Стратегия глубокой защиты

или

О чем мечтают администраторы ИТ и ИБ?

Edvinas Pranculis MM, CISA, CISM, CRISC
Региональный директор по продажам
Центральная и Восточная Европа, Скандинавия, Россия, Кавказ и Средняя Азия
edvinas.pranculis@lumension.com

Lumension™
IT Secured. Success Optimized.

Новая среда

Lumension™
IT Secured. Success Optimized.

БРЕМЯ КОМПЛАЕНС-КОНТРОЛЯ

РАЗВИТИЕ ВРЕДОНОСНОГО КОДА

ЕВОЛЮЦИЯ КОРПОРАТИВНОЙ СЕТИ

ХАКЕРЫ

КОНКУРЕНТЫ

ОРГАНИЗОВАННЫЕ
ПРЕСТУПНИКИ

ИНОСТРАННЫЕ
ПРАВИТЕЛЬСТВА

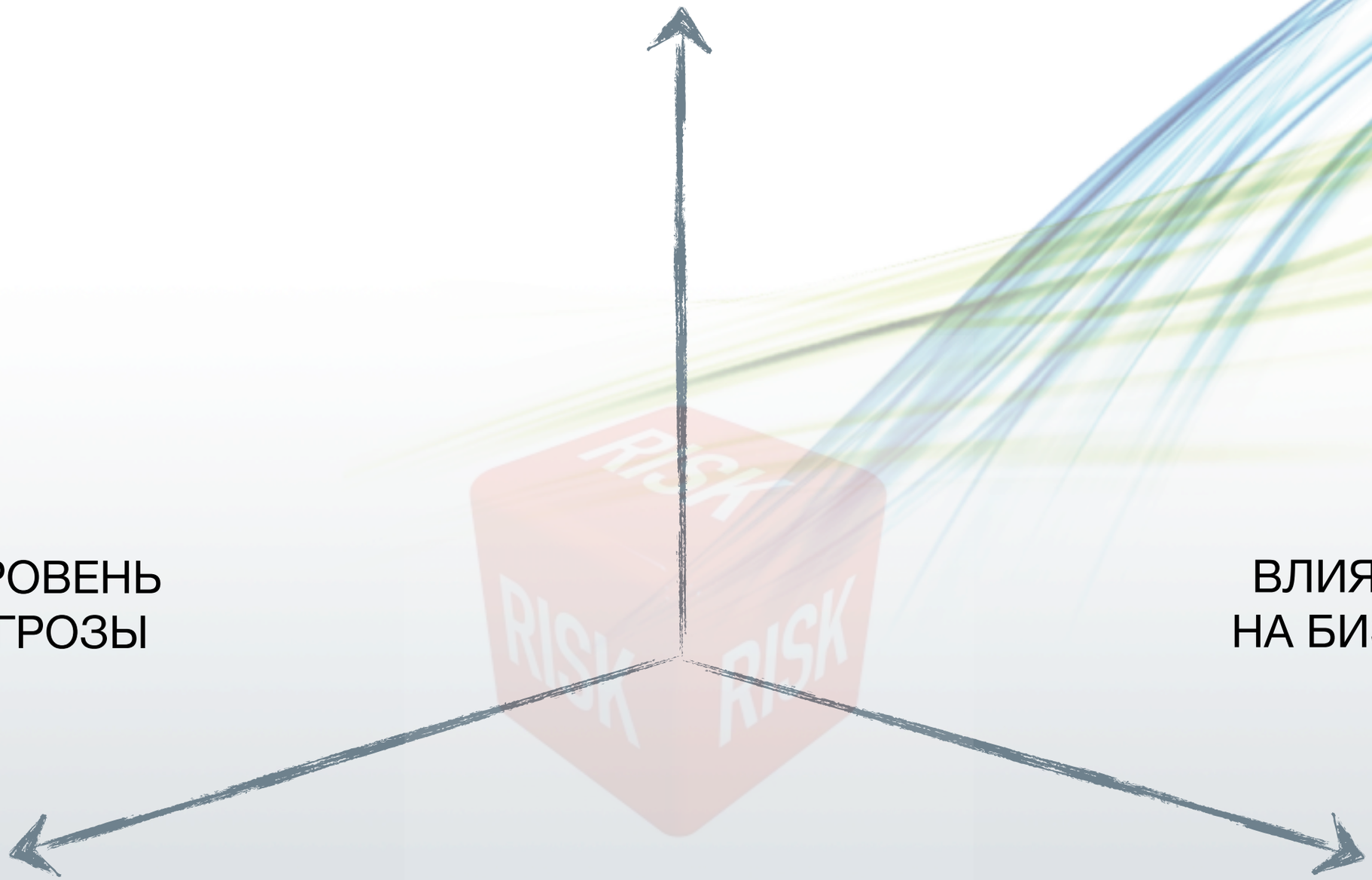
ТЕРРОРИСТЫ

ИНСАЙДЕРЫ

Риск Менеджмент

Lumension™
IT Secured. Success Optimized.

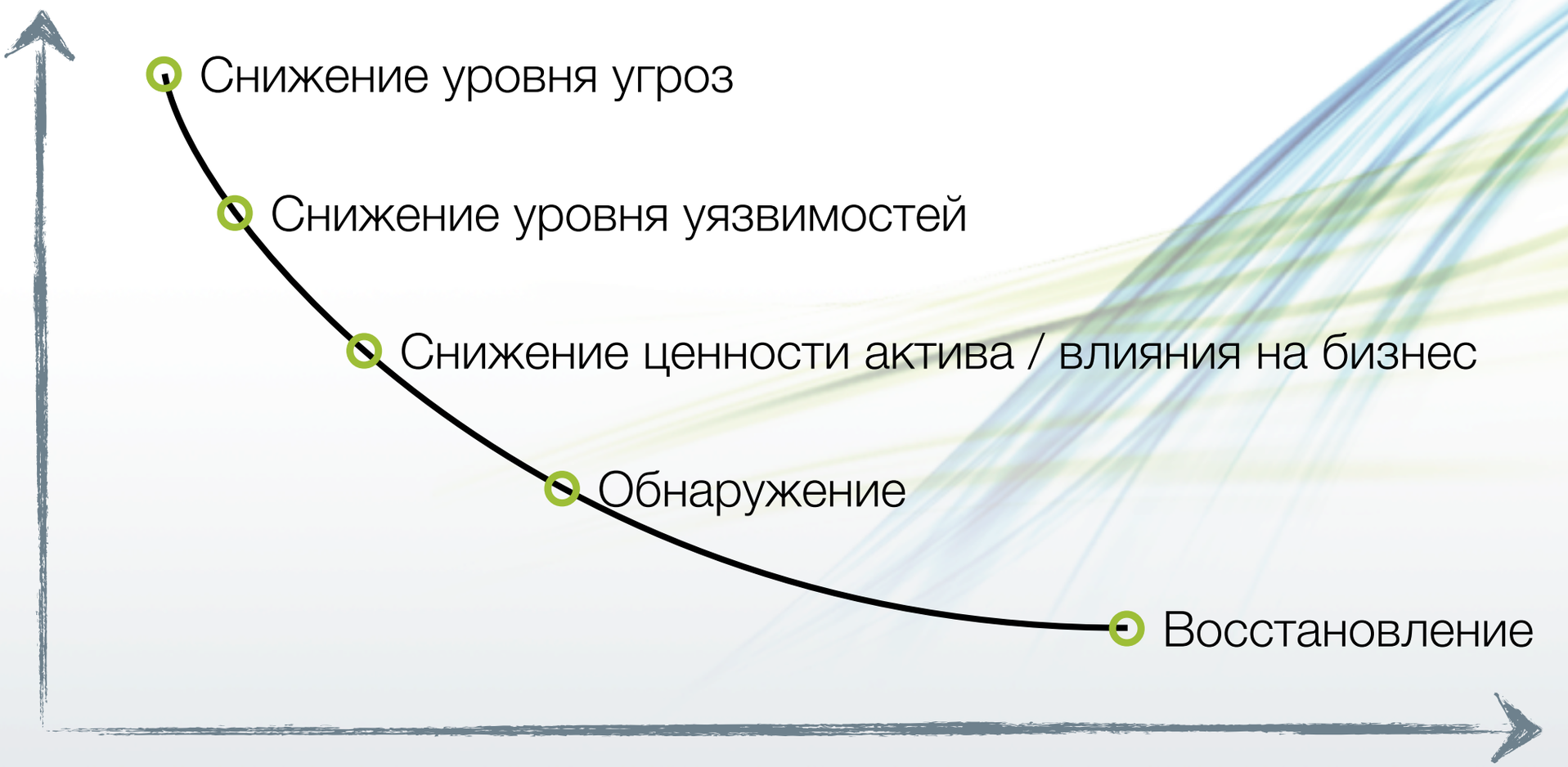
УРОВЕНЬ
УЯЗВИМОСТЕЙ



УРОВЕНЬ
УГРОЗЫ

ВЛИЯНИЕ
НА БИЗНЕС

РЕЗУЛЬТАТИВНОСТЬ



СТОИМОСТЬ

Одно решение

для многослойной защиты

Lumension™
IT Secured. Success Optimized.

Lumension™

IT Secured. Success Optimized.

www.lumension.com

Vulnerability Management I Endpoint Protection I Data Protection I Reporting and Compliance

20+ лет на рынке

5100+ клиентов

70+ стан

14+ милионов конечных точек

www.lumension.com

Vulnerability Management I Endpoint Protection I Data Protection I Reporting and Compliance

Lumension™
IT Secured. Success Optimized.

Глубокая защита

Что это такое?

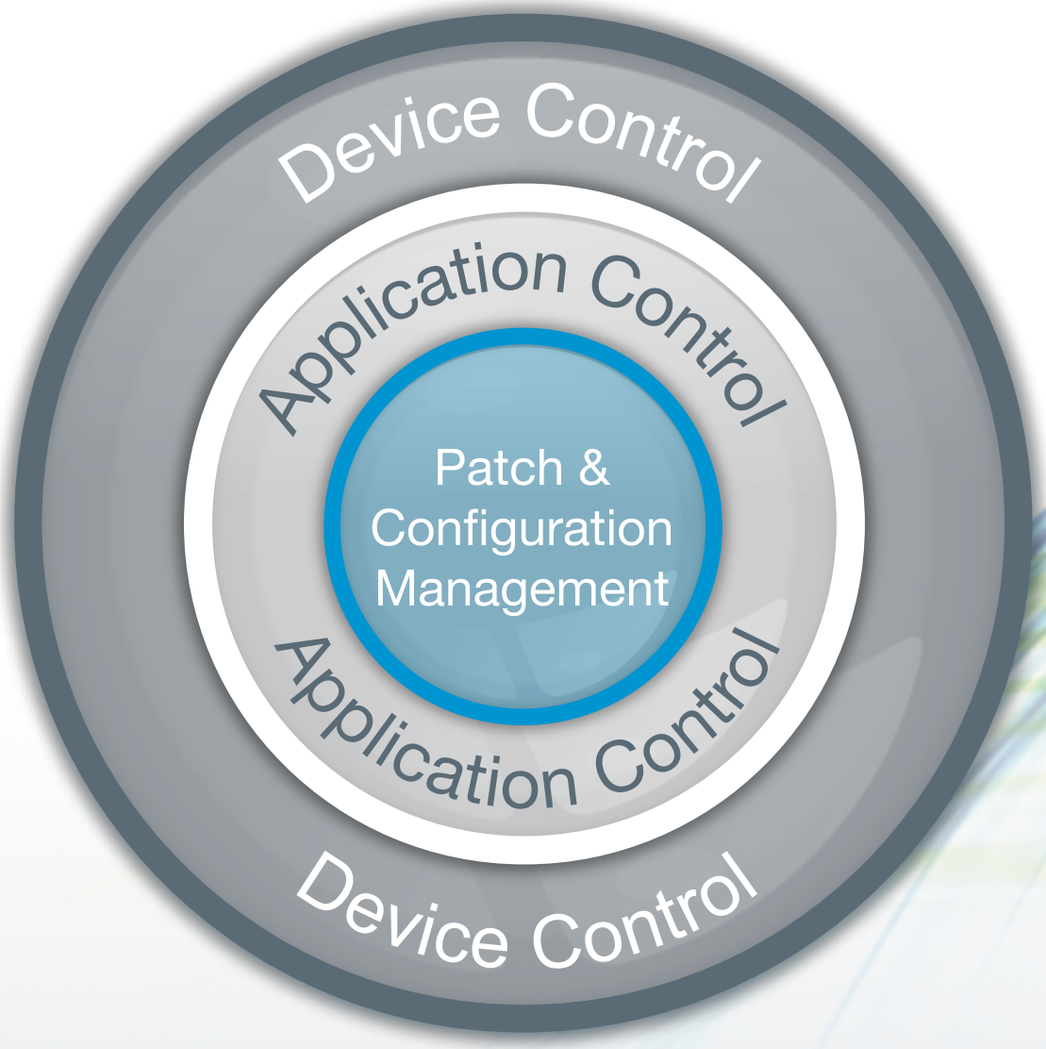
Lumension™
IT Secured. Success Optimized.

