Wake on LAN 8.5 Update 1

User Guide

ivanti

Endpoint Security

powered by HEAT

Notices

Version Information

Ivanti Endpoint Security: Wake on LAN User Guide - Ivanti Endpoint Security: Wake on LAN Version 8.5 Update 1 - Published: May 2017

Document Number: 02_207_8.5 Update 1_171281114

Copyright Information

Table of Contents

Chapter 1

Ivanti Wake on LAN Overview

In this chapter:

Ivanti Wake on LAN is a Ivanti Endpoint Security module you can use to power on endpoints within your network without physically turning them on. With this capability, daily management tasks are simplified, desktop and laptop energy consumption is reduced, and system management tasks that interfere with employee productivity are prevented.

Ivanti Wake on LAN (WOL) is a module you can install within Ivanti Endpoint Security. Use this module to control the power status of endpoints within the network (*on* or *off*), thereby managing tasks that occur at a specific time each day.

Using WOL, you can ensure swift deployment of critical security patches and ensure that every endpoint within the network is powered on during scheduled patch assessment. These functions are especially beneficial to organizations with networks containing thousands of endpoints. Using WOL, you can perform maintenance tasks for multiple endpoints after regular business hours, thus minimizing employee productivity disruption.

Note: Although WOL can wake endpoints from an off state, most network cards include security features to prevent remote boots. Therefore, Ivanti recommends using WOL to wake endpoints in a sleeping or hibernating state.

About Ivanti Wake on LAN

Ivanti Wake on LAN (WOL) is a Ivanti Endpoint Security module containing features you can use to power on network endpoints. To power on endpoints, Ivanti Wake on LAN sends specific Ivanti Wake on LAN network packets, called wake requests, to endpoints hosting the Ivanti Endpoint Security Agent.

Most network interface cards support a listening mode, enabling them to receive network packets even when the endpoints that host them are powered off, hibernating, or sleeping. You can use Ivanti Wake

on LAN to power on endpoints by sending network packets (known as *wake requests*) to endpoints hosting the Ivanti Endpoint Security Agent.

About Wake Requests

Wake Requests are network packets that Ivanti Wake on LAN sends to network endpoints. These packets contain code that wake recipient endpoints from a suspended, hibernating, or powered-off state.

Wake requests are sent from the Ivanti Endpoint Security to wakepoints. Wakepoints then relay the request to managed endpoints. For additional information about wakepoints, refer to About Wakepoints on page 65.

Wakepoints use *limited broadcast* to relay wake requests to agent-managed endpoints within their subnet. During limited broadcast, the wakepoint sends the wake request to the 255.255.255.255 IP address. By sending the wake request to this address, a wake request is sent to all endpoints within the subnet. When managed agents receive the wake request, their host endpoints are woken.

Wake requests send packets called *magic packets*. Magic packets include the broadcast address (255.255.255.255) and endpoint MAC addresses, which are discovered using the Ivanti Endpoint Security Agent. When managed endpoints receive this request, they are powered on after recognizing the broadcast address and their unique MAC address.

Major Features of Ivanti Wake on LAN

Ivanti Wake on LAN (WOL) features are beneficial to organizations of all sizes.

You can use WOL to power on endpoints for maintenance purposes. With WOL, you can maintain large networks containing thousands of endpoints or smaller networks where an administrator only manages a handful of endpoints.

WOL includes the following features:

- Wake Windows endpoints, regardless of operating system version.
- Schedule wake requests to power on endpoints.
- Immediately send wake requests using the *Wake Now* feature.

Advantages of Using Ivanti Wake on LAN

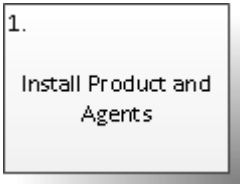
Ivanti Wake on LAN contains features that benefit administrators of networks of all sizes. With Ivanti Wake on LAN, you can power on endpoints at your convenience, and then complete various administration tasks.

The following list itemizes the benefits of using Ivanti Wake on LAN features:

- Enables administrators to complete administrative tasks following business hours using other Ivanti Endpoint Security modules.
- Because endpoint maintenance can be performed following business hours, employees can operate their endpoints without interruption during business hours.
- Because endpoints can be woken, employees can power off their endpoints following business hours, leading to reduced power consumption.
- Ivanti Wake on LAN improves the likelihood that mobile network devices and hardware (devices with unpredictable use patterns) are scanned and updated more frequently, returning them to a state of security policy compliance.
- Ivanti Wake on LAN automation features ensure administrators do not have to repetitively schedule wake times.
- Ivanti Wake on LAN requires minimum maintenance.

The Ivanti Wake on LAN Process

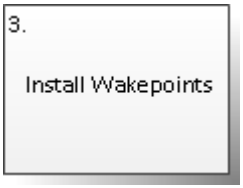
When getting started with Ivanti Wake on LAN, you should perform Ivanti Wake on LAN in a recommended sequence to use the product effectively.



Install Ivanti Endpoint Security on a server and Ivanti Endpoint Security Agent on network endpoints. Installing these products creates the infrastructure to wake network endpoints without being physically present at the endpoints.

Install the Ivanti Wake on LAN module (the Ivanti Wake on LAN module server component) on the Ivanti Endpoint Security server. During this process, all components needed to send network endpoint wake requests are installed.

Note: By default, the Ivanti Wake on LAN platform module is installed with Ivanti Endpoint Security. Therefore, installing the module manually is usually unnecessary.



Define wakepoints. During this step, the Wakepoint module (the Ivanti Wake on LAN module endpoint component) is installed on network endpoints hosting agents. Wakepoints are agents that relay server wake requests to other agents in the wakepoint's network segment (VLAN). Each network segment should contain at least one wakepoint. However, Ivanti recommends installing several wakepoints in each network segment in the event that a router blocks a wake request.

Schedule wake times. During this step, you define how Ivanti Wake on LAN schedules the time to send endpoint wake requests. You can schedule wake times using either agent policy set hours of operation or a custom wake time assigned to specific groups. After the wake time is scheduled, Ivanti Wake on LAN broadcasts wake requests at the scheduled time, and network endpoints are woken.

Note: You can only schedule wake times using agent hours of operation if the Patch and Remediation module is installed.

Chapter 2

Installing Ivanti Wake on LAN

In this chapter:

Successful installation of the Ivanti Endpoint Security Server and Agent components is vital to installing Ivanti Wake on LAN.

Ivanti Wake on LAN is a module within the Ivanti Endpoint Security (Ivanti Endpoint Security). Prior to installing the Ivanti Wake on LAN module, you must have a working Ivanti Endpoint Security network setup in place.

For information on how to install the Ivanti Endpoint Security Server, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .

To install the Ivanti Endpoint Security Agent on endpoints, refer to the Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .

Explaining Module Subcomponents

Ivanti Endpoint Security is a platform for *modules*, which are add-ons that protect your network using different methods. Each Ivanti Endpoint Security module is composed of two subcomponents: the server component and the endpoint component.

Server Component	This subcomponent is installed on the Ivanti Endpoint Security server. The server component must be installed before the endpoint component.

Endpoint Component	This subcomponent is installed on endpoints hosting a Ivanti Endpoint Security Agent. Endpoint components can be installed after the server component and agents are installed. Each installed endpoint subcomponent consumes an agent license for the applicable modules

Note: Ideally all endpoint agents should be the same version as the Ivanti Endpoint Security server.

New releases of the server support all currently supported versions of the endpoint agent. Older agent versions, however, are constrained to the features available when the agent was released and may not support new server functionality.

Minimum Hardware Requirements

To successfully install Ivanti Wake on LAN on the Ivanti Endpoint Security server, your computer must meet or exceed the specified hardware requirements.

To install the Ivanti Wake on LAN module, you must meet the following requirements:

- The server must meet all hardware and software requirements defined in the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .
- The target endpoints must be Windows-based and have Wake on LAN enabled within BIOS.

Supported Wakepoint Client Environments

The Ivanti Wake on LAN module endpoint component, known as the wakepoint, can be installed on any Windows endpoint hosting the Ivanti Endpoint SecurityAgent.

A *wakepoint* is an endpoint that receives wake requests from Ivanti Endpoint Security and relays it to other endpoints using the User Datagram Protocol (UDP) broadcast.

Refer to Defining Wakepoints on page 15 for more information on configuring Windows endpoints to act as wakepoints.

Note:

- By default, Ivanti Wake on LAN does not have any defined wakepoints. Wakepoints must be defined before you can begin using Ivanti Wake on LAN features.
- By default, Windows 8 endpoints (and later) are not configured to accept wake requests. To enable Ivanti Wake on LAN for Windows 8 endpoints (and later), you must disable the **Turn on fast startup** option. For additional information, refer to Disabling Fast Startup on page 85.

Logging In

Get started with Ivanti Endpoint Security by logging in.

You can access the console from any endpoint within your network.

Note: When accessing the Ivanti Endpoint Security console using a Web browser with high security settings enabled, the following message may display:

```
Scripting must be enabled to display this application properly.
```

In this event, Ivanti recommends adding the Ivanti Endpoint Security Web address as a trusted site in your browser settings to view the Web console.

1. Open your Web browser.
2. In your browser's address bar, type the Ivanti Endpoint Security URL (http[s]://*ServerURL*) and press ENTER.

   Tip: You can also use the server IP address.

   Step Result: A dialog prompting you for credentials opens.
3. Type your user name in the **User name** field.

   When logging in for the first time, type the user name of the Windows user account used to install Ivanti Endpoint Security. You can use additional user names after adding new user profiles to Ivanti Endpoint Security. If logging in using a domain account, type the name in the following format: `DOMAIN\Username`.
4. Type your password in the **Password** field.
5. Click **OK**.

Installing the Ivanti Wake on LAN Module Server Component

To begin using Ivanti Wake on LAN (WOL), you must first install the module server component on your Ivanti Endpoint Security (Ivanti Endpoint Security) server.

Install the Ivanti Wake on LAN platform component using the Ivanti Installation Manager. For additional information on using the Ivanti Installation Manager, refer to the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Notice: The Ivanti Wake on LAN module is considered part of the Ivanti Endpoint Security platform and is therefore listed as a platform component within Installation Manager.

1. Select **Tools** > **Launch Installation Manager**.

   Step Result: Installation Manager opens to the ***New/Update Components*** tab.

2. Select a **Suite Version** radio button.
   - If you are updating the entire suite, select the radio button for the latest **Suite Version**.
   - If you are only installing new modules, leave the current suite version selected.

   Tip: When you select a **Suite Version**, other suite versions their components are greyed out to prevent mixing.

3. Select the **Ivanti Wake on LAN** check box for your version of Ivanti Endpoint Security.
4. Click **Install**.

   Step Result: The ***Database backup recommended*** dialog opens.

   Note: During the module install, the installer will update your existing database(s). In the event of hardware failure or data corruption a database backup can ensure you still have functional data in order to restore database files. Refer to *Database Backup* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) for additional information.

5. Select **Next**.

   Step Result: The ***Ready to Install*** dialog opens.

   Tip: Click the **terms and conditions link** to view the company terms and conditions.

6. Click **Install**.

   The following table describes the steps for each dialog page.

Dialog	Step(s)
If the ***Prerequisites*** page opens:	Your server does not meet the recommended system requirements to install the selected content. • If you receive *failure(s)*, you must cancel the installation and resolve the failures before you can install the content. • If you receive *warning(s)*, you may proceed by clicking **Next**. Ivanti recommends resolving the warning(s) before proceeding. **Tip:** Click **Print** for a hard copy of prerequisite deficiencies. Click **Retry** to reassess the server.
If the ***Install/Update Components*** page opens:	Click **OK** to begin the component(s) installation. **Tip:** When the **Don't show this again** check box is selected it collapses the ***Install/Update Components*** dialog and this dialog will no longer be shown.

Dialog	Step(s)
If the ***Install Status*** page opens:	The installation of component(s) begins.

Step Result: The selected component(s) begin downloading and installing.

7. After installation completes, review the ***Confirmation*** page. Click **Finish** when you are done.

Tip:

- Click **View install log** to review the install log.
- Clear the **Launch** checkbox to cancel relaunch of the Web console.

8. Click **Finish**.

Step Result: The ***Confirmation*** page closes.

Result: The **Ivanti Wake on LAN** platform component is installed. To begin using the platform component, reopen Ivanti Endpoint Security.

After Completing This Task:
Complete Post Installation Tasks on page 18.

Uninstalling the Ivanti Wake on LAN Module Server Component

The Ivanti Wake on LAN module server component is listed as a platform component within Ivanti Installation Manager. Platform components cannot be uninstalled.

Tip: For additional information on using the Ivanti Installation Manager, refer to Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Defining Wakepoints

Before you can begin waking managed endpoints, you must define an agent-managed endpoint as a wakepoint within each network segment (VLAN). Wakepoints relay wake requests from the Ivanti Endpoint Security to other network endpoints. You cannot use Ivanti Wake on LAN (WOL) features within your network until you define wakepoints.

Prerequisites:

Ensure agents are installed on endpoints you want to define as wakepoints.

1. Select **Tools** > **Wake on LAN**.

Step Result: The ***Wake on LAN*** page opens to the ***WOL Configuration*** tab.

2. From **Wake Times** section, select how you will wake managed endpoints.
   Select one or both of the following options.

Option	Description
Wake endpoints using start times in Agent Policy Sets - Hours of Operation (HOP)	Wakes endpoints based on the hours of operation (HOP) setting defined in an agent policy set. Wake requests are sent when at the beginning of a HOP range. **Note:** This option is only available when the Patch and Remediation module is installed.
Wake endpoints using custom daily wake times defined for groups	Wakes endpoints in selected Ivanti Endpoint Security groups at a user-defined time.

Step Result: Ivanti Wake on LAN is enabled.

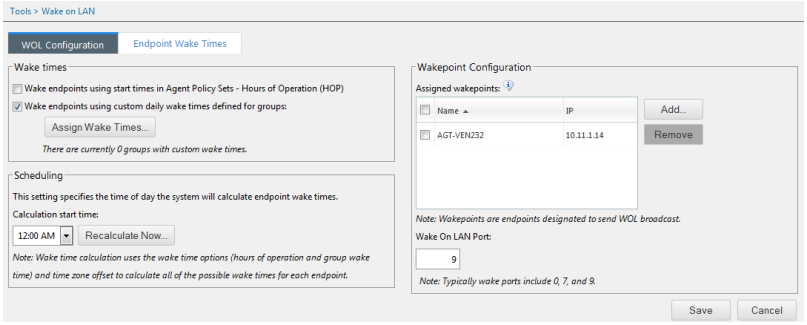


Figure 1: Ivanti Wake on LAN Page

3. From the **Wakepoint Configuration** section, add wakepoint(s).

   Wakepoints are managed endpoints with the Wakepoint module installed. Wakepoints relay wake requests from Ivanti Endpoint Security to managed endpoints within your network.

   a) Under assigned wakepoints click **Add**.

