



Patch Management

Ivanti Endpoint Security (IES) Admin Guide



Contents

Prerequisites for joining IES	2
Logging on to IES:	2
Endpoint Installation	3
Windows	3
Add Windows Endpoint	3
Remove Windows Endpoint	6
Linux	8
Add Linux Endpoint	8
Remove Linux Endpoint	9
Migrate Endpoints	11
Prerequisites	11
Migrate Windows Endpoints	11
Migrate Linux Endpoints	12
Managing Groups	13
Create a Group:	13
Add/Remove Endpoints from a group	14
Assign Agent Policy to a group	15
Schedule Patching	16



Prerequisites for joining IES

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

- a. Outgoing ports 443 and 80 on the endpoint network are open. IES uses pull technology, agents check with the IES server for any patch updates. Note that ports 80 and 443 on the IES 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 IES console.
- c. Supported OS's include Windows Server 2012-2019, RHEL 7-8, Ubuntu 18-20.
- d. The IES agent needs to be installed on the endpoint.
- e. Submit a ticket in Service Now for access to the IES 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 IES. Application patches are available but not supported.

Logging on to IES:

Logon to IES at <https://patching.it.ubc.ca/> using your EAD Admin account- format **EAD\cwluser.adm**

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.



Endpoint Installation

Windows

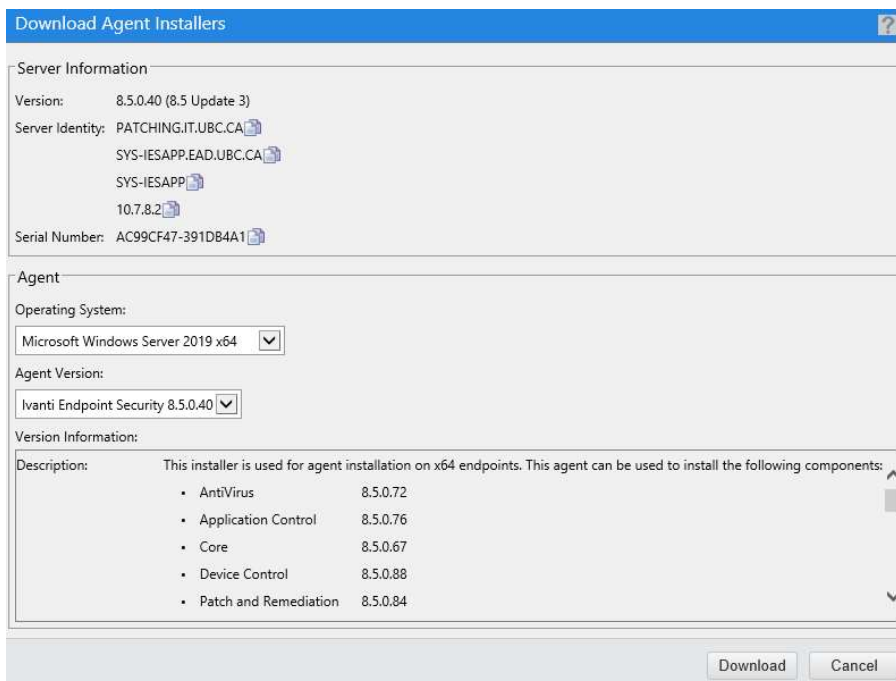
Supported versions:

2012/2016/2019

Add Windows Endpoint

Windows agent can be installed from the IES 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.

- a. Login to the IES console (<https://patching.it.ubc.ca>) with your **EAD Admin** account (EAD\- b. Download the agent from the IES console, click on **Tools/Download Agent Installer...** select OS and click **Download**.



5/17/2021



- c. Open a **Command Prompt (Admin)** and navigate to the directory you downloaded the executable to.
- d. **Run** the command using your department group name in the **GROUPLIST** field:

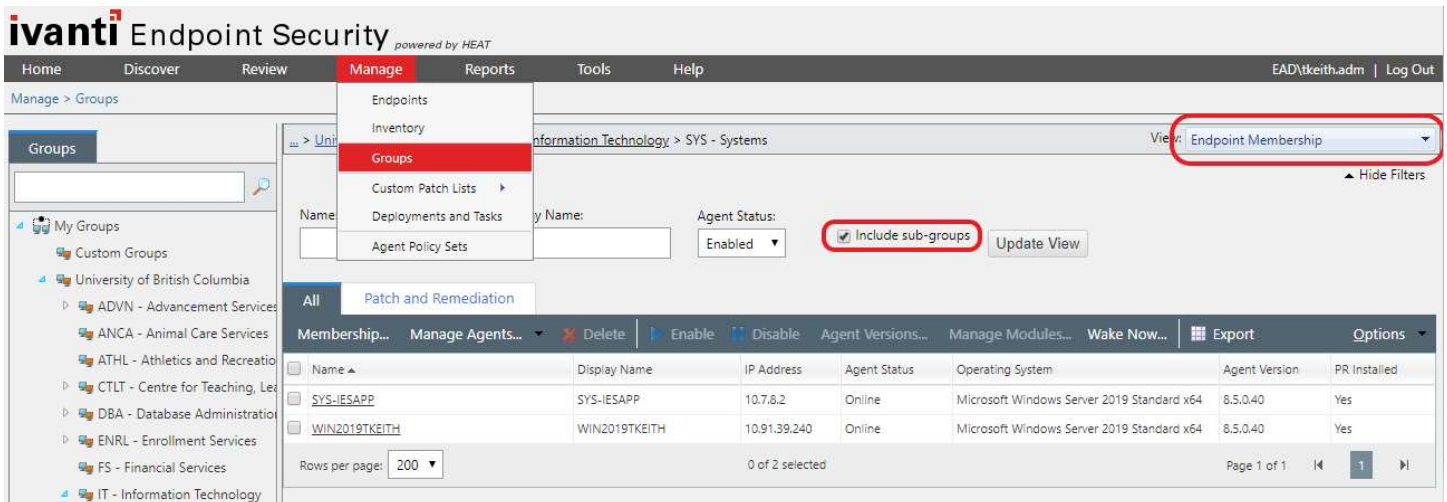
```
Imsetupx64.exe install SERVERIPADDRESS="patching.it.ubc.ca"
MODULELIST="VulnerabilityManagement" GROUPLIST="GRP – YOUR GROUP"
```

