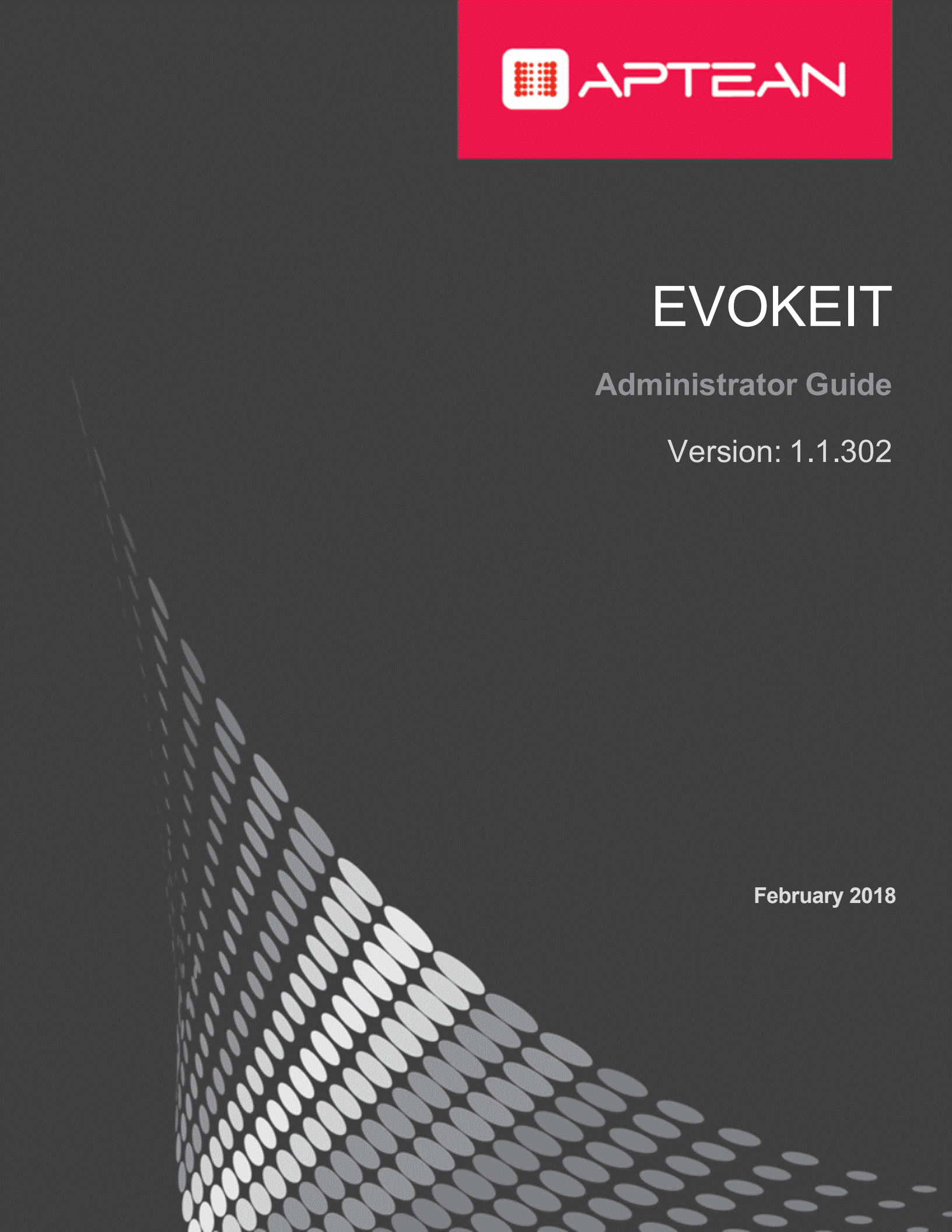


EVOKEIT

Administrator Guide

Version: 1.1.302

February 2018

4325 Alexander Drive, Suite 100 • Alpharetta, GA 30022-3740 • www.aptean.com • info@aptean.com

Contents

1

About EvokeIT

Table 1-1 In this Chapter

Topics
Overview of EvokeIT
Wake Management for PCs
Getting Started with EvokeIT and wake management
Open the Administrator Console
System Settings and Descriptions

Overview of EvokeIT

This section introduces EvokeIT and concepts related to the power state transition of Windows and Mac computers, and other devices.

EvokeIT is a low-cost, low-effort power state transition tool. EvokeIT allows you to keep endpoint devices up-to-date from both a software and driver perspective.

With EvokeIT, you can reliably push software and updates when users are not using their machines. This reduces the likelihood of the user experiencing operational slowdown. As a result, the impact on the end user is substantially decreased.

EvokeIT Features

EvokeIT 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 state transition	Agent-based, non-intrusive PC and Mac power state transition with minimal impact to end-users, business applications, or IT maintenance activity.
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 EvokeIT client agents from a remote location over the web and schedule strategic wake requests to work around scheduled maintenance windows.
Role-based security	Group-oriented administration with role-based security privileges.
Analytics reporting	The dashboard provides actionable information on asset inventory and has wake-related reports.

Configuring Schedule Policies in EvokeIT

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

A device in EvokeIT can be a Windows PC or a Macintosh computer.

A policy contains the following types of settings:

- **Scheduled power level transition** (PC and Mac only) that specify the time at which the device transitions to a lower power state. Each policy can have a unique schedule.
- **Wake up settings** for PC and Mac clients.
- **Logging and data collection settings** for PC and Mac clients.

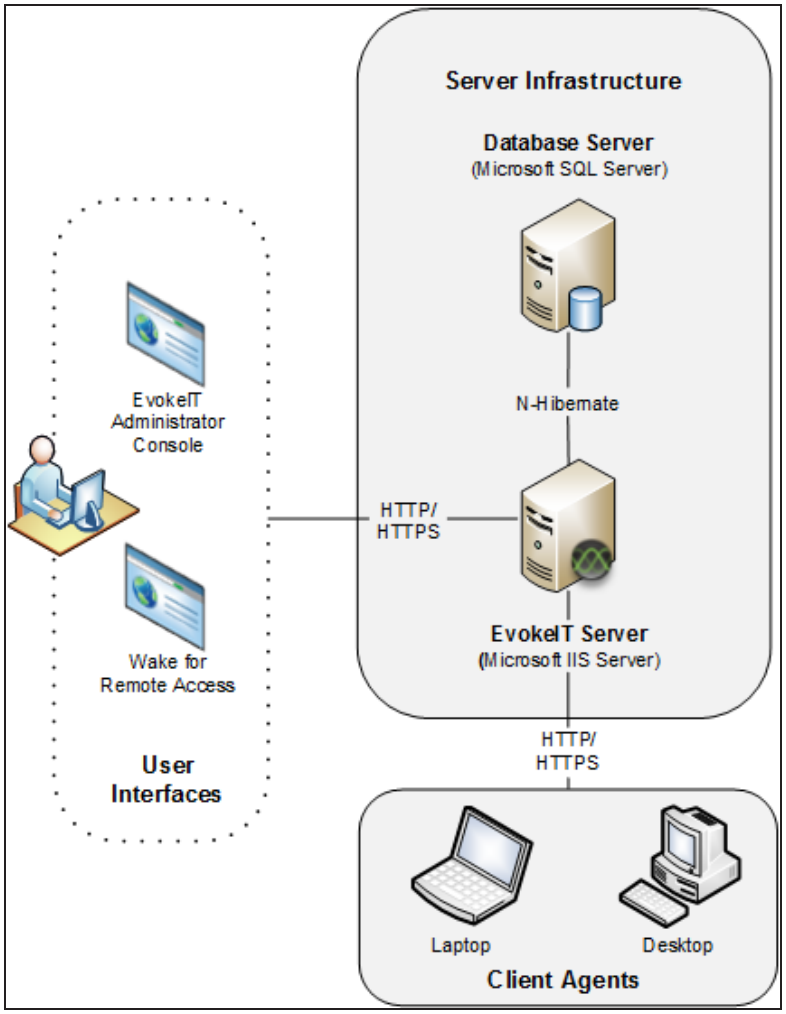
EvokeIT assigns policies manually or through assignment rules that you create. Each device can have only one policy assigned to it, but each policy can contain power level changes, each with its own schedule.