      Step Result: The ***Add Wakepoints*** dialog opens.

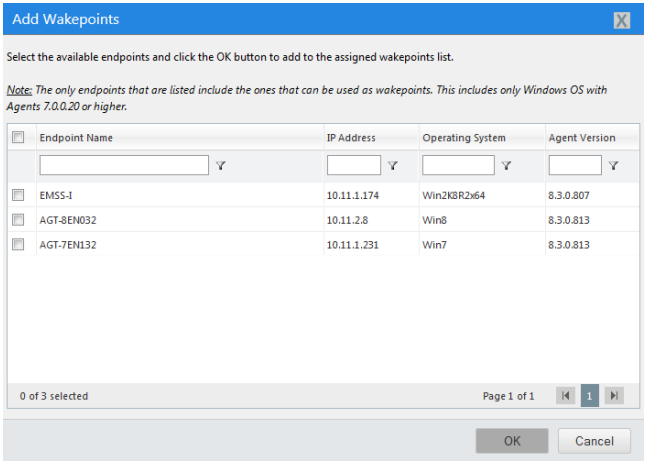


   Figure 2: Add Wakepoints Dialog

   b) Select the endpoints you want to install the wakepoint module on.

   c) Click **OK**.

      Step Result: The ***Add Wakepoints*** dialog closes.

4. Click **Save**.

   Step Result: The changes to your configuration are saved.

Result: Ivanti Endpoint Security configures your chosen endpoints to be wakepoints.

Post Installation Tasks

Following installation of the Ivanti Wake on LAN module server component and the defining wakepoints, you must perform select tasks before you can use Ivanti Wake on LAN features.

- Endpoints to be woken must have an agent installed, must successfully register with the Ivanti Endpoint Security server, and must successfully complete a Discover Applicable Updates (DAU) task. IP address and MAC address information collected during the DAU task are required by Ivanti Wake on LAN.
- Endpoints to be woken must have functional Ivanti Endpoint Security Server-to-Agent communication.
- Endpoints to be woken must have been booted at least once. Endpoints that have never been powered on cannot be woken using Ivanti Wake on LAN.
- Endpoints to be woken must currently be in a sleeping or hibernating state. Many NIC cards do not support waking endpoints from an off state for security reasons.
- Endpoints to be woken must have power still connected to the NIC card. Endpoints cannot be woken without a powered NIC card.

Important: Though the server components of Ivanti Wake on LAN can run on a virtual server, the endpoints to be woken must be physical endpoints. Virtual machines do not respond to Ivanti Wake on LAN requests.

Updating the Ivanti Wake on LAN Module

Periodically, Ivanti releases updates for Ivanti Wake on LAN. Install the latest release to keep Ivanti Wake on LAN up to date.

Ivanti recommends installing updates immediately. Update Ivanti Wake on LAN using the Ivanti Installation Manager.

1. Select **Tools** > **Launch Installation Manager**.

   Step Result: Ivanti Installation Manager opens to the ***New/Update Components*** tab.

2. Select a **Suite Version** radio button.

   - If you are updating the entire suite, select the radio button for the latest **Suite Version**.
   - If you are only installing new modules, leave the current suite version selected.

   Tip: When you select a **Suite Version**, other suite versions their components are greyed out to prevent mixing.

3. Select the Ivanti Wake on LAN check box for your version of Ivanti Endpoint Security.

   Note: This check box is only available if there is an update for the module.

4. Click **Install**.

   Step Result: The ***Database backup recommended*** dialog opens.

   Note: During the module install, the installer will update your existing database(s). In the event of hardware failure or data corruption a database backup can ensure you still have functional data in order to restore database files. Refer to *Database Backup* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) for additional information.

5. Select **Next**.

   Step Result: The ***Ready to Install*** dialog opens.

   Tip: Click the **terms and conditions link** to view the company terms and conditions.

6. Click **Install**.

   The following table describes the steps for each dialog page.

Dialog	Step(s)
If the ***Prerequisites*** page opens:	Your server does not meet the recommended system requirements to install the selected content. • If you receive *failure(s)*, you must cancel the installation and resolve the failures before you can install the content. • If you receive *warning(s)*, you may proceed by clicking **Next**. Ivanti recommends resolving the warning(s) before proceeding. **Tip:** Click **Print** for a hard copy of prerequisite deficiencies. Click **Retry** to reassess the server.
If the ***Install/Update Components*** page opens:	Click **OK** to begin the component(s) installation. **Tip:** When the **Don't show this again** check box is selected it collapses the ***Install/Update Components*** dialog and this dialog will no longer be shown.
If the ***Install Status*** page opens:	The installation of component(s) begins.

Step Result: The selected component(s) begin downloading and installing.

7. After installation completes, review the ***Confirmation*** page. Click **Finish** when you are done.

   Tip:

   - Click **View install log** to review the install log.
   - Clear the **Launch** checkbox to cancel relaunch of the Web console.

8. Click **Finish**.

   Step Result: The ***Confirmation*** page closes.

Result: The module is upgraded.

Chapter 3

Using the Ivanti Endpoint Security Console

In this chapter:

Within the Ivanti Endpoint Security console, you can use a number of common functions to navigate and operate the system. After you log in, Ivanti Endpoint Security opens to the ***Home Page***.

Ivanti Endpoint Security performs the following functions:

- Endpoint Detection
- Agent Installation
- Endpoint Management
- Endpoint Grouping
- Agent Policy Set Creation
- User and Role Creation and Management
- Server Module Management
- Report Generation

Ivanti Endpoint Security consists of a browser-based management console, which provides access to system management, configuration, reporting, and deployment options.

Common Functions

Ivanti Endpoint Security uses standard Web browser conventions and unique conventions. Familiarize yourself with these conventions to facilitate efficient product use.

From the **Navigation Menu** and system pages, you can access all features and functions you are authorized for.

Common Conventions

The Web console supports user interface conventions common to most Web applications.

Table 1: Common User Interface Conventions

Screen Feature	Function
Entry Fields	Depending on text, type data into these fields to either: • Retrieve matching criteria • Enter new information
Drop-Down Menus	Display a list of selectable values when clicked.
Command Buttons	Perform specific actions when clicked.
Check Boxes	A check box is selected or cleared to: • Enable or disable a feature • Initiate functions for list items Some lists include a **Select All** check box for selecting all items, including overflow items.
Radio Buttons	Select the button to select an item.
Sort	Data presented in tables can be sorted by clicking column headers. Columns can be sort in the following orders: • Ascending (default) • Descending
Mouseovers	Move your mouse over an item to display a text description.
Auto Refresh	Some pages feature an **Auto Refresh** check box. Select the check box to automatically refresh the page every 15 seconds.
Scrollbars	Drag scrollbars to see additional data.
Tabs	Select different tabs to display hidden information.
Bread Crumb	Displays the path to the page you are viewing. The breadcrumb lists: • The page you are viewing • Its parent page (if applicable) • The **Navigation Menu** item used to open the page If the breadcrumb contains a link, you can click it to retrace your steps.

Tip: Most pages support right-click.

The Navigation Menu

This menu appears on all Ivanti Endpoint Security pages. Use this menu to navigate through the console.

This menu organizes product features based on functionality. When you select a menu item, a new page, dialog, wizard, or window opens. You can access all system features from this menu (that your access rights authorize).

Note: The menu items available change based on modules you install.

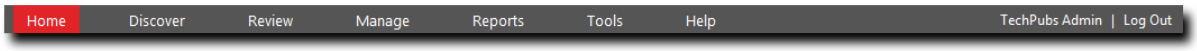


Figure 3: Navigation Menu

Table 2: Navigation Menus

Menu	Description
Home	Opens the ***Home*** page. This link contains no menu items.
Discover	Contains menu items related to running discovery scan jobs and virus and malware scans.
Review	Contains menu items related to reviewing security content, application event logs, virus and malware events, and discovery scan jobs.
Manage	Contains menu items related to managing system features.
Reports	Contains menu items related to creating reports.
Tools	Contains menu items related to system administration.
Help	Contains menu items related to help systems.

Mobile Device Management adds new **Navigation Menu** items.

Most navigation menus contain items. The following table lists each menu item in the **Discover** menu and the actions that occur when they are selected.

Table 3: Discover Menu Items

Menu Item	Description
Assets...	The ***Discover Assets*** dialog.
Assets and Install Agents...	The ***Install Agents*** dialog.
Assets and Uninstall Agents...	The ***Uninstall Agents*** dialog.

Menu Item	Description
Scan Now - Virus and Malware Scan	The ***Virus and Malware Scan*** dialog.

The following table lists each menu item in the **Review** menu and the actions that occur when they are selected.

Table 4: Review Menu Items

Menu Item	Description	
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.	
	Create Custom Patch List	The ***Create Custom Patch List*** dialog.
	Custom Patch List	The **Custom Patch Lists** sub-menu lists the last five custom patch lists that you have edited.
	All Lists	If you have created more than five custom patch lists, the navigation menu lists an **All Lists** item, which will open the ***Patch Content*** page with all custom patch lists displayed.
My Default View	The ***All Content*** page with your saved filters.	
Vulnerabilities	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show only critical vulnerabilities.
	Critical Vulnerabilities	The ***Patch Content*** page, filtered to show only critical vulnerabilities that are not superseded.
	New Vulnerabilities	The ***Patch Content*** page, filtered to show only critical but not superseded vulnerabilities released in the last 30 days.
	Top Vulnerabilities	The ***Patch Content*** page, filtered to show only critical but not superseded vulnerabilities sorted by the greatest number of applicable endpoints that are not patched.

Menu Item	Description	
Software	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show all software.
	Service Packs	The ***Patch Content*** page, filtered to show only service packs.
	Software Installers	The ***Patch Content*** page, filtered to show only software installers.
	Updates	The ***Patch Content*** page, filtered to show only software updates.
Other	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show all non-critical content.
	Detection Only	The ***Patch Content*** page, filtered to display **Detection Only** content.
	Informational	The ***Patch Content*** page, filtered to display only **Information** content.
	Packages	The ***Patch Content*** page, filtered to display only **Packages** content.
	Policies	The ***Patch Content*** page, filtered to display only **Policies** content.
	Recommended	The ***Patch Content*** page, filtered to display only **Recommended** content.
	System Management	The ***Patch Content*** page, filtered to display only **System Management** content.
	Tasks	The ***Patch Content*** page, filtered to display only **Task** content.
	Virus Removal	The ***Patch Content*** page, filtered to display only **Virus Removal** content.
Asset Discovery Job Results	Opens the ***Job Results*** page, which is filtered to display discovery job results.	
Agent Management Job Results	Opens the ***Job Results*** page, which is filtered to display Agent Management Job results.	

Menu Item	Description
Virus and Malware Event Alerts	Opens the ***Virus and Malware Event Alerts*** page.
Application Control Log Queries	Opens the ***Application Control Log Queries*** page, which allows users to create log queries that extract information on application activity.
Device Event Log Queries (Device Control only)	Opens the ***Device Event Log Queries*** page, which you can use to create, edit, or review device event log queries.

The following table lists each menu item in the **Manage** menu and the actions that occur when they are selected.

Table 5: Manage Menu Items

Menu Item	Description	
Endpoints	Opens the ***Endpoints*** page.	
Mobile Endpoints	Opens the ***Mobile Endpoints*** page.	
Inventory	Opens the ***Inventory*** page.	
Groups	Opens the ***Groups*** page.	
Users	Opens the ***Users*** page.	
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.	
	Create Custom Patch List	The ***Create Custom Patch List*** dialog.
	Custom Patch List	The **Custom Patch Lists** sub-menu lists the last five custom patch lists that you have edited.
	All Lists	If you have created more than five custom patch lists, the navigation menu lists an **All Lists** item, which will open the ***Patch Content*** page with all custom patch lists displayed.
Deployments and Tasks	Opens the ***Deployments and Tasks*** page.	
Agent Policy Sets	Opens the ***Agent Policy Sets*** page.	
Mobile Policies	Opens the ***Mobile Policies*** page.	
Antivirus Policies	Opens the ***Antivirus Policies*** page.	

Menu Item	Description	
Application Control Policies	Opens the ***Application Control Policies*** page, which contains the following tabs:	
	Managed Policies	Managed policies include Easy Auditor, Easy Lockdown, Denied Applications Policy, and Supplemental Easy Lockdown/ Auditor Policy. This tab is selected by default.
	Trusted Change	Trusted change policies include Trusted Publisher, Trusted Path, Trusted Updater, and Local Authorization.
	Memory Injection Policies	Memory Injection Policies.
Device Control: Policies (Device Control only)	Opens the ***Device Control Policies*** page, which you use to create, edit, or review Device Control policies.	
Policy Wizards	Opens a sub-menu. The sub-menu contains the following items:	
	Easy Auditor...	The ***Easy Auditor*** wizard.
	Easy Lockdown...	The ***Easy Lockdown*** wizard.
Application Library (Application Control only)	Opens the ***Application Library*** page, which lists the applications and files on your network endpoints.	
Device Library (Device Control only)	Opens the ***Device Library*** page, which lists all devices on your network endpoints.	

The following table lists each menu item in the **Reports** menu and the actions that occur when they are selected.

Table 6: Reports Menu Items

Menu Item	Description
All Reports	Opens the ***All Reports*** page.
AntiVirus	Opens the ***All Reports*** page with antivirus reports expanded.
Configuration	Opens the ***All Reports*** page with configuration reports expanded.
Deployments	Opens the ***All Reports*** page with deployments reports expanded.

