Welcome to Ivanti® Endpoint Security for Endpoint Manager

Ivanti® Endpoint Security for Endpoint Manager provides the tools you need, in a single integrated console, to secure and protect all of the devices and critical data on your enterprise network.

Ivanti® Endpoint Security for Endpoint Manager supports heterogeneous network environments that include Windows, Macintosh, and Linux clients.

Endpoint Security for Endpoint Manager is based on the primary Ivanti® Endpoint Manager functionality that lets you configure and manage network devices, and then enhances and focuses that functionality by adding specific security-related tools like Patch and Compliance, Antivirus, Endpoint Security, Application Control, Ivanti Firewall, Device Control, Agent Watcher, Data Protection, and more; offering a comprehensive and layered security solution.

Comprehensive and layered security solution

Ivanti® Endpoint Security for Endpoint Manager is a complete security management solution that lets you proactively *monitor, evaluate, remediate, verify, defend, and fortify* your network infrastructure and resources.

The fundamental Patch and Compliance tool enables you to scan for and remediate the most prevalent types of security exposures and risks that continually threaten the health and performance of your managed devices, including: known operating system and application vulnerabilities, spyware, viruses, system configuration errors, unauthorized or prohibited applications, and other potential security exposures.

Ivanti Antivirus lets you download the latest virus definition file updates; and configure virus scans that check managed devices for viruses and provide the end user with options for handling infected and quarantined objects. Device Control allows you to monitor and restrict access to managed devices through network connections and I/O devices.

The table below shows how the Endpoint Security for Endpoint Manager tools complement each other and provide a strong, complete network defense:

	• Patch and compliance scan results • Antivirus activity and status information Alerts Reports
Patch management	Patch and Compliance Ivanti updates Driver updates Software updates
Vulnerability assessment and remediation (known industry-published definitions, custom security definitions)	Patch and Compliance Definition and patch file downloads Security scans Compliance scans Patch deployment and installation Autofix
Malware detection and repair	Antivirus • Ivanti Antivirus pattern file updates and scans • Third-party antivirus content updates Spyware scans Riskware scans Real-time scans Application blocker
Device configuration, zero-day attack protection, and lockdown	Endpoint Security

	• Location awareness (network connection control) • Application Control • Ivanti Firewall • Device Control • Trusted File Lists Security threats (system configuration exposures) Windows Firewall configuration Agent Watcher
Unmanaged device scan and discovery	Unmanaged Device Discovery Extended Device Discovery (ARP and WAP)

Once you've installed Ivanti® Endpoint Security for Endpoint Manager and activated your core server with a Endpoint Security for Endpoint Manager license, you can refer to specific help topics for information on starting the console and using the available tools, including the security-specific tools and features listed below.

Navigate the Ivanti® Endpoint Manager and Ivanti® Endpoint Security for Endpoint Manager help topics in the Ivanti Help Center or perform a search using a specific key word or phrase to find the information you want.

> IMPORTANT: **Endpoint Security for Endpoint Manager doesn't include all Endpoint Manager components**
> Keep in mind that some Endpoint Manager components do not apply to a Endpoint Security for Endpoint Manager implementation, such as OS provisioning and rollup cores.

Install and activate Ivanti® Endpoint Security for Endpoint Manager

Ivanti® Endpoint Security for Endpoint Manager and Ivanti® Endpoint Manager both use the same setup program to install the necessary components on your core server. As with other Ivanti software products, such as Endpoint Manager and Inventory Manager, it's when you actually activate the core server with your Ivanti account information that the applicable Endpoint Security for Endpoint Manager functionality is made available in the console.

If your account is licensed for Ivanti® Endpoint Security for Endpoint Manager, you'll see the tools and features described in the Ivanti® Endpoint Security for Endpoint Manager help topics when you log into the console.

Ivanti User Community resources

Installing and deploying enterprise applications like Ivanti systems and security solutions software to a heterogeneous network requires a deliberate methodology and significant planning before you run the setup program.

Because the network infrastructure and database scalability requirements and considerations are similar between Endpoint Manager and Endpoint Security for Endpoint Manager, and because these Ivanti products use the same setup program, you should refer to the *Installation and Deployment* BKM (best known method) documents located at the Ivanti Support User Community.

> NOTE: **The Ivanti User Community**
> The Ivanti User Community has user forums and best known methods for all Ivanti products and technologies. To access this valuable resource, go to: Ivanti User Community Home Page

The User Community hosts several useful documents that provide detailed information on deployment strategies and step-by-step instructions for each phase of your Ivanti software deployment, such as:

- Design your management domain
- Prepare your database
- Install or upgrade the Ivanti core server
- Understand port usage
- Configure managed device agents

Ivanti® Endpoint Security for Endpoint Manager content subscriptions

Ivanti® Endpoint Security for Endpoint Manager offers scanning and remediation support for several different types of security risks, including known OS and application vulnerabilities for supported device platforms, spyware, viruses, system configuration threats, unauthorized applications, and more. Each security risk, of any type, is characterized by definition files. A definition file is typically comprised of an ID, specific attributes, detection rule details, and patch file information if applicable.

Ivanti maintains a database of validated security definition files, referred to as Endpoint Security for Endpoint Manager content or security and patch content, that are continuously updated, verified, and made available via web download. In order to download security and patch content you must have an associated Endpoint Security for Endpoint Manager content subscription.

For information about Endpoint Security for Endpoint Manager content subscriptions, contact your Ivanti reseller, or visit the Ivanti website:

Ivanti Home Page

Download security updates from Ivanti

The Patch and Compliance section in the help describes how to download the security and patch content for which you have subscriptions. For more information, see Download security content.

Related topics

Endpoint Security for Endpoint Manager tools and features