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

For general steps, see *Getting Started with EvokeIT and wake management on page 1-6*.

EvokeIT System Components

In a basic installation for PC and Mac power state transition management, the EvokeITsystem comprises the following components:



Component	Description
EvokeIT Server	Manages policy distribution, sends power state change instructions to client devices, and captures data to send to the EvokeIT database.

Component	Description
Database Server	A Microsoft SQL Server database that stores power state and other device data sent 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 wake management instructions from the EvokeIT server.

Wake Management for PCs

This section is an overview of the history and common issues in PC wake management for software updates.

Overview of wake management for software updates

The IT department is entrusted with the responsibility of ensuring software are updated on a timely basis. To ensure this happens, IT professionals need to push software and updates to endpoints on a continual basis.

Presently, IT professionals do not have a reliable tool or method that they can use to wake machines from a sleep or off state. Because of this, IT professionals need to either push software on a 'When the machine next comes on' basis or push the software at times when they expect it to be on. In both of these circumstances, the user will likely experience operational slowdown of the machines.

A wake management tool like EvokeIT allows IT professionals to wake endpoint devices and perform software distribution and patch management tasks, all of which is centrally controlled.

In summary, by using EvokeIT, IT professionals are able to:

- Wake endpoint devices at the most convenient times.
- Install and update software and perform patch management with greater efficiency.
- Have minimal operational slowdown.
- Centrally control a network of computers.

Getting Started with EvokeIT and wake management

This section provides a suggested workflow to configure wake management settings in EvokeIT.

Setting Up Wake Management in EvokeIT

The Administrator console in EvokeIT helps you set up administrative groups and wake management policies.

You can set up administrative groups and wake 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 wake management settings in a network.

The following workflow suggests how you might consider configuring wake management settings in EvokeIT.

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 > EvokeIT Administrator. For other details, see *Open the Administrator Console on page 1-8*.
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 EvokeIT menu  , click **Devices**, and then click a group name to view its devices. To filter the view, click the Search button  . For more details, see *View Devices and Attributes on page 4-13*.
3	Create groups that reflect your needs for organizing, controlling access to, and reporting on devices.	In the Administrator console, on the EvokeIT menu  , click **Groups**. 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 manually or through assignment rules.	For details on groups, see *Assign Devices to Groups on page 4-17* and *Configure Group Assignment Rules on page 2-5*.
5	Configure security settings to control administrator access to devices and policies (optional).	To configure security settings: In the Administrator console, on the Configure menu  , click **Roles** & **Permissions**. For details, see *Configuring Permissions for Delegated Administration on page 3-2*.

Step	Task	Description
6	Determine the policies you need to enforce wake management in your organization. Modify existing policies or create new ones to meet your needs.	In the Administrator console, on the EvokeIT menu, click **Policies**, and then click a group to view the policies in that group that you have permission to edit. Select a policy and edit the policy settings and schedule including power level changes, and power state transition rules. For details, see *Create and Edit Policies on page 5-7* and *Create and Edit Power State Transition Rules on page 5-14*.
7	When you are ready to start enforcing wake management settings on devices, assign policies to devices manually or through assignment rules. Begin policy enforcement by changing the device policy from the default policy to another policy that enforces wake management settings.	**To assign policies to devices manually**: 1. In the Administrator console, on the EvokeIT 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 a device or set of devices. 3. Right-click a device (or a multi-selected set of devices), and then click **Manually Assign Policy**. For more details, see *Assign Policies to Devices on page 4-18*. **To assign policies to devices automatically:** In the Administrator console, on the Configure menu, click **Auto Policy Assignment Rules**. For details, see *Configure Policy Assignment Rules on page 5-9*.

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 > EvokeIT 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 EvokeIT Knowledge Base.

  Note: If Windows Firewall is enabled on the EvokeIT 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 10-4*.

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

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

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

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 EvokeIT 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. 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. **Recommended setting**: The same number as the number of devices in your largest EvokeIT group. **Note:** Setting this to a large number of devices (thousands) might affect viewing or browsing performance.
When EvokeIT wakes devices	**Batch devices into sets of *X*** 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. **Wait *X* seconds before sending next request** 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. It is preferred to set this as 2 proxies.
Keep detailed diagnostics device data for X days	The number of days that data on device diagnostic events are stored. The default is 7.

Setting	Description
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.
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.

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** When selected, EvokeIT uses the system setting for **Maximum number of devices returned per view** (described above). To specify a local preference for the Administrator console (saved in a cookie for the current browser session), select **Return** and then specify a different number. **Note:** Setting this to a large number of devices (thousands) might affect viewing or browsing performance.

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 EvokeIT 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 4-17* 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.

EvokeIT 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 EvokeIT deployment depends on the needs of your particular organization.

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 EvokeIT 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 EvokeIT to place new devices automatically into the appropriate groups when the devices connect to the server.

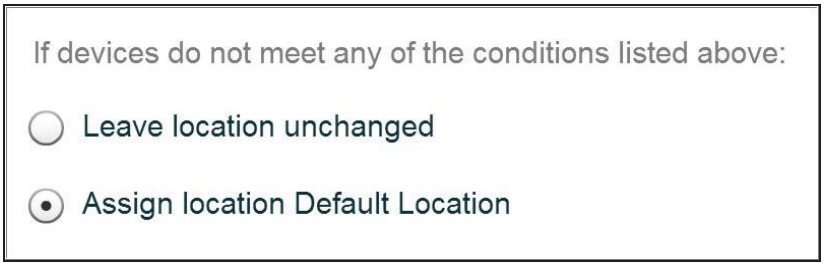
When you configure group assignment rules, devices are automatically assigned to specific groups based on a set of criteria. For example, you can create a rule for a Training Lab group that accepts clients only from a particular IP segment and with the string 'train' in their DNS names.

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 EvokeIT 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.



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 EvokeIT Deployment

Table 3-1 In this Chapter

Topics
Configuring Permissions for Delegated Administration
Grant Root 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 EvokeIT 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 EvokeIT deployment. This topic briefly describes its role-based security and permissions model.

Overview of the Role-based Security Model

EvokeIT 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 EvokeIT 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 EvokeIT deployment. By default, anyone who has local administrator permissions on the EvokeIT 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 EvokeIT 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 3-6*.

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 3-6*.

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 EvokeIT 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)

Create Additional Security Roles and Grant Permissions

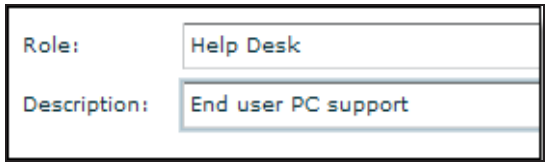
To grant access to perform administrative tasks, you create security roles, configure permissions sets for each role, and then add users to the appropriate roles.

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 EvokeIT server who is also a member of the Root Administrator role in the EvokeIT 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.



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 EvokeIT 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 EvokeIT 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.

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 EvokeIT 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). Does not give access to policies.

Permission	Access level that it allows
	You can move devices from one group to another when you have Manage groups permission for both groups. 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. 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. 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. 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 EvokeIT 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 EvokeIT. 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 wake 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
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
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 EvokeIT can be a Windows PC or Macintosh computer, and wireless access points (WAPs).

Note: The frequency for device check-in and how EvokeIT 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 4-13*.
- Control device power states and levels directly, outside of a policy. For details, see *Manually Control Devices on page 4-20*.
- Assign policies to devices. For details, see *Assign Policies to Devices on page 4-18*.
- Assign devices to groups. For details, see *Assign Devices to Groups on page 4-17*.
- 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 power state changes in the policy schedule.

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. EvokeIT 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 Wake Management Settings on page 5-2*.

Device Connections and Check-ins

When a device connects to the EvokeIT 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 EvokeIT 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 EvokeIT 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 EvokeIT server will mark the device as Not checking in. When the device begins checking in again, the EvokeIT 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 EvokeIT and all types of devices when they connect to, and check in, with EvokeIT.

