Ivanti Endpoint Security 8.6 Update 2

Release Notes

Release Notes

We are pleased to announce the release of Ivanti Endpoint Security (IES) 8.6 Update 2 (8.6.0.30). Read these notes to find out what we've changed and what we've fixed.

IMPORTANT: If you are using Antivirus or Application Control modules, pay special attention to the highlighted updates below.

End of Life Notice

Note that Ivanti Endpoint Security 8.5 Update 2 and earlier versions are now in self-support. Any customers on 8.5 Update 2 or earlier versions should upgrade now to a supported release.

Product Updates

ATTENTION NEEDED: AntiVirus SDK updated to resolve a compatibility issue with Windows 10 21H2

We have updated the Antivirus module to resolve an incompatibility issue between Windows 10 21H2 and Bitdefender SDKs. There is an incompatibility between Windows 10 version 21H2 and Bitdefender's Antirootkit SDK that forms part of the Ivanti Endpoint Security Antivirus module. The incompatibility surfaced as a result of changes introduced in Windows 10 21H2 and occurs for new Windows 10 21H2 installs, or once a machine running the AntiVirus module updates to Windows 10 21H2, and its manifestation consists of one of the following:

- Black screen post-reboot with impossibility of logging-in.
  Issue occurs on 64b systems (32b systems not affected);
- Blue screen of death (BSOD) for Antirootkit SDK components (trufos.*) delivered before 2018.
  Issue occurs on 32b systems (64b systems not affected);
- Hang on init and subsequent hang of the system for Antirookit SDK (trufos.*) components delivered in 2018 and after.
  Issue occurs on 32b systems (64b systems not affected);

This issue does not affect Windows 10 21H1 or previous Windows 10 versions. It does not affect upgrades to Windows 10 versions prior to Windows 10 21H2.

Important: If you are using the Ivanti Endpoint Security AntiVirus module, do not upgrade to Windows 10 21H2 until you have first upgraded your endpoints to Ivanti Endpoint Security 8.6 Update 2.

ATTENTION NEEDED: Upgrading IES 8.6 U1 Application Control endpoints which are in lockdown mode, and which also have Memory Protection enabled.

We have resolved an issue that was introduced on IES 8.6 U1 (8.6.0.10) associated with Application Control and Memory Protection. If an endpoint running on IES 8.6 U1 is locked down with Application Control and the Memory Protection feature is active, an attempt to uninstall another module (e.g. Patch module) from that endpoint will fail and the endpoint agent will get stuck in a restart state, requiring manual intervention.

This issue will also occur if an IES 8.6 U1 endpoint (which is locked down with Application Control and the Memory Protection feature is active) is upgraded to a later version (e.g. IES 8.6 U2). The issue occurs while unloading the memory protection module and occurs regardless of whether the Memory Protection feature is in Audit mode or in Enforcement mode.

If you have IES 8.6 U1 endpoints which are locked down with Application Control and the Memory Protection feature is active, take the following steps before upgrading to IES 8.6 U2 (or before attempting to uninstall another module):

- Disable any active Memory Protection policies in your environment
- Wait sufficient time until the endpoints have implemented the Memory Protection policy change
- Upgrade the endpoints to IES 8.6 U2
- Re-enable the Memory Protection Policies

This issue does not occur for endpoints running on IES versions prior to 8.6U1 and these can be upgraded as normal.