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

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

Please Note: During the agent install if the endpoint group was not specified, or for some reason the endpoint was not added to your group it will end up in **My Groups\System Groups\Ungrouped**. You will need to move it manually to your specific group. (See [Managing Groups](#))

- e. From the menu click on **Manage\Groups** and select the group you specified. Make sure “Endpoint Membership” is selected under “View” if it is not.



- f. Once the agent is installed it will check in with the IES server. Once it shows in IES click on the endpoint and make sure that PR is enabled. “Yes” in the “PR Installed” column confirms that PR is enabled, but if you see “No” then you need to enable it. It may also still be “Pending Install” state so check back in a few minutes.

- g. To enable PR, select the endpoint, and click on “**Manage Modules**”

Name	Display Name	IP Address	Agent Status	Operating System	Agent Version	PR Installed
<input type="checkbox"/> SYS-IESAPP	SYS-IESAPP	10.7.8.2	Online	Microsoft Windows Server 2019 Standard x64	8.5.0.40	Yes
<input checked="" type="checkbox"/> WIN2019TKEITH	WIN2019TKEITH	10.91.39.240	Online	Microsoft Windows Server 2019 Standard x64	8.5.0.40	Pending Install

- h. Select **check box** next to the appropriate endpoint (under Patch), click **OK**. You will see the endpoint go into “**Pending Install**”. After a few minutes you will see PR status change to **YES**.

NOTE: Click on “**Update View**” button to refresh the display (on the listing of Endpoint page).

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	1
Pending	1
Available	1498

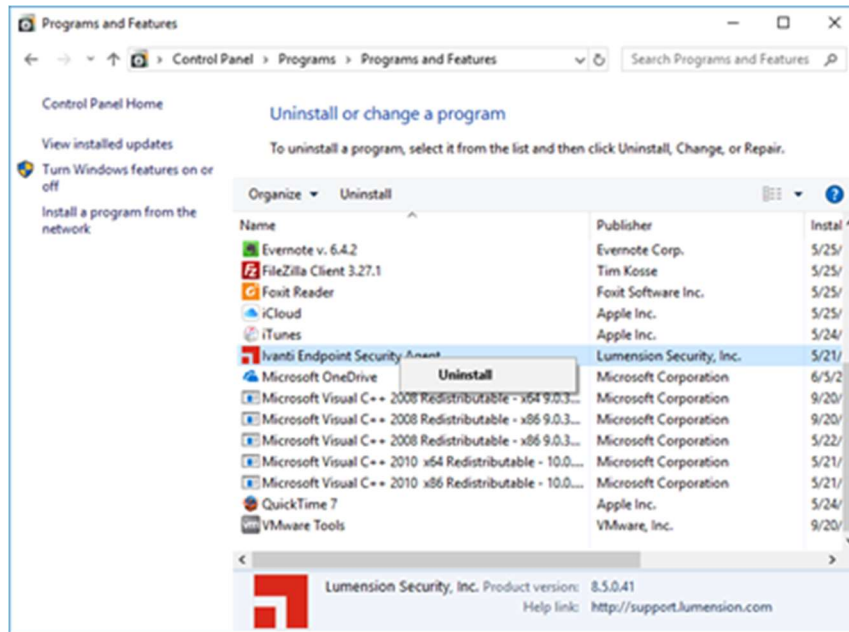
Endpoint Name	IP Address	Agent Version	Patch
WIN2019TKEITH	10.91.39.240	8.5.0.40	<input checked="" type="checkbox"/>

Rows per page: 200 | 0 of 1 selected | Page 1 of 1

OK Cancel

Remove Windows Endpoint

- a. Go into **Program and Features** and uninstall the “**LMAgent**”, “**Heat Endpoint Management**”, “**Security Suite Agent**” or “**Ivanti Endpoint Security Agent**”
(Depending on how old your version of Ivanti Endpoint Security is)



- b. Go to the Ivanti portal and click on **Manage\Endpoints** and locate the endpoint name under the All tab.
- c. Ensure that your filter for **Agent Status** is set to “--- All ---”

NOTE: If it's not there then it removed itself during the agent uninstall and you can **STOP** here.

- d. Disable the endpoint by selecting it and choosing “Disable”

The screenshot shows the Ivanti Endpoint Security web interface. The 'Manage' tab is active, and the 'Endpoints' page is displayed. A table lists several endpoints. The endpoint 'SUC-MEVANS-1W10' is selected, and the 'Disable' button in the 'Manage Agents...' toolbar is highlighted. The table below shows the following data:

Name	Display Name	IP Address	Agent Status	Operating System	Agent Version	AC Installed	AV Installed	DC Installed	PR Installed
SUC-MEVANS-1U6	SUC-MEVANS-1U6	10.25.2.56	Online	CentOS Linux 7 on x...	8.5.037	No	No	No	Yes
SUC-MEVANS-1S16	SUC-MEVANS-1S16	10.25.2.53	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-1W10	SUC-MEVANS-1W10	10.25.2.50	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-1W7	SUC-MEVANS-1W7	10.25.2.54	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-1W8	SUC-MEVANS-1W8	10.25.2.51	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-512	SUC-MEVANS-512	10.25.2.52	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes

- e. Delete the endpoint from the endpoints page so it does not show up in the Ivanti web interface.

