# Verdiem Surveyor

**Version: 6.5.205**

## Administrator Guide

**December 2019**

# Contents

## Chapter 5: Managing Locations, Energy Rates, and Currency     5-1

## Chapter 6: Managing Policies     6-1

# 1

# About Surveyor

**Table 1-1  In this Chapter**

| Topics |
| --- |
| *Overview of Surveyor 6* |
| *Getting Started with Surveyor and Power Management* |
| *Open the Administrator Console* |
| *Power Management for Windows PCs* |
| *About Mac OS X Power Management* |
| *System Settings and Descriptions* |

# Overview of Surveyor 6

This section introduces Surveyor 6 and concepts related to the power management of Windows and Mac computers, and other devices.

Surveyor is a comprehensive power management solution that helps you manage the power states of computers and network-connected devices in a way that reduces energy consumption without disrupting work activity.

Surveyor measures, monitors, and regulates energy consumption of a variety of network devices from a central location, using a web-based administrator console.

- **Measure Costs**: For any device connected to the system, Surveyor can track the time spent in each power state and its energy usage. Surveyor can track Windows PCs, Macintosh computers.
- **Manage Energy**: The administration tools in Surveyor help you manage the power states of network-connected devices using direct commands and scheduled policies that you define to fit your organization's needs.
- **Optimize Savings**: Surveyor reports on the data it collects in useful charts and graphs that show device and user activity. In addition to energy consumption and savings reports, Verdiem provides a range of useful information to help manage your PC fleet.

## Surveyor Features

Surveyor provides the following key features:

| Feature | Description |
| --- | --- |
| Centralized administration | Centralized administration of device power states from a single, easy to use Web-based administrator console. |
| Agent-based power management | Agent-based, non-intrusive PC and Mac power management with minimal impact to end-users, business applications, or IT maintenance activity. |
| Direct device management | The ability to manage and control devices immediately via direct commands, or through policies and scheduled power schemes. |
| Usage data collection | The ability to collect actual usage information for computers to help you optimize intelligent power management policies. |
| Remote access and Wake on LAN support | Unhindered remote access to office computers and high performance Wake on LAN support for waking PC and Mac client agents. End users can wake Surveyor client agents from a remote location over the web and schedule strategic wake requests to work around scheduled maintenance windows. |
| Locations, energy rate schedules, and | Support for multiple location that devices can be assigned to manually or through auto-assignment rules. Each location can have associated energy costs (fixed or variable for TOU and intraday rates) in that location's currency. Reports reflect |

| Feature | Description |
|---|---|
| currencies | correct savings by automatically calculating local currencies exchange rates with the specified system currency. |
| Role-based security | Group-oriented administration with role-based security privileges. |
| Dashboards and Analytics reporting | Role-based dashboards provide actionable information on energy costs, C02 emissions, and asset inventory and health to key stakeholders. Summary reports can be emailed automatically on a scheduled basis. Analytics allow you to generate energy management and IT efficiency reports that dive-down into data based on group, location, and other categories of interest. |
| Device event reporting | Event reporting for analysis and optimization. Important events are recorded and reported to a central server. |

# Configuring Power Management in Surveyor

Power management is the ability to move devices into appropriate power states as demand requires.

A **device** in Surveyor can be a Windows PC, Macintosh computer and wireless access points (WAPs).

When devices first connect to Surveyor, they are automatically assigned the Baseline Data Collection policy. While a device uses this policy, data is collected to measure energy use and user activity; no power management settings are enforced.

Policies contain the following types of settings:

- **Scheduled power schemes** (PC and Mac only) that specify the amount of time of user inactivity before a device transitions to a lower power state. Each scheme can have a unique schedule.
- An unscheduled, **background power scheme** that runs 24/7 when no other power schemes are scheduled.
- **Scheduled power level changes** (such as wake, shutdown, sleep, or restart), each with a unique schedule. Power level changes apply to PC and Mac clients, or PoE devices.
- **Wake up settings** for PC and Mac clients.
- **Logging and data collection settings** for PC and Mac clients.

Surveyor assigns policies manually or through assignment rules that you create. Each device can have only one policy assigned to it, but each policy can contain multiple schemes and power level changes, each with its own schedule.

> **Note:** All power settings in policies apply to PC and Mac clients. For other types of devices, only scheduled power level changes apply. Surveyor collects data for all device types for reporting purposes.

Devices can be assigned to administrative **groups**, either manually or through assignment rules that you create. Groups help you to organize devices logically and aid you in applying role-based permissions for delegated administration.

Devices can also be assigned to locations, which have associated currencies and energy rate schedules. For more details, see *Chapter 5: Managing Locations, Energy Rates, and Currency on page 5-1*.

For general steps, see "Getting started with power management" in the *Surveyor 6 Administrator Guide*.

## Surveyor System Components

In a basic installation for PC and Mac power management, the Surveyor system comprises the following components:
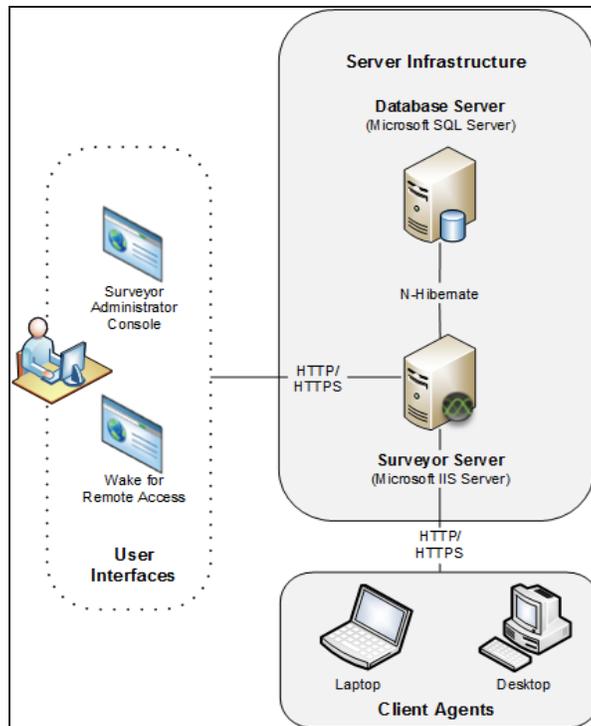


| Component | Description |
|---|---|
| Surveyor Server | Manages policy distribution, sends power state change instructions to client devices, and captures data to send to the Surveyor database. |
| Database | A Microsoft SQL Server database that stores power state and other device data sent |

| Component | Description |
|---|---|
| Server | to the server. |
| Administrator Web Server | A computer running Microsoft IIS. The Administrator console is a web application hosted on an IIS server. You use the Administrator console to configure and schedule power state changes; add, arrange, remove, and monitor devices; manage and delegate permissions; and perform other management tasks. |
| Client Agents | Desktop and laptop Windows PC and Macintosh computers (referred to as clients or client agents) that receive and enforce power management instructions from the Surveyor server. |

# Getting Started with Surveyor and Power Management

Provides a suggested workflow for how to collect baseline data on devices and then configure power management settings in Surveyor.

## Setting Up Power Management in Surveyor

The Administrator console in Surveyor helps you to see how devices are using energy in your organization, and allows you to set up policies with scheduled power schemes to enforce power management.

You can set up administrative groups and power management policies in any order that you choose. But you may want to define security groups first to control administrative permissions and access to devices and power management settings in a network.

The following workflow suggests how you might consider configuring power management settings in Surveyor.

| Step | Task | Description |
|------|------|-------------|
| 1 | Open the Administrator console to view and manage devices, groups, policies, and server settings. | From the Windows Start menu, click All Programs > Verdiem > Surveyor Administrator.<br>For other details, see*Open the Administrator Console on page 1-9*. |
| 2 | View devices to get an overall picture of what devices are connecting to the system. Use different filtering and sorting options to view different sets of devices. | In the Administrator console, on the Surveyor menu ⏻, click **Devices**, and then click a group name to view its devices.<br>To filter the view, click the Search button 🔍.<br>For more details, see *View Devices and Attributes on page 4-15*. |
| 3 | Create groups and locations that reflect your needs for organizing, controlling access to, and reporting on devices. | In the Administrator console, on the Surveyor menu ⏻, click **Groups** and/or **Locations**.<br>For details, see *Overview of Administrative Groups on page 2-2* and *Configuring Permissions for Delegated Administration on page 3-2*. |
| 4 | Determine how you want to view and manage sets of devices. Assign devices to groups and locations manually or through assignment rules.<br>For locations, you can also configure energy rate schedules and corresponding | For details on groups, see *Assign Devices to Groups on page 4-19* and *Configure Group Assignment Rules on page 2-5*.<br>For details on locations, see*Chapter 5: Managing Locations, Energy Rates, and Currency on page 5-1, Add Locations for Devices on page 5-4,* |

| Step | Task | Description |
|------|------|-------------|
| | currencies. | *Manually Assign Locations for Devices on page 5-7* and *Automatically Assign Locations for Devices on page 5-8*. |
| 5 | Configure security settings to control administrator access to devices and policies (optional). | To configure security settings:<br>In the Administrator console, on the Configure menu ⚙, click **Roles** & **Permissions**.<br>For details, see *Configuring Permissions for Delegated Administration on page 3-2*. |
| 6 | Run Surveyor with devices using the Baseline Data Collection policy for at least two weeks to monitor energy usage. Then, view the **Activity: Computer Power States** report to determine policy assignment.<br><br>! **Important:** Verdiem recommends that you assign the Baseline Data Collection policy for a minimum of two work weeks to all new devices connecting to the Surveyor system.<br><br>This practice ensures the most accurate measurements and calculations of energy use and savings when power management policies are enforced. | 1. Run data summarization.<br><br>! **Important:** To view data for reports, you must first run the summarization process. For details, see *About Data Summarization on page 9-18*.<br><br>2. In the Administrator console, on the Surveyor menu ⏻, click **Analytics**.<br><br>3. *Dashboard and Analytics Reports on page 9-4*<br><br>4. Analyze the data in the report.<br><br>5. Use the **Activity: Computer Power States** report to determine the start and end date for your baseline period, or determine the percentages of time per day that devices are in the On, Sleep, or Off power states.<br><br>You can then use these numbers to set the baseline value for each device. For details, see *#unique_21*. |
| 7 | Determine the policies you need to enforce power management in your organization. Modify existing policies or create new ones to meet your needs. | In the Administrator console, on the Surveyor menu ⏻, click **Policies**, and then click a group to view the policies in that group that you have permission to edit.<br>Select a policy and edit the policy settings and schedule including schemes, power level changes, and power state transition rules. For details, see *Create and Edit Policies on page 6-12*, *Create and Edit Power Schemes on page 6-20*, |

| Step | Task | Description |
|------|------|-------------|
| | | and *Create and Edit Power State Transition Rules on page 1*. |
| 8 | When you are ready to start enforcing power management settings on devices, assign policies to devices manually or through assignment rules.<br><br>Begin policy enforcement by changing the device policy from Baseline Data Collection to another policy that enforces power management settings. | **To assign policies to devices manually**:<br><br>1. In the Administrator console, on the Verdiem menu ⏻, click Devices, and then click a group to view the devices assigned to that group.<br><br> Or, in the Administrator console, click the Search button 🔍 and filter the device view.<br><br>2. Select a device or set of devices.<br><br>3. Right-click a device (or a multi-selected set of devices), and then click **Manually Assign Policy**.<br><br>For more details, see *Assign Policies to Devices on page 4-20*.<br><br>**To assign policies to devices automatically:**<br><br>In the Administrator console, on the Configure menu ⚙, click **Auto Policy Assignment Rules**.<br><br>For details, see *Configure Policy Assignment Rules on page 6-14*. |
| 9 | Review reports on user and device activity to fine tune group and policy assignment.<br><br>❗ **Important:** To view data for reports, the data summarization process must run on a regular basis. For details, see *About Data Summarization on page 9-18*. | In the Administrator console, on the Verdiem menu ⏻, click **Analytics**, **Dasbhoard**, or **Devices > Device Events**.<br><br>For details, see *Overview - Reports on page 9-2*. |

# Open the Administrator Console

You use the Administrator console to configure and schedule power state changes; add, arrange, remove, and monitor devices; manage and delegate permissions; and perform other management tasks.

- From the Windows Start menu, click All Programs > Verdiem > Surveyor Administrator.

  If the Administrator console does not open, you may need to enable ASP.NET in IIS. For details, see Application Services and UI issues in the Surveyor Knowledge Base.

  > **Note:** If Windows Firewall is enabled on the Surveyor server, you will need to make sure TCP port 80 is added to the exceptions list. For details see *Configure Windows Firewall to Allow Web Components to Access the Server on page 12-5*.

- (Optionally) In your web browser, enter the URL for the local web site on the computer where you installed the Surveyor server, such as http://hostname/AdminUI/ where *hostname* = Surveyor power management server name.

  For example, http://localhost/AdminUI/ or

  http://myComputerName.myDomain.local/AdminUI/.

# Power Management for Windows PCs

An overview of the history and common issues in Windows PC power management.

## Overview of Windows PC Power Management

Everyone understands that computers, monitors, and other devices use energy when they are on. A typical Windows desktop PC consumes 60-120 watts of electricity (500 – 800kWh annually) when it is on and being used actively.

However, advancements over the past decade in Windows operating systems and device hardware make it possible to control how much energy is used by placing computers and monitors into lower power states when they are not being used actively, or even by turning computers and monitors off and on as needed from a central location.

Power management is the ability to move devices into appropriate power states as demand requires. It doesn't just mean putting devices into lower power states. It means putting them into the right power state for your organization's needs. For example, on is quite often the right power state for a device. Successfully waking a computer at the correct time can be just as important as putting it to sleep at the right time.

By using a power management solution such as Verdiem Surveyor, you can become more aware of the amount of energy used by the computers and other devices in your organization, and then make informed decisions about managing the power states of network-connected devices in a way that reduces energy consumption without disrupting people's work activity.

## Who needs Power Management

Default power option settings in various versions of Windows are only the beginning of power management. The biggest limitation of these settings is that they don't run according to schedule: they are always in effect. As a result, many users choose to turn off these settings completely to avoid any possible work disruption.

Studies show that, in the time that a computer is on during the work day, it's only used actively for a portion of that time. Studies also show that many people do not turn their computers off at the end of the day – another big opportunity for energy and money savings.

During a full work day, and over night, there are many opportunities to put a computer into a lower power state when the computer is not in use.

IT groups also need a reliable way to install updates to computers. Installing patches and maintaining software during the day can be disruptive, but leaving computers on at night when a patching window only takes a small portion of that time wastes a lot of energy.

The ability to centrally control computers is also a big benefit of using power management software through a network. IT groups can rely on scheduled power state transitions to wake computers for patch maintenance, restart computers at the end of the window, and then return

to power management settings for reduced energy use when very few people are using their computers.

# A Brief History of PC Power Management and the Windows Idle Timer

In 1996, Intel, Microsoft, and Toshiba introduced the ACPI standard for Windows PCs. This standard made it possible for operating systems to support lower power states (various levels of sleep states) and offered faster recovery time than turning a PC off.

The Windows idle timer monitors idle activity on a PC. When the idle timer deems a system idle for a specified amount of time—based on different activity thresholds—Windows transitions the PC into a lower power state.

The activity thresholds that the idle timer uses vary, depending on the version of the Windows operating system.

| Version | Activities and thresholds used by the idle timer | Factors that determine PC behavior |
|---|---|---|
| Windows 98, Windows 2000 | Disk activity (spinning, disk use) CPU processor activity Keyboard touch Mouse movement | Activity thresholds are set at high levels that prevent machines from transitioning to lower states. Older hardware doesn't support the idle timer. |
| Windows XP | Disk activity (spinning, disk use) CPU processor activity Keyboard touch Mouse movement | Activity thresholds are set to lower levels than Windows 2000, but false positives for a PC being "in use" are still possible. |
| Windows Vista | CPU processor activity Keyboard touch Mouse movement | No longer monitors disk activity. Activity thresholds are set lower than Windows XP. |
| Windows 7 | Keyboard touch Mouse movement | No longer monitors disk or CPU processor activity. Application developers can write to a facility in Windows 7 to ensure the computer stays awake during application operations. |

The Windows idle timer was developed to specify the activity measures that determine when a PC should go into a lower power state. When applications are active, they can make a resource call to the operating system and lock the idle timer. However, many applications do not contain this functionality in their code. Because many applications are controlled less intelligently by very general settings in the operating system, PCs do not transition to lower power states as often as they should.

# The Windows Idle Timer and User Activity

The difficulty of using the Windows idle timer for power management lies with correctly determining when a computer is actually in use. Keyboard and mouse activity are always clear indicators that the machine is in use. When these indicators are missing, an application must rely on ambiguous indicators such as CPU or disk utilization, which makes it more difficult to determine whether the machine is idle or in use.

One common problem leading to an incorrect idle determination occurs when a user is using the PC actively (such as reading a long article), but isn't moving the mouse or pressing keyboard for a long time. This issue can usually be resolved in setting sleep timeout to a longer period of time ( > 1 hour) during daytime work hours.

An application can also incorrectly determine that a PC is idle and transition to sleep when an automatic maintenance application (such as a virus checker or software update) runs.

Using secondary indicators for usage like a CPU or disk utilization threshold can alleviate this problem, but can also easily interfere with power savings, because there is no way to define the processes running on a computer that are doing useful work.

For example, it is common for animations running in an open web browser to generate enough activity to reset the timer countdown and keep the machine awake. The thresholds for CPU and disk utilization are not configurable in most versions of Windows, only on Vista.

# About PC Power States and Sleep

The power states that Surveyor monitors for PCs include: on, idle, sleep, hibernate, and off.

When a PC is on and being used actively, it consumes 60-250 watts of electricity. When you want to put a computer into a low power state, you have the following options:

- **Sleep** (also called Standby): Uses the least amount of power while leaving the computer turned on. Programs or documents that are open are written to computer memory and remain open while the computer is in sleep mode. When you return and wake the computer, you can pick up where you left off.

- **Hibernate**: Saves open documents to the disk, closes programs, and then turns off the computer. On most computers, you can wake the computer and resume working by pressing the power button.

- **Off**: All programs are closed, the operating system is shut down, and the computer is powered off. The operating system and all programs must be restarted when the computer is turned on.

  In the Off state, most modern machines use a small amount of power is for the network card to listen for a Wake on LAN magic packet.

The following table shows the pros and cons of low power states as they relate to power management.

**Table 1-2  Sleep (or Standby)**

| Pros | Cons |
|---|---|
| • Generally supported by software developed after 2005 and hardware manufactured after 2005.<br>• Data for open applications is loaded into RAM enabling faster waking from standby<br>• Waking the system from this state is easy (through mouse or keyboard).<br>• Wake from standby can be scheduled or done through Wake on LAN.<br>• Applications generally don't block standby transitions. | • Uses slightly more energy than other low power states (1-2 W).<br>• Potential data loss in the event of a power outage. |

**Table 1-3  Hibernate**

| Pros | Cons |
|---|---|
| • Increased energy savings over standby.<br>• Data loss less likely in a power outage, because information is stored on the physical drive. | • Errors can occur in some software when the computer goes into the hibernate state.<br>• Not all hardware fully supports this state.<br>• Most computers can wake from hibernate only through Wake on LAN. However, scheduled wakes are possible for some computers.<br>• Because data is no longer loaded into RAM, waking from this state is slower than from standby.<br>• User wakes the computer by pressing the power button. |

**Table 1-4  Power off**

| Pros | Cons |
|---|---|
| • Some increased energy savings over standby and hibernate. | • Potential data loss when shutting down open applications (if using a forced shutdown).<br>• System might not shut down if blocked by an application (if not using forced shutdown).<br>• Computers can wake only through Wake on LAN.<br>• Because data is stored on physical drive space, waking from this state is slower than from standby. |

**Table 1-4  Power off (continued)**

| Pros | Cons |
|---|---|
|  | • User wakes the computer by pressing the power button. |

# The Benefits of Transitioning to Sleep

Although the off and hibernate states provide some increased energy savings over sleep (known as standby in Windows XP), the savings are so insignificant that the disadvantages far outweigh the savings. Wake and network issues are common when the computers have been set to Hibernate or Off.

To get a clearer idea of the trivial differences in savings, here is energy usage data based on manufacturer specs of 100 systems:

- Standby: 3-5 W
- Hibernate: 2-3 W
- Off: 2-3 W

When a computer or any device goes into a lower power state, users expect it to wake up quickly as soon as they try to access it. Using policies that transition PCs to sleep offer the fastest wake up experience for users and significant energy savings over time, while having the least impact on productivity.

# Keys to Intelligent Power Management

Smart power management starts with:

- Understanding PC power states and how they affect PC energy consumption.
- Knowing how much energy PCs and devices in your organization use, why, and at what times of day users are most active.

Surveyor helps you gather data on the energy use and user activity in your organization and reports on that energy use to help you determine your organization's baseline, which is the amount of energy used by PCs and network devices before centralized power management has been implemented and enforced.

After you determine your baseline energy use, you can assess daily and weekly usage patterns to determine what policies should be enforced at particular times of the day and week.

The policies you enforce should reduce energy consumption, yet not interfere with user productivity or IT software maintenance windows. Surveyor allows you to apply power settings on a scheduled basis to gracefully transition PCs into low power states based on inactivity.

# Addressing Windows PC Insomnia through the Surveyor Idle Timer

This topic describes why Windows might not recognize that a computer is inactive, and how to ensure that clients transition to standby even if Windows does not recognize that the computer is idle.

## About PC Insomnia

PC insomnia is a condition in which a computer initiates a low power state, but something on the system erroneously keeps the computer awake. PC insomnia can diminish the integrity of your overall power management plan, because it keeps affected computers running on full power at all times. In the case of laptops, it can also be inconvenient, causing batteries to run out when the computer is not in use; or dangerous, causing overheating and hard disk damage.

> **Note:** For information on insomnia and the sleep timer on Macintosh computers, see *About Mac OS X Power Management on page 1-17*.

## About the Windows Idle Timer

Within Windows is a tool called an idle timer which monitors idle activity on your PC and, when the idle timer deems a system idle for a specified amount of time, Windows moves the PC into a lower power state (such as sleep mode).

The lack of sleeping (PC insomnia) is generally caused by various applications and processes that can reset the Windows idle timer. Some common examples include search archiving, virus scans, backup processes, and interactive Web pages. Media applications, when running, are also common examples of items that can keep a computer awake.

## PC Insomnia Causes

A variety of conditions can cause PC insomnia, including the following:

- **Software**: Programs running in the background, such as media players or virus scanners. Terminal emulation software, media players, and some custom-developed applications may not allow the system to enter a lower power state. Also includes legacy software that remains on the disk image, such as video card adapters.
- **Custom Device Drivers**: Device drivers not written to the Advanced Configuration & Power Interface (ACPI) specification may not allow the PC to enter lower power states.
- **Network activity and traffic**: Numerous services or agents within a PC image of an enterprise may spike CPU activity during periods of inactivity, causing the Windows idle timer to reset.

# How Surveyor Resolves PC Insomnia

The Surveyor idle timer helps to ensure accurate and predictable sleep transitions. When you enable it, you configure it to do the following:

- Ignore false activity reports. Client computers transition to low power states at the right time, even if the Windows idle timer does not recognize that they are inactive.
- Recognize applications and other activity that always report a true active state. This prevents computers from transitioning to a low power state if they run critical applications.

The idle timer provides options for:

- Tracking CPU usage to determine inactivity and setting the CPU activity threshold.
- Tracking disk usage to determine inactivity and setting the disk activity threshold.
- Tracking network usage to determine inactivity and setting the network activity threshold.
- Displaying a message to users before transitioning to sleep.

**Note:** Options for tracking CPU usage, disk usage, or network usage to determine inactivity apply to Windows PCs only.

**Important:** The Surveyor idle timer is enabled by default in schemes. The Surveyor idle timer must be enabled to use power state transition rules in a scheme.

# About Mac OS X Power Management

A brief overview of Mac power states.

Mac OS X computers can transition to or from the following power states:

- sleep
- wake
- shutdown or restart

The type of sleep state the computer transitions to depends primarily on user or system activity.

> **Note:** Mac OS X does not support Wake on WAN/LAN from the off state (only from sleep). For details, see Mac OS X v10.6: About Wake on Demand.

| Sleep type | Description |
|---|---|
| Idle sleep, including:<br><br>- Display sleep<br>- Hard disk sleep | Occurs when there has been no activity during the time interval the user selects in the Energy Saver preferences (tracked by the computer's sleep timer).<br><br>To wake a computer from idle sleep, the user can move the mouse, touch the trackpad, or press a key on the keyboard. |
| System sleep | Occurs when the user chooses Sleep from the Apple menu or closes the lid of a laptop.<br><br>To wake the computer from system sleep, the user can open the lid of a laptop or briefly press the power button. |

# Additional Information and Troubleshooting

A number of issues can cause a Mac to not remain in sleep mode as expected. For comprehensive information about troubleshooting these issues, the Mac sleep states, and the sleep timer, see Why your Mac might not sleep or stay in sleep mode on the Apple support site.

# System Settings and Descriptions

The table in this topic contains settings from System Settings page.

## Display the Server Settings

To access the settings, in the Surveyor Administrator console, on the Configure menu ⚙️, click System Settings.

## System Settings

These settings originate at the server and affect anyone using the Administrator console, whether locally or remotely.

| Setting | Description |
|---------|-------------|
| Maximum number of devices returned per view | Sets the maximum number of devices to display in device lists or reports, given the currently selected group or search parameters. <br><br> A status message on the Devices page indicates the number of devices being shown in the current tab. If more devices exist than those that appear in the list, the status message also indicates the total number of devices. <br><br> **Recommended setting**: The same number as the number of devices in your largest Surveyor group. <br><br> **Note:** Setting this to a large number of devices (thousands) might affect viewing or browsing performance. |
| When Surveyor wakes devices | **Batch devices into sets of *X*** <br> The number of clients to wake in one batch. Each subsequent wake batch is sent after the specified number of seconds. The default value is 500 clients. <br> **Wait *X* seconds before sending next request** <br> The number of seconds to wait after sending a wake job before sending the next one. This parameter takes effect if you set the wake batch size to a number that's less than the total number of clients to wake. The default value is 60 seconds. |
| Devices should check in every X minutes | The amount of time that the client device waits before checking with the server again for power-state updates. The default value is 10 minutes. |
| Number of computers to keep awake as Wake on WAN proxies | The number of PC clients in each subnet to keep awake at all times to receive magic packet requests from the server and relay them to the other clients in their broadcast segment. This setting takes effect only if you enable Wake on WAN. By default, this is set to 2 proxies. <br> It is preferred to set this as 2 proxies. |
| Keep detailed diagnostics | The number of days that data on device diagnostic events are stored. The default is 7. |

| Setting | Description |
|---|---|
| device data for X days | |
| Keep device wake job data for X days | The number of days that data on client wake jobs are stored. Storing wake job data for 1 month is usually sufficient for troubleshooting purposes. The default is 45 days. |
| Keep detailed reporting device data for X days | The number of days for which historical reporting data on devices is stored. The default is 2000. Keeping historical data improves the information available for device-specific reports. |
| Keep detailed hourly reporting device data for X days | The number of days that detailed hourly data on client reporting data is stored. Storing reporting data improves the information available for device-specific reports. The separate setting for reporting device data allows for lower granularity data to be retained for a longer period, lessening the data storage impact. The default is 60 days. |
| Reclaim licenses for inactive devices after X days | The number of days since last check in after which a device's license can be claimed for use by a different device. The default is 30 days. |
| Policy assignment rules run | Specifies when assignment rules will and can run: On each connection and on demand, On first connection and on demand, Only on demand. |
| Group assignment rules run | Specifies when assignment rules will run: On each connection and on demand, On first connection and on demand, Only on demand. |
| Location assignment rules run | Specifies when assignment rules will run: On each connection and on demand, On first connection and on demand, Only on demand. |

# Browser Cookie Settings

When you use the Administrator console remotely, you can set some display behavior on your own computer, without affecting others using the console.

| Setting | Description |
|---|---|
| Hide unlicensed devices in device lists | When selected, unlicensed devices are hidden in devices lists. |
| Number of devices returned per view | **Use server default setting**<br>When selected, Surveyor uses the system setting for **Maximum number of devices returned per view** (described above). To specify a local preference |

| Setting | Description |
|---|---|
|  | for the Administrator console (saved in a cookie for the current browser session), select **Return** and then specify a different number.<br><br>**Note:** Setting this to a large number of devices (thousands) might affect viewing or browsing performance. |

# Default Baseline Section

The default baseline settings determine the baseline values that are used by default for individual devices. To change a device's baseline settings, see *Set the Baseline Value for a Device on page 4-22*.

| Setting | Description |
|---|---|
| System is On | Percentage of time during a reporting period in which a computer was on. |
| System is Off | Percentage of time during a reporting period in which a computer was on. |
| Display is On | Percentage of time during a reporting period in which a display was on. |
| Display is Off | Percentage of time during a reporting period in which a display was off. |
| System is Asleep | Percentage of time during a reporting period in which a computer was asleep. |

# 2

# Managing Administrative Groups

**Table 2-1  In this Chapter**

| Topics |
| --- |
| *Overview of Administrative Groups* |
| *Create Administrative Groups* |
| *Assign Devices to Groups* |
| *Configure Group Assignment Rules* |

# Overview of Administrative Groups

This section includes information on strategies for creating groups, how to create and edit groups, and how to configure rules for assigning devices to groups automatically.

Groups in Surveyor serve two important functions by providing:

- A mechanism for role-based system security that allows you to assign group-level permissions and control administrator access to devices.

    For more details on role-based security and group-level permissions, see *Configuring Permissions for Delegated Administration on page 3-2*.

- A logical way for you to organize the devices in the system to easily access and manage sets of devices.

Devices can be assigned to groups, either manually or through assignment rules that you create (see *Assign Devices to Groups on page 4-19* and *Configure Group Assignment Rules on page 2-5*. Policies and groups have no direct relationship; you can assign policies to devices, but not to groups.

You create groups on the Groups page (see *Create Administrative Groups on the next page*). When you create a group, you can specify a parent group to create nested groups.

Surveyor provides a root My Organization group and a Default Group to start with. New devices that connect to the server and don't otherwise meet any group assignment rules that you've set up appear in the Default Group.

## Strategies for Creating Groups

When you create groups for devices, you'll want to consider how you are planning to apply security and role-based permissions for the groups.

You might create groups based on geographic location or a particular business function, such as distributed administration. For example, you could create a Help Desk group that can wake or restart computers as needed.

How you ultimately refine your group structure in the full Surveyor deployment depends on the needs of your particular organization.

You will likely determine your initial security groups during the two-week period in which devices connected to Surveyor are using the Baseline Data Collection policy. After you set up your initial security groups, you can then set assignment rules so that computers and other devices are placed into groups as they're added to the system. For details, see *Configure Group Assignment Rules on page 2-5*.

# Create Administrative Groups

When you create a group, you can specify a parent group to create nested groups.

1. In the Administrator console, click the Surveyor button ⏻, and then click **Groups**.

2. On the Groups page, click **New Group**.

3. Type a name for the group, a description, and then select a parent for the group.

4. Click **Save**.

# Assign Devices to Groups

You can assign devices to groups manually from the device list view, or automatically using group assignment rules. For details on configuring group assignment rules, see *Configure Group Assignment Rules on the next page*.

For details on creating groups, see *Create Administrative Groups on the previous page*.

1. In the Administrator console, click the Search button 🔍 and filter the device view to see the devices your want to assign to a group.

2. Select the device or devices in the resulting list.

3. On the **Item Actions** menu, click **Manually Assign Group** or **Use Group Assignment Rules**.

   > **Note:** When you manually assign a policy to a device, it is automatically flagged as being manually assigned. To clear the manually assigned flag, you must select the device from the device list, and then on the **Item Actions** menu, click **Use Group Assignment Rules**.
   > If you choose **Use Group Assignment Rules** and one or more of the selected devices was manually assigned (previously), you will need to select the option **Include *N* manually assigned devices** and then click **OK** to confirm that you want to change from a manually assigned group to rule-based assignment.

4. For manual assignment: Click the group name, and then click **OK**. For rule-based assignment, click **OK**.

# Configure Group Assignment Rules

After you create groups, you can configure Surveyor to place new devices automatically into the appropriate groups when the devices connect to the server.

When you configure group assignment rules, devices are automatically assigned to specific groups based on a set of criteria. For example, you can create a rule for a Training Lab group that accepts clients only from a particular IP segment and with the string 'train' in their DNS names.

Because rules that you set up for automatically assigning devices to a group are saved as a set, their order is important and you will need to consider the best order to get the results you want.

You have the option to automatically run the rule set only when new devices connect, or for all connections, which means that rules will be run whenever a device wakes or whenever the device moves from one network card to another, such as a computer moving from a network line to a wireless connection.

Each rule can then contain a set of conditions that a device must meet to be placed into the group. When you connect new devices to the server, only the devices that comply with a group's conditions can be placed into that group.

---

**Note:** If a device meets the conditions in a specific rule, the device is placed into the rule's target group and Surveyor does not check the conditions defined in any other subsequent rules.

If a device does not meet any conditions of a rule set, you have the option to leave the group for the device unchanged, or to assign a device to the Default Group.

If devices do not meet any of the conditions listed above:

○ Leave location unchanged

◉ Assign location Default Location

---

1. In the Administrator console, on the Configure menu ⚙, click **Auto Group Assignment Rules**.

2. Click **New Rule**. Type a name and a description for the rule, and then select the name of the group to be assigned when the rule runs.

3. Add conditions as needed.

   As you add conditions, you can test what the result will be by clicking the **Test Rule** tab.

4. Specify whether the rule should be enforced when all conditions are satisfied, or when any condition is satisfied.

5. Specify whether the rule should be run automatically when new devices connect to the server, or when all devices connect to the server.

> **Note:** With **All connections**, the rules run whenever a computer wakes up or whenever a computer moves from one network card to another (such as from a network line to a wireless connection or back).

6. Click **Save** to save all changes.

7. Reorder rules by selecting a rule in the set and then clicking **Move Up** or **Move Down**.

# 3

# Security and Permissions in the Surveyor Deployment

**Table 3-1  In this Chapter**

| Topics |
| --- |
| Configuring Permissions for Delegated Administration |
| Grant Root Administrator Permissions |
| Grant Rate Administrator Permissions |
| Create Additional Security Roles and Grant Permissions |
| Administrative Permissions and Descriptions |
| Configure Windows Firewall to Allow Web Components to Access the Server |

# Configuring Permissions for Delegated Administration

This section provides information about the Surveyor role-based security model. It describes the concept of using roles for delegated administration, permissions types, how to configure permissions in roles, and how to add users to roles.

You can configure different levels of access to the Surveyor deployment. This topic briefly describes its role-based security and permissions model.

## Overview of the Role-based Security Model

Surveyor uses a role-based approach to security, following guidelines of the National Institute of Standards and Technology RBAC (role based access control) model. In this model:

- Roles are created to contain sets of permissions required to access particular administration tasks.
- To grant users access to perform the tasks, you add them to the roles that contain the required permissions.
- The Windows user or group has no direct relationship with the Surveyor task or component. Instead, roles represent business functions, such as Help Desk or Policy Administrator.

## Using Roles for Delegated Administration

A built-in Root Administrator role gives members of that role complete access to the Surveyor deployment. By default, anyone who has local administrator permissions on the Surveyor server has Root Administrator access level.

To set up delegated administration, a member of the Root Administrator role does the following in the Administrator console:

- Adds others to the built-in Administrator role by selecting them from Windows users and groups.
- Creates security roles for specific permissions sets.
- Configures system-wide or group-level permissions in the roles.
- Adds Windows users (or groups) to the roles to apply the role's permissions sets to those users.