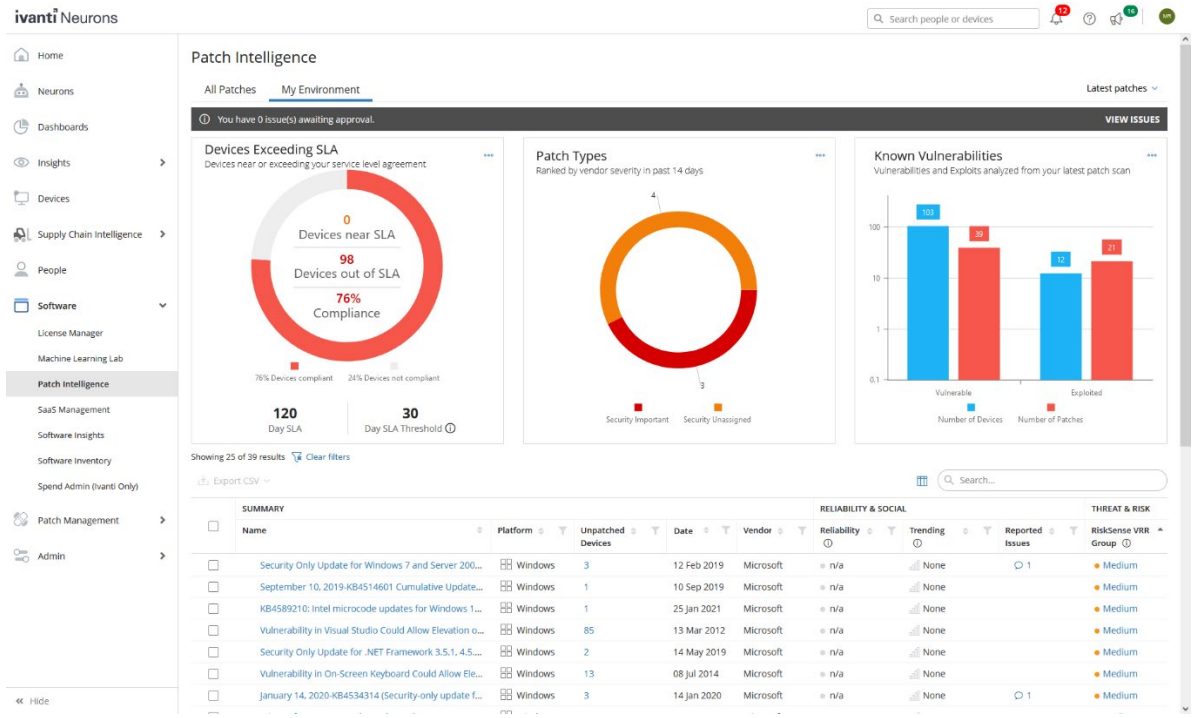
Ivanti Neurons for Patch Intelligence integration

Ivanti Neurons for Patch Intelligence delivers automated insight into your risk exposure by providing remediation prioritization based on adversarial risk. It helps you quickly understand which remediation actions to take first, with Vulnerability Risk Rating (VRR). Threat-context for vulnerabilities, via supervised and unsupervised machine-learning, provides the real-time intelligence on vulnerability exploits that are actively trending in the wild, and those that have ties to ransomware.

Ivanti Endpoint Security now integrates with Ivanti Neurons for Patch Intelligence to help you act faster against risk exposure and prioritize where to patch. What does this integration achieve? By connecting to Ivanti Neurons for Patch Intelligence, you can populate the endpoint and patch content information from Ivanti Endpoint Security into Ivanti Neurons and then you can leverage the risk context and threat insights that we have in Patch Intelligence to ensure that you are taking that risk-based, prioritized action for patch management. This integration enables you to see the vulnerability risk associated with your specific environment and help you understand where you need to focus your attention to reduce that risk.

You can use Patch Intelligence data to gain a deeper level of vulnerability insight with:

- **Risk-Based Prioritization**:
  Understand your adversarial risk with Vulnerability Risk Rating (VRR), threat-context for exploit and malware insights from RiskSense. RiskSense VRR is designed to decipher cybersecurity risk, using an algorithm that intelligently separates and elevates the highest risk weaknesses. It takes in the highest fidelity vulnerability and threat data, together with human validation of exploits from penetration testing. Insight into denial of service, privilege escalation, remote code execution, web application, ransomware, and exploit kit vulnerabilities support the risk-based prioritization of the greatest risks in your environment.
- **Patch Reliability**:
  Achieve faster SLAs for vulnerability remediation efforts, with patch reliability and trending insight to focus testing efforts and reduce time to patch. Reduce your research efforts with crowd-sourced insight from a variety of sources, including social media trending data, reported known issues from vendor, user, and Ivanti sources in one centralized view. The patch downvote gives a quick indicator of a negative experience.
- **Patch Compliance**:
  Use the SLA data to see how compliant the devices are within your environment to identify which devices and patches need prioritizing based on your specific SLA timescales and dates.