Больше чем 90% кибер-атак реализуются через известные уязвимости, для которых существуют исправления

- Gartner Group -

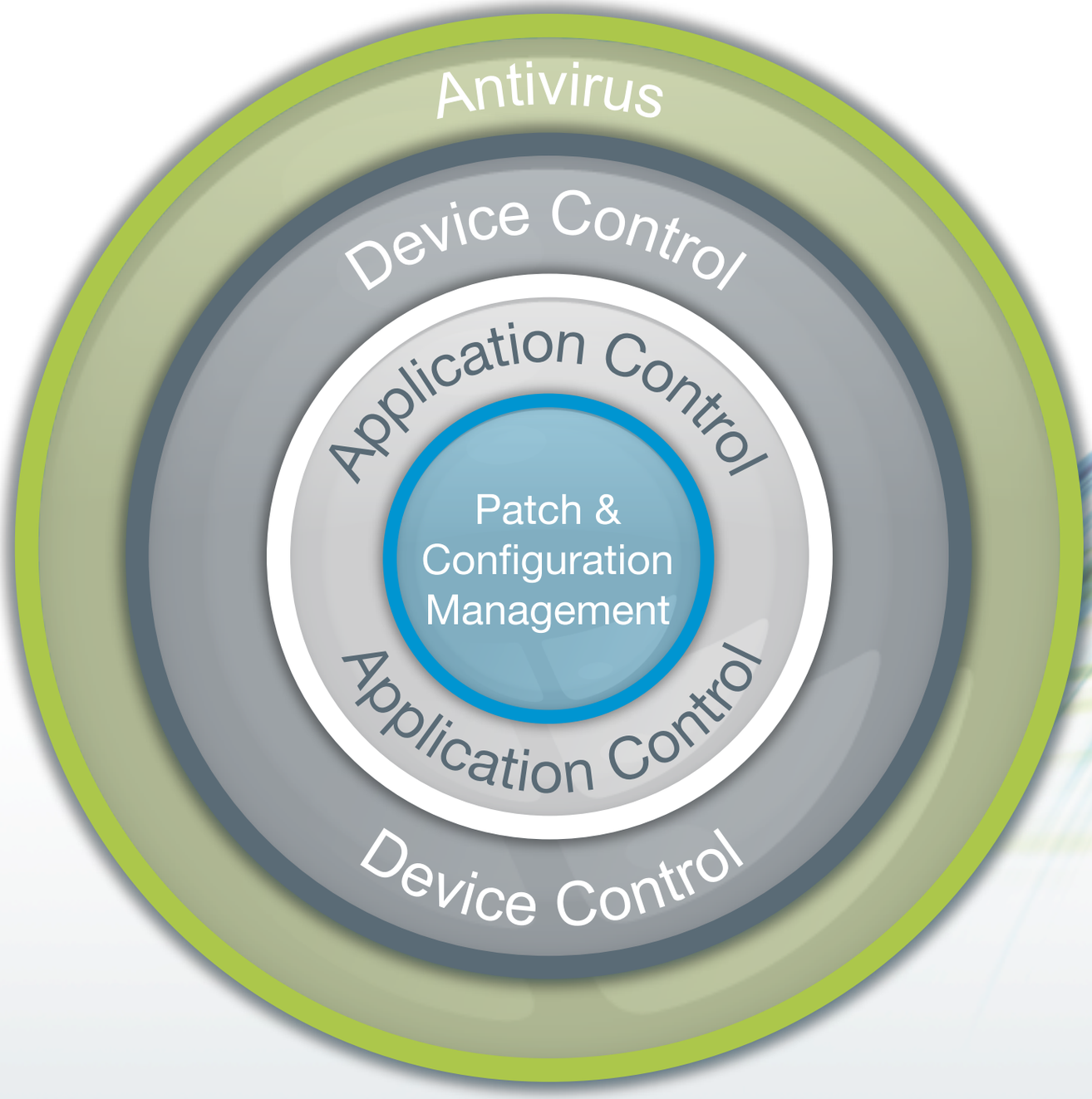
Каждый месяц появляется почти 3 милиона сигнатур вредоносного кода

- AV-Test.org -



2012 году было проданно ~4 милиярда USB устройств

- Ponemon Institute -



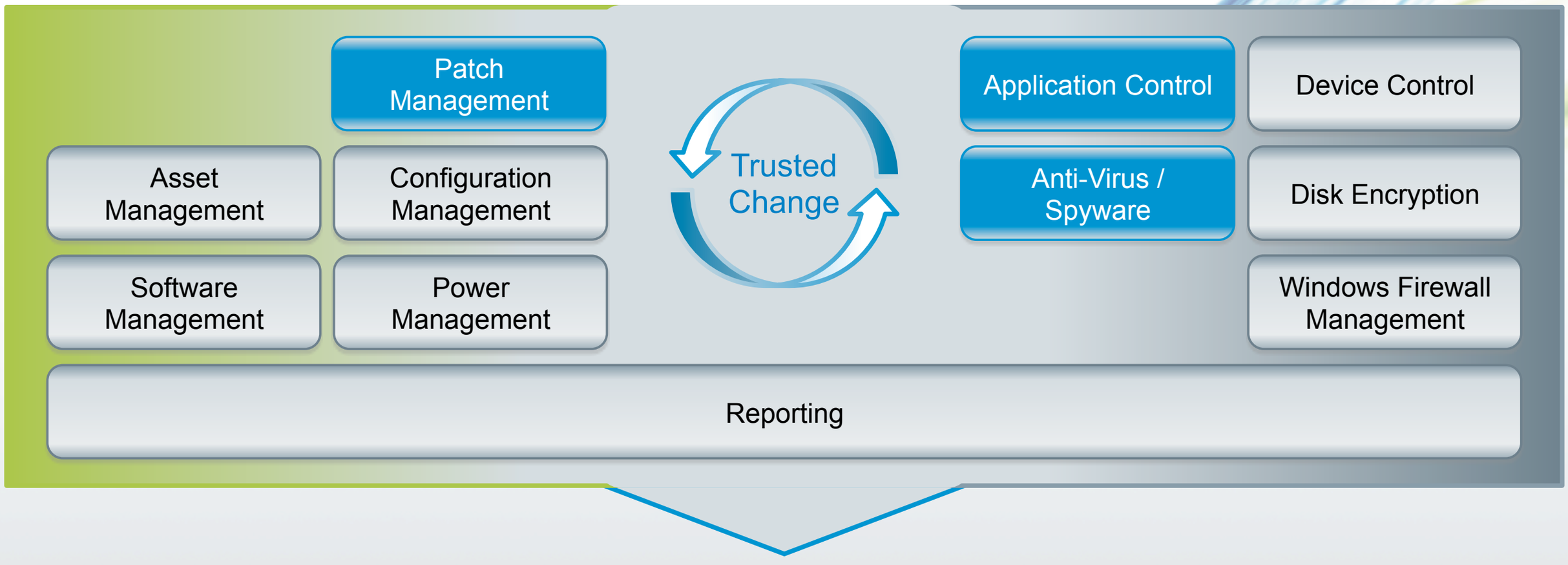
В первый день опознается < 20% вредоносного кода,
и только 62% - через 30 дней

- Cyveillance -

Endpoint Operations

Intelligent Whitelisting

Endpoint Security

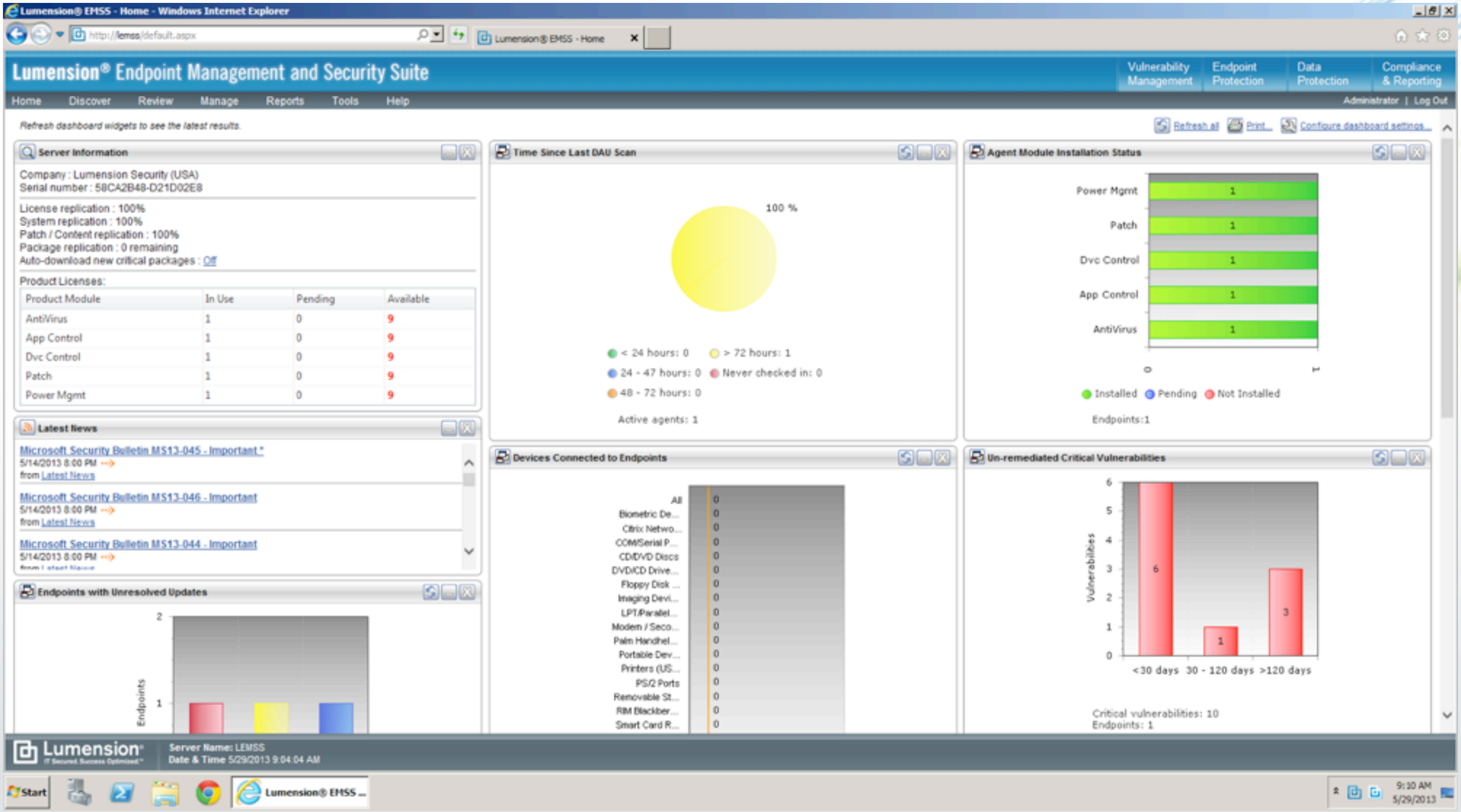


Одна консоль + один агент

LEMSS

Lumension Endpoint Management & Security Suite

Lumension
IT Secured. Success Optimized.


