



Patch Management

HEMMS documentation for agent installation and Schedule Patching for Admins



Prerequisite for joining the HEMMS server for automated patching solution

In order to join the HEMMS automated patching, the following conditions have to be met:

- a. Outgoing ports 443 and 80 on the endpoint network are open. HEMMS uses pull technology, agents check with the HEMMS server for any patch updates. Note that ports 80 and 443 on the HEMMS server are open to all UBC networks, but any new networks (UBC) may require firewall rule changes.
- b. Admins must have an EAD Admin account for access to the HEMMS console.
- c. Supported OS's include versions of Windows 2008, Windows 2012, Windows 7, Windows 10, RHEL 6 and RHEL 7.
- d. The HEMMS agent needs to be installed on the endpoint.
- e. Submit a ticket in Service Now for access to the HEMMS console. Click on this link to submit a ticket to the UBCIT Systems: <http://web.it.ubc.ca/forms/systems/>

NOTE: Please note that at this time only OS patches are supported in HEMMS. Application patches are available but not supported.

Logging on to HEMMS:

Logon to HEMMS using your EAD Admin account. <https://patch.it.ubc.ca>.

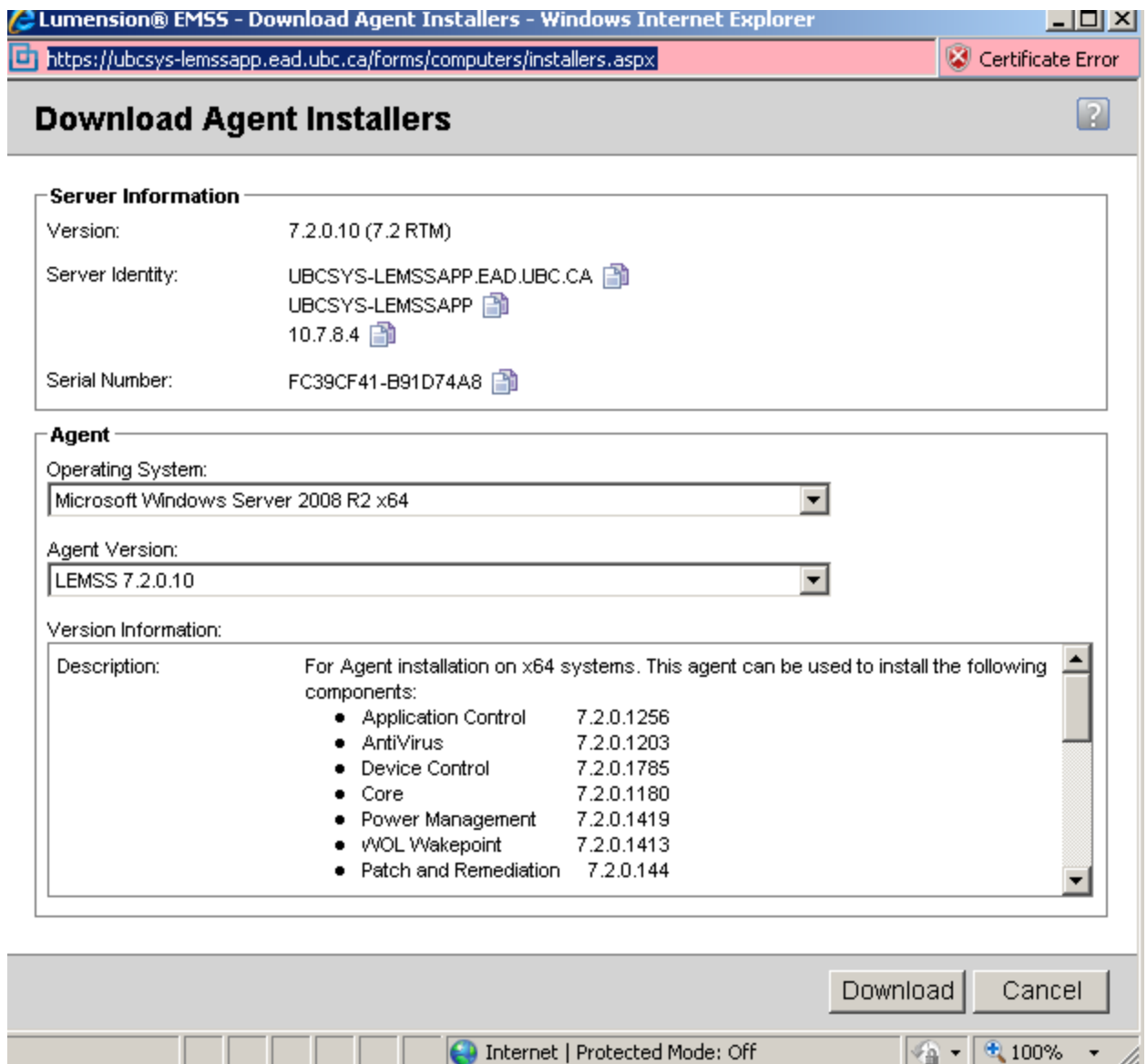
Please note that you will only see the endpoints that you have access to. Contact UBCIT Systems If you are not able to see your group.

1. Installing HEMMS agent on the endpoint and discovering it in HEMMS

Windows agent:

Windows agent can be installed from the HEMMS console, but it requires additional firewall ports to be opened (Windows Print File Sharing ports). To avoid that, download the appropriate Windows agent and install it on the endpoint. Here are the steps:

- Login to the HEMMS console with your EAD Admin account.
- download the agent from the HEMMS console, click on Tools, Download Agent Installer and you will see the following window (note you may get prompted to login if you are not already logged in):



Download Agent Installers

Server Information

Version: 7.2.0.10 (7.2 RTM)

Server Identity: UBCSYS-LEMSSAPP.EAD.UBC.CA
UBCSYS-LEMSSAPP
10.7.8.4

Serial Number: FC39CF41-B91D74A8

Agent

Operating System: Microsoft Windows Server 2008 R2 x64

Agent Version: LEMSS 7.2.0.10

Version Information:

Description: For Agent installation on x64 systems. This agent can be used to install the following components:

- Application Control 7.2.0.1256
- AntiVirus 7.2.0.1203
- Device Control 7.2.0.1785
- Core 7.2.0.1180
- Power Management 7.2.0.1419
- WOL Wakepoint 7.2.0.1413
- Patch and Remediation 7.2.0.144

Download Cancel

Internet | Protected Mode: Off 100%

10/7/2019

- c. Open a Command Prompt and navigate to the directory you downloaded the install executable to.
- d. Run the command using your department group name in the GROUPLIST field,
`lmsetupx64.exe install SERVERIPADDRESS="patch.it.ubc.ca" GROUPLIST="GRP - YOUR GROUP"`.

To find your group name, login to HEMMS (<https://patch.it.ubc.ca>).

Click on Manage, Groups. In the left pane, expand My Groups, University of British Columbia

During the agent install if the endpoint group was not specified then you need to contact the UBCIT Systems group to add the endpoint to your department group and enable LPR (Lumension Patch Remediation module).

- e. From the menu click on Manage, Groups and select the group you specified in step d. Make Endpoint Membership is selected under View. Make sure to enable “Include sub-groups” next to the Update View button.

Name	IP Address	Operating System	Agent Status	Agent Type	Agent Version	LPR Installed
UBCENRL-SSFAADB	142.103.1.132	Microsoft Windows Server 2008 R2 Enterprise x64	Online	LEMSS	7.2.0.10	Yes
UBCENRL-SFADBV1	142.103.219.69	Microsoft Windows Server 2008 R2 Enterprise x64	Online	LEMSS	7.2.0.10	Yes

- f. Once the agent is installed it will check in with the HEMMS server. Once it shows in HEMMS click on the endpoint and make sure that LPR is enabled. “Yes” in the LPR Installed column confirms that LPR is enabled, but if you see “No” then you need to enable it.
- g. To enable LPR, select the endpoint, and click on “Manage Modules”



Lumension® Endpoint Management and Security Suite

Home Discover Review **Manage** Reports Tools Help

Vulnerability Management Endpoint Protection Data Protection Compliance & Reporting

Manage > Endpoints > Information for LEMSS-WINTEST1

Information Vulnerabilities Inventory **Deployments and Tasks**

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

Endpoint Name: LEMSS-WINTEST1
DNS: lemss-wintest1.systems.ubc.ca
IP: 137.82.132.86
MAC Address: 00:50:56:81:02:34
Description: VSS Provisioned Image

Operating System: Win2K8
OS Version: 6.0
OS Service Pack: Service Pack 2
OS Build Number: 6002