### Permissions Categories

Security roles can include the following categories:

- **Global (server-wide)**: Permission to manage a particular area of functionality across the entire Surveyor deployment.

- **Group level**: Permission to perform specified management tasks on selected groups.

Security roles can contain global or group permissions or both types. For example, the built-in **Policy Administrator** role has Manage policies (global) permission by default. But you could also grant this role **Apply policies** permission for specific groups.

For information about each setting and determining effective permissions, see *Administrative Permissions and Descriptions on page 3-8*.

Security roles can contain global or group permissions or both types. For example, the built-in Policy Administrator role has Manage policies (global) permission by default. But you could also grant this role Apply policies permission for specific groups.

For information about each setting and determining effective permissions, see *Administrative Permissions and Descriptions on page 3-8*.

# Grant Root Administrator Permissions

A user or group that has root administrator permissions is granted access to all tasks and groups in the system.

To complete this procedure, you must have local administrator permissions on the Surveyor server computer.

1. In the Administrator console, on the Configure menu ⚙, click Roles & Permissions.

2. In the list of roles on the Security Permissions page, select Root Administrator.

3. On the Users tab, for each Windows user or group that you want to include in the role, click Add User or Group to find and select the user.

    📝 **Note:** Search operations are limited to the current domain, even if your user account has access to multiple domains. If you specify a different domain, the search returns a "user not found" message.

4. When you're done adding users to the Root Administrator role, click Save.

**Search Notes**

- Search operations are limited to the current domain, even if you are logged in as a user who has access to multiple domains. If you specify a different domain, the search returns a "user not found" message.

- Search results return users and groups that contain the search string you enter, and wildcard characters * and ? are treated as text characters.

- Search operations are case-insensitive for finding domain users and case-sensitive for finding local users. For example:

    Searching for admin returns

    - DOMAIN\Admin2 (domain user)
    - DOMAIN\Administrator (domain user)

    Searching for Admin returns

    - DOMAIN\Admin2 (domain user)
    - DOMAIN\Administrator (domain user)
    - BUILTIN\Administrators (local group)
    - Administrator (local user)

# Grant Rate Administrator Permissions

A user or group that has rate administrator permissions is granted access to define energy rates for each location. A user or group with only Rate Administrator permissions will not be able to perform any other actions.

To complete this procedure, you must have local administrator permissions on the Surveyor server.

To create a new Rate Administrator Role:

1. In the Administrator console, on the Configure menu ⚙, click **Roles & Permissions**.
2. Click **New Role.**
3. Enter appropriate information in the **Role** and **Description** fields.
4. Click the **Global Permissions** tab and select **Can make changes to Rates**.
5. Click **Save**.

To add user or group as Rate Administrator:

1. In the Administrator console, on the Configure menu ⚙, click **Roles & Permissions**.
2. On the **Users** tab, for each Windows user or group that you want to include in the role, click **Add User or Group** to find and select the user.

   > **Note:** Search operations are limited to the current domain, even if your user account has access to multiple domains. If you specify a different domain, the search returns a "user not found" message.

3. When you're done adding users to the Rate Administrator role, click **Save**.

**Search Notes**

- Search results return users and groups that contain the search string you enter, and wildcard characters **\*** and **?** are treated as text characters.
- Search operations are not case-sensitive for finding domain users and case-sensitive for finding local users. For example:

  Searching for admin returns:

  - DOMAIN\Admin2 (domain user)
  - DOMAIN\Administrator (domain user)

  Searching for Admin returns:

  - DOMAIN\Admin2 (domain user)
  - DOMAIN\Administrator (domain user)

- BUILTIN\Administrators (local group)

- Administrator (local user)

# Create Additional Security Roles and Grant Permissions

To grant access to perform administrative tasks, you create security roles, configure permissions sets for each role, and then add users to the appropriate roles.

Before you complete this procedure, become familiar with the topic *Configuring Permissions for Delegated Administration on page 3-2*.

In addition, this procedure must be completed by a local administrator of the Surveyor server who is also a member of the Root Administrator role in the Surveyor Administrator console.

1. In the Administrator console, on the Configure menu ⚙️, and then click **Roles** & **Permissions**.

2. Click **New Role**, or select an existing role to customize or copy.

   If you create or copy a role, give the new role a name and description.

   | Role: | Help Desk |
   | --- | --- |
   | Description: | End user PC support |

3. On the **Users** tab, for each Windows user or group that you want to include in the role, click **Add User or Group** to find and select the user.

   > **Note:** Search operations are limited to the current domain, even if your user account has access to multiple domains. If you specify a different domain, the search returns a "user not found" message.

4. Configure permissions for this role. For details about what each permission level gives access to, see *Administrative Permissions and Descriptions on the next page*.

   a. On the **Group Permissions** tab, expand the tree to display the groups that you want this role to have access to, and then select the appropriate permissions.

      > **Note:** When you enable permissions on a group, they are enabled also on its subgroups.

   b. On the **Global Permissions** tab, if you want this role to have access to policies or group assignment rules across the entire system (independent from group-level permissions), select the appropriate check box.

      Skip this step to grant only group-level permissions.

5. When you complete assigning permissions, click **Save**.

# Administrative Permissions and Descriptions

This topic defines the permission types that you can enable across the system or on specific device groups to set up a delegated administration environment.

## Permission Types

You can assign the following permission types to roles that you create in the Administrator console:

- **Global (server-wide)**: Permission to manage a particular area of functionality across the entire Surveyor deployment.
- **Group level**: Permission to perform specified management tasks on selected groups.

For example, a Policy Administrator role might be granted permission to create and edit policies across the system, but not to apply policies to devices. A Help Desk role might have permission only to change the power state of devices in specific groups.

### Global Permissions

In the Administrator console, you can grant administrative permissions across the entire Surveyor deployment.

- **Manage group assignment rules**: Permission to create, modify, or delete group assignment rules and conditions, which are designed to move devices from one location in the organizational tree to another.
- **Manage power estimates for summarization**: Permission to edit the watt draw values on the Device Power Draws page, and also to resummarize data used for reports.
- **Manage energy rates**: Permission to define energy rates for each location on the Locations page.

Global permissions can effectively expand a role's access to some group-level tasks. For information, see *Effective Permissions on the next page*.

> ⚠ **Caution:** Global permissions grant access to the selected area over the entire Surveyor deployment. If you have these permissions, consider changes carefully and only after you have a clear understanding of how those changes will affect existing policies and devices.

### Group Permissions

The table below describes the levels of access that you can allow on specific groups.

> 📝 **Note:** Permissions that you enable on a group are inherited on all of its subgroups.

| Permission | Access level that it allows |
|---|---|
| View group | View devices and their attributes in a group and its subgroups. |
| Manage group | Add, remove, and edit settings on groups or its subgroups, as well as remove devices from them (for example, renaming a group or changing its parent). <br><br> Does not give access to policies. <br><br> You can move devices from one group to another when you have Manage groups permission for both groups. <br><br> The exception to this is that you can manually run group assignment rules for a set of devices if you have Manage groups permission on the source group but not the destination group (as defined in the rule's conditions). |
| Assign policy | Assign policies to new devices; assign different policies to existing devices. <br><br> Does not give access to create, modify, or delete policies. |
| Manage policy | Create, modify, or delete policies for a group and its subgroups. |
| Wake devices | Wake specified devices from a low power state. This is the standard permission level for the user that runs the Wake for Remote Access service. You might also grant Help Desk staff this permission level. <br><br> If you want to allow someone transition devices to low power states as well, use the **Change device state** level. |
| Change state | Perform any type of power state change on devices; for example, wake, transition to sleep. |
| Edit devices | Change device properties, such as whether a device can receive a license, and its description. <br><br> Does not give access to policies. |

## Effective Permissions

If a user is a member of multiple roles, the effective permissions that the user has on a group is the set that provides the highest level of access. This is true whether the role is given permissions directly on the group or indirectly through inheritance from an ancestor group.

In addition, sometimes having global permissions for an area can effectively expand group-level permissions, as in the following example.

Enabling global permissions set **Manage group assignment rules** gives access to create rules that move any device to any location in the organizational tree. Moving devices among groups is considered a "management" task that can be done through this global permissions set even if the **Manage group** permission is not enabled at the group level.

# Configure Windows Firewall to Allow Web Components to Access the Server

If you use Surveyor components that access the server through http, and Windows Firewall is enabled on the server, make sure TCP port 80 and port 443 is added to the exceptions list.

You would need to access the server through http if you do any of the following:

- Enable Wake for Remote Access for your end users to wake their computers from home or another off-site location.

  Wake for Remote Access is an add-on component that comes with Surveyor. For information see the Wake for Remote Access Guide.

- Administer the server from a remote computer; for example, as you would if you set up delegated administration.

1. On the server computer, navigate to **Windows Start menu / Control Panel / Windows Firewall**.
2. On the **Exceptions** tab, click **Add Port**.
3. In the Add a Port dialog box, do the following:

   a. Type a name that indicates that the exception is for power management components. (This name appears in the exceptions list.)

   b. Specify port 80 or port 443 if using an https configuration.

   c. Select TCP.

4. Click OK, and then click OK in the Windows Firewall dialog box.

For additional information, refer to the Microsoft TechNet topic Add a Port to the Firewall Rules List.

# 4

# Managing and Viewing Devices

**Table 4-1  In this Chapter**

| Topics |
| --- |
| *Overview of Device Management* |
| *View Devices and Attributes* |
| *Assign Devices to Groups* |
| *Assign Policies to Devices* |
| *Set System Default Baseline Values for Devices* |
| *Set the Baseline Value for a Device* |
| *Configure Watt Draws for Computers* |
| *Assign Unknown Devices to Device Families* |
| *Manually Control Devices* |
| *Set Device Properties and Attributes* |
| *Retire a Device from the System* |
| *Reclaim Licenses for Inactive Devices* |

**Table 4-1  In this Chapter (continued)**

| Topics |
| --- |
| *View Device Charts* |
| *View the Device Events Report* |

# Overview of Device Management

This section describes how you can search for and view devices in a comprehensive device list view, and how you can perform various tasks such as setting device attributes, changing power levels directly, and assigning devices to groups and policies.

You can view and access information on any device on the Devices page or on the Search page in the Administrator console.

A device in Surveyor can be a Windows PC or Macintosh computer, and wireless access points (WAPs).

Surveyor collects data on all devices that are connected to the system for reporting purposes. This data and reporting helps you to understand how much energy is used by devices in your organization, why, and at what times of day users are most active.

Surveyor begins collecting data for all devices as each device connects to the system. Surveyor updates this data each time a device checks in.

> **Note:** The frequency for device check-in and how Surveyor staggers check-ins is set in System Settings page under Devices should check-in every X minutes.

From the device list in the Administrator console, you can:

- View devices according to very broad or very specific search and filtering criteria. For details, see *View Devices and Attributes on page 4-15*.
- Control device power states and levels directly, outside of a policy. For details, see *Manually Control Devices on page 4-25*.
- Assign policies to devices. For details, see *Assign Policies to Devices on page 4-20*.
- Assign devices to groups. For details, see *Assign Devices to Groups on page 4-19*.
- Assign devices to locations. For details, see *Chapter 5: Managing Locations, Energy Rates, and Currency on page 5-1* and *Manually Assign Locations for Devices on page 5-7*.
- Edit PC and Mac properties.
- Manage Wake on WAN proxies.
- Run policy or group assignment rules.
- View report charts on device activity and type, policy assignment, and group membership.

## Devices, Policies, and Power Level Settings

Each device can have only one policy assigned to it, but each policy can contain multiple schemes and power state changes in the policy schedule.

> **Note:** Scheduled power schemes cannot overlap.

You can assign a policy to a device, either manually from the Item Actions menu on the Devices page or through policy assignment rules that you create.

> **Note:** All power settings in policies apply to PCs and Macs. For other types of devices, only scheduled power level changes apply. Surveyor collects data for all device types for reporting purposes.

Outside of a policy, you can apply power state changes to any device, PC and Mac device properties either individually, or as a set.

For more details, see *Overview of Policies and Power ManagementSettings on page 6-2*.

## Device Connections and Check-ins

When a device connects to the Surveyor server for the first time, or whenever a device reestablishes contact with the server after being out of contact for a specified period of time, the server and client agent exchange a series of queries and responses referred to as a handshake. During a handshake, the server:

- Sends a query for the device GUID, netBIOS, MAC address, and policy version.
- Evaluates clients as Wake on WAN proxies.
- Evaluates group and policy assignment rules.
- Compares its policy version with the policy version reported by the device.

Computers (via the proxy server) send a message to the server the first time they connect to the Surveyor server, or any time they attempt to reestablish contact with the server after being out of contact with the server for a period of time.

A computer will send this message when it: starts up, reboots, transitions out of sleep or a low power state to on, reestablishes network connectivity after being disconnected from the network (i.e., when the computer is out of contact with the server for any reason, for a period of time, and then reestablishes network connectivity).

## "Checking in" versus "Not checking in"

All devices check in with the Surveyor server based on the value set for Devices should check-in every X minutes on the System Settings page). Each time a device checks in, the server records the check-in time.

If a device misses two consecutive check-in intervals, the Surveyor server will mark the device as Not checking in. When the device begins checking in again, the Surveyor server will set the device status to Checking in again.

> **Note:** Whether a device is checking in or not checking in is not related to its power state, or whether the device is on or off. It simply is an indication of whether the device is communicating with the server.

The following table describes the communication that takes place between Surveyor and all types of devices when they connect to, and check in, with Surveyor.

| Action | Description |
|---|---|
| Connections (New and Reestablished) | • Device asks the Surveyor server for what pieces of information it should send.<br><br>• Surveyor server asks the device to send four key pieces of information: Device GUID, netBIOS, MAC address, and policy version.<br><br>  Server receives the device GUID, netBIOS, and MAC address values from the device, and then registers the device as appropriate.<br><br>  For PCs and Macs, the server uses these values to determine if the computer is new, existing, or an imaged computer that has been replicated.<br><br>• Server tells the device the check-in interval based on the interval setting in the Configure Server Settings page.<br><br>> **Note:** There are three different check-in interval settings: Device check-in, and Wake on WAN proxy check-in. Only the device check-in interval can be set on the Configure Server Settings page. The other settings are set in an Surveyor configuration file.<br><br>• Server assigns a computer to a broadcast domain based on its IP address (if new).<br><br>• Server evaluates a computer client as a candidate for Wake on WAN proxy.<br><br>• Server evaluates group and policy assignment rules.<br><br>  If the rule is set for **New connections only**, the server will evaluate the rule only on first connection. If the rule is set for **All connections**, the server will evaluate the rule every time the device reestablishes a connection with the server.<br><br>• Server compares its policy version with the policy version reported by the device. If the device policy is out of date, the server will send an updated policy to the device. |
| Check-ins (subsequent) | • Server tells the device its check-in interval.<br><br>• Server records the check-in time and flags the device status as Checking in if it was previously Not checking in.<br><br>• Devices with updated information, such as attribute changes, or power usage data, send this data to the server.<br><br>• Server evaluates group and policy assignment rules (if the rule is set for All |

| Action | Description |
|---|---|
| | connections). |
| | • Server evaluates computer clients as a candidates for Wake on WAN proxy. |
| | **Note:** When a computer client that is a Wake on WAN proxy is flagged by the server as Not checking in, Surveyor will deselect that computer client from being a proxy and search for a new Wake on WAN proxy. |
| | • Server compares its policy version with the policy version reported by the device. If the versions do not match and the device is checking in regularly, the server will send the latest policy information to the device. |
| | If a computer client or device is not actively checking in, the server will send the latest policy information the next time the client or device restarts or transitions out of a low power state and reconnects to the server. |
| Policy changes | • Whenever a policy is modified, the server will find all devices that are assigned that policy that are actively checking in, and then will put a policy change message into the server message queue for these devices to receive the next time they check in or reconnect with the server (as a result of restarting or transitioning out of a low power state). |

# Devices and Groups

A device can be assigned to one group at a time. You can assign devices to groups, either manually or through assignment rules that you create.

For details creating groups, see *Overview of Administrative Groups on page 2-2* and *Create Administrative Groups on page 2-3*.

For details on role-based security and group-level permissions, see *Configuring Permissions for Delegated Administration on page 3-2*

# Viewing Device Information

Use the Devices or Search page to access device information. You can view and search for any device based on a variety of attributes, including by group, by policy, by device family, or by subnet (computers only). All devices that meet the filter or search criteria appear in the device list view.

**Note:** By default, the device list view displays the first 2000 devices that meet the search and filter criteria. If you need to view a larger set of devices, on the Configure menu ⚙, click System Settings, and then increase the Maximum

> number of devices returned per view value. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

- Click the Customize View button on the Devices page to add columns to, or remove the columns from the view.
- Change the order of columns by dragging a column to a new position in the list view.
- Click the Distribution Charts and Status Chart tabs to see a high-level picture of device activity and membership.

> **Note:** The chart data is based on the current result set of devices being viewed in the device list (2000 by default). For a representative sample of devices in the charts, you may need to increase the **Maximum number of devices returned per view** value on the System Settings page.

> **Note:** Click one of the reports on the Surveyor ⏻ menu to view details on operational state, user activity, and event log information for devices.

# Power States and Activity

Surveyor tracks different power states for computers versus other devices. For more information on device power states and activity, see *About Power State Changes on page 6-11*.

The power states and activity that Surveyor tracks for PCs and Macs are:

- On
- Sleep
- Hibernate (tracked as Sleep)
- Off
- User active

The power states that Surveyor tracks for monitors are:

- Low power
- On
- Off

Surveyor also tracks user activity for computers, which can include mouse clicks, keyboard touches, or any type of hard disk or processor activity.

Surveyor manages the following power state changes for PCs:

- Wake
- Sleep
- Hibernate
- Shutdown
- Restart

Surveyor manages the following power state changes for Mac computers:

- Wake
- Sleep
- Hibernate

> **Note:** For Macintosh computers, Surveyor translates Hibernate to Sleep. When Surveyor puts a Mac into its low power state the Mac will write RAM to disk if "Safe Sleep" is enabled on the Mac. Macs in their low power state are reported as being in the Sleep state in Surveyor regardless of the "Safe Sleep" setting.

- Shutdown
- Restart

## Device Charts

The Distribution Charts and Status Chart tabs on the Devices page include charts that give you a high-level picture of device activity and membership based on the current result set of devices being viewed in the device list.

> **Note:** The chart data is based on the current result set of devices being viewed in the device list (2000 by default). For a representative sample of devices in the charts, you may need to increase the Maximum number of devices returned per view value on the System Settings page.

For more details on viewing device charts, see *View Device Charts on page 4-29*.

# Device Properties and Attributes

The Surveyor server stores device properties for each device that connects to the server. (Some fields may not be populated for devices in some device families.) Device properties and attributes can be viewed in the Surveyor Administrator console on the Devices page. Some device attributes are created by the server and some are reported by the device. The Surveyor agent software reports attributes for Windows PC and Macintosh computers.

## Descriptions of Properties and Attributes

> **Tip:** To view a device's properties in a scrollable window, double-click the device row. You can then page through property lists for each device by clicking the Previous and Next buttons in that window.

### Default

| Column Name | Description | Searchable |
|---|---|---|
| Assigned Group | The name of the Surveyor group that the device is assigned to. | No, but devices can be filtered based on assigned group. |
| Assigned Location | The name of the location the device is associated with. | No, but devices can be filtered based on assigned group. |
| Assigned Policy | The name of the Surveyor policy assigned to the device. | No, but devices can be filtered based on assigned policy. |
| Computer Model | The model name of the computer. For example, OptiPlex GX260. | Yes |
| Days Registered | The number of days since the first time a device connected to Surveyor. | Yes |
| Device Family | Used for reporting. Possible values: PC, Mac, IP Phone, WAP (wireless access point), Switch, Router, Router Module, iPDU, Security Camera, Unknown, Interface.<br>Unknown indicates that the device family is not supported in Surveyor. | Yes. Devices can be filtered based on device family. |
| Device Name | For PCs and Macs, this is the NetBIOS name. | Yes |

| Column Name | Description | Searchable |
|---|---|---|
| IP Address | For a PC or Mac client, switch the IP address most recently used for communication with the Surveyor server. This address is the only port that Surveyor will use to attempt wake on LAN.<br><br>Assignment rules are applied to the collection of all network adapters. | Yes |
| Last Connected | Date and time of the last complete connection. | No |
| Manufacturer | The name of the company that manufactures the computer or device. | Yes |
| OS Version | The name and version of current operating system. For example, *Windows XP Professional SP 3*. | Yes |
| Portable | **Yes** if a Windows notebook, **No** otherwise. This is a derived (computed) field, based on the values of Chassis Type and Platform Power Role. | No |
| Status Summary | The current state of a device. For PCs and Macs, the state can be: Unlicensed, Policy Pending, Applying Policy, Policy Conflict, WOW Proxy, Current.<br><br>Policy Pending indicates that a PC or Mac has not connected to Surveyor since the policy was applied. | No |
| Usage in Watts | The power draw of an entity in watts. Surveyor reads this value from a device, PC, or Mac client.<br><br>If the Caliber is *Actual*, this value varies with the actual watt usage of the device. For example, a phone uses more power when its speaker is on than when off. Usage sampled while the phone is on will be higher than when it is off. | No |

## Advanced

| Column Name | Description | Searchable |
|---|---|---|
| Baseboard Manufacturer | The name of the organization responsible for producing the physical element of the baseboard. For example, Dell Computer Corporation. | No |
| Baseboard Product | The baseboard part number defined by the manufacturer. For example, OOT606 | No |
| Baseline Assign Date | The date that a system administrator entered | No |
| Baseline Display Off Percentage | The percentage of time during the specified baseline measurement period in which a display is off. | No |

| Column Name | Description | Searchable |
|---|---|---|
| Baseline Display On Percentage | The percentage of time during the specified baseline measurement period in which a display is on. | No |
| Baseline End Date | The end date entered by a system administrator for an automatically calculated baseline period. | No |
| Baseline Off Percentage | The percentage of time during the specified baseline measurement period in which a computer is off. | No |
| Baseline On Percentage | The percentage of time during the specified baseline measurement period in which a computer is on. | No |
| Baseline Sleep Percentage | The percentage of time during the specified baseline measurement period in which a computer is asleep. | No |
| Baseline Source | DateRange, Manual, or Default | No |
| Baseline Start Date | The start date entered by a system administrator for an automatically calculated baseline period. | No |
| CPU | The processor on a PC or Mac. For example, Intel Pentium 4 CPU 2.40GHz. | Yes |
| Chassis Type | The physical container that houses the components of a computer. For example: Desktop or Laptop. | No |
| DNS Name | The fully qualified domain name of the computer. | Yes |
| Date Registered | The date on which the device first connected to Surveyor. | Yes |
| Description | A text string that describes a Windows PC or Macintosh computer client. This property is editable. | Yes |
| Device GUID | The unique identifier of the device. | No |
| LDAP Distinguished Name | Distinguished name from LDAP server. | Yes |
| Licensing Disabled | Yes indicates that licensing is disabled for the device. No indicates a license will be allocated when it is available. or no - find the description of this. <br><br> The setting is controlled by the option selected in Device Licensing for a device. | No |
| Power Platform Role | Indicates an OEM's preferred power management profile for a computer. These values are read from the Preferred_PM_Profile field of the Fixed ACPI Description Table (FADT). For example: PlatformRoleDesktop or PlatformRoleMobile. | No |

| Column Name | Description | Searchable |
|---|---|---|
| System BIOS | BIOS string text. For example, DELL - 8, 02/26/03 | No |

## Troubleshooting

| Column Name | Description | Searchable |
|---|---|---|
| Client Version | Build number of Surveyor agent software installed on a device. | Yes |
| Device Status | Indicates whether the device is checking in regularly.<br><br>Devices check in with the Surveyor server based on the value set for **Devices should check-in every X minutes** on the System Settings page). Each time the client checks in, the server records the check in time.<br><br>If a device misses two consecutive check-in intervals, the Surveyor server will mark the device as **Not checking in**. When the device begins **Checking in again**, the Surveyor server will set the device status to Checking in again.<br><br>**Note:** Whether a device is checking in or not checking in is not related to its power state, or whether the device is on or off. It simply is an indication of whether the device is communicating with the server. | No |
| Group Assignment | **Rule** indicates the group is being assigned automatically through assignment rules. **Manual** indicates the group has been assigned manually.<br><br>**Note:** When you manually assign a group to a device, it is automatically flagged as being manually assigned. To clear the manually assigned flag, you must select the device from the device list on the Manage Devices page, and then on the **Move to Group** menu, click **Use Group Assignment Rules**. | No |
| Licensed | Indicates whether the device has a valid Surveyor license. Green check mark = yes; Red X = no. | No |

| Column Name | Description | Searchable |
|---|---|---|
| MAC Address | The MAC address of the interface most recently used for communication with the server. | Yes |
| Memory (KB) | Available memory in KB. | No |
| NetBIOS Name | The basic NetBIOS name of the PC or Mac device. | Yes |
| Network Address | The unique identifier of the device on the network (at layer 3). | Yes |
| Policy Assignment | **Rule** indicates the policy is being assigned automatically through assignment rules. **Manual** indicates the policy has been assigned manually.<br><br>Note: When you manually assign a policy to a device, it is automatically flagged as being manually assigned. To clear the manually assigned flag, you must select the device from the device list on the Manage Devices page, and then on the **Assign Policies** menu, click **Use Policy Assignment Rules**. | No |
| Policy Status | Specifies whether a named policy has been retrieved from the Surveyor server and the proxy server or device has acknowledged receipt of the most current policy.<br><br>Possible values: **Delivered** or **Pending**.<br><br>**Pending** means the PC or Mac client agent server has not retrieved the most current policy yet.<br><br>**Delivered** means the PC or Mac client agent server has retrieved the most current policy from the Surveyor server.<br><br>Note: **Delivered** does not necessarily mean the policy has been completely applied. | No |
| Proxy Wake on WAN Preference | Indicates the ranking for the computer as a Wake on WAN proxy.<br><br>**Preferred**: The computer is ranked higher in proxy-selection criteria.<br><br>**Never**: The computer will never be selected as a proxy.<br><br>**Default**: Other computer attributes are used as | No |

| Column Name | Description | Searchable |
|---|---|---|
| | selection criteria only if no preferred proxies available.<br><br>The setting is controlled by an option selected in Edit Device Properties (right-click a device in list view, and then click **Edit Device Properties**.) | |
| Subnet Mask | The subnet mask (network mask and an address of a host in the network) of the broadcast domain. | No |
| Wake On WAN Proxy | A green check mark indicates the computer is operating as a Wake On WAN proxy. Only computers can be elected as proxies. | No |

# View Devices and Attributes

The Device page and Search page in Surveyor provides a view of clients and devices that you can filter as needed.

All device information and attributes can be accessed on the Devices page or Search page in the Administrator console.

- On the Devices page: View any device by its group assignment. Note that you can only view devices based on group assignment on this page.
- On the Search page: Search for and filter devices by assigned group, assigned policy, assigned location, device family, or subnet. You can view all devices, regardless of group assignment on the Search page and then filter the view as needed.

**Tip:** To view a device's properties in a scrollable window, double-click the device row. You can then page through property lists for each device by clicking the Previous and Next buttons in that window.

For a complete list of device properties and attributes and their descriptions, see *Device Properties and Attributes on page 4-9*.

**Note:** By default, the device list view displays the first 2000 devices that meet the search and filter criteria. If you need to view a larger set of devices, on the Configure button ⚙, click System Settings, and increase the Maximum number of devices returned per view value. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

# Changing the Columns or Devices in View

- Click the **Customize View** button on the Devices page to add columns to, or remove the columns from the view.
- Change the order of columns by dragging a column to a new position in the list view.
- To view only licensed devices, select the option **Hide unlicensed devices in device lists** on the System Settings page.
- Devices that appear as **Interface** in the device list view are ports with no IP phones, wireless access points, or other PoE devices plugged into them. To hide interfaces from the device list view, select the option **Include Interface device family in device lists and reports** on the System Settings page.

1. On the Surveyor menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

2. To filter the view, click the Search button 🔍.

   Select different options in the device filters to display the set of devices you want, type a search string (optional), and then click the **Search** button to view the results set in the device list .

# Control the Number of Devices Returned in List, Chart, and Report Views

This topic describes how to change the number of devices that can be displayed in Administrator console views.

By default, the device list view, chart views, and reports display the first 2000 devices that meet the search and filter criteria. If you need to view a larger set of devices increase the **Maximum number of devices returned per view** value on the System Settings page. The maximum value allowed is 20,000.

The recommended setting is the same number as the number of devices in your largest Surveyor group.

> **Note:** Setting this value to a higher number can result in longer display times.

1. In the Administrator console, on the Configure button ⚙, click **System Settings**.

2. For **Maximum number of devices returned per view**, select the number of devices.

3. Click **Save**.

# Show or Hide Unlicensed Devices in Device Lists

To view only licensed devices in device lists, select the option **Show unlicensed devices in device lists** on the System Settings page.

For information on retiring a device or disabling its licensing, see *Retire a Device from the System on page 4-27*.

1. In the Surveyor Administrator console, on the Configure menu ⚙, click **System Settings**.

2. Select or clear the **Show unlicensed devices in device lists** check box.

3. Click **Save**.

> 📝 **Note:** Refresh the browser to see the changes in the device list.

For more information on viewing devices, see *View Devices and Attributes on page 4-15*.

# Assign Devices to Groups

You can assign devices to groups manually from the device list view, or automatically using group assignment rules. For details on configuring group assignment rules, see *Configure Group Assignment Rules on page 2-5*.

For details on creating groups, see *Create Administrative Groups on page 2-3*.

1. In the Administrator console, click the Search button 🔍 and filter the device view to see the devices your want to assign to a group.

2. Select the device or devices in the resulting list.

3. On the **Item Actions** menu, click **Manually Assign Group** or **Use Group Assignment Rules**.

> **Note:** When you manually assign a policy to a device, it is automatically flagged as being manually assigned. To clear the manually assigned flag, you must select the device from the device list, and then on the **Item Actions** menu, click **Use Group Assignment Rules**.
> If you choose **Use Group Assignment Rules** and one or more of the selected devices was manually assigned (previously), you will need to select the option **Include *N* manually assigned devices** and then click **OK** to confirm that you want to change from a manually assigned group to rule-based assignment.

4. For manual assignment: Click the group name, and then click **OK**. For rule-based assignment, click **OK**.

# Assign Policies to Devices

You can assign policies to devices manually in device list view, or automatically using policy assignment rules. For details on configuring policy assignment rules, see *Configure Policy Assignment Rules on page 6-14*.

> **Note:** All power settings in policies apply to PCs and Macs. For other types of devices, only scheduled power level changes apply. Surveyor collects data for all device types for reporting purposes.

For details on creating policies, see *Create and Edit Policies on page 6-12*.

1. In the Administrator console, on the Surveyor menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

   Or, in the Administrator console, click the Search button 🔍 and filter the device view.

2. Select the device or multiple devices in the resulting list.

3. On the **Item Actions** menu, click **Manually Assign Policy** or **Use Policy Assignment Rules**.

> **Note:** When you manually assign a policy to a device, it is automatically flagged as being manually assigned. To clear the manually assigned flag, you must select the device from the device list, and then on the **Item Actions** menu, click **Use Policy Assignment Rules**.
> If you choose **Use Policy Assignment Rules** and one or more of the selected devices was manually assigned (previously), you will need to select the option **Include *N* manually assigned devices** and then click OK to confirm that you want to change from a manually assigned policy to rule-based assignment.

4. For manual assignment: Click the policy name, and then click **OK**. For rule-based assignment, click **OK**.

# Set System Default Baseline Values for Devices

The baseline values that you set in the System Settings page are used to calculate energy savings in reports when the option Use system default baseline values is selected in a device's Edit Device Baseline dialog box. Device baseline values are used in energy savings calculations for reports.

Before you enter the baseline values, you will need to determine what the values should be by following the steps in "Establishing the baseline level of energy use" in the *Surveyor 6 Installation Guide*.

1. In the Administrator console, on the Configure menu ⚙, click **System Settings**.

2. In the Default Baseline section, enter percentages for:

    - System is On
    - System is Off
    - System is Asleep
    - Display is On
    - Display is Off

3. Click **Save**.

# Set the Baseline Value for a Device

You can set the baseline values for devices automatically (using a start and end date range) or manually. Or you can use the Default Baseline settings from the System Settings page. Device baseline values are used in energy savings calculations for reports.

Before you set manual or default baseline values for a device, you will need to determine what the values should be by following the steps in "Establishing the baseline level of energy use" in the *Surveyor 6 Installation Guide*.

If you plan to use the system default baseline settings, you will first need to enter those values in the Systems Settings page. For details, see "Set system default baseline values for devices" in the *Surveyor 6 Installation Guide*.

1. In the Administrator console, on the Verdiem menu ⏻, click **Devices**, and then click a group name to view its devices.

   To filter the view, click the Search button 🔍. Select different options in the device filters to display the set of devices you want, type a search string (optional), and then click the **Search** button to view the results set in the device list.

2. Right-click a device (or a multi-selected set of devices), and then click **Edit Device Baseline**.

- (**Recommended option**) If you know the start and end dates for the baseline period, click **Auto-calculate baseline values from the data collected over time**, and then click **OK**.

- To use the default baseline settings, click **Use the system default baseline values**, and then click **OK**.

# Configure Watt Draws for Computers

To increase the accuracy of reporting, you can specify watt draw values for individual computer models on the Reporting Settings page. These values are used in the calculations for data summarization, which affect the data displayed in the Surveyor reports.

The default values for laptop and desktop computers are shown in the **Default Watt Draws** section. You can edit the watts-related fields to change the default settings.

The models in the **Power Draw By Model** section are initially seeded with the default values from the **Default Watt Draws** section. The Source column indicates whether a model is using default values or custom values that you enter in this table. Custom values override the default values.

The **Power Draw By Model** section shows the manufacturer and models of the computers that have connected to the Surveyor server. There is one row for each unique manufactured/model combination. The **Device Count** column shows how many devices of that manufacturer/model have connected.

You can improve energy consumption calculations with the least amount of work by specifying the watt draw values for only your most prevalent computer models. If a large majority of your computers represent only a few models, you need only to edit a few rows of this table to improve accuracy of energy consumption calculations.

1. In the Administrator console, on the Configure menu ⚙, click **Reporting Settings**, and then click the **Computer Energy Use** tab.

2. To set the default watt draws for laptop and desktop computers, click in a watts-related field in the **Default Watt Draws** section of the page, and then change the watt value.

3. To set specific values for specific computer models, click in a watts-related field in the **Power Draw By Model** section of the page, and then change the watt value.

4. Click **Save**.

   Changing the watt values will affect how data is summarized in Surveyor reports from the time of this change, forward. To use the new watt values for historical data as well, click the **Resummarize** button.

   For details, see *About resummarizing dataThe following settings and values affect data summarization calculations and how data is grouped and displayed in the Surveyor reports*.

# Assign Unknown Devices to Device Families

When a PoE device that Surveyor does not recognize, you can assign it to a device family.

1. On the Configure menu ⚙, click **Device Family Assignments**.

2. For each device, click the drop-down list to select the device family.

3. Click **Save**.

# Manually Control Devices

You can change the power levels of devices directly, outside of policy settings, from the device list view.

For details on enforcing power state changes within policies, see*Create and Edit Policies on page 6-12Create and Edit Policies on page 6-12.*

1. In the Administrator console, on the Surveyor menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

   Or, in the Administrator console, click the Search button 🔍 and filter the device view.