Lumension® EMSS - Home - Windows Internet Explorer
http://lemss/default.aspx
Lumension® EMSS - Home
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Refresh dashboard widgets to see the latest results.
Refresh all
Print...
Configure dashboard settings...
Server Information
Company : Lumension Security (USA)
Serial number : 58CA2B48-D21D02E8
License replication : 100%
System replication : 100%
Patch / Content replication : 100%
Package replication : 0 remaining
Auto-download new critical packages : Off
Product Licenses:
Product Module | In Use | Pending | Available
AntiVirus | 1 | 0 | 9
App Control | 1 | 0 | 9
Dvc Control | 1 | 0 | 9
Patch | 1 | 0 | 9
Power Mgmt | 1 | 0 | 9
Time Since Last DAU Scan
100 %
< 24 hours: 0
> 72 hours: 1
24 - 47 hours: 0
Never checked in: 0
48 - 72 hours: 0
Active agents: 1
Agent Module Installation Status
Power Mgmt
Patch
Dvc Control
App Control
AntiVirus
Installed
Pending
Not Installed
Endpoints:1
Latest News
Microsoft Security Bulletin MS13-045 - Important *
5/14/2013 8:00 PM
from Latest News
Microsoft Security Bulletin MS13-046 - Important
5/14/2013 8:00 PM
from Latest News
Microsoft Security Bulletin MS13-044 - Important
5/14/2013 8:00 PM
Endpoints with Unresolved Updates
Endpoints
Devices Connected to Endpoints
All
Biometric De...
Citrix Netwo...
COM/Serial P...
CD/DVD Discs
DVD/CD Drive...
Floppy Disk ...
Imaging Devi...
LPT/Parallel...
Modem / Seco...
Palm Handhel...
Portable Dev...
Printers (US...
PS/2 Ports
Removable St...
RIM Blackber...
Smart Card R...
Un-remediated Critical Vulnerabilities
Vulnerabilities
<30 days
30 - 120 days
>120 days
Critical vulnerabilities: 10
Endpoints: 1
Lumension
Server Name: LEMSS
Date & Time 5/29/2013 9:04:04 AM
Start
Lumension® EMSS ...
9:10 AM
5/29/2013

Lumension® EMSS - Endpoints - Windows Internet Explorer

http://lemss/forms/computers/ComputerDetails1.aspx?AgentID=2250914d-4(

Lumension® EMSS - Endpoints

Lumension® Endpoint Management and Security Suite

Vulnerability Management | Endpoint Protection | Data Protection | Compliance & Reporting

Home | Discover | Review | Manage | Reports | Tools | Help

Administrator | Log Out

Manage > Endpoints > Information for LEMSS

Information | Vulnerabilities | Security Configuration | Inventory | Deployments and Tasks | Virus and Malware | AntiVirus Policies | Easy Lockdown/Auditor Files | Application Control Policies | Device Control Policies

Deploy... | Enable | Disable | Agent Versions... | Manage Modules... | Scan Now | Reboot Now... | Manage Remotely | Wake Now... | Export

Endpoint Name: LEMSS
DNS: LEMSS
IP: 10.0.2.15
MAC Address: 08:00:27:B6:E2:1B
Description: LEMSS

Operating System: Win2K8R2x64
OS Version: 6.1
OS Service Pack: Service Pack 1
OS Build Number: 7601

Agent Information

Agent version: 7.3.0.10
Agent installation date (Server): 5/9/2013 9:25:36 AM
Uninstall password: View...

Status Information

Agent status: Online
Last connected date (Server): 5/29/2013 9:03:55 AM
LPR status: Idle
Last DAU scan status: Success
Last DAU scan time (Server): 5/29/2013 9:05:00 AM
Last LPM reporting time (Server): Not Available

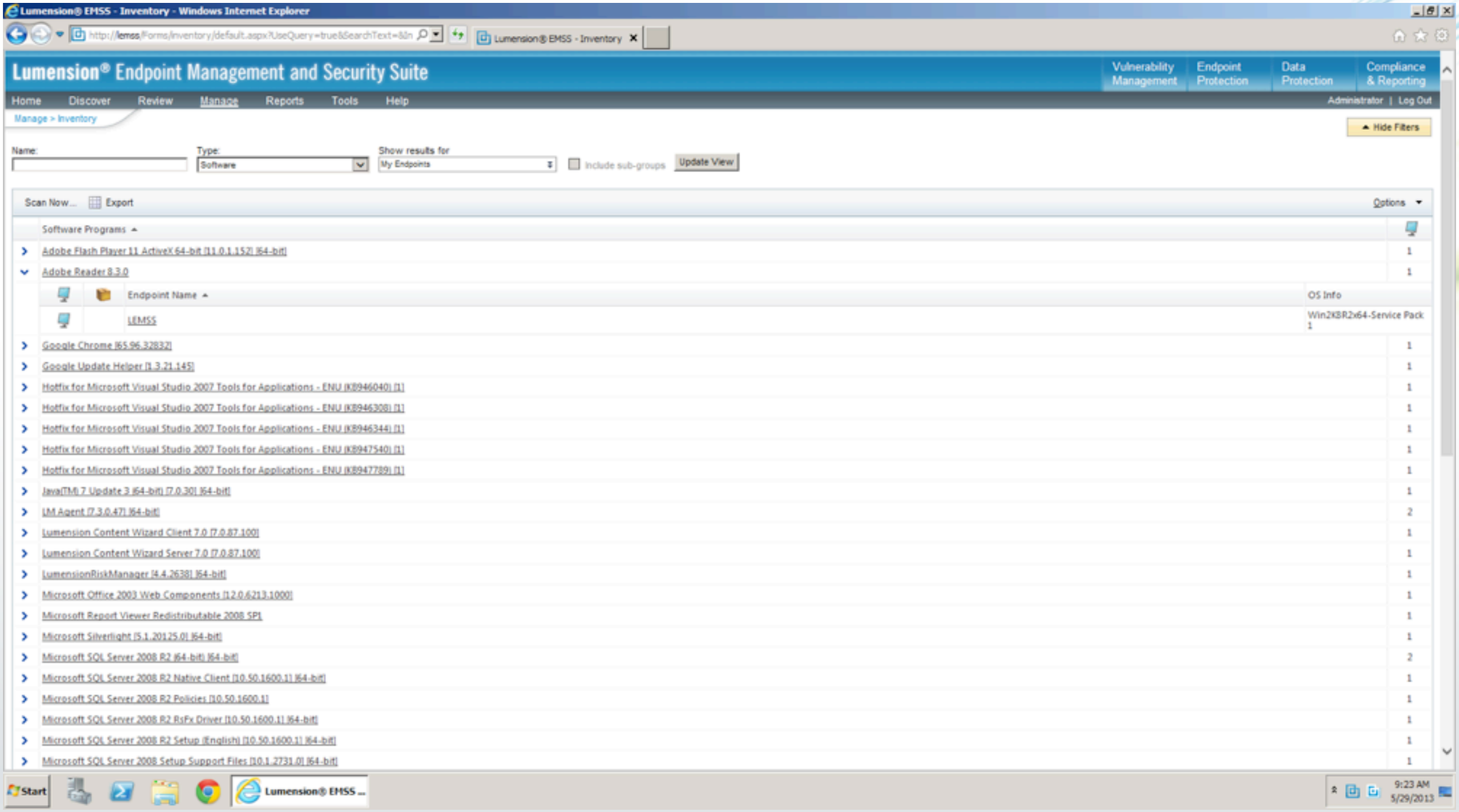
Component Information

Component	Available with this Agent Version	Installed	Installation Date/Time (Server)	Running Version	Policy Version
AntiVirus	Yes	Yes	5/14/2013 12:56:20 AM	7.3.0.56	7.3.0.56
App Control	Yes	Yes	5/14/2013 1:09:56 AM	7.3.0.70	7.3.0.70
Core	Yes	Yes	5/7/2013 5:03:40 PM	7.3.0.47	7.3.0.47
Dvc Control	Yes	Yes	5/14/2013 8:50:45 AM	7.3.0.74	7.3.0.74
Patch	Yes	Yes	5/9/2013 9:24:23 AM	7.3.0.20	7.3.0.20
Power Mgmt	Yes	Yes	5/8/2013 12:35:57 AM	7.3.0.310	7.3.0.310
WOL Wakepoint	Yes	No			7.3.0.304

Group Information

Group Name	Originating Group	Type	Deployments Applicable	Added By	Date Added (Server)
10.0.2.x	10.0.2.x	System Group	Yes	System	5/14/2013 8:23:36 AM
CEE	CEE	Custom Group	Yes	Administrator	5/8/2013 11:10:58 PM
Sales & Marketing	Sales & Marketing	Custom Group	Yes	Administrator	5/8/2013 11:10:42 PM
Win2K8R2x64	Win2K8R2x64	System Group	Yes	System	5/7/2013 5:03:44 PM
10.0.x.x	10.0.2.x	System Group	Yes	System	5/14/2013 8:23:36 AM
10.x.x.x	10.0.2.x	System Group	Yes	System	5/14/2013 8:23:36 AM
By Function	Sales & Marketing	Custom Group	Yes	Administrator	5/8/2013 11:10:42 PM

Start | Lumension® EMSS ... | 9:15 AM 5/29/2013


Lumension® EMSS - Inventory - Windows Internet Explorer
http://lemss/Forms/Inventory/default.aspx?UseQuery=true&SearchText=&In
Lumension® EMSS - Inventory
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Manage > Inventory
Hide Filters
Name:
Type:
Software
Show results for
My Endpoints
Include sub-groups
Update View
Scan Now...
Export
Options
Software Programs
Adobe Flash Player 11 ActiveX 64-bit [11.0.1.152] [64-bit] 1
Adobe Reader 8.3.0 1
Endpoint Name
OS Info
LEMSS
Win2K8R2x64-Service Pack 1
Google Chrome [65.96.32832] 1
Google Update Helper [1.3.21.145] 1
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946040) [1] 1
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946308) [1] 1
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB946344) [1] 1
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB947540) [1] 1
Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB947789) [1] 1
Java(TM) 7 Update 3 (64-bit) [7.0.30] [64-bit] 1
LM Agent [7.3.0.47] [64-bit] 2
Lumension Content Wizard Client 7.0 [7.0.87.100] 1
Lumension Content Wizard Server 7.0 [7.0.87.100] 1
LumensionRiskManager [4.4.2638] [64-bit] 1
Microsoft Office 2003 Web Components [12.0.6213.1000] 1
Microsoft Report Viewer Redistributable 2008 SP1 1
Microsoft Silverlight [5.1.20125.0] [64-bit] 1
Microsoft SQL Server 2008 R2 (64-bit) [64-bit] 2
Microsoft SQL Server 2008 R2 Native Client [10.50.1600.1] [64-bit] 1
Microsoft SQL Server 2008 R2 Policies [10.50.1600.1] 1
Microsoft SQL Server 2008 R2 RsPx Driver [10.50.1600.1] [64-bit] 1
Microsoft SQL Server 2008 R2 Setup (English) [10.50.1600.1] [64-bit] 1
Microsoft SQL Server 2008 Setup Support Files [10.1.2731.0] [64-bit] 1
Start
Lumension® EMSS ...
9:23 AM
5/29/2013

Lumension® EMSS - Critical Vulnerabilities - Windows Internet Explorer

http://lemss/forms/vulnerability/default.aspx?ContentType=CBNS&Detection

Lumension® EMSS - Critical ...

