upgrade procedure begins.

Note: During the upgrade procedure, agent hardening is disabled on the server so agents do not have to be uninstalled and reinstalled for the upgrade. Additionally, the upgrade procedure uses the same SQL Server instance used for your previous installation, be it local or remote.

8. After installation completes, click **Finish**.

9. Acknowledge the notification that appears by clicking **OK**.

Result: Your version of Lumension EMSS is upgraded.

After Completing This Task:

Proceed to [Logging In to Lumension Endpoint Management and Security Suite](#) on page 73.

Upgrading from Lumension Patch and Remediation 6.4 SP2

When upgrading from Lumension Patch and Remediation 6.4 SP2, the installation procedure differs slightly.

Prerequisites:

- Complete [Downloading Lumension Endpoint Management and Security Suite](#) on page 22.
 - As applicable to your network environment, you have gathered the information and completed the tasks defined in the [Server Upgrade Checklist](#) on page 18.
-

To initiate the upgrade procedure, open the Lumension EMSS installer.

- Log on to the server where you want to install Lumension EMSS using either a local or domain user account with system administrator privileges.



2. Double-click the Lumension EMSS installer at the location defined during downloading.

Step Result: The installer opens to the *Installation Method* page.

Note: If Windows Installer 4.5 or .NET Framework 3.5 are not present on your server, you are notified they will be installed. Additionally, if at any time during the installation procedure you are prompted to reboot, reboot your server. The installer automatically reopens.

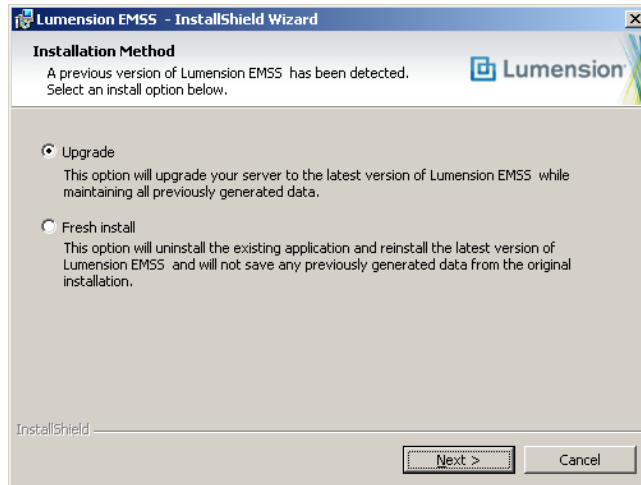


Figure 71: Installation Method Page

3. Ensure the **Upgrade** option is selected.



4. Click Next.

Step Result: The *License Agreement* page opens.

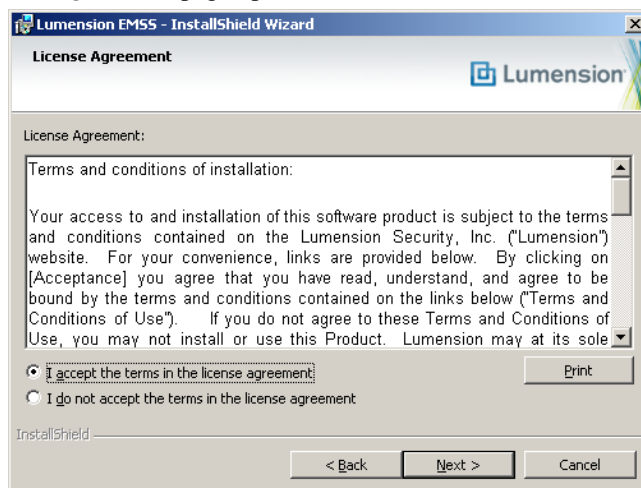


Figure 72: License Agreement Page

Tip: Click **Print** for a hard copy of the license agreement.

5. Review the License Agreement and select the I accept the terms of the license agreement option.

6. Click **Next**.

A new page or dialog opens.