Agent Information

Agent version: 7.1.0.70
Agent installation date (Server): 11/07/2012 2:16:29 PM
Uninstall password: [View...](#)

Status Information

Agent status: Online
Last connected date (Server): 08/08/2012 9:54:38 AM
LPR status: Idle
Last DAU scan status: [Success](#)
Last DAU scan time (Server): 08/08/2012 1:55:00 AM

Component Information

Component	Available with this Agent Version	Installed	Installation Date/Time (Server)	Running Version	Policy Version
Core	Yes	Yes	11/07/2012 7:43:18 AM	7.1.0.1209	7.1.0.1209
Patch	Yes	Yes	11/07/2012 2:14:49 PM	7.1.0.103	7.1.0.103
WOL Wakepoint	Yes	No			7.1.0.1448

Group Information

Group Name	Originating Group	Type	Deployments Applicable	Added By	Date Added (Server)
137.82.132.x	137.82.132.x	System Group	Yes	PatchLink Corp.	11/07/2012 2:17:47 PM
Ungrouped	Ungrouped	System Groups	Yes	PatchLink Corp.	11/07/2012 7:43:19 AM
VMWare	VMWare	System Group	Yes	PatchLink Corp.	11/07/2012 7:44:16 AM
Win2K8	Win2K8	System Group	Yes	PatchLink Corp.	11/07/2012 7:43:19 AM
137.82.x.x	137.82.132.x	System Group	Yes	PatchLink Corp.	11/07/2012 2:17:47 PM

- h. Select check box next to the appropriate endpoint (under Patch), click OK. You will see the endpoint go into "Pending". After a few minutes you will see LPR status change to YES.
NOTE: Click on "Update View" button to refresh the display (on the listing of Endpoint page).



Lumension® EMSS - Windows Internet Explorer
https://ubcsys-lemssapp.ead.ubc.ca/forms/admin/ModuleLicense.aspx?Endpoints=4130f6c5-4a77-470b-bd7b-2fdade5d858c

Add/Remove Modules

Select the modules you would like to add or deselect the ones you would like to remove.

Licenses	Patch
Purchased (non-expired)	1500
In Use	45
Pending	0
Available	1455

Endpoint Name	IP Address	Agent Version	Patch
LEMSS-WINTEST1	137.82.132.86	7.1.0.70	<input checked="" type="checkbox"/>

Rows per page: 100 Page 1 of 1

OK Cancel

Done Internet | Protected Mode: Off 100%

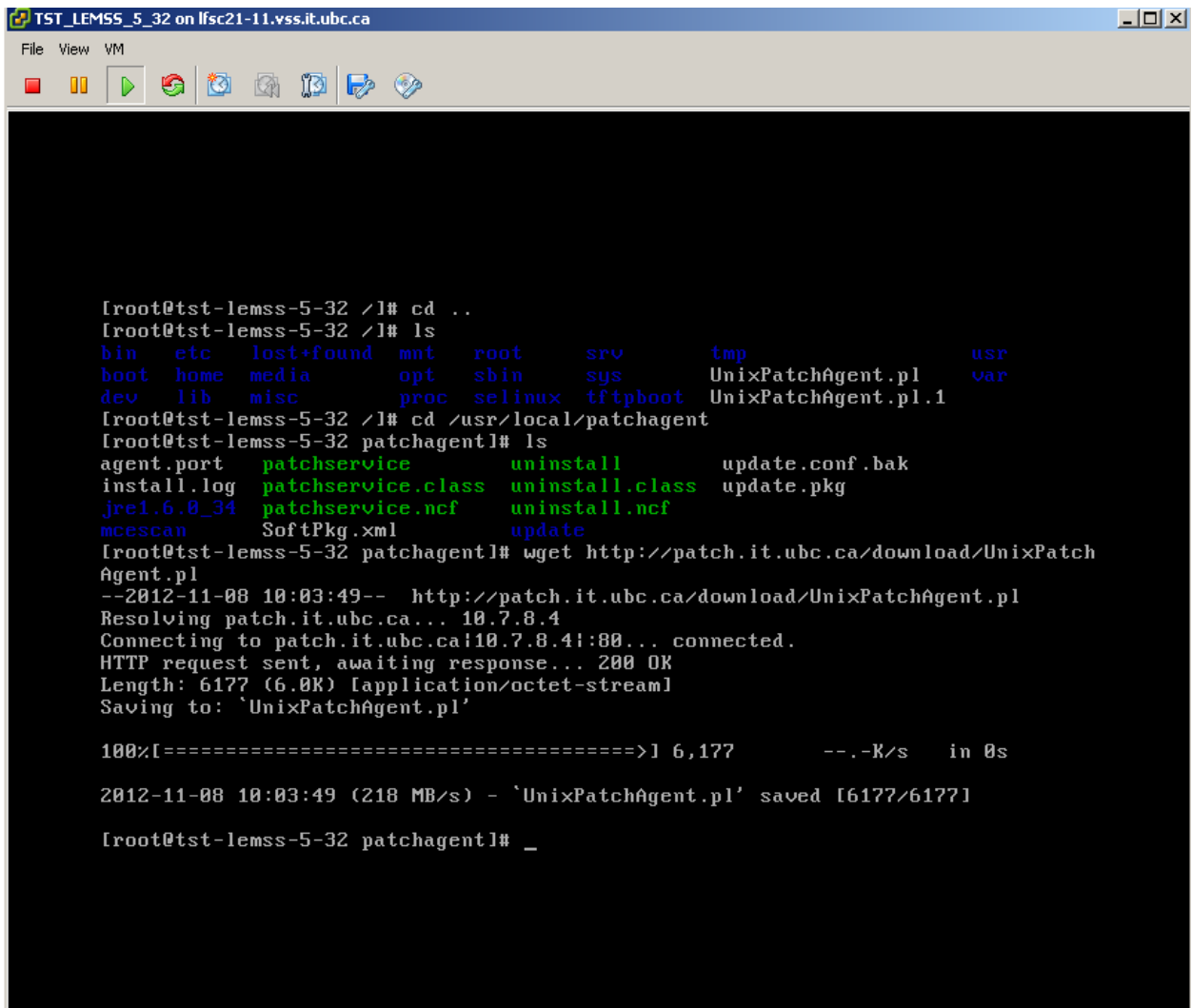


Linux Agent:

HEMMS Linux agent can be installed on Red Hat Enterprise Linux 6 and 7 (32bit or 64bit). Login as root and enter the following commands to install the HEMMS Linux agent.

- a. # `wget http://patch.it.ubc.ca/download/UnixPatchAgent.pl`.

This will download the agent on your server (endpoint), you will see the following message:



```
[root@tst-lemss-5-32 /]# cd ..
[root@tst-lemss-5-32 /]# ls
bin  etc  lost+found  mnt  root  srv  tmp  usr
boot  home  media  opt  sbin  sys  UnixPatchAgent.pl  var
dev  lib  misc  proc  selinux  tftpboot  UnixPatchAgent.pl.1
[root@tst-lemss-5-32 /]# cd /usr/local/patchagent
[root@tst-lemss-5-32 patchagent]# ls
agent.port  patchservice  uninstall  update.conf.bak
install.log  patchservice.class  uninstall.class  update.pkg
jre1.6.0_34  patchservice.ncf  uninstall.ncf
mcescan  SoftPkg.xml  update
[root@tst-lemss-5-32 patchagent]# wget http://patch.it.ubc.ca/download/UnixPatchAgent.pl
--2012-11-08 10:03:49-- http://patch.it.ubc.ca/download/UnixPatchAgent.pl
Resolving patch.it.ubc.ca... 10.7.8.4
Connecting to patch.it.ubc.ca|10.7.8.4|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6177 (6.0K) [application/octet-stream]
Saving to: `UnixPatchAgent.pl'

100%[=====>] 6,177  --.-K/s  in 0s

2012-11-08 10:03:49 (218 MB/s) - `UnixPatchAgent.pl' saved [6177/6177]

[root@tst-lemss-5-32 patchagent]# _
```