Menu Item	Description
Device Control (Device Control only)	Opens the ***All Reports*** page with Device Control reports expanded.
Inventory	Opens the ***All Reports*** page with inventory reports expanded.
Management/Status	Opens the ***All Reports*** page with management/status reports expanded.
Policy and Compliance	Opens the ***All Reports*** page with policy and compliance reports expanded.
Power Management (Power Management only)	Opens the ***All Reports*** page with Power Management reports expanded.
Risks	Opens the ***All Reports*** page with risks reports expanded.
Vulnerabilities/Patch Content	Opens the ***All Reports*** page with vulnerabilities/patch content reports expanded.
Enhanced Reports	Opens a custom, user-defined URL. This URL is usually used to open a third-party reporting Web page.

The following table lists each menu item in the **Tools** menu and the actions that occur when they are selected.

Table 7: Tools Menu Items

Menu Item	Description
Users and Roles	Opens the ***Users and Roles*** page.
Change My Password...	Opens the ***Change My Password*** dialog.
Download Agent Installer...	Opens the ***Download Agent Installer*** dialog opens over the currently selected page.
Wake on LAN	Opens the ***Wake on LAN*** page.
Power Management (Power Management only)	Opens the ***Power Management*** page.
Directory Sync Schedule	Opens the ***Directory Sync Schedule*** page.

Menu Item	Description	
Device Control Device Control only)	Opens the **Device Control** submenu. The submenu includes the following items:	
	Recover Password	Opens the ***Recover Password*** dialog, which you can use to help network users recover forgotten passwords for encrypted devices.
	Grant Temporary Permissions	Opens the ***Grant Temporary Permissions*** dialog, which you can use to extend network users temporary access to certain network devices.
Launch Installation Manager...	Opens the ***Installation Manager*** in a new window.	
Subscription Updates	Opens the ***Subscription Updates*** page.	
Mobile Management Setup	Opens the ***Mobile Management Setup*** page.	
Mobile Endpoint Registration	Opens the ***Mobile Endpoint Registration*** dialog.	
Email Notifications	Opens the ***Email Notifications*** page.	
Options	Opens the ***Options*** page.	

The following table lists each menu item in the **Help** menu and the actions that occur when they are selected.

Table 8: Help Menu Items

Menu Item	Description
Help Topics...	Opens the ***Help*** page.
Knowledge Base...	Opens the Ivanti knowledge base.
New Users Start Here...	Opens the ***New Users Start Here*** page.
Technical Support	Opens the ***Technical Support*** page.
Product Licensing	Opens the ***Product Licensing*** page.

Menu Item	Description
About...	Opens the ***About*** dialog.

Note: Any unavailable or absent menus, menu items, or sub-menu items are due to restricted access rights or unavailable modules. Contact your network administrator if you require access to unavailable features.

The Page Banner

A page banner displays when the page is added for a new module. Use this banner to identify the module that the page belongs to.

Figure 4: Page Banner

For example, pages for Ivanti Patch and Remediation display a Patch and Remediation page banner. Page banners are color-coded by module.

List Pages

Most pages feature lists of selectable items. These items represent different product features that can be edited using menus and buttons.

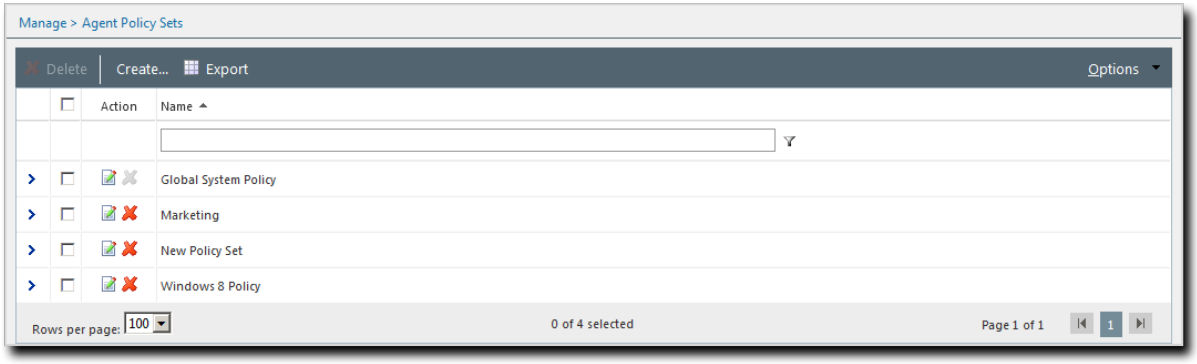


Figure 5: List Page

To select a single list item:

- Select a check box.
- Click a list row.

To select multiple list items:

- Select the **Select All** check box.
- Select multiple, concurrent items by using `SHIFT+Click` and mousing over list rows.

Toolbars

Toolbars appear on most Web console pages. They contain menus and buttons you can use to initiate page features.

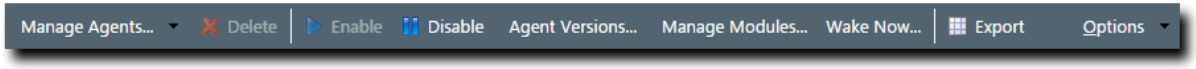


Figure 6: Toolbar

- The menus and buttons displayed vary according to page.
- Click the available menus and buttons to use them.
- User roles determine which buttons are available.

The Options Menu

Toolbars feature an **Options** menu. You can use these options to change how the page displays information.

Table 9: Options Menu Items

Option	Description
Show results on page load	Toggles automatic page results on and off. • When enabled, the page list automatically populates with results. • When disabled, you must define page filters and click **Update View** before results populate. For more information, see Filters on page 32.
Save as default view	Saves the current page settings as the default view.
Clear default view	Resets the saved view to the system default.
Show Filter Row[1]	Toggles the **Filter Row** on and off. For additional information, refer to Using Filter Rows on page 34
Show Group By Row[2]	Toggles the **Show Group By Row** on and off. For additional information, refer to Group By on page 36.
Enable Copy to Clipboard[3]	Toggles the ability to select text for clipboard copy.

1. This option title changes to **Hide Filter Row** when toggled.
2. This option title changes to **Hide Group By Row** when toggled.
3. Selecting this option disables other features, such as right-click context menus and list item dragging.

Filters

Filters appear on most list pages. You can use them to search pages for specific data.

Depending on which page you are viewing, you can filter pages using one of the following features. Only one feature appears per page.

- Filters
- Filter Row

Filters appear above page lists. They feature different fields, lists, and check boxes used for filtering. Filters vary according to page.

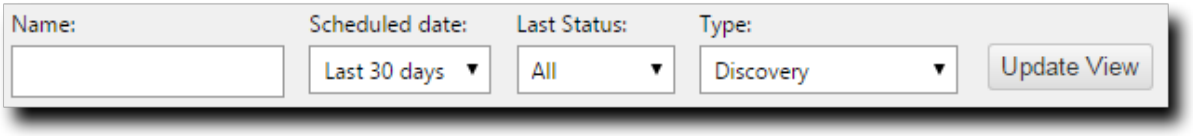


Figure 7: Filters

You can save frequently used filter settings as your default view. To save your settings, select **Options** > **Save as default view** from the toolbar. The toolbar **Options** menu contains the following options for filtering.

Table 10: Filter Options

Option	Function
Show results on page load	Automatically retrieves and displays results when selected.

Save as default view	Saves the active filter and sort criteria as the default view for the page.
	• The default view displays each time the page is accessed, including the following events:
	  • Browsing to a different page.
	  • Logging out of the Web console.
	• The default view is saved until you save a new one or you clear it.

Clear default view	Resets a saved default view to the system default view.

Filter Rows

Filter rows appear in the lists themselves. Rows feature a field for each column.

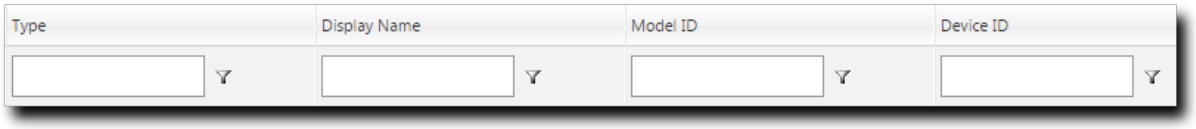


Figure 8: Filter Row

- Filters are not case sensitive.
- Columns can be filtered using a variety of data types. For example, you can use a **Contains** filter or a **StartsWith** filter.
- Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.

Supported Wildcards

When searching for or filtering vulnerabilities, you can use wildcards to make search results more specific and efficient.

Wildcards can be used anywhere within the search string. The following table lists the supported operators and wildcards in Ivanti Endpoint Security. Type any wildcards that you intend to use in the **Name or CVE-ID** field.

Table 11: Supported Wildcards

Wildcard	Description	Example
%	Any string. The string can be empty or contain any number of characters.	Typing `Microsoft%Server` in the **Name or CVE-ID** field returns any vulnerability with the words *Microsoft* and *Server* in any part of the name, such as: • MS12-043 Security Update for **Microsoft** Office SharePoint **Server** 2007 32-Bit Edition (KB2687497) • The 2007 **Microsoft** Office **Server**s Service Pack 3 (SP3), 32-bit Edition (KB2526299)
_ (underscore)	An underscore can be used as a Wildcard placeholder for any single character.	Typing `_itrix` or `Citri_` in the **Name or CVE-ID** field returns any vulnerabilities with *Citrix* in the name.
[ ]	Any single character within the brackets. You can also type a range ([a-f]) or set ([acegik]).	Typing `[m]ic` in the **Name or CVE-ID** field returns vulnerabilities with the string *mic* within the name (*Microsoft* and *Dynamic*). Typing `200[78]` in the **Name or CVE-ID** field returns vulnerabilities with 2007 or 2008 within the name.

Wildcard	Description	Example
[^]	Any single character **not** specified within the brackets. You can also type a range ([^a-f]) or set ([^acegik]).	Typing `M[^i]cro` in the **Name or CVE-ID** field returns results that: • Replace *i* with all remaining alphanumeric and symbolic characters (a, $, and so on). • Include all other characters remaining in the string (m, c, r, o). Results would include Macro, Mecro, M$cro, and so on. If a vulnerability contains Micro and a valid combination like Macro in its name (e.g. `MS99-999 Microsoft Word 2010 Vulnerability Could Enable Macros to Run Automatically`), it will be returned in the results.

Using Filters
When list pages are overpopulated with items, use filters to search for specific list items. Use this feature to filter list pages by criteria specific to the page.

Filters are available on most list pages.

1. Select a list page. For additional information, refer to List Pages on page 30.
2. Ensure filters are displayed.
   If filters are not displayed, click **Show Filters**.
3. Define filter criteria.

   Note: Available filters differ by page.

   - In filter fields, type the desired criteria.
   - From filter lists, select the desired list item.
4. If applicable, select the **Include sub-groups** check box.

   Note: This check box only appears on list pages related to groups.
5. Click **Update View**.

   Step Result: The list is filtered according to the filter criteria.
6. [Optional] Save the filter criteria by selecting **Options** > **Save as default view** from the toolbar.

Using Filter Rows
Some list pages use filter rows rather than filters. Use these rows, which are the first row of applicable lists, to filter column results. Filter column results to search for specific list items.

These rows appear on several list pages.

1. Select a page featuring the filter row.
2. Ensure the filter row is displayed.
   a) If the filter row is not displayed, select **Options** > **Show Filter Row** from the toolbar.
3. Type criteria in a filter row field.
4. Apply a filter type.
   a) Click the **Filter** icon.

      Step Result: A menu opens.

   b) Select a filter type.

      The following table describes each filter type.

      Table 12: Data Filtering Types

Type	Description
NoFilter	Removes previously applied filtering.
Contains	Returns results that contain the value applied to the filter.
DoesNotContain	Returns results that do not contain the value applied to the filter.
StartsWith	Returns results that start with the value applied to the filter.
EndsWith	Returns results that end with the value applied to the filter
EqualTo	Returns results equal to the value applied to the filter.
NotEqualTo	Returns results that are not equal to the value applied to the filter.
Greater Than	Returns results that are greater than the value applied to the filter.
Less Than	Returns results that are less than the value applied to the filter.
GreaterThanOrEqualTo	Returns results that are greater than or equal to the value applied to the filter.
LessThanOrEqualTo	Returns results that are less than or equal to the value applied to the filter.
Between	Returns results that are between two values. Place a space between the two values.
NotBetween	Returns results that are not between two values. Place a space between the values.
IsEmpty	Returns results that are empty.
NotIsEmpty	Returns results that are not empty.
IsNull	Returns results that have no value.

Type	Description
NotIsNull	Returns results that have a value.

Note:

- Filters are not case sensitive.
- Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.
- The availability of filtering options depends on the type of data displayed in the column. For example, filtering options that can only apply to numeric data are available in columns that contain text data.

Result: The list column is filtered according to the criteria. If desired, repeat the process to filter additional columns.

Using a Custom Date Range Filter

Use the Custom Date Range filter on Virus and Malware Event pages and tabs to display events that have occurred over a specific time period.

Prerequisites:

You must have launched the **Custom Date Range** dialog from the **Last Date Detected** filter field of a Virus and Malware Event page or tab.

1. Enter Start and End dates and times that cover the period you want to view alerts for, then click **OK**.

   Calendar and Time View popups can be opened to facilitate the entry of dates and times. Times that can be selected are provided in 30-minute intervals.

   Note: Your Start date should be less than 90 days from the current date, as event alerts raised outside that range are removed from view.

2. Click **Update View** to display the filtered results.

Result: The list is filtered according to the custom date range criteria you entered. Last Detected Dates are always displayed using server time.

Tip: As Malware and Virus Event alerts can be removed from view, the results list may not display all alerts that occurred within your custom date range. However, removed alerts are not deleted from the database and can therefore be viewed by generating an appropriate report.

Group By

The **Group By** row lets you sort list items into groups based on column headers. Use this feature to see which list items share similarities.

To use the **Group By** row, ensure **Options** > **Show Group By Row** is selected from the toolbar, and then drag a column header into the row. You may drag multiple columns to the row, but you may only drag one column into the row at a time.

To ungroup the list, right-click on the row and select **Cancel All Groupings**. To hide the **Group By** row, select **Options** > **Hide Group By Row**.