Page/Dialog	Step
<p>If the <i>Required IIS Features</i> page opens:</p>	<p>Your server does not have the required IIS features installed. Click Next to install the features and proceed.</p> <hr/> <p>Note: On Windows Server 2008, the default installation of IIS lacks components necessary for Lumension EMSS. The Lumension EMSS installer installs the following IIS components if not present:</p> <ul style="list-style-type: none"> • Static Content • Default Document • HTTP Errors • ASP.NET • .NET Extensibility • ASP • ISAPI Extensions • ISAPI Filters • Basic Authentication • Windows Authentication • Static Content Compression • Dynamic Content Compression <hr/>
<p>If the <i>System Requirements</i> page opens:</p>	<p>Your server does not meet the minimum installation requirements.</p> <ul style="list-style-type: none"> • If you receive only system requirement <i>warnings</i>, you may proceed with installation by clicking Next. Lumension recommends resolving warnings before proceeding with installation. • If you receive any system requirement <i>failures</i>, you must cancel the installation, resolve these failures, and then proceed with installation. <hr/> <p>Tip: Click View all Failures/Warnings for detailed information about prerequisite status deficiencies.</p> <hr/>



Page/Dialog	Step
<p>If the <i>SQL Server Configuration Requirements</i> page opens:</p>	<p>The pre-installed instance of SQL Server is not configured to work with Lumension EMSS.</p> <ul style="list-style-type: none"> • If you only receive SQL Server configuration requirement <i>informationals</i> or <i>warnings</i>, click Next to continue (the Lumension EMSS installation will automatically reconfigure SQL Server). Proceed to the next step. • If you receive any SQL Server configuration requirement <i>failures</i>, you must cancel the installation, resolve the failures, and then proceed with the installation. <hr/> <p>Tip: Click View all Features/Warnings for detailed information about SQL Server configuration status requirements.</p>
<p>If the <i>Service Accounts</i> page opens:</p>	<p>Proceed to the next step.</p>

7. Define usernames and passwords for the Web client account and service account that Lumension EMSS uses.
 - a) If desired, edit the **Web Client Account Username** field.
 - b) In the **Web Client Account Password** field, type the desired password.
 - c) In the **Web Client Account Confirm password** field, retype the password.
 - d) If desired, edit the **Service Account Username** field.
 - e) In the **Service Account Password** field, type the desired password.
 - f) In the **Service Account Confirm password** field, retype the password.

Note: Lumension recommends using the default Web client account and service account user names.



8. Click Next.

Step Result: The *Server Identity* page opens.

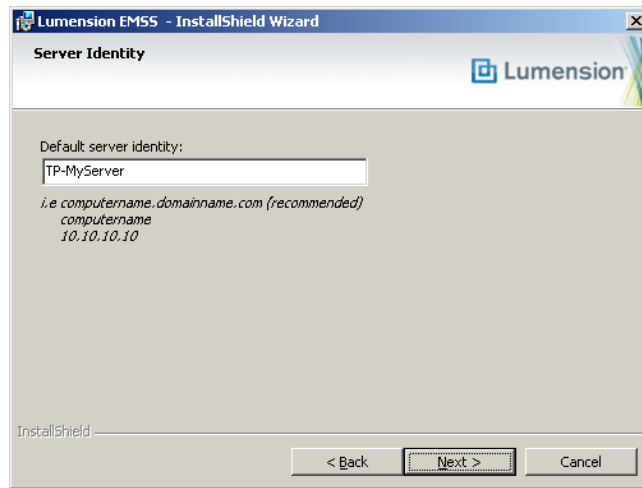


Figure 73: Server Identity Page

9. In the **Default server identity field, type the name of your server in one of the following formats:**

- DNS name (*computername.domainname.com*)
- Computer name (*computername*)
- IP address (*10.10.10.10*)

During agent registration, the Lumension EMSS agents use this name to identify the server.

Note: If using SSL, the server name that you type in the field must match the server named on your certificate.



10. Click Next.

Step Result: The *Destination Location* page opens.