The screenshot shows the Ivanti Endpoint Security web interface. The 'Manage' tab is active, and the 'Endpoints' page is displayed. The 'Agent Status' dropdown menu is set to 'All'. The endpoint 'SUC-MEVANS-1W10' is selected, and the 'Delete' button in the 'Manage Agents...' toolbar is highlighted. The table below shows the following data:

Name	Display Name	IP Address	Agent Status	Operating System	Agent Version	AC Installed	AV Installed	DC Installed	PR Installed
SUC-MEVANS-1U6	SUC-MEVANS-1U6	10.25.2.56	Online	CentOS Linux 7 on x...	8.5.037	No	No	No	Yes
SUC-MEVANS-1S16	SUC-MEVANS-1S16	10.25.2.53	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-1W10	SUC-MEVANS-1W10	10.25.2.50	Disabled	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-1W7	SUC-MEVANS-1W7	10.25.2.54	Disabled	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-1W8	SUC-MEVANS-1W8	10.25.2.51	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes
SUC-MEVANS-512	SUC-MEVANS-512	10.25.2.52	Online	Microsoft Windows ...	8.5.0.30	Yes	Yes	Yes	Yes



Linux

Supported versions:

Red Hat Enterprise Linux: 7.x/8.x

Ubuntu Linux: 18/20

Add Linux Endpoint

- a. Issue the following command as root:

```
# perl <(curl https://bootstrap.it.ubc.ca/download/UnixPatchAgent.pl)
```

- b. When prompted, enter the group this server should be joined to.

To find your group name 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 **"PR Installed"** you should see **"Yes"**. See the screenshot below.

Please Note: During the agent install if the endpoint group was not specified, or for some reason the endpoint was not added to your group it will end up in **My Groups\System Groups\Ungrouped**. You will need to move it manually to your specific group. (See [Managing Groups](#))



- d. If PR is not installed, select the endpoint, and click on “**Manage Modules**”

Name	Display Name	IP Address	Agent Status	Operating System	Agent Version	PR Installed
<input type="checkbox"/> SYS-IESAPP	SYS-IESAPP	10.7.8.2	Online	Microsoft Windows Server 2019 Standard x64	8.5.0.40	Yes
<input checked="" type="checkbox"/> WIN2019TKEITH	WIN2019TKEITH	10.91.39.240	Online	Microsoft Windows Server 2019 Standard x64	8.5.0.40	Pending Install

- e. Select check box next to the appropriate endpoint (under Patch), click **OK**. You will see the endpoint go into “**Pending Install**”. After a few minutes you will see PR status change to **YES**.

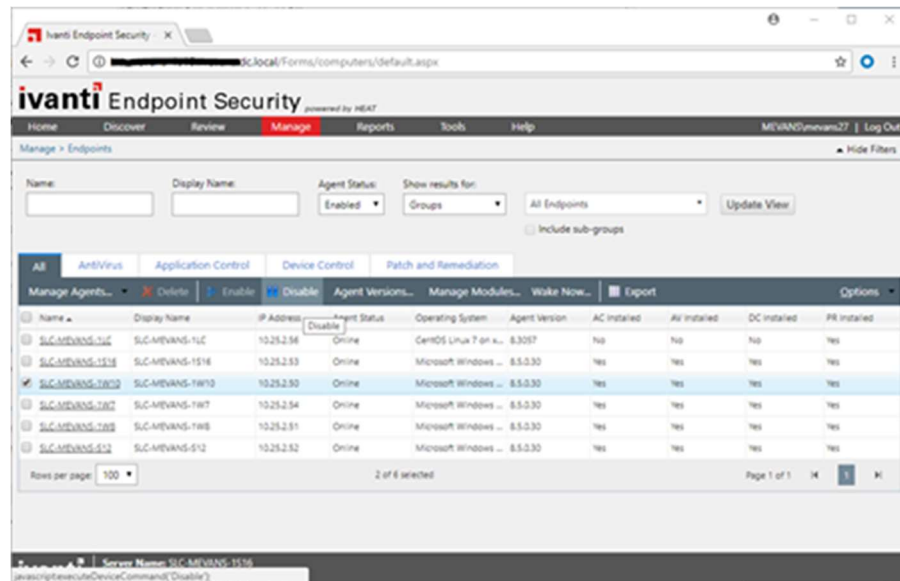
NOTE: Click on “Update View” button to refresh the display (on the listing of Endpoint page)

Remove Linux Endpoint

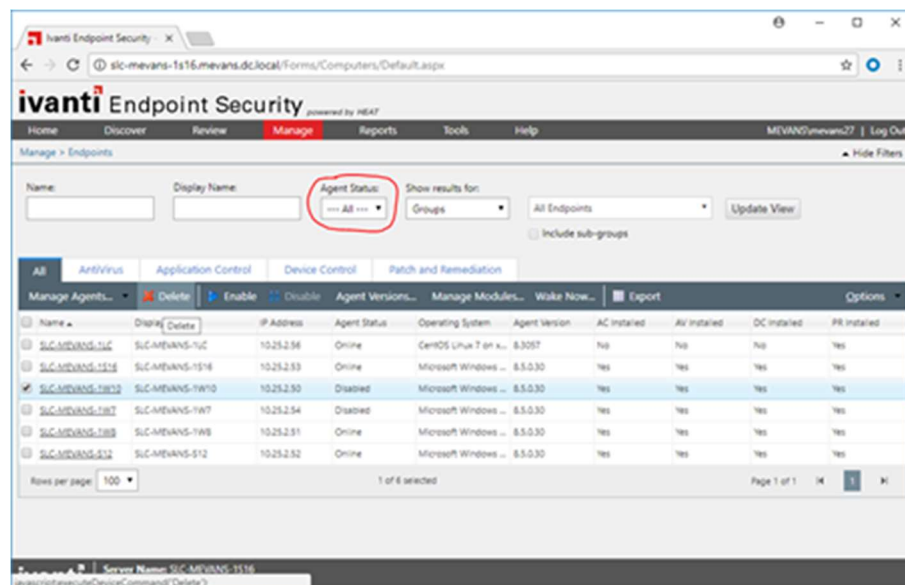
- Run the EMSS agent uninstaller on the endpoint:
`# /usr/local/patchagent/uninstall`
- Delete the patchagent directory:
`# rm -rf /usr/local/patchagent`
- Go to the Ivanti portal and click on **Manage\Endpoints** and locate the endpoint name under the All tab.