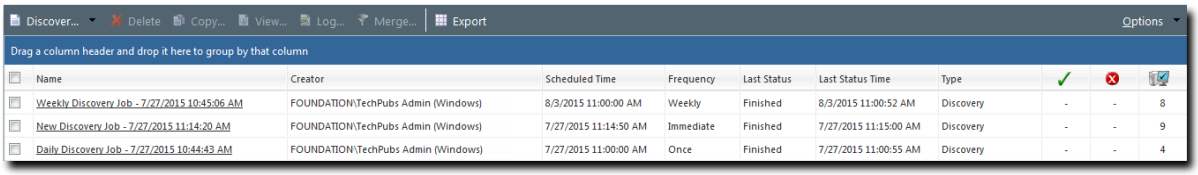


Figure 9: Group By Row

Expanding and Collapsing Structures

Certain structures in the Web console are expandable and collapsible. Expand structures to view additional information or options. Collapse them to conserve screen space.

Click available **Plus** icons (+), **Minus** icons (-), and **Rotating Chevron** icons (>) to expand or collapse a structure.

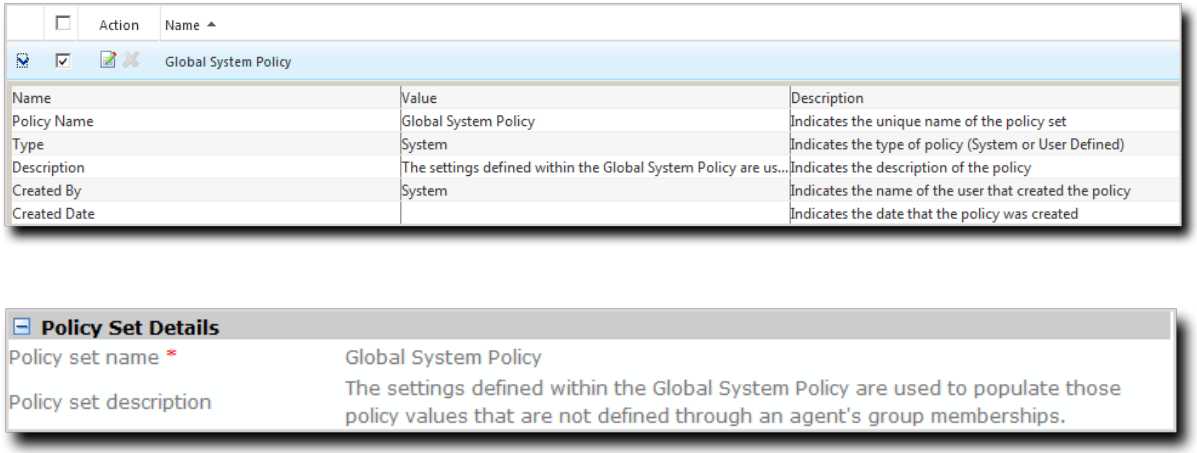


Figure 10: Expandable Structure Examples

Advancing Through Pages

When a list page contains an overflow of items, pagination links are created to manage the overflow. Click these links to advance through list items.

The number of list items and the page you are viewing determines the number of pagination links.

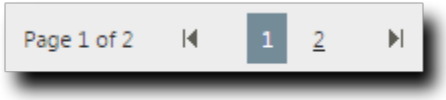


Figure 11: Pagination Feature

Table 13: Pagination Feature Functions

Icon or Link	Title	Function
	**Final Page Link**	Advances to the final page of list items.
	**First Page Link**	Returns to the first page of list items.
...	**Next Ten/Previous Ten Pages Link**	Displays the next ten or previous ten page links available. Fewer page links will display if the remaining list items cannot populate ten pages.
1 2 3 4 5	**Pagination Links**	Advances or returns to the selected pagination link.

Each page also features a **Rows Per Page Drop-Down List**. This list modifies the number of list items displayed on a single page (25, 50, 100, 200, 500).

Help

Ivanti Endpoint Security contains context-sensitive HTML help that includes feature explanations, step-by-step procedures, and reference materials.

Accessing Help differs according to context.

- From a page, select **Help** > **Help Topics**.
- From a dialog, click the **Question Mark** icon (**?**).

Use the following features to navigate through Help:

- From the ***Content*** tab, expand the bookmarks and click links to display Help topics.
- From the ***Search*** tab, type criteria in the **Keywords** field and click **Search** to display Help topics related to your search.

Exporting Data

On many system pages, you can export the listed data to a comma-separated value file (`.csv`) available for use outside of the Web console. Use this exported data for management purposes (reporting, noting trends, and so on).

You can export data from a variety of pages.

Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

1. Open a system page or dialog that you can export information from.
2. [Optional] Use the page filters to refine the items listed.
3. Click **Export**.

   Step Result: The ***File Download*** dialog opens.
4. Use the browser controls to complete the data export.

Result: The data is exported. All data results export, including data on overflow pages.

The Home Page

The entry point to Ivanti Endpoint Security is the ***Home Page***. From this page you can view the dashboard, which features drag-gable widgets that display information about Ivanti Endpoint Security and agent-managed endpoints.

Some widgets display general information about the system, others provide links to documentation, and still others summarize activity for Ivanti Endpoint Security modules you are licensed for.

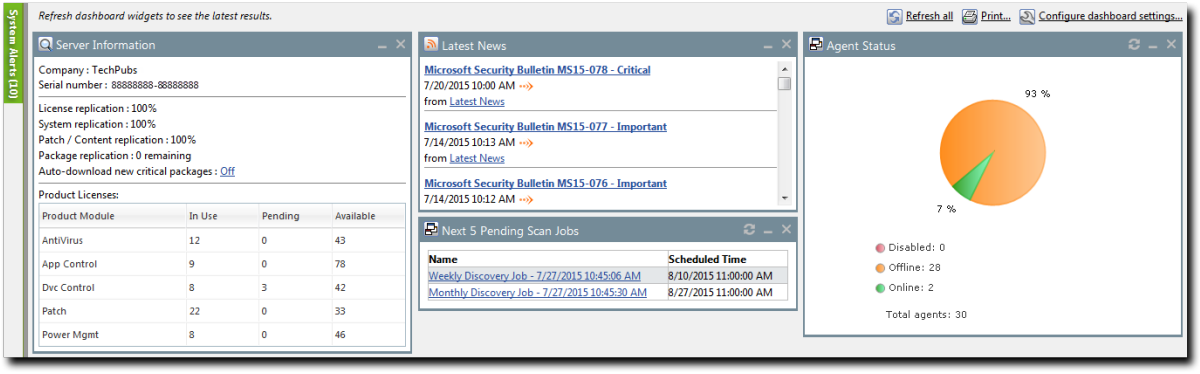


Figure 12: The Home Page

The Dashboard

The **dashboard** displays widgets depicting the activity on your protected network. Located on the ***Home*** page, the dashboard provides convenient information you can use to ensure your network protection is up to standard. Additionally, you can customize the dashboard to display the widgets most applicable to your network environment.

Widget graphs are generated based on the latest data and statistics available from endpoints, groups, module-specific data, and so on.

The following ***Dashboard*** widgets are available:

The Agent Module Installation Status Widget

This widget displays the installation and licensing stats of each agent module.

A graph bar displays for each installed module. The following table describes the widget graph.

Table 14: Graph Bar Color Descriptions

Bar Color	Description
Blue	The number of endpoints with the module pending install or uninstall.
Green	The number of endpoints with the module installed.
Red	The number of endpoints without the module installed.

Tip: Click the graph to open the ***Endpoints*** page.

Note: Endpoints with an agent version that does not support a module are not counted.

The Agent Status Widget

This widget displays all agents grouped by agent status.

Table 15: Agent Status Widget Fields

Field	Description
Online	The number of agents that are online.
Offline	The number of agents that are offline. **Tip:** Offline status is determined by the amount of time since the agent last communicated as determined on the ***Options*** page.
Disabled	The number of agents that are disabled.
Total Agents	The total number of agents in your environment.

Tip: Click the graph to open the ***Endpoints*** page. The page is filtered to display all agents.

The Applicable Content Updates Widget

This widget displays applicable content updates grouped by content type. View this widget when determining what content is applicable to endpoints in your network.

Table 16: Applicable Content Updates Widget Graph Bars

Bar	Description
Critical	The number of critical content items that are applicable to the your endpoints.

Bar	Description
Recommended	The number of recommended content items that are applicable to your endpoints.
Optional	The number of optional software, informational, and virus removal content items that are applicable to your endpoints.

Tip: Click the widget graph to open the ***Content*** page, which is filtered to display all applicable non-patched content.

Table 17: Applicable Content Updates Widget Fields

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.
Endpoints	The total number of endpoints with applicable updates.

Note:

- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.
- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Application Library File Assessment Widget

This widget displays a summary of the verification levels of the Application Library files that have been submitted to the Ivanti Endpoint Integrity Service for assessment.

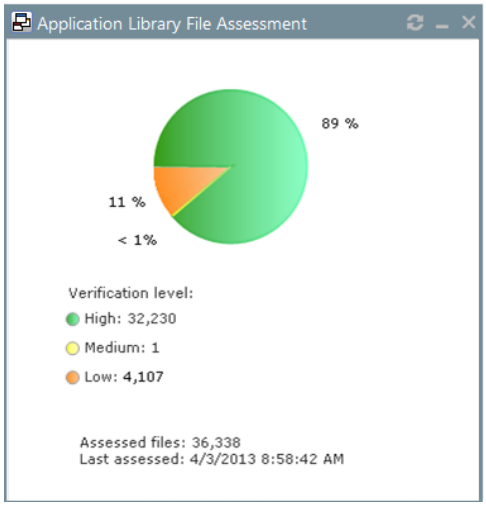


Figure 13: Application Library File Assessment Widget

Each pie chart segment corresponds to a file verification level. The following table describes the ***Application Library File Assessment*** widget fields.

Table 18: Application Library File Assessment Widget Fields

Field	Description
High (Green)	Files have matches in the Ivanti Endpoint Integrity Service. This is a web service maintained by Ivanti that contains a database of verified application files.
Medium (Yellow)	Files have one or both of the following: • A high-prevalence match in the user network (the collection of servers that have sent files to Endpoint Integrity Service for assessment). • A match in the National Software Reference Library (NSLR), a project of the National Institute of Standards and Technology that maintains a reference data set of known software hashes.
Low (Orange)	Files have low-prevalence matches in the user network, or no match was found.
Assessed files	The total number of files in Application Library that have been submitted to Endpoint Integrity Service for assessment.
Last assessed	The date and time that a file assessment was last performed.

The Critical Patch Status by Endpoint Widget
This widget depicts the patch status of all managed endpoints. Each bar indicates the number of managed endpoints with applicable vulnerabilities within a given release date range.

The following table describes the **Critical Patch Status By Endpoint** widget. Green bars indicate endpoints that are patched for critical vulnerabilities, while red bars indicate endpoints that are not patched for critical vulnerabilities.

Table 19: Critical Patch Status By Endpoint Bars

Graph Bar	Description
<30 days	The number of endpoints with applicable critical vulnerabilities fewer than 30 days old.
30 - 120 days	The number of endpoints with applicable critical vulnerabilities between 30 to 120 days old.
>120 days	The number of endpoints with applicable critical vulnerabilities greater than 120 days old.

The following table describes the widget fields.

Table 20: Critical Patch Status By Endpoint Fields

Field	Description
Endpoints	The total number of endpoints with applicable critical vulnerabilities.
Critical vulnerabilities	The total number of critical vulnerabilities applicable to your environment.

Tip: Click the graph to open the ***Critical Vulnerabilities*** content page.

Note:

- If an endpoint is marked as *Do Not Patch* for a critical vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved critical vulnerabilities.
- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the **Critical vulnerabilities** count.

The Discovery Scan Results: Agents Widget
This widget displays the number of endpoints capable of hosting agents discovered in the latest Discovery Scan Job. The endpoints are classified in to two groups: endpoints with agents and endpoints without agents.

Table 21: Discovery Scan Results: Agents Widget Fields

Field	Description
As of	The name of the Discovery Scan Job used to generate the widget graph and statistics. This job is the job most recently run.
Endpoints with agents	The number of agent-compatible endpoints discovered that have agents installed.
Endpoints without agents	The number of agent-compatible endpoints discovered that have no agents installed.
Endpoints	The total number of agent-compatible endpoints discovered.

Tip: Click the widget to open the ***Results*** page for the most recently run Discovery Scan Job.

The Endpoints with Unresolved Updates Widget
This widget displays all endpoints with unapplied applicable content updates, grouped by content type. View this widget when determining if an endpoint requires deployment.

An unresolved update is an occurrence of an endpoint that has not had an applicable content item installed.

Bar	Description
Critical	The number of endpoints that have unresolved critical content updates.
Recommended	The number of endpoints that have unresolved recommended content updates.
Optional	The number of endpoints that have unresolved software, informational, and virus removal content updates.

Tip: Click a widget graph bar to open the ***Content*** page, which is filtered to display all unapplied applicable content.

Field	Description
Endpoints	The number of endpoints with applicable updates within your network.

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.

Note:

- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved updates.
- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.

The Incomplete Deployments Widget

This widget displays all deployments with elapsed start dates and a status of *not started* or *in progress*.

Table 22: Incomplete Deployment Widget Fields

Field	Description
<25%	The number of deployments that are less than 25 percent complete. This field includes deployments that have not started.
25% - 49%	The number of deployments that are 25 to 49 percent complete.
50% - 69%	The number of deployments that are 50 to 69 percent complete.
70% - 79%	The number of deployments that are 70 to 79 percent complete.
80% - 89%	The number of deployments that are 80 to 89 percent complete.
>90%	The number of deployments that are more than 90 percent complete.
Total	The total number of deployments that have a status of *in progress* or *not started* with an elapsed start time.
Total affected endpoints	The total number of endpoints receiving pending or in-progress deployments.

The Last 5 Completed Scan Jobs Widget

This widget contains information about the last five completed discovery scan jobs. Each job name is a link to the associated ***Result*** page.

Table 23: Last 5 Completed Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the name to open the ***Results*** page for the job.

Column	Description
Completed Date	The date and time the job completed on the server.
Status	The status of the completed job.

The Latest News Widget
This widget displays important announcements and other information in Ivanti Endpoint Security.

Click a link to view additional details about an announcement.

The Mandatory Baseline Compliance Widget
This widget displays the Mandatory Baseline status for all endpoints that have the Patch and Remediation module installed.

Table 24: Mandatory Baseline Compliance Widget Fields

Field	Description
Compliant	The number of endpoints with all Mandatory Baseline content installed. **Note:** Endpoints that don't have Mandatory Baseline content installed that's marked *Do Not Patch* are considered compliant.
In process	The number of endpoints currently downloading Mandatory Baseline content.
No baseline	The number of endpoints with no content assigned to their Mandatory Baselines.
Non compliant	The number of endpoints that do not have all content in their Mandatory Baselines installed.
Total number of endpoints	The number of endpoints with an agent installed.

