ivanti

Endpoint Security

powered by HEAT

Release Notes

Version 8.5 Update 1

Release Notes

We're pleased to announce the release of Ivanti Endpoint Security 8.5 Update 1! Read these notes to find out what's new and what we've fixed.

Important Notice

Endpoints Using Red Hat Enterprise Linux Versions 5 and 6

DO NOT install a new or upgrade your existing EMSS Server to 8.5 if you have Red Hat 5.x and 6.x endpoints using the Red Hat Network Classic (RHN) subscription model.

EMSS 8.5 can't provide new patch content to these endpoints. You may continue to use earlier EMSS versions to patch them until Red Hat drops RHN subscriptions in July 2017.

Red Hat is replacing its Red Hat Network Classic (RHN) subscription model with a newer one, Red Hat Subscription Management (RHSM). This affects how HEAT EMSS handles patch content for Red Hat Enterprise Linux versions 5.x and 6.x.

You **MUST** migrate your Red Hat 5.x and 6.x endpoints from RHN to RHSM before using EMSS 8.5. For full details and migration instructions, see Knowledge Base Article #24419.

New Features

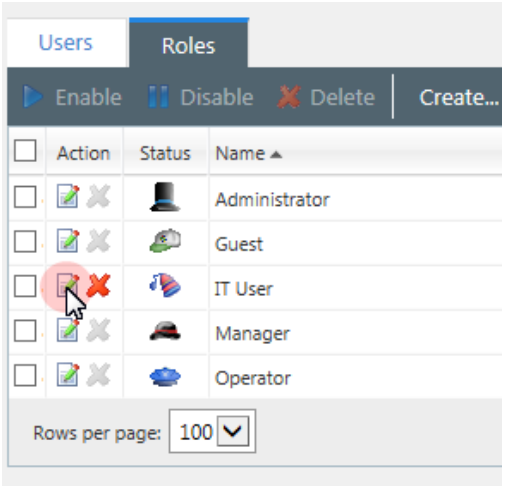
Brand Refresh

If you haven't already heard, HEAT Software has merged with LANdesk to form a brand-new company, **Ivanti**! We've renamed HEAT Endpoint Management Security Suite to Ivanti Endpoint Security. After upgrading to 8.5 Update 1, you'll see some updated branding within the product.

New "Manage System Tasks" Access Right

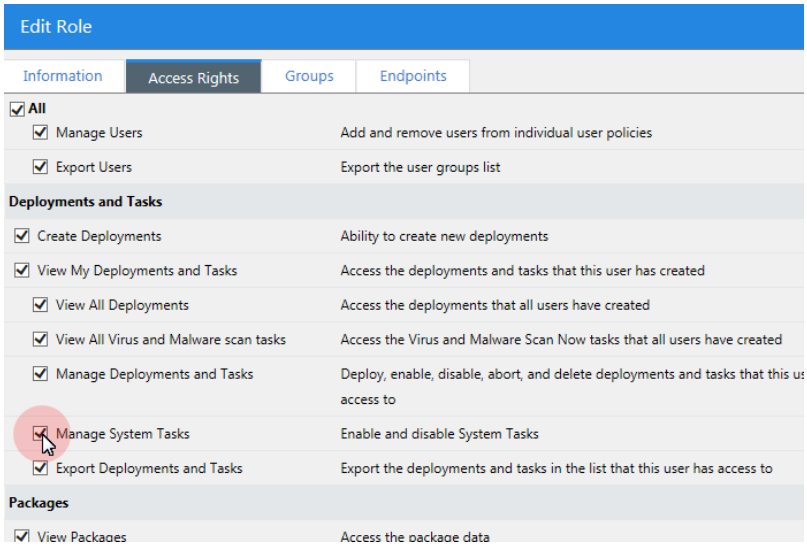
You can assign it to new roles you create and existing roles so users can enable and disable system tasks. It is enabled by default for Administrators only.

1. Select **Tools > Users and Roles**.
2. Select the **Roles** tab.
3. Find the role you want to assign the access right to and click **Edit Role**. You can't edit template roles, just ones you have created (those that are deletable on the list).



4. Select the **Access Rights** tab.

5. Scroll down to the **Deployments and Tasks** section and select **Manage System Tasks**.



Added Server Support for Microsoft Windows Server 2016 (Standard and Datacenter editions)

Essentials is not supported as it is a domain controller. An error message will display if you attempt to install on it.

Support for Universal Disk Format (UDF) Removable Devices

You are no longer bound to a 4GB file size portable encryption limit.

Migration to Cryptography Next Generation

This cryptography API is a replacement for the original Windows CryptoAPI. It allows for the use of newer, stronger encryption and signing algorithms when implementing cryptography.

Support for Encryption of pre-8.5 Update 1 Endpoints

When upgrading an agent to the latest version, you can still use password recovery on a USB stick that was encrypted with the old agent.

Publicly Available Help Online

You can now access the Ivanti Endpoint Security Help content (both PDFs and WebHelp) at https://help.ivanti.com. We encourage you to use the WebHelp as it's updated frequently, and new content is added on a regular basis.

Notices

End of Support for EMSS 8.0 Approaching

From 29 May 2017, Ivanti will no longer offer assistance for EMSS 8.0.

Resolved Issues

Core

ID	Description
249767	Fixed an issue where the HEAT EMSS Web console displayed Windows 10 LTSB 2015 even though 2016 was installed.
250386	Fixed an issue with the PolicyInfo.xml that caused agents to go offline periodically.
250770	Fixed an 8.2 to 8.5 upgrade failure issue that caused by the error "INSERT failed because the following SET options have incorrect settings".