NOTE: If it's not there then it removed itself during the agent uninstall and you can **STOP** here.

- Disable the endpoint by selecting it and choosing “Disable”



- **Delete** the endpoint from the endpoints page so it does not show up in the Ivanti web interface.
If you do not see the agent, ensure your filter for Agent Status is set to “--- All ---”





Migrate Endpoints

If you have any endpoints you need migrated to the new Ivanti portal you can follow this guide.

Prerequisites

- a. Document your group before migrating.
 - To find your group name, login to IES (<https://patching.it.ubc.ca>).
 - Click on Manage/Groups. Write down the Group your endpoint should go in.
- b. Enter this Group in the fields where requested during Windows or Linux installs.
- c. RHEL8 endpoints require Python to be installed for DAU Scanning to work.
- d. Linux endpoints may require bc and nc. See Troubleshooting during Linux migration steps.

Migrate Windows Endpoints

- a. On your Windows endpoint download the new agent from the Ivanti Portal at (<https://patching.it.ubc.ca>)
Tools>Download Agent Installer...
- b. Open **Command Prompt (Admin)** and navigate to the directory you downloaded the install executable to.
- c. **Run command:** (To uninstall old HEMSS Patch Agent)
Imsetupx64.exe uninstall
- d. Wait and **verify/confirm** the current Heat Agent has been uninstalled.
- e. **Run command:** (To install new Ivanti Patch Agent. Use the group name in the **GROUPLIST** field)
*Imsetupx64.exe install SERVERIPADDRESS="patching.it.ubc.ca" MODULELIST="VulnerabilityManagement"
GROUPLIST="GRP – YOUR GROUP"*

Please Note: This process will uninstall the old endpoint agent and install the new agent to Ivanti. *The endpoint may end up in **My Groups\System Groups\Ungrouped**. You will need to move it manually to your specific group.* (See [Managing Groups](#))



Migrate Linux Endpoints

Linux Endpoints need to download and install the new agent which will upgrade the Patch Agent and register it in the new Ivanti Service:

- a. On your Linux endpoint **run** the new agent script to upgrade:

```
perl <(curl https://bootstrap.it.ubc.ca/download/UnixPatchAgent.pl)
```

- b. It will ask you to enter the Group you want to register the patch agent to.

- c. It should now complete the upgrade. The endpoint should now show up in your group in Ivanti.

Please Note: This process will upgrade the endpoint agent and start talking to Ivanti. *The endpoint may end up in **My Groups\System Groups\Ungrouped**. You will need to move it manually to your specific group.* (See [Managing Groups](#))

Troubleshooting:

- “Python” is required for all RHEL8 endpoints. If you experience DAU scan issues please confirm you have Python installed and updated.

- “bc” may also be required on some Linux endpoints and may cause the installer to fail. To correct this install bc.
yum install bc

- “nc” may also be required on some Linux endpoints and may cause the installer to fail. To correct this install nc.
yum install nc

Managing Groups

Create a Group:

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

Name	Display Name	IP Address	Agent Status	Operating System	Agent Version	PR Installed
SYS-IESAPP	SYS-IESAPP	10.7.8.2	Online	Microsoft Windows Server 2019 Standard x64	8.5.0.40	Yes
WIN2019TKEITH	WIN2019TKEITH	10.91.39.240	Online	Microsoft Windows Server 2019 Standard x64	8.5.0.40	Yes

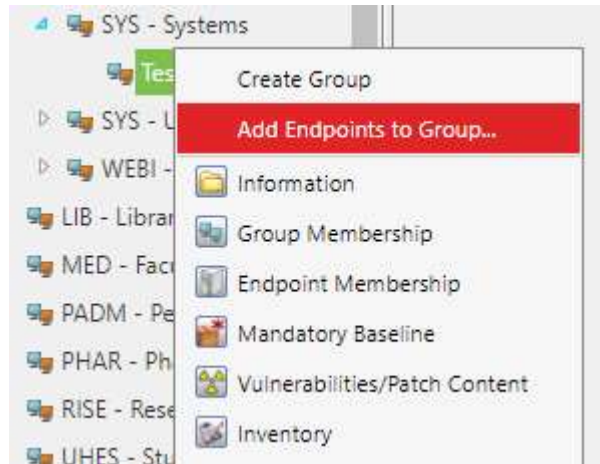
Name the group and click Save Icon:

Action	Name	Description	Distinguished Name	Endpoints
	Testing			

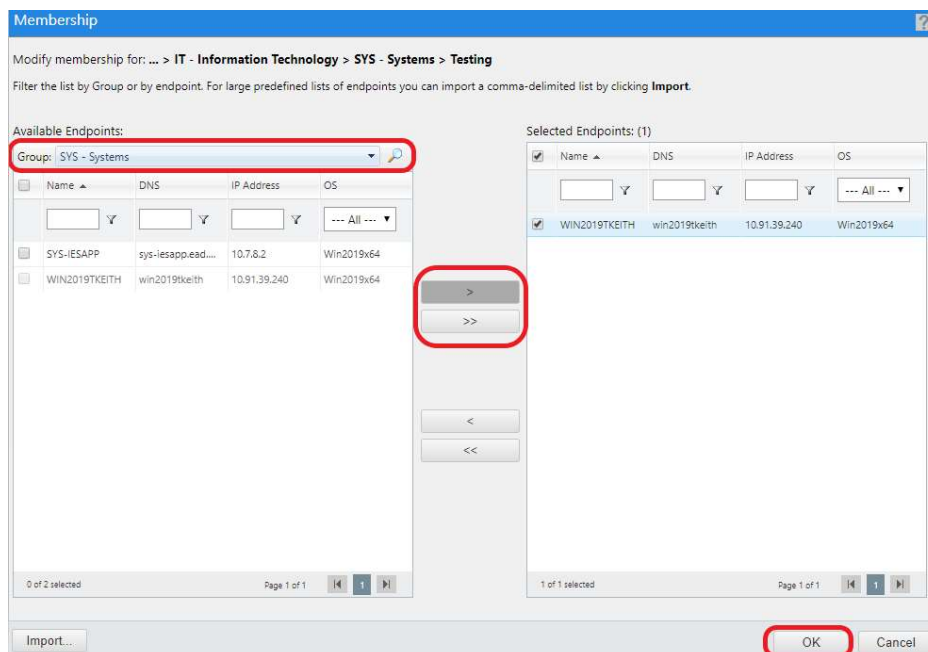
No results found.

Add/Remove Endpoints from a group

- Click on **Manage\Groups**.
- Right click on the group that you want to add an endpoint and select **"Add Endpoints to Group..."**.

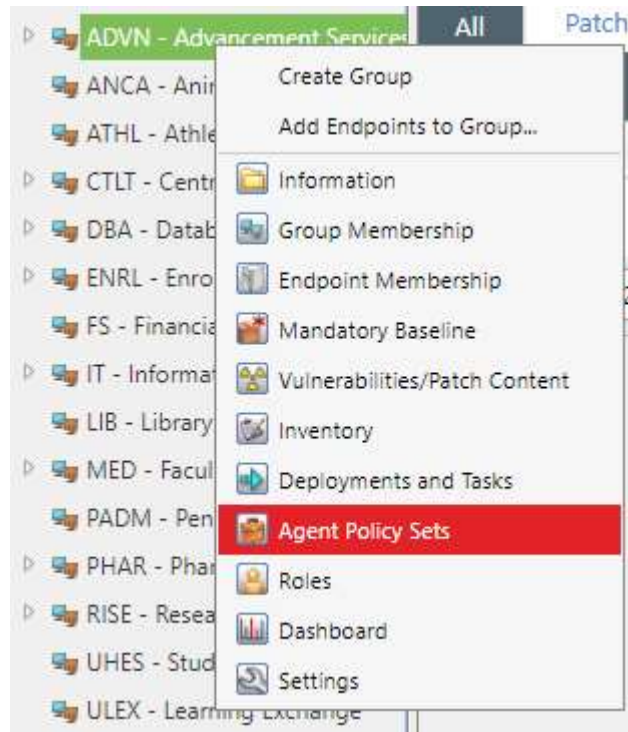


- Select your main group from the drop-down list and click on **Search**.
- Select the endpoints you wish to add to the group and hit the **arrow** to add.
- Click **OK**
- Follow this same procedure to remove an Endpoint from a group by using the arrow to move it out.



Assign Agent Policy to a group

- d. Click on **Manage\Groups**.
- e. Right click on the group that you want to add a policy and select **“Agent Policy Sets”**



- f. Click **Assign** and choose a Policy from the **drop down** list and click the **Save** icon



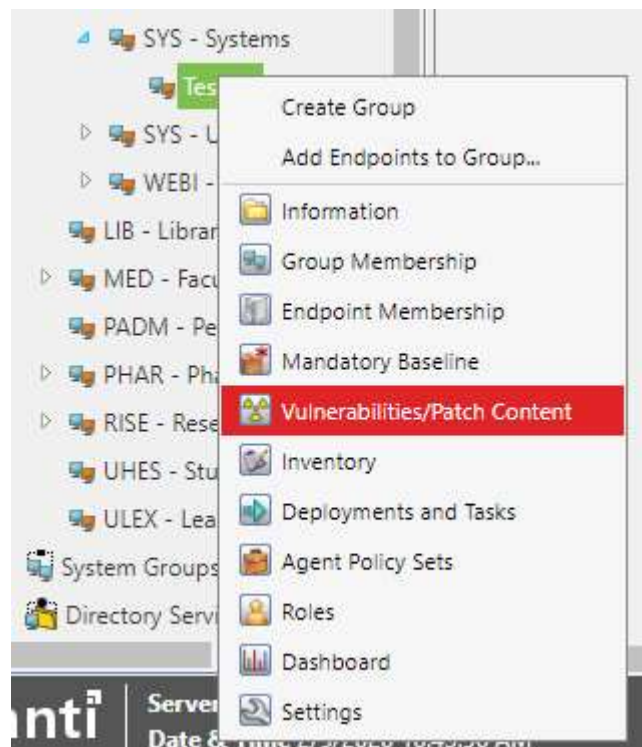
Note: Agent Policies applied to a group will apply to below sub-groups. If no policy is applied to a group or sub-group the Global Agent Policy is applied.

