

Ivanti Endpoint Security 8.6

Release Notes

Release Notes

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

End of Life Notice

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


Multi-factor authentication for the Endpoint Security Console

In the current security environment with cybercriminal attacks becoming smarter and more difficult to prevent, traditional authentication methods using username and password have become less secure. This is mainly due to techniques such as account takeovers and brute force attacks.

Multi-factor authentication is now considered to be one of the most effective ways to provide authentication security. Ivanti Endpoint Security 8.6 introduces multi-factor authentication for accessing the Console. This optional feature is disabled by default, but it can be enabled by the administrator. If your business requires, the feature can also run in PCI compliance mode.

Multi-factor authentication works with authenticators provided by Google and Microsoft.



Authentication		EnterCode
<p>Please provide credentials for website access</p> <p>Login name <input type="text" value="Administrator"/></p> <p>Password <input type="password" value="....."/></p> <p><input type="button" value="Next"/></p>	 <p>Hello Administrator, please add an authenticator by scanning the QR code below with your authenticator app on your phone.</p> <p>...or alternatively write the text below in your authenticator:</p> <p>MDXWVEZJWBERD4CIGFJTESKJJBFEUZZDPJKT5R0LJBXQGM0H9K5ZA</p>	<p>Please enter the code to sign in.</p> <p><input type="text"/></p> <p><input type="button" value="Login"/> <input type="button" value="Cancel"/></p>

For more information on setting up and using this feature refer [to this article](#)

CVE Import

The Common Vulnerabilities and Exposures (CVE) List is a public reference of known cybersecurity vulnerabilities. This list, maintained by the MITRE Corporation, continually changes as new vulnerabilities are detected. If your organization uses the CVE list, it can be difficult to determine exactly which patches you need to deploy to protect your machines from the threats identified in the list.

Many organizations utilize separate vulnerability analysis tools to detect vulnerabilities in their environment. In most cases it is then the responsibility of the IT team to remediate those vulnerabilities and it can be a time-consuming exercise to determine which patches you need to deploy to protect your machines from the threats (CVEs) identified in the list.

With the new CVE import feature, you can import vulnerability lists into the product and automatically create patch lists that contain fixes for the imported CVEs. This is a tremendous time saver since it removes the manual overhead involved and eliminates potential errors.

CVE Import

Select a file with CVEs (CSV, TXT, or XML)

vulnerabilities list.csv x Remove

Process file

Select the name of the existing list or type the name of a new list to which you would like to add the selected content.

CVE Import

<input type="checkbox"/>	Bulletin Name	Content Type	Vendor	Release date	CVEs
<input type="checkbox"/>	Adobe APSB11-24 Acrobat 3D ...	Critical - 01	Adobe Systems, Inc	13/09/2011	CVE-2011-1353, CVE-2011-24...
<input type="checkbox"/>	Adobe APSB10-06 Flash Player...	Critical - 01	Adobe Systems, Inc	11/02/2010	CVE-2009-3794, CVE-2009-37...
<input type="checkbox"/>	MS09-004 Security Update for ...	Critical - 05	Microsoft Corp.	10/02/2009	CVE-2008-5416
<input type="checkbox"/>	Adobe APSB13-15 Reader X 10...	Critical - 05	Adobe Systems, Inc	14/05/2013	CVE-2013-2549, CVE-2013-25...
<input type="checkbox"/>	MS15-118 Security Update for ...	Critical - 01	Microsoft Corp.	10/11/2015	CVE-2015-6096, CVE-2015-60...
<input type="checkbox"/>	MS15-124 Cumulative Security...	Critical - 05	Microsoft Corp.	08/12/2015	CVE-2015-6083, CVE-2015-61...
<input type="checkbox"/>	Adobe APSB11-17 Shockwave ...	Critical - 05	Adobe Systems, Inc	14/06/2011	CVE-2011-0317, CVE-2011-03...
<input type="checkbox"/>	MS15-119 Security Update for ...	Critical - 01	Microsoft Corp.	10/11/2015	CVE-2015-2478
<input type="checkbox"/>	MS15-018 Cumulative Security...	Critical - 05	Microsoft Corp.	10/03/2015	CVE-2015-0032, CVE-2015-00...
<input type="checkbox"/>	MS15-132 Security Update for ...	Critical - 05	Microsoft Corp.	08/12/2015	CVE-2015-6128, CVE-2015-61...
<input type="checkbox"/>	Apple iTunes 11.1.2 for Windo...	Critical - 05	Apple	22/10/2013	CVE-2011-3102, CVE-2012-08...
<input type="checkbox"/>	Adobe APSB12-08 Acrobat Pro...	Critical - 01	Adobe Systems, Inc	10/04/2012	CVE-2012-0774, CVE-2012-07...