The Mobile Endpoint Last Check In Widget
This widget displays your mobile endpoints, which are grouped by the duration or their last check in.

The total number of mobile endpoints is grouped into six different time categories. Click the graph to open the ***Mobile Endpoints*** page, which will be sorted by date with the oldest endpoints listed on top.

Graph Bar	Description
1 day (Green)	The number of mobile endpoints that last checked in one day ago.
2 days (Light Green)	The number of mobile endpoints that last checked in two days ago.
3 days (Blue)	The number of mobile endpoints that last checked in three days ago.
4-7 days (Yellow)	The number of mobile endpoints that last checked in four to seven days ago.

Graph Bar	Description
8-14 days (Orange)	The number of mobile endpoints that last checked in 8 to 14 days ago.
14+ days (Red)	The number of mobile endpoints that last checked in 14 days ago or more.

The Mobile Endpoint Status Widget
This widget shows the last known status of all registered mobile endpoints. A pie chart displays the percentage of endpoints in each status.

Status	Description
Online	The number of endpoints that have checked in within the set communication interval without issue.
Online Jailbroken	The number of jailbroken iOS endpoints that have checked in within the set communication interval.
Online Rooted	The number of rooted Android endpoints that have checked in within the set communication interval.
Offline	The number of endpoints that have not checked in within the set communication interval.
Disabled	The number of disabled mobile endpoints.
Unmanaged	The number of mobile endpoints that have their profile removed or the app uninstalled.
Expired	The number of endpoints issued an expired license.
Wiped	The number of endpoints that have been sent a command to revert to factory settings.
Total mobile endpoints	The total number of mobile endpoints registered with Ivanti Endpoint Security.

Tip: Click an endpoint status to open the ***Mobile Endpoints*** page, which is filtered to display the clicked endpoint status.

The Mobile Endpoints with Policy Widget
This chart displays all mobile endpoints and their policy assignment status.

This table describes each widget bar.

Bar	Description
No Policy	The number of mobile endpoints that have no policy assignments.

Bar	Description
Blocked	The number of mobile endpoints that have policy assignments that are not being enforced because the endpoint has a status of **Unmanaged**, **Offline**, or **Expired**.
Pending	The number of mobile endpoints that have had a policy assignment that has not yet been applied.
Applied	The number of mobile endpoints that have a policy assignment applied successfully.

The Next 5 Pending Scan Jobs Widget
This widget displays information about the next five pending discovery scan jobs.

Table 25: Next 5 Pending Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the link to view the ***Discovery Scan Jobs*** page ***Scheduled*** tab.
Scheduled Time	The date and time the job is scheduled for on the server.

Tip: Click a job name link to view the ***Discovery Scan Jobs*** page ***Scheduled*** tab.

The Offline Patch Endpoints Widget
This widget displays all offline Patch and Remediation endpoints. These endpoints are grouped by time ranges since they last checked in.

Table 26: Offline Agents Widget Fields

Field	Description
< 48 hours	The number of Patch and Remediation endpoints offline fewer than 48 hours.
48 - 72 hours	The number of Patch and Remediation endpoints offline 48 to 72 hours.
> 72	The number of Patch and Remediation endpoints offline greater than 72 hours.
Total number of offline agents	The number of Patch and Remediation endpoints that are offline (since their last scheduled Discover Applicable Updates task).

Tip: Clicking the **Offline Patch Endpoints** widget pie chart opens the ***Endpoints*** page ***Patch and Remediation*** tab, which is filtered to display offline patch endpoints.

The Patch Agent Module Status Widget

This widget displays all endpoints with the Patch and Remediation module installed, which are grouped by Patch and Remediation status.

Table 27: Patch Agent Module Status Widget Fields

Field	Description
Working	The number of Patch and Remediation endpoints that are working on a deployment task.
Idle	The number of Patch and Remediation endpoints that are idle.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Sleeping	The number of Patch and Remediation endpoints that are sleeping.
Offline	The number of Patch and Remediation endpoints that are offline.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Agents with PR module installed.	The number of endpoints with the Patch and Remediation module installed.
Total Agents	The total number of Patch and Remediation endpoints in your network.

Tip: Click the graph to open the ***Endpoints*** page ***Ivanti Patch and Remediation*** tab.

The Scheduled Deployments Widget

This widget displays endpoints that have not-yet installed applicable content. These endpoints are divided in to two categories: endpoints with deployments scheduled and endpoints with deployments not scheduled. These categories are further divided into three categories: endpoints with not-yet applied critical content, endpoints with not-yet applied recommended content, and endpoints with not-yet applied optional content.

Orange graph bars indicate endpoints that are not scheduled to receive applicable content, while blue graph bars indicate endpoints that are scheduled to receive applicable content.

Table 28: Scheduled Deployments Widget Graph Bars

Graph Bar	Description
Critical	The number of endpoints scheduled or not scheduled to receive deployments for critical content.
Recommended	The number of endpoints scheduled or not scheduled to receive deployments for recommended content.

Graph Bar	Description
Optional	The number of endpoints scheduled or not scheduled to receive deployments for optional content.

Tip: Clicking the **Scheduled Deployments** widget opens the ***Deployments and Tasks*** page, which is filtered to display scheduled deployments.

Table 29: Scheduled Deployments Widget Field

Field	Description
Endpoint with unresolved updates	The number of endpoints with unresolved updates.

The Server Information Widget

This widget lists your serial number, number of licenses available, number of licenses in use, and information about current license usage and availability.

Table 30: Server Information Widget Fields

Field Name	Description
Company	The company your server is registered to as defined during installation.
Serial Number	The license number (serial number) assigned to your server.
License Replication	The subscription status between your server and the Global Subscription Service (GSS).
System Replication	The system replication status between your server and the GSS.
Patch / Content Replication	The replication status between your server and the GSS.
Package Replication	The number of packages remaining for replication.
Auto-download New Critical Packages	The indication of whether your automatically downloads packages for critical vulnerabilities. Click the link to open the ***Subscription Service Configuration*** dialog. For additional information refer to Configuring the Service Tab.

Table 31: Product Licenses Table Columns

Column	Description
Product Module	The module for which you purchased licenses.
In Use	The number of module licenses in use.

Column	Description
Pending	The number of licenses pending use or pending removal. Licenses pending removal become available upon removal completion.
Available	The number of licenses available.

Note: A license expiration notice displays if all available licenses are expired.

The Time Since Last DAU Scan Widget
This widget displays all active agents (not including *disabled* or *offline*) grouped by the amount of time since their last Discover Applicable Updates task.

Table 32: Time Since Last Agent Scan Widget Fields

Field	Description
< 24 hours	The number of agents that last performed a Discover Applicable Updates (DAU) task and checked in fewer than 24 hours ago.
24 - 47 hours	The number of agents that last performed a DAU task and checked in 24 to 47 hours ago.
48 - 72 hours	The number of agents that last performed a DAU task and checked in 48 to 72 hours ago.
> 72 hours	The number of agents that performed a DAU task and last checked in greater than 72 hours ago.
Never checked in	The number of agents that have registered yet have not completed a DAU task.
Total active agents	The total number of active agents.

Tip: Click the **Time Since Last Agent Scan** widget graph to open the ***Endpoints*** page, which is filtered to display enabled endpoints.

The Un-remediated Critical Vulnerabilities Widget
This widget displays the total number of unremediated critical vulnerabilities that are applicable to your environment grouped by age.

Table 33: Un-remediated Critical Vulnerabilities Widget Graph

Graph Bar	Description
<30 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network fewer than 30 days old.

Graph Bar	Description
30 - 120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network that are 30 to 120 days old.
>120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network greater than 120 days old.

Tip: Click the graph to open the ***Vulnerabilities*** page, which is filtered to display critical but not superseded applicable vulnerabilities.

Table 34: Un-remediated Critical Vulnerabilities Widget Fields

Field	Description
Critical Vulnerabilities	The number of critical but not superseded vulnerabilities applicable in your network.
Endpoints	The number of endpoints with critical but not superseded applicable vulnerabilities.

Note:

- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Critical vulnerabilities** count.
- If an endpoint is marked as *Do Not Patch* for an applicable vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Endpoints with Unresolved AV Alerts Widget

This widget displays the number of endpoints with unresolved antivirus event alerts.

There are two types of unresolved antivirus event alerts, *not cleaned* and *quarantined*. If an endpoint has multiple not cleaned event alerts, it is counted only once in the **Not Cleaned** column. Likewise, if it has multiple quarantined event alerts, it is counted only once in the **Quarantined** column. However,

if an endpoint has both not cleaned and quarantined event alerts, it is counted twice (once in each column).

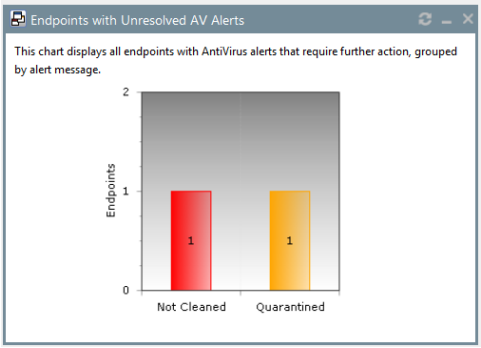


Figure 14: Endpoints with Unresolved AV Alerts Widget

The following table describes each graph bar.

Bar	Description
Not Cleaned	The number of endpoints with not cleaned event alerts.
Quarantined	The number of endpoints with quarantined event alerts.
Tip: Clicking a widget graph bar opens the ***Virus and Malware Event Alerts*** page, which is filtered on the endpoint name.	

The Top 10 Infected Endpoints Widget
This widget displays the 10 endpoints which have received the most event alerts in the last 10 days, and a breakdown of each endpoint's alert status.

The widget lists all event alert types, including cleaned, not cleaned, deleted, and quarantined.

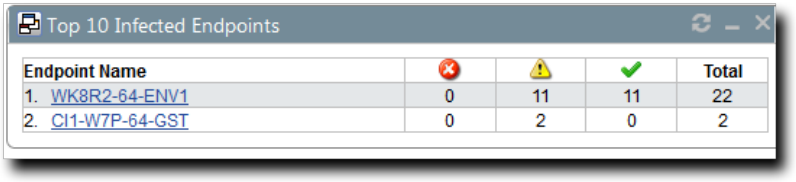


Figure 15: Top 10 Infected Endpoints Widget

The following table describes each column in the widget.

Column	Description
Endpoint Name	The name of the endpoint, with a link to its ***Details*** page.
Not Cleaned	The number of alerts on the endpoint where it was not possible to clean a suspect file.

Column	Description
Quarantined	The number of alerts on the endpoint where the file was moved to quarantine.
Cleaned	The number of alerts on the endpoint where a file was successfully cleaned.
Deleted	The number of alerts on the endpoint where a suspect file was deleted.
Total	The total number of all alerts on the endpoint. This is the number on which the ranking of the list is based.

The Top 10 Virus/Malware Threats Widget

This widget displays the 10 types of virus or malware that have generated the most event alerts in the last 10 days.

The malware types are listed from the top down in descending order of frequency, and the number of endpoints affected is displayed along the bottom of the widget.

Note: The display is based on the number of event alerts generated by each virus/malware type, regardless of how the event was handled (cleaned, not cleaned, deleted, or quarantined).

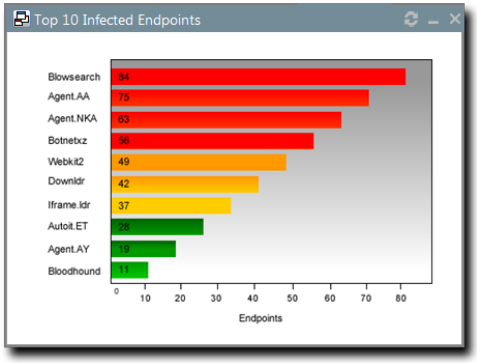


Figure 16: Top 10 Virus/Malware Threats

Clicking on any virus/malware bar will bring you to its ***Virus/Malware Details*** page.

The Estimated Energy Savings: Daily Widget

This widget displays the energy savings for the previous day. This calculation is based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 35: Estimated Energy Savings: Daily Widget Fields

Field	Description
Results for the day of	The date for which the widget displays the results.
Desktop count	The number of monitored desktops.

Field	Description
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Weekly Widget
This widget displays the energy savings of the past seven days based on your endpoints' actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 36: Estimated Energy Savings: Weekly Widget Fields

Field	Description
Results for the week from	The dates for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Monthly Widget

This widget displays the energy savings of the past 30 days based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

The following table describes the fields in the **Estimated Energy Savings: Monthly** widget.

Table 37: Estimated Energy Savings: Monthly Widget Fields

Field	Description
Results for the month from	The month for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Device Control Denied Actions Widget

This widget displays the users with the highest number of actions blocked by device control policies. View this widget when determining the lists of users for whom action block occurred due to the device control policies.

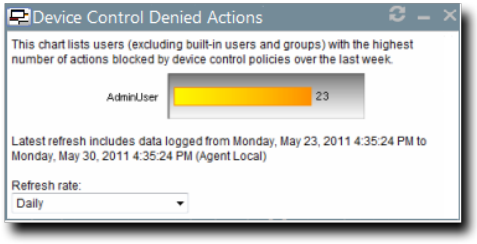


Figure 17: Device Control Denied Actions Widget

The chart displays the users with the highest number of actions blocked by device control policies. The widget can displays five users with the highest number of actions blocked by device control policies.The count on the bar displays the number of times the user actions were blocked by the device control policies.

The Devices Connected to Endpoints Widget

This widget displays the number of peripheral device classes that were connected to endpoints. View this widget when determining which devices were connected to endpoints over the last week.