- b. # `perl UnixPatchAgent.pl "GRP - YOURGROUP"`

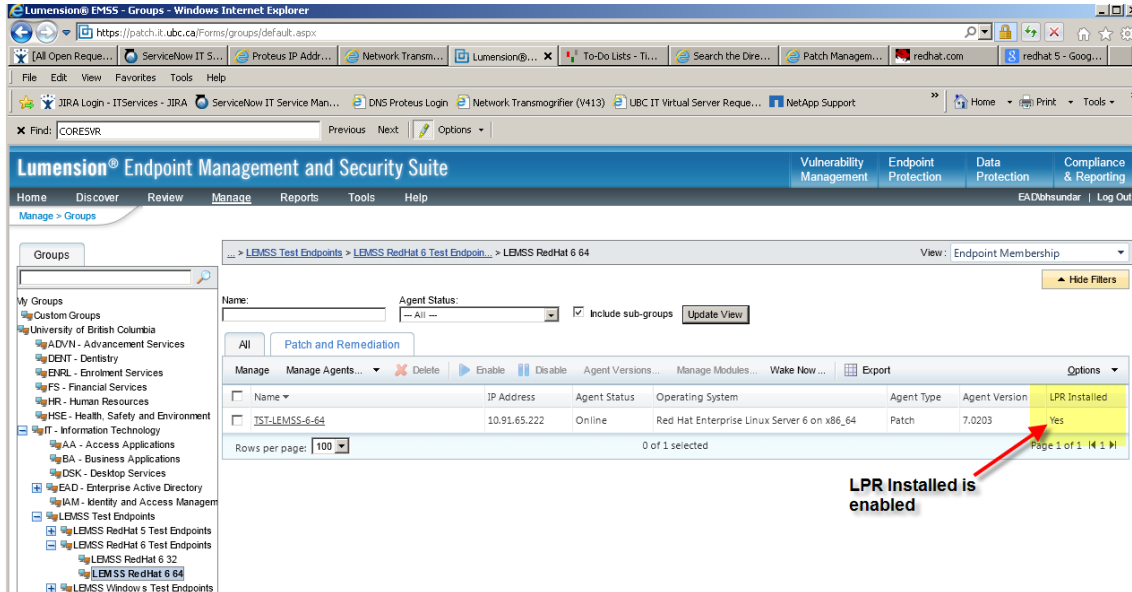
Using the endpoint group this server should belong to

To find your group name, login to HEMMS (<https://patch.it.ubc.ca>).

Click on Manage, Groups. In the left pane, expand My Groups, University of British Columbia.



- c. After a few seconds you should see your endpoint in the appropriate group. Note that under column named “LPR Installed” you should see “Yes”. See the screenshot below.



NOTE:

If the endpoint is not added automatically to a group then the endpoint will go into the general pool and UBCIT Systems group will need to add it to your group before you can see it in HEMMS.

You can create sub group by right clicking on a group and selecting Create Group.

To add or move an endpoint to a group follow the steps below.

a. Click on Manage, Groups.

The screenshot shows the Lumension Endpoint Management and Security Suite interface. The 'Manage' menu is open, and the 'Groups' option is highlighted. The main window displays a list of vulnerabilities for the 'Linux 6' group. The table below shows the details of these vulnerabilities.

Name	Content type	Severity	Applicability	State	Detection status	Include sub-groups	Update View
Red Hat 2012-0386-01 RHBA yum bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0387-01 RHSA Critical: firefox security and bug fix update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0393-01 RHSA Moderate: glibc security and bug fix update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0412-01 RHBA tzdata enhancement update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0415-01 RHBA chkconfig bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0418-01 RHBA cups bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0419-01 RHBA libvirt bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0429-01 RHSA Important: gnutils security update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0430-01 RHBA curl bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0431-01 RHBA libssh2 bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0435-01 RHBA qdm enhancement update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0451-01 RHSA Important: rpm security update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0464-01 RHBA libarchive bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0465-01 RHSA Critical: samba security update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0467-01 RHSA Important: freetype security update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100

b. Right click on the group that you want to add an endpoint and select "Endpoint Membership".

The screenshot shows the Lumension Endpoint Management and Security Suite interface. The 'Endpoint Membership' option is highlighted in the context menu. The main window displays a list of vulnerabilities for the 'Linux 6' group.

Name	Content type	Severity	Applicability	State	Detection status	Include sub-groups	Update View
Red Hat 2012-0386-01 RHBA yum bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0387-01 RHSA Critical: firefox security and bug fix update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0393-01 RHSA Moderate: glibc security and bug fix update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0412-01 RHBA tzdata enhancement update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0415-01 RHBA chkconfig bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0418-01 RHBA cups bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0419-01 RHBA libvirt bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0429-01 RHSA Important: gnutils security update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0430-01 RHBA curl bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0431-01 RHBA libssh2 bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0435-01 RHBA qdm enhancement update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100
Red Hat 2012-0451-01 RHSA Important: rpm security update for RHEL 6 x86_64	Critical - 01	0	1	0	0	1	100
Red Hat 2012-0464-01 RHBA libarchive bug fix update for RHEL 6 x86_64	Recommended	0	1	0	0	1	100



c. Click "Manage".

The screenshot shows the Lumension Endpoint Management and Security Suite interface. The breadcrumb navigation is: IT - Information Technology > SYS - Systems Infrastructure > Linux 6. The 'Manage' button in the top toolbar is circled in red. Below the toolbar, there is a table with columns: Name, IP Address, Agent Status, Operating System, Agent Type, Agent Version, and LPR Installed. The table contains one row: TST-LEMSS-6-64, 10.91.65.222, Online, Red Hat Enterprise Linux Server 6 on x86_64, Patch, 7.0203, Yes. The 'Rows per page' is set to 100, and it shows '0 of 1 selected'.

d. Select the appropriate endpoint and click "Assign". The endpoint will show in windows above, click OK.

The screenshot shows the Lumension Endpoint Management and Security Suite interface. The breadcrumb navigation is: IT - Information Technology > SYS - Systems Infrastructure > Linux 6. The 'Selected Endpoints: 2' section shows a table with columns: Endpoint Name, DNS Name, and OS. The table contains two rows: TST-LEMSS-6-64-QJAVA (selected) and TST-LEMSS-6-64. Below this, there is a table with columns: Endpoint Name, DNS Name, and OS. The table contains 43 rows of endpoints. The 'Assign' button is circled in red. The 'Rows Per Page' is set to 100, and it shows '1 of 1 Pages'.

10/7/2019



2. Schedule Patching

Patching can be scheduled by group or by individual endpoints. In this example we will show how to schedule patching by group as long as all endpoints in the group have the same OS version.

NOTE: Please note that at this time only OS patches should be deployed using HEMMS. Third party application patches are available, but not supported by UBCIT at this time.

- a. Click Manage, Groups. You should see the groups you have access to.

The screenshot shows the Lumension Endpoint Management and Security Suite interface. The main window displays a list of groups under the heading 'My Groups > University of British Columbia'. The interface includes a navigation menu on the left with categories like 'My Groups', 'Custom Groups', and 'Directory Service Groups'. The main area shows a table of groups with columns for Action, Name, Description, Distinguished Name, and Endpoints. The table lists three groups: 'ADVN - Advancement Services', 'ENRL - Enrolment Services', and 'IT - Information Technology'. The 'ENRL - Enrolment Services' group has 2 endpoints. The interface also includes a 'Rows per page' dropdown set to 100 and a 'Page 1 of 1' indicator.

Action	Name	Description	Distinguished Name	Endpoints
	ADVN - Advancement Services		OU=ADVN - Advancement Services,OU=Universi...	0
	ENRL - Enrolment Services	Enrolment Services	OU=ENRL - Enrolment Services,OU=University of...	2
	IT - Information Technology		OU=IT - Information Technology,OU=University ...	0



b. Right click on the appropriate group, and select Vulnerabilities.

The screenshot shows the Lumension Endpoint Management and Security Suite interface. The top navigation bar includes 'Home', 'Discover', 'Review', 'Manage', 'Reports', 'Tools', and 'Help'. The main content area is titled 'Groups' and shows a tree view of organizational groups. The 'IT - Information Technology' group is expanded, and the 'TST-LEMSS-DEV' group is selected. A context menu is open over the 'TST-LEMSS-RHE' group, with 'Vulnerabilities' highlighted. The main pane displays a list of vulnerabilities for the selected group. The table below shows the details of these vulnerabilities.

Name or CVE-ID	Content type	Applicability	State	Detection status							
Red Hat 2014:0126-01 RHSA Moderate: openldap security and bug fix update for RHEL 6	Critical	Applicable	Enabled	Not Patched	0	1	0	0	1	100	
Red Hat 2014:0127-02 RHSA Moderate: librsync2 security update for RHEL 6	Critical	Applicable	Enabled	Not Patched	0	1	0	0	1	100	
Red Hat 2014:0132-01 RHSA Critical: firefox security update for RHEL 6 x86_64	Critical	Applicable	Enabled	Not Patched	0	1	0	0	1	100	
Red Hat 2014:0151-01 RHSA Low: wget security and bug fix update for RHEL 6	Critical	Applicable	Enabled	Not Patched	0	1	0	0	1	100	
Red Hat 2014:0159-01 RHSA Important: kernel security and bug fix update for RHEL 6	Critical	Applicable	Enabled	Not Patched	0	1	0	0	1	100	
Red Hat 2014:0164-01 RHSA Moderate: mysql security and bug fix update for RHEL 6	Critical	Applicable	Enabled	Not Patched	0	1	0	0	1	100	



- d. Patching can be selected by Content type, Applicability, State or Detection Status. It is recommended that you select the following options, Applicable for Applicability, Enabled for State, Not Patched for Detection status. For Content type it all depends how you want to patch your endpoint. It is recommended that you select “Critical and Not Superseded”.