Action	Description
Connections (New and Reestablished)	• Device asks the EvokeIT server for what pieces of information it should send. • EvokeIT server asks the device to send four key pieces of information: Device GUID, netBIOS, MAC address, and policy version. Server receives the device GUID, netBIOS, and MAC address values from the device, and then registers the device as appropriate.

Action	Description
	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. • Server tells the device the check-in interval based on the interval setting in the Configure Server Settings page. **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 EvokeIT configuration file. • Server assigns a computer to a broadcast domain based on its IP address (if new). • Server evaluates a computer client as a candidate for Wake on WAN proxy. • Server evaluates group and policy assignment rules. 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. • 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. • Server records the check-in time and flags the device status as Checking in if it was previously Not checking in. • Devices with updated information, such as attribute changes, or power usage data, send this data to the server. • Server evaluates group and policy assignment rules (if the rule is set for All 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, EvokeIT 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

Action	Description
	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 EvokeIT menu to view details on operational state, user activity, and event log information for devices.

Power States and Activity

EvokeIT 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 5-6*.

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

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

The power states that EvokeIT tracks for monitors are:

- Low power
- On
- Off

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

EvokeIT manages the following power state changes for PCs:

- Wake
- Sleep
- Hibernate
- Shutdown
- Restart

EvokeIT manages the following power state changes for Mac computers:

- Wake
- Sleep
- Hibernate

> **Note:** For Macintosh computers, EvokeIT translates Hibernate to Sleep. When EvokeIT 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 EvokeIT 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 4-24*.

Device Properties and Attributes

The EvokeIT 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 EvokeIT Administrator console on the Devices page. Some device attributes are created by the server and some are reported by the device. The EvokeIT 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 EvokeIT group that the device is assigned to.	No, but devices can be filtered based on assigned group.
Assigned Policy	The name of the EvokeIT policy assigned to the device.	No, but devices can be filtered based on assigned policy.
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 EvokeIT.	Yes
Device Family	Used for reporting. Possible values: PC and Mac.	Yes. Devices can be filtered based on device family.
Device Name	For PCs and Macs, this is the NetBIOS name.	Yes
IP Address	For a PC or Mac client, switch the IP address most recently used for communication with the EvokeIT server. This address is the only port that EvokeIT will use to attempt wake on LAN. Assignment rules are applied to the collection of all network adapters.	Yes
Last Connected	Date and time of the last complete connection.	No

Column Name	Description	Searchable
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. Policy Pending indicates that a PC or Mac has not connected to EvokeIT since the policy was applied.	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
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 EvokeIT.	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. The setting is controlled by the option selected in Device Licensing for a device.	No
System BIOS	BIOS string text. For example, DELL - 8, 02/26/03	No

Troubleshooting

Column Name	Description	Searchable
Client Version	Build number of EvokeIT agent software installed on a device.	Yes
Device Status	Indicates whether the device is checking in regularly. Devices check in with the EvokeIT 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. If a device misses two consecutive check-in intervals, the EvokeIT server will mark the device as **Not checking in**. When the device begins **Checking in again**, the EvokeIT 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.	No
Group Assignment	**Rule** indicates the group is being assigned automatically through assignment rules. **Manual** indicates the group has been assigned manually. **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 EvokeIT license. Green check mark = yes; Red X = no.	No
MAC Address	The MAC address of the interface most recently used for communication with the server.	Yes
Memory (KB)	Available memory in KB.	No

Column Name	Description	Searchable
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.  **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 EvokeIT server and the proxy server or device has acknowledged receipt of the most current policy. Possible values: **Delivered** or **Pending**. **Pending** means the PC or Mac client agent server has not retrieved the most current policy yet. **Delivered** means the PC or Mac client agent server has retrieved the most current policy from the EvokeIT server.  **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. **Preferred**: The computer is ranked higher in proxy-selection criteria. **Never**: The computer will never be selected as a proxy. **Default**: Other computer attributes are used as selection criteria only if no preferred proxies available. The setting is controlled by an option selected in Edit Device Properties (right-click a device in list view,	No

Column Name	Description	Searchable
	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 EvokeIT 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, 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 4-8*.

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 EvokeIT 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 EvokeIT 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 4-22*.

1. In the EvokeIT 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 4-13*.

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 5-9*.

Note: All power settings in policies apply to PCs and Macs. For other types of devices, only scheduled power level changes apply.

For details on creating policies, see *Create and Edit Policies on page 5-7*.

1. In the Administrator console, on the EvokeIT 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**.

Assign Unknown Devices to Device Families

When a PoE device that EvokeIT 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 5-7*.

1. In the Administrator console, on the EvokeIT 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 6-18*.

1. In the Administrator console, on the EvokeIT 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 EvokeIT system, or unlicense a device, you can disable the license that is allocated to the device on the Devices page.

EvokeIT 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 EvokeIT 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 EvokeIT 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 4-8*.

1. In the Administrator console, on the EvokeIT 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 EvokeIT 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 EvokeIT 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 8: Viewing Diagnostic Information from Event Logs on page 8-1* and *Display Event Data in the Administrator Console on page 8-12*.

5

Managing Policies

Table 5-1 In this Chapter

Topics
Overview of Policies and Wake Management Settings
About Power State Changes
Create and Edit Policies
Configure Policy Assignment Rules
Edit Default Wake and Data Collection Settings for Policies
Enforce Wake Management Policies
Disable a Policy

Overview of Policies and Wake Management Settings

Introduction

Policies contain the collection of the settings EvokeIT uses to enforce wake management in your organization's network, such as , power level changes, and power state transition rules. This section describes how to create, edit, and manage policies in EvokeIT. 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 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. EvokeIT collects data for all device types for reporting purposes.

Policies can contain the following types of settings:

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 EvokeIT what action to take when a particular application (such as **iexplore.exe** or **firefox.exe**) is running and EvokeIT attempts to transition the computer to standby or shutdown. The rules take effect whenever their associated policy takes effect.
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 6-16*.
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 8-2*

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 power state transition rules that are in effect.
- Power state changes, and power state transition rules that run according to schedule.

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 5-2 General steps for setting up a policy in EvokeIT

Step	Tasks	Procedure
1	Create a policy.	In the Administrator console, on the EvokeIT menu, click **Policy Schedules**, and then click **New Policy**.
2	Create a comprehensive schedule for the policy. The schedule can include one or more power state changes that run on specific days and times.	While editing a policy: Click the **Schedule** tab and then click **Insert PSTM Rule** or **Insert Power Level Transition**.
3	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.
4	Review the wake settings.	While editing a policy: Click the **Wake Settings** tab.
5	Review settings for logging and data collection.	While editing a policy: Click the **Data Collection** tab.
6 (optional)	Create, edit, or reorder policy assignment rules.	On the Configure menu, click **Auto Policy Assignment Rules**.
7 (optional)	Create or edit power state transition rules.	On the EvokeIT 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 power level transition level.

Strategies for Creating Policies

The policies you create should be based on your knowledge of the times of day users are most active, and patch management needs.

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.

Enforce Wake Management Policies

After you determine initial policies, you can assign them to devices.

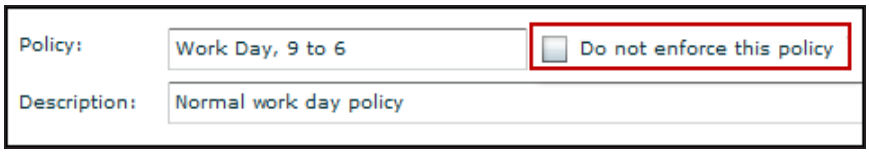
This topic assumes either of the following situations:

- You have created initial wake management policies 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 created policies but you have not assigned them to devices, see “Assign policies to devices” in the *EvokeIT Administrator Guide*.

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

1. Click the EvokeIT button , and then click **Policies**.
2. Select a policy to see its settings. If you already assigned a policy, confirm that the **Do not enforce this policy** option is not selected.



3. Click **Save**.

About Power State Changes

A power state change is part of a policy that can be scheduled, and instructs a device to wake, 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 (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 EvokeIT uses to enforce wake 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. EvokeIT collects data for all device types for reporting purposes.