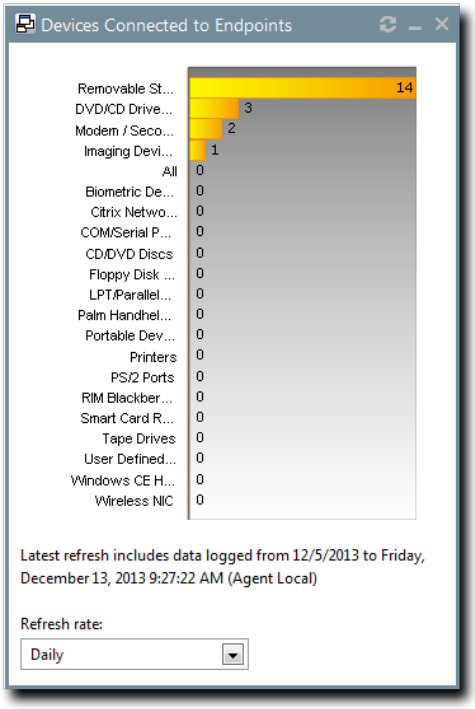


Figure 18: Devices Connected to Endpoints Widget

The chart displays the number of devices in each device class connected to the endpoints. The count on the bar displays the number of devices in a particular device class that were connected to the endpoints.

Dashboard Setting and Behavior Icons

Setting and behavior icons are UI controls used to manage the dashboard. Click these icons to maximize, minimize, hide, and refresh the dashboard and widgets.

The following table describes each icon action.

Table 38: Widget Setting and Behavior Icons

Icon	Action
	Opens the ***Dashboard Settings*** dialog.
	Opens the dashboard in print preview mode.

Icon	Action
	Collapses the associated widget.
	Expands the associated collapsed widget.
	Hides the associated widget.
	Refreshes the associated widget (or the entire dashboard).

Note: Not all widgets contain **Refresh** icons.

Previewing and Printing the Dashboard

When viewing the dashboard, you can reformat it for printing. This reformat omits the Web site header and footer, reorganizing the dashboard to display only the selected widgets, making it ideal for printing.

1. From the **Navigation Menu**, select **Home**.
2. Click  .

   Step Result: The dashboard print preview opens in a new Web browser window.
3. [Optional] Use your Web browser controls to print the dashboard.

Editing the Dashboard

You can customize how widgets are arranged and prioritized. Edit the dashboard to display only the widgets useful in your environment.

Edit the dashboard from the ***Dashboard Settings*** dialog.

1. From the **Navigation Menu**, select **Home**.
2. Click  .

   Step Result: The ***Dashboard Settings*** dialog opens.
3. Choose which widgets you want to display on the dashboard.
   - Select widget check boxes to display them.
   - Clear widget check boxes to hide them.
4. Prioritize the widgets in the desired order.
   - Click  to increase a widget priority.
   - Click  to decrease a widget priority.

   Highly prioritized widgets are more prominently placed.

5. Display or hide widget descriptions.
   - Click to display descriptions.
   - Click to hide descriptions.
6. Choose a widget layout.
   - Click to display widgets in two columns.
   - Click to display widgets in three columns.
7. Click **OK**.

Result: Your dashboard settings are saved. The ***Home*** page displays the selected widgets in the priority you defined.

The System Alert Pane

The ***System Alert*** pane displays information about changing conditions in your environment. This pane alerts you to required actions and links to related help topics.

The **System Alert** pane displays in the dashboard and shows the number of alerts that require your attention.

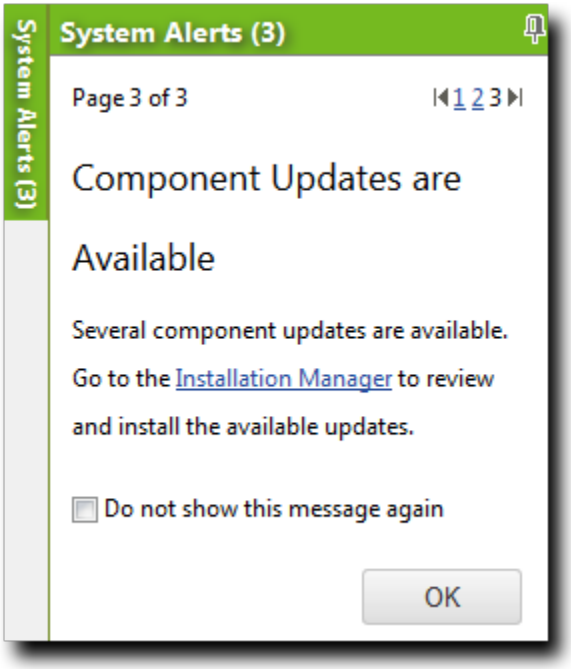


Figure 19: The System Alert Pane

The following functions can be found in the ***System Alert*** pane.

Table 39: Options Menu Items

Option	Description
Pin (icon)	Docks the ***System Alert*** pane. Clicking this icon again collapses it.
Pagination Links	Allows you to navigate between alerts. For more information, see Advancing Through Pages on page 38.
Action Link	Opens the appropriate application page, external Web page, or context-sensitive help topic, depending on the action specified in the alert.
Don't show this again (check box)	Collapses the ***System Alert*** pane. The alert shown in the ***System Alert*** pane when this check box is selected will no longer be shown.
OK (button)	Collapses the ***System Alert*** pane.

Note:

- Dismissing a notification only dismisses the notification for logged in user. The notification still displays for others.
- The system automatically dismisses alerts as you complete their related actions, regardless of whether you dismiss the alerts.

License Expiration

When licensing for a module expires, the module behavior changes. All functionality is restored when the licensing is renewed.

Note: When a subscription expires, the module history and configuration is retained. No work is lost when the module is renewed.

Table 40: License Expiration Scenario and Events

Scenario	Event(s)
Server Module Expiration	• Endpoint module functionality is partially disabled. • The module cannot be installed on additional endpoints. • The ***Endpoints*** page list the module status as `Expired`. • The ***Home*** page lists the **Available** license count as `Expired`.
Endpoint Module Expiration	• Endpoint module functionality is partially disabled. • The module cannot be installed on additional endpoints. • The ***Endpoints*** page list the module status as `Expired`. • The ***Home*** page lists the **Available** license count as `Expired`. • The Patch and Remediation endpoint module component continues to inventory its host, but no longer enforces Patch and Remediation policies or downloads deployments. • The AntiVirus endpoint module continues enforcing policies and completing scans, but no longer downloads new virus definitions. • The Application Control endpoint component stops enforcing all policies, no longer blocking or logging applications. • The Device Control endpoint component allows all actions and stop logging activity.

Table 41: License Expiration Scenario and Events for Mobile Endpoints

Scenario	Event

Mobile Endpoint Module Expiration	• The ***Mobile Endpoints*** page list the module status as `Expired`.
	  • Endpoints with the oldest check ins expire first.
	  • Endpoints that attempt to register when your license count is depleted are listed with a status of `Expired`.
	  • Endpoints cannot be issued commands with the exception of **Delete**.
	  • Any push notifications available on expired endpoints are removed.
	  • Any policy events queued or issued to expired endpoints have display a status of `Expired`.
	• Endpoints cease communications with the server and the cloud.
	• The ***Home*** page lists the available license count as `0`.

	Note: Endpoints in an `Offline` or `Wiped` status hold their license until deleted.

To reactivate your licenses following renewal, open the ***Subscription Updates*** page and click **Update Now**. Your server replicates updated subscription information. The page refreshes when the update completes, and all previous module functionality is restored.

Note: For more information about renewing or adding licenses, contact Ivanti Sales Support (sales@ivanti.com) .

Chapter 4

Managing Wakepoints

In this chapter:

Ivanti Wake on LAN uses *wakepoints* to send wake requests to network endpoints. Before you can begin waking endpoints, you must define wakepoints.

About Wakepoints

To power-on network endpoints, Ivanti Wake on LAN requires you to designate wakepoints. Wakepoints are endpoints that relay server wake requests to other network endpoints, thus waking them without a physical presence.

Ivanti Wake on LAN sends wake requests to wakepoints using the user datagram protocol (UDP). Wakepoints then relay the request to agent-managed endpoints.

Wakepoints disperse relayed wake requests through routers and firewalls. This avoids direct broadcast and multicast, which can cause excessive network bandwidth consumption. Additionally, routers may block UDP packets sent by other subnets. Successful wake request outcomes are contingent upon firewall and router settings.

Each segment of your network (VLAN) requires at least one wakepoint. However, Ivanti recommends assigning multiple wakepoints to each network segment. This practice ensures there are multiple distribution points within a network segment, therefore ensuring endpoints receive wake requests in the event that a router blocks a wake request.

Configuring Wakepoints

You should select wakepoints based on a managed endpoint's online status, installed agent version, and operating system.

Wakepoints must meet the following requirements:

- Wakepoints must be Windows-based.

Additionally, Ivanti recommends that endpoints designated as wakepoints should always be powered on.

Important: You must select at least one Wakepoint within a network segment (VLAN).

Working with Wakepoints

Manage wakepoints from the ***Wake on LAN*** page ***WOL Configuration*** tab.

You can perform the following tasks related to wakepoint management:

- Adding a Wakepoint on page 66
- Removing a Wakepoint on page 67

Adding a Wakepoint

The ***Assigned Wakepoints*** list itemizes the currently selected wakepoints and provides you with options to add additional ones.

1. Select **Tools** > **Wake on LAN**.

   Step Result: The page opens to the ***WOL Configuration*** tab.

2. From the **Wakepoint Configuration** section, add wakepoint(s).

   Wakepoints are managed endpoints with the Wakepoint module installed. Wakepoints relay wake requests from Ivanti Endpoint Security to managed endpoints within your network.

   a) Under assigned wakepoints click **Add**.

   Step Result: The ***Add Wakepoints*** dialog opens.

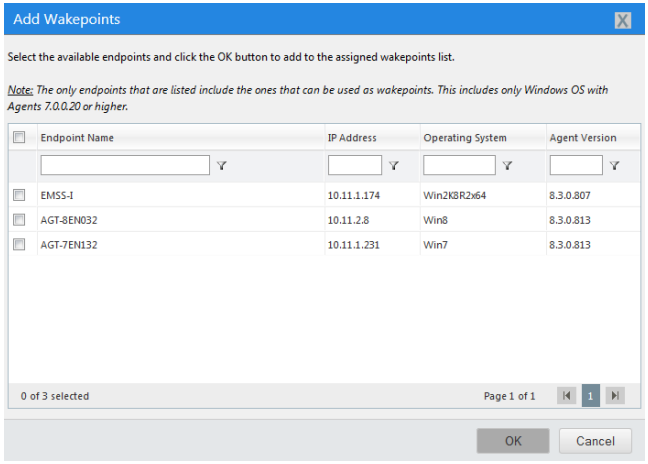


Figure 20: Add Wakepoints Dialog

   b) Select the endpoints you want to function as wakepoints.

c) Click **OK**.

Step Result: The ***Add Wakepoints*** dialog closes and the selected endpoints are added to the ***Assigned Wakepoints*** list.

3. From the **Wakepoint Configuration** section, edit the **Wake on LAN Port** (0-65535) if applicable.

   This port is the port wakepoints use to relay wake requests to endpoints. When defining the **Wake on LAN Port**, remember the following:

   - Under most network conditions, this field does not require editing.
   - Ivanti Wake on LAN uses **9** by default.
   - Ivanti recommends using **0**, **7**, or **9**.

4. Click **Save**.

   Step Result: The changes to your configuration are saved.

Result: The defined wakepoint(s) and port number are saved. The saved settings will be used during the next schedule wake request broadcast.

Removing a Wakepoint

The ***Assigned Wakepoints*** list itemizes the currently selected wakepoints and provides options to remove wakepoints you no longer need.

1. Select **Tools** > **Wake on LAN**.

   Step Result: The page opens to the ***WOL Configuration*** tab.

2. Within the **Wakepoint Configuration** section, remove the wakepoint(s) you no longer need.

   a) Select the desired wakepoint(s) in the ***Assigned wakepoints*** list.
   b) Click **Remove**.

   Step Result: A confirmation dialog displays.

   c) Click **OK**.

3. Click **Save**.

   Step Result: The changes to your configuration are saved.

Result: The selected endpoint(s) are no longer wakepoint(s).

Note: Removing a wakepoint only prevents an endpoint from continuing to function as a wakepoint. It does not remove the Ivanti Endpoint Security agent from the selected endpoint.

Chapter 5

Waking Endpoints

In this chapter:

After installing Ivanti Wake on LAN (WOL) and wakepoints, you can power on any managed endpoint using the Ivanti Endpoint Security Web console. You can manage endpoint wake times, configurations, and logging functions.

Important:

- You can only wake agent-managed endpoints.
- Due to changes made by Microsoft, Windows 8 endpoints do not respond to Ivanti Wake on LAN wake requests if their last shutdown was initiated using the Windows 8 GUI. Shutting down Windows 8 using this method closes sockets used by Ivanti Wake on LAN to initiate wake requests.

Use the WOL module to boot agent-managed endpoints using network communication. Send wake requests to a managed endpoint, thus booting the endpoint. Using this module in conjunction with other Ivanti Endpoint Security modules facilitates security administration after business hours.

Note: WOL is a send-only model. Therefore, managed endpoints do not indicate wake request outcomes. To determine the outcome of wake requests, view an agent's status in Ivanti Endpoint Security from the ***Endpoints*** page (`online` or `offline`).

Ivanti Wake on LAN Scheduling Methods

When using Ivanti Wake on LAN, you can send endpoint wake requests using different scheduling methods: hours of operation (HOP), custom daily wake times, and wake now.

Ivanti Wake on LAN includes the following methods to schedule wake requests:

Wake during Hours of Operation	This method schedules wake requests based on endpoint HOP settings, which are defined in agent policy set(s). HOP settings define the days and times an endpoint's agent is operational. Within Ivanti Endpoint Security, you can create many agent policy sets. Therefore, the agent policy set applied to a given group governs its agents' behavior. When multiple agent policy sets are applied to a group, HOP are an accumulation of all applicable agent policy sets' defined HOP. For additional information about agent policy sets and HOP, refer to the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) . **Remember:** Agent hours of operation are based on the host endpoint's local time. **Note: Wake during Hours of Operation** wake request are only available in Ivanti Endpoint Security environments with the Patch and Remediation module installed.
Group Wakeup Times	This method schedules wake requests based on a time you assign to an endpoint group. Wake requests are sent based on the server local time.
Wake Now	This method schedules a wake request for a selected endpoint immediately.

Note: You can use multiple schedule methods to wake endpoints. Methods can operate in conjunction without conflict because Ivanti Wake on LAN uses the combined information from HOP and group wakeup times.

The Ivanti Wake on LAN Page

Use this page to define wakepoints and wake times for managed endpoints.