The screenshot shows the Lumension Endpoint Management and Security Suite interface. The top navigation bar includes Home, Discover, Review, Manage, Reports, Tools, and Help. The main content area is titled "Manage > Groups" and shows a tree view of groups on the left. The right pane displays the "Vulnerabilities" view for the group "IT - Information Technology > TST-LEMSS-DEV > TST-LEMSS-RHEL6-64".

Filters are set to: Content type: Critical and Not Superseded, Applicability: Applicable, State: Enabled, Detection status: Not Patched. The "Include sub-groups" checkbox is checked. The "Patch and Remediation" section is active, showing a table of vulnerabilities.

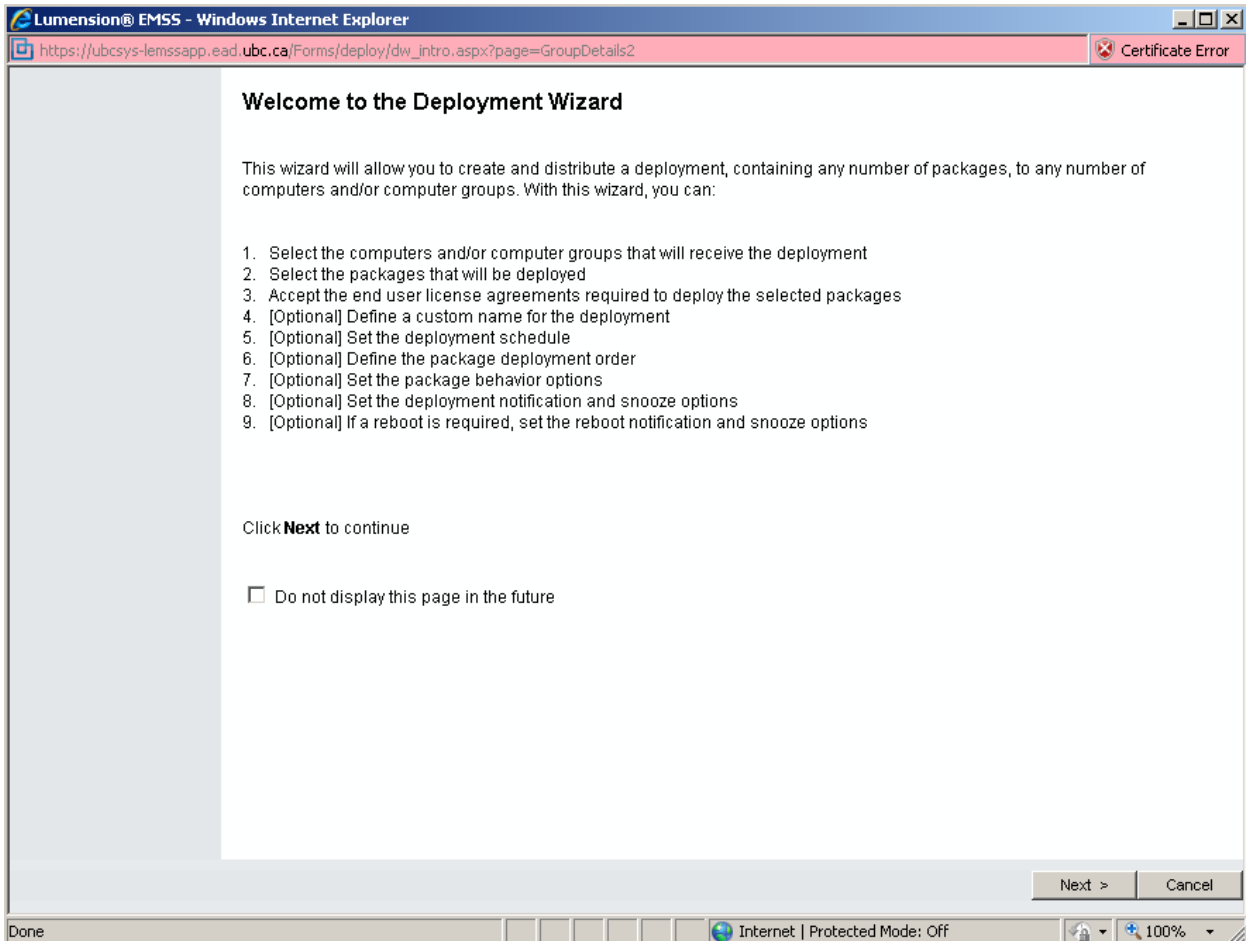
<input type="checkbox"/>	Name	Content type	✓	✗	🔄	📄	📊
<input type="checkbox"/>	Red Hat 2014:0126-01 RHSA Moderate: openldap security and bug fix upda...	Critical	0	1	0	0	1
<input type="checkbox"/>	Red Hat 2014:0127-02 RHSA Moderate: librsvg2 security update for RHEL 6...	Critical	0	1	0	0	1
<input type="checkbox"/>	Red Hat 2014:0132-01 RHSA Critical: firefox security update for RHEL 6 x86_64	Critical	0	1	0	0	1
<input type="checkbox"/>	Red Hat 2014:0151-01 RHSA Low: wget security and bug fix update for RHE...	Critical	0	1	0	0	1
<input type="checkbox"/>	Red Hat 2014:0159-01 RHSA Important: kernel security and bug fix update f...	Critical	0	1	0	0	1
<input type="checkbox"/>	Red Hat 2014:0164-01 RHSA Moderate: mysql security and bug fix update f...	Critical	0	1	0	0	1

- e. Click on the check box next to Name and all patches will be selected, click Deploy.

This screenshot is similar to the previous one, but the "Deploy..." button in the "Patch and Remediation" section is circled in blue. Additionally, the checkboxes in the first column of the table are now checked, indicating that all patches are selected.

<input checked="" type="checkbox"/>	Name	Content type	✓	✗	🔄	📄	📊
<input checked="" type="checkbox"/>	Red Hat 2014:0126-01 RHSA Moderate: openldap security and bug fix upda...	Critical	0	1	0	0	1
<input checked="" type="checkbox"/>	Red Hat 2014:0127-02 RHSA Moderate: librsvg2 security update for RHEL 6 x...	Critical	0	1	0	0	1
<input checked="" type="checkbox"/>	Red Hat 2014:0132-01 RHSA Critical: firefox security update for RHEL 6 x86_64	Critical	0	1	0	0	1
<input checked="" type="checkbox"/>	Red Hat 2014:0151-01 RHSA Low: wget security and bug fix update for RHE...	Critical	0	1	0	0	1
<input checked="" type="checkbox"/>	Red Hat 2014:0159-01 RHSA Important: kernel security and bug fix update f...	Critical	0	1	0	0	1
<input checked="" type="checkbox"/>	Red Hat 2014:0164-01 RHSA Moderate: mysql security and bug fix update f...	Critical	0	1	0	0	1

f. Click Next in the Welcome to the Deployment Wizard.



The screenshot shows a web browser window titled "Lumension® EMSS - Windows Internet Explorer". The address bar shows the URL: https://ubcsys-lemssapp.ead.ubc.ca/Forms/deploy/dw_intro.aspx?page=GroupDetails2. A "Certificate Error" icon is visible in the top right corner of the browser window.