2. Select the device or devices in the resulting list view.

3. Click the **Item Actions** menu, and then select a power level.

   > **Note:** You can also right-click a device to select a power level from a context menu.

   For PCs and Macs only: If you select **Sleep**, **Shutdown**, **Restart**, you can choose whether you want to force the change in power state by selecting **Force transition**. You also can choose whether to force a transition for Wake on WAN proxies.

   > **Note:** Use **Force transition** only when absolutely necessary. Some applications may block normal Windows shutdown requests. For example, Word or Notepad may display a dialog box asking a PC user to save document changes. When you select **Force transition**, applications are prevented from blocking shutdown and any unsaved changes in the user's application will be lost.

4. For PCs and Macs only: Type and select the options you want to use for the transition (message, force transition), and then click **OK**.

   > **Note:** The options for forcing a transition or displaying a message are ignored for non-computer device families.

# Set Device Properties and Attributes

You can change device properties for PC or Mac computers (such as description, Wake on WAN) directly from the device list view in the Devices page.

For PCs and Macs, you can specify the ranking as a Wake on WAN proxy. In the Edit Device Properties dialog box, select the Wake on WAN proxy preference check box, and then select:

- Preferred increases the ranking of the selected computers in the proxy-selection criteria.
- Never prevents the selected computers from being selected as proxies.
- Default or Don't change means that other computer attributes will be used as selection criteria, and only if there are no preferred proxies available.

For other details, see *Set a Client to be a Preferred Wake on WAN Proxy on page 8-20*.

1. In the Administrator console, on the Surveyor menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

   Or, in the Administrator console, click the Search button 🔍 and filter the device view.

2. Select the device or multiple devices in the resulting list.
3. On the **Item Actions** menu, click **Edit Device Properties**.
4. Type and select the options you want to use, and then click **OK**.

# Retire a Device from the System

When you need to remove a device from the Surveyor system, or unlicense a device, you can disable the license that is allocated to the device on the Devices page.

Surveyor stops collecting and reporting data for any devices that have their licensing disabled. However, historical data collected while the device was licensed is retained.

At a later time you can bring a device out of retirement by choosing the option **Allocate a license when one is available** in the **License Devices** dialog box.

> **Note:** To view only devices that are currently licensed in the device list, uncheck the option **Show unlicensed in device lists** on the System Settings page.

1.  In the Administrator console on the Surveyor menu ⏻, click **Computers**, and then click a group to view the devices assigned to that group.

    Or, in the Administrator console, click the Search button 🔍 and filter the device view.

2.  Select the device or devices in the resulting list view.

3.  On the **Item Actions** menu, click **Edit Device Properties**.

    > **Note:** You can also right-click a device and click Edit Device Properties.

4.  Select the **Licensing** check box and select **Do not license**, and then click **OK**.

    > **Note:** At a later time you can bring a device out of retirement by choosing the option **Allow licensing** in the **Edit Device Properties** dialog box.

# Reclaim Licenses for Inactive Devices

Rather than removing licenses from inactive devices, you can specify a time period in which Surveyor will automatically reclaim licenses for inactive devices and make those licenses available for use by other devices.

1. In the Administrator console, on the Configure menu ⚙, click **System Settings**.

2. For **Reclaim licenses for inactive devices after**, specify the number of days after the last check-in, in which a device's license can be claimed for use by a different device.

3. Click **Save**.

# View Device Charts

The Distribution Charts and Status Chart tabs on the Devices page includes the following charts to give you a high-level picture of device activity and membership:

## Status Chart

- Last Connected Time. Shows a histogram of how many clients and devices have connected to the system on the current day, in the past 1-3 days, or in the past 8-30 days.

## Distribution Chart

- Policies. Shows the number and percentage of devices in the selected group, by policy assignment.
- Device Family. Shows the number and percentage of devices belonging to each device family.
- Groups. Shows the number and percentage of devices, by group membership.

> **Note:** Move the mouse cursor over different areas of the chart to see more details on various data points.

> **Attention:** Chart and device data is based on the current result set of devices being viewed in the device list, based on the selected group or search filter. A maximum of 2002 devices is displayed by default. For a representative sample of devices in the charts, you may need to increase the **Maximum number of devices returned per view** value on the System Settings page. (However, setting this value to a higher number can result in longer display times for search results.)

For a complete list of device properties and attributes, see *Device Properties and Attributes on page 4-9*.

1. In the Administrator console, on the Surveyor menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

   Or, in the Administrator console, click the Search button 🔍 and filter the device view.

2. Select the device or multiple devices in the resulting list.

3. Click the **Distribution Charts** or **Status Charts** tab.

> **Note:** The chart data is based on the current result set of devices being viewed in the device list (2000 by default). For a representative sample of devices in the charts, you may need to increase the **Maximum**

**number of devices returned per view** value on the System Settings page.

# View the Device Events Report

The Device Events reports shows event data from all devices reporting in to the Surveyor server.

---

**Note:** The device data that appears in each report is determined by the filters that you set for the view, and also by the Maximum number of devices returned per view value set on the System Settings page.
By default, the device list view displays the first 2000 devices that meet the search and filter criteria. If you need to view a larger set of devices, on the Configure menu ⚙, click System Settings, and then increase the Maximum number of devices returned per view value. The maximum value allowed is 20,000. Setting this value to a higher number can result in longer display times for search results.

---

1. Click the Surveyor button ⏻, and then under **Devices**, click **Device Events**.

2. Select a date range and the view (day or hour).

3. Select an **Event Category** (or all categories).

4. Specify the filter parameters to define the set of devices you want to view in the report results, and then click the **Show** button.

5. In the resulting report, double-click an area of the pie chart to see more details on that event category.

---

**Tip:** Move the mouse cursor over different areas of the chart to see more details.
Click the Devices tab to see results by device; click the Events tab to see results by event.

---

6. Click **Print** to print the current view (saving is not an option).

For details on how to use event data for troubleshooting and optimization, see *Chapter 10: Viewing Diagnostic Information from Event Logs on page 10-1* and *Display Event Data in the Administrator Console on page 10-14*.

# 5

# Managing Locations, Energy Rates, and Currency

**Table 5-1  In this Chapter**

| Topics |
| --- |
| *About Locations, Energy Rates, and Currencies* |
| *Add Locations for Devices* |
| *Manually Assign Locations for Devices* |
| *Automatically Assign Locations for Devices* |
| *Add Currencies and Exchange Rates* |

# About Locations, Energy Rates, and Currencies

Locations can be assigned for devices, along with energy rate schedules to help you more accurately track and report energy savings for devices.

Energy rates differ greatly depending on location and time of year. Many locations also have energy costs that vary throughout the day known as time-of-use (TOU) energy rates. By *Add Locations for Devices on page 5-4* and assigning devices to locations, you can more accurately track and manage energy consumption and costs across international boundaries, rates, and currencies.

Each location has an associated *Add an Energy Rate Schedule for a Location on page 5-5* that refers to a *Add Currencies and Exchange Rates on page 5-10* for that location. You can assign the correct exchange rate for each location's currency, compared to the system currency.

Only a Root Administrator has permissions to add currencies and exchange rates. A rate administrator or a root administrator has permissions to manage energy rates.
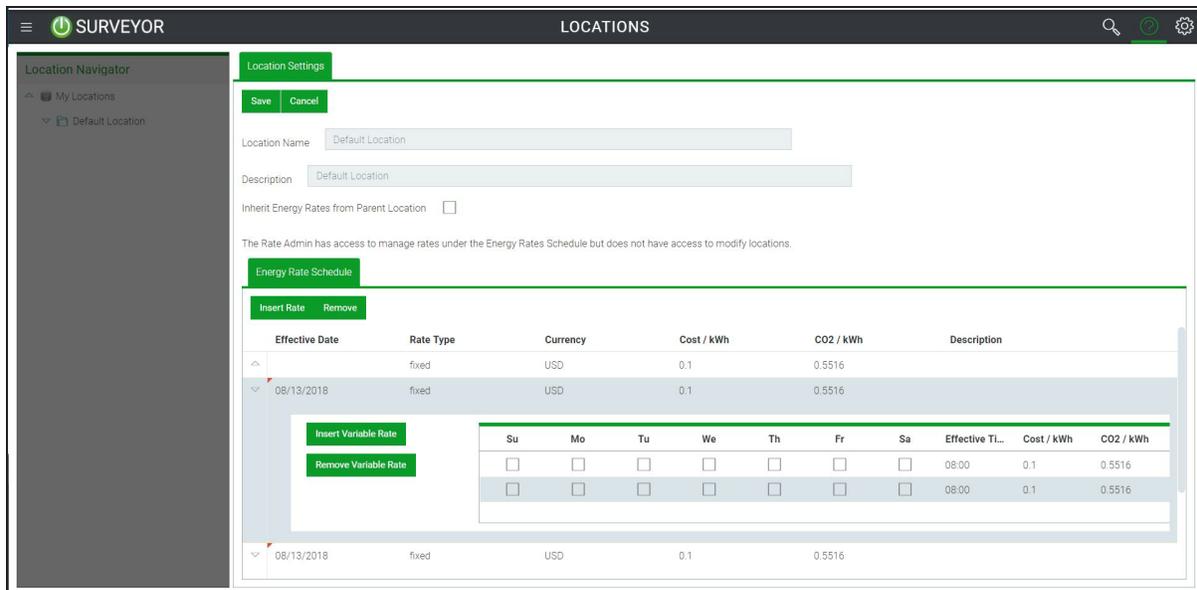


> ❗ **Important:** The default system currency is U.S. Dollars (USD). If you want to change the system currency, make sure that you choose a currency before you start summarizing data and setting up locations and energy rates, and that you keep the same system currency in place going forward. Changing the system currency at a later date can affect historical data and many data calculations and settings throughout the Surveyor system.

The **Default Location** is initially assigned for each device. After you define other locations, you can either manually assign devices to those locations or define automatic assignment rules that associate devices with specific locations.

For example, you can identify device locations based on IP addresses and automatically associate the device with the specific location's energy rates in the local currency. In addition,

all of the devices within one office location are tied to specific energy policies that can be optimized based on local TOU energy rates.

# Actions Allowed on Devices in Locations View

Users viewing devices in the Locations view can:

- View devices by location in a device table, and view a summary of device attributes.
- *Manually Assign Locations for Devices on page 5-7* to a device or multi-selected set of devices.
- *Automatically Assign Locations for Devices on page 5-8* for a device or multiple devices using Auto Location Assignment Rules.

# Location Attributes

- All devices are initially assigned to the Default Location.
- Each location can have devices associated with it.
- Each device can have only one assigned location, but a device can be moved to a different location at any time.
- A Location History is tracked for each device (for reporting purposes).
- By default, each location inherits settings from its parent. If the **Inherit Energy Rates from Parent Location** checkbox in not selected, parent settings are then copied initially.
- Each location has the following attributes (either by having them locally set or by inheriting from parent):

  Time Zone (e.g. Mountain Time Zone, including DST) Energy Cost Currency (e.g USD)

  If different than System Currency, Default Exchange Rate to System Currency: (e.g. 1.25 USD = 1 Euro)

  Default Energy Costs for Location: .1405 USD

  Default $CO_2$ Emissions (kg per kWh): 2.123 kg of $CO_2$ emitted for each 1 kWh power consumed

- Locations can optionally have energy rates that change over time (fixed or variable).

all of the devices within one office location are tied to specific energy policies that can be optimized based on local TOU energy rates.

# Add Locations for Devices

Use this page to create and manage the locations for devices.

Each location can have an associated energy rate or rate schedule that includes multiple fixed or variable energy rates for that region.

After you create a location, you can then assign the location for devices in the system either manually or through **Auto Location Assignment Rules** (on the Configure menu).

To create new location or move a location, right-click **Default Location** in the Location Navigator, and then select **Add Location** or **Move Location**.

Click the Device List tab to view the devices for the selected location. Select one or more devices and then click **Set Device Location** to manually set the location.

1. In the Administrator console, on the Verdiem menu ⏻, click **Locations**.

2. Right-click any location node in the Location Navigator, and then select **Add Location**.

3. Type the name and a description for the location and then click **OK**.

# Add an Energy Rate Schedule for a Location

> **Note:** Only a Rate Administrator or Root Administrator has permissions to perform this task.

1. In the Administrator console, on the Verdiem menu ⏻, click **Locations**.

2. Select the location node that you want to edit in the Location Navigator.

3. Clear the option **Inherit energy rates from parent location** .

4. Click **Insert Rate** to add a rate.

   Enter the date on which the rate goes into effect, select the currency (or use default), enter the cost per kWh (or use default), enter the CO2 per kWh (or use default), and type a description.

5. **To include a variable rate**: Click the plus sign + for the rate, and then click **Insert Variable Rate**.

   Select the days on which the rate applies and the time in which the rate goes into effect. Enter the cost per kWh (or use default) and the CO2 per kWh (or use default).

6. Click **Save** to save all rate settings.

> **Note:** Be aware that when you change energy rate information, you will need to resummarize data for the new settings be calulated for reports. For details, see *About Data Summarization on page 9-18*.

# Move a Location in the Location Hierarchy

1. In the Administrator console, on the Verdiem menu ⏻, click **Locations**.

2. Right-click any location node in the Location Navigator, and then select **Move Location**.

3. Select the new parent location for the location, and then click **OK**.

# Manually Assign Locations for Devices

1. In the Administrator console, on the Verdiem menu ⏻, click **Locations**.

2. Select the Default Location node in the Location Navigator.

   If you want to change the location for devices assigned to another location, select that location name in the Location Navigator.

3. Click the Device List tab.

4. Select one or more devices in the list.

5. Click **Set Device Location**, select the new location, and then click **OK**.

# Automatically Assign Locations for Devices

After you create locations, you can configure Surveyor to assign the appropriate location to new devices automatically when the devices connect to the server.

When you configure location assignment rules, locations are automatically assigned to specific devices based on a set of criteria. For example, you can create a rule for a Tacoma location that accepts clients only from a particular IP segment.

Because rules that you set up for automatically assigning locations to devices are saved as a set, their order is important and you will need to consider the best order to get the results you want.

You have the option to automatically run the rule set only when new devices connect, or for all connections, which means that rules will be run whenever a device wakes or whenever the device moves from one network card to another, such as a computer moving from a network line to a wireless connection.

Each rule can then contain a set of conditions that a location must meet to be assigned to the device. When you connect new devices to the server, they must comply with a location's conditions for the location to be automatically assigned to a set of devices.

**Note:** If a device does not meet any conditions of a rule set, you have the option to leave the group for the device unchanged, or to assign the Default Location for the device.



If devices do not meet any of the conditions listed above:

○ Leave location unchanged

◉ Assign location Default Location

1. In the Administrator console, on the Configure menu ⚙, click **Auto Location Assignment Rules**.

2. Click **New Rule**. Type a name and a description for the rule, and then select the name of the policy to be assigned when the rule runs.

3. Click **Add Condition** to add as many conditions as necessary.

   As you add conditions, you can test what the result will be by clicking the **Test Rule** tab.

4. Specify whether the rule should be enforced when all conditions are satisfied, or when any condition is satisfied.

5. Specify whether the rule should be run automatically when new devices connect to the server, or when all devices connect to the server.

> **Note:** With All connections, the rules run whenever a computer wakes up or whenever a computer moves from one network card to another (such as from a network line to a wireless connection or back).

6. Reorder rules by selecting a rule in the set and then clicking **Move Up** or **Move Down**.

7. Click **Save** to save all changes.

# Add Currencies and Exchange Rates

Any currency that is added to the system also requires an exchange rate compared to the system currency. You can update exchange rates for a currency when needed.

1. In the Administrator console, on the Configure menu ⚙, click **Currencies**.

---

! **Important:** The default system currency is U.S. Dollars (USD). If you want to change the system currency, make sure that you choose a currency before you start summarizing data and setting up locations and energy rates, and that you keep the same system currency in place going forward. Changing the system currency at a later date can affect historical data and many data calculations and settings throughout the Surveyor system.

---

2. Click **New Currency**.

   Enter the currency name, short name, and exchange rate compared to the system currency.

3. Click **OK**, and then click **Save**.

4. **To update a rate**: Select the currency and then click **Insert Updated Rate**. Select the date that the rate change went into effect and specify the new exchange rate.

   Click **Save**.

# Set the System Currency

The default system currency is U.S. Dollars (USD). If you want to change the system currency, make sure that you choose a currency before you start summarizing data and setting up locations and energy rates, and that you keep the same system currency in place going forward. Changing the system currency at a later date can affect historical data and many data calculations and settings throughout the Surveyor system.

1.  In the Administrator console, on the Configure menu ⚙, click **Currencies**.

2.  Select a currency in the list of available currencies. (*Add Currencies and Exchange Rates on the previous page* if necessary.)

3.  Click **Set System Currency**, and then click **Save**.

# 6

# Managing Policies

**Table 6-1  In this Chapter**

| Topics |
|---|
| *Overview of Policies and Power ManagementSettings* |
| *About Power State Changes* |
| *Create and Edit Policies* |
| *Configure Policy Assignment Rules* |
| *Edit Default Wake and Data Collection Settings for Policies* |
| *Enforce Power Management Policies* |
| *Disable a Policy* |
| *Working with Power Schemes* |
| *Managing Open Applications During Power State Changes* |

# Overview of Policies and Power ManagementSettings

## Introduction

Policies contain the collection of the settings Surveyor uses to enforce power management in your organization's network, such as power schemes, power level changes, and power state transition rules. This section describes how to create, edit, and manage policies in Surveyor. You can assign the same policy to multiple devices in a network.

Each device can have only one policy assigned to it, but each policy can contain multiple schemes and power state changes, each with its own schedule.

> **Note:** All power settings in policies apply to Windows PCs and Macintosh computers. For other types of devices, only scheduled power level changes apply. Surveyor collects data for all device types for reporting purposes.

Policies can contain the following types of settings:

| | |
|---|---|
| Background scheme | A background scheme, which is a power scheme that runs 24 hours a day, 7 days a week, when no other schemes are explicitly scheduled. |
| | You can create a policy with just the background power scheme to serve as a default for basic computer power management. |
| Power scheme | One or more power schemes, each with a unique schedule. Each scheme can also include one or more power state transition rules (for different applications). |
| | Power state transition rules can prevent a PC or Mac from transitioning to standby or shutdown while a specified application is running. |
| Power level changes | One or more power level changes (such as wake, sleep, or restart), each with a unique schedule. |
| Power state transition rules (PCs only) | Power state transition rules apply to Windows PCs only. |
| | Power state transition rules tell Surveyor what action to take when a particular application (such as **iexplore.exe** or **firefox.exe**) is running and Surveyor attempts to transition the computer to standby or shutdown. |
| | Rules can run unscheduled as part of the background settings, or as part of a scheduled scheme. The rules take effect whenever their associated scheme takes effect, including the background scheme. |
| Wake settings | These settings affect how you can wake computers from the Administrator console, as well as how end users can wake their own computers. |
| | For details, see *Enable Policy Wake on WAN Settings on page 8-18*. |
| Data collection | Logging and data collection settings for PC and Mac clients. These settings affect data collected for event reporting, troubleshooting, user activity, and power state |

| | transitions. |
| :-- | :-- |
| | For details, see *Data recorded in Event Logs and How Long it is Retained on page 10-2* |

# Baseline Data Collection Policy

Each device is assigned the default **Baseline Data Collection** policy until you explicitly assign a different policy, either manually or though policy assignment rules. Surveyor captures data and events for devices using the **Baseline Data Collection** policy, but does not enforce any power settings or schemes.

For any device using the **Baseline Data Collection** policy, Surveyor begins collecting data for the device when it first connects to the system. The data updates each time a device checks in. You can then view this data in different reports and device views.

## Setting up New Policies

When you create a new policy, it uses the policy default settings for wake settings and data collection. You can then select:

- The background scheme and power state transition rules that are in effect when the background scheme is in effect.
- Power schemes, power, and power state transition rules that run according to schedule and override background settings.

> **Note:** New polices that you create inherit policy default settings. To change these settings, you can edit the settings on a policy's Wake Settings and Data Collection tabs.

**Table 6-2  General steps for setting up a policy in Surveyor**

| Step | Tasks | Procedure |
| :--: | :-- | :-- |
| 1 | Create a policy. | In the Administrator console, on the Surveyor menu ⏻, click **Policies**, and then click **New Policy**. |
| 2 | Set the power scheme that should run when no other schemes are scheduled (called the Background scheme). Also, set any transition rules that should run when no other schemes are scheduled. | Click the **Background** tab. |
| 3 | Create a comprehensive schedule for the policy. The schedule can include one or more schemes that run during specific days and times, and one or more power state changes that run on specific | While editing a policy: Click the **Schedule** tab and then click **Insert Scheme** or **Insert Power Level Transition**. |

**Table 6-2  General steps for setting up a policy in Surveyor (continued)**

| Step | Tasks | Procedure |
|------|-------|-----------|
| | days and times.<br><br>**Note:** Scheduled power schemes cannot overlap.<br><br>If you need to create or edit a power scheme: On the Verdiem ⏻ menu, click **Power Schemes**. | |
| 4 | Add one or more transition rules if necessary. | While editing a policy: Click the **Schedule** tab, click **Insert PSTM Rule**, and then click the **Power State Transition Rules** tab. |
| 5 | Review the wake settings. | While editing a policy: Click the **Wake Settings** tab. |
| 6 | Review settings for logging and data collection. | While editing a policy: Click the **Data Collection** tab. |
| 7 (optional) | Create, edit, or reorder policy assignment rules. | On the Configure menu ⚙, click **Auto Policy Assignment Rules**. |
| 8 (optional) | Create or edit power state transition rules. | On the Surveyor menu ⏻, click **Power Transition Rules**. |

## Inheritance in Policies

All new policies inherit wake and data collection settings from the **Policy Defaults** page, which are wake settings, and logging and data collection settings that have no scheduled component. You can apply the same wake and data collection settings for all policies by using the default settings, or customize wake and data collection settings for specific policies as needed.

Each new policy that you create must include a background scheme, which can include a scheme and power state transition rules that automatically apply 24 hours a day, 7 days a week (24x7) unless you explicitly schedule other schemes and rules.

Scheduled power settings that you specify (schemes, power state changes, power state transition rules) and unique wake and data collection settings take precedence over background settings.

The background scheme and scheduled power schemes can also have associated power state transition rules that are active when the particular schemes are active.

## Strategies for Creating Policies

The policies you create should be based on your knowledge of how much energy computers and other devices in your organization use, the times of day users are most active, and patch management needs.

Analyzing the Computer State/Activity report and Device Events report during the baseline period can help you gain understanding of when devices are On but not actively being used.

For more details on implementing power management through policies, see "Gathering baseline data and creating initial power management policies" in the *Surveyor 6 Installation Guide*.

After you create a policy, you can assign it to one or more devices manually in the device list view, or automatically through policy assignment rules.

# Determine Initial Power State Settings from User and System Activity

This topic describes how to view a user and system activity report, which you use to determine how to optimize power use through power management policies.

Complete this task after you run devices using the Baseline Data Collection policy for a minimum of two weeks of normal operation. You will view hourly activity over a few days to see trends in user activity that you can build policies around.

1. In the Administrator console, on the Verdiem menu ⏻, click **Analytics**.

2. Select the **Activity: Computer Power States** report.

3. For Range, select **Last Full Month**.

4. For Granularity, select **Daily**.

   > **Note:** Typically the baseline data collection period involves all Windows and Mac clients in the system. But if you are using only a subset, use the **Groups** or **Policies** filters to run the report only on the relevant computers.

5. Specify the filter parameters for **Locations** or **Groups** to refine the set of devices you want to view in the report results.

6. Click **Run**.

   The resulting graph should show a trend of higher user activity during your working hours, tapering off toward the end of your work day. If the graph shows inconsistent use, find a different date range within the baseline period that shows consistent and predictable use before you view only one day.

7. If the graph shows consistent use over the weekdays, drill down to just one day (such as a Tuesday or Wednesday) by clicking that day in the graph.

8. Note the times when user activity picks up and tapers off for the day.

9. Use this data to create your initial power management policies.
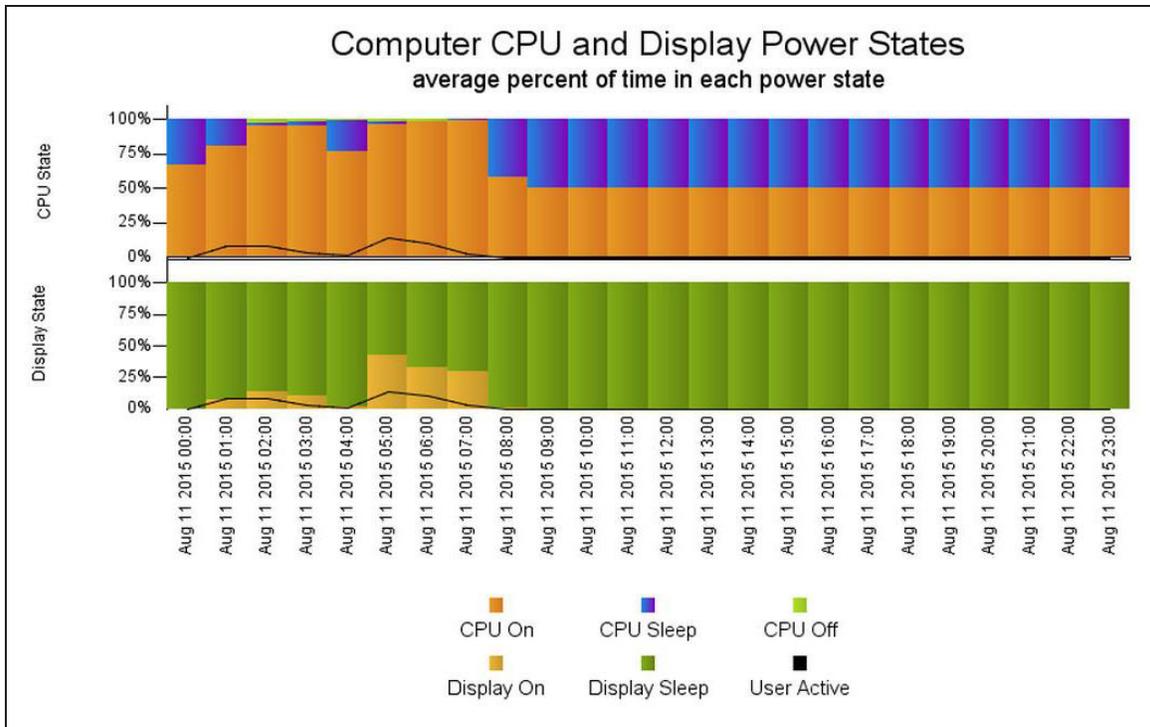
User and system activity over one day

The graph here shows most of the user activity occurring between 6:00am and 6:00pm, so it might make sense to configure power schemes to match this activity level.

In a weekday policy based on this data, you might include the following (with corresponding areas in the image indicated):

- (A) A background scheme that transitions computers to standby after a short time of inactivity. For example, after 10 mins. of idle time.
- (B) A scheduled power-state change that wakes computers at 6:00am.
- (C) A daytime scheme that lengthens the amount of idle time before computers transition to standby.
- (D) A scheduled power-state change at 7:00pm that transitions computers to sleep.

This step is optional, because if no scheme is scheduled, the background scheme will take effect, and the computers will transition to sleep when idle for the amount of time you specified.

| | Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|---|---|---|---|---|---|---|---|
| all-day | Monitor 10m /System **A** | Monitor 10m /System | Monitor 10m /System | Monitor 10m /System | Monitor 10m /System | Monitor 10m /System | Monitor 10m /System |
| 6am | | 6 - 7 Wake **B** | 6 - 7 Wake | 6 - 7 Wake | 6 - 7 Wake | 6 - 7 Wake | |
| 8am | | 8 - 6 Monitor 30m / System 120m | 8 - 6 Monitor 30m / System 120m | 8 - 6 Monitor 30m / System 120m | 8 - 6 Monitor 30m / System 120m | 8 - 6 Monitor 30m / System 120m | |
| 10am | **A** | **C** | | | | | |
| 7pm | | 7 - 8 Sleep **D** | 7 - 8 Sleep | 7 - 8 Sleep | 7 - 8 Sleep | 7 - 8 Sleep | |

Example policy created based on user activity

After you create your initial policies, you assign them to devices. After that, you can refine them to include assignment rules and other settings.

For more information, see *Overview of Policies and Power ManagementSettings on page 6-2* and *Assign Policies to Devices on page 4-20* in the *Surveyor 6 Administrator Guide*.

# Enforce Power Management Policies

After you determine initial policies, you can assign them to devices to start measuring and managing power use on the devices.

This topic assumes either of the following situations:

- You have created initial power management policies after completing the baseline data collection phase and you have assigned the policies to devices.

- The **Do not enforce this policy** option is selected for a policy for another reason, such as at the suggestion of a Technical Support representative for troubleshooting purposes.

If you have not obtained baseline numbers or created initial policies yet, see an overview of the process at "Establishing the baseline level of energy use" in the *Surveyor 6 Installation Guide*.

If you have created policies but you have not assigned them to devices, see "Assign policies to devices" in the *Surveyor 6 Administrator Guide*.

Make sure that the policies you're using are not disabled:

1. Click the Surveyor button ⏻, and then click **Policies**.

2. Select a policy to see its settings. If you already assigned a policy other than Baseline Data Collection to a device, confirm that the **Do not enforce this policy** option is not selected.



3. Click **Save**.

# Determine Whether Clients are Following Policy Instructions

This topic shows you how to use event log data to quickly determine whether client agents successfully transition power states according to policy instructions.

Specifically, this topic describes how to:

- View one day of system and user activity for Windows and Mac clients that have the same policy assignment.
- Compare activity with the policy settings.

1. In the Administrator console, on the Verdiem menu ⏻, click **Analytics**.
2. Select the **Activity: Computer Power States** report.
3. For Range, select **Last Full Month**.
4. For Granularity, select **Daily**.
5. Under **Policies**, select the policy you want to check.

   > **Note:** Typically the baseline data collection period involves all Windows and Mac clients in the system. But if you are using only a subset, use the Groups or Policies filters to run the report only on the relevant computers.

6. Click **Run**.

   The resulting graph should show a trend of higher user activity during your working hours, tapering off toward the end of your work day. If the graph shows inconsistent use, find a different date range within the baseline period that shows consistent and predictable use before you view only one day.

7. Drill down to just one day (such as a Tuesday or Wednesday) by clicking that day in the graph.
8. Confirm that the policy settings match the activity. If you're not sure, check the policy settings:

   a. Click the Verdiem button ⏻, and then click **Policies**.

   b. Select the policy, and then click the **Schedule** tab.

# About Power State Changes

A power state change is part of a policy that can be scheduled, and instructs a device to wake, sleep, hibernate, shutdown, restart.

You can also change the power levels of devices directly, outside of policy settings, from the device list view.

Options for power state changes are available in the Policies page on the Schedule tab.

For PCs and Macs: When you specify a power state change of sleep, hibernate (PCs only), shutdown, or restart, you also can specify options for forcing a transition (directly or in a policy), or allowing a user to delay or skip a transition for a specified period of time (policies only).

> **Note:** The options for skipping, delaying, or forcing a transition, or displaying a message are ignored for non-computer devices.
> Use **Force transition** only when absolutely necessary. Some applications may block normal shutdown requests. For example, Word or Notepad may display a dialog box asking the user to save document changes. When you select **Force transition**, applications are prevented from blocking shutdown and any unsaved changes in the user's application will be lost.

# Create and Edit Policies

A policy contains a collection of the settings Surveyor uses to enforce power management in your organization's network. You can assign the same policy to multiple devices in a network.

> **Note:** All power settings in policies apply to Windows PCs and Macintosh computers. For other types of devices, only scheduled power level changes apply. For non-computer devices, it is likely a scheduled power level change would be the only setting you will apply using a policy. Surveyor collects data for all device types for reporting purposes.

1. In the Administrator console, on the Surveyor menu ⏻, click **Policies**.

2. Click **New Policy** or select a policy in the list. You can also click **Copy** to start with an existing policy as your template.

3. For a new policy, type the policy name and a description.

4. On the **Schedule** tab, select the background power scheme that will be used whenever no other scheme is scheduled.

   You can optionally click the **Background** tab to select a background power scheme, and also to specify power state transition rules that run when no other power state transition rules are scheduled.

5. Click **Insert Scheme** to add a scheduled power scheme to the policy.

6. Select the scheme, days, and time range, and then click **Insert**.

   Continue to add schemes as needed for the policy. (Scheduled power schemes cannot overlap.)

   To include a power state transition rule (or rules) to accompany the scheduled scheme:

   a. Click the **Power State Transition Rules** tab.

   b. Click **Insert**, select the rule (or rules) you want to add, and then click **Add**.

      Click **New Rule** to add a rule to the list.

      Power state transition rules can apply to applications running locally, or on the network, or both. The application name that you provide should be the executable name as it appears in the Windows Task Manager under Processes, for example: **firefox.exe**.

   c. Click the **Schedule** tab when you are done.

7. On the **Insert Power Level Transition** menu, click a power state change to add it to the policy.

   For PCs and Macs only: If you select **Insert Sleep**, **Insert Hibernate** (PCs only), **Insert Shutdown**, or **Insert Restart** you can choose whether you want to force the change in

power state by selecting **Force transition**. You also can choose whether to force a transition for Wake on WAN proxies.

> **Note:** Use **Force transition** only when absolutely necessary. Some applications may block normal shutdown requests. For example, Word or Notepad may display a dialog box asking a user to save document changes. When you select **Force transition**, applications are prevented from blocking shutdown and any unsaved changes in the user's application will be lost.

For computers only: You can also specify whether users can skip or delay a transition and the message that is displayed for Sleep, Hibernate, Shut Down, or Restart.

> **Note:** Options for skipping, delaying, or forcing a transition, or displaying a message are ignored for non-computer devices.

8.  Select the days and time, and then click **Insert**.

    Continue to add power state changes as needed for the policy.

9.  Adjust the **Wake Settings** and **Data Collection** tab settings (these settings affect computers only), if needed.

    If you clear the **Collect power state data** option, power state change data will not be available in reports.

10. Click **Save**.

> **Note:** Refresh the browser to see policy changes in device lists.

# Configure Policy Assignment Rules

After you create policies, you can configure Surveyor to assign the appropriate policies to new devices automatically when the devices connect to the server.

When you configure policy assignment rules, policies are automatically assigned to specific devices based on a set of criteria. Because rules that you set up for automatically assigning policies to devices are saved as a set, their order is important and you will need to consider the best order to get the results you want.

You have the option to automatically run the rule set only when new devices connect, or for all connections, which means that rules will be run whenever a device wakes or whenever the device moves from one network card to another, such as a computer moving from a network line to a wireless connection.

Each rule can then contain a set of conditions that a policy must meet to be assigned to the device. When you connect new devices to the server, they must comply with a policy's conditions for the policy to be automatically assigned to a set of devices.

> **Note:** If a device does not meet any conditions of a rule set, you have the option to leave the group for the device unchanged, or to assign the Baseline Data Collection  policy for the device.

> If devices do not meet any of the conditions listed above:
>
> ○ Leave location unchanged
>
> ⊙ Assign location Default Location

1. In the Administrator console, on the Configure menu ⚙, click **Auto Policy Assignment Rules**.

2. Click **New Rule**. Type a name and a description for the rule, and then select the name of the policy to be assigned when the rule runs.

3. Click **Add Condition** to add as many conditions as necessary.

   As you add conditions, you can test what the result will be by clicking the **Test Rule** tab.