Lumension® Endpoint Management and Security Suite

Vulnerability Management | Endpoint Protection | Data Protection | Compliance & Reporting

Home | Discover | Review | Manage | Reports | Tools | Help

Administrator | Log Out

Review > Vulnerabilities > Critical Vulnerabilities

Hide Filters

Name or CVE-ID: | Content type: Critical and Not Superseded | Applicability: Applicable | State: Enabled | Detection status: Not Patched | Show results for: My Endpoints | Update View

Include sub-groups

Patch and Remediation

Disable | Update Cache | Deploy... | Scan Now... | Export | Options

Name	Content type	✓	✗	⊘	⏱	🖳	%
Adobe APSB13-14 Flash Player 11.7.700.202 (Internet Explorer) for Windows (Update) (All Languages)	Critical	0	1	0	0	1	100
Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 (KB2820197)	Critical	0	1	0	0	1	100
MS13-037 Cumulative Security Update for Internet Explorer 10 for Windows Server 2008 R2 Service Pack 1 x64 (KB2829530)	Critical	0	1	0	0	1	100
MS13-040 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 x64 (KB2804579)	Critical	0	1	0	0	1	100

Type: Active Vulnerability Analysis
Content type: Critical
Status: Enabled
Downloaded On: 5/20/2013 10:05:10 AM (UTC)
Vulnerability Results: Current

Associated Packages: 1
Packages Status: Not Cached
Vendor: Microsoft Corp
Released On: 5/14/2013 5:00:00 PM (UTC)
Vendor Product ID: MS13-040

Common Vulnerability Exploit (CVE): CVE-2013-1336
Vulnerability Code Description: The Common Language Runtime (CLR) in Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4, and 4.5 does not properly check signatures, which allows remote attackers to make undetected changes to signed XML documents via unspecified vectors that preserve signature validity, aka "XML Digital Signature Spoofing Vulnerability."
Reference Text: MS:MS13-040

Common Vulnerability Exploit (CVE): CVE-2013-1337
Vulnerability Code Description: Microsoft .NET Framework 4.5 does not properly create policy requirements for custom Windows Communication Foundation (WCF) endpoint authentication in certain situations involving passwords over HTTPS, which allows remote attackers to bypass authentication by sending queries to an endpoint, aka "Authentication Bypass Vulnerability."
Reference Text: MS:MS13-040

Description: LSAC(v2)/LSAC(v3)
A security issue has been identified that could allow an attacker to misrepresent a system action or behavior without the knowledge of the user. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.
More Information

MS13-046 Security Update for Windows Server 2008 R2 x64 (KB2829361)	Critical	0	1	0	0	1	100
MS13-046 Security Update for Windows Server 2008 R2 x64 (KB2830290)	Critical	0	1	0	0	1	100
Adobe APSB11-24 Reader 8.3.1 for Windows (Update) (English)	Critical - 01	0	1	0	0	1	100
Microsoft SQL Server 2008 R2 Service Pack 1 (KB2528583)	Critical - 01	0	1	0	0	1	100
MS 2630458 Microsoft SQL Server 2008 R2/2008 R2 Express Service Pack 2 (64Bit) (See Notes)	Critical - 01	0	1	0	0	1	100

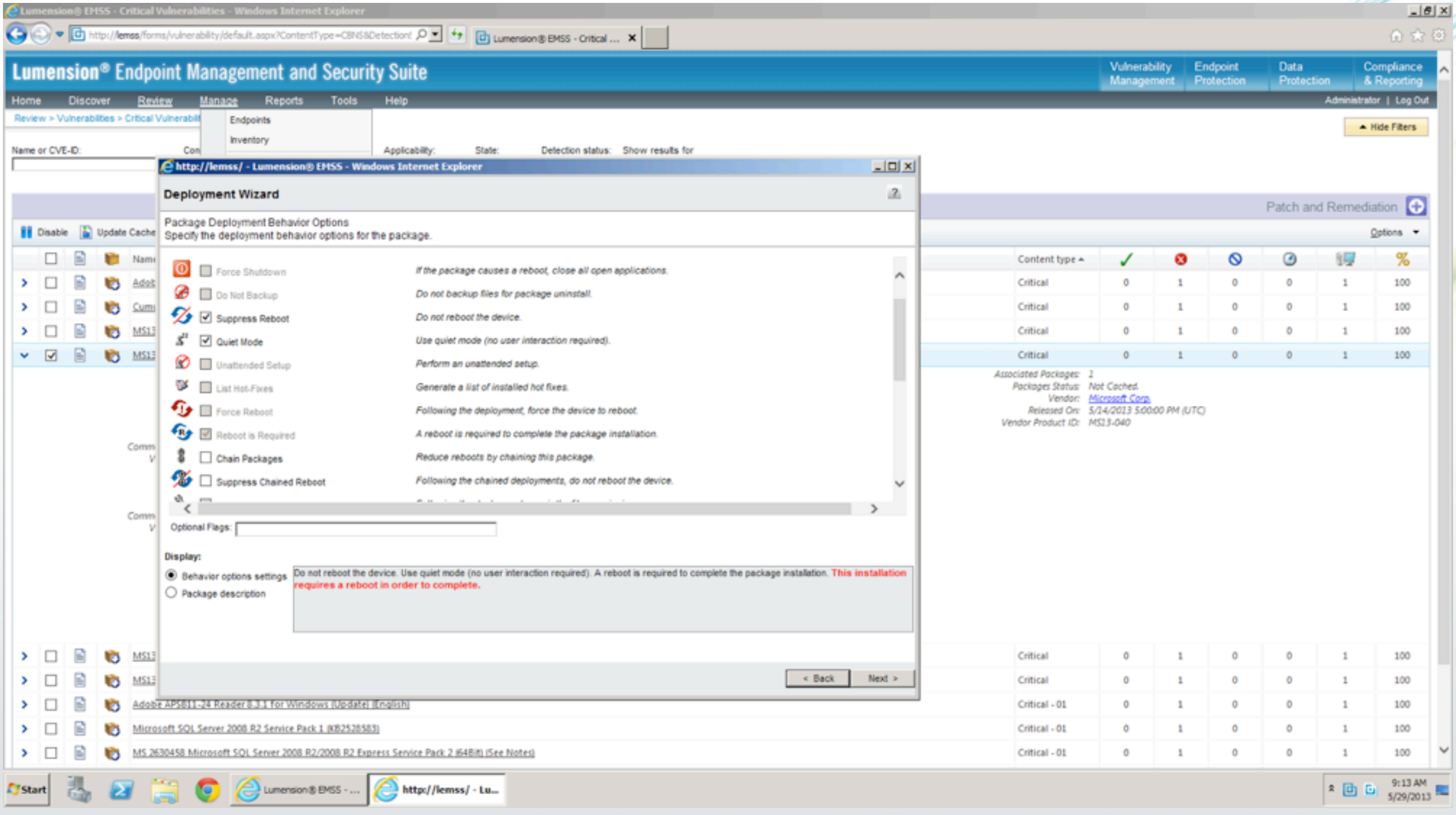
http://lemss/default.aspx

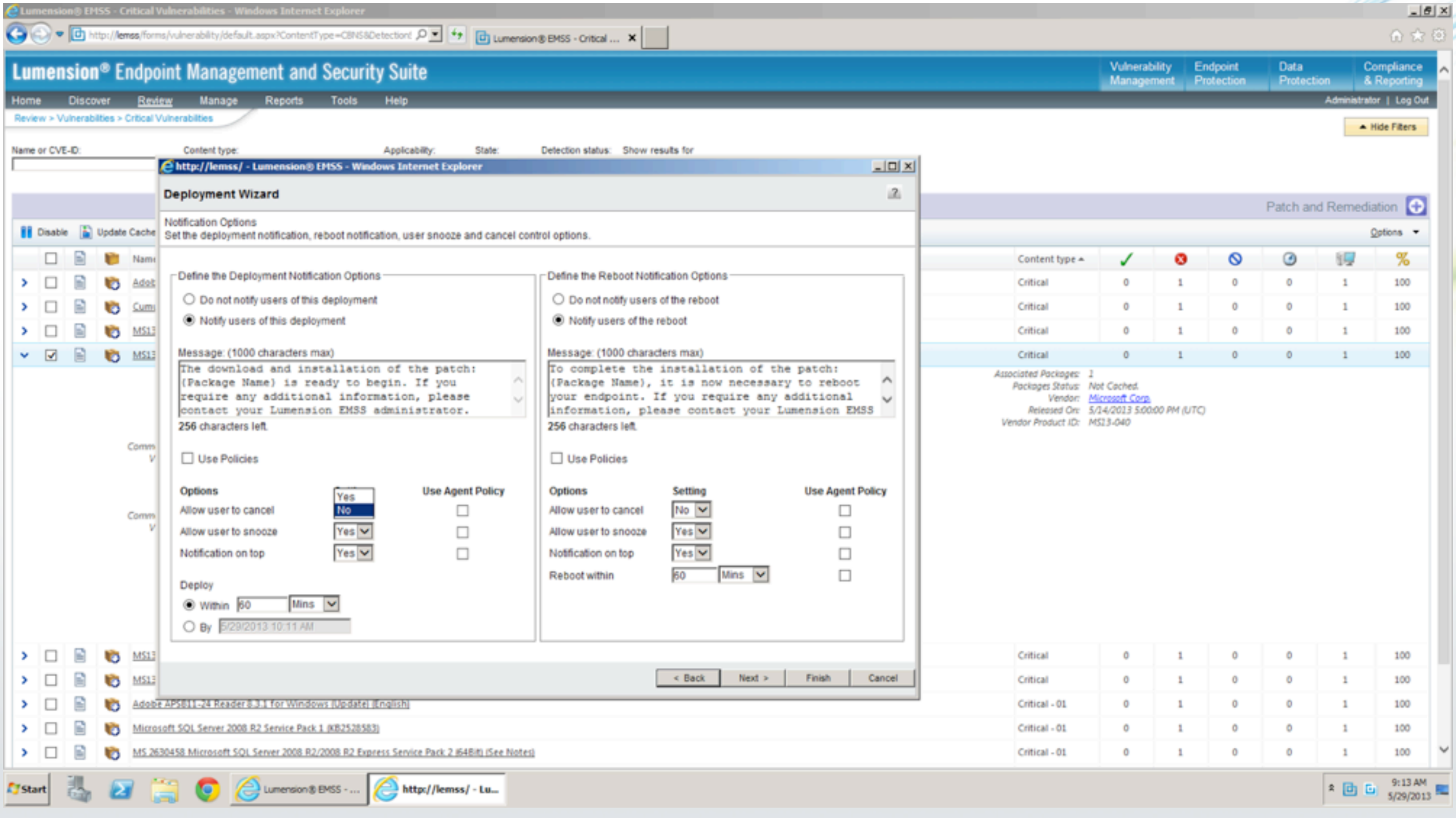
Start | Lumension® EMSS ... | 9:11 AM 5/29/2013