The ***Wake on LAN*** page is added to the Web console following installation of the Ivanti Wake on LAN module.

View this page by selecting **Tools** > **Wake on LAN** from the Navigation Menu.

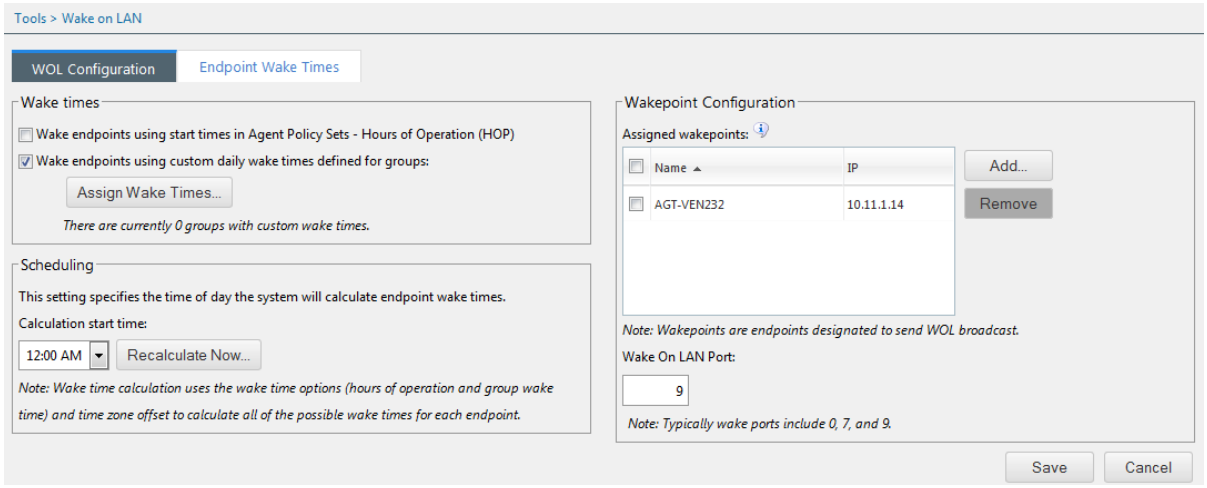


Figure 21: Wake on LAN

The ***Wake on LAN*** page contains the following tabs:

- The WOL Configuration Tab on page 72
- The Endpoint Wake Times Tab on page 74

The WOL Configuration Tab

The ***WOL Configuration*** tab contains controls for configuring wake requests or wakepoints.

When you open the Ivanti Endpoint Security Web console and select the ***Wake on LAN*** page, the ***WOL Configuration*** tab displays.

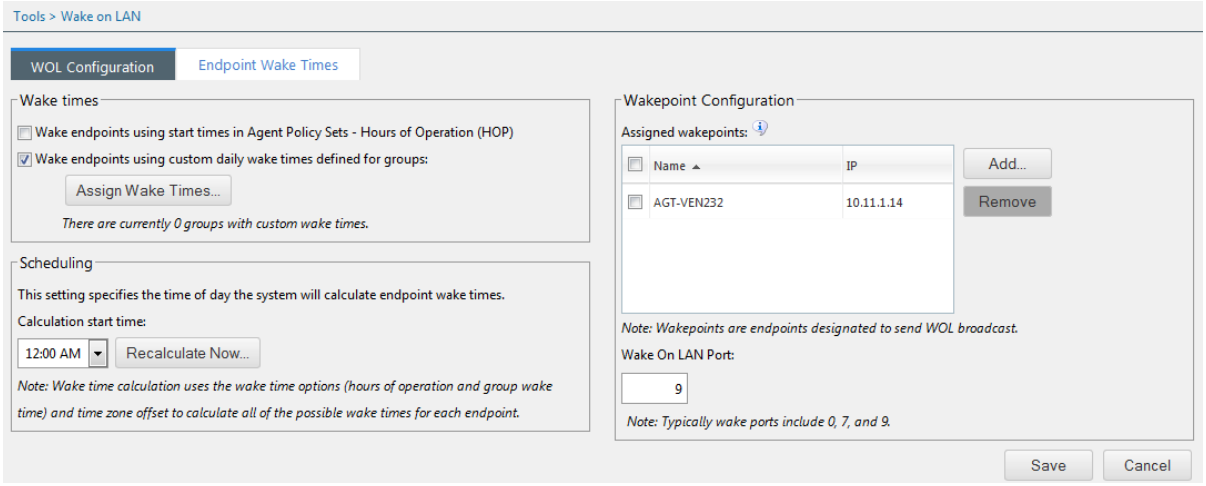


Figure 22: The WOL Configuration Tab

Wake Times

These options define the scheduling methods used to determine wake times.

The following table describes the **Wake times** options.

Table 42: Wake Times

Option	Description
Wake endpoints using start times in Agent Policy Sets - Hours of Operation (HOP) (check box)	Enables the wake time calculation to use hours of operation (HOP) to calculate possible wake times for endpoints that have HOP defined. **Note: Wake during Hours of Operation** wake request are only available in Ivanti Endpoint Security environments with the Patch and Remediation module installed.
Wake endpoints using custom daily wake times defined for groups (check box)	Enables the wake time calculation to use the custom wake times for groups to calculate possible wake times.

Option	Description
Assign Wake Times (button)	Opens the ***Define Daily Wake Times*** dialog. For additional information, refer to Scheduling Wake Requests by Custom Daily Times on page 80.

Scheduling

Use these options to define the time that Ivanti Wake on LAN calculates endpoint wake times.

The following table describes the **Scheduling** options.

Table 43: Scheduling

Option	Description
Calculation start time (list)	Defines the time used to calculate endpoint wake times. Times are available in 30 minute increments.
Recalculate Now... (button)	Calculates endpoint wake times immediately. For additional information, refer to Calculating Endpoint Wake Times on page 79. **Note:** The default time is **12:00 am** server time.

For additional information about scheduling options, refer to Ivanti Wake on LAN Scheduling Methods on page 70.

Wakepoint Configuration

Use these controls to define wakepoints, which are the endpoints Ivanti Wake on LAN uses to relay wake requests to network endpoints.

The following table describes the **Assigned Wakepoints** list, which displays in **Wakepoint Configuration** options. This list itemizes defined wakepoints.

Table 44: Assigned Wakepoints

Column	Description
Name	The name of the assigned wakepoint.
IP	The IP address of the assigned wakepoint.

Note: The **Information** icon provides a detailed explanation of **Wakepoint** functionality.

The following table describes the buttons used to edit the **Assigned Wakepoints** list.

Table 45: Assigned Wakepoint Buttons

Button	Description
Add	Adds a wakepoint to the **Assigned Wakepoints** list. For additional information, refer to Adding a Wakepoint on page 66.
Remove	Removes a selected wakepoint from the **Assigned Wakepoints**. For additional information, refer to Removing a Wakepoint on page 67.

The following table describes the remaining **Wakepoint Configuration** option.

Option	Description
Ivanti Wake on LAN Port (field)	Defines the port that wakepoints use to communicate with Ivanti Wake on LAN. For additional information, refer to Adding a Wakepoint on page 66.

The Endpoint Wake Times Tab

The ***Endpoint Wake Times*** tab lists endpoints for which wake times have been defined. From this tab, you can also wake endpoints immediately.

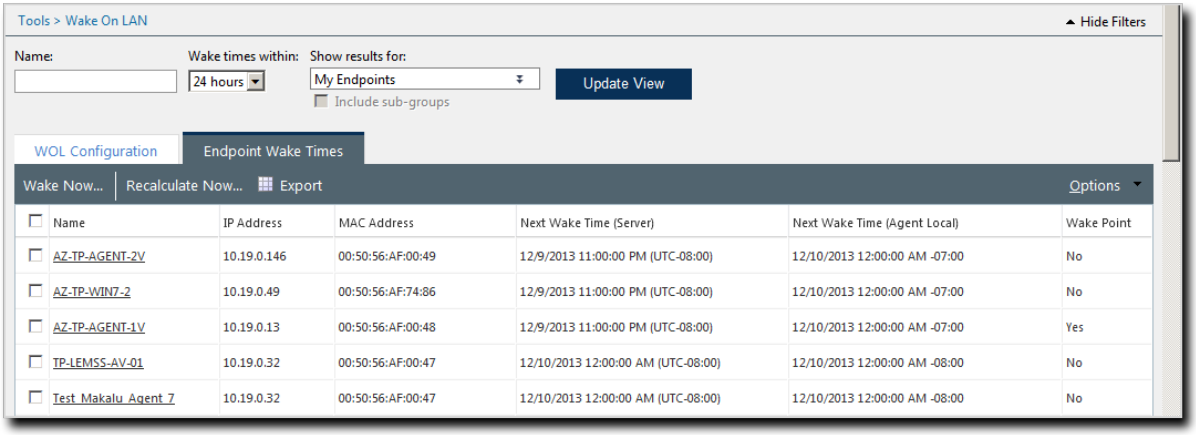


Figure 23: Endpoint Wake Times Tab

The Endpoint Wake Times Tab Toolbar

This toolbar contains buttons used to initiate Ivanti Wake on LAN features.

The following table describes each toolbar button's function.

Table 46: Endpoint Wake Times Tab Toolbar

Button	Description
Wake Now...	Wakes the endpoints selected from the ***Endpoint Wake Times*** tab list. For additional information, refer to Wake Endpoints from the Endpoint Wake Times Tab on page 82.
Recalculate Now...	Recalculates the wake times for the endpoints selected from the ***Endpoint Wake Times*** tab list. For additional information, refer to Calculating Endpoint Wake Times on page 79.
Export	Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 31.

The Endpoint Wake Times Tab List

This list itemizes all network endpoints scheduled to receive wake requests. This list also features additional information about endpoints and their next wake time.

The following table describes each list column.

Table 47: Endpoint Wake Times Tab List

Column	Description
Name	Indicates the endpoint name.
IP Address	Indicates the endpoint IP Address.
MAC Address	Indicates the endpoint MAC address.
Next Wake Time (Server)	Indicates the next time the endpoint will be woken based on server settings.
Next Wake Time (Agent Local)	Indicates the next time the endpoint will be woken based on endpoint settings.

Column	Description
Wake Point	Indicates if the endpoint is a wakepoint.

Working with Ivanti Wake on LAN

After defining wakepoints, you can begin waking endpoints remotely.

You can perform the following tasks related to waking endpoints.

Scheduling Wake Requests by Hours of Operation

You can schedule wake request broadcasts for endpoints using hours of operation settings, which are defined within agent policy sets.

Prerequisites:

Ensure hours of operation for the applicable agent policy sets are defined. For additional information, refer to Defining Hours of Operation for Endpoints on page 77.

Note: Wake during Hours of Operation wake request are only available in Ivanti Endpoint Security environments with the Patch and Remediation module installed.

1. Select **Tools** > **Wake on LAN**.

   Step Result: The page opens to the ***WOL Configuration*** tab.

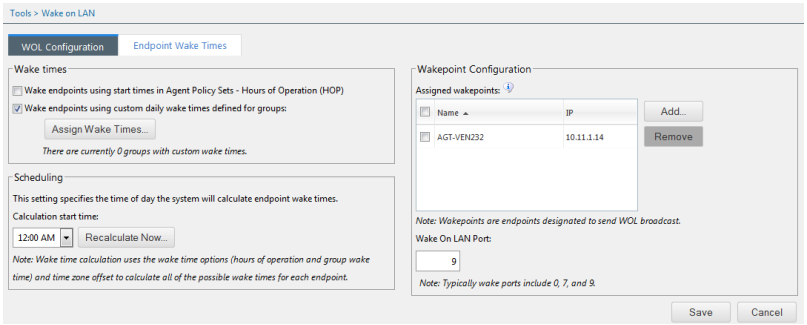


Figure 24: Ivanti Wake on LAN Configuration Tab

2. Select the **Wake endpoints using start times in Agent Policy Sets - Hours of Operation (HOP)** check box.
3. Click **Save**.

Result: The endpoints are configured to wake up according to the assigned hours of operation.

> **Note:** Successful wake request outcomes are contingent upon firewall and router settings. Firewall and routers must be configured to permit packet broadcasts. Refer to your router's user manual for more information on how to configure firewall settings.

After Completing This Task:
Complete Calculating Endpoint Wake Times on page 79.

Defining Hours of Operation for Endpoints
When scheduling wake times based on agent hours of operation (HOP), you must define these hours within agent policy sets prior to using Ivanti Wake on LAN. HOP determines when an agent is active on its host endpoint. When used in conjunction with Ivanti Wake on LAN, HOP also determines when the host endpoint is powered on.

Edit agent hours of operation when creating or editing an agent policy set.

> **Note: Wake during Hours of Operation** wake request are only available in Ivanti Endpoint Security environments with the Patch and Remediation module installed.

1. Select **Manage** > **Agent Policy Sets**.
2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

Step Result: Either the ***Create Agent Policy Set*** or the ***Edit a Policy Set*** dialog opens.

3. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click the **Define** button beside the **Hours of Operation** field.

Context	Procedure
If you are editing an agent policy set:	Click the **Modify** button beside the **Hours of Operation** field.

Step Result: The ***Edit Agent Hours of Operation*** dialog opens.

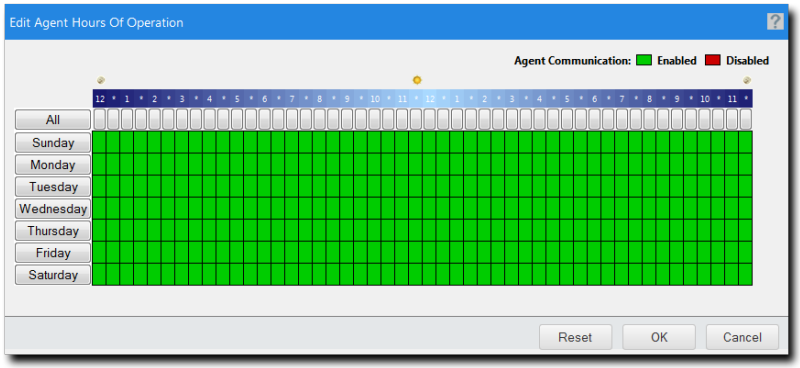


Figure 25: Edit Agent Hours of Operation Dialog

4. Click time units to define agent hours of operation.

   Green units indicate days and times of enablement, while red units indicate days and times of disablement.