4. Specify whether the rule should be enforced when all conditions are satisfied, or when any condition is satisfied.

5. Specify whether the rule should be run automatically when new devices connect to the server, or when all devices connect to the server.

> **Note:** With **All connections**, the rules run whenever a computer wakes up or whenever a computer moves from one network card to another (such as from a network line to a wireless connection or back).

6. Reorder rules by selecting a rule in the set and then clicking **Move Up** or **Move Down**.

7. Click **Save** to save all changes.

# Edit Default Wake and Data Collection Settings for Policies

1. On the **Configure** menu ⚙, click **Policy Defaults**.

2. Click the Wake Settings tab to set wake defaults. For details, see *Enable Policy Wake on WAN Settings on page 8-18*.

3. Click the Data Collection tab to set server logging levels and file size. For details, see *Specify Server Logging Levels and File Size on page 10-17*.

4. Click **Save**.

# Disable a Policy

If you need to disable a policy for all devices that use that policy, you can select the option Do not enforce this policy on the Policies page.

| Policy Name | Work Day, 9 to 6 | ☐ Do not enforce this policy ☐ Mark as GoGreen policy |
|---|---|---|
| Group | /My Organization | |
| Description | Normal work day policy | |

You may also want to create a new policy for a specific set of devices to which you can apply the **Do not enforce this policy** option as needed.

Notify your Surveyor Administrator when you make this change to ensure that the PCs or devices in question receive the correct enforcement instructions for your organization.

**Note:** You can optionally apply the **Baseline Data Collection** policy to devices as a way to disable policy enforcement.

1. Click the Surveyor button, and then click **Policies**.
2. In the policy list, select the policy you want to disable.
3. Select **Do not enforce this policy**.
4. Click **Save**.

# Working with Power Schemes

## What is a Power Scheme

A power scheme is part of a policy that can be scheduled for Windows PCs and Macintosh computers, and provides instructions about when a computer should change power levels, such as transitioning the system to sleep after 1 hour of no activity, or turning the monitor off after 15 minutes.

Schemes include the following settings:

- Basic settings for system standby, monitor (on or off), and narcolepsy timeout.

  > **Note:** Narcolepsy timeout refers the period of time in which the operating system is prevented from putting a computer back to sleep during a period of no activity (such as during maintenance windows), even if no user is logged in. You can also disable narcolepsy behavior completely.

- Use of the Computer idle timer versus Surveyor idle timer settings.

  For information on PC insomnia, the Windows idle timer, and the Surveyor idle timer, see *Addressing Windows PC Insomnia through the Surveyor Idle Timer on page 1-15*.

  For information on insomnia and the sleep timer on Macintosh computers, see *About Mac OS X Power Management on page 1-17*.

  > **Note:** The Surveyor idle timer is enabled by default in schemes. The Surveyor idle timer must be enabled to use power state transition rules in a scheme.

- Advanced settings that apply to specific versions of Windows (Vista, or Windows 7).

## Default Power Schemes in Surveyor

Surveyor includes several pre-defined schemes that you can use in policies, or modify to fit the particular needs or your organization. You can edit these schemes or create your own custom schemes as needed on the **Power Schemes** page.

You apply schemes to policies using the **Schedule** tab in the Policies page.

| Scheme | Description |
| --- | --- |
| Monitor 10m / System Never | <ul><li>System sleep: Never</li><li>Turn off monitor after 10 minutes</li><li>Narcolepsy timeout</li><li>Surveyor idle timer on by default (Computer idle timer disabled)</li></ul> |

| Scheme | Description |
|---|---|
| Monitor 15m / System 30m | • System sleep after<br><br>• Turn off monitor after<br><br>• Narcolepsy timeout after<br><br>• Surveyor idle timer on by default (Computer idle timer disabled) |
| Monitor 20m / System 60m | • System sleep after<br><br>• Turn off monitor after<br><br>• Narcolepsy timeout after<br><br>• Surveyor idle timer on by default (Computer idle timer disabled) |
| Monitor 30m / System 120m | • System sleep after<br><br>• Turn off monitor after<br><br>• Narcolepsy timeout after<br><br>• Surveyor idle timer on by default (Computer idle timer disabled) |
| Monitor 30m / System Never | • System sleep - Never<br><br>• Turn off monitor after<br><br>• Narcolepsy timeout after<br><br>• Surveyor idle timer on by default (Computer idle timer disabled) |
| Monitor Never / System Never | • System sleep - Never<br><br>• Turn off monitor - Never<br><br>• Narcolepsy timeout - Never<br><br>• Surveyor idle timer on by default (Computer idle timer disabled) |

# Create and Edit Power Schemes

A power scheme is part of a policy that can be scheduled for Windows PC and Macintosh computers, and provides instructions about when a device should change power levels, such as transitioning the system to sleep after 1 hour of no activity, or turning the monitor off after 15 minutes.

The process of creating or editing a power scheme is separate from assigning the scheme to a policy. You must first create a power scheme to be able to add it to a policy.

1. On the Verdiem menu ⏻, click **Power Schemes**.

2. Click **New Scheme** or select an existing scheme to edit it. You can also click **Copy** to start with an existing policy as your template.

3. For a new scheme, type the scheme name and a description.

4. On the **Basic Settings** tab, select the main settings for the scheme.

   You can optionally click the **Advanced Settings** tab to specify settings that affect specific versions of Windows.

5. On the **Idle Timer Settings** tab, select whether the scheme should use the Computer idle timer or the Surveyor idle timer.

   Select further options for refining how inactivity is determined by the Surveyor idle timer. Options for tracking CPU usage, disk usage, or network usage to determine inactivity apply to Windows PCs only.)

   > **Note:** The Surveyor idle timer must be enabled to use power state transition rules in a scheme. (The Surveyor idle timer is enabled by default in schemes.)
   > For background information on PC insomnia, the Windows idle timer, and the Surveyor idle timer, see *Addressing Windows PC Insomnia through the Surveyor Idle Timer on page 1-15Addressing Windows PC Insomnia through the Surveyor Idle Timer on page 1-15Addressing Windows PC Insomnia through the Surveyor Idle Timer on page 1-15*.
   > For information on insomnia and the sleep timer on Macintosh computers, see *About Mac OS X Power Management on page 1-17*.

6. Click **Save**.

# Advanced Settings

The following Windows power settings options are available on the Advanced Settings tab of Power Schemes.

A setting of Don't change specifies that Surveyor should use the Windows Power Setting as it is currently set.

| Setting | Options | Operating System | Description |
|---------|---------|------------------|-------------|
| Adaptive display timeout | Disable, Enable, **Don't change** | Vista, Windows 7 | Extends the time Windows waits to turn off the display if an end user repeatedly turns on or awakens the display using the keyboard or mouse. |
| Allow display required | Disable, Enable, **Don't change** | Windows 7 | Specifies whether Windows allows applications to temporarily prevent the display from automatically reducing brightness or turning off to save power. |
| Default display brightness | 10% - 100%, **Don't change** | Windows 7 | Specifies the default display brightness level. This setting applies only to portable computers that support Windows control of the brightness level of an integrated display device. |
| Dim display | After x minutes, After x hours, Never **After 3 minutes** | Vista, Windows 7 | The period of inactivity before the display brightness is automatically reduced. This setting applies only to portable computers that support Windows control of the brightness level of an integrated display device. |
| Dim display brightness | 10% - 100%, **Don't change** | Windows 7 | Reduced display brightness level after the dim idle timeout has been reached. This setting applies only to portable computers that support Windows control of the brightness level of an integrated display device. |
| Allow hybrid sleep | Disable, Enable, **Don't change** | Vista, Windows 7 | A combination of Hibernate and Standby, where the system state is stored both in RAM and on disk, in an effort to protect the state data should power be unexpectedly cut to the workstation; of primary use for desktops. Can be problematic with legacy hardware and/or device drivers. |
| Automatically wake for tasks | Disable, Enable, **Don't change** | Windows 7 | Specifies whether the system uses the system-wide |

| Setting | Options | Operating System | Description |
|---------|---------|------------------|-------------|
| | | | wake-on-timer capability. The system can automatically use wake-on-timer on capable hardware to perform scheduled tasks. For example, the system might wake automatically to install updates. |
| System hibernates | After x minutes, After x hours, **Never** | XP, Vista, Windows 7 | Duration of time after Sleep that the system automatically wakes and enters Hibernate. |
| Lid closed action | **Don't change**, Do nothing, Shutdown, Sleep, Hibernate | Vista, Windows 7 | Specifies the action that Windows takes when a user closes the lid on a laptop. If set to Sleep, it is still possible that a laptop can reawaken while in transit (while in a computer bag, for example), leaving either less or no battery power available when reaching the destination. If set to Hibernate, an end user can shut their laptop lid, put the laptop in their bag, and upon returning home from work, startup from where they left off. |
| Power button action | **Don't change**, Do nothing, Shutdown, Sleep, Hibernate | Vista, Windows 7 | The action that Windows takes when an end user presses the Power button. |
| Power button force shutdown | Disable, Enable, **Don't change** | Windows 7 | The type of system shutdown that occurs when the system power button is pressed if the power button action is set to Shut Down.<br><br>Enabled - Forced shutdown Disabled - Normal shutdown If this setting is enabled and a user presses the power button to shut down the system, any open documents might not be saved and data loss could occur. |
| Sleep button action | **Don't change**, Do nothing, Sleep, Hibernate | Vista, Windows 7 | Specifies the action that Windows takes when an end user presses the Sleep button. |
| Desktop slideshow | Disable, Enable, **Don't change** | Windows 7 | Configures the behavior of the desktop background slideshow. |
| Media sharing | **Don't change**, Allow idle sleep, Allow away mode, Prevent idle sleep | Vista, Windows 7 | Away Mode was designed to handle media sharing scenarios where the PC is required to be running, yet seem Off (no display or sound); when entering Away Mode, the display is Off, audio is muted, |

| Setting | Options | Operating System | Description |
|---|---|---|---|
| | | | and keyboard and mouse input are ignored. Away Mode is not recommended for enterprise deployments. |
| When playing video | **Don't change**, Optimize Video Quality, Balanced, Optimize Power Savings | Windows 7 | Specifies whether Windows Media Player favors power savings or performance in playing video content. Optimize Video Quality - Favor video quality at the expense of power savings. Balanced - Balance video quality and power savings.<br><br>Optimize Power Savings - Favor power savings at the expense of video quality. |
| Device idle policy | **Don't change**, Performance, Power Savings | Windows 7 | Determines whether Conservation idle timeouts or Performance idle timeouts are used for devices that are integrated with Windows kernel power manager device idle detection. Performance - Performance idle timeouts are used. Power Savings -Conservation idle timeouts are used. |
| PCI Express link state | **Don't change**, Off, Moderate savings, Maximum savings | Vista, Windows 7 | Governs the power management state for the PCI Express bus (if present). Experiment with the two power saving levels;<br><br>higher-end graphics cards may present display issues if this is set too aggressively. |
| Turn off hard disks | After x minutes, After x hours, **Never** | XP, Vista, Windows 7, Macintosh | The period of inactivity before the disk is automatically powered down. |
| USB selective suspend | Disable, Enable, **Don't change** | Vista, Windows 7 | Turns off internally integrated USB devices when idle, yet maintains near-real-time availability by reawakening these devices when ready for use. Largely reliant on device driver support. |
| Wireless adapter | **Don't change**, Max performance, Low power saving, Mid power saving, Max power saving | Vista, Windows 7 | These power saving choices enable the wireless adapter to consume less power by sleeping and waking periodically; however, note that this depends in part on the cooperation of the access point.<br><br>Connectivity and/or throughput issues may be an indication that this is set too aggressively. |

# Managing Open Applications During Power State Changes

End users often leave open documents on their computers. When Surveyor is scheduled to shut down clients, many open applications cannot save and close documents until a user confirms the action. This prevents the computer from properly shutting down as scheduled.

The schemes that you assign to Surveyor policies can include power state transition rules that gracefully shut down applications that would otherwise keep computers awake.

The rules you create can automatically close running applications on a client, save work in a temporary folder, and allow the computer to continue to shutdown. Alternatively, you can specify that a particular application should prevent a client from shutting down.

> **Note:** Power state transition rules and settings apply to Windows PCs only.

## Using Power State Transition Rules and Custom Scripts

To configure Surveyor to use power state transition rules, you must:

1. *Create and Edit Power State Transition Rules on page 1*.

2. Apply the rule to the appropriate devices. You do this by adding the power state transition rule to a scheme in a policy that is assigned to the devices. You can also assign a power state transition rule to the background scheme that runs when no other scheme is scheduled.

   To configure policy settings, see *Create and Edit Policies on page 6-12*. When you insert a scheme, you have the option to insert a power state transition rule.

   To assign a policy to a device, see *Assign Policies to Devices on page 4-20*.

One of the actions a rule can trigger is to run a custom power state transition script. If you want to run a custom script in response to a rule, you must take these additional steps:

1. Create a script (JavaScript or VBScript).

2. Upload the custom script to Surveyor.

3. Assign the custom script to a power state transition rule.

4. Install a code signing certificate on the Surveyor server.

5. Install the same code signing certificate on all targeted clients in the group.

For details, see *Upload a Script for a Power State Transition Rule on page 6-29*, *Assign a Custom Script to a Power State Transition Rule on page 6-30*, and *Signing Power State Transition Scripts with Digital Certificates on page 6-32*.

# About Power State Transition Rules

Power state transition rules tell Surveyor what action to take when a particular application (such as notepad.exe) is running on a PC and Surveyor attempts to transition a computer to standby or shutdown.

> ❗ **Important:** The Surveyor Idle Timer must be enabled to use power state transition rules in a scheme. (The Surveyor Idle Timer is enabled by default in schemes.)

Power state transition rules can prevent a PC from transitioning to standby or shutdown while a specified application is running. Power state transition rules can run as part of the background scheme, or as part of a scheduled power scheme. The rules take effect whenever their associated scheme takes effect, including the background scheme.

You can also run a script as part of a power state transition rule (see *Upload a Script for a Power State Transition Rule on page 6-29*, *Assign a Custom Script to a Power State Transition Rule on page 6-30Assign a Custom Script to a Power State Transition Rule on page 6-30*, and *Signing Power State Transition Scripts with Digital Certificates on page 6-32*.

> 📝 **Note:** Power state transition rules apply to Windows PCs only.

Power state transition rules can be useful for preventing data loss, such as when a user forgets to save changes in an open word processing document. They can also be useful for terminating applications (such as some media applications) that are known to cause problems when you need to restart a machine to install a patch.

> 📝 **Note:** Power state transition rules defined with the background scheme (on the **Background** tab of a policy) apply at all times unless rules are defined for the period when another scheme is scheduled using the **Insert Power Scheme** dialog box (via the **Schedule** tab for a policy). Background power state transition rules do not apply while a scheduled scheme is in effect. Only the power state transition rules defined for the scheme apply while the scheduled scheme is running.
> If you want the same background power state transition rules to apply during a scheduled power scheme, you must specify the same power state transition rules for the scheduled scheme.

Also see *Managing Open Applications During Power State Changes on the previous page*.

# Create and Edit Power State Transition Rules

To make a power state transition rule available for schemes in policies, you must have first created the rule.

The following procedure creates or edits rules that then become available for assignment to a background or scheduled power scheme. You can then assign a rule to a policy or background (for details, see *Create and Edit Policies on page 6-12*).

**Note:** Power state transition rules and settings apply to Windows PCs only.

1. On the Verdiem menu ⏻, click **Power Transition Rules**.

2. Click **New Rule**, select the **Rule Type**, and then click **Next**.
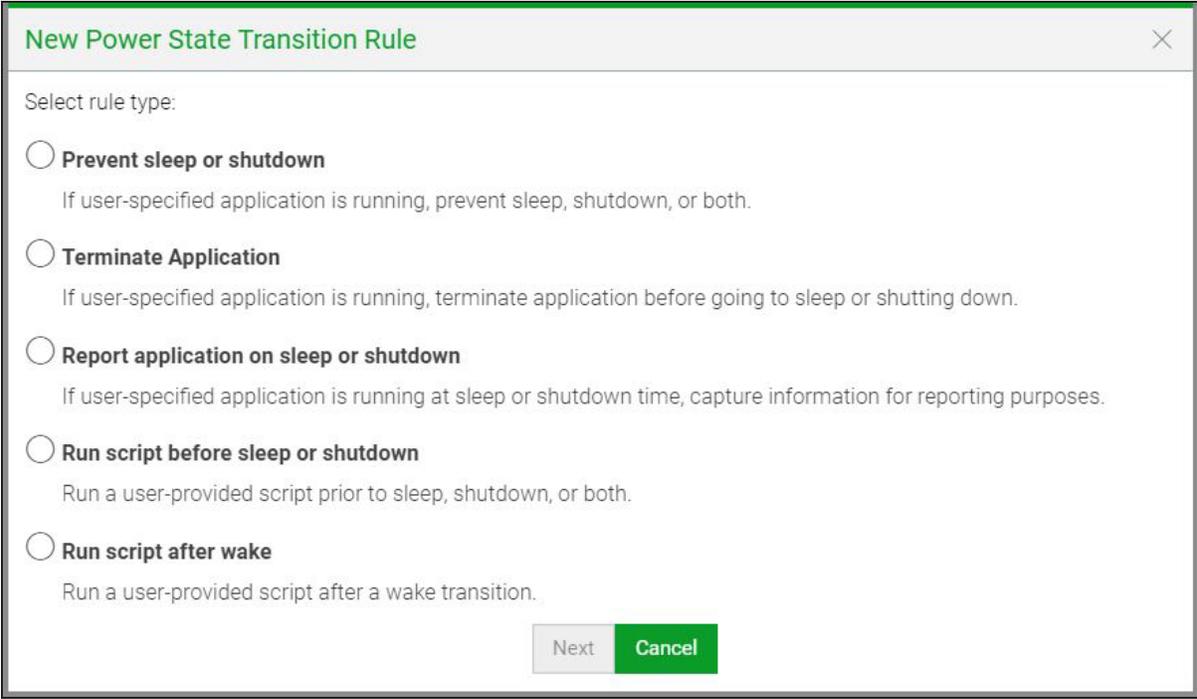


Or select an existing rule, and then click **Edit**.

3. For a new rule, type the name for the transition rule.



4. Type the exact name of the executable file for the application (such as *notepad.exe*, or select an existing .exe file by browsing.

> **Note:** Power state transition rules can apply to applications running locally, or on the network, or both. The application name that you provide should be the executable name as it appears in the Windows Task Manager under Processes.

5. Select the location of the executable file (Local, Network, or both).

6. Select the transitions the rule should apply to (Sleep, Shutdown, or both).

7. If you select a **Run Script** option, you will need to select a custom script that has been written in JavaScript or VBScript, and a code-signing certificate for the script must be installed on both the client and the Surveyor server. For details on using power state transition scripts, see *Upload a Script for a Power State Transition Rule on page 6-29*, *Signing Power State Transition Scripts with Digital Certificates on page 6-32*, and *Managing Open Applications During Power State Changes on page 6-24*.

## New Power State Transition Rule

Transition Rule Name: [                    ]

Group:  /My Organization/India

**Settings for: Run script before sleep or shutdown**

Run a user-provided script prior to sleep, shutdown, or both.

Application's executable file: [ Type file name or brow ]  **Browse**

Executable file location: [ Local and Network ▽ ]

Apply rule to:  ☑ Shutdown  ☑ Sleep

Script: [ Select a script.... ▽ ]

Execution context:  ⦿ Each User  ◯ System

Note:
This rule only applies to transitions initiated by Surveyor.
All power state transition events will be recorded by the server for reporting purposes.

[ Save ]  **Cancel**

8. Click **Save**.

   To apply a power state transition rule to the appropriate devices, you will need to add the rule to a scheme in a policy that is assigned to the devices. You can also assign a power state transition rule to the background scheme that runs when no other scheme is scheduled.

   To configure policy settings, see *Create and Edit Policies on page 6-12*. When you insert a scheme, you have the option to insert a power state transition rule.

   To assign a policy to a device, see *Assign Policies to Devices on page 4-20*.

# Upload a Script for a Power State Transition Rule

When you use a use a power state transition rule to prevent application errors during a power state change, you have the option to run a power state transition script. A power state transition script can include commands that cause the application to save its content in a temporary location, and perform any other necessary tasks.

Surveyor supports power state transition scripts written in JavaScript or VBScript. You must create and edit power state transition scripts outside of Surveyor, make sure they are digitally signed before you upload them, and then upload the scripts into Surveyor. For details on signing scripts, see *Signing Power State Transition Scripts with Digital Certificates on page 6-32*.

To upload scripts:

1.  On the Surveyor menu ⏻, click **Power Transition Rule**.

2.  Click the **Power Transition Scripts** tab, and then click **Upload Script**.

3.  Select the script and type a name for the script.

    You can view the code for the script by clicking **+ Show Script**.

4.  Click **Upload & Save**.

    The script is now available for power state transition rules when you select the **Run script before sleep or shutdown** or **Run script before sleep or shutdown** option in the New Power State Transition Rule dialog box. See *Assign a Custom Script to a Power State Transition Rule on the next pageAssign a Custom Script to a Power State Transition Rule on the next page*.

# Assign a Custom Script to a Power State Transition Rule

When you use a use a power state transition rule to prevent application errors during a power state change, you have the option to run a power state transition script. A power state transition script can include commands that cause the application to save its content in a temporary location, perform any other necessary tasks.

Surveyor supports power state transition scripts written in JavaScript or VBScript. You must create and edit power state transition scripts outside of Surveyor. Digital certificates for the scripts must be installed on both the client and the Surveyor server (see *Signing Power State Transition Scripts with Digital Certificates on page 6-32* and *Managing Open Applications During Power State Changes on page 6-24*).

To edit scripts:

1. On the Surveyor menu ⏻, click **Power Transition Rule**.

2. Click **New Rule** on the **Power Transition Rules** tab.

3. Click **Run script before sleep or shutdown** or **Run script after wake**, and then click **Next.**
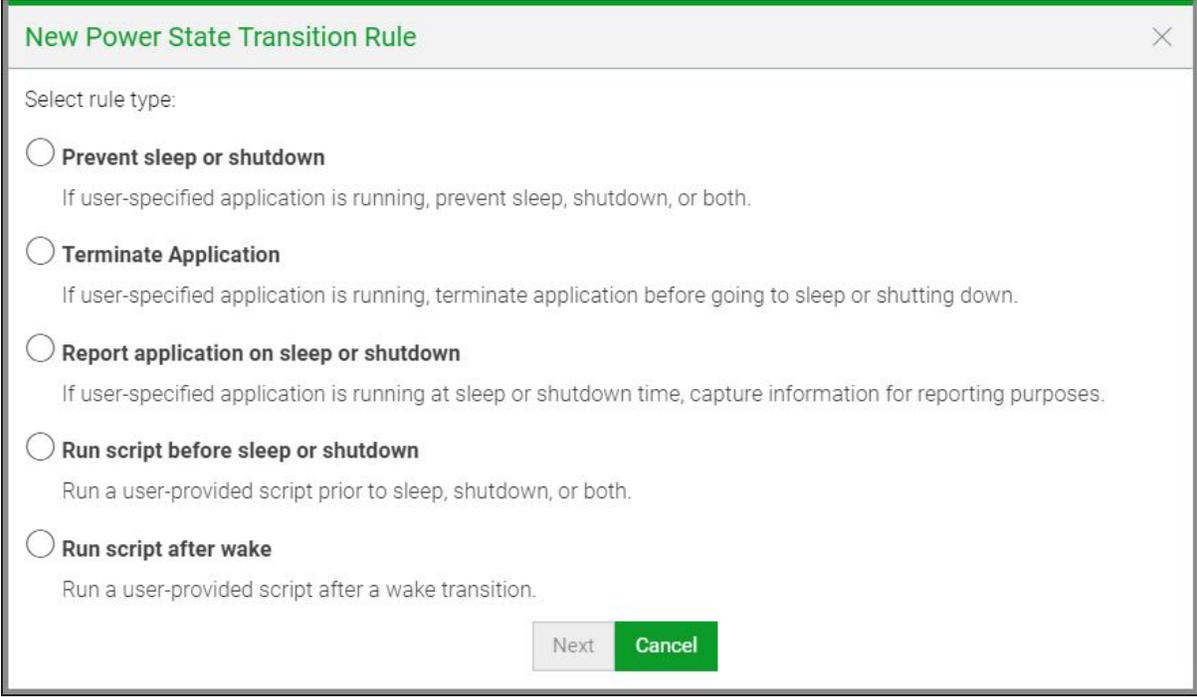


4. Type a name for the rule.

5. Type the exact name of the executable file for the application, or select an existing .exe file.

6.  Select the location of the executable file (Local, Network, or both).

7.  Select the transitions the rule should apply to (Sleep, Shutdown, or both).

---

**New Power State Transition Rule**

Transition Rule Name: [                    ]

Group: /My Organization/India

**Settings for: Run script before sleep or shutdown**
Run a user-provided script prior to sleep, shutdown, or both.

Application's executable file: [ Type file name or brow ] [ Browse ]

Executable file location: [ Local and Network ▽ ]

Apply rule to: ☑ Shutdown ☑ Sleep

Script: [ Select a script.... ▽ ]

Execution context: ⦿ Each User ○ System

Note:
This rule only applies to transitions initiated by Surveyor.
All power state transition events will be recorded by the server for reporting purposes.

[ Save ] [ **Cancel** ]

---

8.  Select a custom script (JavaScript or VBScript) that you uploaded to Surveyor.

> **Note:** A code-signing certificate for the script must be installed on both the client and the Surveyor server. For details on using power state transition scripts, see *Upload a Script for a Power State Transition Rule on page 6-29*, *Signing Power State Transition Scripts with Digital Certificates on the next page*, and *Managing Open Applications During Power State Changes on page 6-24*.

9.  Click **Save**.

    To apply a power state transition rule to the appropriate devices, you will need to add the rule to a scheme in a policy that is assigned to the devices. You can also assign a power state transition rule to the background scheme that runs when no other scheme is scheduled.

    To configure policy settings, see *Create and Edit Policies on page 6-12*. When you insert a scheme, you have the option to insert a power state transition rule.

    To assign a policy to a device, see *Assign Policies to Devices on page 4-20*.

# Signing Power State Transition Scripts with Digital Certificates

As a security measure, every script that can run as part of a power state transition rule must be signed with a digital certificate, and the certificate for the script must be installed on both the client and the Surveyor server.

You can use a self-signed certificate, or a certificate signed by a recognized Certificate Authority (CA). If multiple certificates are installed on the Surveyor server, you can select a specific certificate for each script.

## Using Self-signed Certificates

A CA certificate and a code signing certificate must be installed on the Surveyor server. The public portion of both certificates must be installed on each client machine.

To create a self-signed root CA certificate use the **makecert** program distributed with the Windows .NET 2.0 SDK.

1. Make sure that the folder containing the **makecert** and **certMgr** executable is in your Windows path system variable.

2. On the machine hosting Surveyor server, run the following from the command prompt:

```
makecert -n "CN=Local Surveyor Script Certificate Root" -a
sha1 -eku 1.3.6.1.5.5.7.3.3 -r -sv root.pvk root.cer -ss
Root -sr localMachine
```

3. Enter and re-enter a password.

   Two files are created: **root.cer** is the certificate that will be distributed to clients, and **root.pvk** is the private key portion that will be used to sign the code signing certificate.

4. Create a code signing certificate by running the following command:

```
makecert -pe -n "CN=Local Verdiem Scripting User" -ss MY
-a sha1 -eku 1.3.6.1.5.5.7.3.3 -iv root.pvk -ic root.cer
```

5. Enter the password you created for the CA certificate.

6. Install the public portion of the CA certificate on the client machine.

   Copy the **root.cer** file to the client machine and run the **certmgr.exe** program:

```
certmgr.exe /add root.cer /s /r localMachine root
```

If you don't want users to be required to verify that they trust the publisher, you must install the code signing certificate, in addition to the CA certificate, on the client machine:

1. Export the code signing certificate.

At the command prompt on the Surveyor server computer, type **certmgr.exe**, and then click **OK**.

2. Click the **Personal** tab.

3. Locate and select the code-signing certificate previously created.

4. Click **Export**.

> **Note:** Some versions of the Certificate Manager do not display an **Export** button. If this is the case, right-click on the certificate and choose **All Tasks** > **Export.**

5. Choose the option to not export the private key.

6. Select **DER encoded binary X.509 (.CER)**, or ensure that it is already selected.

7. Enter the name of the file for the exported certificate.

8. Click **Finish** in the wizard to export the certificate.

9. Copy the code signing certificate file to the client machine, and install it by running the following command:

```
certmgr.exe /add {certificate export file name} /s /r
localMachine trustedPublisher
```

# 7

## Managing GoGreen

**Table 7-1  In this Chapter**

| Topics |
| --- |
| Overview |
| Creating a New GoGreen Policy |
| Converting Existing Policies to GoGreen Policies |
| Converting a GoGreen Policy to a Non-GoGreen Policy |
| Advertising and Unadvertising GoGreen |

# Overview

The new GoGreen feature in Surveyor aims at improving energy savings by involving the end users in the process. The GoGreen feature spreads the responsibility of power savings right down to the end users. As a result, users become aware of their role in the power-saving process. This feature also provides more control to the end users, leading to improved efficiency in how Surveyor is used.

With GoGreen, the Administrator is able to advertise a GoGreen policy to the Agent Device at the group level or the device level. A GoGreen policy has all the capabilities of a Surveyor policy such as power schemes, power level changes, and power state transition rules. The difference is, the user has to accept the policy for it to take effect. The Administrator is able to unadvertise or edit a GoGreen policy as necessary. For more information on policy and power management see *Overview of Policies and Power ManagementSettings on page 6-2.*

Once a GoGreen policy is advertised, a GoGreen shortcut is created on the Agent Device's desktop. Opening the shortcut gives the user the option to either accept the advertised GoGreen policy or to stay with the default power management settings. The user has the option to switch back to default power management settings even after accepting a GoGreen policy. This allows the user to optimize power savings with GoGreen while having the flexibility to turn it off when necessary.

Features of GoGreen:

| Feature | Description |
|---|---|
| GoGreen Policy | GoGreen policies are similar to other Surveyor policies. GoGreen policies need to be accepted by the end user for them to take effect. |
| Advertise | Assign GoGreen policies to the end user. |
| Unadvertise | Unassign an advertised GoGreen policy and revert to default power management settings. |
| GoGreen Reports | · GoGreen Savings: Shows the savings made on devices with GoGreen policies applied.<br>· GoGreen Advertisement Statistics: Shows a comparison of savings between devices with GoGreen policies applied and devices without GoGreen policies applied. |
| Languages | GoGreen Agent UI is supported in English and French. |

# Creating a New GoGreen Policy

Any user with permissions to manage policies will be able to create GoGreen policies.

To create a new GoGreen Policy:

1. In the Administrator console, on the Verdiem menu ⏻, click **Policies**.
2. Click **New Policy**.
3. Type the policy name and a description.
4. Select **Mark as GoGreen Policy**. The policy name gets appended with a green icon.
5. On the **Schedule** tab, select a background power scheme that will be used when no other scheme is scheduled.

   You can optionally click the **Background** tab to select a background power scheme and also to specify power state transition rules that run when no other power state transition rules are scheduled.

6. Click **Insert Scheme** to add a scheduled power scheme to the policy.
7. Select the **scheme**, **days**, and **time range** and click **Insert**.

   Continue to add schemes as needed for the policy. (Scheduled power schemes cannot overlap.)

   To include a power state transition rule (or rules) to accompany the scheduled scheme:

   a. Click the **Power State Transition Rules** tab.

   b. Click **Insert**, select the rule (or rules) you want to add, and then click **Add**.

      Click **New Rule** to add a rule to the list.

      Power state transition rules can apply to applications running locally, on the network, or both. The application name that you provide should be the executable name as it appears in the Windows Task Manager under Processes, for example: **firefox.exe**.

   c. Click the **Schedule** tab when you are done.

8. On the **Insert Power Level Transition** menu, click a power state change to add it to the policy.

   For PCs and Macs only: If you select **Insert Sleep**, **Insert Hibernate** (PCs only), **Insert Shutdown**, or **Insert Restart** you can choose if you want to force the change in power state by selecting **Force transition**. You also can choose whether to force a transition for Wake on WAN proxies.

> **Note:** Use **Force transition** only when absolutely necessary. Some applications may block normal shutdown requests. For example, Word or Notepad may display a dialog box asking a user to save document changes. When you select **Force transition**, applications are prevented from blocking shutdown and any unsaved changes in the user's application will be lost.

For computers only: You can also specify whether users can skip or delay a transition and the message that is displayed for Sleep, Hibernate, Shut Down, or Restart.

> **Note:** Options for skipping, delaying, or forcing a transition, or displaying a message are ignored for non-computer devices.

9. Select the **days** and **time**, and then click **Insert**.

   Continue to add power state changes as needed for the policy.

10. Adjust the **Wake Settings** and **Data Collection** tab settings (these settings affect computers only), if needed.

   If you clear the **Collect power state data** option, power state change data will not be available in reports.

11. Click **Save**.

> **Note:** Refresh the browser to see policy changes in device lists.

> **Note:** A policy marked as GoGreen will not be listed on the Auto Policy Assignment Rules page in the Admin UI

# Converting Existing Policies to GoGreen Policies

To convert an existing policy to GoGreen:

1. In the Administrator console, on the Verdiem menu ⏻, click **Policies**.

2. Select the policy.

3. Select **Mark as GoGreen Policy**. The policy name gets appended with a green icon.

4. Click **Save**.

# Converting a GoGreen Policy to a Non-GoGreen Policy

To convert a GoGreen policy to a non-GoGreen Policy:

1. Unadvertise the desired GoGreen policy from all the agent devices to which it is advertised or applied. For further information see, *Advertising and Unadvertising GoGreen on the next page*

2. In the Administrator console, on the Verdiem menu ⏻, click Policies.

3. On the **Policies** page, under **Policy Name**, select the desired GoGreen policy.

4. Clear the **Mark as GoGreen Policy** check box and click **Save**.

# Advertising and Unadvertising GoGreen

Any user with permissions to assign policies will be able to advertise and unadvertise GoGreen policies.

## Advertising a GoGreen Policy:

GoGreen policies are advertised at the group level or the device level.

To advertise at a group level:

1. In the Administrator console, on the Verdiem menu ⏻, click **Computers**.
2. In **Group Navigator**, right-click on the required group and select **Advertise GoGreen**.
3. In the **Advertise GoGreen to Group** pop-up window, select the required policy and click **OK**.

To advertise at a device level:

1. In the Administrator console, on the Verdiem menu ⏻, click **Computers**.
2. Select the required devices.
3. Under **Item Actions**, select **Advertise GoGreen**.
4. In the **Advertise GoGreen to Device** pop-up window, select the required policy and click **OK**.

> **Note:** If a device has GoGreen advertised on it, **Manually assign policy** and **Run policy assignment rules** cannot be used on the device.

## Unadvertising a GoGreen Policy:

GoGreen policies can be unadvertised at the group level or the device level.

To unadvertise at a group level:

1. In the Administrator console, on the Verdiem menu ⏻, click **Computers**.
2. In **Group Navigator**, right-click on the required group and select **Unadvertise GoGreen**.
3. In the **Unadvertise GoGreen** pop-up window, click **OK**.

To unadvertise at a device level:

1. In the Administrator console, on the Verdiem menu ⏻, click **Computers**.
2. Select the required devices.
3. Under **Item Actions**, select **Unadvertise GoGreen**.
4. In the **Unadvertise GoGreen** pop-up window, click **OK**.