The main content area of the browser displays the "Welcome to the Deployment Wizard" page. The page title is "Welcome to the Deployment Wizard". Below the title, the text reads: "This wizard will allow you to create and distribute a deployment, containing any number of packages, to any number of computers and/or computer groups. With this wizard, you can:"

1. Select the computers and/or computer groups that will receive the deployment
2. Select the packages that will be deployed
3. Accept the end user license agreements required to deploy the selected packages
4. [Optional] Define a custom name for the deployment
5. [Optional] Set the deployment schedule
6. [Optional] Define the package deployment order
7. [Optional] Set the package behavior options
8. [Optional] Set the deployment notification and snooze options
9. [Optional] If a reboot is required, set the reboot notification and snooze options

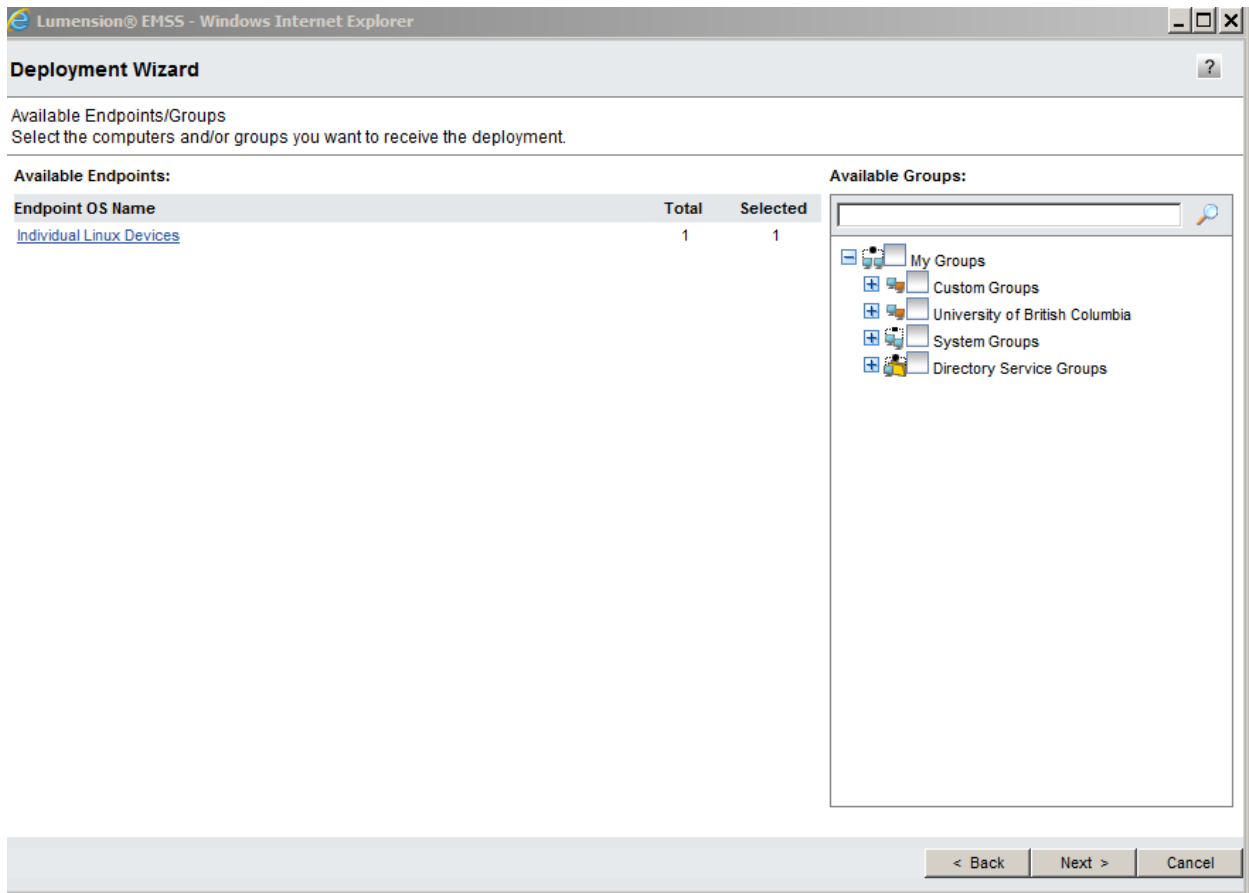
Below the list, the text says: "Click **Next** to continue".

There is a checkbox labeled "Do not display this page in the future" which is currently unchecked.

At the bottom right of the content area, there are two buttons: "Next >" and "Cancel".

The browser's status bar at the bottom shows "Done" on the left, "Internet | Protected Mode: Off" in the center, and a zoom level of "100%" on the right.

- g. Click Next in the next window (Available Endpoints) showing the endpoints that will be patched.



Endpoint OS Name	Total	Selected
Individual Linux Devices	1	1

Available Groups:

- My Groups
 - Custom Groups
 - University of British Columbia
 - System Groups
 - Directory Service Groups



h. Click Next in the next window showing the available patches.

Deployment Wizard

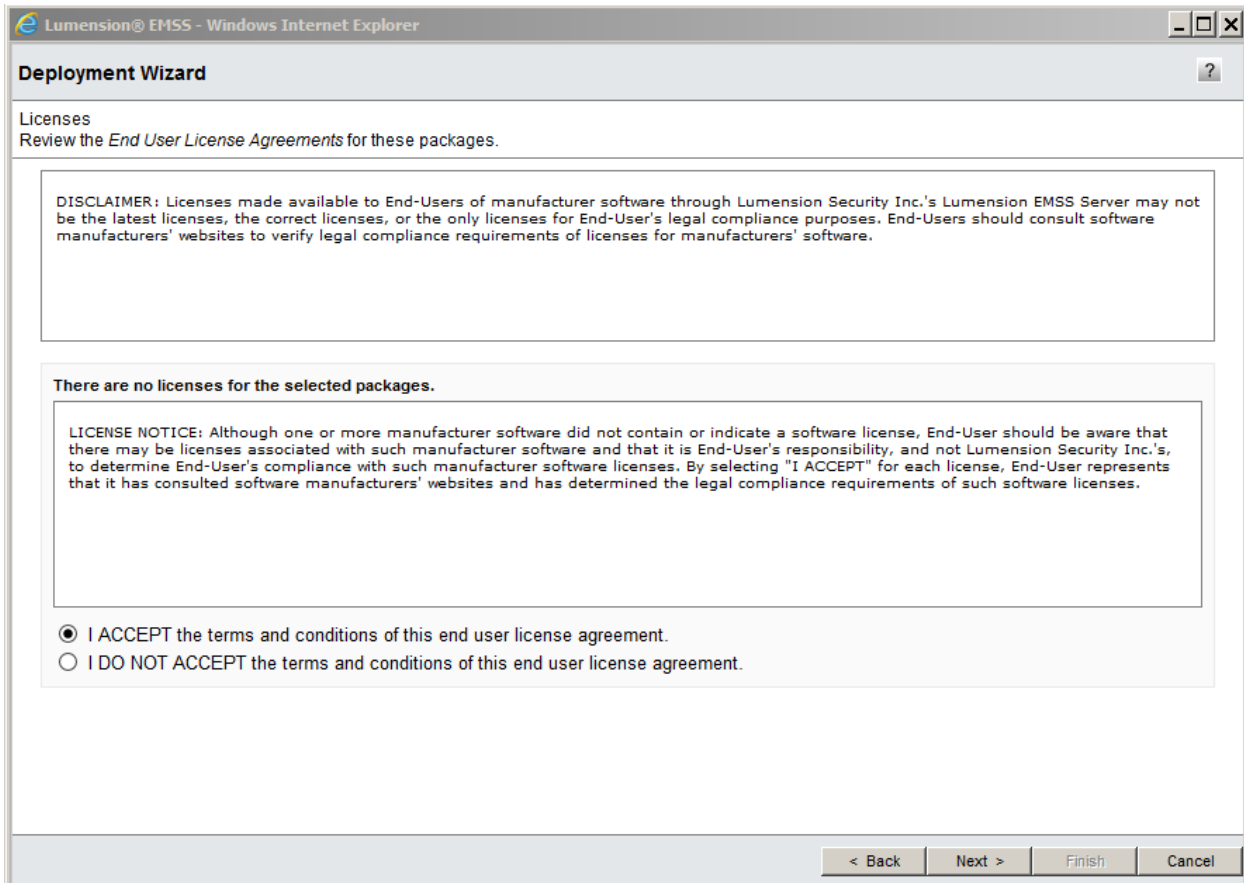
Available Packages
Select the packages you want to deploy.

Vendor Name	Total	Selected
Lumension Security	5	0
Red Hat (Exclusive)	2141	6
Third Party	1	0

Select a vendor to display their available packages.

< Back Next > Cancel

- i. Select radio button to “I ACCEPT the terms and conditions of this end user license agreement” and click Next.



Lumension® EMSS - Windows Internet Explorer

Deployment Wizard

Licenses
Review the *End User License Agreements* for these packages.

DISCLAIMER: Licenses made available to End-Users of manufacturer software through Lumension Security Inc.'s Lumension EMSS Server may not be the latest licenses, the correct licenses, or the only licenses for End-User's legal compliance purposes. End-Users should consult software manufacturers' websites to verify legal compliance requirements of licenses for manufacturers' software.