To learn more about Ivanti Neurons for Patch Intelligence and to request a 45-day trial, go to https://www.ivanti.com/products/ivanti-neurons-patch-intelligence. Take a look at our Setting up Ivanti Endpoint Security connector help page to understand what's involved with setting up a connector and what data is imported into Ivanti Neurons.

Support for additional browsers / Microsoft Silverlight removal

Microsoft Silverlight reached end of support on October 12th, 2021 and we have replaced this with a new solution, based on SignalR. In addition to updating the underlying technology to a supported platform, this change also means that you will no longer need to use Internet Explorer 11 to run Install Manager. You can now use your browser-of-choice to install new components. To avail of this change, simply upgrade to IES 8.6 U2. The necessary component changes will happen in the background as part of the upgrade.

SIEM integration (Device Control)

Many organizations use Security Information and Event Management (SIEM) platforms (e.g. Splunk, Rapid7, LogRhythm) to aggregate and analyze activity from many different solutions in their environment. To help you integrate with your SIEM of choice, we have developed a plug-in solution for Device Control events. This solution is an agent-side implementation in the IES 8.6U2 release (for Device Control events only) which enables you to forward events from IES DC agents directly to the SIEM solution.

The following KB article (https://forums.ivanti.com/s/article/Ivanti-Endpoint-Security-Device-Control-SIEM-Integration) provides sample code and further documentation to enable you to integrate with your SIEM solution.

OS Support Updates

Windows Server 2022 was released by Microsoft on September 1st and is supported on the 8.6 U2 release.

Windows 11 was released on October 5th and is supported for Patch & Remediation, Application Control and AntiVirus modules. Windows 11 is not yet supported for the Device Control module.

Note: If you have the Device Control module installed on endpoints, you should not upgrade these endpoints to Windows 11 at this time.

As noted earlier, there is a compatibility issue between Windows 10 21H2 and Bitdefender SDKs.

Note: If you have the AntiVirus module installed on endpoints, you should not upgrade these endpoints to Windows 10 21H2 until you have first upgraded your endpoints to Ivanti Endpoint Security 8.6 U2.

Bugs Fixed

The following customer support issues have been resolved in this release:

Problem ID	Title
86387	Unable to remove additional modules such as Patch and Remediation when AC module is installed, easy lockdown in in place and memory protection policies are in place.
78311	Im.detection fails to perform CBS detection on Windows 10 1809 with previous SSUs applied
77519	Internal Server error when accessing the AntiVirus section of the Manage > Endpoints view
75291	Installing IES agent on Microsoft Windows 10 Enterprise for Virtual Desktops fails with “OS Not Supported” message

How do I obtain 8.6 Update 2?

New Server Installs	Download the installer from the Ivanti Community Downloads page.
Existing Installs (Upgrades)	Within the Ivanti Endpoint Security console, replicate with the Global Subscription Service. Then download the 8.6 Update 2 components using Installation Manager.

How do I install the 8.6 Update 2 Server?

New Server Install	For new server installs, launch the installer you downloaded from the Ivanti Community.
Existing Server Upgrades	1. Open the Ivanti Endpoint Security console. 2. From the toolbar, select **Tools** > **Launch Installation Manager**. 3. Upgrade the manager when prompted. 4. Select the ***New/Update Components*** tab. 5. Choose 8.6 Update 2 (8.6.0.30) and begin the upgrade.

How do I install the 8.6 Update 2 Agent?

New Agent Installs	1. Log on to your endpoint. 2. Open the Ivanti Endpoint Security console and select **Tools** > **Download Agent Installer**. 3. Select agent version 8.6.0.30 and run the installer.
Existing Agent Upgrades	**1.** Open the Ivanti Endpoint Security console and select **Manage > Endpoints** from the navigation menu. 2. Select endpoints to upgrade and click the **Agent Versions** button on the toolbar. 3. From the toolbar, select **Tools** > **Launch Installation Manager**. 4. Apply the most recent version of the agent to your endpoints and click OK.

How do I determine if my upgrade was successful?

Server	From the Ivanti Endpoint Security console, navigate to **Help** > **About**. Successful upgrades will display a **Server Suite Version** of 8.6.0.30.
Agent	From the Ivanti Endpoint Security console, navigate to **Manage** > **Endpoints**. Successful agent upgrades will display a version of 8.6.0.30.