# Adding the GoGreen Status Column:

The **GoGreen Status** column on the **Computers** page shows the GoGreen status of each device.

To insert a **GoGreen Status** column:

1.  In the Administrator console, on the Verdiem menu ⏻, click **Computers**.
2.  On the **Computers page**, click **Customize View**.
3.  In **Choose Columns to Display** window, click **Advanced** tab and select **GoGreen Status**.
4.  Click **Save**.

The following table describes the GoGreen status.

**Table 7-2  GoGreen Status**

| Status | Description |
|---|---|
| Not Advertised | No GoGreen policy is advertised to the device. |
| Advertised | A GoGreen policy is advertised to the device, but the policy is not accepted by the user. |
| Accepted | The advertised GoGreen policy is accepted by the user.<br><br>📝 **Note:**  The **Assigned Policy** column will display the name of the accepted GoGreen policy. |

# 8

# Waking Computers

**Table 8-1  In this Chapter**

| Topics |
| --- |
| *Waking Clients from a Low Power State* |
| *Determine Whether Windows Computers can wake from Low Power States* |
| *About Wake on WAN* |
| *Wake Selected Devices* |
| *Wake Devices on a Regular Schedule* |

# Waking Clients from a Low Power State

The method you choose to wake computers from the server depends on the context. For example, if you want to set up a patch management schedule, you might want to wake computers once per week at a specific time of day and for a specific length of time. Or if you want to wake computers on demand, you might use a Wake on LAN magic packet. This section describes the methods through which you can wake computers, with guidelines on which method to use when.

This topic describes the ways that you can set wake events through the server, as well as the ways end users can wake their own computers.

## Waking Clients Through the Server

You can set up the server to wake clients as part of power management policies, to prepare them to receive patch updates, or to troubleshoot issues. Through the server, you can wake clients the following ways:

- Schedule a wake event in a policy.

  For example, wake computers at 6:00 every morning before end users come in for their work day.

- Schedule a Wake on WAN event in a policy to send a Wake on LAN magic packet to proxy computers, after which proxies wake the remaining clients on their subnets.

  A standard scheduled wake event can wake computers from the sleep state, but cannot wake computers that have been turned off. If you want to reach as many clients as possible for a system update, set a Wake on LAN event to run shortly after a standard wake operation.

  > **Note:** Most computers manufactured within the past couple of years are enabled for Wake on LAN by default. However, if you have some older computers or network cards, you might need to enable Wake on LAN on those computers. For information see *Configure Client Computers for Wake on LAN on page 8-4*

- Select a set of clients in the Administrator console and manually choose the Wake command.

You might do this if you need to apply an urgent patch update that cannot wait until your next scheduled maintenance window.

# How End Users Can Wake Their Computers

End users can wake their computers if they want to use them during a time when the computers are normally transitioned to the sleep state.

- Depending on the computer and device settings, an end user can wake his or her computer by moving the mouse, pressing the Enter key on the keyboard, or tapping the power button.

- If you have users who need to access their client computer from a remote location, you can implement the Surveyor Wake for Remote Access functionality, so they can wake the computer through a web browser.

For more details, see *Overview - Wake for Remote Access on page 11-2*.

> **Note:** Part of minimizing the impact of centralized power management on end users is to make sure that device drivers on client computers are up-to-date and support the methods for waking computers as described in the list above.

# Configure Client Computers for Wake on LAN

This topic provides some examples for when you might use Wake on LAN, as well as some general configuration information that you can adapt for your equipment.

If you are not familiar with the Surveyor Wake on WAN concepts yet, see *About Wake on WAN on page 8-10* in the before you read this topic.

You might need to configure client computers for Wake on LAN if:

- they can transition to standby but wake immediately after.
- you have followed the steps for enabling Surveyor Wake on WAN, and some clients do not respond to wake requests sent by Wake on WAN proxies.

> **Note:** Computers that are not enabled for Wake on LAN cannot receive wake requests that are sent through Wake on LAN specifically. However, you can create Surveyor scheduled tasks for power-state changes and measure energy use on those computers.

## Configuring a Computer for Wake on LAN

Wake on LAN is enabled in the computer's BIOS and the network card.

The information in these steps assumes that you are using up-to-date hardware that supports Wake on LAN. Your settings might vary slightly. If you have specific questions about Wake on LAN support on your systems, refer to the documentation provided by the hardware vendor.

### To Configure a Computer for Wake on LAN

1. In the Control Panel, open the network card's dialog box.

   **On Windows Vista:**

   a. In the Windows Control Panel, open **Network Connections**, right-click the connection that the computer uses, and choose **Properties**.

   b. On the **General** tab, click **Configure**.

   **On Windows 7, Windows 8 and Windows 10:**

   a. In the Windows Control Panel, open **Network and Internet** > **Network and Sharing Center** > **Change Adapter Settings**.

   b. Right-click the connection that the computer uses, and choose **Properties**.

   c. On the **Networking** tab, click **Configure**.

2. On the Advanced tab of the network card's dialog box, select the following

| Property | Value |
|---|---|
| **Wake From Shutdown** | Enabled or On |
| **Wake-Up Capabilities** | Magic Packet or Enabled (depending on the choice) |

3. On the Power Management tab, select all three check boxes, and then click **OK** and close the Control Panel.
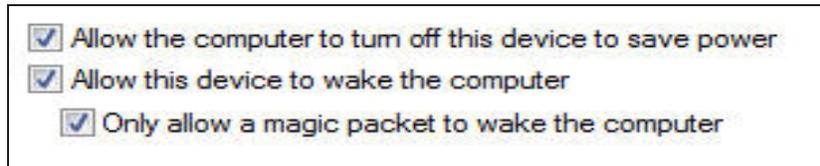


**Tip:** When you have clients that do not stay in standby because network traffic wakes them up, selecting **Only allow management stations to bring the computer out of standby** resolves the problem.

4. To configure the BIOS, you need to restart your computer, and during the startup process, press the keyboard key that it indicates to enter the BIOS settings. This option appears before Windows starts, and it can vary depending on the computer.

When you have access to the BIOS settings, you enable settings related to devices waking the computer.

For more information, see *Manually Configure the BIOS for Wake on LAN (Windows Only) on page 8-16* or the computer manufacturer's documentation.

# Configure Wake on Demand on a Mac OS X Computer

This topic contains basic steps for enabling Wake on Demand. It also provides a link to a recommended Apple Support article for OS X v10.6 computers. For best results, use the information here alongside the specified support article.

1. Open the **System Preferences**, and then open the **Energy Saver** pane.

2. Click Options, and then select the check box that enables waking for network access.

   The specific text that you see for the check box indicates the capabilities of the Mac:

   | Check box text | Indicates the Mac supports Wake on Demand over |
   | --- | --- |
   | **Wake for network access** | Both Ethernet and AirPort |
   | **Wake for Ethernet network access** | Ethernet only |
   | **Wake for AirPort network access** | AirPort only |

   On computers older than v10.6, the text might show **Wake for Ethernet network administrator access**, wake support is not as extensive as with Wake on Demand.

3. For further instructions, see the following article on the Apple Support site:

   - About Wake on Demand

   This article describes how the Wake on Demand service works and lists its key features. It also contains complete instructions for setting up Wake on Demand, with additional information for waking from a Windows computer, waking portable computers, and waking over wireless networks.

   **Note:** Mac OS X does not support Wake on WAN/LAN from the off state (only from sleep). For details, see .

# Determine Whether Windows Computers can wake from Low Power States

Most Surveyor-compatible computers support transitioning to a low power states and waking through a user action. If any of your users has a problem waking a computer, however, you can perform simple tests to determine the computer's wake support.

This procedure contains standard tests for determining a computer's wake capabilities. Following the procedure are suggestions for next steps depending on the results.

1. If the computer is on, transition it to sleep through the Windows Start menu.

2. Do any of the following to test wake capability:

   - Press a key on the keyboard.

   - Move or click the mouse.

   - Press the power button for one second. (Holding the button down longer might shut down the computer.)

3. Repeat the previous two steps, so that you try each method of waking the computer.

**Next steps**

- If the computer wakes when you press the power button but not through the keyboard or mouse, you can enable the keyboard and mouse. See *Configure Mouse or Keyboard to Wake the Computer (Windows) on the next page*.

- If the computer does not wake when you press the power button, see Pressing power button does not wake computer on the Verdiem Knowledge Base.

# Configure Mouse or Keyboard to Wake the Computer (Windows)

If you've confirmed that mouse or keyboard actions do not wake a Windows computer from sleep, you can enable them to do so.

1. Open the Windows Control panel, and open Device Manager.

2. Select either the **Mouse** or **Keyboard**, then right click and click **Properties**.

3. On the Power Management tab, select **Allow this device to wake the computer**.





> **Note:** If a Power Management tab does not appear in the Mouse or Keyboard Properties dialog box, the device might not support waking from sleep. To support this action, you might need to upgrade the driver or the device itself.

# Configure Wake on Mouse/Keyboard from the Administrator Console (Windows)

In some cases, you need to configure support for end users waking their computers through the mouse or keyboard. You can enable multiple devices at once through the Administrator console.

1. On the Verdiem menu ⏻, click **Policies**, select a policy in the list, and then click the **Wake Settings** tab.

2. Under **Basic Settings**, set the following:

| Setting | Set to |
|---|---|
| **Wake on mouse movement** | Enable |
| **Wake on keyboard press** | Enable |
| **Require password on wake** | As appropriate for your organization |

3. Under **Advanced Settings**, enable all settings.

> **Note:** If you change these settings in an individual policy, that policy will not inherit future changes you make to the policy defaults.

For information about the **Wake on WAN Settings** section, see *About Wake on WAN on the next page*.

# About Wake on WAN

Wake on WAN extends Wake on LAN technology to provide a reliable and practical method for waking computers over a large-organization network. It also complies with the standard IT practice of preventing data packets from routing across subnet boundaries.

## Wake on WAN Overview

Surveyor wakes computers in a network through Wake on WAN proxy computers. When Wake on WAN proxies are enabled, Surveyor auto-elects Windows or Mac clients on each subnet to serve as primary and secondary Wake on WAN proxies. While other computers transition to a low power state during periods of inactivity, the proxy computers CPUs are kept awake. The primary proxy on each subnet works with the Surveyor server to receive wake requests and forward them to client peers on the same subnet.

By default, Wake on WAN proxies are not enabled when you first start Surveyor for baseline data collection. After the baseline period is over, it is recommended that you set the proxy number to 2 per subnet.

Why elect two Wake on WAN proxies? If the existing primary proxy experiences a problem that interferes with its ability to communicate with the server, the server can immediately promote the secondary proxy to primary. At the same time, the server uses built-in and configurable selection criteria to select another computer on the subnet, waking it if necessary, to act as the new secondary proxy.

You can select as many proxies as you want per subnet (or even specify zero proxies for subnets in which you don't ever want to wake computers from Sleep or Off). However, best practice is to designate at least two.

## How Wake on WAN Works
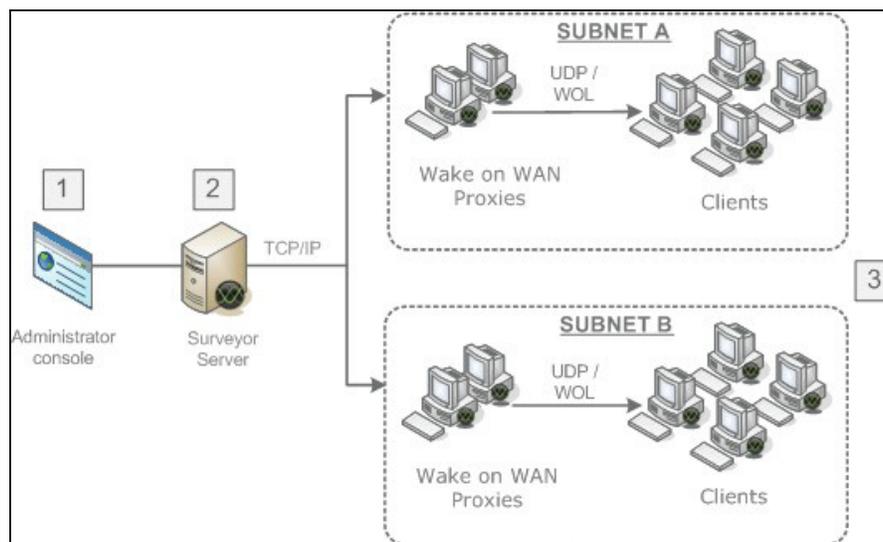
1. Wake request is sent to the server from the Administrator console (on schedule through power scheme or on demand by administrator).

2. Server receives request and sends Wake on LAN magic packet to Wake on WAN proxies on each subnet.

3. The proxy acting as primary receives the message and sends a Wake on LAN packet that contains the target client's MAC address over its subnet. The target computer receives the Wake on LAN packet and wakes.

> **Note:** The additional Wake on WAN proxy role is performed alongside the primary role as a Surveyor client agent. For example, a client elected as a primary proxy forwards wake requests to other clients within the broadcast domain and continues to capture user activity levels. This eliminates the need to install additional agents.

# Network-specific Wake on WAN Configurations

Surveyor Wake on WAN includes optional settings for specifying network-specific configurations to override the default proxy count or to configure networks for subnet-directed broadcasts. For details, see *Configure Specific Networks for Wake on WAN on page 8-23* and *Configure Specific Networks for Wake on WAN on page 8-23*.

Each network that you specify for Wake on WAN can include multiple subnets with Surveyor clients. Surveyor will maintain the number of Wake on WAN proxies that you specify for each subnet.

For networks that use port-based network access control (PNAC), you can specify broadcast networks that will be used with Wake on WAN to wake computers when sleeping computers move from an authorized network to a different, unauthorized network. Additional broadcast networks are especially useful where 802.1x network security is deployed and devices change networks when they are turned off or sleeping. For details, see *Configure Specific Networks for Wake on WAN on page 8-23* and *About Wake on WAN and Port-based Network Access Control on page 8-26*.

> **Note:** Switches for the networks that you specify as additional broadcast networks must be configured to receive subnet-directed broadcasts from the Surveyor server. See your switch manufacturer documentation for details.

## Setting up the System for Wake on WAN

Wake on WAN is disabled by default on the Surveyor server.

To enable Wake on WAN:

- Set Wake on WAN to be enabled in Surveyor server, and also enable policy wake settings. For details, see *Enable Policy Wake on WAN Settings on page 8-18*.

- Confirm that Wake on LAN is enabled on client computers. For information, see *Configure Client Computers for Wake on LAN on page 8-4*.

**Wake on WAN versus scheduled wake from sleep**

If your power management policies include scheduled wake requests, waking a computer from sleep this way does not always require Wake on LAN functionality. Enable Wake on WAN if you want to wake clients for operations that are not on a regular schedule, or to wake them from an off state. For best practice information about when to use either method, see *Wake Devices on a Regular Schedule on page 8-33*.

## How Surveyor Determines Subnet Boundaries

Surveyor uses IP network number clustering and assumes that computers within the same IP network number can broadcast Wake on LAN packets to each other.

The primary Wake on WAN proxy that receives the magic packet broadcasts it to the remaining clients on the subnet using port 7 and the subnet broadcast address. This address is formed by using the subnet's prefix, followed by all 1s. For example for 10.35.0.0/255.255.255.0 the broadcast address would be 10.35.0.255.

---

**Note:** Surveyor 5.2 and 5.3 clients broadcast magic packets through port 9. If you used either of these earlier versions and configured the firewall for port 9, make sure that you update the firewall settings to allow communications through port 7.

---

# How Surveyor Elects Wake on WAN Proxies

Surveyor uses a built-in selection criteria for selecting new proxies. This helps you determine which devices to set as preferred proxies or to never be proxies.

## Device Ranking for Proxy Selection

In the Administrator console, you can specify Wake on WAN proxy preference for devices in the device properties (right-click selected devices and choose Device Properties).

When the Surveyor server detects that it needs to select a new Wake on WAN proxy for a broadcast domain, it uses this preference setting along with other criteria to determine which device to select. It does so in the following order of preference:

1. Devices with the **Wake on WAN proxy** preference setting of **Preferred**.
2. Devices with a **Wake on WAN proxy** preference setting of **Default** if the device is not a laptop.
3. Laptops with a **Wake on WAN proxy** preference setting of **Defaul**t.

The server runs through a series of additional checks to determine whether the computer meets other requirements for relaying data packets. For example, it confirms that the device's network card, IP address, and subnet mask are set properly for Wake on LAN within its broadcast domain.

**Note:** If a new device joins a broadcast domain, and it has a higher preference ranking than an existing proxy, Surveyor will un-assign the existing proxy and select the new device in its place.

### Determining Which Devices to Set as Preferred Proxies

Wake on WAN proxies remain on at all times. Therefore, some devices are more appropriate than others to serve as proxies. For example, devices that need to be on 24/7 to serve critical functions are good candidates to set as preferred proxies.

On the other hand, laptops tend to be moved around frequently, so it's better to set as many laptops as you can to never be preferred proxies, and leave the remaining laptops in the default setting.

Beyond these two suggestions, the best practice is to leave most devices with the **Wake on WAN proxy** preference setting of **Default**, and allow Surveyor to use its built-in criteria to select new proxies as needed.

# Determine Wake on LAN Support for Computers

To use Surveyor Wake on WAN, computers must be enabled for Wake on LAN (Windows) or Wake on Demand (Mac). Here are some basic steps, along with symptoms that can indicate that computers are not enabled.

## Wake on LAN in Windows Computers

In most cases, Windows computers are Wake on LAN capable when they are:

- Purchased and deployed within the last five years.
- Qualified as Energy Star version 4.0 and later.

However, even if a computer supports Wake on LAN, it may not be enabled by default.

Issues that can indicate that computers are not enabled for Wake on LAN include:

- They can transition to a low power state, but they wake immediately after.
- You have followed the steps for enabling Wake on WAN, and clients do not respond to wake requests sent by Wake on WAN proxies (originating either from a power scheme or an on-demand wake request that you initiated in the Administrator console).

To test Wake on LAN support among a group of computers, you can send a wake request manually from the Administrator console.

Wake on LAN is enabled in the Windows computer's BIOS and the network card (NIC), so settings vary among hardware manufacturers. If you cannot determine whether a computer supports Wake on LAN by using these simple guidelines, the best place to find information specific to the computer is in the documentation provided by the hardware vendor.

> **Note:** Surveyor clients that do not support Wake on LAN can still receive wake requests that you schedule in the Administrator console. You can also continue to measure power use on those clients. These clients are also good candidates for Wake on WAN proxies. For information, see *Set a Client to be a Preferred Wake on WAN Proxy on page 8-20*.

## Wake on Demand in Mac OS X Computers

Starting with OS X v10.6 (Snow Leopard), remote wake, called *Wake on Demand*, is enabled by default. It works along with the Bonjour Sleep Proxy service, which runs on an AirPort Base Station or Time Capsule.

You can read more in Apple Support article Mac OS X v10.6: About Wake on Demand.

# Enabling Wake on LAN or Wake on Demand

If you determine that clients support Wake on LAN, but it is not enabled, see the following topics:

- *Manually Configure the BIOS for Wake on LAN (Windows Only) on the next page*
- *Manually Configure the BIOS for Wake on LAN (Windows Only) on the next page*
- *Configure Wake on Demand on a Mac OS X Computer on page 8-6*

# Manually Configure the NIC for Wake on LAN (Windows Only)

1. In the Control Panel, open the network card's dialog box.

    **On Windows Vista:**

    a. In the Windows Control Panel, open **Network Connections**, right-click the connection that the computer uses, and choose **Properties**.

    b. On the General tab, click **Configure**.

    **On Windows 7, Windows 8 and Windows 10:**

    a. In the Windows Control Panel, open **Network and Internet > Network and Sharing Center > Change Adapter Settings**.

    b. Right-click the connection that the computer uses, and choose **Properties**.

    c. On the **Networking** tab, click **Configure**.

2. On the **Power Management** tab (or **Advanced** tab, depending on the driver) of the network card's dialog box, look for Wake on LAN settings such as the following

| Property | Value |
|---|---|
| **Wake From Shutdown (or power off state)** | Enabled or On |
| **Wake-Up Capabilities or Wake on LAN** | Magic Packet or Enabled (depending on the choice) |

3. Also look for and enable settings such as the following, which allow management systems to initiate power state changes.
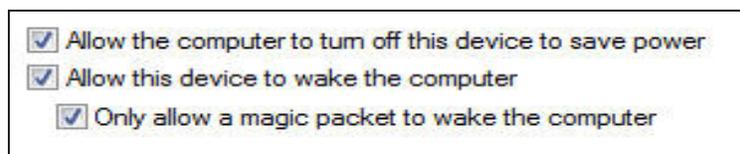
💡 **Tip:** When clients do not stay in a low power state because network traffic wakes them up, selecting **Only allow management stations to bring the computer out of standby** resolves the problem.

📝 **Note:**

• If you update the NIC driver, the settings you change in this procedure may revert back to their defaults, which can prevent the client from following Surveyor power management policies. Be sure to check these settings any time you update the NIC driver.

• If you use a Dell Optiplex computer, see the Verdiem Knowledge Base article Dell Optiplex computers do not wake from off using default Wake on LAN settings.

# Manually Configure the BIOS for Wake on LAN (Windows Only)

1. Restart the computer.

2. During the startup process, press the keyboard key indicated to enter the BIOS settings. This option appears before Windows starts, and it can vary among computer vendors.

3. When you have access to the BIOS settings, look for the settings related to devices waking the computer, and enable these devices. For specific settings, refer to the hardware documentation.

Example of Wake on LAN BIOS settings on a Dell computer.
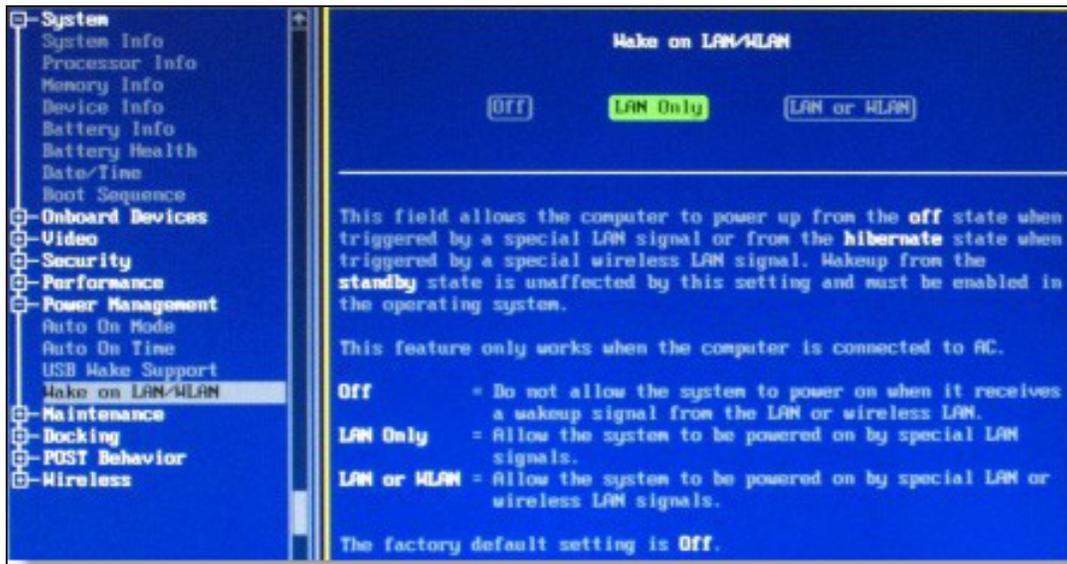
Example of Wake on LAN BIOS settings on an HP computer.
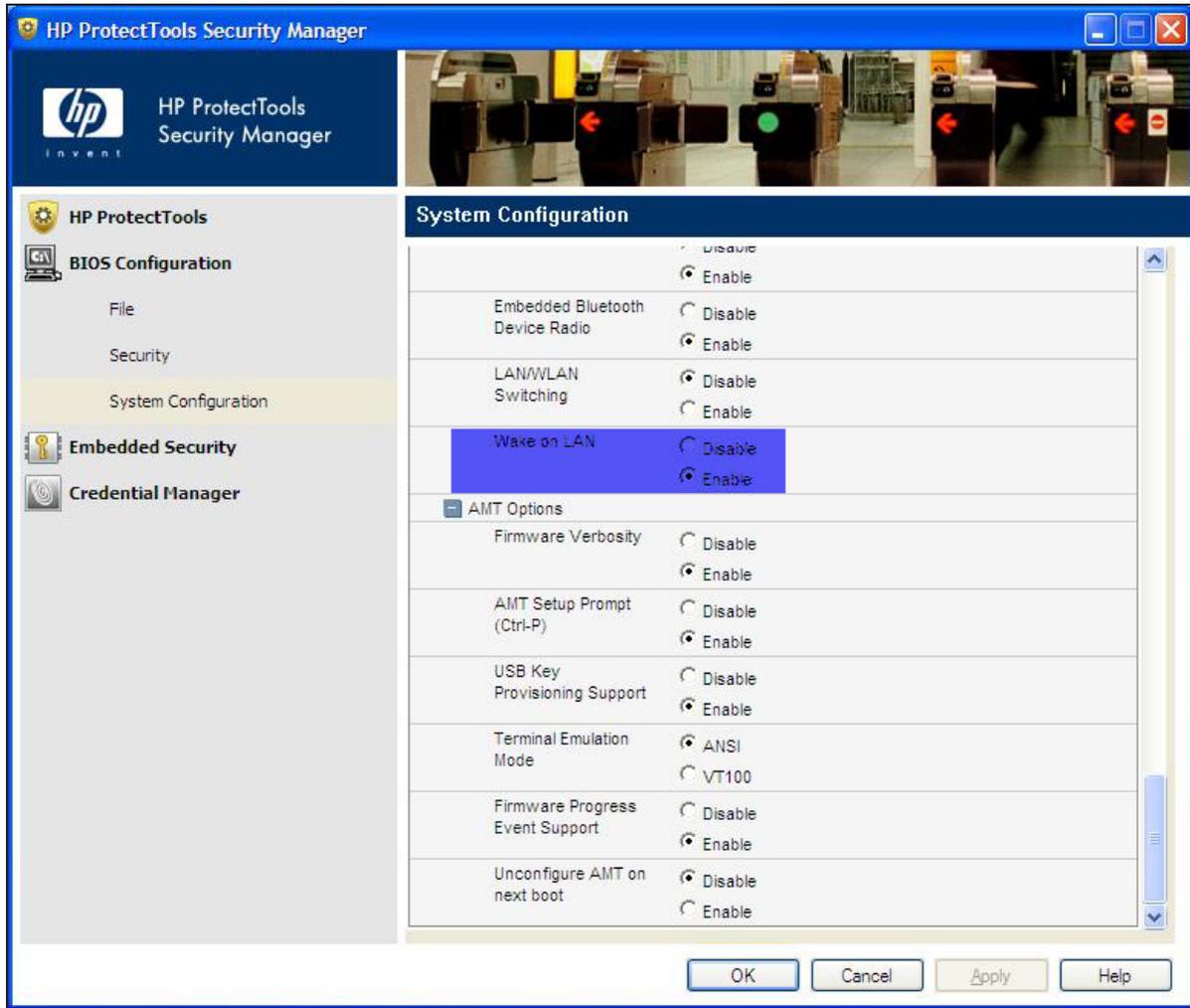
# Enable Policy Wake on WAN Settings

Along with making sure client computers are enabled for Wake on LAN, you enable Surveyor Wake on WAN in your policy settings.

You can change wake settings for a specific policy, or you can set new policy default wake settings.

1.  On the Surveyor menu ⏻, click **Policies**, select a policy in the list, and then click the **Wake Settings** tab.

    > **Note:**  You can change wake settings for a specific policy, or you can set new policy default wake settings.
    > **To change the settings that all new policies created will inherit**:
    > • On the Configure menu, click **Policy Defaults**, and then click the **Wake Settings** tab.

2.  Under **Wake on WAN Settings**, select **Enable all settings**.

On Windows computers, these settings correspond to the network card settings that you configure through the Windows Control Panel. For Mac clients, the only setting that is used is **Wake on magic packet only** (which can be enabled only when the other two are enabled as well).

> **Note:**  The remaining settings on this tab also apply only to Windows clients.
> For more information, see *Enable Policy Wake on WAN Settings above*.

After you enable the wake settings, run a test wake operation through Wake on LAN. If some clients do not respond, you might need to configure the network card and BIOS separately on those clients.

## Wake Settings Descriptions

This topic lists and defines the settings on the **Wake Settings** tab, which is part of creating and editing policies.

These settings affect how you can wake PCs from the Administrator console, as well as how end users can wake their own PCs.

You can change wake settings for a specific policy, or you can set new policy default wake settings.

**To change the settings that all new policies created will inherit:**

- On the Configure menu, click Policy Defaults, and then click the Wake Settings tab.

**To change the settings for a specific policy:**

1. In the Administrator console, on the Surveyor menu ⏻, click **Policies**.

2. Select that policy in the list, and then click the **Wake Settings** tab in the main content section and change the settings as needed.

> **Note:** The setting **Don't change** means to use whatever is set in the operating system or hardware for this action.

# Basic Settings (Windows Clients Only)

These settings affect how end users can wake their computers from a sleep state.

- **Wake on mouse movement and Wake on keyboard press**: These are enabled by default, so that users can move the mouse or press a key on the keyboard to wake their computers.
- **Require password on wake**: Enable this setting to add a layer of security to waking on mouse movement or keyboard press.

# Advanced Settings (Windows Clients Only)

| Turn on display on wake | Turns on the monitor when a wake request is sent through Wake on LAN or policy schedule change. |
|---|---|
| Wake enable USB | Enable this for USB mouse or other pointing devices. |
| Allow suspend with remote user | Use this and you wish to change the default behavior in Surveyor that keeps remote sessions always on. |
| | If this setting is enabled, the computer is able to transition to a low power state according to the scheme set for it, while the user is logged in from another location but is not active on the computer. |
| | If this setting is not enabled (default), the computer remains on while the user is logged in, regardless of activity. |

# Wake on WAN Settings (Windows and Mac Clients)

The three settings in this section correspond to Windows network card settings, with the third setting (Wake on magic packet) also applying to Mac computers. All three essentially work together to enable Surveyor clients to wake through a Wake on LAN magic packet.

All of these settings are enabled by default, to enable the Surveyor Wake on WAN feature. For information, see *About Wake on WAN on page 8-10*. If you do not want to use Wake on WAN, select **Disable all settings**.

# Set a Client to be a Preferred Wake on WAN Proxy

If you enable Wake on WAN, you might also want to designate particular clients that Surveyor will check first when it needs to select a new Wake on WAN proxy. These steps show you how to do that.

1. In the Administrator console, on the Surveyor menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

   Or, in the Administrator console, click the Search button 🔍 and filter the device view.

   Configure the search filters to match the attributes of the computers that you want to set as preferred proxies, or that you want to set to never be selected as a proxy.

   > 📝 **Note:** For tips and more information, see *How Surveyor Elects Wake on WAN Proxies on page 8-13*.

2. Select one or more of the computers in the device list, and then from the **Item Actions** menu, click **Edit Device Properties**.

3. In the Edit Device Properties dialog box, select the **Wake on WAN proxy preference** check box, and then select the setting that you want for the selected computers.

   - **Preferred** increases the ranking of the selected computers in the proxy-selection criteria.
   - **Never** prevents the selected computers from being selected as proxies.
   - **Default** means that other computer attributes will be used as selection criteria, and these computers are selected only if there are no preferred proxies available.

# Set the Number of Wake on WAN Proxies Per Broadcast Domain

By default, Surveyor designates two Wake on WAN proxies per broadcast domain, a primary and secondary. You can use the server settings page to change the number assigned within each broadcast domain.

This information assumes that you are familiar with Wake on WAN, and it applies only to policies in which you enabled this feature. For more information, see *About Wake on WAN on page 8-10*.

1. In the Surveyor Administrator console, on the Configure menu ⚙, click **System Settings**.

2. Under **Server Settings**, use the arrows or enter a value for **Number of computers to keep awake as Wake on WAN proxies**.



> Note: Two proxies per broadcast domain is the recommended minimum. This ensures that a secondary proxy can take over if the primary proxy becomes unavailable. If your environment includes broadcast domains with fewer than six devices, work with a professional services consultant to determine the best settings for your environment.

3. If you <u>increase</u> the number of proxies per broadcast domain, save the new settings. You do not need to complete the remaining steps. Surveyor selects the additional proxies based on its built-in selection criteria, as well as Preferred Proxy settings that you can set on individual clients.

   If you <u>reduce</u> the number of proxies, complete the remaining steps to change the settings on the clients that you want to clear of proxy status.

4. In the Administrator console, click the Search button 🔍.

5. On the Search tab, use the **By Subnets** filter and specify the subnets to display.

6. In the device view, make sure the **Wake on WAN Proxy** column is displayed.

If it isn't, click **Customize View**, and select it on the **Troubleshooting** tab. After you display the column, you can drag it to the left, so you don't have to scroll to see it.

7. Click the Wake on WAN Proxy column heading once or twice to sort the display with the proxies listed at the top.

8. Determine which of the proxies you want to run as standard devices (that is, transition to low power states according to policies assigned to them). Select them, and on the **Item Actions** drop-down menu, click **Edit Device Properties**.

9. For **Preferred Wake on WAN proxy**, select **Never**.

   After you change the setting, a polling interval set on proxies can take them up to 15 minutes to receive the change from the server.

10. When all of the devices you selected are cleared of proxy status, you can then set the **Preferred Wake on WAN proxy** setting on any of them to **Preferred** or **Default**, so that they can be returned to the pool of devices that are available for proxy selection.

For information about preferred Wake on WAN proxy settings, see *Set a Client to be a Preferred Wake on WAN Proxy on page 8-20*.

Also see: *Configure Specific Networks for Wake on WAN on the next page* and *Configure Specific Networks for Wake on WAN on the next page*.

# Configure Specific Networks for Wake on WAN

Surveyor uses IP network number clustering and assumes that computers within the same IP network number can broadcast Wake on LAN packets to each other. You can specify the subnets on which Surveyor maintains proxies, and also the number of proxies per subnet.
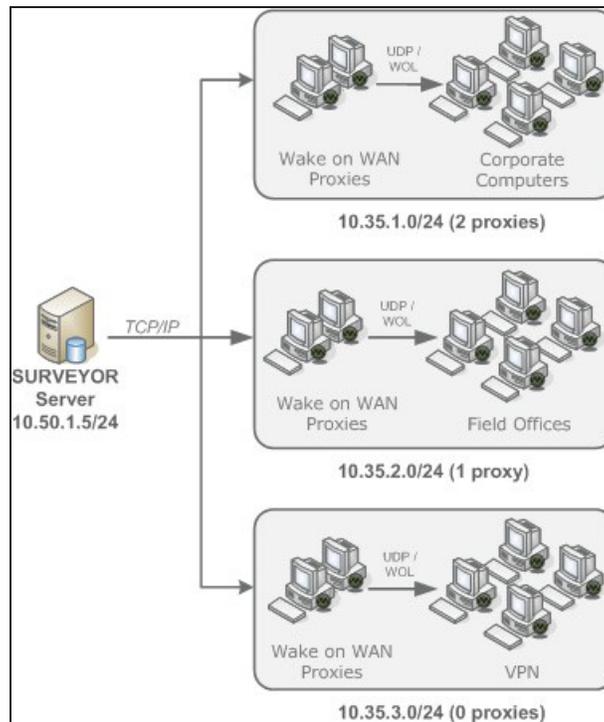


Two proxies per broadcast domain is the recommended minimum. This ensures that a secondary proxy can take over if the primary proxy becomes unavailable. However, for a network where you don't want any computers to wake from Off or Sleep, set the proxy count for that network address to 0 proxies. If your environment includes broadcast domains with fewer than six devices, work with a professional services consultant to determine the best settings for your environment.