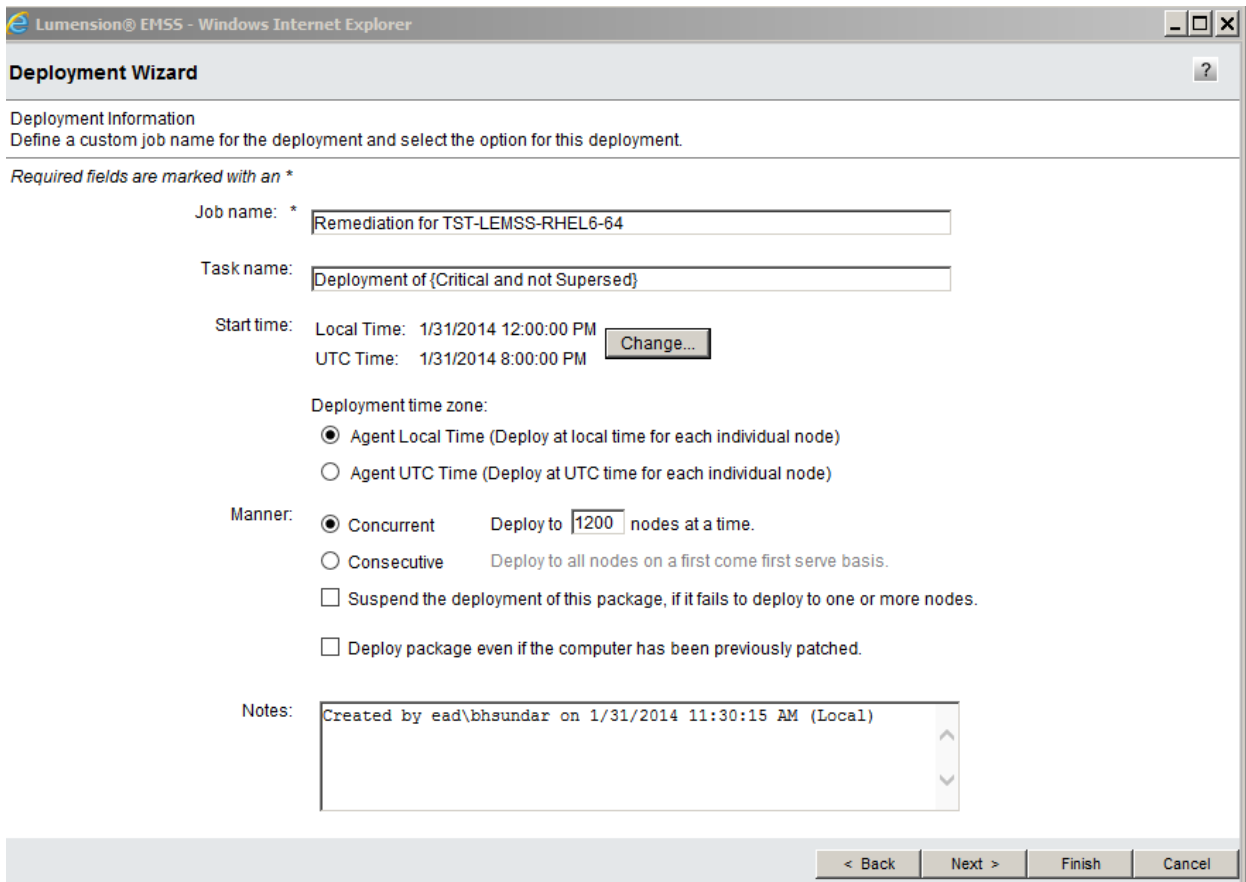
There are no licenses for the selected packages.

LICENSE NOTICE: Although one or more manufacturer software did not contain or indicate a software license, End-User should be aware that there may be licenses associated with such manufacturer software and that it is End-User's responsibility, and not Lumension Security Inc.'s, to determine End-User's compliance with such manufacturer software licenses. By selecting "I ACCEPT" for each license, End-User represents that it has consulted software manufacturers' websites and has determined the legal compliance requirements of such software licenses.

I ACCEPT the terms and conditions of this end user license agreement.
 I DO NOT ACCEPT the terms and conditions of this end user license agreement.

< Back Next > Finish Cancel

- j. Give appropriate names to your Job and Task. Naming task same as the endpoint or group patch is recommended. Click on “Change” button to set a schedule.



Lumension® EMSS - Windows Internet Explorer

Deployment Wizard

Deployment Information
Define a custom job name for the deployment and select the option for this deployment.

Required fields are marked with an *

Job name: * Remediation for TST-LEMSS-RHEL6-64

Task name: Deployment of {Critical and not Superseded}

Start time: Local Time: 1/31/2014 12:00:00 PM
UTC Time: 1/31/2014 8:00:00 PM

Deployment time zone:

Agent Local Time (Deploy at local time for each individual node)
 Agent UTC Time (Deploy at UTC time for each individual node)

Manner:

Concurrent Deploy to 1200 nodes at a time.
 Consecutive Deploy to all nodes on a first come first serve basis.
 Suspend the deployment of this package, if it fails to deploy to one or more nodes.
 Deploy package even if the computer has been previously patched.

Notes: Created by ead\bhsundar on 1/31/2014 11:30:15 AM (Local)

< Back Next > Finish Cancel



K. Review the deployment order and Click Next

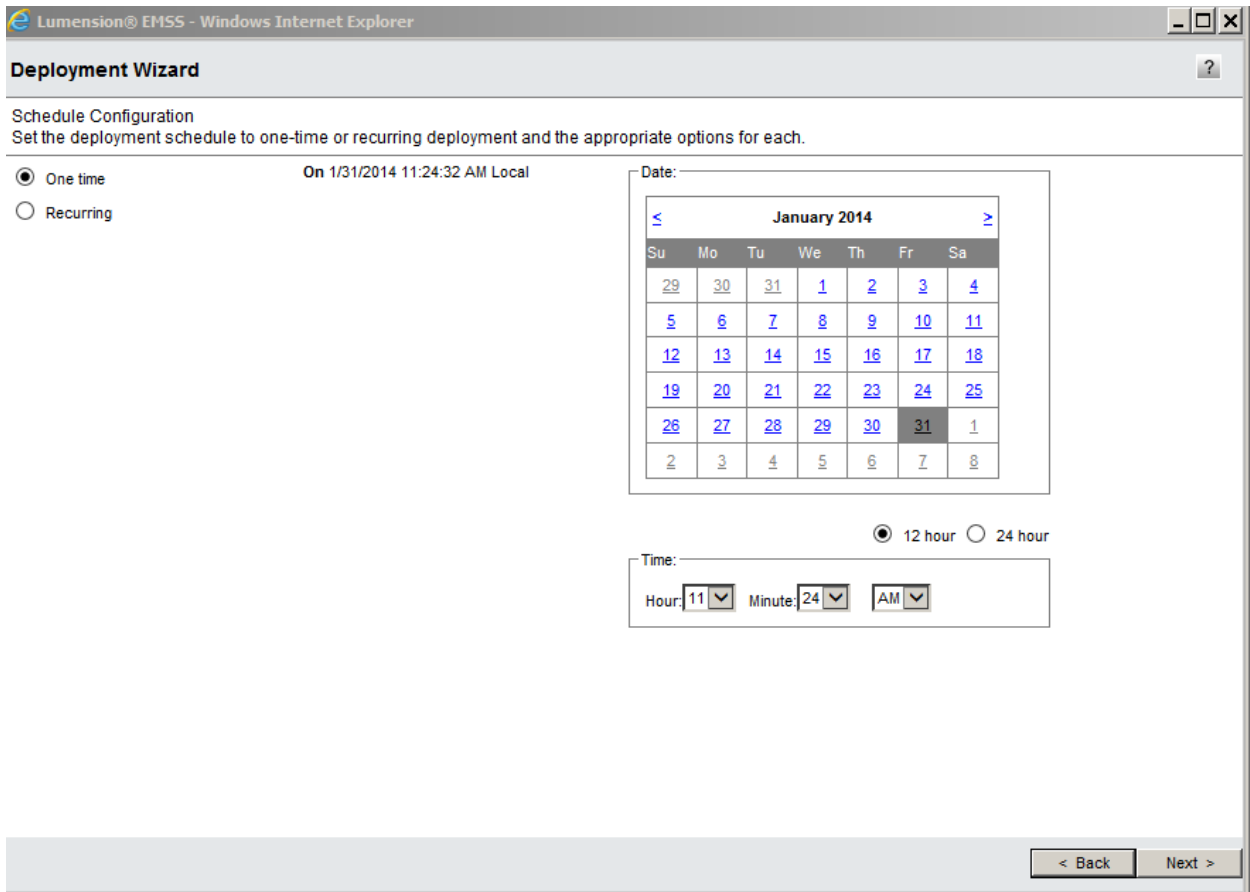
The screenshot shows the 'Deployment Wizard' window in a Windows Internet Explorer browser. The title bar reads 'Lumension® EMSS - Windows Internet Explorer'. The main heading is 'Deployment Wizard' with a help icon. Below this, the text says 'Package Deployment Order and Behavior' and 'Set the deployment order and behavior for each individual package.' A table lists six Red Hat security updates, each with a checkbox, a small icon, an action order number, and a package name. The table has columns for 'Action Order', 'Package Name', 'Selected Options', and 'Reboot'. At the bottom of the window, there are navigation buttons: 'Restore Defaults', '< Back', 'Next >', 'Finish', and 'Cancel'. A pagination bar at the bottom of the table area shows '|< < 1 of 1 Pages > >|' and 'Rows Per Page: 200'.