1. In the Administrator console, on the EvokeIT menu, click **Policy Schedules**.
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. Click **Insert PSTM Rule** to add power state transition rules to the policy.
5. On the Schedule tab, select the days and time time range.
6. Click the **Power State Transition Rules** tab.
   a. Click **Insert** on the top of the window
   b. Select the rule (or rules) you want to add, and then click **Add**.

   Note: For information about how to create a new power state transition rule, see *Create and Edit Power State Transition Rules on page 5-14*

   c. Click **Insert** on the bottom of the window.
7. On the **Insert Power Level Transition** menu, select a power state change to add it to the policy.

   For PCs and Macs only: If you select **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 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.

10. Click **Save**.

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

Configure Policy Assignment Rules

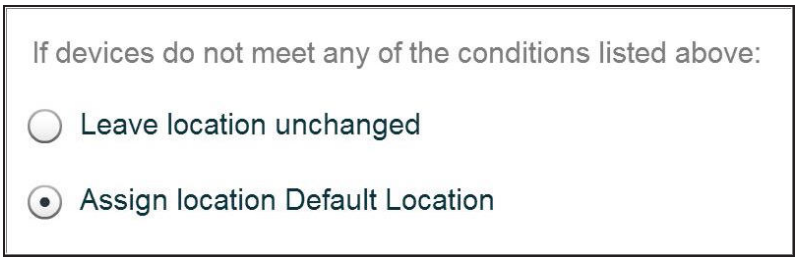
After you create policies, you can configure EvokeIT to assign the appropriate policies to new devices automatically when the devices connect to the server.

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 default policy for the device.



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 6-16*.
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 8-14*.
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.

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

1. Click the EvokeIT 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**.

About Power State Transition Rules

Power state transition rules tell EvokeIT which script to run when EvokeIT attempts to transition a computer to wake state (see *Upload a Script for a Power State Transition Rule on page 5-16*, *Assign a Custom Script to a Power State Transition Rule on page 5-17*, and *Signing Power State Transition Scripts with Digital Certificates on page 5-19*.

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

Create and Edit Power State Transition Rules

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

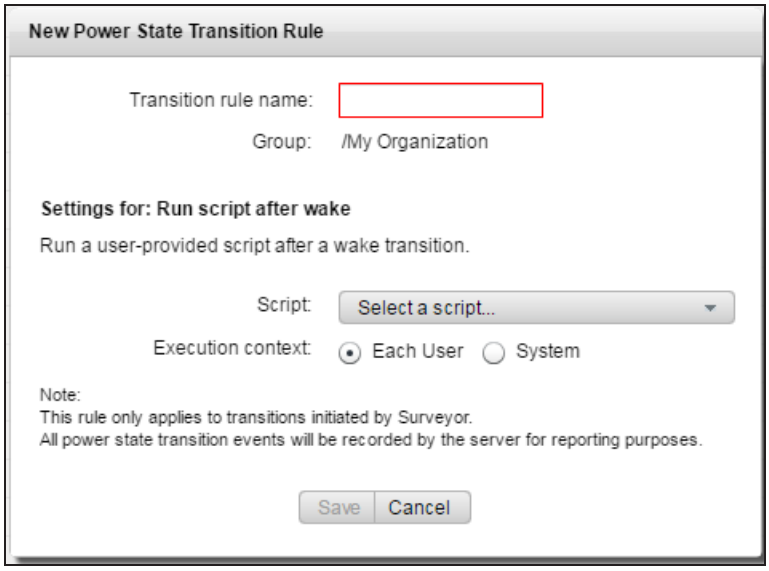
The following procedure creates or edits rules that then become available for assignment to policies (for details, see *Create and Edit Policies on page 5-7*).

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

1. On the EvokeIT menu, click **Power Transition Rules**.
2. Click **New Rule**, confirm 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. 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 EvokeIT server. For details on using power state transition scripts, see *Upload a Script for a Power State Transition Rule on page 5-16*, *Signing Power State Transition Scripts with Digital Certificates on page 5-19*



5. Click **Save**.

   To apply a power state transition rule to the appropriate devices, you will need to add the rule to a policy that is assigned to the devices.

   To configure policy settings, see *Create and Edit Policies on page 5-7*.

   To assign a policy to a device, see *Assign Policies to Devices on page 4-18*.

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.

EvokeIT supports power state transition scripts written in JavaScript or VBScript. You must create and edit power state transition scripts outside of EvokeIT, make sure they are digitally signed before you upload them, and then upload the scripts into EvokeIT. For details on signing scripts, see *Signing Power State Transition Scripts with Digital Certificates on page 5-19*.

To upload scripts:

1. On the EvokeIT 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 page*.

Assign a Custom Script to a Power State Transition Rule

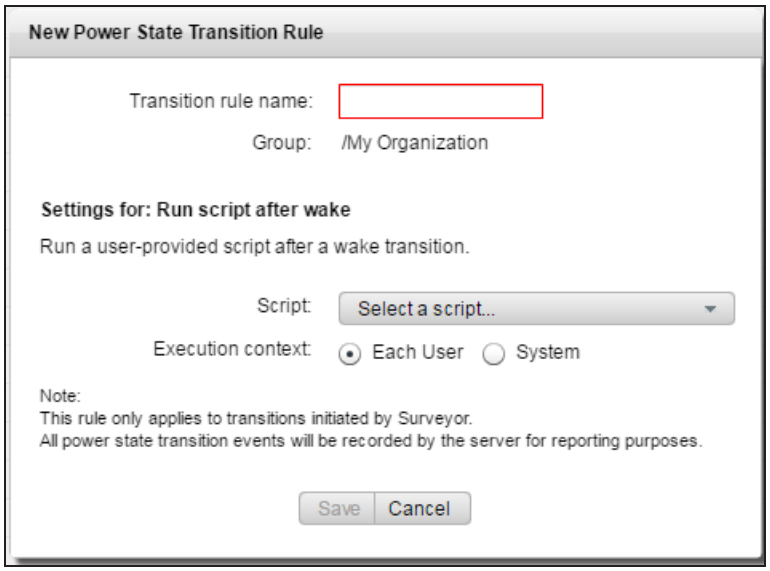
When you use a use a power state transition rule to prevent application errors during a power state change, you have the option to run a power state transition script. A power state transition script can include commands that cause the application to save its content in a temporary location, perform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

EvokeIT supports power state transition scripts written in JavaScript or VBScript. You must create and edit power state transition scripts outside of EvokeIT. Digital certificates for the scripts must be installed on both the client and the EvokeIT server (see *Signing Power State Transition Scripts with Digital Certificates on page 5-19* and *Managing Open Applications During Power State Changes on page 1*).

To edit scripts:

1. On the EvokeIT menu  , click **Power Transition Rules**.
2. Click **New Rule** on the **Power state transition rules in My Organization** tab.
3. Click **Run script after wake**, and then click **Next.**

4. Type a name for the rule.
5. Select a custom script (JavaScript or VBScript) that you uploaded to EvokeIT.



Note: A code-signing certificate for the script must be installed on both the client and the EvokeIT server. For details on using power state transition scripts, see *Upload a Script for a Power State Transition Rule on page 5-16*, *Signing Power State Transition Scripts with Digital Certificates on the next page*, and *Managing Open Applications During Power State Changes on page 1*.

6. Click **Save**.

To apply a power state transition rule to the appropriate devices, you will need to add the rule to a policy that is assigned to the devices.

To configure policy settings, see *Create and Edit Policies on page 5-7*. To assign a policy to a device, see *Assign Policies to Devices on page 4-18*.

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 EvokeIT 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 EvokeIT 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 EvokeIT 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 EvokeIT server, run the following from the command prompt:

```
makecert -n "CN=Local EvokeIT 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 EvokeIT 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
```

6

Waking Computers

Table 6-1 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 wake 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 6-4*

- 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 EvokeIT 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 9-2*.

Note: Part of minimizing the impact of centralized wake 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 EvokeIT Wake on WAN concepts yet, see *About Wake on WAN on page 6-8* 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 EvokeIT 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 EvokeIT scheduled tasks for power-state changes 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**.

