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 3 and earlier versions are now in self-support. Any customers on 8.5 Update 3 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.

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.
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](image)

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:

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

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:

<table>
<thead>
<tr>
<th>Problem ID</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>73362</td>
<td>When DC module is installed, devices like eSIM, SmartCard Readers, build-in GPS devices stop working</td>
</tr>
</tbody>
</table>
# How do I obtain 8.6?

<table>
<thead>
<tr>
<th>New Server Installs</th>
<th>Download the installer from the <a href="#">Ivanti Community Downloads page</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Installs (Upgrades)</td>
<td>Within the Ivanti Endpoint Security console, replicate with the Global Subscription Service. Then download the 8.6 components using Installation Manager.</td>
</tr>
</tbody>
</table>

# How do I install the 8.6 Server?

<table>
<thead>
<tr>
<th>New Server Install</th>
<th>For new server installs, launch the installer you downloaded from the Ivanti Community.</th>
</tr>
</thead>
</table>
| 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 (8.6.0.10) and begin the upgrade. |

# How do I install the 8.6 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 8.6.0.10 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 InstallationManager**.  
4. Apply the most recent version of the agent to your endpoints and click OK. |

# How do I determine if my upgrade was successful?

<table>
<thead>
<tr>
<th>Server</th>
<th>From the Ivanti Endpoint Security console, navigate to <strong>Help &gt; About</strong>. Successful upgrades will display a <strong>Server Suite Version</strong> of 8.6.0.10.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>From the Ivanti Endpoint Security console, navigate to <strong>Manage &gt; Endpoints</strong>. Successful agent upgrades will display a version of 8.6.0.10.</td>
</tr>
</tbody>
</table>