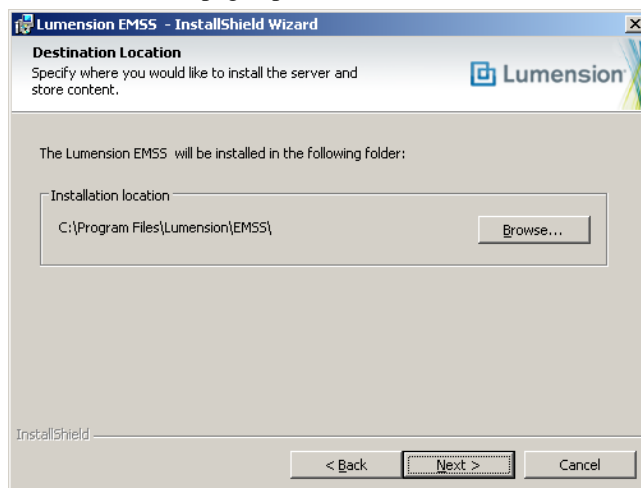


Figure 74: Destination Location Page

11. If desired, change the Lumension EMSS installation location.

- a) Click **Browse**.
- b) Define the desired file path using either the **Look in** lists or the **Folder name** field.
- c) Click **OK**.

Step Result: The **Installation Folder** field reflects your changes.

Note: Although Lumension EMSS can be installed on a 64-bit server, the program itself is not 64-bit. On 64-bit servers, Lumension recommends installing Lumension EMSS at C:\Program Files (x86).

12. Click Next.

Important: Due to architectural changes from Patch and Remediation 6.4 SP2 to Lumension EMSS 7.0 SP1, certain data cannot be retained when upgrading Patch and Remediation 6.4 SP2. This data includes:

- Deployment history
- Mandatory Baselines
- Server logs
- System group settings
- Subscription history
- Content cache status



For your convenience, the installation procedure archives this 6.4 SP2 data at <Installation Directory>\Lumension\EMSS\Archive. This data is archived only for reference purposes.

Step Result: The *Data Accessibility* page opens. This page lists the data that will be retained during the upgrade.

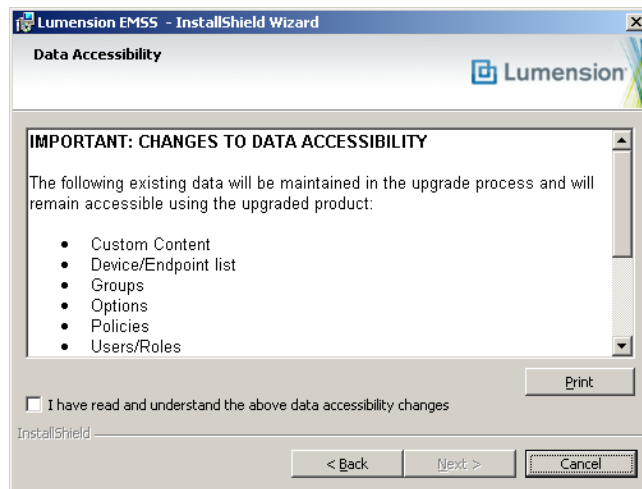


Figure 75: Data Accessibility Page

Note: If the storage directory defined on the *Destination Location* page does not contain the recommended disk space available, the *Data Accessibility* page does not open. Rather, a dialog opens that lets you redefine the storage location.

13. Review the notification and select the **I have read and understand the above data accessibility changes** check box.



14. Click Next.

Step Result: The *Installation Ready* page opens.

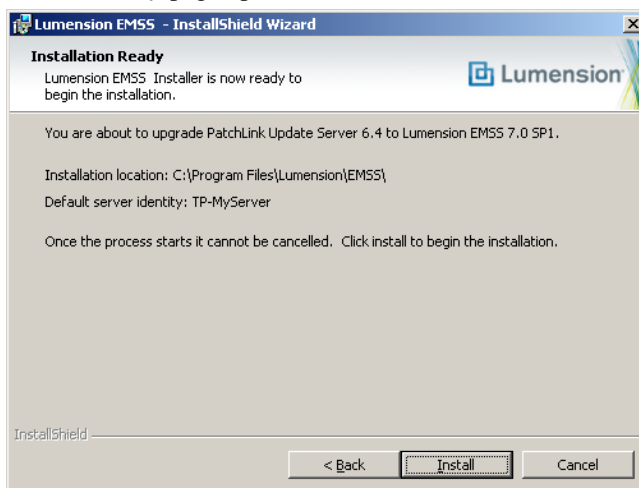


Figure 76: Installation Ready Page

15. Click Install.

Step Result: The upgrade procedure begins.

Note: During the upgrade procedure, agent hardening is turned off on the server so agents do not have to be uninstalled and reinstalled for the upgrade. Additionally, the upgrade procedure uses the same local SQL Server instance used for your previous installation.