Device Control

ID	Description
248290	Fixed an issue that caused Credential Guard process CPU usage to exceed 25% when Device Control was installed on Windows 10 Enterprise.
241291	Fixed an issue where users with pre-8.3 encrypted devices could not generate a valid passphrase while trying to recover a password.
241292	Fixed an issue that caused the Security code generated on the HEMSS Agent "Recover Password" screen to not match the Encrypted Medium ID.
249534	Fixed an issue where UDF-1.02 formatted CD/DVD discs were not being authorised as part of a Media Collection.
249765	Fixed an issue that was blocking Device Control drivers from installing and starting on Windows 10 v1607 (Anniversary update) with secure boot enabled.
250104	Fixed an issue that caused the Temporary Offline Permissions unlock code to not be accepted on an endpoint.
251823	Fixed an issue that caused the Surface Book wireless device to not switch between online and offline states properly.

Application Control

ID	Description
248162	Fixed an issue where certain apps that make use of .NET 2.0 had performance issues or failed to operate correctly on endpoints with EMSS Application Control installed and no Easy Lockdown//Easy Auditor policy applied.

ID	Description
248372	Fixed an issue where users were unable to Trust a file from an Application Log Query or the Application Library due to a server communication error.
250080	Fixed an issue that was causing the authorization of files from an AC query to a policy to take up to 8 minutes.
249165	Fixed an issue where the AC module did not operate properly on endpoints running Windows 10 LSTB with UEFI Secure boot enabled.
250959	Fixed an issue that caused the the Trusted Updater system process (PID 4) to generate large amounts of tracked packages and slowed endpoint performance.
251159	Fixed an issue where certain files were added to the Application Control whitelist despite being marked as infected with malware by AntiVirus.

Patch and Remediation

ID	Description
248797	Fixed an issue that caused an Internal Server error and timeout when exporting from the Deployments and Tasks page.
248798	Fixed an issue that intermittently caused endpoint information to not appear on the first pane of the Deployment Wizard.
249867	Fixed performance issues related to very large Mandatory Baselines (2000+ bulletins, 3000+ endpoints). They caused the Mandatory Baseline list to load very slowly (5+ minutes) or not display at all (data exception).
249928	Fixed an issue that prevented users from filtering the Vulnerabilities page because the Vendor Release Date was not being accepted.
250236	Fixed an issue where Windows Defender patches did not show as applicable for 8.5 endpoints.
250944	Fixed an issue that caused User Role assignments to not be considered when clicking Deploy on Manage > Endpoints > PR Tab.
250753	Fixed an issue where enabling a previously disabled vulnerability was not possible and caused a timeout error.
251225	Fixed an issue that caused patch content replication to fail after several minutes.

Known Issues

Ivanti Endpoint Security contains some known issues.

Description
Encryption pop-ups do not appear on agents running Windows 10 version 1607 (Anniversary edition). **Workaround**: Right-click on the device and select Decrypt Medium.
Upgrading an endpoint's operating system to a major version (for example, Windows 8 to Windows 10, and even Windows 10 to Windows 10 Anniversary Update 1607) may fail if the endpoint is in Application Control Easy Lockdown mode. **Workaround**: Disable Application Control Easy Lockdown before upgrade and re-enable after.
AntiVirus scans may behave unexpectedly on removable devices in cases where an endpoint has both Device Control and AntiVirus installed and Device Control is configured so only specific users can read/write removable media.. For example, if Real-time monitoring is enabled for attached media, this configuration will lead to failure in deleting or quarantining an infected file. The infection will still be detected and it will be reported, the infection will also be cleaned if cleanable, but the AV component will not be able to remove the file. **Workaround**: Add read/write permissions for the localsystem user account in the Device Control policy.
Non-ASCII characters cannot be used in an Application Scan Temporary file extraction location path on English language endpoints. A Warning () icon is displayed and you will be prevented from starting the scan.
Some types of archive files cannot be targeted by Application Scans.
It is not possible to close the Application Scan window while a scan is in progress. **Workaround**: End the process tree for `AppControlAuthorizationWizard.exe` in Windows Task Manager.
When an empty folder is targeted as an Application Scan source the scan will complete with an error.
When the Installation Manager prompts for an update prior to installing components, clicking the **Existing Components** tab will display an error. **Workaround**: Close and re-open your browser. Open the Installation Manager and click **Install** on the **New/Update Components** tab. This updates the Installation Manager.

Description
While upgrading modules using Installation Manager, a message may display stating that a module is not available as part of the upgrade. **Workaround**: Clear your browser's cache, relaunch your browser and attempt the upgrade again.
While upgrading Endpoint Security using Installation Manager, it fails with the following error: "Error occured while executing installer script: MigrateAVRecurringScanPolicies at step load reconfigured @value value Incorrect syntax near '...'" **Cause**: There is an apostrophe in one of your AntiVirus exclusions. This apostrophe causes an error during the upgrade. **Workaround**: Temporarily remove any exclusions that contain an apostrophe, and then re-add them following successful upgrade. Navigate to **Manage > AntiVirus** in Endpoint Security Console, and edit any policies that have an apostrophe in the exclusion path. The most common exclusion that contains an apostrophe is for Malwarebytes' products. If you have a Malwarebytes' exclusion in your environment, remove the following exclusions: • C:\Program Files (x86)\Malwarebytes' Managed Client\ • C:\Program Files (x86)\Malwarebytes' Anti-Malware\ For more information about this issue, refer to Knowledge Base Article 22511 at Ivanti Self-Service Portal .