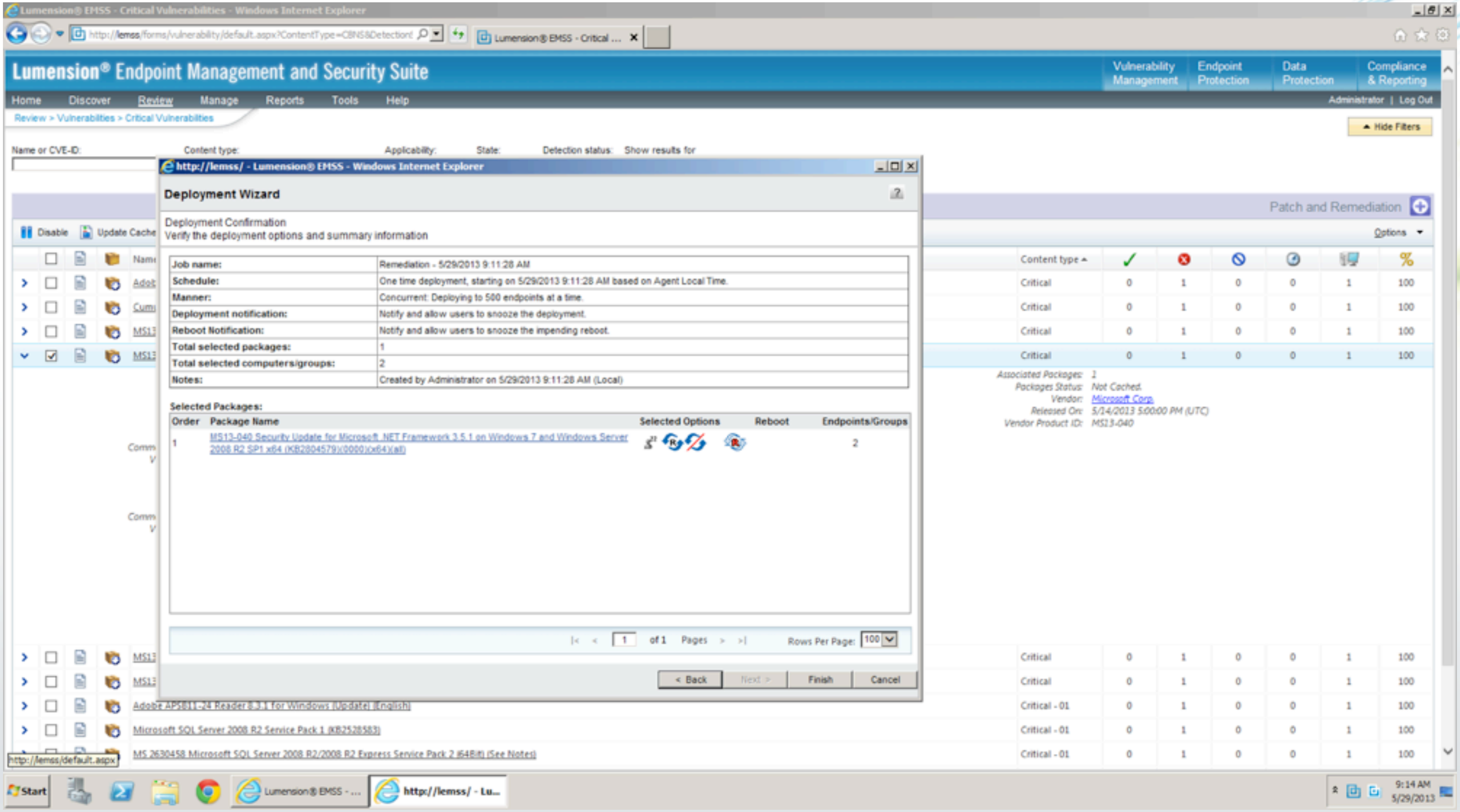
www.lumension.com

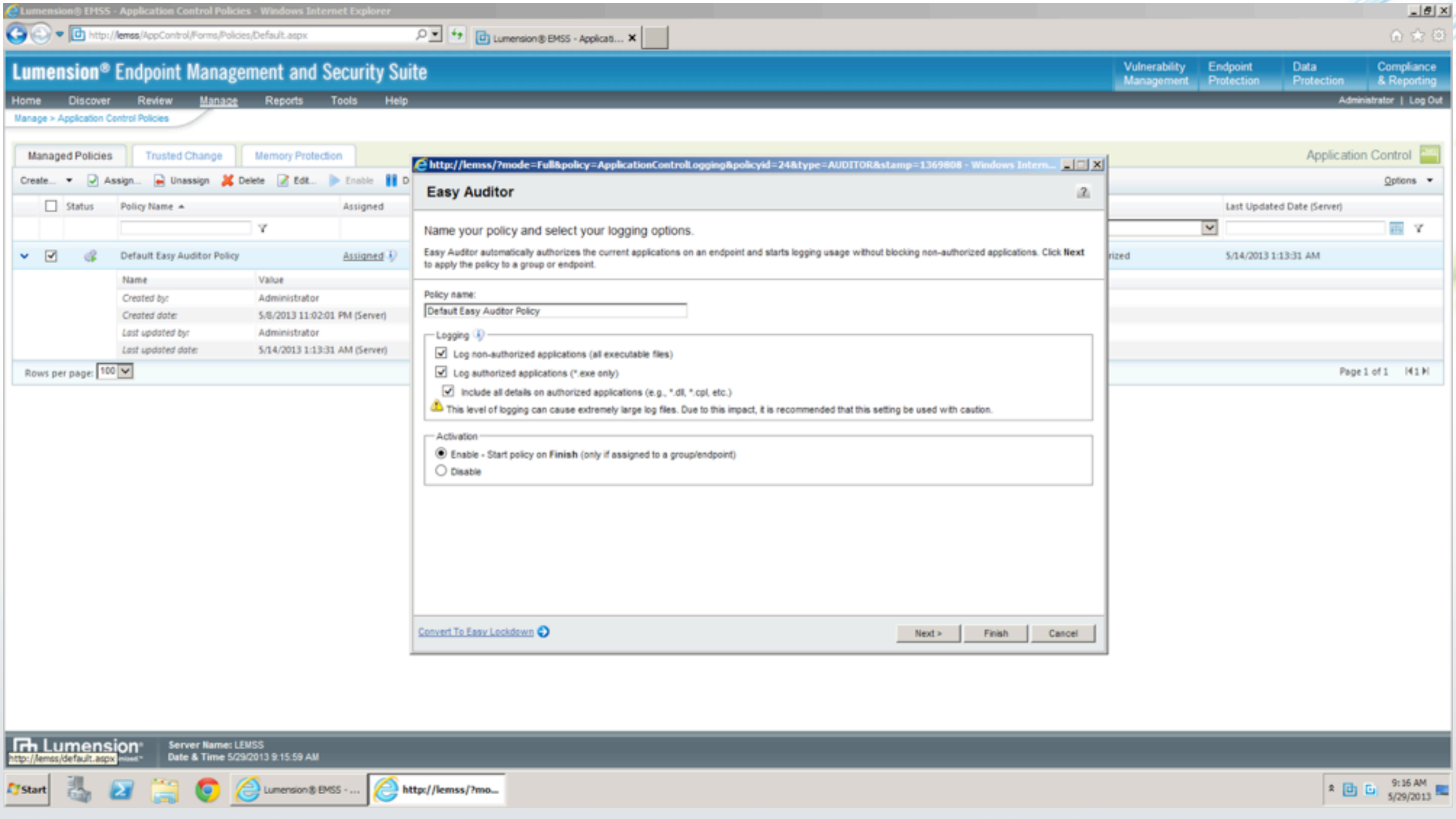
Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance

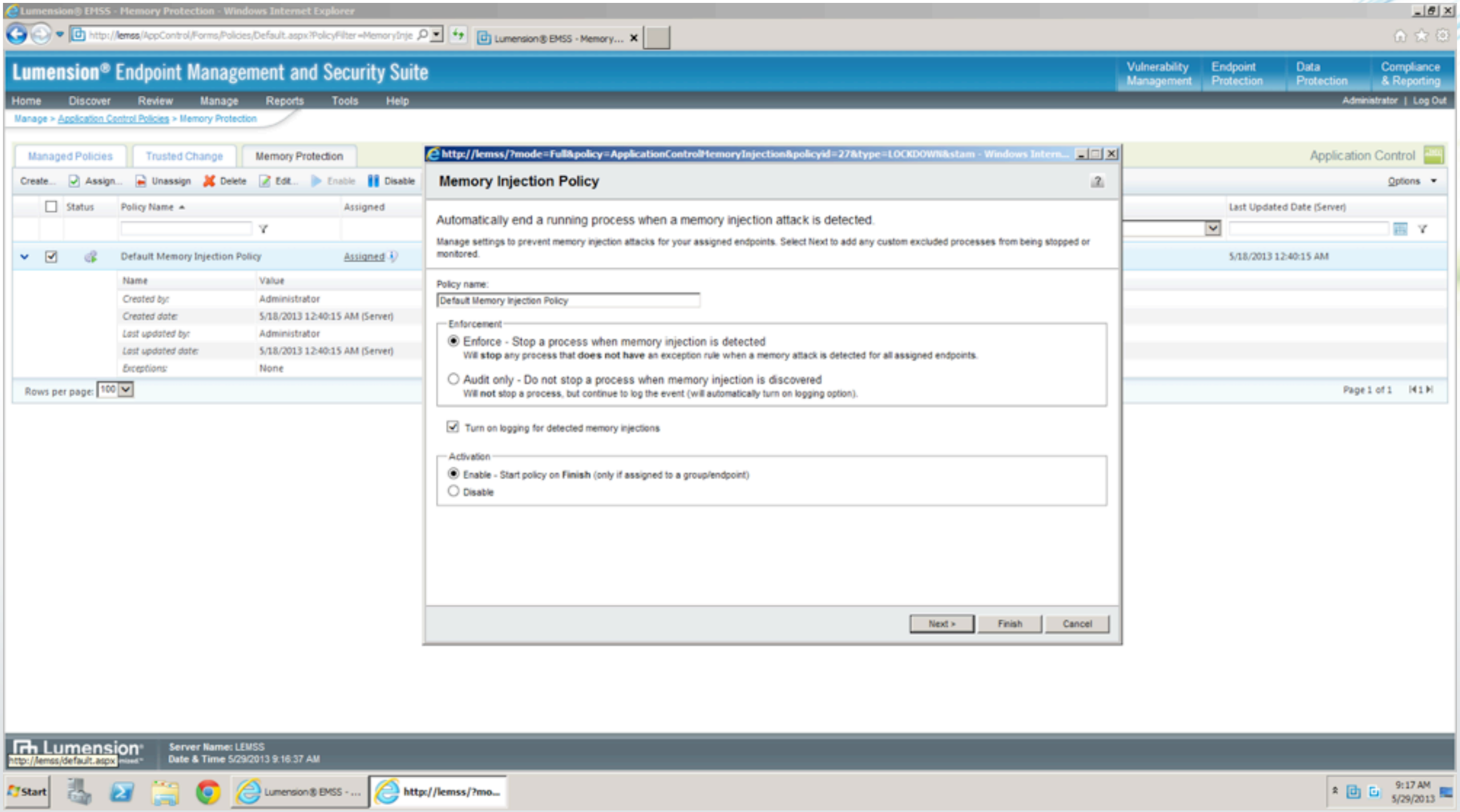
Lumension™
IT Secured. Success Optimized.