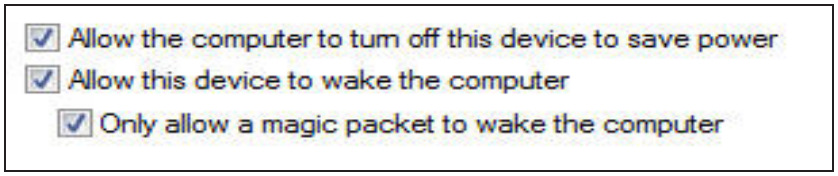
   b. Right-click the connection that the computer uses, and choose **Properties**.

   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 6-14* 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 **EvokeIT** 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 EvokeIT-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 page 1*.
- 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.

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

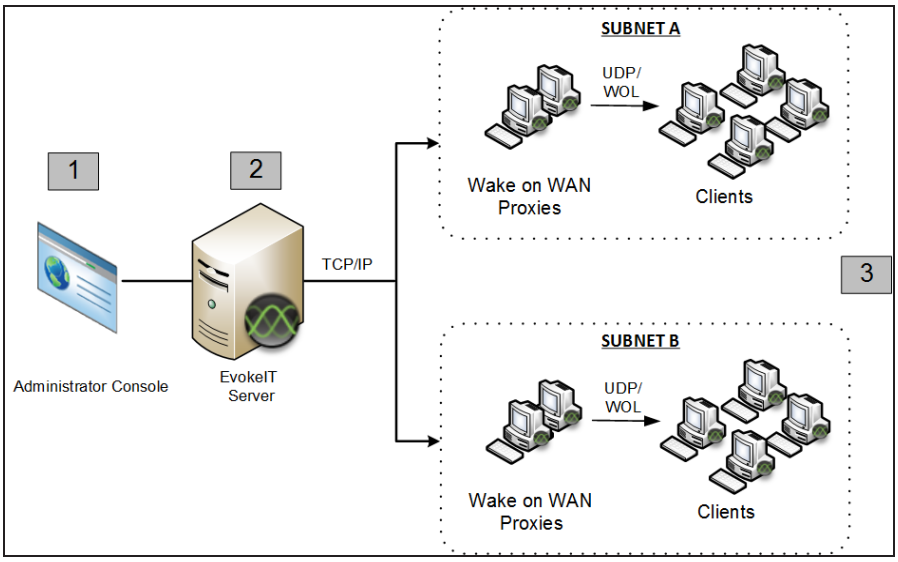
EvokeIT wakes computers in a network through Wake on WAN proxy computers. When Wake on WAN proxies are enabled, EvokeIT auto-elects Windows or Mac clients on each subnet to serve as primary and secondary Wake on WAN proxies. While other computers transition to a low power state during periods of inactivity, the proxy computers CPUs are kept awake. The primary proxy on each subnet works with the EvokeIT 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 EvokeIT. 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 scheduled policy 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 EvokeIT 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

EvokeIT 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 6-21* and *Configure Specific Networks for Wake on WAN on page 6-21*.

Each network that you specify for Wake on WAN can include multiple subnets with EvokeIT clients. EvokeIT 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 6-21* and *About Wake on WAN and Port-based Network Access Control on page 6-24*.

Note: Switches for the networks that you specify as additional broadcast networks must be configured to receive subnet-directed broadcasts from the EvokeIT 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 EvokeIT server.

To enable Wake on WAN:

- Set Wake on WAN to be enabled in EvokeIT server, and also enable policy wake settings. For details, see *Enable Policy Wake on WAN Settings on page 6-16*.
- Confirm that Wake on LAN is enabled on client computers. For information, see *Configure Client Computers for Wake on LAN on page 6-4*.

Wake on WAN versus scheduled wake from sleep

If your wake 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 6-30*.

How EvokeIT Determines Subnet Boundaries

EvokeIT 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.

How EvokeIT Elects Wake on WAN Proxies

EvokeIT 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 EvokeIT 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 **Default**.

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, EvokeIT 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 EvokeIT to use its built-in criteria to select new proxies as needed.

Determine Wake on LAN Support for Computers

To use EvokeIT 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 scheduled policy 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: EvokeIT 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 6-18*.

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 6-6*

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**.

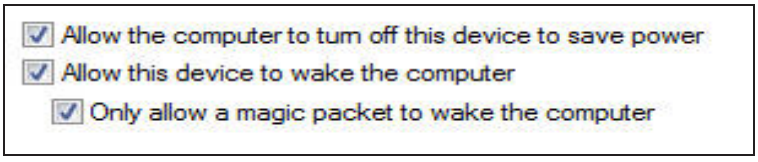
   b. Right-click the connection that the computer uses, and choose **Properties**.

   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 EvokeIT

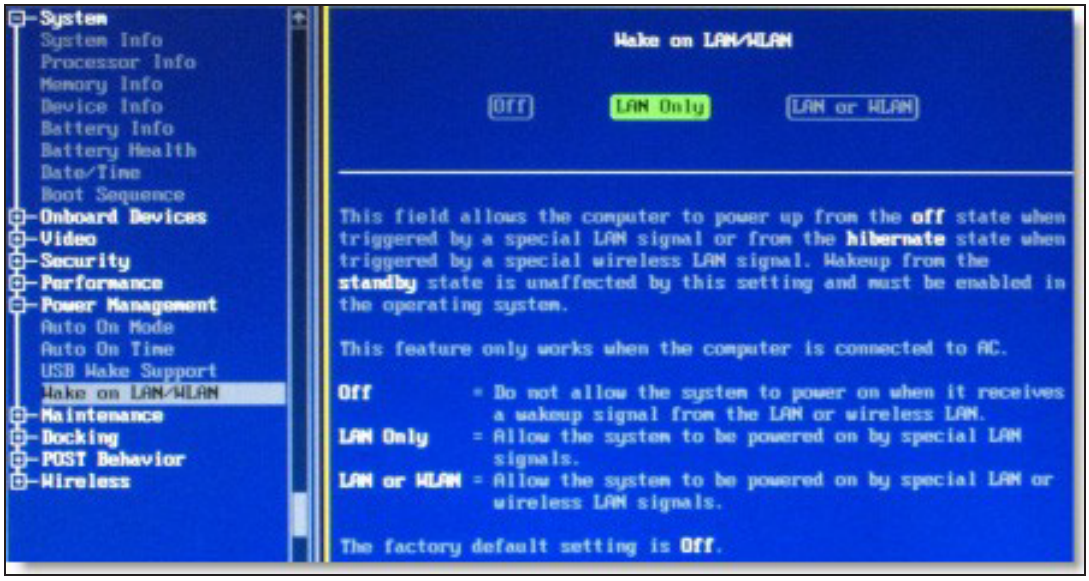
wake management policies. Be sure to check these settings any time you update the NIC driver.

• 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.