1. In the Surveyor Administrator console, on the Configure menu ⚙, click **System Settings**, and then click **Wake-on-WAN Configuration**.



2. In the **Wake-on-WAN Configuration** dialog box, click **Add**.

3. For **Address block**, type the network address of the subnet and the number of proxies to be kept awake per subnet.

Add new wake-on-WAN configuration                                                                    ✕

For any block of IP addresses, you can configure:

- How many WOW Proxies will be kept awake in each subnet within the block.
- How and where Wake-on-LAN packets will be sent to awaken computers.

A single Address Block in Wake-on-WAN Configuration can span many subnets. For example: to configure all the subnets starting with 10.10.*.*, you can use the address block 10.10.0.0/16.
For more examples, search for "Wake-on-WAN Configuration" in the Surveyor knowledge base.

AddressBlock:                                          Number of proxies:

10.35.3.0/24                                           0

☐ Use subnet-directed broadcast
Additional broadcast networks (comma-separated):

Description

VPN Computer

Save    Cancel

**Note:** Address blocks can be entered as either IP address and netmask pairs (such as 192.168.10.0 255.255.255.0) or by using CIDR notation (such as 192.168.10.0/24).

4. Type a **Description** to help you identify the network and its Wake on WAN settings.

5. Click **Save**.

# Override the Default Number of Wake on WAN Proxies on a Network

Surveyor auto-elects two Windows or Mac clients on each subnet to serve as primary and secondary Wake on WAN proxies. However, you can specify the number of proxies that Surveyor maintains for each subnet.

You can select as many proxies as you want per subnet (or even specify zero proxies for subnets on which you don't ever want to wake computers). However, best practice is to designate at least two.

For a network where you don't want any computers to wake from Off or Sleep, set the proxy count for that network address to 0 proxies.

1. In the Surveyor Administrator console, on the Configure menu ⚙, click **System Settings**, and then click **Wake-on-WAN Configuration**.



2. For **Address block**, type the network address of the subnet and the number of proxies to be kept awake per subnet.



> ✍ **Note:** Address blocks can be entered as either IP address and netmask pairs (such as 192.168.10.0 255.255.255.0) or by using CIDR notation (such as 192.168.10.0/24).

3. Type a **Description** to help you identify the network and its Wake on WAN settings.

4. Click **Save**.

## About Wake on WAN and Port-based Network Access Control

Port-based network access control (PNAC) can be configured on some types of network switches to require Ethernet devices to send credentials before being allowed to connect to an authorized network.

For example, an organization using PNAC may configure the network so that a system using Windows Domain user accounts will automatically be allowed access to the internal network, but

computers that are not part of the Windows Domain are prevented from sending or receiving network traffic.

Where PNAC is used, computers in Sleep mode are removed from an authorized network and placed into another, unauthorized network by the network switch. By default, when the Surveyor server is asked to wake sleeping machines using Wake on WAN, the Surveyor server will try to wake computers by sending Wake on LAN (WOL) packets to Wake on WAN proxy computer in the last authorized network from which the proxy computer connected to Surveyor. Because the sleeping computer has been moved to another network by the network switches, the WOL packet never reaches the sleeping computer and it does not awaken.

To wake computers in networks that use PNAC, you can configure Wake on WAN in Surveyor to send subnet-directed broadcasts to specific network addresses. For networks that use port-based network access control (PNAC), you can associate a specific subnet with broadcast networks that will be used for Wake on WAN to wake computers when sleeping computers move from an authenticated network to a different, unauthenticated network. Additional broadcast networks are especially useful where 802.1x network security is deployed and devices change networks when they are turned off or sleeping.

In addition to sending wake packets on the subnet where each device was last detected, Surveyor will send wake packets to each network in the list of additional broadcast networks. Additional broadcast networks can be entered in either IP address and netmask pairs (such as 192.168.10.0 255.255.255.0) or using CIDR notation (such as 192.168.10.0/24).

## Subnet-directed Broadcasts from Surveyor

Surveyor Wake on WAN includes settings for specifying a network and associated broadcast networks that can receive WOL packets through subnet-directed broadcasts.
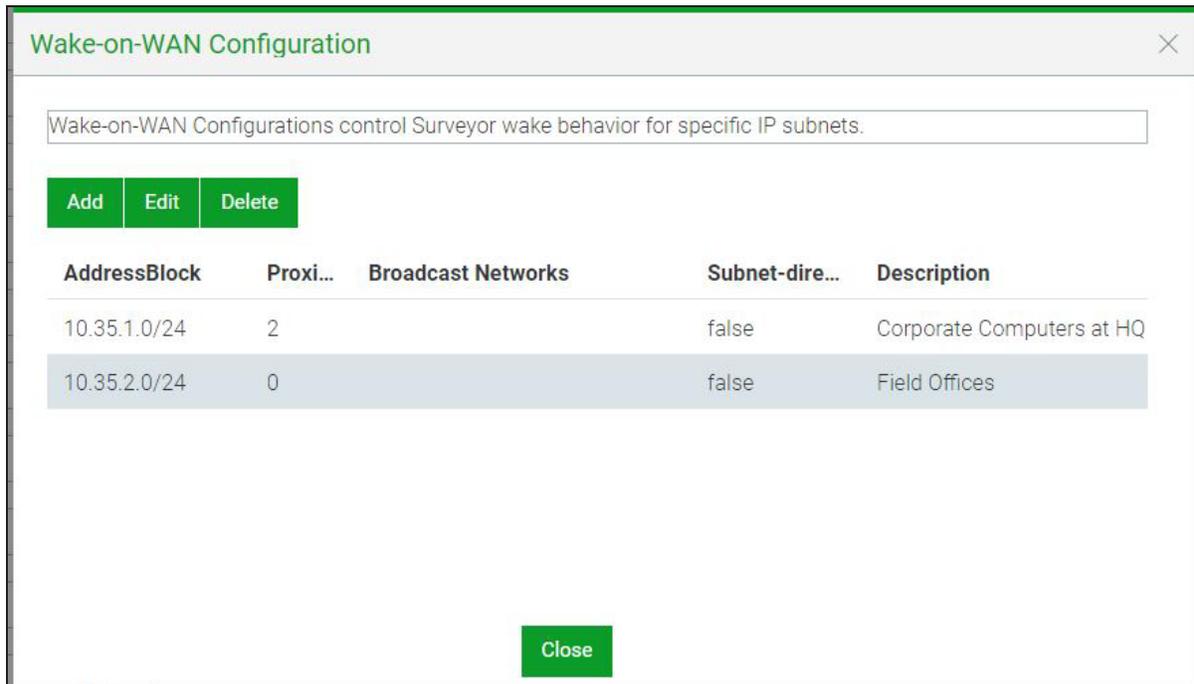
For networks that use port-based network access control (PNAC), you can specify broadcast networks that Surveyor will use to wake computers when sleeping computers move from an authorized network to a different, unauthorized network.
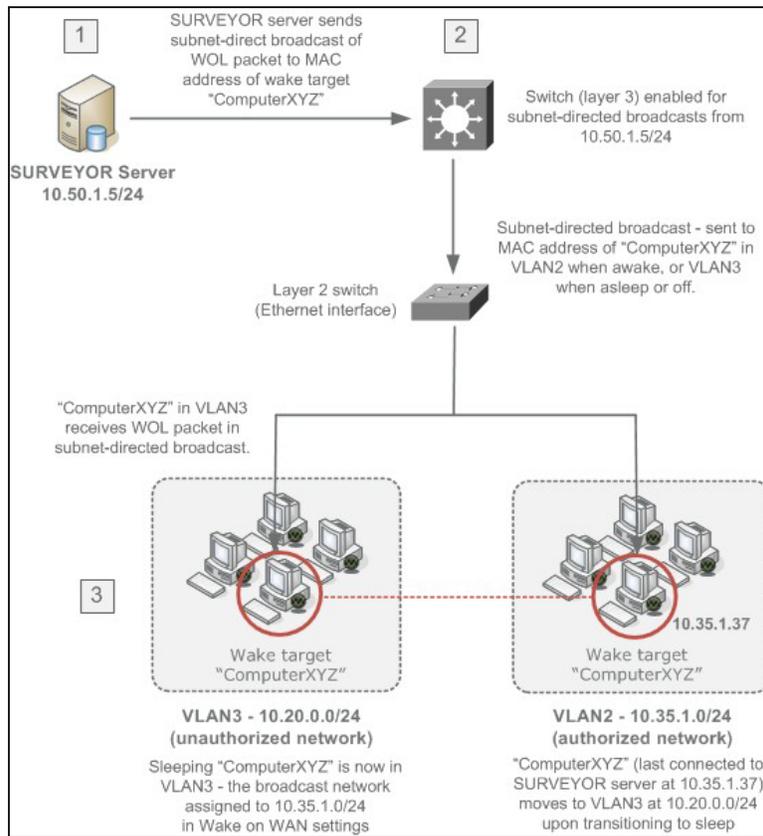


> ≡📝 **Note:** Switches for the networks that you specify as additional broadcast networks must be configured to receive subnet-directed broadcasts from the Surveyor server. See your switch manufacturer documentation for details.

In a network that uses PNAC, the Wake on LAN packet is handled in the following way:

1. The wake target falls asleep and moves from VLAN2 to VLAN3.

2. Wake request is sent to the server from the Administrator console (on schedule through power scheme or on demand by administrator).

3. Surveyor server receives request and sends a subnet-directed broadcast of a Wake on LAN (WOL) magic packet to the master switch (enabled to receive subnet-directed broadcasts specifically from that server address). The WOL packet contains the MAC address of the target client.

4. The wake target receives the WOL packet in VLAN3 and wakes.

## Configure Wake on WAN for Subnet-directed Broadcasts

Use network-specific configurations in Wake on WAN to override the default proxy count or configure networks for subnet-directed broadcasts.

For each network with Surveyor clients. Network-specific configurations in Wake on WAN give you more control over the subnets that should receive Wake on LAN packets from Surveyor server. You can also specify the number of proxies for each subnet.

**Note:** By default, Wake on WAN proxies are not enabled when you first start Surveyor for baseline data collection. After the baseline period is over, it is recommended that you set the proxy number to 2 per subnet.

For networks that use port-based network access control (PNAC), you can associate a specific subnet with broadcast networks that will be used for Wake on WAN to wake computers when sleeping computers move from an authenticated network to a different, unauthenticated network. In addition to sending wake packets on the subnet where each device was last detected, Surveyor will send wake packets to each network in the list of additional broadcast networks. See the topic *About Wake on WAN and Port-based Network Access Control on page 8-26* for other details.

**Note:** Additional broadcast networks are especially useful where 802.1x network security is deployed and devices change networks when they are turned off or sleeping.

**Important:** Switches for the networks that you specify as additional broadcast networks must be configured to receive subnet-directed broadcasts from the Surveyor server. See your switch manufacturer documentation for details.

1. In the Surveyor Administrator console, on the Configure menu ⚙️, click **System Settings**, and then click **Wake-on-WAN Configuration**.

Server Settings

Save | Cancel

| | | |
|---|---|---|
| Maximum number of devices returned per view: | 2000 ⇕ | |
| Devices should check in every: | 1 ⇕ | minutes |
| Number of computers to keep awake as Wake on WAN proxies: | 2 ⇕ | per subnet, unless a specific **Wake-on-WAN Configuration** has been set |
| Keep detailed diagnostics device data for: | 45 ⇕ | days |

2. In the **Wake-on-WAN Configuration** dialog box, select an existing address block entry, and then click **Edit**. Or click **Add** to create a new entry.f

3. Select the option **Use subnet-directed broadcast**.

4. For Address block, type the network address of the subnet and the number of proxies to be kept awake per subnet (if you are not already editing an existing subnet).

> **Note:** Address blocks can be entered as either IP address and netmask pairs (such as 192.168.10.0 255.255.255.0) or by using CIDR notation (such as 192.168.10.0/24).

5. For Additional broadcast networks, type the address block (comma-separated) for each broadcast network that should receive the wake packet for this particular subnet.

## Add new wake-on-WAN configuration ✕

For any block of IP addresses, you can configure:

- How many WOW Proxies will be kept awake in each subnet within the block.
- How and where Wake-on-LAN packets will be sent to awaken computers.

A single Address Block in Wake-on-WAN Configuration can span many subnets. For example: to configure all the subnets starting with 10.10.*.*, you can use the address block 10.10.0.0/16.
For more examples, search for "Wake-on-WAN Configuration" in the Surveyor knowledge base.

AddressBlock:

10.35.1.0/24

Number of proxies:

2

☐ Use subnet-directed broadcast

Additional broadcast networks (comma-separated):

Description

Save  Cancel

6. Type or edit the **Description** to help you identify the network and its Wake on WAN settings.

7. Click **Save**.

# Wake Selected Devices

One of the ways you can wake client devices is to select them in the Administrator console and run the Wake command.

You might sometimes need to wake clients for a specific reason, such as to apply an urgent security patch. To do this, you can select devices in the Administrator console and manually run a wake request on them.

If you want to wake devices from the off state as well as from sleep states, you can do so through Wake on WAN. For information about enabling Wake on WAN, see *About Wake on WAN on page 8-10*.

1. In the Administrator console, on the Surveyor menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

   Or, in the Administrator console, click the Search button 🔍 and filter the device view. Use any of the search filters to show the devices you want to wake up, and then click **Search**.

   For example, use the By Policies filter on the Search page to wake only clients that have a particular policy assigned to them.

2. Select the device or devices in the resulting list view that you want to wake up.

3. On the **Item Actions** menu, click **Wake**.

# Wake Devices on a Regular Schedule

You can set devices to wake at a regular specified time through a policy schedule.

For example, if end users start working on their computers at 7:00am, set a wake request to run at 6:50. Or set computers to wake in preparation for your scheduled maintenance window.

**Wake from sleep vs. wake from off**

You can set a scheduled task to wake computers from sleep (standby) without having to go through Wake on LAN. This option works well for waking computers at the beginning of the work day.

However, if you want to wake computers for maintenance, you might also want to reach the computers that have been turned off. To wake computers from the off state, you need to enable Wake on WAN. After that, you include a second wake task in the policy, which you set to go through Wake on WAN.

The following procedure includes both types of wake tasks.

1. In the Administrator console, on the Surveyor menu ⏻, click **Policies**.

2. Create a new policy or select an existing one, and then click the **Schedule** tab.

3. On the **Insert Power Level Transition** menu, click **Insert Wake**.

4. In the **Insert Power Level Change** dialog box:

   - Select the days of the week on which you want to wake computers.

   - Enter the time of day you want the transition to start.

   - If you want this wake event to reach computers in the off state, select **Wake using Wake on WAN**.

     If you aren't sure whether to use Wake on WAN, see Wake from sleep vs. wake from off earlier in this topic.

5. Configure any additional policy settings and save the changes.

   For example, if you wake computers at the beginning of the day, you might also want to set a work-hours power scheme. For more information about creating policies, see *Overview of Policies and Power ManagementSettings on page 6-2*.

# 9

# Viewing Reports

**Table 9-1  In this Chapter**

| Topics |
| --- |
| *Overview - Reports* |
| *Reporting Settings and Descriptions* |
| *Dashboard and Analytics Reports* |
| *E-mail Reports* |
| *About Data Summarization* |

# Overview - Reports

Surveyor reports provide views of current and summarized information about power states for devices, computer and user activity, and eventswake jobs, device status (by time, by policy, etc) and license status. This section describes the reports that are available in Surveyor and the summarization process that is required to make report data available.

> **Note:** Surveyor 6.4.101 and above use SSRS for reporting. SSRS must be deployed and configured for the reporting services to function.

The following types of reports are available in Surveyor:

| Report | Description |
|---|---|
| Dashboard | **Dashboard reports** are role-based dashboards that provide actionable information on energy costs, C02 emissions, and asset inventory and health to key stakeholders. Dashboard Summary reports can be E-mail reports on page 171.<br><br>For Dashboard reports, click **Dashboard** on the Surveyor menu 📊.<br><br>For details on Dashboard reports, see *Dashboard and Analytics Reports on page 9-4* and *Dashboard and Analytics Reports on page 9-4*. |
| Analytics | **Analytics reports** allow you to generate energy management and IT efficiency reports that dive-down into data based on group, location, and other categories of interest.<br><br>For Analytics reports, click **Analytics** on the Verdiem menu 📊 .<br><br>For details on Analytics reports, see *Dashboard and Analytics Reports on page 9-4*and *Dashboard and Analytics Reports on page 9-4*. |
| Device Events | **Device Event reports** for analysis and optimization. Important events are recorded and reported to a central server. Event data is current as of the last time a device has checked into Surveyor.<br><br>For event reporting, click **Device Events** under Devices on the Verdiem menu ⏻.<br><br>For details on how to use event data for troubleshooting and optimization, see *Chapter 10: Viewing Diagnostic Information from Event Logs on page 10-1* and *Display Event Data in the Administrator Console on page 10-14*. |

**Data Summarization**

Surveyor provides summarized views of data in Dashboards and Analytics reports. By default, the data is summarized on an hourly basis and is kept in 15 minute increments for all devices. For details, see *About Data Summarization on page 9-18*.

# Reporting Settings and Descriptions

The table in this topic contains settings from Reporting Settings page.

## Display the Reporting Settings

To access the settings, in the Surveyor Administrator console, on the Configure menu ⚙, click **Reporting Settings**.

Use Reporting Settings to configure values used when generating reports.

To increase the accuracy of reporting, you can specify watt draw values for individual computer models.

All costs are in the system currency, which can be changed on the Currencies page ( on the Configure menu ⚙, click **Currencies**).

- **Computer Energy Use** tab: Specifies watt draw values for individual computer models on the Reporting Settings page. These values are used in the calculations for data summarization, which affect the data displayed in the Surveyor reports.

  You can improve energy consumption calculations with the least amount of work by specifying the watt draw values for only your most prevalent computer models. If a large majority of your computers represent only a few models, you need only to edit a few rows of this table to improve accuracy of energy consumption calculations.

  Clicking **Resummarize** deletes all summarized computer data and generates new summarized data using the current watt draws, groups, policies, and kilowatt costs. This operation may take some time to complete.

- **Units and Email Settings** tab.

| Setting | Description |
|---------|-------------|
| $CO_2$ units | Configures what units are used in reports for carbon dioxide emissions |
| Gasoline units | Configures what units are used in reports for gasoline. |
| Passenger vehicle, tree seedling, and litre of gasoling $CO_2$ equivalents | Configures how carbon dioxide savings are used to display equivalent savings for passenger vehicle fuel consumption, carbon sequestration by trees, and gasoline savings, used in Advanced Reporting. The EPA provides metrics that can be used to compute these values at http://www.epa.gov/cleanenergy/energy-resources/refs.html. |
| Configure email server settings | Specifies what server is used to send the email reports. |
| Configure email report distribution | Specifies what report is used, email text, and recipients. |

# Dashboard and Analytics Reports

Dashboard and Analytics reports in Surveyor provide you with views of device data from many different angles. Surveyor's Analytics functionality uses a world-class business intelligence (BI) engine, powered by SSRS.

> ❗ **Important:** Data summarization must run for data to be available in reports. For details, see *About Data Summarization on page 9-18*. Also, for some savings reports, *Set the Baseline Value for a Device on page 4-22* before data is summarized to generate meaningful report data.
> The default system currency is U.S. Dollars (USD). If you want to change the system currency, make sure that you choose a currency before you start summarizing data and setting up locations and energy rates, and that you keep the same system currency in place going forward. Changing the system currency at a later date can affect historical data and many data calculations and settings throughout the Surveyor system.

On the Surveyor menu ⏻, when you click Dashboard, the following reports are available to you.

## Details Dashboard

For IT and energy managers, this dashboard provides a breakdown of energy savings and consumption by attributes such as location, group, device type, and power saving policy.

- **Annualized Average Computer Energy Use by Group** - Shows average estimated annual electrical energy use (kWh) per computer and baseline energy use for the selected time period.

- **Computer Power State Activity** - Shows daily percent of time in each power state over the last three months.

- **Cumulative Savings** - Shows cumulative energy savings over the last three months.

- **Energy Savings by Group** - Shows the total energy savings of the top 10 high-level groups for the last twelve weeks.

- **Energy Savings Summary** - Shows energy savings in various units across all devices, groups, and locations for the selected time period.

- **Managed Device Trend** - Shows the number of devices registered with Surveyor and under active power management.

# Status Dashboard

During deployment and ongoing operations, this view helps you to track progress and identify system health issues such as devices not reporting energy information. IT can also flag devices that are underutilized and therefore possible candidates for elimination, consolidation, or virtualization.



- **Computers by Agent Version** - Shows the versions of Verdiem agents deployed and counts of computers by version.

- **Recent Computer Power State Activity** - Shows hourly percent of time in each power state over the last three days.

- **No of Wake Jobs for 7 Days** - Shows the number of wake jobs during the last 7 days. Drill down to see the status of the wake jobs and daily and hourly numbers.

- **Wake Jobs by Category** - Shows the number of wake jobs by category. Drill down to see the status of the wake jobs and daily and hourly numbers.
- **Devices by Group** - Shows the number of devices in the top 10 groups. Drill-down to see lists of specific devices.
- **Installation and Licensing** - Shows key statistics and information about Surveyor agents, including date of last summarization, actively connecting computers, computers with active policies, computers with unenforced policies, computers without baseline settings, perpetual computer licenses, number of PCs and Macs that are licensed, numbers of computers without licenses, numbers of computers intentionally not licensed.

## Analytics Reports

The reports available in Analytics are similar to the Dashboard reports, but allow you to dive down into the report data in more detail (down to 15 minute increments) when you click on data points in the report.

On the Surveyor menu ⏻, when you click Analytics, the following reports are available to you:

| Report | Description |
|---|---|
| **Activity - Computer Power States by Time** | Shows percent of time in CPU and Display power states along with user activity. |
| **Activity- Computer Power States - 15 Minute Intervals** | Shows systems in each power and use state at 15 minute intervals. This can be a long-running report. Select a very small number of days for useful results. Click any power state to see a list of devices in the state at that time. |
| **Costs - Annualized Energy cost by Time** | Charts annualized energy costs for each time period. Answers the question, "If all the selected devices consumed energy as they did during the selected time period, what would be the annual cost?" |
| **Costs - Average Annualized Cost vs. Baseline - Top Groups** | Charts the per-computer average annualized energy cost and baseline cost of the top-10 high-level groups. |
| **Costs - Average Annualized Cost vs. Baseline - Top Locations** | Charts the per-computer average annualized energy cost and baseline cost of the top-10 high-level locations. |
| **Costs - Two Time Period Analysis** | Shows the difference in energy use and costs for two different time periods. |
| **Operations - Computers by Agent Version** | Shows the versions of Verdiem Surveyor agents deployed and counts of computers by version. |
| **Operations - Computers by Model** | Model and manufacturer of computers reporting to Verdiem Surveyor. |
| **Operations - Computers by Operating System** | Current Operating System of computers reporting to Surveyor. |
| **Operations - Device Count by** | Shows the number of devices in each group. |

| Report | Description |
|---|---|
| **Group** | |
| **Operations - Policy Details** | Shows the percentage of devices assigned to each power management policy. |
| **Operations - Device Count by Time** | Shows the number of devices that have reported data by time. |
| **Operations - GoGreen Statistics** | Shows GoGreen advertisement statistics. |
| **Operations - Installation and Licensing Summary** | Shows key statistics and information related to deploying Surveyor. |
| **Operations - Wake Jobs by Category** | Shows the count of different types of wake jobs. |
| **Operations - Wake on WAN Job Status** | Shows history of use of Wake on WAN to wake devices. |
| **Operations - Wake on WAN Device Status** | Shows daily device status history for Wake on WAN, filtered by group, location, and time period. |
| **Operations - Computer Utilization** | Shows the average daily user activity for computers. Allows drill down to individual devices. |
| **Savings - Annualized Computer Savings Summary** | Shows the estimated annualized computer energy savings. Annualized projection uses data only from selected date range. |
| **Savings - Annualized Per-Computer Savings** | Shows the estimated annualized per computer energy use. Annualized projection uses data only from selected date range. |
| **Savings - Cumulative Savings** | Shows cumulative energy savings. |
| **Savings - Energy Savings - Top Groups** | Shows the total energy savings of the top-10 high-level groups. |
| **Savings - GoGreen Savings summary with Equivalents (Fuel, Trees, Cars)** | GoGreen savings summary including metrics such as fuel equivalents and equivalent cars off the road for one year. |
| **Savings - Savings summary with Equivalents (Fuel, Trees, Cars)** | Savings summary including metrics such as fuel equivalents and equivalent cars off the road for one year. |
| **Savings - Surveyor Savings Summary (PDF)** | PDF report showing device-level energy savings and consumption details. This report often takes several minutes to generate. |
| **Savings - Surveyor Savings Summary (Excel)** | Excel report showing device-level energy savings and consumption details. This report often takes several minutes to generate. |
| **Savings - Surveyor Annual Report** | PDF report showing various report and recommendation for previous year. |

# View and Print Dashboard Reports

1. On the Surveyor menu ⏻, click **Dashboard**.

> 📝 **Note:** Data summarization needs to run for data to be available in reports. For details on data summarization, see *About Data Summarization on page 9-18*.

> ❗ **Important:** You must Set the baseline value for a device on page 68 before running summarization to get meaningful data for savings reports.

2. Click **Details** or **Status** to view each type of dashboard.

   For the **Details** dashboard, you can also select the date range for the view (Today, Yesterday, Last 7 days, Last 31 days, Last 12 weeks, Last 12 months), and then click **Refresh**.

3. Click the 💾 icon to the view the report in one of the following formats and print it.

   The following formats are available.

   - XML file with report data
   - CSV (comma delimted)
   - PDF
   - MHTML (web archive)
   - Excel
   - TIFF file
   - Word

4. For a more detailed view of the dashboard data, click a chart or graph (this capability is only supported for some views).

# View Analytics Reports

1. On the Surveyor menu ⏻, click Analytics.

> 📝 **Note:** Data summarization needs to run for data to be available in reports. For details on data summarization, see *About Data Summarization on page 9-18*.

2. Expand the type of report in the category tree, and then select the report name.

3. Select the date range and granularity (hourly, daily, weekly, or monthly).

> **Note:** Selecting a small granularity and a long date range (for example, Granularity: Daily and Date Range: Annual) may cause performance issues. For more information see, *Factors Affecting Processing Time on page 9-19*.

4. To further filter results, select different Display Units (if applicable), Locations, Groups, Policies, or Device Families (if applicable).

5. Click **Run** to view the results.
   Click different data points in the resulting report view for more details.

# View the Activity: Computer Power States by Time report

The **Activity: Computer Power States by Time** report shows summarized information about computer and display power states, and user activity.

The **Activity: Computer Power States by Time** report shows the percentage of time in CPU and Display power states (on, sleeping, or off) along with user activity. Because the **Activity: Computer Power States by Time** data is summarized, data for some devices may be incomplete in the most recent reporting period (days/hours) until summarization runs again.

The data displayed in the **Activity: Computer Power States by Time** report is aggregated, summarized data. For details, see *About Data Summarization on page 9-18* in the *Surveyor 6 Installation Guide*.

To run other Analytics reports, click **Analytics** on the Verdiem menu ⏻.

Click the mouse cursor over different areas of the chart to see more details on various data points.

1. On the Verdiem menu ⏻, click **Analytics**.

2. Select the **Activity: Computer Power States by Time** report.

3. Select a date range and granularity (daily, hourly, weekly, or monthly).

4. Specify the filter parameters (**Locations, Groups, Policies**) to define the set of devices you want to view in the report results, and then click **Run**.

5. Click the 🖫 icon to the view the report in one of the following formats and print it.

   The following formats are available.

   - XML file with report data

   - CSV (comma delimted)

   - PDF

   - MHTML (web archive)

   - Excel

- TIFF file

- Word

> **Note:** If a subset of devices in the Devices page is not checking in regularly and reporting data to the Surveyor server, data for these devices will not be included in summarization and as a result, the devices for will not be represented in the **Activity: Computer Power States** report for that period of time.

# Printer Analytics and Printers Dashboard Reports

Printer Analytics and the Printers dashboard in Surveyor provides detailed data on print devices (including local printer) and end user print behavior, as well as the abilty to measure and manage energy usage across multiple IT devices.

> **Note:** Printer Analytics and the Printers dashboard are available with a Verdiem Printer & Power Analyzer license.

Use Printer Analytics reports to:

- Identify local and networked printers.
- Track end user behavior (who, what, when, and where)
- Monitor energy consumption of printers and PCs/Macs
- Use optimization reports to streamline your print environment

The Surveyor server does not connect to printers directly to collect printer data, instead it detects print job interaction with network and local printers connected to computers in the Surveyor system.

> **Important:** Data summarization must run for data to be available in reports. For details, see *About Data Summarization on page 9-18*. The default system currency is U.S. Dollars (USD). If you want to change the system currency, make sure that you choose a currency before you start summarizing data and setting up locations and energy rates, and that you keep the same system currency in place going forward. Changing the system currency at a later date can affect historical data and many data calculations and settings throughout the Surveyor system.

## Printers Dashboard

On the Verdiem menu ⏻, when you click **Dashboard**, and then click **Printers**, the following reports are available to you.
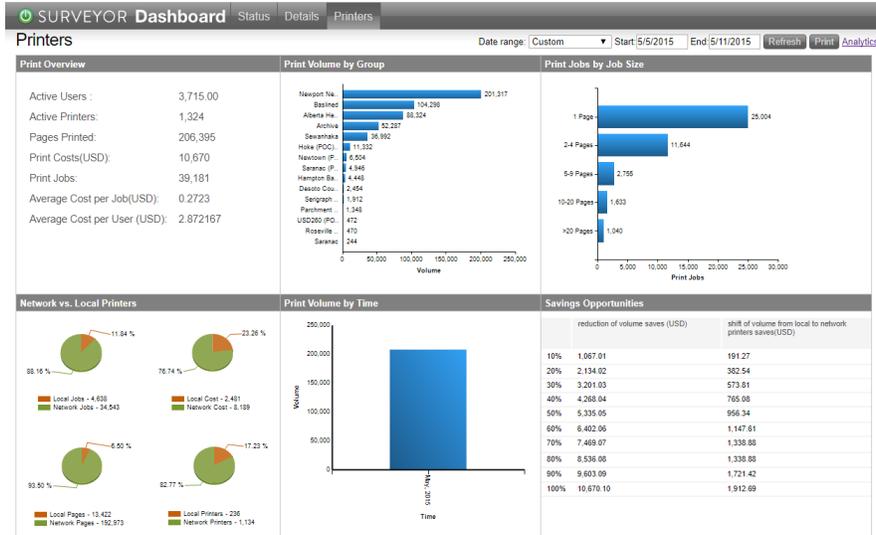
- **Print Overview** - Shows a summary of printing for the time period selected under **Date Range**. This report includes the number of active users, number of active printers, number of pages printed, print costs, number of print jobs, average cost per print job, and average cost per user.

- **Print Volume by Group** - Shows the number of pages printed by top groups for the time period selected under **Date Range**.

- **Print Jobs by Job Size** - Shows the count of print jobs categorized by the number of pages printed in the job for the time period selected under **Date Range**.

- **Network vs. Local Printers** - Shows comparisons of network vs. local printer counts, costs, and volume for the time period selected under **Date Range**.

- **Print Volume by Time** - Shows the count of page impressions for the time period selected under **Date Range**.

- **Savings Opportunities** - Shows the savings that could be achieved by reducing or shifting print volume for the time period selected under **Date Range**.

# Printer Analytics Reports

The reports available in Printer Analytics are similar to the Dashboard reports, but allow you to dive down into the report data in more detail (down to 15 minute increments) when you click on data points in the report.

On the Verdiem menu ⏻, when you click Printer Analytics, the following reports are available to you:

| Report | Description |
|---|---|
| **Active Local Printers** | List of active local printers along with print volume, job count, and print costs for the selected time range, group, and location. Allows drilling into details of each printer. |

| Report | Description |
|---|---|
| **Active NetworkPrinters** | List of active network printers along with print volume, job count, and print costs for the selected time range, group, and location. Allows drilling into details of each printer. |
| **Least Used Local Printers** | Shows the bottom 10 number of page impressions by local printers. |
| **Least Used Network Printers** | Shows the bottom 10 number of page impressions by network printers. |
| **Most Used Local Printers** | Shows the top 10 number of page impressions by local printers. |
| **Most Used Network Printers** | Shows the top 10 number of page impressions by network printers. |
| **Network vs. Local Printing Comparison** | Pie charts comparing network vs. local volumes, costs, and jobs. |
| **Jobs by Job Size** | Chart of the number of print jobs by the number of pages printed per job in buckets of one, 2-4, 5-9, 10-20 and >20 pages. |
| **Savings Opportunity - Print Volume Reduction** | Shows the savings opportunity possible by reducing print volume or moving to lower cost . |
| **Savings Opportunity - Shifting Local Jobs to Network** | Shows the savings opportunity possible by reducing print volume or moving to lower cost printers. |
| **Print Costs by Model** | Shows top 25 paper and page printing costs by model. |
| **Print Costs by User** | Shows top 25 paper and page printing costs by owner. |
| **Print Volume by Model** | Shows the top 25 number of page impressions by model. |
| **Print Volume by Time - Color vs. Monochrome** | Shows color vs. monochrome page impressions over time. |
| **Print Volume by Time - Network vs. Local** | Shows network vs local page impressions over time. |
| **Print Volume by Time - Single vs. Duplex** | Shows single vs. duplex print volumes by time. Drills into a list of all groups. |
| **Print Volume by User** | Shows top 25 number of page impressions per user. |

## Enabling printer data collection

Printer Analytics reports are available in Surveyor when you load Verdiem Print & Power Analyzer licenses in Surveyor, assign the correct license type to PCs or Macs, and enable the collection of printer data in policies assigned to the computers for which you want to track printer use.

> **Note:** Printer Analytics and the Printers dashboard are available in Surveyor only with a Verdiem Printer & Power Analyzer license (starting with Surveyor platform version 6.0.7xx).

1. Install the licenses for Verdiem Print & Power Analyzer.

   For details, see "Add or remove a license file" in the Surveyor 6 Installation guide.

2. Set license type for computers to **PC-Measure + Printer**.

   a. In the Administrator console, on the Verdiem menu ⏻, click **Devices**, and then click a group to view the devices assigned to that group.

      Or, in the Administrator console, click the Search button **Q** and filter the device view. Use any of the search filters to show the devices you want to wake up, and then click **Search**.

   b. Select the computers in the resulting list view that you want to set the license type for.

   c. Right-click the selection, and then click **Edit Device Properties**.

   d. For **License Type**, select **PC-Measure + Printer**, and then click **OK**.

   > **Note:** Select **PC-Manage + Printer** only if you intend to manage computer power states with Surveyor.

3. Set up data collection for policies assigned to the PCs and Macs to collect printer data. You can modify current policies or create new policies specifically for collecting printer data.

   a. In the Administrator console, on the Verdiem menu ⏻, click **Policies**.

   b. Select a policy, and then click the **Data Collection** tab.

   c. Select **Collect printer data**.

   > **Note:** You can set up **Policy Defaults** for **Collect printer data** to be enabled in all new policies your create. For details, see *Edit Default Wake and Data Collection Settings for Policies on page 6-16*.