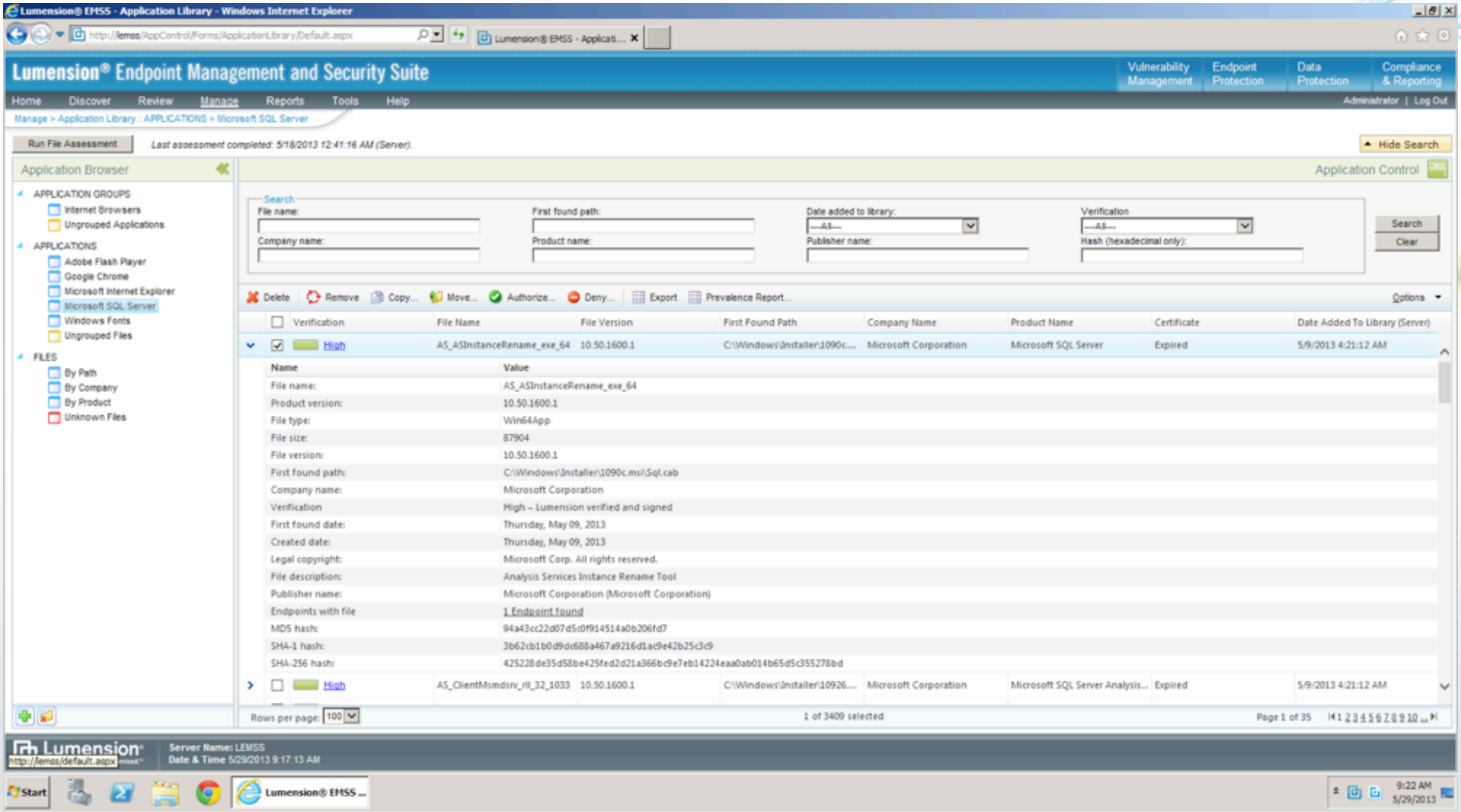

Lumension® EMSS - Critical Vulnerabilities - Windows Internet Explorer
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Endpoints
Inventory
Hide Filters
Name or CVE-ID:
Applicability:
State:
Detection status:
Show results for
http://lemss/ - Lumension® EMSS - Windows Internet Explorer
Deployment Wizard
Package Deployment Behavior Options
Specify the deployment behavior options for the package.
Force Shutdown
If the package causes a reboot, close all open applications.
Do Not Backup
Do not backup files for package uninstall.
Suppress Reboot
Do not reboot the device.
Quiet Mode
Use quiet mode (no user interaction required).
Unattended Setup
Perform an unattended setup.
List Hot-Fixes
Generate a list of installed hot fixes.
Force Reboot
Following the deployment, force the device to reboot.
Reboot is Required
A reboot is required to complete the package installation.
Chain Packages
Reduce reboots by chaining this package.
Suppress Chained Reboot
Following the chained deployments, do not reboot the device.
Optional Flags:
Display:
Behavior options settings
Package description
Do not reboot the device. Use quiet mode (no user interaction required). A reboot is required to complete the package installation. This installation requires a reboot in order to complete.
< Back
Next >
Patch and Remediation
Disable
Update Cache
Options
Content type
Critical
Associated Packages: 1
Packages Status: Not Cached
Vendor: Microsoft Corp
Released On: 5/14/2013 5:00:00 PM (UTC)
Vendor Product ID: MS13-040
Adobe APSB11-24 Reader 8.3.1 for Windows (Update) (English)
Microsoft SQL Server 2008 R2 Service Pack 1 (KB2528583)
MS 2630458 Microsoft SQL Server 2008 R2/2008 R2 Express Service Pack 2 (64Bit) (See Notes)
Critical - 01
Start
Lumension® EMSS - ...
http://lemss/ - Lu...
9:13 AM
5/29/2013


Lumension® EMSS - Critical Vulnerabilities - Windows Internet Explorer
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Review > Vulnerabilities > Critical Vulnerabilities
Hide Filters
Name or CVE-ID:
Content type:
Applicability:
State:
Detection status:
Show results for
http://lemss/ - Lumension® EMSS - Windows Internet Explorer
Deployment Wizard
Notification Options
Set the deployment notification, reboot notification, user snooze and cancel control options.
Define the Deployment Notification Options
Do not notify users of this deployment
Notify users of this deployment
Message: (1000 characters max)
The download and installation of the patch: (Package Name) is ready to begin. If you require any additional information, please contact your Lumension EMSS administrator.
256 characters left.
Use Policies
Options
Use Agent Policy
Allow user to cancel
Allow user to snooze
Notification on top
Deploy
Within
Mins
By
5/29/2013 10:11 AM
Define the Reboot Notification Options
Do not notify users of the reboot
Notify users of the reboot
Message: (1000 characters max)
To complete the installation of the patch: (Package Name), it is now necessary to reboot your endpoint. If you require any additional information, please contact your Lumension EMSS
256 characters left.
Use Policies
Options
Setting
Use Agent Policy
Allow user to cancel
Allow user to snooze
Notification on top
Reboot within
Mins
< Back
Next >
Finish
Cancel
Patch and Remediation
Disable
Update Cache
Options
Content type
Critical
Associated Packages: 1
Packages Status: Not Cached
Vendor: Microsoft Corp
Released On: 5/14/2013 5:00:00 PM (UTC)
Vendor Product ID: MS13-040
Adobe APSB11-24 Reader 8.3.1 for Windows (Update) (English)
Microsoft SQL Server 2008 R2 Service Pack 1 (KB2528583)
MS 2630458 Microsoft SQL Server 2008 R2/2008 R2 Express Service Pack 2 (64Bit) (See Notes)
Start
Lumension® EMSS - ...
http://lemss/ - Lu...
9:13 AM
5/29/2013


Lumension® EMSS - Critical Vulnerabilities - Windows Internet Explorer
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Review > Vulnerabilities > Critical Vulnerabilities
Hide Filters
Name or CVE-ID:
Content type:
Applicability:
State:
Detection status:
Show results for
http://lemss/ - Lumension® EMSS - Windows Internet Explorer
Deployment Wizard
Deployment Confirmation
Verify the deployment options and summary information
Job name: Remediation - 5/29/2013 9:11:28 AM
Schedule: One time deployment, starting on 5/29/2013 9:11:28 AM based on Agent Local Time.
Manner: Concurrent: Deploying to 500 endpoints at a time.
Deployment notification: Notify and allow users to snooze the deployment.
Reboot Notification: Notify and allow users to snooze the impending reboot.
Total selected packages: 1
Total selected computers/groups: 2
Notes: Created by Administrator on 5/29/2013 9:11:28 AM (Local)
Selected Packages:
Order
Package Name
Selected Options
Reboot
Endpoints/Groups
1
MS13-040 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 x64 (KB2804579)(3000)(x64)(all)
2
of 1 Pages
Rows Per Page: 100
< Back
Next >
Finish
Cancel
Patch and Remediation
Disable
Update Cache
Options
Content type
Critical
Associated Packages: 1
Packages Status: Not Cached
Vendor: Microsoft Corp
Vendor Product ID: MS13-040
Adobe AR5811-24 Reader 8.3.1 for Windows (Update) (English)
Microsoft SQL Server 2008 R2 Service Pack 1 (KB2528583)
MS 2630458 Microsoft SQL Server 2008 R2/2008 R2 Express Service Pack 2 (64Bit) (See Notes)
http://lemss/default.aspx
Start
Lumension® EMSS - ...
http://lemss/ - Lu...
9:14 AM
5/29/2013


Lumension® EMSS - Application Control Policies - Windows Internet Explorer
http://lemss/AppControl/Forms/Policies/Default.aspx
Lumension® EMSS - Applicati...
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Manage > Application Control Policies
Managed Policies
Trusted Change
Memory Protection
Application Control
Create...
Assign...
Unassign
Delete
Edit...
Enable
Options
Status
Policy Name
Assigned
Last Updated Date (Server)
Default Easy Auditor Policy
Assigned
5/14/2013 1:13:31 AM
Name
Value
Created by:
Administrator
Created date:
5/8/2013 11:02:01 PM (Server)
Last updated by:
Administrator
Last updated date:
5/14/2013 1:13:31 AM (Server)
Rows per page:
100
Page 1 of 1
http://lemss/?mode=Full&policy=ApplicationControlLogging&policyid=24&type=AUDITOR&stamp=1369808 - Windows Intern...
Easy Auditor
Name your policy and select your logging options.
Easy Auditor automatically authorizes the current applications on an endpoint and starts logging usage without blocking non-authorized applications. Click Next to apply the policy to a group or endpoint.
Policy name:
Default Easy Auditor Policy
Logging
Log non-authorized applications (all executable files)
Log authorized applications (*.exe only)
Include all details on authorized applications (e.g., *.dll, *.cpl, etc.)
This level of logging can cause extremely large log files. Due to this impact, it is recommended that this setting be used with caution.
Activation
Enable - Start policy on Finish (only if assigned to a group/endpoint)
Disable
Convert To Easy Lockdown
Next >
Finish
Cancel
Lumension
http://lemss/default.aspx
Server Name: LEMSS
Date & Time 5/29/2013 9:15:59 AM
Start
Lumension® EMSS - ...
http://lemss/?mo...
9:16 AM
5/29/2013