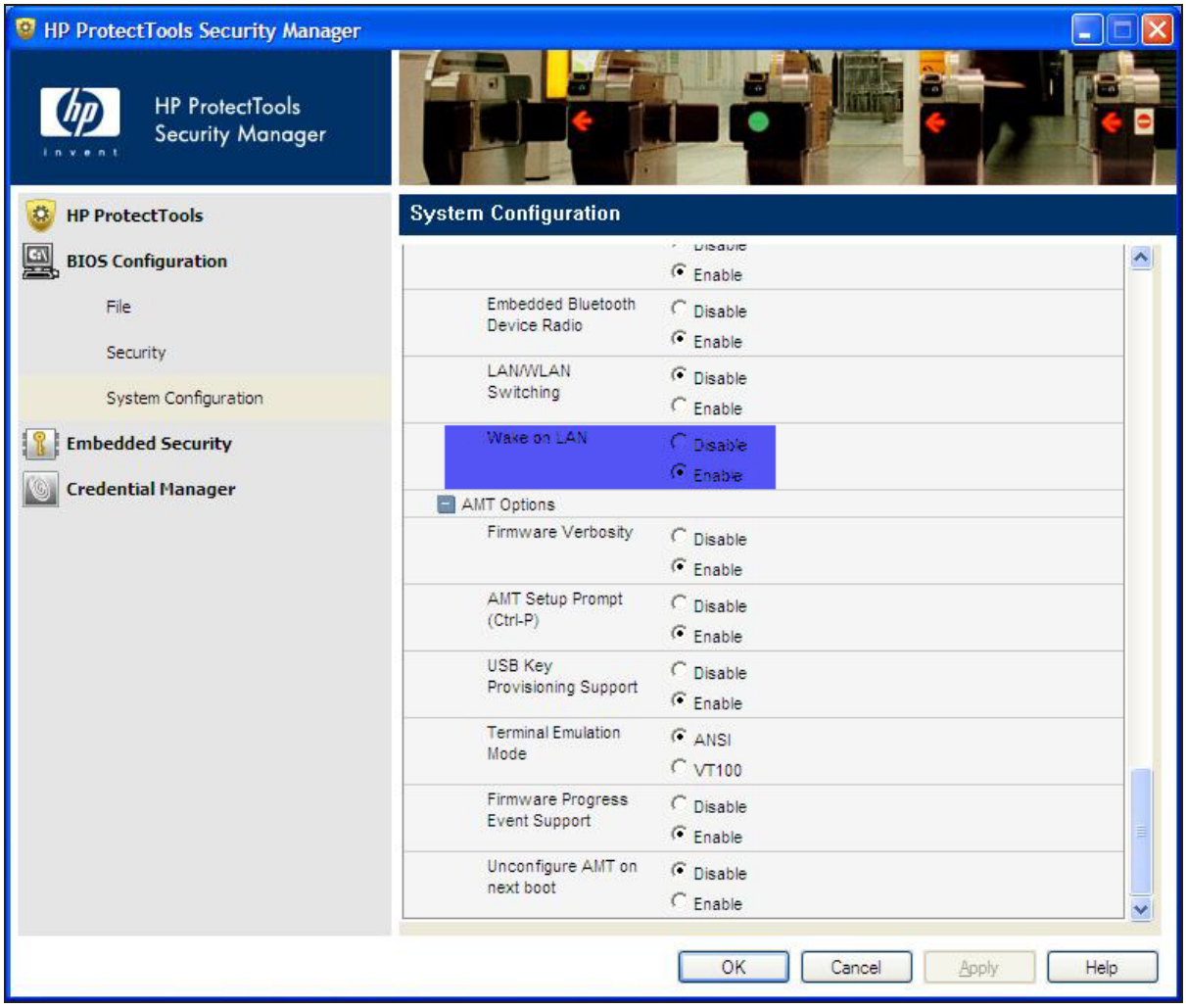
Manually Configure the BIOS for Wake on LAN (Windows Only)

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 EvokeIT 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 EvokeIT 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 EvokeIT 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 EvokeIT 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 policy 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 EvokeIT clients to wake through a Wake on LAN magic packet.

All of these settings are enabled by default, to enable the EvokeIT Wake on WAN feature. For information, see *About Wake on WAN on page 6-8*. 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 EvokeIT 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 EvokeIT 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 EvokeIT Elects Wake on WAN Proxies on page 6-11*.

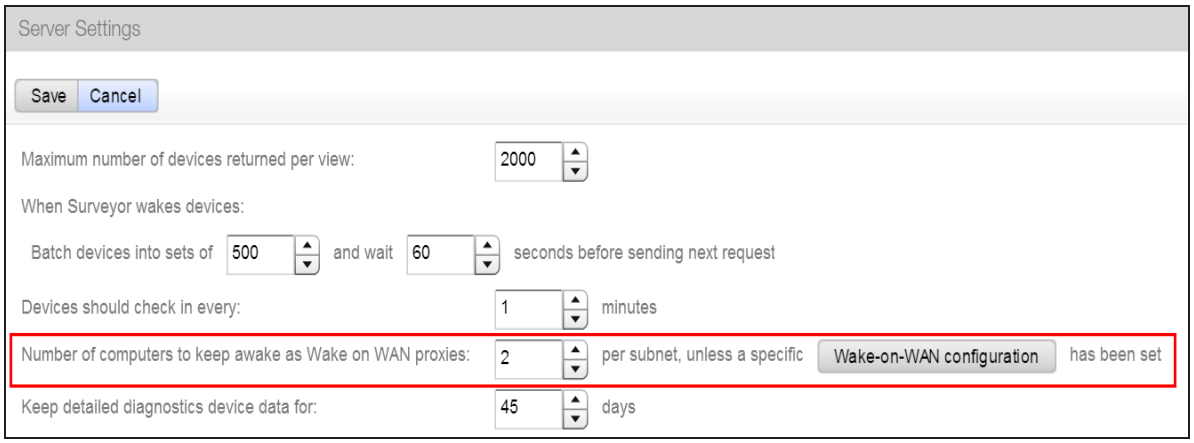
2. Select one or more of the computers in the device list, and then from the **Item Actions** menu, click **Edit Device Properties**.
3. In the Edit Device Properties dialog box, select the **Wake on WAN proxy preference** check box, and then select the setting that you want for the selected computers.
   - **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, EvokeIT 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 6-8*.

1. In the EvokeIT 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 increase the number of proxies per broadcast domain, save the new settings. You do not need to complete the remaining steps. EvokeIT 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 reduce 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.

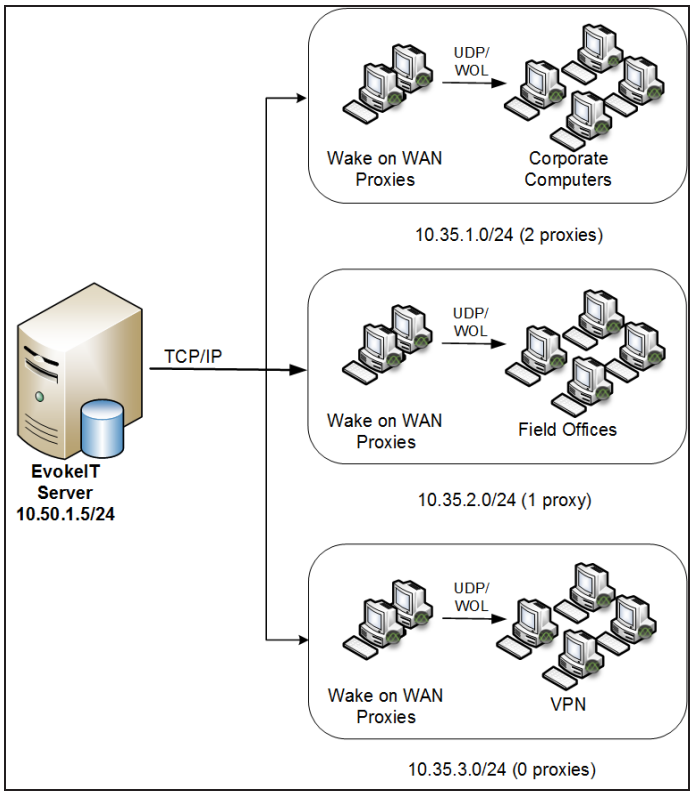
10. When all of the devices you selected are cleared of proxy status, you can then set the **Preferred Wake on WAN proxy** setting on any of them to **Preferred** or **Default**, so that they can be returned to the pool of devices that are available for proxy selection.

For information about preferred Wake on WAN proxy settings, see *Set a Client to be a Preferred Wake on WAN Proxy on page 6-18*.

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*.