Schedule Patching

Patching can be scheduled by group or by individual endpoints. In this example we will show how to schedule patching by group.

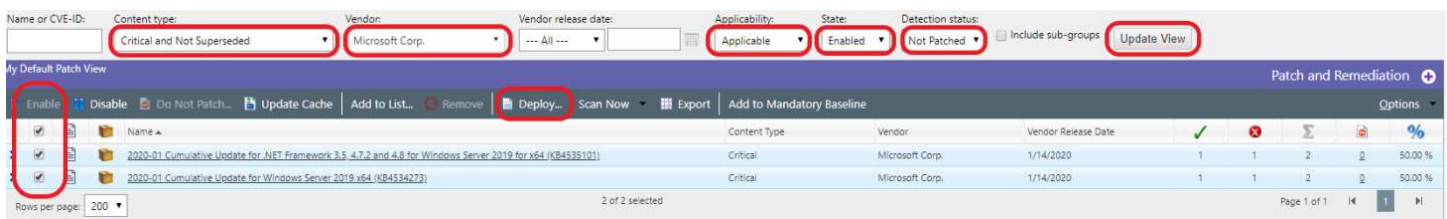
NOTE: Please note that at this time only OS patches should be deployed using IES. Third party application patches are available, but not supported by UBCIT at this time.

- a. Click **Manage, Groups**
- b. Right click on the appropriate group, and select **Vulnerabilities/Patch Content**.



While viewing the **Vulnerabilities/Patch Content** for your group, we **recommend** you select the following filters:

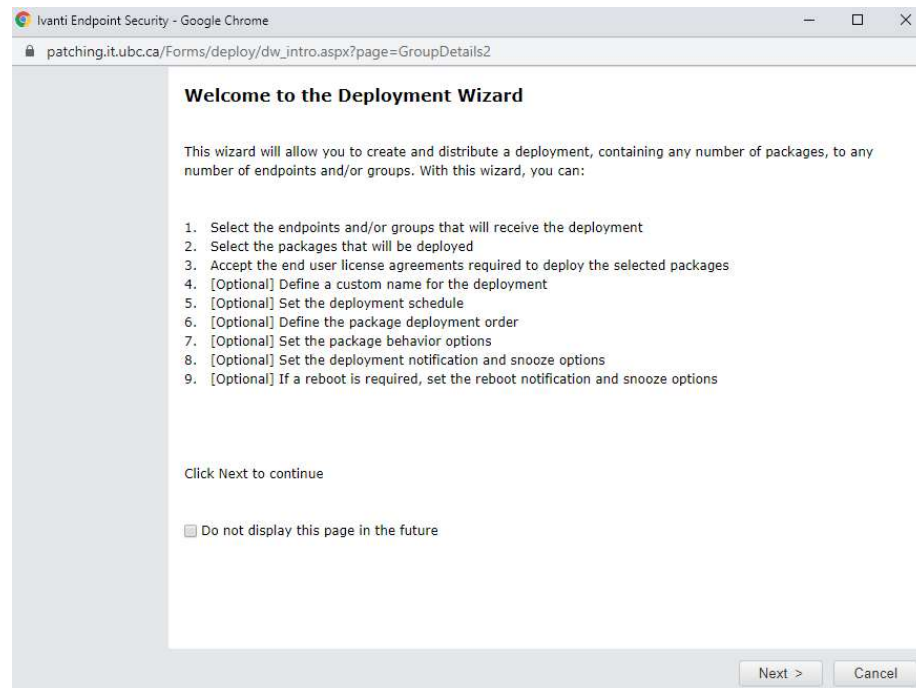
- c. Content Type: **Critical and Not Superseded**
- d. Vendor: **Microsoft Corp./Red Hat/Canonical Ltd. (Windows/Red Hat/Ubuntu)**
- e. Applicability: **Applicable**
- f. State: **Enabled**
- g. Detection Status: **Not Patched**
- h. Click **Update View** to refresh the list
- i. **Select** the patches you wish to deploy
- j. Click **Deploy...**



The screenshot shows the 'My Default Patch View' interface. At the top, there are filter dropdowns for 'Content type' (set to 'Critical and Not Superseded'), 'Vendor' (set to 'Microsoft Corp.'), 'Vendor release date' (set to 'All'), 'Applicability' (set to 'Applicable'), 'State' (set to 'Enabled'), and 'Detection status' (set to 'Not Patched'). There is also an 'Update View' button. Below the filters is a toolbar with buttons for 'Enable', 'Disable', 'Do Not Patch...', 'Update Cache', 'Add to List...', 'Remove', 'Deploy...', 'Scan Now', 'Export', and 'Add to Mandatory Baseline'. The 'Deploy...' button is highlighted. Below the toolbar is a table with columns: Name, Content Type, Vendor, Vendor Release Date, and a progress bar. Two patches are listed, both with a 50.00% progress bar. The 'Enable' checkbox in the toolbar is also highlighted.

Name	Content Type	Vendor	Vendor Release Date	Progress
2020-01 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4535101)	Critical	Microsoft Corp.	1/14/2020	50.00 %
2020-01 Cumulative Update for Windows Server 2019 x64 (KB4534273)	Critical	Microsoft Corp.	1/14/2020	50.00 %

- k. In the **Deployment Wizard** click **Next**.



The screenshot shows the 'Welcome to the Deployment Wizard' screen. The title is 'Welcome to the Deployment Wizard'. Below the title, there is a paragraph: 'This wizard will allow you to create and distribute a deployment, containing any number of packages, to any number of endpoints and/or groups. With this wizard, you can:'. Below this paragraph is a numbered list of 9 steps: 1. Select the endpoints and/or 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, there is a 'Click Next to continue' instruction and a checkbox labeled 'Do not display this page in the future'. At the bottom right, there are 'Next >' and 'Cancel' buttons.