Lumension® EMSS - Memory Protection - Windows Internet Explorer
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Manage > Application Control Policies > Memory Protection
Managed Policies
Trusted Change
Memory Protection
Create...
Assign...
Unassign
Delete
Edit...
Enable
Disable
Status
Policy Name
Assigned
Default Memory Injection Policy
Assigned
Name
Value
Created by:
Administrator
Created date:
5/18/2013 12:40:15 AM (Server)
Last updated by:
Administrator
Last updated date:
5/18/2013 12:40:15 AM (Server)
Exceptions:
None
Rows per page: 100
http://lemss/?mode=Full&policy=ApplicationControlMemoryInjection&policyid=27&type=LOCKDOWN&stam - Windows Intern...
Memory Injection Policy
Automatically end a running process when a memory injection attack is detected.
Manage settings to prevent memory injection attacks for your assigned endpoints. Select Next to add any custom excluded processes from being stopped or monitored.
Policy name:
Default Memory Injection Policy
Enforcement
Enforce - Stop a process when memory injection is detected
Will stop any process that does not have an exception rule when a memory attack is detected for all assigned endpoints.
Audit only - Do not stop a process when memory injection is discovered
Will not stop a process, but continue to log the event (will automatically turn on logging option).
Turn on logging for detected memory injections
Activation
Enable - Start policy on Finish (only if assigned to a group/endpoint)
Disable
Next >
Finish
Cancel
Application Control
Options
Last Updated Date (Server)
5/18/2013 12:40:15 AM
Page 1 of 1
Lumension
http://lemss/default.aspx
Server Name: LEMSS
Date & Time 5/29/2013 9:16:37 AM
Start
Lumension® EMSS - ...
http://lemss/?mo...
9:17 AM
5/29/2013


Lumension® EMSS - Application Library - Windows Internet Explorer
http://lemss/AppControl/Forms/ApplicationLibrary/Default.aspx
Lumension® EMSS - Applicati...
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Manage > Application Library : APPLICATIONS > Microsoft SQL Server
Run File Assessment
Last assessment completed: 5/18/2013 12:41:16 AM (Server).
Hide Search
Application Browser
APPLICATION GROUPS
Internet Browsers
Ungrouped Applications
APPLICATIONS
Adobe Flash Player
Google Chrome
Microsoft Internet Explorer
Microsoft SQL Server
Windows Fonts
Ungrouped Files
FILES
By Path
By Company
By Product
Unknown Files
Application Control
Search
File name:
First found path:
Date added to library:
---All---
Verification
---All---
Company name:
Product name:
Publisher name:
Hash (hexadecimal only):
Search
Clear
Delete
Remove
Copy...
Move...
Authorize...
Deny...
Export
Prevalence Report...
Options
Verification
File Name
File Version
First Found Path
Company Name
Product Name
Certificate
Date Added To Library (Server)
High
AS_ASInstanceRename_exe_64
10.50.1600.1
C:\Windows\Installer\1090c....
Microsoft Corporation
Microsoft SQL Server
Expired
5/9/2013 4:21:12 AM
Name
Value
File name: AS_ASInstanceRename_exe_64
Product version: 10.50.1600.1
File type: Win64App
File size: 87904
File version: 10.50.1600.1
First found path: C:\Windows\Installer\1090c.msi\Sql.cab
Company name: Microsoft Corporation
Verification: High – Lumension verified and signed
First found date: Thursday, May 09, 2013
Created date: Thursday, May 09, 2013
Legal copyright: Microsoft Corp. All rights reserved.
File description: Analysis Services Instance Rename Tool
Publisher name: Microsoft Corporation (Microsoft Corporation)
Endpoints with file: 1 Endpoint found
MD5 hash: 94a43cc22d07d5c0f914514a0b206fd7
SHA-1 hash: 3b62cb1b0d9dc688a467a9216d1ac9e42b25c3c9
SHA-256 hash: 425228de35d58be425fed2d21a366bc9e7eb14224eaa0ab014b65d5c355278bd
High
AS_ClientMsmdsrv_rll_32_1033
10.50.1600.1
C:\Windows\Installer\10926....
Microsoft Corporation
Microsoft SQL Server Analysis...
Expired
5/9/2013 4:21:12 AM
Rows per page: 100
1 of 3409 selected
Page 1 of 35
1 2 3 4 5 6 7 8 9 10 ...
Lumension
Server Name: LEMSS
Date & Time 5/29/2013 9:17:13 AM
http://lemss/default.aspx
Start
Lumension® EMSS ...
9:22 AM
5/29/2013

Lumension® EMSS - Device Control Policies - Windows Internet Explorer

http://lemss/DevCtrl/Forms/Policies/Policies.aspx

Lumension® EMSS - Device ...

Lumension® Endpoint Management and Security Suite

Vulnerability Management | Endpoint Protection | Data Protection | Compliance & Reporting

Home | Discover | Review | Manage | Reports | Tools | Help

Administrator | Log Out

Manage > Device Control Policies

Hide Filters

Policy Type: ---All---

Device Collection:

Update View

Device Control

Create... | Assign... | Unassign | Delete | Edit... | Enable | Disable | Export | Options

	Status	Policy Name	Assigned	Policy Type	Device Class	Device Collection	Last Update (Server)
		Device Control Global Policy	Assigned	Global Device Policy	All	Any	5/7/2013 5:01:59 PM
		Default Policy for Biometric Devices	Assigned	Device Class Policy	Biometric Devices	Any	5/7/2013 5:02:00 PM
		Default Policy for Citrix Network Shares	Assigned	Device Class Policy	Citrix Network Shares	Any	5/7/2013 5:02:00 PM
		Default Policy for COM/Serial Ports	Assigned	Device Class Policy	COM/Serial Ports	Any	5/7/2013 5:02:00 PM
		Default Policy for DVD/CD Drives	Assigned	Device Class Policy	DVD/CD Drives	Any	5/7/2013 5:01:59 PM
		Default Policy for Floppy Disk Drives	Assigned	Device Class Policy	Floppy Disk Drives	Any	5/7/2013 5:01:59 PM
		Default Policy for Imaging Devices	Assigned	Device Class Policy	Imaging Devices	Any	5/7/2013 5:02:00 PM
		Default Policy for LPT/Parallel Ports	Assigned	Device Class Policy	LPT/Parallel Ports	Any	5/7/2013 5:02:00 PM
	☑	Default Policy for Network Access Devices	Assigned	Device Class Policy	Modem / Secondary Network Access Device	Any	5/7/2013 5:02:00 PM
		Default Policy for Palm Handheld Devices	Assigned	Device Class Policy	Palm Handheld Devices	Any	5/7/2013 5:02:00 PM
		Default Policy for Portable Devices	Assigned	Device Class Policy	Portable Devices	Any	5/7/2013 5:02:00 PM
		Default Policy for Printers (USB)	Assigned	Device Class Policy	Printers (USB)	Any	5/7/2013 5:02:00 PM
		Default Policy for PS/2 Ports	Assigned	Device Class Policy	PS/2 Ports	Any	5/7/2013 5:02:00 PM
		Default Policy for Removable Storage Devices	Assigned	Device Class Policy	Removable Storage Devices	Any	5/7/2013 5:02:00 PM
		Default Policy for RIM BlackBerry Handhelds	Assigned	Device Class Policy	RIM Blackberry Handhelds	Any	5/7/2013 5:02:00 PM

Rows per page: 100

1 of 20 selected

Page 1 of 1

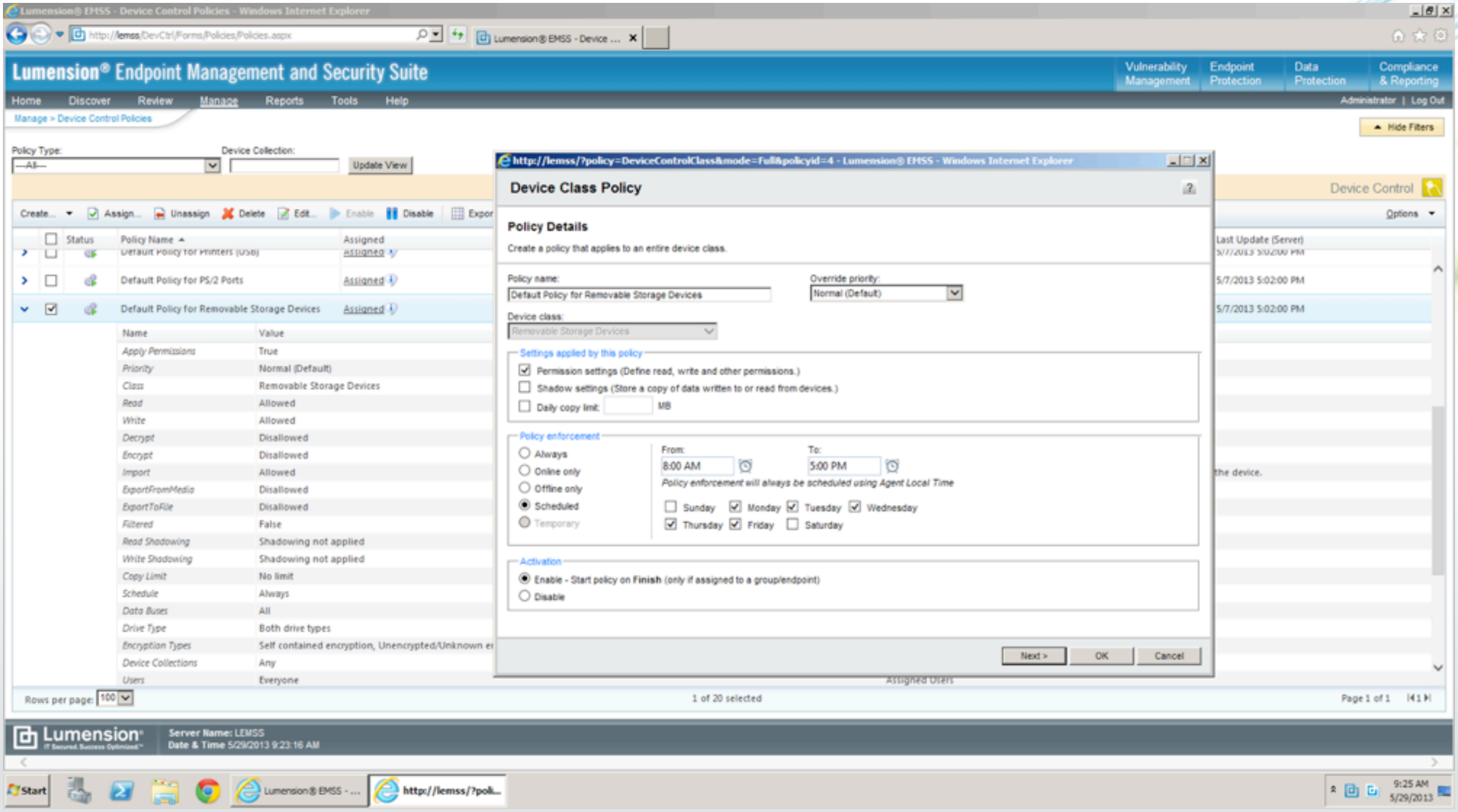
Lumension IT Secured. Success Optimized.

Server Name: LEMSS

Date & Time 5/29/2013 9:23:16 AM

Start | Lumension® EMSS ...