   - Click **All** to toggle all ***Time*** units on or off.
   - Click a ***Day*** button to toggle time units for a day on or off.
   - Click ***Time*** units to toggle individual units on or off.

5. Click **OK**.
6. Finish any desired edits in the dialog and click **Save**.

Note: Changes made to the **Hours of Operation** schedule will not be saved until you have clicked **Save** in the ***Agent Policy Set*** dialog.

Result: Your edits are saved. These edits take effect the next time Ivanti Endpoint Security and the applicable agents communicate.

How Endpoint Wake Times are Calculated

Ivanti Wake on LAN boots endpoints remotely after calculating wake times on a daily basis. You can select the daily time when this calculation occurs. This calculation checks for edits to agent hours of operation or custom daily wake time changes.

Using respective settings on the ***WOL Configuration*** tab, wake times calculation are based upon (hours of operation and group wake times) and the time zone offset to calculate the actual wake times for each endpoint.

Note: The default value of the **Calculation Start Time** option is 12:00 am server time.

Calculating Endpoint Wake Times

Following any edits you make to hours of operation edits, you should immediately recalculate wake times. This recalculation ensures that endpoints are woken at their scheduled times.

Note: Wake times calculation may become CPU intensive with increasing numbers of endpoints. Recalculating immediately offers the ability to choose the recalculation time so that you can select the ideal time when the server is not busy.

1. Select **Tools** > **Wake on LAN**.

   Step Result: The page opens to the ***WOL Configuration*** tab.

2. Select one of the following tabs to access the **Recalculate Now** button.

Tab	Description
WOL Configuration	Contains controls for configuring wake requests or wakepoints.
Endpoint Wake Times	Contains controls and a list of endpoints for which times have need defined.

3. Click **Recalculate Now**.

   Step Result: The ***Recalculate Now*** dialog opens.

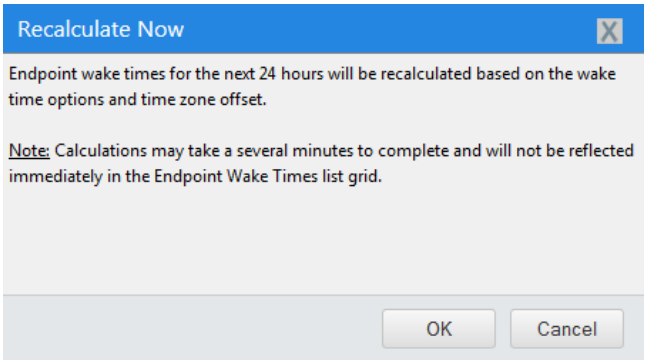


Figure 26: Recalculate Now Dialog

4. Click **OK** to confirm the calculation action.

Result: Ivanti Wake on LAN recalculates endpoint wake times.

Scheduling Wake Requests by Custom Daily Times

You can configure Ivanti Wake on LAN (WOL) to wake endpoint groups at a specific time each day.

1. Select **Tools** > **Wake on LAN**.

   Step Result: The page opens to the ***WOL Configuration*** tab.

2. Ensure the **Wake endpoints using custom daily wake times defined for groups** check box is selected.

   Step Result: The **Assign Wake Times** button becomes available.

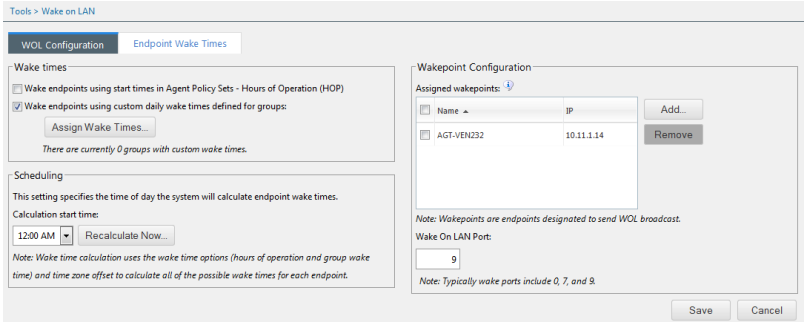


Figure 27: Ivanti Wake on LAN Configuration Tab

3. Click **Assign Wake Times**.

   Step Result: The ***Assign Daily Group Wake Times*** dialog opens.

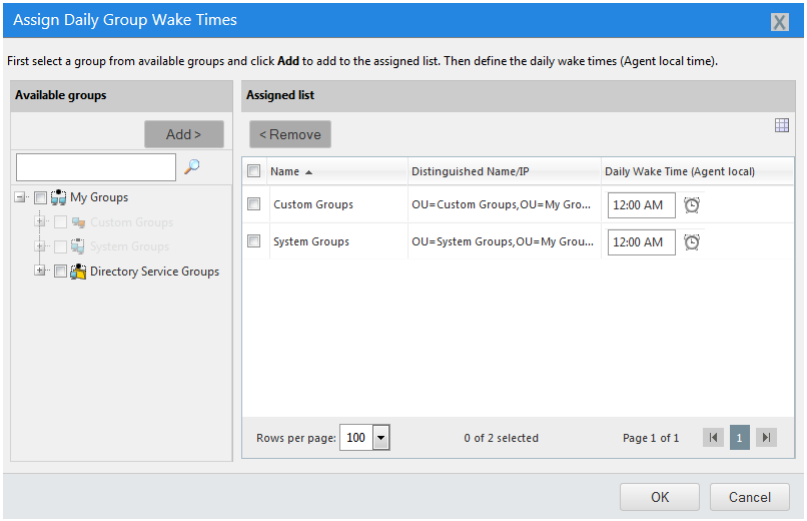


Figure 28: The Assign Daily Group Wake Times Dialog

4. Select the groups from the ***Available groups*** list to add to the **Assigned** list.

   Tip: You can use the **Available groups** field to search for groups.

5. Click **Add**.

   Step Result: The selected groups are added to the ***Assigned list***.

6. Set the **Daily Wake Time** for each group.

   a) Type a time in all empty **Daily Wake Time** fields (`hh:mm`). You can type time in 12-hour or 24-hour formats.

   Tip: Click the **Clock** icon to select a time from a menu. Times are available for every 30 minute interval.

7. Click **Apply** after edits are completed.

   Step Result: Your changes are applied (dialog remains open).

8. Click **OK**.

   Step Result: Your changes are applied and the ***Assign Daily Group Wake Times*** dialog closes.

9. Click **Save**.

Result: The endpoints are configured to be woken at the defined wake times.

> **Note:** For more information on creating and managing groups, refer to the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

After Completing This Task:
Complete Calculating Endpoint Wake Times on page 79.

Wake Endpoints from the Endpoint Wake Times Tab

You can wake managed endpoints at any time.

Perform this task from the ***Endpoint Wake Times*** tab.

1. Select **Tools** > **Wake on LAN**.

   Step Result: The page opens to the ***WOL Configuration*** tab.

2. Select the ***Endpoint Wake Times*** tab.

   Step Result: The ***Endpoint Wake Times*** tab opens.

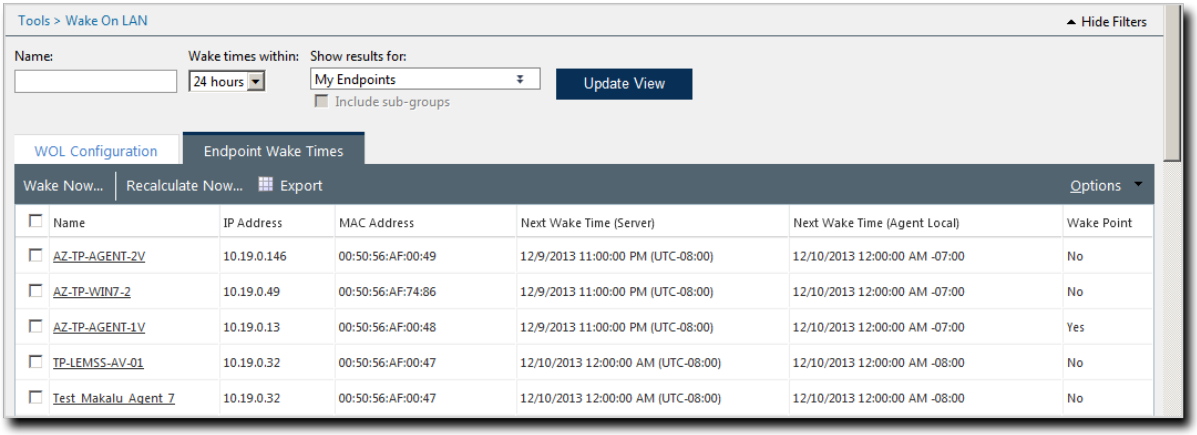


Figure 29: Endpoint Wake Times Tab

3. Select the check box(es) associated with the endpoint(s) you want to wake.
4. Click **Wake Now**.

   Step Result: The ***Wake Now*** dialog appears.

5. Click **OK** to confirm the wake action.

Result: The selected endpoint(s) are woken within five minutes.

Wake Endpoints from the Manage Endpoints Page

After installing Ivanti Wake on LAN, you can wake managed endpoints immediately from the ***Endpoints*** page.

Wake endpoints immediately from the ***Endpoints*** page ***All*** tab.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints Page*** opens to the ***All*** tab.

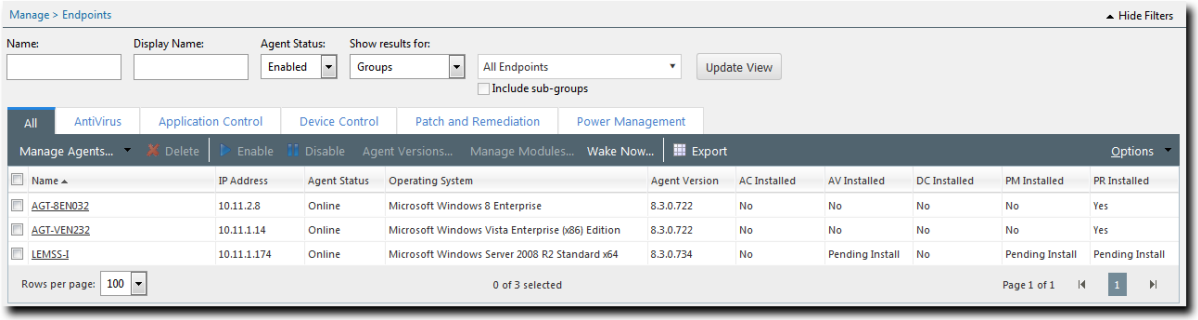


   Figure 30: Endpoints Page

2. Select the check box(es) associated with the endpoint(s) you want to wake.
3. Click **Wake Now**.

   Step Result: The ***Wake Now*** dialog appears.

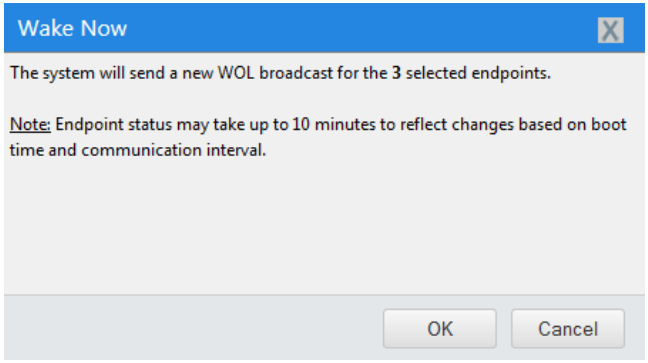


   Figure 31: Wake Now Dialog

4. Click **OK** to confirm the wake action.

Result: The wake signal is broadcast. Selected endpoints will boot within ten minutes.

Waking Endpoints (Groups Page)
After installing Ivanti Wake on LAN, you can wake managed endpoints immediately from the ***Groups*** page ***Endpoint Membership*** view.

Wake endpoints from the ***Groups*** page ***Endpoint Membership*** view.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page opens.

2. From the **View List**, select **Endpoint Membership**.

   Step Result: The ***Endpoint Membership*** view opens.

3. Ensure the **All** tab is selected.
4. From the directory tree, select the group containing endpoints you want to reboot.
5. Select the check box(es) associated with the endpoint(s) you want to wake.
6. Click **Wake Now**.

   Step Result: The ***Wake Now*** dialog appears.

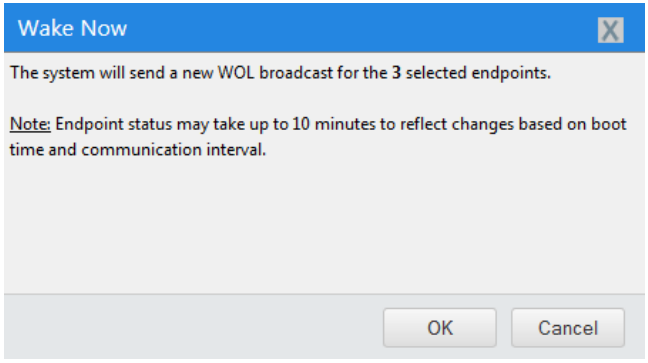


Figure 32: Wake Now Dialog

7. Click **OK** to confirm the wake action.

Result: The wake signal is broadcast. Selected endpoints will wake within ten minutes.

Appendix
A

Configuring Windows 8 Endpoints for Ivanti Wake on LAN

In this appendix:

By default, Windows 8 endpoints (and later operating system) are not configured to accept wake requests. Before using Ivanti Wake on LAN with you Windows 8 endpoints, you must reconfigure their power settings.

Disabling Fast Startup

The Fast Startup feature disables Ivanti Wake on LAN functionality. Disable Fast Startup to use Ivanti Wake on LAN for your Windows 8 endpoints (and later releases).

Disable Fast Startup within the Power Settings.

1. Press the **Windows Logo** key.
2. Type **Control Panel** and press ENTER.

   Step Result: ***Windows Control Panel*** opens.
3. From the **View by** list, ensure **Category** is selected.
4. Click **Hardware and Sound**.

   Step Result: The **Hardware and Sounds** options display.
5. Click **Power Options**.

   Step Result: The **Power Options** display.
6. Click the **Choose what the power buttons do** link.
7. Within **Shutdown settings**, ensure the **Turn on fast startup** option checkbox is cleared and click **Save changes**.

Result: The **Turn on fast startup** option is disabled. The Windows 8 (or later) endpoint will accept wake requests after it is shut down.