Data will be collected for any printers that are used by the computers you have set up to use a PC-Measure + Printer or PC-Manage + Printer license type. After data summarization runs (and enough data is available), you can view Printer Analytics reports and the Printers dashboard. For details, see *Printer Analytics and Printers Dashboard Reports on page 9-11*.

# View Printer Analytics Reports

1. On the Verdiem menu ⏻, click **Printer Analytics**.

> **Note:** Data summarization needs to run for data to be available in reports. For details on data summarization, see *About Data Summarization on page 9-18*.

2. Click Printers in the category tree, and then select the report name from the list of available reports.

3. Select the date range and granularity (hourly, daily, weekly, or monthly), as applicable.

4. To further filter results, select different Locations or Groups, as applicable.

5. Click **Run** to view the results.
   Click different data points in the resulting report view for more details.

# View the Printers Dashboard

1. On the Verdiem menu ⏻, click Dashboard.

> **Note:** Data summarization needs to run for data to be available in reports. For details on data summarization, see *About Data Summarization on page 9-18*.

> ❗ **Important:** You must *Set the Baseline Value for a Device on page 4-22* before running summarization to get meaningful data for savings reports.

2. Click **Printers** to view that dashboard.

   You can also select the date range for the view (Today, Yesterday, Last 7 days, Last 30 days, Last 12 weeks, Last 12 months), and then click **Refresh**.

3. For a more detailed view of the dashboard data, click a chart or graph (this capability is only supported for some views), and then click on data points in resulting views for more details.

# E-mail Reports

Surveyor includes the ability to automatically send summary reports via e-mail, on a scheduled basis. The two types of automated reports are:

- Surveyor Savings Summary Report - provides monthly energy usage, savings, and deployment status for stakeholders. This report is sent in PDF format.



- Surveyor Savings Details Report - provides summary information plus device-level detail of savings and status. This report is sent in XLS format.

| Name | Licensed? | Portable? | Manufacturer | Model | kWh Savings | Actual kWh | Baseline kWh | CPU On Minutes | CPU Sleep Minutes |
|---|---|---|---|---|---|---|---|---|---|
| ws003dt0613prd | Y | N | Dell Inc. | OptiPlex 755 | 2.4688 | 5.6177 | 8.0865 | 4470 | 4525 |
| ws003dt0606prd | Y | N | Dell Inc. | OptiPlex 755 | 1.7208 | 6.3703 | 8.0911 | 5193 | 3804 |
| dga1wks01vrdm | Y | N | VMware, Inc. | VMware Virtual Platform | .2517 | 1.1229 | 1.3746 | 1063 | 0 |
| dga1ws08pivdv | Y | N | VMware, Inc. | VMware Virtual Platform | -6.9408 | 15.5424 | 8.6016 | 9568 | 0 |
| ws003dt0045prd | Y | N | Dell Inc. | OptiPlex 755 | .1130 | .0434 | .1564 | 29 | 143 |
| ws003dt0001prd | Y | N | Dell Inc. | OptiPlex 745 | .9703 | 6.9671 | 7.9374 | 6683 | 2145 |
| ws003lt1501prd | Y | Y | Dell Inc. | Vostro 1500 | .2241 | .0532 | .2772 | 6 | 0 |
| ws003dt0502prd | Y | N | Dell Inc. | OptiPlex 755 | 4.2358 | 2.3617 | 6.5976 | 1743 | 5595 |

After you set up the required *E-mail Reports above* in Reporting Settings, scheduled tasks for sending each of these reports run on the 3rd day of every month.

When you install Surveyor 6 (starting with version 6.0.502), two tasks for sending these reports are automatically configured in the Windows Task Scheduler:

- Surveyor E-Mail Savings Summary - Runs at 11:30pm day 3 of January - December
- Surveyor E-Mail Savings Details - Runs at 11:30pm day 3 of January - December
- Surveyor E-Mail Annual Report - Runs at 11:30pm day 3 of January - December

# Configure e-mail Reports

When e-mail reports are configured in **Reporting Settings** on the the **Units and E-mail Settings** tab, scheduled tasks for sending these reports automatically run on the 3rd day of every month. You can also send e-mail reports immediately by click the **Send Now** button in the Report e-mail Report Distribution dialog box.

1. In the Administrator console, on the Configure menu ⚙, and then click **Reporting Settings**, and then click the **Units and e-mail Settings** tab.

2. Click **Configure e-mail server settings**.

   a. Enter the e-mail addresses for **From** and **Reply to**.

   b. Enter the SMTP server information.

   c. If you would like to send a test e-mail, enter the addresses for the test, and then click **Send Test**.

   d. Click **Save** and **Close**.

3. Click **Configure e-mail report distribution**.

   a. Select a report (**Surveyor Savings Summary** or **Surveyor Savings Details** or **Surveyor Annual Report**).

   b. Type the e-mail addresses for the e-mail recipients.

   c. Edit the **Subject** and **Body Text** as you wish.

   d. Edit the attachment file name as you wish.

   Note that for the Surveyor Savings Details report, it is recommended that the attachement uses the extensions .xls.rename to ensure that e-mail applications will not block the e-mail. You will also want to remind recipients to save the attachment with an .xls extension so it can be opened in Excel (included by default in the subject text for this report).

   e. Click **Save**.

   Optionally click **Send Now** if you want to send the report out immediately.

   The scheduled tasks that send these reports will automatically send the reports, based on these configuration settings, as scheduled.

# About Data Summarization

This topic describes how to configure, schedule, run, and check the status of the summarization process.

The data displayed in higher level Surveyor dashboard and analytics reports is aggregated, summarized data.

When you install Surveyor 6 (starting with version 6.0.502), the following data summarization tasks are automatically configured in the Windows Task Scheduler, and use the AdminCommand.exe tool found in C:\Program Files\Verdiem\Surveyor\Tools:

- **Surveyor Resummarize Current Day** - Summarizes data incrementally. After this task is triggered soon after installation, the task runs every hour to summarize the past hour of data.

- **Surveyor Resummarize Past 30 Days** - Summarizes data incrementally at 11:45 p.m. After this task is triggered, the task runs every evening to summarize the past 30 days of Surveyor data.

- **Surveyor Resummarize All Data** - Completely resummarizes all available Surveyor data. This task is disabled by default. Running this task will take more time to complete than the tasks that summarize data incrementally.

> **Note:** The time required for a data summarization task to complete depends on the amount of data to be processed. Data that is summarized on an incremental basis typically takes less time to complete.

Another scheduled task, **Surveyor Delete Old History Data**, runs every day at 10:30 p.m. and triggers the removal of historical data from the database that older than the number of days specified in **System Settings** option **Keep detailed reporting device data for**.

The **Verdiem Surveyor Database Index Maintenance** is another scheduled task that runs every Saturday at 2:00 AM and triggers the shrinking and re-indexing of the database. This reduces the size of the database and improves the database performance.

## Running the Summarization Process

The data summarization tasks that are already setup for Surveyor should usually be sufficient to meet your data needs for Surveyor reports. You can also set up your own scheduled tasks that call the AdminCommand.exe tool. For details, see *About Data Summarization above*.

If you need to resummarize data outside of the already scheduled Surveyor tasks, you can do so using the AdminCommand.exe tool with the start_summarization command. For details, see *About Data Summarization above*.

For details on resummarizing all data, see *About Data Summarization above*.

**To view the results of the summarization task:**

- Open the **summarization** log file in **C:\Program Files\Verdiem\Surveyor\Logs**.

# Settings that Affect Data Summarization and Reporting

The following settings and values affect data summarization calculations and how data is grouped and displayed in Surveyor reports:

- Device group, location, and policy assignments
- Historical rate information for locations
- Historical currency exchange rates
- Device power draws
- Device family assignments
- Device baseline values

If possible, it is recommended that you define these values before you run the summarization process for the first time to get the most accurate and uniform report results over time.

When you make changes to default baseline settings in the System Settings page or through a device's right-click menu, watt draw values, device family assignments, locations (device assignment), groups (device assignment), policies (device assignment), business units in metadata, only data that is collected and summarized from the time of the change will reflect the new settings (historical data will still be based on the old settings). To get the most accurate and uniform reporting results, you may need to resummarize data.

# Factors Affecting Processing Time

When a large amount of data is being processed, the computer running the summarization process can use significant system resources and the process may take some time to complete. When resummarizing data, it is best to run the task when Surveyor server is not required to be active.

Factors affecting the time required for the summarization process to complete the first time it runs:

- **Database I/O**: The summarization process potentially requests large amounts of data for the database to read out. The speed of database I/O can affect how quickly the summarization process completes.
- **Defragmentation**: Table indexes are defragmented during the summarization process. The amount of defragmentation required can affect how quickly the summarization process completes.
- **Groups, locations, policies**: Number of locations, business units, policies, and administrative groups.
- **Memory**: Available memory for SQL sand the summarization process also can affect the time required.

# Resummarize Data Incrementally Using the AdminCommand.exe tool

If you need to resummarize data outside of the already scheduled Surveyor tasks, you can do so using the AdminCommand.exe tool with the `start_summarization` command.

The syntax for AdminCommand.exe is:

```
start_summarization [<days into past>] force
```

This command starts, or restarts summarization. If summarization is already running and the force option is omitted, there is no effect (the previous summarization job continues). If summarization is already running and and the force option is included, the existing summarization job is canceled. If the number of days to be summarized isn't specified, a full re-summarization is performed.

1. Launch the Windows command prompt as an administrator.**AdminCommand.exe** from the command prompt as an administrator.

2. Run `AdminCommand.exe start_summarization` *<days into past>* from the **C:\Program Files\Verdiem\Surveyor\Tools** folder on the Surveyor server.

   For example:

   ```
   AdminCommand.exe start_summarization 30 force
   ```

**To view the results of the summarization task:**

Open the **summarization** log file in **C:\Program Files\Verdiem\Surveyor\Logs**.

# Resummarize Data Incrementally Using a Windows Task

This topic describes the Windows tasks available to Surveyor 6.0.5xx that handle resummarizing data incrementally.

When you install Surveyor 6 (starting with version 6.0.502), the following data summarization tasks related to are automatically configured and scheduled to run in the Windows Task Scheduler:

- **Surveyor Resummarize Current Day** - Summarizes data incrementally. After this task is triggered soon after installation, the task runs every hour to summarize the past hour of data.

The corresponding command line for this task is:

`AdminCommand.exe start_summarization 1`

The corresponding action is:

"C:\Program Files (x86)\Verdiem\Surveyor\Tools\AdminCommand.exe" start_summarization 1

- **Surveyor Resummarize Past 30 Days** - Summarizes data incrementally at 11:45 p.m. After this task is triggered, the task runs every evening to summarize the past 30 days of Surveyor data.

  The corresponding command line for this task is:

  `AdminCommand.exe start_summarization 30 force`

  The corresponding action is:

  "C:\Program Files (x86)\Verdiem\Surveyor\Tools\AdminCommand.exe" start_summarization

  30 force

- **Surveyor resummarize all data** -Summarizes all data incrementally at 11:50 p.m. After this task is triggered, the task runs to summarize all Surveyor data. By default, this is disabled.

  The corresponding command line for this task is:

  `AdminCommand.exe start_summarization force`

  The Corresponding action is:

  "C:\Program Files (x86)\Verdiem\Surveyor\Tools\AdminCommand.exe" start_summarization force

  The corresponding command line for this task is:

> **Note:** Ensure that no two data summarization tasks run at the same time.

Though these tasks are already scheduled by default, you can trigger these tasks at any time, or edit the schedule, or create your own data summarization tasks.

1. Open the Windows Task Scheduler (Windows Start menu > Administrative Tools > Task Scheduler.
2. Select **Task Scheduler Library**.
3. Select the name of the Surveyor summarization task, and then click **Run**.

# Configure a Scheduled Task for Data Summarization (Windows Server 2008)

This topic describes how to create a data summarization task in the Windows Task Scheduler.

1. To open Windows Task Scheduler, browse to the Windows Start menu > Administrative Tools, and then click **Task Scheduler**.

2. In the Task Scheduler, right-click **Task Scheduler (local)**, and then click **Create Task**. Name the task.

3. On the **General** tab of the Create Task dialog box:

   a. Name the task.

   b. Under **Security Options**, specify any user as long as they have permissions to the following directories: **C:\Program Files\Verdiem\Surveyor\Tools\**.

   c. Select **Run whether user is logged on or not**.

   d. Click **OK**.

4. On the **Actions** tab:

   a. Click **New**.

   b. For **Action**, select **Start a program**.

   c. For Program/script, click Browse, and then select AdminCommand.exe.

      By default, this file is installed to C:\Program Files\Verdiem\Surveyor\Tools\ on same computer as the Surveyor server.

   d. For **Add arguments**, type *start_summarization*, the number of days, and force.

      For example: start_summarization 15 force.

   e. For **Start in (optional)**, type the directory location of the **AdminCommand.exe** file: **C:\Program Files\Verdiem\Surveyor\Tools\** (by default).

   f. Click **OK**.

5. On the **Triggers** tab:

   a. For Begins the task, select how often the task should run.

      For more up-to-date reporting, it is recommended that you run this task at least once a day.

   b. Select other advanced settings as required for your needs.

   c. Click OK on the Triggers tab.

6. Click OK in the Create Task dialog box.

At this point, you will need to provide your password.

To ensure the task works correctly, you can select the task you just created and click **Run**.

The message "The operation completed successfully (0x0)" in the **Last Run Result** column indicates the task is running correctly.

**To view the results of the summarization process**:

- Open the **summarization** log file in **C:\Program Files\Verdiem\Surveyor\Logs**.

# Resummarize All Data

This topic describes how to reset summarization data for cases where you might want to resummarize data completely, from scratch.

You can resummarize data by clicking the **Resummarize** button on the Reporting Settings page in the Surveyor Administrator console, or by running the **Surveyor Resummarize All Data** Windows task which uses the AdminCommand.exe start_summarization force command.

> **Note:**  Do not click **Resummarize** unless you are certain that you want to resummarize data. If you are interested in keeping the historical data in some form, back up the Surveyor database before resummarizing all of the data. Any system settings that have changed since the previous summarization process has run will be applied to all historical data in the database. This includes changes to device baseline values, watt draw values, policies, groups, business units, or locations.
>
> If you are running the summarization process on the Surveyor server computer (recommended), be sure to run the process when the Surveyor server is not required to be active.

To completely resummarize all Surveyor data:

1. In the Surveyor Administrator console, on the Configure menu ⚙, click **Reporting Settings**, and then click the **Computer Energy Use** tab.

2. Click the **Resummarize** button.

   Optionally, you can trigger the **Surveyor Resummarize All Data** task in the Windows Task Scheduler.

   Or, manually resummarize all data by running AdminCommand.exe start_summarization force from the command prompt as an administrator from **C:\Program Files\Verdiem\Surveyor\Tools** on the Surveyor server.

**To view the results of the summarization task:**

- Open the **summarization** log file in **C:\Program Files\Verdiem\Surveyor\Logs**.

# 10

# Viewing Diagnostic Information from Event Logs

**Table 10-1  In this Chapter**

| Topics |
| --- |
| *Data recorded in Event Logs and How Long it is Retained* |
| *Display Event Data in the Administrator Console* |
| *Specify Server Logging Levels and File Size* |
| *Server Log File Locations* |
| *Client Log File Locations* |

# Data recorded in Event Logs and How Long it is Retained

Clients report end-user and power-state actions in log files, which you can view from the Administrator console. Each action that is logged is referred to as an event. Event logs help you determine whether policies are effective, and help you quickly detect and resolve errors. This section contains information about log file settings and locations, how to view the log data, and how to change parameters that determine what information is displayed.

This topic provides an overview of the event categories and types that are recorded in event logs. It also lists some of the factors that determine how much historical data is retained.

## Event Categories and Types

When you view data logged from system or user activity, one of the ways to filter that data is to select a specific **event category**. When you do this, the view is broken down by **event types** for the selected category. Event types represent the specific actions or errors that occurred, such as a power-state transition to sleep or wake, a user action that delayed a power-state change, and so on.

The following table lists the event categories and describes the event types logged under each.

| Category | Description |
|---|---|
| Admin Actions | Includes all manual transitions to low-power states that an administrator sets on devices. |
| Idle Timer Actions | Transitions to low power states that occur specifically when the client is inactive (idle) for the length of time set in the policy assigned to it. |
| Policy Actions | This category includes events that occur through power state transition manager (PSTM) rules, and other events that occur when policies set schemes and change power states.<br><br>Other events recorded in this category include initial power scheme value when the client service is started, when a power scheme is set according to the policy schedule, when scheme is set by the user (because the scheme is created to allow the user to override it), and so on. |
| Scheduled Actions | Any power-state change that occurs according to the schedule set in the policy assigned to the client. |
| Service Events | Events logged by the client service, such as start, stop, or device check in. Events also include new database creation, and if data collection stops or starts for power state changes and user activity. |
| State Changes | Detailed power state change data and the request source (Surveyor server, a third party, or an unknown trigger). Also includes display-only logs for power-state changes. |

| Category | Description |
|---|---|
| User Actions | This category includes events that are logged when users take actions on power schemes or power-state change notifications, when you make these actions available to them through the policy configuration. For example, you can allow users to skip or delay a power-state change or to change the power scheme in the Windows Control Panel. |
| User Activity | Events that indicate whether a user is active or not, whether a transition to a low power state based on idle time is pending, and if user activity is unknown (in which case data and activity collection may have stopped, which will be indicated by an event in the Service Events category). |
| Configuration Errors | Errors setting, querying, or deleting a power scheme; changing wake settings on mouse, keyboard (including whether it's a USB device); or loading, parsing, or saving .config files. |
| Policy Errors | Errors that prevent a PSTM rule from running. For example, PSTM fails to veto a power state change, terminate an application, or report that an application has terminated. |
| Service Errors | Errors that cause the client service to stop running properly. For example, the client computer loses power abnormally; the service fails to parse or run a request from the power management service; performance counter for the idle timer missing or failed; errors that occur while querying the user or display state. |
| Transition Errors | Problems that occur when the API for a power state transition is called but returns a failure code; errors occurring while processing a power state transition; failure to dispatch a Wake on LAN magic packet; unexpected errors while trying to prevent narcolepsy (computer transitions to sleep while in use). |

If you want to make the event report view more granular, you can combine the event category filter with any combination of the other standard filters that are available for searching. For example, view successful transitions for a particular policy or user actions in a particular device group or subnet.

# How Much Data is Retained

The historical period for which you can report on events depends upon a variety of system factors. These include the number of devices being managed, the reporting interval, the database server hardware, and so on. These factors determine the rate at which events are generated and the speed at which the database can process large numbers of events.

Under reasonable circumstances, you should be able to view events for 2–7 months in the past. However, you might need to trim the data sooner to achieve acceptable performance.

The Surveyor database contains a table for all events, along with a separate table for PC power state and user activity events. The latter events are retained for a longer period of time than error events. Error events are generally used for troubleshooting and resolved relatively shortly after a problem occurs.

## Where to Find Client Log Files

Log file location:

**C:\Program Files\Verdiem\Surveyor Agent\Logs**

Log file names:

- The current file is named **PwrMgrService.log**.
- Files that contain older log messages are named PwrMgrService.log.1, PwrMgrService.log.2, and so on.

> **Note:** On 64-bit versions of Windows, the client agent folders and files are under Program Files (x86).

# List of Event Types for Each Event Category

This topic lists the event types that can occur under the categories shown in the Administrator console.

## Introduction

When you view the Event Summary Report, specific events are grouped under different categories. This article lists every event type that can occur under each event category.

## Client Log Location

C:\Program Files\Verdiem\Surveyor Agent\Logs

## Content links

| | |
|---|---|
| • *Table 10-2 below* | • *Table 10-9 on page 10-10* |
| • *Table 10-3 on the next page* | • *Table 10-10 on page 10-11* |
| • *Table 10-4 on the next page* | • *Table 10-11 on page 10-11* |
| • *Table 10-5 on page 10-7* | • *Table 10-12 on page 10-12* |
| • *Table 10-6 on page 10-8* | • *Table 10-13 on page 10-13* |
| • *Table 10-7 on page 10-9* | |
| • *Table 10-8 on page 10-9* | |

**Admin Actions Event Category**

Includes all manual transitions to low-power states that an administrator sets on devices.

**Table 10-2  Admin Actions Event Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Sleep by Admin | Indicates Administrator API call to the client operating system's API for sleep (from menu in the Administrator console). | yes |
| Hibernate by Admin | Indicates Administrator API call to the OS's API for hibernate (from menu in the Administrator console). | yes |
| Shut down by Admin | Indicates Administrator API call to the OS's API for shut down (from menu in the Administrator console). | yes |
| Restart by Admin | Indicates Administrator API call to the OS's API for restart (from menu in the Administrator console). | yes |

### Idle Timer Actions Category

Transitions to low power states that occur specifically when the client is inactive (idle) for the length of time set in the policy assigned to it.

**Table 10-3  Idle Timer Actions Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Sleep by Idle Timer | Indicates call to the OS's API for sleep when the Surveyor idle time countdown has expired. In other words, the client agent has been inactive for the amount of time specified for the CPU in the current policy. | yes |
| Hibernate by Idle Timer | Indicates call to the OS's API for hibernate when the Surveyor idle time countdown has expired. In other words, the client agent the CPU in the current policy. | yes |

### Policy Actions Category

This category includes events that occur through power state transition manager (PSTM) rules, and other events that occur when policies set schemes and change power states.

Other events recorded in this category include initial power scheme value when the client service is started, when a power scheme is set according to the policy schedule, when scheme is set by the user (because the scheme is created to allow the user to override it), and so on.

**Table 10-4  Policy Actions Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Application Protected | The PSTM vetoed a state change because a protected application was running. | yes |
| Script Vetoed | A PSTM script vetoed a state change. | yes |
| Application Detected | An application of interest was detected by way of PSTM rules. | yes |
| Application Terminated | PSTM terminated the indicated application. | yes |
| Scheme Initial Value | The initial value for the power scheme when the client service was started. | yes |
| Scheme Set by Policy | A switch to the power scheme enforced by the current policy when a scheduled event in the policy fires. | yes |
| User Scheme Restored | Restored the user's preferred scheme, because the currently scheduled policy allows for it. | yes |
| User Scheme Restored after Service Stop | Restored the user's preferred scheme because the Surveyor client service was stopped. | yes |

## Scheduled Actions Category

Any power-state change that occurs according to the schedule set in the policy assigned to the client.

**Table 10-5  Scheduled Actions Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Sleep by Policy | The OS's API for sleep was called because a scheduled policy change occurred. | yes |
| Hibernate by Policy | The OS's API for hibernate was called because a scheduled policy change occurred. | yes |
| Shut Down by Policy | The OS's API for shut down was called because a scheduled policy change occurred. | yes |
| Restart by Policy | The OS's API for restart was called because a scheduled policy change occurred. | yes |
| Wake by Policy | Indicates a scheduled policy has triggered a wake event (always appears in conjunction with 104-Power Wake) | yes |

## Service Events Category

Events logged by the client service, such as start, stop, or device check in. Events also include new database creation, and if data collection stops or starts for power state changes and user activity.

**Table 10-6  Service Events Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Service Started | The client service was started. CPU on is assumed; all other states are unknown. | yes |
| Service Stopped | The client service was stopped. All states should be considered unknown unless the subtype is Shutdown (CPU off). | no |
| Power State Collection Started | Indicates start of data collection for power state transitions. CPU on can be assumed; all other power states are unknown. | yes |
| Power State Collection Stopped | Indicates data collection stop for power state transitions; all power states go unknown. | no |
| User Activity Collection Started | Indicates start of data collection of user actions. Power states for all users go unknown. | yes |
| User Activity Collection | Indicates stop of data collection for user actions; power states for all users go unknown. | no |

**Table 10-6  Service Events Category (continued)**

| Event Types | Description | Normal event? |
|---|---|---|
| Stopped | | |
| Database Created | Always the first event in a new database. | yes |
| High Sequence Number Changed | Indicates that the client updated its high sequence number to accommodate a detected re-imaging. | yes |
| Device Check-in | Client agent checks with the server for latest instructions (as set on the Server Settings page of Administrator console). | yes |

## State Changes Category

Detailed power state change data and the request source (Surveyor server, a third party, or an unknown trigger). Also includes display-only logs for power-state changes.

**Table 10-7  State Changes Category**

| Event Types | Description | Normal event? |
|---|---|---|
| On State | The current CPU state is on. This event is generated any time power state collection is started (through service start or a policy change). | yes |
| Shutdown State | Surveyor received notification from Windows that the CPU will turn off soon (user has received notification and allowed the shut down). | yes |
| Sleep State | Surveyor received notification from Windows that the CPU will transition to the sleep state soon (user has received notification and allowed the transition). | yes |
| Wake State | Surveyor client device wakes from a low power state (sleep or hibernate). | yes |
| Unknown State | This event is generated any time that power state collection is stopped (for example, if the client agent is uninstalled). | no |
| Sleep by Third-party | Indicates that a third-party, called the OS sleep API. | yes |
| Hibernate by Third-party | Indicates that a third-party called the OS hibernate API. | yes |
| Shut Down by Third-party | Indicates that a third-party called the OS shut down API. | yes |
| Restart by Third-party | Indicates that a third-party called the OS restart API. | yes |
| Sleep by Unknown | Indicates that an unknown source has called the OS sleep API. | no |

**Table 10-7  State Changes Category (continued)**

| Event Types | Description | Normal event? |
|---|---|---|
| Hibernate by Unknown | Indicates that an unknown source has called the OS hibernate API. | no |
| Shut Down by Unknown | Indicates that an unknown source has called the OS shut down API. | no |
| Restart by Unknown | Indicates that an unknown source has called the OS restart API. | no |
| Wake by Unknown | Indicates that an unknown source has called the OS wake API. | no |
| Display On | One or more displays are in an on state. The power state (D-value) for each display is held. | yes |
| Display Sleep | No displays are in an on state, but at least one is in a sleep state. | yes |
| Display Unknown | The display state is unknown. This can indicate either that power state collection stopped or a failure of the detection APIs. | no |

## User Actions Category

This category includes events that are logged when users take actions on power schemes or

power-state change notifications, when you make these actions available to them through the policy configuration. For example, you can allow users to skip or delay a power-state change or to change the power scheme in the Windows Control Panel.

**Table 10-8  User Actions Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Scheme Changed by User | The end user or a third-party application changed the power scheme through the Windows Control Panel. | yes |
| Scheme Changed (No Policy) | The end user or a third-party application switched off the enforced policy. | yes |
| State Change Skipped | The end user chose to cancel a power state change when a notification message appears on their screen. | yes |
| State Change Delayed | The end user chose to delay a power state change when a notification message appears on their screen. | yes |

## User Activity Category

Events that indicate whether a user is active or not, whether a transition to a low power state based on idle time is pending, and if user activity is unknown (in which case data and activity collection may have stopped, which will be indicated by an event in the Service Events category).

**Table 10-9  User Activity Category**

| Event Types | Description | Normal event? |
|---|---|---|
| User Active | Mouse or keyboard activity indicates that user is active on a client computer. | yes |
| User Activity Unknown | The state of user activity is unknown. This can indicate that data collection has stopped or detection APIs have failed. | no |
| User Idle | Mouse or keyboard activity indicates that user is not active on a client computer. | yes |
| User Idle Pending | Mouse or keyboard activity indicates that user is not active on a client computer, and a transition to a low power state is pending. | yes |

## Configuration Errors Category

Errors setting, querying, or deleting a power scheme; changing wake settings on mouse, keyboard (including whether it's a USB device); or loading, parsing, or saving .config files.

**Table 10-10  Configuration Errors Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Scheme Set API Failure | An error occurred setting the power scheme in the operating system. | no |
| Scheme Get API Failure | An error occurred while querying the power scheme in the OS. | no |
| Scheme Delete API Failure | An error occurred while deleting the power scheme in the OS. | no |
| Wake Mouse Failure | Mouse movement failed to wake client. | no |
| Wake Keyboard Failure | Keyboard use failed to wake client. | no |
| Wake USB Failure | Use of USB device (mouse, keyboard) failed to wake client. (Registry setting is required on Windows XP) | no |
| Wake Network Failure | Client did not wake because of failed network card settings. | no |
| Logging Config Failure | Failed to update the logging configuration. | no |
| Server Config Load Failure | Failed to load the Surveyor server config file. | no |
| Server Config ParseFailure | Failed to parse the Surveyor server config file. | no |
| Server Config | Failed to save the Surveyor server config file. | no |

**Table 10-10  Configuration Errors Category (continued)**

| Event Types | Description | Normal event? |
|---|---|---|
| Save Failure | | |

## Policy Errors Category

Errors that prevent a PSTM rule from running. For example, PSTM fails to veto a power state change, terminate an application, or report that an application has terminated.

**Table 10-11  Policy Errors Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Script Failure | A PSTM script threw an exception. | no |
| Check Condition Failure | There was an error while checking for a PSTM condition. | no |
| Veto Failure | There was an error when the PSTM attempted to veto a state change as specified in a PSTM rule. | no |
| Application Terminate Failure | There was an error when the PSTM attempted to terminate an application as specified in a PSTM rule. | no |
| Application Detect Failure | There was an error when the PSTM attempted to report that an application was running. | no |
| Idle Timer Block Failure | There was an error when the PSTM attempted to block the idle timer (when PSTM rule specifies to stop transition if a particular application is running). | no |

## Service Errors Category

Errors that cause the client service to stop running properly. For example, the client computer loses power abnormally; the service fails to parse or run a request from the power management service; performance counter for the idle timer missing or failed; errors that occur while querying the user or display state.

**Table 10-12  Service Errors Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Service Crash | The client service terminated unexpectedly. This is detected the next time the service starts. | no |
| Abnormal Power Off | The client computer was turned off in an abnormal way. For example, a power outage or computer was unplugged. This is detected the next time the service starts. | no |
| Resume Power Failed | The client machine lost power after going into suspend. (Also detected at service start.) | no |

**Table 10-12  Service Errors Category (continued)**

| Event Types | Description | Normal event? |
|---|---|---|
| Usage Query Failure | An error occurred while querying the state of user activity. | no |
| Display Query Failure | An error occurred while querying the state of display activity. | no |
| Scheduler Failure | An error occurred in the scheduler module. | no |
| PMP Message Parse Failure | Failed to parse a PMP (power management protocol service) message, such as a power state transition request. | no |
| PMP Message Dispatch Failure | Failed to execute a PMP (power management protocol) message, such as a power state transition request. | no |
| Device Query Failure | Failed while executing a device query. For example, to get a list of network adapters. | no |
| Performance Counter Missing | A performance counter that is used with the Surveyor idle timer is missing. | no |
| Performance Counter Failure | A performance counter that is used with the Surveyor idle timer failed. | no |

## Transition Errors Category

Problems that occur when the API for a power state transition is called but returns a failure code; errors occurring while processing a power state transition; failure to dispatch a Wake on LAN magic packet; unexpected errors while trying to prevent narcolepsy (computer transitions to sleep while in use).

**Table 10-13  Transition Errors Category**

| Event Types | Description | Normal event? |
|---|---|---|
| Sleep Failure | The sleep API was called, but it returned a failure code. | no |
| Shutdown Failure | The shutdown API was called, but it returned a failure code. | no |
| Hibernate Failure | The hibernate API was called, but it returned a failure code. | no |
| Sleep General Failure | An unexpected error occurred while processing a sleep request. | no |
| Shut Down General Failure | An unexpected error occurred while processing a shutdown request. | no |
| Hibernate General Failure | An unexpected error occurred while processing a hibernate request. | no |
| Wake on WAN Dispatch Failure | Failed to dispatch the Wake on WAN magic packet (UDP broadcast). | no |

**Table 10-13  Transition Errors Category (continued)**

| Event Types | Description | Normal event? |
|---|---|---|
| Narcolepsy Prevention Failure | There was an unexpected error while trying to prevent narcolepsy (condition in which the client transitions to a sleep state while still considered active). | no |

**See also**

Topics under *Chapter 10: Viewing Diagnostic Information from Event Logs on page 10-1* in the *Surveyor 6 Administrator Guide*.

**Applies to**

**Product**

- Surveyor 6

# Display Event Data in the Administrator Console

You can view client agent activity in a summary report, or view a list of devices by event or events by event type.

In addition, you can use search filters to fine-tune the data. For example, view events only in a particular administration group, events to which a particular policy is assigned, and so on.

---

**Note:** To control the number of days of data in which events are stored, on the Configure menu ⚙, click **System Settings**, and then evaluate the **Keep detailed diagnostics device data for**: setting. This setting specifies the number of days in which event data is stored. 32 days is usually sufficient for troubleshooting purposes.