9:25 AM 5/29/2013


Lumension® EMSS - Device Control Policies - Windows Internet Explorer
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Manage > Device Control Policies
Hide Filters
Policy Type:
---All---
Device Collection:
Update View
Device Control
Create...
Assign...
Unassign
Delete
Edit...
Enable
Disable
Options
Status
Policy Name
Assigned
Last Update (Server)
Default Policy for Printers (USB)
Default Policy for PS/2 Ports
5/7/2013 5:02:00 PM
Default Policy for Removable Storage Devices
5/7/2013 5:02:00 PM
Name
Value
Apply Permissions
True
Priority
Normal (Default)
Class
Removable Storage Devices
Read
Allowed
Write
Allowed
Decrypt
Disallowed
Encrypt
Disallowed
Import
Allowed
ExportFromMedia
Disallowed
ExportToFile
Disallowed
Filtered
False
Read Shadowing
Shadowing not applied
Write Shadowing
Shadowing not applied
Copy Limit
No limit
Schedule
Always
Data Buses
All
Drive Type
Both drive types
Encryption Types
Self contained encryption, Unencrypted/Unknown e
Device Collections
Any
Users
Everyone
Assigned Users
Rows per page: 100
1 of 20 selected
Page 1 of 1
http://lemss/?policy=DeviceControlClass&mode=Full&policyid=4 - Lumension® EMSS - Windows Internet Explorer
Device Class Policy
Policy Details
Create a policy that applies to an entire device class.
Policy name:
Default Policy for Removable Storage Devices
Override priority:
Normal (Default)
Device class:
Removable Storage Devices
Settings applied by this policy
Permission settings (Define read, write and other permissions.)
Shadow settings (Store a copy of data written to or read from devices.)
Daily copy limit:
MB
Policy enforcement
Always
Online only
Offline only
Scheduled
Temporary
From:
8:00 AM
To:
5:00 PM
Policy enforcement will always be scheduled using Agent Local Time
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Activation
Enable - Start policy on Finish (only if assigned to a group/endpoint)
Disable
Next >
OK
Cancel
the device.
Lumension
Server Name: LEMSS
Date & Time 5/29/2013 9:23:16 AM
Start
Lumension® EMSS - ...
http://lemss/?poli...
9:25 AM
5/29/2013

Lumension® EMSS - AntiVirus Policies - Windows Internet Explorer

http://lemss/antivirus/forms/Policies/Policies.aspx

Lumension® EMSS - AntiViru...

Lumension® Endpoint Management and Security Suite

Vulnerability Management | Endpoint Protection | Data Protection | Compliance & Reporting

Home | Discover | Review | Manage | Reports | Tools | Help

Administrator | Log Out

Manage > AntiVirus Policies

AntiVirus

Create | Assign | Unassign | Delete | Edit... | Enable | Disable | Export | Options

	Status	Policy Name	Assigned	Policy Type	Created By	Created Date (Server)	Last Updated By	Last Updated Date (Server)
☐		Default Real-Time Monitoring Policy	Assigned	Real-time Monitoring	Administrator	5/8/2013 10:52:53 PM	Administrator	5/8/2013 10:52:53 PM

Name	Value	Description
Virus Detection Action	Attempt to clean then quarantine then delete	Indicates actions to take upon virus/malware detection
Local users	Scan on both read/execute and write	Indicates real-time scan options for local users
Services and remote users	Scan on both read/execute and write	Indicates real-time scan options for services and remote users
Exclude Path/Filename		Indicates if path(s)/filename(s) will be excluded from the scan
Optional drives	Yes	Indicates if optional drives will be included in the scan

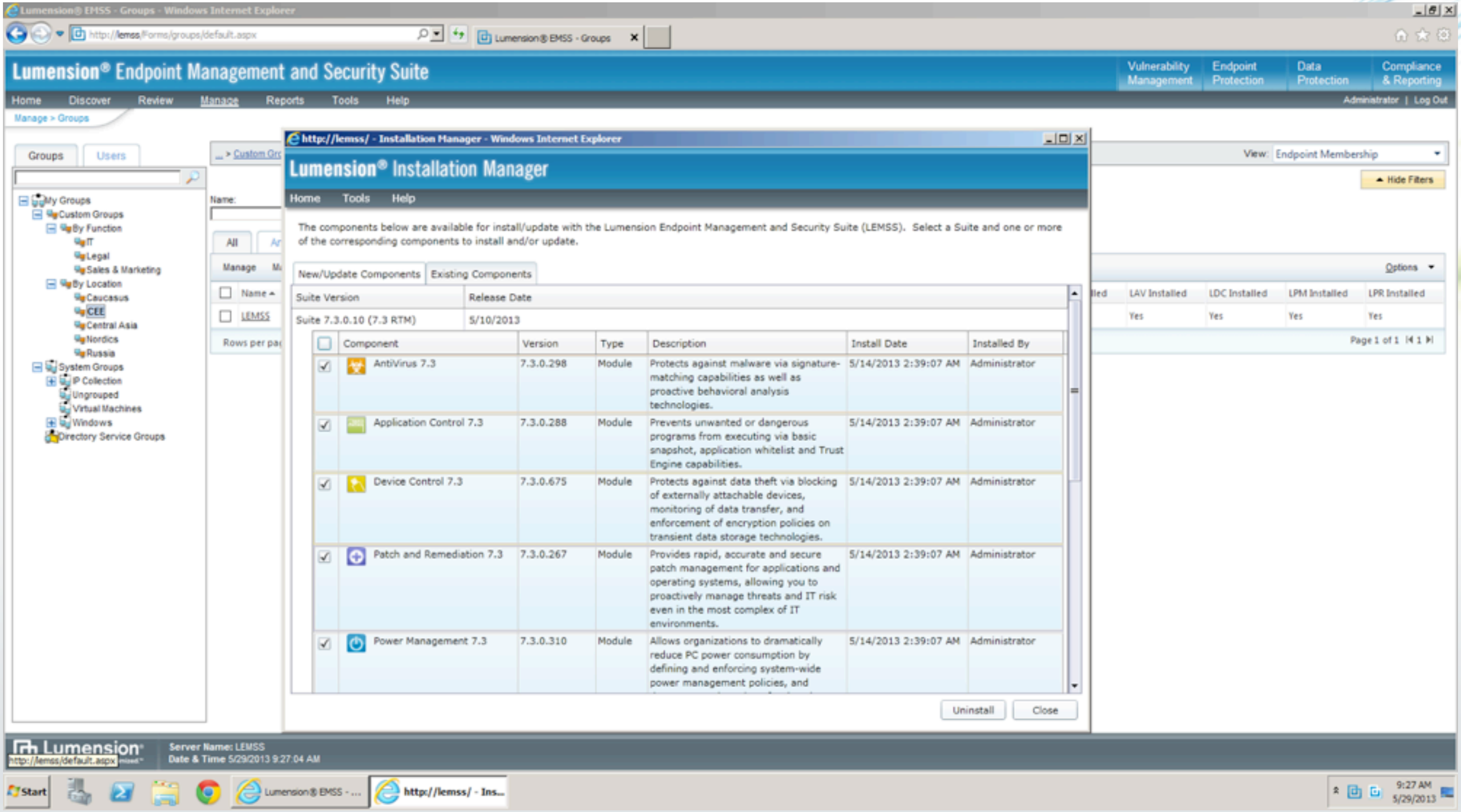
	Status	Policy Name	Assigned	Policy Type	Created By	Created Date (Server)	Last Updated By	Last Updated Date (Server)
☑		Default Recurring Virus and Malware Scan	Assigned	Recurring Scan	Administrator	5/8/2013 10:55:35 PM	Administrator	5/8/2013 10:55:35 PM

Name	Value	Description
Scheduling	Recurs every week - on Wednesdays - at 3:00 AM (agent local time).	Indicates the frequency of scanning
First Occurrence	5/8/2013 3:00:00 AM (Agent local)	Indicates the first occurence of the scan
Next Occurrence	6/5/2013 3:00:00 AM (Agent local)	Indicates when the next occurence of the scan is due
CPU Utilization	High	Indicates the level of CPU utilization selected - low, medium, high
Virus Detection Action	Attempt to clean then quarantine then delete	Indicates actions to take upon virus/malware detection
Scan Boot Sectors	Yes	Indicates whether boot sectors are included in the scan
Scan Archives	Yes	Indicates whether archives are included in the scan
Scan Memory	Yes	Indicates whether memory is included in the scan
Logging	Normal logging level (includes results summary)	Indicates the logging level selected - none, normal, detailed
Exclude Path/Filename		Indicates if path(s)/filename(s) will be excluded from the scan
Optional Drives	Yes	Indicates if optional drives will be included in the scan

Rows per page: 100 | 1 of 2 selected | Page 1 of 1

Lumension® IT Secured. Success Optimized.™ Server Name: LEMSS Date & Time 5/29/2013 9:26:02 AM

Start | Lumension® EMSS ... | 9:26 AM 5/29/2013


Lumension® EMSS - Groups - Windows Internet Explorer
http://lemss/Forms/groups/default.aspx
Lumension® EMSS - Groups
Lumension® Endpoint Management and Security Suite
Vulnerability Management
Endpoint Protection
Data Protection
Compliance & Reporting
Home
Discover
Review
Manage
Reports
Tools
Help
Administrator | Log Out
Manage > Groups
Groups
Users
My Groups
Custom Groups
By Function
IT
Legal
Sales & Marketing
By Location
Caucasus
CEE
Central Asia
Nordics
Russia
System Groups
IP Collection
Ungrouped
Virtual Machines
Windows
Directory Service Groups
Name:
All
Manage
Name
LEMSS
Rows per pa
View: Endpoint Membership
Hide Filters
Options
LAV Installed
LDC Installed
LPM Installed
LPR Installed
Yes
Yes
Yes
Yes
Page 1 of 1
http://lemss/ - Installation Manager - Windows Internet Explorer
Lumension® Installation Manager
Home
Tools
Help
The components below are available for install/update with the Lumension Endpoint Management and Security Suite (LEMSS). Select a Suite and one or more of the corresponding components to install and/or update.
New/Update Components
Existing Components
Suite Version
Release Date
Suite 7.3.0.10 (7.3 RTM)
5/10/2013
Component
Version
Type
Description
Install Date
Installed By
AntiVirus 7.3
7.3.0.298
Module
Protects against malware via signature-matching capabilities as well as proactive behavioral analysis technologies.
5/14/2013 2:39:07 AM
Administrator
Application Control 7.3
7.3.0.288
Module
Prevents unwanted or dangerous programs from executing via basic snapshot, application whitelist and Trust Engine capabilities.
5/14/2013 2:39:07 AM
Administrator
Device Control 7.3
7.3.0.675
Module
Protects against data theft via blocking of externally attachable devices, monitoring of data transfer, and enforcement of encryption policies on transient data storage technologies.
5/14/2013 2:39:07 AM
Administrator
Patch and Remediation 7.3
7.3.0.267
Module
Provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments.
5/14/2013 2:39:07 AM
Administrator
Power Management 7.3
7.3.0.310
Module
Allows organizations to dramatically reduce PC power consumption by defining and enforcing system-wide power management policies, and
5/14/2013 2:39:07 AM
Administrator
Uninstall
Close
Lumension
http://lemss/default.aspx
Server Name: LEMSS
Date & Time 5/29/2013 9:27:04 AM
Start
Lumension® EMSS - ...
http://lemss/ - Ins...
9:27 AM
5/29/2013

Спасибо!

Edvinas Pranculis MM, CISA, CISM, CRISC
Региональный директор по продажам
Центральная и Восточная Европа, Скандинавия, Россия, Кавказ и Средняя Азия
edvinas.pranculis@lumension.com

Lumension™
IT Secured. Success Optimized.