Action Order	Package Name	Selected Options	Reboot
<input type="checkbox"/> 1	Red Hat 2014:0126-01 RHSA Moderate: openldap security and bug fix update for RHEL 6 Server x86_64		
<input type="checkbox"/> 2	Red Hat 2014:0127-02 RHSA Moderate: librsync2 security update for RHEL 6 Server x86_64		
<input type="checkbox"/> 3	Red Hat 2014:0132-01 RHSA Critical: firefox security update for RHEL 6 Server x86_64		
<input type="checkbox"/> 4	Red Hat 2014:0151-01 RHSA Low: wget security and bug fix update for RHEL 6 Server x86_64		
<input type="checkbox"/> 5	Red Hat 2014:0159-01 RHSA Important: kernel security and bug fix update for RHEL 6 Server x86_64		
<input type="checkbox"/> 6	Red Hat 2014:0164-01 RHSA Moderate: mysql security and bug fix update for RHEL 6 Server x86_64		

- L. In the next window select the options to schedule your patching and click Next. See the e.g. in the screen shot

Note:

Recurring means it will apply the same patches over again.



Lumension® EMSS - Windows Internet Explorer

Deployment Wizard

Schedule Configuration
Set the deployment schedule to one-time or recurring deployment and the appropriate options for each.

One time On 1/31/2014 11:24:32 AM Local

Recurring

Date:

January 2014						
Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

12 hour 24 hour

Time:

Hour: 11 Minute: 24 AM

< Back Next >



M. In the next window confirm the schedule you set and click Next.

Lumension® EMSS - Windows Internet Explorer

Deployment Wizard

Deployment Information
Define a custom job name for the deployment and select the option for this deployment.

*Required fields are marked with an **

Job name: * Remediation for TST-LEMSS-RHEL6-64

Task name: Deployment of {Critical and not Superseded}

Start time: Local Time: 1/31/2014 12:00:00 PM
UTC Time: 1/31/2014 8:00:00 PM

Deployment time zone:

Agent Local Time (Deploy at local time for each individual node)
 Agent UTC Time (Deploy at UTC time for each individual node)

Manner:

Concurrent Deploy to 1200 nodes at a time.
 Consecutive Deploy to all nodes on a first come first serve basis.
 Suspend the deployment of this package, if it fails to deploy to one or more nodes.
 Deploy package even if the computer has been previously patched.

Notes: Created by ead\bhsundar on 1/31/2014 11:30:15 AM (Local)

< Back Next > Finish Cancel



- a. In the next window you will see the packages scheduled for deployment and the options like “chaining” to reduce reboot, what packages require reboot and quiet mode (no user intervention required) etc. You can hover your mouse over the symbols to see what each symbol means. Click Next.

The screenshot shows a web browser window titled "Lumension@ EMSS - Windows Internet Explorer" displaying a "Deployment Wizard" interface. The wizard is titled "Package Deployment Order and Behavior" and instructs the user to "Set the deployment order and behavior for each individual package." Below this instruction is a table with the following columns: "Action", "Order", "Package Name", "Selected Options", and "Reboot". There are six rows of packages listed, each with a checkbox, a small icon, and a number in the "Order" column. The "Package Name" column contains details about Red Hat updates for RHEL 6 Server x86_64. At the bottom of the window, there are navigation buttons: "Restore Defaults", "< Back", "Next >", "Finish", and "Cancel". A pagination bar at the bottom of the table shows "1 of 1 Pages" and "Rows Per Page: 200".

Action	Order	Package Name	Selected Options	Reboot
<input type="checkbox"/>	1	Red Hat 2014:0015-01 RHSA Important: openssl security update for RHEL 6 Server x86_64		
<input type="checkbox"/>	2	Red Hat 2014:0018-01 RHSA Important: libXfont security update for RHEL 6 Server x86_64		
<input type="checkbox"/>	3	Red Hat 2014:0043-01 RHSA Moderate: bind security update for RHEL 6 Server x86_64		
<input type="checkbox"/>	4	Red Hat 2014:0044-01 RHSA Moderate: augeas security update for RHEL 6 Server x86_64		
<input type="checkbox"/>	5	Red Hat 2014:0097-01 RHSA Important: java-1.6.0-openjdk security update for RHEL 6 Server x86_64		
<input type="checkbox"/>	6	Red Hat 2014:0103-01 RHSA Moderate: libvirt security and bug fix update for RHEL 6 Server x86_64		



b. In the next window, select whether you want to receive notification, click Next.

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: {Critical and Not Superseded} is ready to begin. If you require any additional information, please contact your Lumension EMSS
818 characters left.

Use Policies

Options	Setting	Use Agent Policy
Allow user to cancel	No	<input type="checkbox"/>
Allow user to snooze	Yes	<input type="checkbox"/>
Notification on top	Yes	<input type="checkbox"/>

Deploy

Within 60 Mins
 By 09/08/2012 12:00 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
804 characters left.

Use Policies

Options	Setting	Use Agent Policy
Allow user to cancel	No	<input type="checkbox"/>
Allow user to snooze	Yes	<input type="checkbox"/>
Reboot within	60 Mins	<input type="checkbox"/>

< Back Next > Finish Cancel

Done Internet | Protected Mode: Off 100%



c. In the next window you will see Deployment Confirmation, Click Finish.

Deployment Wizard

Deployment Confirmation
Verify the deployment options and summary information

Job name:	Remediation for TST-LEMSS-RHEL6-64
Schedule:	One time deployment, starting on 1/31/2014 12:00:00 PM based on Agent Local Time.
Manner:	Concurrent: Deploying to 1200 endpoints at a time.
Deployment notification:	Users will not be notified of the deployment.
Reboot Notification:	The deployment does not require a reboot.
Total selected packages:	6
Total selected computers/groups:	1
Notes:	Created by ead/bhsundar on 1/31/2014 11:30:15 AM (Local)

Selected Packages:

Order	Package Name	Selected Options	Reboot	Endpoints/Groups
1	Red Hat 2014:0015-01 RHSA Important: openssl security update for RHEL 6 Server x86_64			1
2	Red Hat 2014:0018-01 RHSA Important: libXfont security update for RHEL 6 Server x86_64			1
3	Red Hat 2014:0043-01 RHSA Moderate: bind security update for RHEL 6 Server x86_64			1
4	Red Hat 2014:0044-01 RHSA Moderate: augeas security update for RHEL 6 Server x86_64			1
5	Red Hat 2014:0097-01 RHSA Important: java-1.6.0-openjdk security update for RHEL 6 Server x86_64			1
6	Red Hat 2014:0103-01 RHSA Moderate: libvirt security and bug fix update for RHEL 6 Server x86_64			1

Navigation: |< < 1 of 1 Pages > >| Rows Per Page: 200

Buttons: < Back Next > Finish Cancel



- d. If the packages are not cached you will see the packages being cached, wait until all packages are cached. You will see the status as “Requesting”, this could take several minutes depending on how many packages are being cached. You may deploy without caching by clicking on the “Deploy Unordered” button.

Deployment Wizard

Deployment Summary
Click specific package name to view the deployment details. Click Close to exit the wizard.