---

1. In the Administrator console, on the Surveyor menu ⏻, click **Device Events**.

   By default, a chart view appears, showing events from all event categories, by hour over the past day. Charts represent the event categories, and the graph represents the number of events, with lines representing event categories.
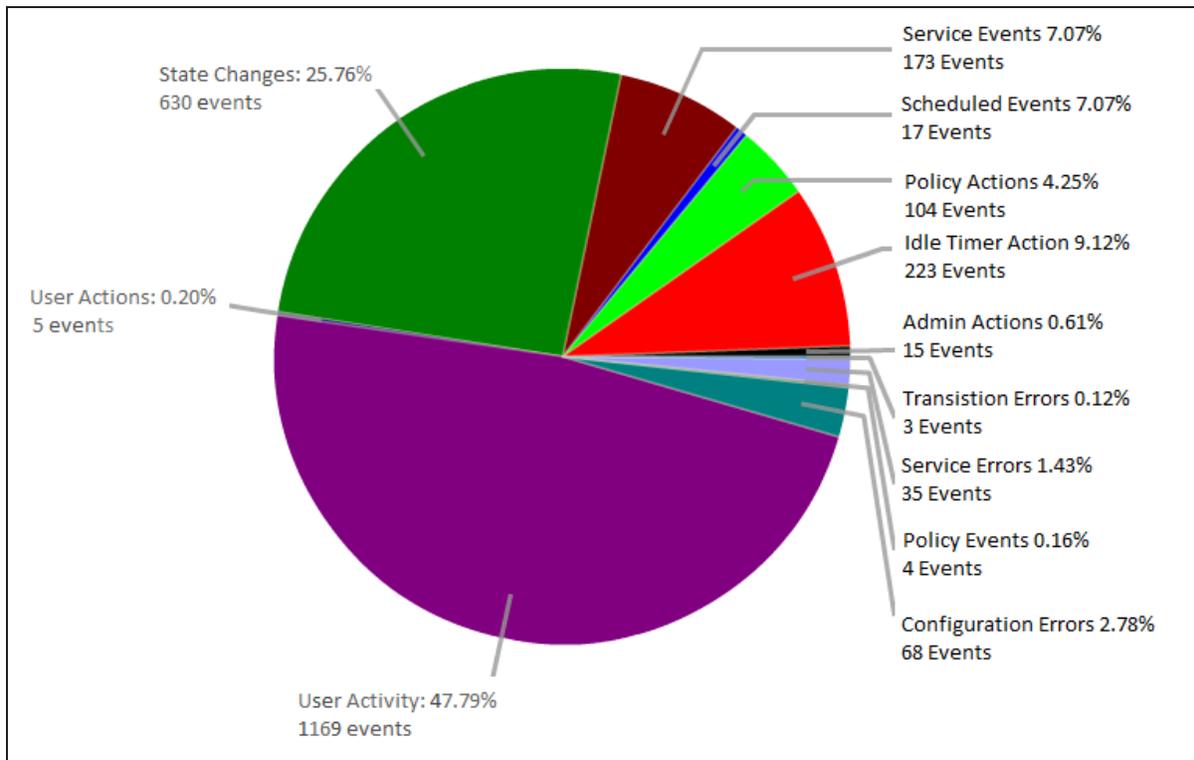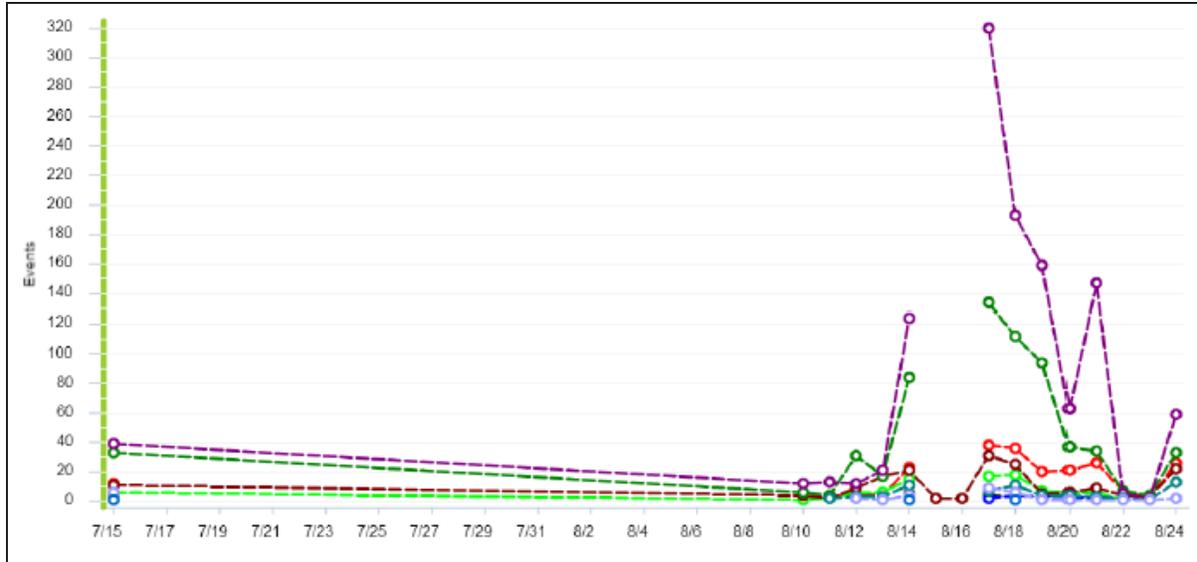
2.  To fine-tune the data shown or view the same data in different ways, do any of the following or combinations of the following.

| To view: | Do this: |
|---|---|
| More detail about a part of the chart in the report view. | Hover the mouse over the section of a pie chart or on a data point of a bar chart. |
| All of the event types that occurred within an event category. | Double-click the event category in a pie chart. A new chart appears, showing event types within that category. |
| Information from devices based on particular device attributes. | • Use the device filters on the left to refine the view by administration group, policy, device family, subnet.<br><br>• Type a search string to filter by device name or description. |
| Events reported by a particular device | In the Event Summary report view, click the **Devices** tab.<br><br>Click **Customize View** to add or remove columns to view only the information you want. |
| All events that occurred on each device or on a specific device. How many times a particular event was logged and when it occurred. | In the Event Summary view, click the **Events** tab. |
| A different chart | Select a specific category in the Event category drop-down list. |

## Variations and Tips

- To analyze power-state transitions for one specific device, type the device name in the Search box and enter the appropriate start and end dates.

- View transitions by day for a larger set of devices or longer date ranges. Click column headings to sort by other parameters.

## Search Phrase Tips

- Search phrases that you type are not case-sensitive.

- Surveyor returns results that contain the search string. Wildcard characters * and ? are processed as text characters, not as wildcards.

For more information about viewing devices in the Administrator console, see *View Devices and Attributes on page 4-15*.

# Specify Server Logging Levels and File Size

This procedure contains steps for changing settings for server logging level and log file size, to set policy default settings or override the defaults in individual policies.

1. On the Configure menu ⚙️, click **Policy Defaults**.

2. On the **Data Collection** tab, select the logging level that you want all new policies you create to contain by default.

   - **Error**: Error messages only.

   - **Warning**: Warning and error messages.

   - **Info**: Informational messages, warning messages, and error messages.

   - **Debug**: Contains messages that enable developers to know what part of the code is generating them. This level is sometimes used for troubleshooting when you work with Technical Support.

   - **Trace**: The most verbose and frequent logging. This level includes error, warning, info, and debug messages, plus messages that indicate when code functions are entered and exited.

     Because of the logging frequency at this level, the maximum log file size and number of log files are reached quickly. This level is advised only under some conditions when you are working with a Technical Support representative, and typically only on a limited subset of clients at a time.

3. Select the remaining device log file and data settings.

| Setting | Value |
|---------|-------|
| **Max log file size** | Sets the maximum size of log file you want to maintain. When the current log file reaches the maximum size, Surveyor creates a new file for subsequent messages, until that file reaches the maximum size, and so on. |
| **Max number of log files** | Sets the maximum number of log files to store on client machines. When the maximum is reached, the oldest file is deleted to make room for a new file. |
| **Collect power state data** | Select to record power state transition events, including successful transitions and transition errors. |
| **Collect user activity data** | Select to record user activity events. Includes actions such as delaying or skipping a power state change, or using the Windows Control Panel to change the power scheme from the one set by Surveyor. |

To access these settings in an individual policy, on the Surveyor menu ⏻, click **Policies** , select a policy, and then click the **Data Collection** tab.

# Server Log File Locations

The following table lists the various locations in which you can find log files that contain status and diagnostic information for the Surveyor server components, and other related components.

> **Tip:** To quickly gather available server (and related) log files and save them in a .zip file, you can run **ZipVerdiemLogs.bat** as an administrator. ZipVerdiemLogs.bat is available from **C:\\Program Files\Verdiem\Surveyor\Scripts**. The companion file ZipVerdiemLogs.vbs is used to collect the logs into a single ZIP file. The ZIP file is saved in the same folder as this script .

When a new log file is created, the date is appended to the existing log's file name. For example, PMPWebService.*yyyy.mm.dd*.log. The most current log takes the base file name.

| Server component | Path to log files |
|---|---|
| PMP Web Service | `C:\Program Files\Verdiem\Surveyor\Logs\ PMP WebService.log` |
| Enterprise Power Management Service | `C:\Program Files\Verdiem\Surveyor\Logs\PowerManagementProcessor.log` |
| Administrator web service | `C:\Program Files\Verdiem\Surveyor\Logs\AdminWebService.log` |
| Data Summarization | `C:\Program Files\Verdiem\Surveyor\logs\Summarization.log` |
| Wake for Remote Access | `C:\Program Files\Verdiem\Surveyor\Logs\wra.log` |
| Connect for Microsoft System Center (Verdiem Integration for SCCM) | `C:\Program Files\Verdiem\Power Management Pack for ConfigMgr\Logs\PowerPackForConfigMgr.log` |
| ActiveMQ | `C:\Program Files\Verdiem\Surveyor\activemq-5.13.4\bin\win32\wrapper.log` |
| IIS | `C:\inetpubs\logs\logfiles` |
| Analytics and Dashboard | `C:\Program Files\Verdiem\Surveyor\Logs\`ReportExecution.log |

> **Note:** Archived logs may be available and will include a date stamp in the file name. The most current log will not have a date stamp and will be named as indicated in the table.

# IIS Log File Size

If your IIS log file size is getting too large, you can either reduce the amount of data being logged, or you can run a daily scheduled task to periodically trim the Surveyor data logged in the IIS log file to the last 30 days.

## Reduce the Amount of Data Being Logged

In Surveyor Server Settings, set the check-in interval to a higher number of minutes.

*Server Log File Locations on the previous page*

## Run a Daily Scheduled Task to Trim the IIS Log File Size

Starting with Surveyor 6.0.505, the download installation package includes the script **DeleteIISLogs.ren** (in the **..\Surveyor 6_x_xxx\Extras\Scripts** folder) that you can run as a daily scheduled task on high traffic web servers to avoid running out of disc space.

The script assumes the IIS log directory is **C:\inetpub\logs**. Update the script if the path is different, or you wish to use a different number of days for data retention.

# Client Log File Locations

## 6x Log Files

On Surveyor 6 client computers, log files are saved in the following locations:

**Surveyor Client Logs: C:\Program Files\Verdiem\Surveyor Agent\Logs**.

The files are named PwrMgrService.log.n, where n is a positive integer.

Windows Vista, Windows 7, Windows 8, or Windows 10 -
**C:\Users\<user>\AppData\Local\Verdiem\Surveyor\Logs**

The files are named PwrMgrUserSession.log.n, where n is a positive integer.

**Macintosh Clients:**

~\library\logs\verdiem

## 5x Log Files

On Surveyor 5 client computers, log files are saved in the following location:

**Surveyor Client Logs: C:\Program Files\Verdiem\SurveyorSD\Logs**.

The files are named surveyorsd.log.n, where n is a positive integer.

Surveyor Session LogsWindows XP - **C:\Documents and Settings\<user>\local Settings\Application Data\Verdiem\Surveyor\Logs**

Windows Vista, Windows 7, Windows 8 or Windows 10-
**C:\Users\<user>\AppData\Local\Verdiem\Surveyor\Logs**

The files are named surveyorsession.log.n, where n is a positive integer.

**Macintosh clients:**

**~\library\logs\verdiem**

# 11

# Using Wake for Remote Access

**Table 11-1  In this Chapter**

| Topics |
| --- |
| *Overview - Wake for Remote Access* |
| *Options for Customizing Wake for Remote Access* |
| *Open the Wake for Remote Access Web Page* |
| *Application Settings that You Can Customize in IIS Manager* |
| *Customizing the Wake for Remote Access (WRA) Front End* |

# Overview - Wake for Remote Access

This section contains information about customizing Wake for Remote Access. You can do this both on the server side, modifying IIS application settings, and on the client side, changing the styles and layout for the browser pages that end users visit to wake their computers.

Wake for Remote Access enables members of your organization to access their computers on site when they're working offsite, even after their on-site computers have transitioned to sleep.

As a component of the Surveyor system, it does this through the unique Surveyor Wake on WAN technology.

Using a standard web browser and a simple web interface, end users enter or search for their computer name. They then click to send a request to the Surveyor power management server to wake their computer. When the computer is awake, the end user follows your organization's established remote login procedures to access the computer.

The following diagram shows a basic Wake for Remote Access overview (database and Administrator console shown for context).
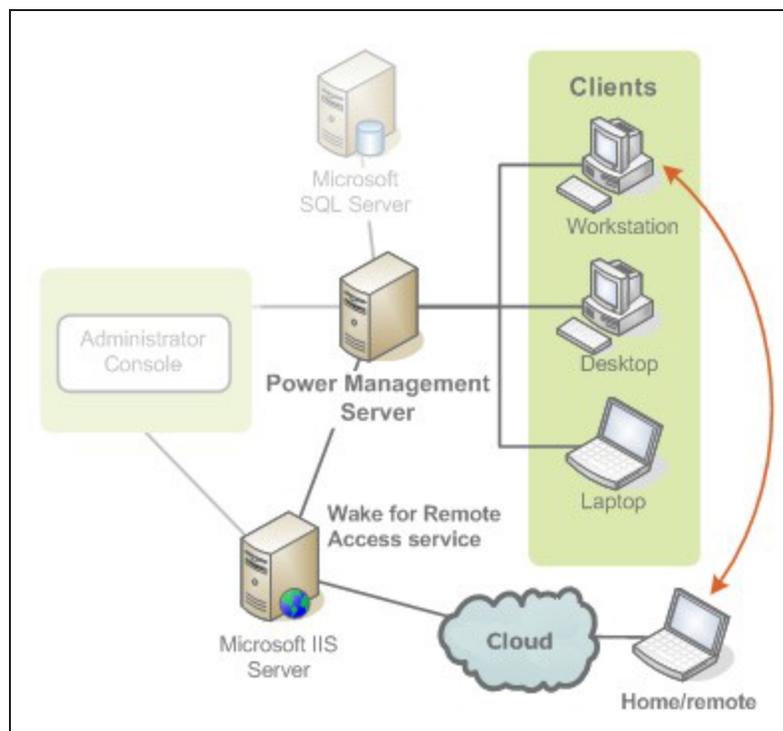


**Tip:** The users' computers on site must have the Surveyor client agent installed, but they do not need to install it on their remote computers to use Wake for Remote Access.

# Options for Customizing Wake for Remote Access

You can customize Wake for Remote Access in these ways:

- Help end users find their computers if they aren't sure of the computer name, such as allowing wildcard searches.
- Configure parameters to comply with your organization's IT policies, such as disabling browser cookies.
- Specify the maximum number of computers that are returned in the search results.
- Modify the browser pages that end users view to do the following:
  - Match your organization's branding.
  - Modify the Help tips to reflect application customizations you make or add other tips that would help your end users.

To customize application parameters you use the IIS Manager. To customize the Wake for Remote Access browser pages, you edit content in the .aspx and .css files.

# Open the Wake for Remote Access Web Page

- From the Windows Start menu, click All Programs > Verdiem > Wake for Remote Access.

  If the Wake for Remote Access web page does not open, you may need to enable ASP.NET in IIS. For details, see Application Services and UI issues in the Surveyor Knowledge Base.

  > **Note:** If Windows Firewall is enabled on the Surveyor server, you will need to make sure TCP port 80 is added to the exceptions list. For details see *Configure Windows Firewall to Allow Web Components to Access the Server on page 12-5*.

- (Optionally) In your web browser, enter the URL for the local web site on the computer where you installed the Surveyor server, such as **http://hostname/WRA/** where *hostname* = Surveyor power management server name.

  For example, **http://localhost/WRA/** or **http://myComputerName.myDomain.local/WRA/**.

# Advanced WRA

For the administrator, there is no change in the functionality of WRA for administrator.

**For Non-administrator**

When the user log in, WRA provides the list of machines that are recently logged in. It will help the user to wake the machines based on the permissions given in Surveyor.

After waking the machine, the user will be able to initiate a RDP session to the desired machine.

For enabling and disabling the wake permissions, refer to Surveyor 6  Administration Guide.

For Technical Support contact information or to log on to the portal, visit the Support page on avolin.com.

# Application Settings that You Can Customize in IIS Manager

This topic describes the changes you can make to the Wake for Remote Access application settings in IIS Manager.

For example, you can control the search options that are available to end users.

## Search form Customizations

When end users go to the Wake for Remote Access web site, they can enter search criteria to find the computer they want to wake.
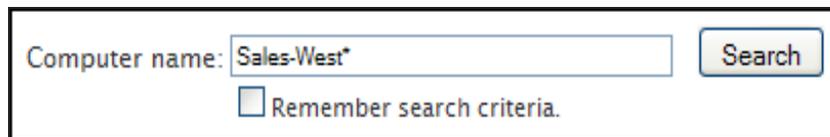


Search for computers with names that contain Sales-West. By default, the following search features are enabled:

- Support for wildcard characters (* or _), for finding similar computer names.

  > **Note:** By default, users must type at least three characters in the Search form. If they try to use a single asterisk to return all clients, they get a message to try again.

- The option to remember the search criteria that the user last entered (through a cookie).

  If users select the box to remember the search criteria, the next time they use Wake for Remote Access, the Search form is populated with their saved search text.

  You can disable either of these options, as well as change the minimum number of characters required and other parameters, in the IIS Manager.

## Search and Wake Results Customization

When users include wildcard characters in their searches, a list of matching computers is returned. By default, the search results page displays only the first five computers that match the search criteria.

If the user's computer is not listed in the first five results, he or she must refine the search criteria and try again.

You can use the IIS Manager to change the maximum number of computers that are returned in search results. For information about customizing additional information returned with the results, see *Customizing the Wake for Remote Access (WRA) Front End on page 11-12.*

**Note:** Search results return only computers on which a licensed Surveyor client agent is installed. (Unlicensed agents are not returned.)
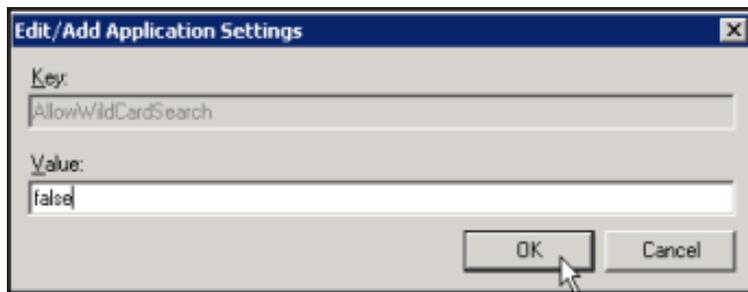
# How to Customize Application Settings in IIS Manager

These steps describe how to access and modify the WRA application settings in IIS depending on the version you use.

## Access WRA Application Settings in IIS 6

1. On the IIS server, use the Windows Start menu to open the IIS Manager.

2. In the IIS Manager, navigate to the WRA site, right-click it, and choose **Properties**.

3. In the Properties dialog box, click the **ASP.NET** tab, and then click **Edit Configuration**.

4. Customize the application settings you want.

   For descriptions, see *Wake for Remote Access (WRA) Application Settings and Descriptions on page 11-10*.



## Access WRA Application Settings in IIS 7

1. On the IIS server, use the Windows Start menu to open the IIS Manager.

2. Navigate to *hostname/Sites/Default* Web Site, and select WRA.

3. On the Home page, under **ASP.Net** double-click **Application Settings**.

4. Customize the application settings you want.

For descriptions, see *Wake for Remote Access (WRA) Application Settings and Descriptions on page 11-10*.

# Wake for Remote Access (WRA) Application Settings and Descriptions

The following table lists and defines the WRA application settings that you can customize in IIS Manager.

| Setting Name | Default Value | Description |
|---|---|---|
| AllowWildCardSearch | True | Allow users to include the * and ? wildcards in searches. If you set it to false, users must enter their exact computer name.<br><br>If you disable wildcards, you should also edit the Tips content in the Default.aspx page, so that it does not describe how to include wildcards in searches. For information, see *Edit Web Page Tip Text to Reflect Modified Application Settings on page 11-13*. |
| AutoPing | True | Pings the computer the user wants to wake before sending the wake request, to determine whether the computer is already awake.<br><br>For more information, see Timeouts during the wake process. |
| MaxReturn | 5 | Sets the maximum number of results that are displayed on the search results page. |
| MinSearchLength | 3 (including wildcards) | Sets the minimum number of characters a user must enter in the Search form. |
| Refresh | 2 | Number of seconds to wait before refreshing the status on the wake results page.<br><br>This excludes the page load time, so the actual result can take a few seconds longer than the value specified. |
| ServerName | Your Surveyor server name | A text string that displays the name of the power management server that the WRA service communicates with. |
| ShowCookieCheckBox | True | Specifies whether to allow users to save their search criteria. If they do, a browser cookie is set on their computer.<br><br>If you set this to false, the check box and label do not appear on the home page. |
| SupportText | If you continue to receive this error, please contact your support department. | This message appears on the search results page if the Wake for Remote Access service has a problem communicating with the Surveyor server when a user searches for a computer.<br><br>This can occur, for example, if the server is offline, or |

| Setting Name | Default Value | Description |
|---|---|---|
| | | the server name setting is not correct in the IIS Manager. |
| Timeout | 900 | Number of seconds to wait before determining that the computer is not reachable. |
| | | If you want to change this, we recommend using 1.5 times the value set for Devices should check-in every X minutes  on the System Settings page of the Surveyor Administrator console (default is 10 mins). |

# Customizing the Wake for Remote Access (WRA) Front End

If you have experience with XHTML and CSS, you can customize the Wake for Remote Access front-end browser pages.

You might want to do this if, for example:

- You disable wildcard characters in searches and want to remove the Tips text that describes how to use them.
- You want the pages to better reflect your company's branding.
- You want less computer information to appear in search results.

## Browser Page Location

The web pages are in the root of the Wake for Remote Access site:

**Program Files\Verdiem\Surveyor\WRA**

Users view the following pages:

- Default.aspx (home page)
- SearchResults.aspx
- WakeResults.aspx

Within each of these pages is a section of XHTML code that contains the Tip text and other page elements, including code that inserts the Wake for Remote Access application.

The title bar text for the browser window is specified in the **MasterPage.master** file.

The .css style sheet in the **Styles** directory defines the header image and other style and layout attributes.

> ⚠ **Caution:** Before you edit the .aspx, .master, and .css files, create backup copies. Edit them at your own risk. Verdiem Technical Support cannot troubleshoot errors you receive after customizing these pages.

# Edit Web Page Tip Text to Reflect Modified Application Settings

If you change the WRA application settings in IIS, you also will want to update any related text on the Wake for Remote Access front-end web pages.

1. On the IIS server computer, navigate to Program Files\Verdiem\Surveyor\WRA, and open one of the .aspx pages in a code or text editor. For example, Default.aspx.

2. Search for the text you want to edit, and then change it to reflect what you want your end users to know, incorporating any XHTML code to display it the way you want.

   For example, if you disable wild cards, you would want to remove the section of code selected in the following image, showing Tip text for Default.aspx:

# Modify Which Computer Attributes are Returned with Search Results

For each computer returned, search results include the computer's name, IP address, MAC address, and the option to wake or ping it.

If you want to restrict information that appears in search results, you will need to edit the XHTML code that displays the information. For example, you can comment out the Ping button or the IP or MAC address.

1. Navigate to **Program Files\Verdiem\Surveyor\WRA**, and make a backup copy of SearchResults.aspx.

2. Open the original SearchResults.aspx file in a code or text editor.

3. Under <ItemTemplate>, look for the table row that contains the information you want to remove, and comment out that row.

   For example, to remove the IP address, comment out this code block:

   ```
   <tr>
   <td><strong>IP Address</strong></td>
   <td><%# DataBinder.Eval(Container.DataItem, "IP") %>
   </td></tr>
   ```

4. Make any other changes you want, and then save and close the file.

5. Test the page to make sure your changes give the expected results.

If you are comfortable with your changes after they've been in production for awhile, you can remove the code, but make sure you keep the original backup copy.

# Changing the Header Text and Logo Image

You can customize the styles for Wake for Remote Access (WRA) so it uses your organization's logo and color palette.

To do this you edit the following files inProgram Files\Verdiem\Surveyor\WRA:

- **MasterPage.master**

  Here you can remove or modify the text that appears in the header section of each page.

- **Styles\wra.css**

  Here you can change the header, body, or content backgrounds and customize colors, fonts, and other style and layout attributes.

# 12

# Troubleshooting

**Table 12-1  In this Chapter**

| Topics |
| --- |
| *Administrator Console Does not Open in Browser* |
| *Configure Windows Firewall to Allow Web Components to Access the Server* |
| *Configure the web server to allow ASP.NET v.2.0.50727 applications* |
| *Wake for Remote Access Troubleshooting* |

# Administrator Console Does not Open in Browser

This section includes troubleshooting information for Surveyor server and Wake for Remote Access.

This article describes the IIS settings that you can configure if the Administrator console does not open in a browser.

## Symptoms

When you attempt to open the Administrator console, the console does not open. In some cases, you might see a 404 - file not found error.

## Cause

The most common causes include:

- *Administrator Console Does not Open in Browser above*
- *Administrator Console Does not Open in Browser above*
- *Administrator Console Does not Open in Browser above*
- *Administrator Console Does not Open in Browser above*

## Solution

All solutions involve configuring settings in the IIS Manager.

### IIS is not Configured to Allow ASP.NET v.2.0.50727 Applications

If this is the issue none of the Surveyor web components will open, and you might get an error 404. For steps to allow ASP.NET applications, see *Configure the web server to allow ASP.NET v.2.0.50727 applications on page 12-6*.

### ASP.NET is not Registered in IIS

This might be the case in one of the following circumstances:

- The 32-bit version of the .NET framework has been installed on a computer running a 64-bit operating system.

  To resolve the issue, enable IIS to run 32-bit applications.

- IIS was installed after the .NET framework, and multiple versions of ASP.NET exist.

To resolve the issue, you run the ASP.NET Registration Tool (Aspnet_regiis.exe) from the command line and appropriate location.

The command uses the -i parameter, which installs the ASP.NET version that is associated with the registration tool and updates the script maps for the Sustainability Dashboard and other ASP.NET applications that use an earlier version of ASP.NET. (Applications that use a later version are not affected.)

```
<.NET installDir>\aspnet_regiis.exe -i
```

Run the registration tool from the location that will register the dashboard with the correct version of ASP.NET.

**For example**

```
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_
regiis.exe -i
```

**Note:** To download the tool and get additional information about what it can do, see ASP.NET IIS Registration on the MSDN web site.

## Multiple Versions of ASP.NET Registered in IIS

In cases where ASP.NET 4.0 was registered with the IIS, you may need to unregister ASP.NET 4.0 and then re-register ASP.NET 2.0.

**Note:** On Windows Server 2003 x64, IIS does not show the ASP.NET tab to change the version.

- Unregister ASP.NET 4.0:

  C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe /u

- Re-register ASP.NET 2.0:

  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe /i

# Windows Server 2008 Systems: Windows Authentication is not Enabled in IIS 7

To enable Windows Authentication in IIS 7:

1. Open IIS Manager and click the **Default Web Site**.
2. In the IIS section, double-click **Authentication**.
3. Right-click **Windows Authentication** and choose **Enable**.

**Applies to**

**Product**

- Verdiem Surveyor 5.x versions

**Component**

- Administrator console

**Other**

- IIS 6.0
- IIS 7.0

# Configure Windows Firewall to Allow Web Components to Access the Server

If you use Surveyor components that access the server through http, and Windows Firewall is enabled on the server, make sure TCP port 80 and port 443 is added to the exceptions list.

You would need to access the server through http if you do any of the following:

- Enable Wake for Remote Access for your end users to wake their computers from home or another off-site location.

  Wake for Remote Access is an add-on component that comes with Surveyor. For information see the Wake for Remote Access Guide.

- Administer the server from a remote computer; for example, as you would if you set up delegated administration.

1. On the server computer, navigate to **Windows Start menu / Control Panel / Windows Firewall**.

2. On the **Exceptions** tab, click **Add Port**.

3. In the Add a Port dialog box, do the following:

   a. Type a name that indicates that the exception is for power management components. (This name appears in the exceptions list.)

   b. Specify port 80 or port 443 if using an https configuration.

   c. Select TCP.

4. Click OK, and then click OK in the Windows Firewall dialog box.

For additional information, refer to the Microsoft TechNet topic Add a Port to the Firewall Rules List.

# Configure the web server to allow ASP.NET v.2.0.50727 applications

The correct version of ASP.NET must be allowed on any computer that hosts the Surveyor server or Wake for Remote Access.

Open IIS Manager, and allow ASP.NET v2.0.50727.

- **IIS 6**: Click **Web Service Extensions**, select **ASP.NET v2.0.50727**, and then click **Allow**.
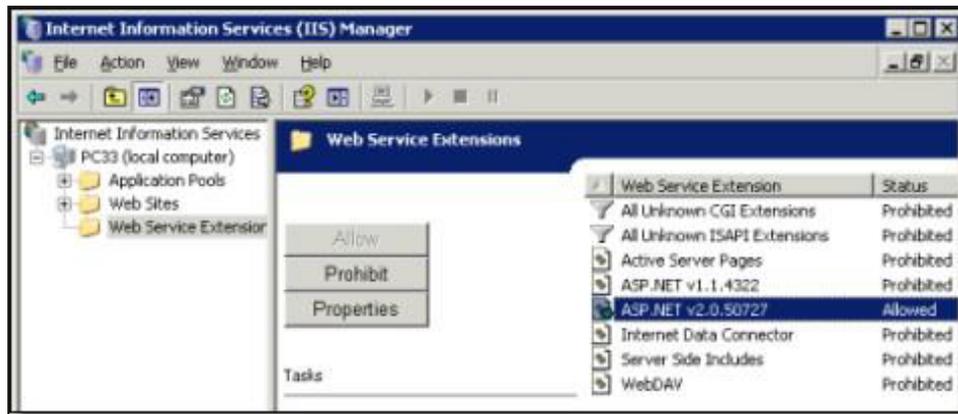


- **IIS 7**: Select the server home, double-click **ISAPI and CGI Restrictions**, and then allow **ASP.NET v2.0.50727**.
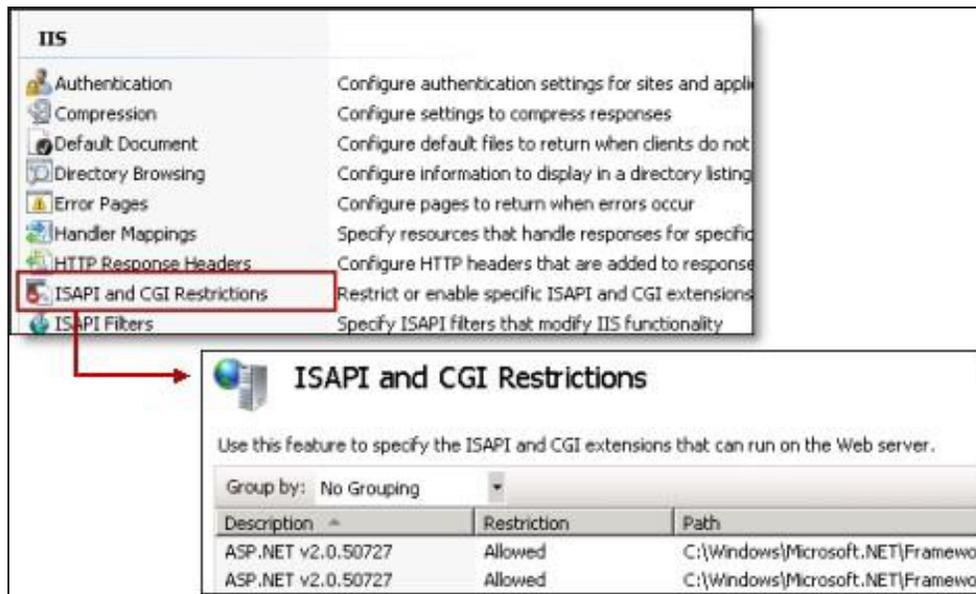
# Wake for Remote Access Troubleshooting

This section provides solutions to common errors that can occur when you run Wake for Remote Access after installing it, and describes the test files that come with the Wake for Remote Access installation.

# Security Message Trying to Display the Wake for Remote Access Home Page on Windows 2003

This error can occur if Internet Explorer identifies Wake for Remote Access as an Internet or untrusted zone.

## Issue

You might get a security message if you open the home page (Default.aspx) in Internet Explorer, particularly on a Windows Server 2003 computer, on which the Internet Explorer Enhanced Security Configuration component is enabled. Under these conditions, the Wake for Remote Access site could be identified as an Internet, or untrusted, zone, and it does not display the page.

## Solution

To resolve the error, you can do one of the following:

- Disable Internet Explorer Enhanced Security Configuration through Control Panel, in the Add/Remove Windows Components section under Add/Remove Programs.

- Leave Enhanced Security Configuration enabled, and add the Wake for Remote Access server URL to the intranet zone in Internet Explorer:

  1. In IE, choose **Tools / Internet Options**, and on the Security tab, click **Local intranet**.

  2. Click **Sites**, click **Advanced**, and then add the Wake for Remote Access server URL to the intranet zone.

For more information, see Microsoft Knowledgebase Article 303650.

# Timeouts During the Wake Process

## Issue

A user receives a timeout error when trying to wake his or her computer.

## Conditions and Cause

The **Device check-in interval**, set on the Server Settings page in the Administrator console, can affect how long a wake request takes if the following conditions are true:

- A computer is already awake when a user sends a wake request through Wake for Remote Access.

  AND

- The *Wake for Remote Access (WRA) Application Settings and Descriptions on page 11-10* is set to false.

Under these conditions, if a user sends a wake request to a client through Wake for Remote Access shortly after the client's last check-in, the wake process can take almost as long as the check-in interval.

By contrast, if the computer is asleep, it receives the wake request when the server makes the request available.

## Solution

To resolve this issue, set **AutoPing** to true, which is the default value.

> **Note:** The **wake results** browser page contains information to alert the user that frequent timeouts can indicate that the computer is awake. From there it suggests that the user try to log in to the computer normally.

# Wake for Remote Access Issues Related to the IIS Application

This topic describes issues that can occur under specific conditions on the IIS server that hosts Wake for Remote Access.

## IIS Application Pool Unexpectedly Exits When a Worker Process Shuts Down or is Recycled

This problem can occur if the user running the Wake for Remote Access service is not a member of the Windows group IIS_WPG on the IIS server. For information, see *Wake for Remote Access permissions requirements* and [Microsoft Knowledgebase article 918041](#).

### IIS Application Error

The following IIS error occurs:

An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

### Resolution

You can try to view the web page from the computer on which Wake for Remote Access is installed. You can also temporarily enable the viewing of error details remotely.

> **Note:** Enabling the viewing of error details remotely may impact Wake for Remote Access performance and is best for temporary troubleshooting use.

## WRA Error: Unable to Process Wake

When the following attached error appears on the Wake for Remote Access web page:

| Computer Wake Information | |
|---|---|
| Computer Name | w2k557 |
| Status | Unable to process wake. If you continue to receive this error, please contact your support department. |
| Elapsed time | 0:02 (Action Complete) |

A possible cause of this error is that the application pool identity does not have wake access in Surveyor.

## Resolution

In IIS, right-click the WRA application pool, and then choose Properties. Click the Identity tab and ensure the correct security account is selected for this application pool.

# Duplicate Computer Names Returned in Search Results

## Issue

An end user performs a search, and the results return more than one computer with the same name.

## Solution

To find the source of this problem, open the Administrator console, and display the duplicate computers to see why there are two or more of them.

Most commonly, this issue occurs if you need to replace a computer or a network card, but you still use the same computer name. The **Last Connected** value can help you determine whether this is the case. Make sure that instances of the computer that are not in current use are unlicensed in Surveyor, so they do not appear in Wake for Remote Access search results.

# Using the Wake for Remote Access (WRA) Test Files for Troubleshooting

You can use the Wake for Remote Access test files if the issue you're experiencing is not covered earlier in this section.

These test files can provide you and Verdiem Technical Support with useful information for where to start troubleshooting unknown issues.

The test files reside in the **Program Files\Verdiem\Surveyor\WRA** directory.

## How to Use the Test Files

When you receive an error message or otherwise are not able to run Wake for Remote Access, open a web browser, and enter the test file URL in the address bar. For example, *http://YourServerName/WRA/* test file name, where test file name is one of the following:

**test.html**—This HTML content is a simple success message. If it does not display, the source of the issue is in IIS or your Internet connection.

**test.aspx**—This file tests ASP.NET and the power management server connection. When you open this file, it displays the results of a series of tests.

The results tell you where the tests failed. For example, if **Result** shows **Connected**, but the **Permissions Test** shows **Failed**, you know that you have access to the power management server, but the current user does not have the required permissions on the power management server.

# Configuring Report Execution Timeout

A default timeout of 5 minutes (300000 milliseconds) has been set for report execution. After this timeout, report execution is stopped and error message is displayed. Additionally, a log entry reading `The operation has timed out` is added in the report execution log.

This timeout value is configurable. However, you cannot set a value below 1 minute (60000 milliseconds).

**To configure the report execution timeout:**

1. Navigate to C:\Program Files (x86)\Verdiem\Surveyor\Reports

2. Open **DeployReportsConfig** XML file in a text editor (Notepad).

3. Modify the numerical value of **ReportTimeout**.

```
<DeploymentStatus>0</DeploymentStatus>
<ReportTimeout>300000</ReportTimeout>
</RSParameter>
```

4. Save the file.

5. Restart IIS using the following steps.

   a. Select **Run Command** and type **services.msc**.

   b. Select "**IIS**" and right click and select "**Restart**".