16. After installation completes, click Finish.**17. Acknowledge the notification that appears by clicking OK.**

Result: Patch and Remediation 6.4 SP2 is upgraded to Lumension EMSS 7.0 SP1.

After Completing This Task:

Proceed to *Logging In to Lumension Endpoint Management and Security Suite* on page 73.



Installing Cleanly Over an Existing Installation

You can install Lumension Endpoint Management and Security Suite (Lumension EMSS) cleanly over previous versions of existing product installations. Installing the product cleanly over a previous installation completely removes the existing version, along with any associated data.

Prerequisites:

- Complete *Downloading Lumension Endpoint Management and Security Suite* on page 22.
- As applicable to your network environment, you have gathered the information and completed the tasks defined in the *Server Upgrade Checklist* on page 18.

Note: The Lumension EMSS installation includes creation of a Web client account and a service account. These accounts are used to operate components critical to Lumension EMSS. However, you may use preexisting accounts if they meet the requirements itemized in *Defining the Web Client Account and Service Account* on page 22.

Lumension recommends creating new accounts via the Lumension EMSS installer.

Begin a clean installation by opening the latest Lumension EMSS installer on your Lumension EMSS server.

1. Log on to the server where you want to install Lumension EMSS using either a local or domain user account with system administrator privileges.
2. From its download location, double-click the Lumension EMSS installer.

Step Result: The installer opens to the *Installation Method* page.

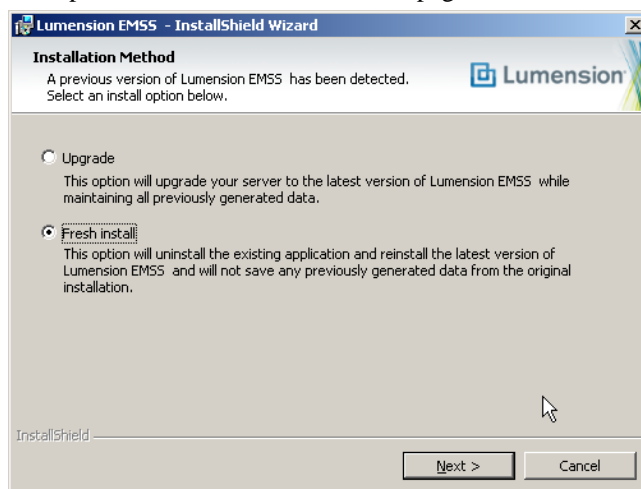


Figure 77: Installation Method Page

3. Ensure the **Fresh install** option is selected.



4. Click **Next** and complete the applicable installation procedures listed in *Selecting an Installation Method* on page 23.

Important: All data from your previous install will be deleted. Additionally, if using an preexisting instance of SQL Server, the instance cannot contain any data from previous installations.



Appendix

D

Installation Checklist

In this appendix:

- Server Installation Checklist
- Server Upgrade Checklist

For your convenience, an additional installation checklist and upgrade checklist are provided.

Server Installation Checklist

This checklist itemizes the information you will need and tasks you will need to complete when installing the Lumension Endpoint Management and Security Suite (Lumension EMSS) server.

Prior to installing Lumension EMSS, you must gather and confirm the following information:

- Your target computer meets or exceeds the requirements defined in *System Requirements* on page 11.
- Your server is *not* a Domain Controller.
- Internet Information Services (IIS) is installed and running. If necessary refer to one of the following links for details about IIS:
 - *How to Configure a Computer Running Windows Server 2003 as a Web Server* (<http://support.microsoft.com/kb/324742>)
 - *Install IIS 7 on Windows Server 2008* (<http://learn.iis.net/page.aspx/29/installing-iis-70-on-windows-server-2008>)
- All required service packs have been installed, as defined in *System Requirements* on page 11.
- If your server is a member of a domain, only the default security policies are in effect.
- Your server DNS host name is: _____
- Your local SMTP mail host name is: _____
- Your Lumension EMSS serial number is: _____ - _____
- Your target system is connected to the Internet.