Job name:	Sysms Windows Remediation - 08/08/2012 11:54:20 AM
Schedule:	Recurring deployment, starting on 08/08/2012 11:00:00 PM based on Agent Local Time.
Manner:	Concurrent. Deploying to 1000 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:	6
Total selected computers/groups:	2
Notes:	Created by ead\bhsundar on 08/08/2012 4:54:20 AM (Local)

Selected Packages: (4 of 6 packages have been cached) Auto-Refresh:

Package Name	Status
MS 2468871 Update for .NET Framework 4.0 (All Languages) (64Bit)	Requesting
MS 2533523 Reliability Update 1 for .NET Framework 4.0 (All Languages) (64Bit)	Requesting
MS 2639658 Workaround for Vulnerability in TrueType Font Parsing (Disabled) (64Bit)	Cached
MS 2719615 Workaround for Vulnerability in in Microsoft XML Core Services (Disabled)	Cached
MS 931125 Update for Root Certificates (April 2012) (All Languages)	Cached
MS 973688 Update for XML Core Services 4.0 Service Pack 2 (64Bit)	Cached

|< < 1 of 1 Pages > >| Rows Per Page: 100

Your packages have been requested; once all requested packages have been cached, the deployment will begin as scheduled.

Refresh Deploy Unordered Cancel



e. Click Close to complete the scheduling.

Lumension® EMSS - Windows Internet Explorer

Deployment Wizard

Deployment Summary
Click specific package name to view the deployment details. Click Close to exit the wizard.

Job name:	Remediation for TST-LEMSS-RHEL6-64
Schedule:	One time deployment, starting on 1/31/2014 12:00:00 PM based on Agent Local Time.
Manner:	Concurrent: Deploying to 1200 endpoints at a time.
Deployment notification:	Users will not be notified of the deployment.
Reboot Notification:	The deployment does not require a reboot.
Total selected packages:	6
Total selected computers/groups:	1
Notes:	Created by ead\lhsundar on 1/31/2014 11:30:15 AM (Local)

Selected Packages:

Order	Package Name	Selected Options	Reboot	Endpoints/Groups
1	Red Hat 2014:0015-01 RHSA Important: openssl security update for RHEL 6 Server x86_64			1
2	Red Hat 2014:0018-01 RHSA Important: libXfont security update for RHEL 6 Server x86_64			1
3	Red Hat 2014:0043-01 RHSA Moderate: bind security update for RHEL 6 Server x86_64			1
4	Red Hat 2014:0044-01 RHSA Moderate: auqegas security update for RHEL 6 Server x86_64			1
5	Red Hat 2014:0097-01 RHSA Important: java-1.6.0-openjdk security update for RHEL 6 Server x86_64			1
6	Red Hat 2014:0103-01 RHSA Moderate: libvirt security and bug fix update for RHEL 6 Server x86_64			1

Rows Per Page: 200

Close

f. Click on Manage, Deployment and Tasks to see your newly created patching schedule.

Lumension® Endpoint Management and Security Suite

Home Discover Review **Manage** Reports Tools Help

Manage > Deployments and Tasks

Status: All Type: All Update View

Enable Disable Abort Deletes Deploy... Export Options

Name	Type	Created Date	Created By
Remediation for TST-LEMSS-RHEL6-64	Package Deployment	1/31/2014 11:39:51 AM (Local)	EAD\lhsundar
Mandatory Baseline: Red Hat 2014:0101-01 RHEA tzda...	Mandatory Baseline Deployment	1/31/2014 11:15:08 AM (Local)	System
Mandatory Baseline: Red Hat 2014:0104-01 RHEA ope...	Mandatory Baseline Deployment	1/31/2014 11:15:08 AM (Local)	System
Mandatory Baseline: Red Hat 2013:1867-01 RHEA tzdat...	Mandatory Baseline Deployment	1/31/2014 11:15:08 AM (Local)	System


3. Deploy same Patches to different Groups or Endpoints

Follow the instructions below to apply a set of patches that has already been tested on a group or endpoint e.g. Development group to another group or endpoint e.g. Production group.

NOTE:

The patches must be for the same OS version.

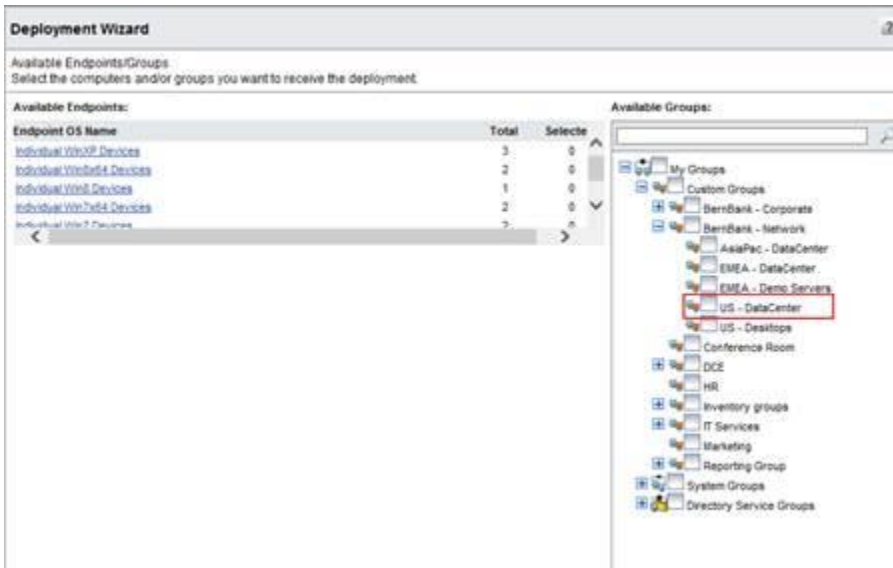
How to redeploy a Deployment Steps

- Select Manage  Deployments and Tasks
- Select a Deployment that already exists and has been test on a group or endpoint e.g. Development group or endpoint
- Select Deploy...



Remediation - 12/13/2013 7:14:11 AM									
Name	Type	Created Date	Created By						
Remediation - 12/13/2013 7:14:11 AM	Package Deployment	12/13/2013 7:14:32 AM (local)	LUMENSONIreneg						
Action	Name	Scheduled Date	Status	✓	✗	📄	📁	📧	%
<input checked="" type="checkbox"/>	Deployment of MS13-097 Cumulative Security Update for Internet Explorer 10 for Windows Server 2008 R2 Service Pack 1 x64 (KB2887051)(x64)(all)	12/13/2013 7:00:00 PM (local)	Completed	1	0	1	0	1	100%
<input checked="" type="checkbox"/>	Deployment of MS13-099 Security Update for Windows Server 2008 R2 x64 (KB2892074)(x64)(all)	12/13/2013 7:00:00 PM (local)	Completed	1	0	1	0	1	100%
<input checked="" type="checkbox"/>	Deployment of MS13-101 Security Update for Windows Server 2008 R2 x64 (KB2887069)(x64)(all)	12/13/2013 7:00:00 PM (local)	Completed	1	0	1	0	1	100%
<input checked="" type="checkbox"/>	Deployment of MS13-101 Security Update for Windows Server 2008 R2 x64 (KB2892084)(x64)(all)	12/13/2013 7:00:00 PM (local)	Completed	1	0	1	0	1	100%
<input checked="" type="checkbox"/>	Deployment of Security Update for Windows Vista, Windows 7, Server 2008, Server 2008 R2 (KB2917500)(x64)(all)	12/13/2013 7:00:00 PM (local)	Completed	1	0	1	0	1	100%
<input checked="" type="checkbox"/>	Deployment of MS13-098 Security Update for Windows Server 2008 R2 x64 (KB2893294)(x64)(all)	12/13/2013 7:00:00 PM (local)	Completed	1	0	1	0	1	100%

- d. Select Custom, System Group or endpoint to deploy e.g. a production group or endpoint.



- e. Go through Deployment Wizard\Schedule



4. Patching through Mandatory Baseline Policy

A **Mandatory Baseline** is a minimum set of content that *must* be installed on a group's endpoints. Composed of user-defined content items deemed essential to the group, this **baseline** continually verifies that the applicable items are installed on group endpoints. If a group endpoint is found in a *non-compliant* state (does not have an item defined in the **baseline** installed), Lumension Endpoint Management and Security Suite automatically deploys the applicable content until the endpoint is once again compliant. Mandatory **Baselines** ensure group endpoints are never without essential security content.

It is recommended when implementing Mandatory Baseline policy you should also implement Agent Policy set for the same group so hours of operation can be defined, i.e. set specific time to apply patches to an endpoint or a group of endpoints. If this is not done then the Mandatory Baseline policy will push the patches as soon as it's detected and server could be rebooted after patches are applied.

Get more details on Baseline policy and Agent policy set from the HEMMS console, click on Help, New Users Start Here...

Uninstalling Linux Agent:

- i. Login as root. Change the directory to `/usr/local/patchagent`.
- ii. Execute command `./uninstall`. When prompted, reply `y`.
- iii. Execute the following command from the `/usr/local` to delete the patchagent directory: `rm -rf patchagent`