- I. Now you can select the whole group or just specific endpoints within the group that you want to receive the deployment and click **Next**

Available Endpoints/Groups

Select the endpoints and/or groups you want to receive the deployment.
Items flagged as Do Not Patch or Not Applicable will be filtered out upon completion of this wizard.

Available Endpoints:

Endpoint OS Name	Total	Selected
Individual Win2019x64 Endpoints	2	1

<input type="checkbox"/>	Endpoint Name	Status	Platform Info	DNS Name	IP Address
<input type="checkbox"/>	SYS-IESAPP	Sleeping	Microsoft Wind...	sys-iesapp.ead...	10.7.8.2
<input checked="" type="checkbox"/>	SYS-IESSQL	Sleeping	Microsoft Wind...	sys-iessql.ead.u...	10.7.16.23

Available Groups:

- DSK - Desktop Services
- EIP - Enterprise Integration
- SA - Systems Architecture
 - Patch Management
 - HEMSS
 - IES
- SYS - Systems
- SYS - UBCO - OKIT
- WEBI - Web Infrastructure
- LIB - Library
- MED - Faculty of Medicine
- PADM - Pensions
- PHAR - Pharmacy

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

< Back Next > Cancel



- m. In **Available Packages** it shows the specific number of packages already "**Selected**" under **Microsoft Corp./Red Hat**. Just click **Next** to continue.
(If you click on Microsoft Corp./Red Hat it could list thousands of available packages so don't click here since you selected the packages earlier)

Available Packages

Select the packages you want to deploy.

Lumension	2	0
Martin Prikryl	1	0
Microsoft Corp.	476	2
Mozilla	1	0
Opera Software ASA	1	0
Oracle Corporation	3	0
RealVNC Ltd.	2	0

Select a vendor to display their available packages.

< Back Next > Cancel



- n. Click **I ACCEPT** to accept package EULA and click **Next**.

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



- o. Click **Change** button to change deployment time if required and click **Next** (If you click **Finish** instead it will use the Endpoints Policy Defaults)

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 - Windows 2019 Server [X]

Task name:* Deployment of Critical and not Superseded

Start time: Local Time: 2/5/2020 10:56:11 AM
UTC Time: 2/5/2020 6:56:11 PM Change...

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 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\theith.adm on 2/5/2020 10:56:11 AM (Local)

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

One time **On 2/10/2020 3:00:00 PM Local**
 Recurring

Date: Date: [X]

February 2020						
Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	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
1	2	3	4	5	6	7

12 hour 24 hour

Time: Time: [X]

Hour: Minute:



p. **Optional:** Edit **Package Deployment Order and Behavior** option

Package Deployment Order and Behavior

Set the deployment order and behavior for each individual package.

Action Order	Package Name	Selected Options	Reboot
1	2020-01 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4535101)(0001)(x64)(all)		
2	2020-01 Cumulative Update for Windows Server 2019 x64 (KB4534273)(0000)(x64)(all)		

Navigation icons: up, down, up, down

Package Deployment Behavior Options

Specify the deployment behavior options for the package.

Behavior	Description
<input type="checkbox"/> Uninstall	Uninstall the package.
<input type="checkbox"/> Force Shutdown	If the package causes a reboot, close all open applications.
<input type="checkbox"/> Do Not Backup	Do not backup files for package uninstall.
<input checked="" type="checkbox"/> Suppress Reboot	Do not reboot the device.
<input checked="" type="checkbox"/> Quiet Mode	Use quiet mode (no user interaction required).
<input type="checkbox"/> Unattended Setup	Perform an unattended setup.
<input type="checkbox"/> List Hot-Fixes	Generate a list of installed hot fixes.
<input type="checkbox"/> Force Reboot	Following the deployment, force the device to reboot.
<input checked="" type="checkbox"/> Reboot is Required	A reboot is required to complete the package installation.
<input checked="" type="checkbox"/> Chain Packages	Reduce reboots by chaining this package.
<input type="checkbox"/> Suppress Chained Reboot	Following the chained deployments, do not reboot the device.
<input type="checkbox"/> Repair File Permissions	Following the deployment, repair the file permissions.
<input type="checkbox"/> Download Only	Download only, do not install the package.
<input type="checkbox"/> Suppress Notification	Do not display user messages during installation.
<input type="checkbox"/> Debug Mode	Perform the installation using 'Debug' mode.
<input type="checkbox"/> Do Not Repair Permissions	Following the deployment, do not repair the file permissions.
<input type="checkbox"/> May Reboot	This package may require (force) a reboot.
<input type="checkbox"/> Multi-User Mode	Perform the installation using 'Multi-user' mode.
<input type="checkbox"/> Single-User Mode	Perform the installation using 'Single-user' mode.
<input type="checkbox"/> Restart Service	Following the deployment, restart the service.
<input type="checkbox"/> Do Not Restart Service	Following the deployment, do not restart the service.
<input type="checkbox"/> Reconfigure	Following the deployment, perform the system reconfigure task.
<input type="checkbox"/> Do Not Reconfigure	Following the deployment, do not perform the system reconfigure task.

Optional Flags:

Display:

<input checked="" type="radio"/> Behavior options settings	Do not reboot the device. Use quiet mode (no user interaction required). A reboot is required to complete the package installation. Reduce reboots by chaining this package. This installation requires a reboot in order to complete.
<input type="radio"/> Package description	

q. Once you have **reviewed and confirmed** packages for deployment click **Next**



- r. In the **Notification Options** select if you wish to notify users and, if **Yes**, set **Options** or choose notifications based on Agent policies by checking the **Use Policies** box and click **Next**

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 Ivanti Endpoint Security administrator.

