Patch Management

Ivanti Endpoint Security (IES formerly HEMMS) 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 6-8, Ubuntu 14-18.

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\<username.adm>) on the Endpoint you wish to add to Ivanti.

b. Download the agent from the IES console, click on Tools/Download Agent Installer... select OS and click Download.
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:

```
$ 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](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 in 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”

![Manage Modules](image)

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).

![Update View](image)
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”

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

Supported versions:
Red Hat Enterprise Linux: 6.x/7.x/8.x
Ubuntu Linux: 14/16/18

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”

![Image showing the Manage Modules option]

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

---

Remove Linux Endpoint

a. Run the EMSS agent uninstaller on the endpoint:

```
#/usr/local/patchagent/uninstall
```

b. Delete the patchagent directory:

```
# rm -rf /usr/local/patchagent
```

c. 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.

---

11/5/2020
- 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)
   lmsetupx64.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)
   lmsetupx64.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
  ```

11/5/2020
Managing Groups

Create a Group:

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

Name the group and click Save Icon:
Add/Remove Endpoints from a group

a. Click on Manage\Groups.
b. Right click on the group that you want to add an endpoint and select “Add Endpoints to Group…”.
c. Select your main group from the drop-down list and click on Search.
d. Select the endpoints you wish to add to the group and hit the arrow to add.
e. Click OK
f. 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...

k. In the Deployment Wizard click Next.
Now you can select the whole group or just specific endpoints within the group that you want to receive the deployment and click **Next**.
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)
n. Click **I ACCEPT** to accept package EULA and click **Next**.
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)
## Package Deployment Order and Behavior

Set the deployment order and behavior for each individual package.

<table>
<thead>
<tr>
<th>Action Order</th>
<th>Package Name</th>
<th>Selected Options</th>
<th>Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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)</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>2</td>
<td>2020-01 Cumulative Update for Windows Server 2019 x64 (KB4534273) (0000)(x64)(all)</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
</tbody>
</table>
### Package Deployment Behavior Options

Specify the deployment behavior options for the package.

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

#### Display:

- **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.**

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

![Deployment Confirmation](image)

**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:**

<table>
<thead>
<tr>
<th>Order</th>
<th>Package Name</th>
<th>Selected Options</th>
<th>Reboot</th>
<th>Endpoints/Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2020-01 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2012 for x64 (KB4535101)(0001)(x64)(all)</td>
<td>$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2020-01 Cumulative Update for Windows Server 2012 x64 (KB45242737/0001)(x64)(all)</td>
<td>$</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

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

![Endpoint Security](image)
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 DETAIL5: 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

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

POF
**LINUX Patching options:**

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

1. Change the Vendor to “Lumension”
   
   ![Vendor Input Field]

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

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