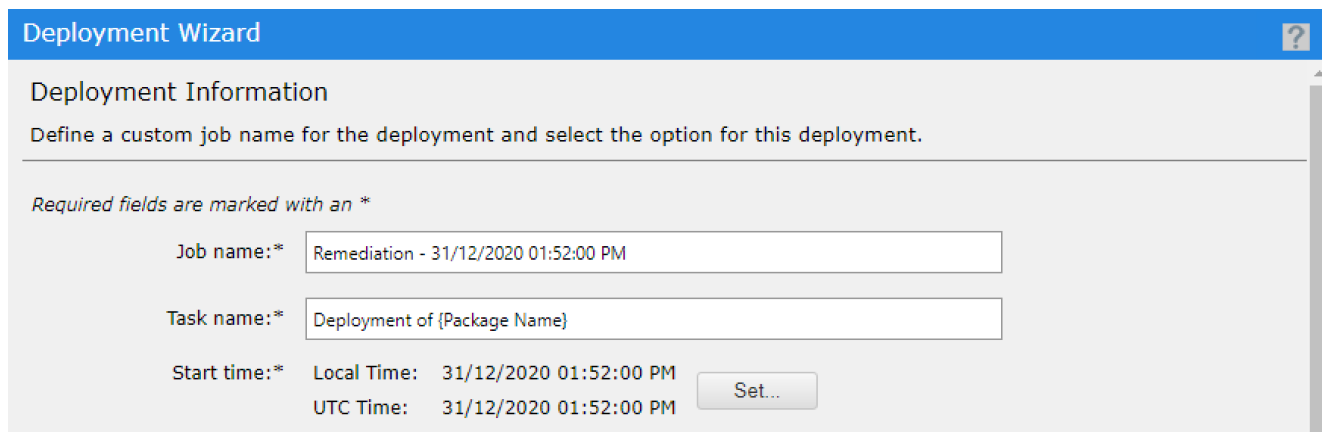
Import

Cancel

Deployment wizard enhancements

We've received a number of enhancement requests for the patch deployment wizard through our Ideas Portal (<https://forums.ivanti.com/s/product-enhancement-requests>) and we have included several of these in the 8.6 release. The deployment wizard is a tool that patch administrators use frequently and the associated enhancements are designed to improve usability and reduce errors.

- **Default option on Licenses screen changed to I ACCEPT** – On the Licenses screen, the **I ACCEPT** option will be selected by default when going through the deployment wizard. Previously, the default setting was **I DO NOT ACCEPT**, forcing the user to change the option before they could click **Next**.
- **Default Job Name updated to deployment start time** – On the Deployment Information screen, we update the default Job Name to use the deployment start date and time as soon as the user has selected it. People using the default Job Names can more easily determine when deployments are going to occur. As always, users can update the job name to another name of their choosing.
- **Default deployment start time** – On the Deployment Information screen the deployment start time will no longer be populated automatically using the current time. Instead the user is required to select the deployment time. This should help avoid situations where users accidentally trigger deployments to occur immediately after clicking **Finish** on the wizard.



- **Number of affected endpoints** – On the deployment confirmation screen, the **Total selected endpoints/groups** have been updated to better highlight the groups and endpoints that may be affected by the deployment. This can be used as a sanity check that you have selected the correct groups and help avoid pushing the updates to more than the desired number of targets. Numbers shown are a confirmation of the number of endpoints and groups that have been selected for the deployment. This is not the same as the number of endpoints or groups for which the deployment is

applicable, as this calculation is only performed when the deployment executes.

Deployment Wizard

Deployment Confirmation
Verify the deployment options and summary information

Job name:	Remediation - 02/12/2020 01:19:00 PM
Schedule:	One time deployment, starting on 02/12/2020 13:19:00 based on Agent Local Time.
Manner:	Concurrent: Deploying to 500 endpoints at a time.
Deployment notification:	Users will not be notified of the deployment.
Reboot Notification:	Notify and allow users to snooze the impending reboot.
Total selected packages:	402
Total selected endpoints/groups:	2 / 0
Notes:	Created by test\catalina.baboschi on 02/12/2020 13:19:59 (Local)

Rest API – Update endpoint Display Name

Ivanti Endpoint Security 8.6 continues to improve and facilitate the integration with 3rd party orchestration/automation tools. With this update we've added the option to change the endpoint Display Name using REST API methods. This will provide better visibility and identification of the assets.

The endpoint Display Name is an alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. This may include what system it belongs to, where it is located, and what it is used for. The Display Name field defaults to providing the same information as the endpoint Name field.

Additional OS Changes

Microsoft no longer supports Windows Servers on x86 architecture. While Endpoint Security does not prevent the solution from being installed on 32-bit servers, we will not release any fixes for any issues encountered on these servers.

Bugs Fixed

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

Problem ID	Title
74834	Add SQL Server 2019 Support to installer for IES
74527	Possible memory leak from EPS.SYS
74963	During the encryption wizard > add user > add windows user > unable to add domain groups
759534	Additional web.config hardening to prevent potential unauthorized access to storage folder

Bugs Fixed from Ivanti Device and Application Control

The following customer support issues have been addressed in the version of the Ivanti Device and Application Control agent which is used in Ivanti Endpoint Security 8.6:

Problem ID	Title
73362	When DC module is installed, devices like eSIM, SmartCard Readers, build-in GPS devices stop working

How do I obtain 8.6?

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 components using Installation Manager.

How do I install the 8.6 Server?

New Server Install	For new server installs, launch the installer you downloaded from the Ivanti Community.
Existing Server Upgrades	<ol style="list-style-type: none"> 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 (8.6.0.10) and begin the upgrade.

How do I install the 8.6 Agent?

New Agent Installs	<ol style="list-style-type: none"> 1. Log on to your endpoint. 2. Open the Ivanti Endpoint Security console and select Tools > Download Agent Installer. 3. Select agent version 8.6.0.10 and run the installer.
Existing Agent Upgrades	<ol style="list-style-type: none"> 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 8.6.0.10.
Agent	From the Ivanti Endpoint Security console, navigate to Manage > Endpoints . Successful agent upgrades will display a version of 8.6.0.10.