820 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	No ▾	<input type="checkbox"/>

Deploy

Within 60 Mins ▾
 By 2/10/2020 1:00 PM

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 Ivanti Endpoint Security administrator.

794 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"/>

Reboot within 60 Mins ▾



- s. Review the **Deployment Confirmation** and click **Finish** to schedule/deploy packages.

Deployment Confirmation

Verify the deployment options and summary information

Job name:	Remediation - 2020-02-10 3:00:00 PM
Schedule:	One time deployment, starting on 2/10/2020 3:00:00 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:	2
Total selected endpoints/groups:	1
Notes:	IES SQL Patches

Selected Packages:

Order	Package Name	Selected Options	Reboot	Endpoints/Groups
1	2020-01 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4535101)(0001)(x64)(all)			1
2	2020-01 Cumulative Update for Windows Server 2019 x64 (KB4534273)(0000)(x64)(all)			1

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

- t. Click **Close** to close the window.
- u. You can monitor the progress by going to **Manage/Deployments and Tasks**

ivanti Endpoint Security powered by HEAT

Home Discover Review **Manage** Reports Tools Help

Manage > Deployments and Tasks

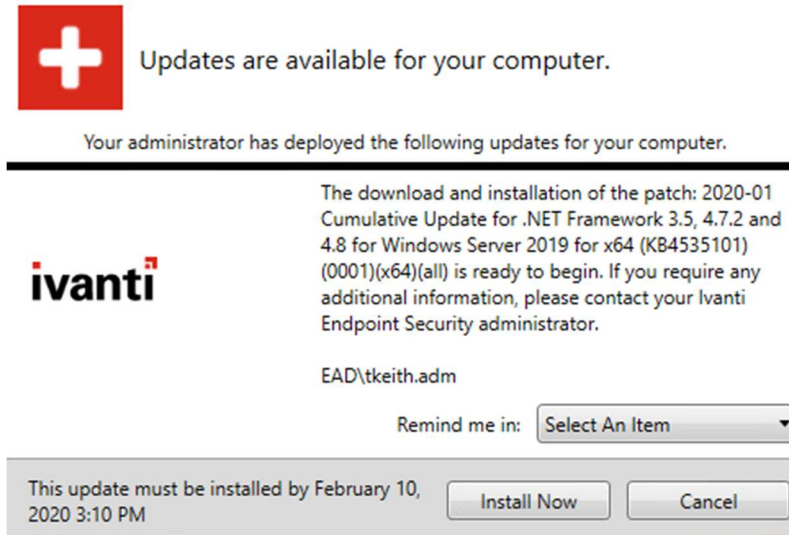
Status: --- All --- Type: --- All ---

- Endpoints
- Inventory
- Groups
- Custom Patch Lists
- Deployments and Tasks**
- Agent Policy Sets

Name	Type	Created Date
<input type="checkbox"/> Remediation - Windows 2019 Server	Package Deployment	2/5/2020 11:17:59 AM (Local)
<input type="checkbox"/> Reboot	System Task	12/11/2019 4:06:49 PM (Local)
<input type="checkbox"/> Discover Applicable Updates	System Task	12/11/2019 4:06:49 PM (Local)

Rows per page: 200 ▼ 0 of 3 selected

- v. If you are connected to the **Windows endpoint** you should see an update notification (if selected) like below during the update time:



Each update will have its own notification

- w. This will allow you to install now, snooze, or cancel the update depending on your agent policy.
- x. When all patches are completed the endpoint will reboot **or** ask for user response beforehand depending what was specified in your job settings or agent policy.





- y. If you are on a **Linux Endpoint** you can check the patch agent status by running:
(/usr/local/patchagent/)
./patchservice checknow

```
[root@rhel7tkeith patchagent]# ./patchservice checknow
Telling HEAT PatchLink Agent to query server for pending tasks ...
<AgentInfo><Version>8.3057</Version></AgentInfo>
[root@rhel7tkeith patchagent]#
Message from root@rhel7tkeith.systems.it.ubc.ca on <no tty> at 12:20 ...
-----
DEPLOYMENT DETAILS: The download and installation of the patch:
binutils-2.27-41.base.el7_7.2.x86_64 is ready to begin. If you
require any additional information, please contact your Ivanti
Endpoint Security administrator.
ISSUED BY: EAD\tkeith.adm
*****
YOUR SYSTEM ADMINISTRATOR REQUIRES THAT THIS PATCH BE INSTALLED
ON THIS SYSTEM BY: 02/19/2020 12:25:40
*****
-----
EOF
```



LINUX Patching options:

If you wish to install **ALL** updates for a specific Linux system:

1. Change the Vendor to “Lumension”

A screenshot of a web interface showing a dropdown menu labeled 'Vendor:'. The dropdown is open, and 'Lumension' is selected and displayed in the input field.

2. Type “Apply all” in the “Name or CVE-ID” search box and click “Update View”

A screenshot of a web interface showing a search box labeled 'Name or CVE-ID:'. The search box contains the text 'Apply all'. To the right of the search box is a button labeled 'Update View'.

3. Choose the apply all package for the OS you wish to deploy to:
 - a. Apply all applicable packages from local repositories according to yum (Red Hat)
 - b. Apply all applicable packages from local repositories according to apt-get (Ubuntu)
4. OPTIONAL: If you find the linux systems do not reboot after applying packages, and you wish to have your server always restart afterwards, you can add a reboot task after the packages to ensure the system reboots after applying all selected packages.
 - a. Using the same steps above search for “reboot” and click “Update View”
 - b. Add the “Task - Reboot System” package to your deployment