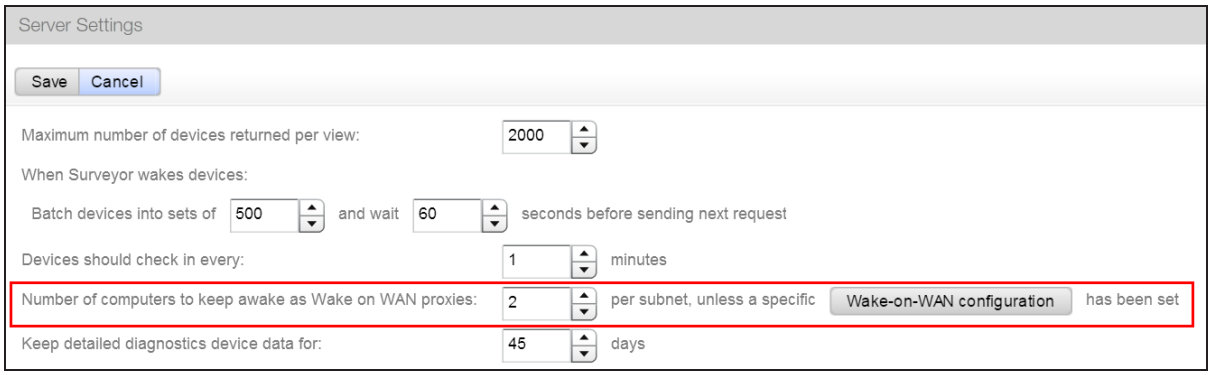
Configure Specific Networks for Wake on WAN

EvokeIT 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 EvokeIT maintains proxies, and also the number of proxies per subnet.

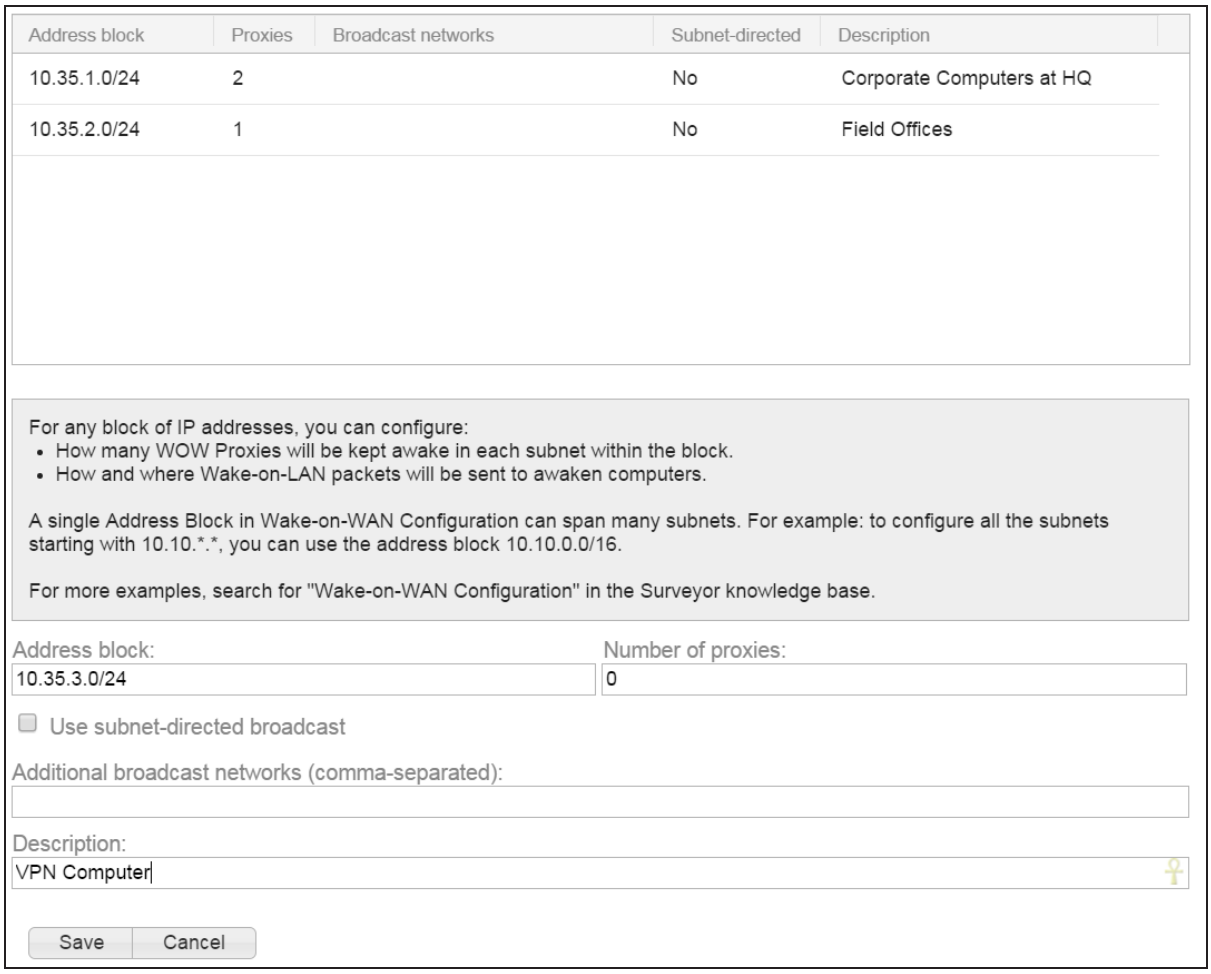


Two proxies per broadcast domain is the recommended minimum. This ensures that a secondary proxy can take over if the primary proxy becomes unavailable. However, for a network where you don't want any computers to wake from Off or Sleep, set the proxy count for that network address to 0 proxies. If your 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 EvokeIT 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.



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**.

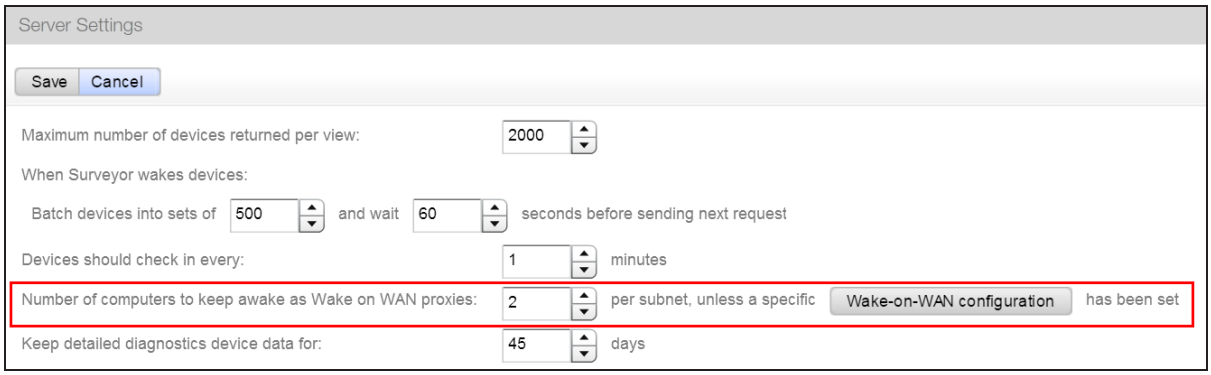
Override the Default Number of Wake on WAN Proxies on a Network

EvokeIT 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 EvokeIT maintains for each subnet.

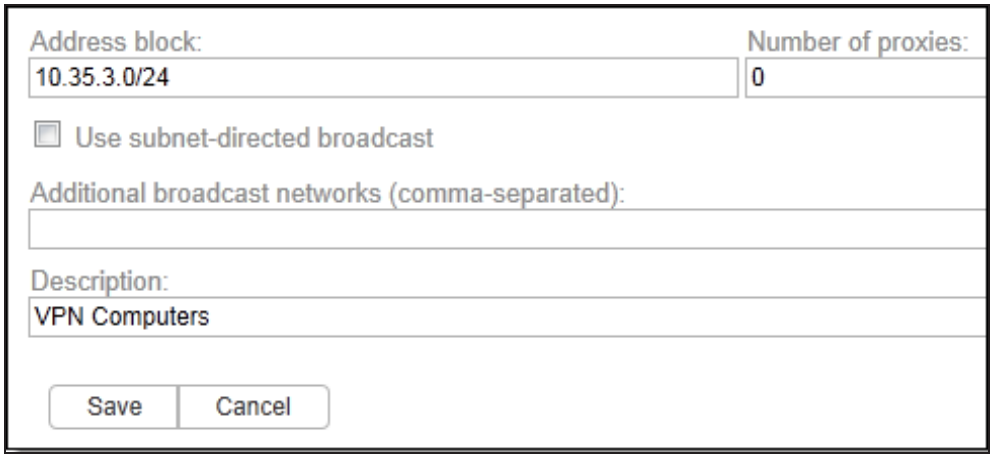
You can select as many proxies as you want per subnet (or even specify zero proxies for subnets on which you don't ever want to wake computers). However, best practice is to designate at least two.