- If you are using SSL, a valid SSL Web certificate has been obtained.
Note: If you are using SSL, you need to obtain a valid Web certificate, from a trust provider such as Verisign Inc. (www.verisign.com) or Entrust (www.entrust.com), prior to installing Lumension EMSS.
- If you are using SSL, you have started the first portion of one of the following topics based on your operating system (the second portion is completed after installation).
 - [Configuring Windows Server 2003 for SSL](#) on page 85
 - [Configuring Windows Server 2008 for SSL](#) on page 93
- If a proxy server will be used, you know the proxy server's name, IP address, port, user name, and password.
 - Name: _____
 - IP address: ____ - ____ - ____ - ____
 - Port: _____
 - User name: _____
 - Password: _____
- If you are using a preexisting instance of SQL Server, the instance is set to one of the following collation values:
 - SQL_Latin1_General_CP1_CI_AS
 - Latin1_General_CI_AS
- If you are using a remote instance of SQL Server, the server hosting the instance is set to an English locale.
- If you are using a remote SQL instance, the instance is configured to accept remote connections. For additional information refer to [Configuring SQL Server to Accept Remote Connections](#) on page 82.
- If you are using a remote SQL instance, and that instance is behind a firewall, the firewall is configured to allow the Lumension EMSS server access. For additional information, refer to [Configuring Windows Firewall for SQL Server Instance Access](#) on page 84.

Server Upgrade Checklist

This checklist itemizes the information you will need and tasks you will need to complete when upgrading the Lumension Endpoint Management and Security Suite (Lumension EMSS) server. The information you will gather varies according to your upgrade scenario.

Before upgrading Lumension EMSS 7.0 or Lumension Patch and Remediation 6.4 SP2 to Lumension EMSS 7.0 SP1, you must gather and confirm the following information for both upgrade types (upgrade and fresh install):

- Your target computer meets or exceeds the requirements defined in [System Requirements](#) on page 11.
- Your target server has either Lumension Endpoint Management and Security Suite 7.0 or Lumension Patch and Remediation 6.4 SP2 installed.



- Your server is *not* a Domain Controller.
- Internet Information Services (IIS) is installed and running. If necessary refer to one of the following links for details about IIS:
 - [How to Configure a Computer Running Windows Server 2003 as a Web Server \(http://support.microsoft.com/kb/324742\)](http://support.microsoft.com/kb/324742)
 - [Install IIS 7 on Windows Server 2008 \(http://learn.iis.net/page.aspx/29/installing-iis-70-on-windows-server-2008\)](http://learn.iis.net/page.aspx/29/installing-iis-70-on-windows-server-2008)
- All required service packs have been installed, as defined in [System Requirements](#) on page 11.
- If your server is a member of a domain, only the default security policies are in effect.
- Your server DNS host name is: _____
- Your local SMTP mail host name is: _____

Prior to upgrading Lumension EMSS 7.0 or Lumension Patch and Remediation 6.4 SP2 to Lumension EMSS 7.0 SP1 via a fresh installation, you must gather and confirm the additional following information.

- Your Lumension EMSS serial number is: _____ - _____
- Your target system is connected to the Internet.
- If you are using SSL, a valid SSL Web certificate has been obtained.

Note: If you are using SSL, you need to obtain a valid Web certificate, from a trust provider such as Verisign Inc. (www.verisign.com) or Entrust (www.entrust.com), prior to installing Lumension EMSS.

- If you are using SSL, you have started the first portion of one of the following topics based on your operating system (the second portion is completed after installation).
 - [Configuring Windows Server 2003 for SSL](#) on page 85
 - [Configuring Windows Server 2008 for SSL](#) on page 93
- If a proxy server will be used, you know the proxy server's name, IP address, port, user name, and password.
 - Name: _____
 - IP address: ____-____-____-____
 - Port: _____
 - User name: _____
 - Password: _____
- If you are using a remote instance of SQL Server, the server hosting the instance is set to an English locale.



- If you are using a preexisting instance of SQL Server, the instance is set to one of the following collation values:
 - SQL_Latin1_General_CP1_CI_AS
 - Latin1_General_CI_AS
- If you are using a remote SQL instance, the instance is configured to accept remote connections. For additional information refer to [Configuring SQL Server to Accept Remote Connections](#) on page 82.
- If you are using a remote SQL instance, and that instance is behind a firewall, the firewall is configured to allow the Lumension EMSS server access. For additional information, refer to [Configuring Windows Firewall for SQL Server Instance Access](#) on page 84.