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 EvokeIT 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.

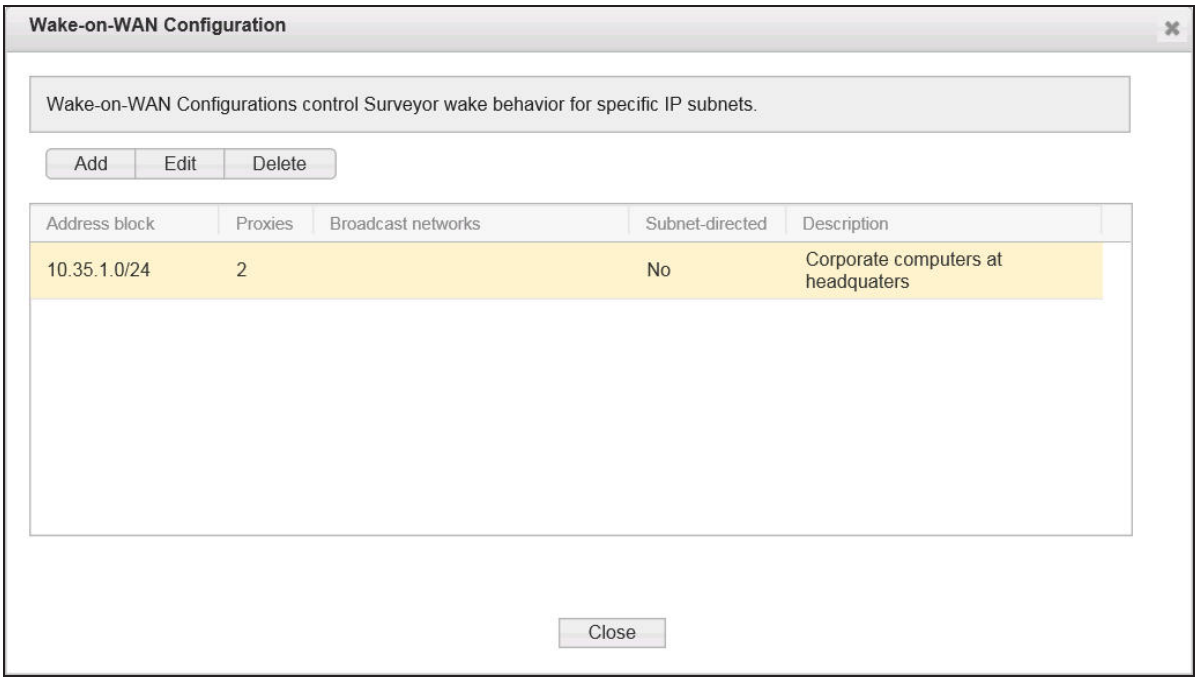
Where PNAC is used, computers in Sleep mode are removed from an authorized network and placed into another, unauthorized network by the network switch. By default, when the EvokeIT server is asked to wake sleeping machines using Wake on WAN, the EvokeIT server will try to wake computers by sending Wake on LAN (WOL) packets to Wake on WAN proxy computer in the last authorized network from which the proxy computer connected to EvokeIT. 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 EvokeIT 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.

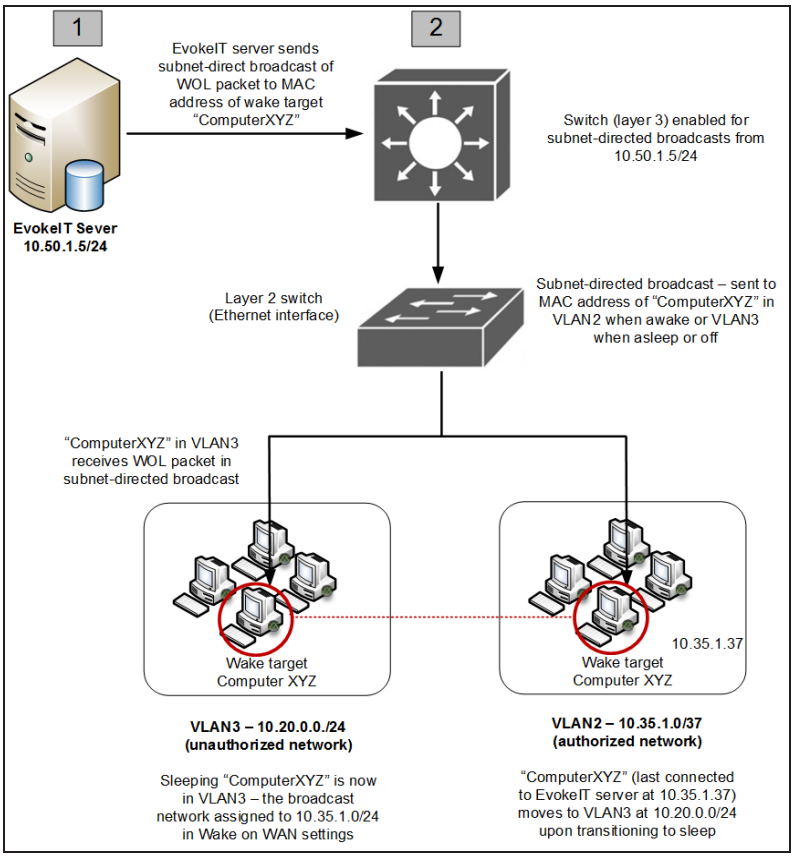
In addition to sending wake packets on the subnet where each device was last detected, EvokeIT will send wake packets to each network in the list of additional broadcast networks. Additional broadcast networks can be entered in either IP address and netmask pairs (such as 192.168.10.0 255.255.255.0) or using CIDR notation (such as 192.168.10.0/24).

Subnet-directed Broadcasts from EvokeIT

EvokeIT 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 EvokeIT 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 EvokeIT 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 scheduled policy or on demand by administrator).
3. EvokeIT 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 EvokeIT clients. Network-specific configurations in Wake on WAN give you more control over the subnets that should receive Wake on LAN packets from EvokeIT server. You can also specify the number of proxies for each subnet.

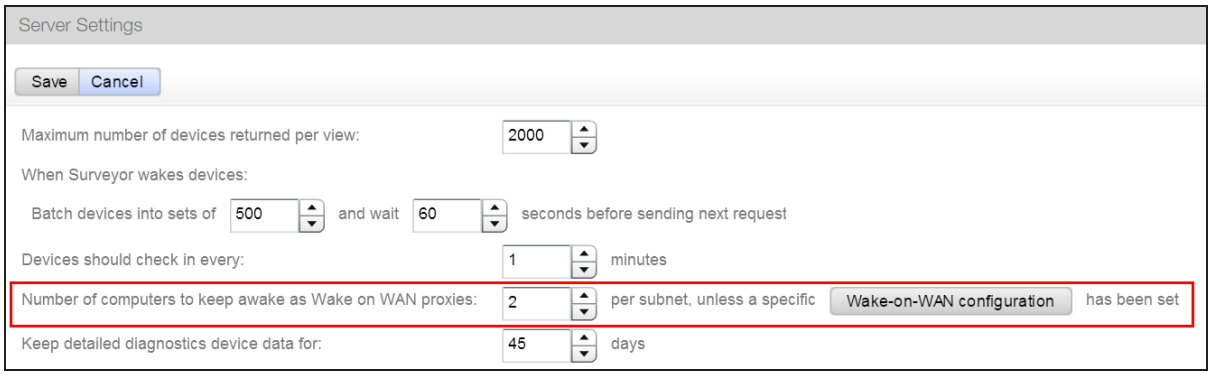
Note: By default, Wake on WAN proxies are not enabled when you first start EvokeIT. It is recommended that you set the proxy number to 2 per subnet.

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, EvokeIT 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 6-24* 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 EvokeIT server. See your switch manufacturer documentation for details.

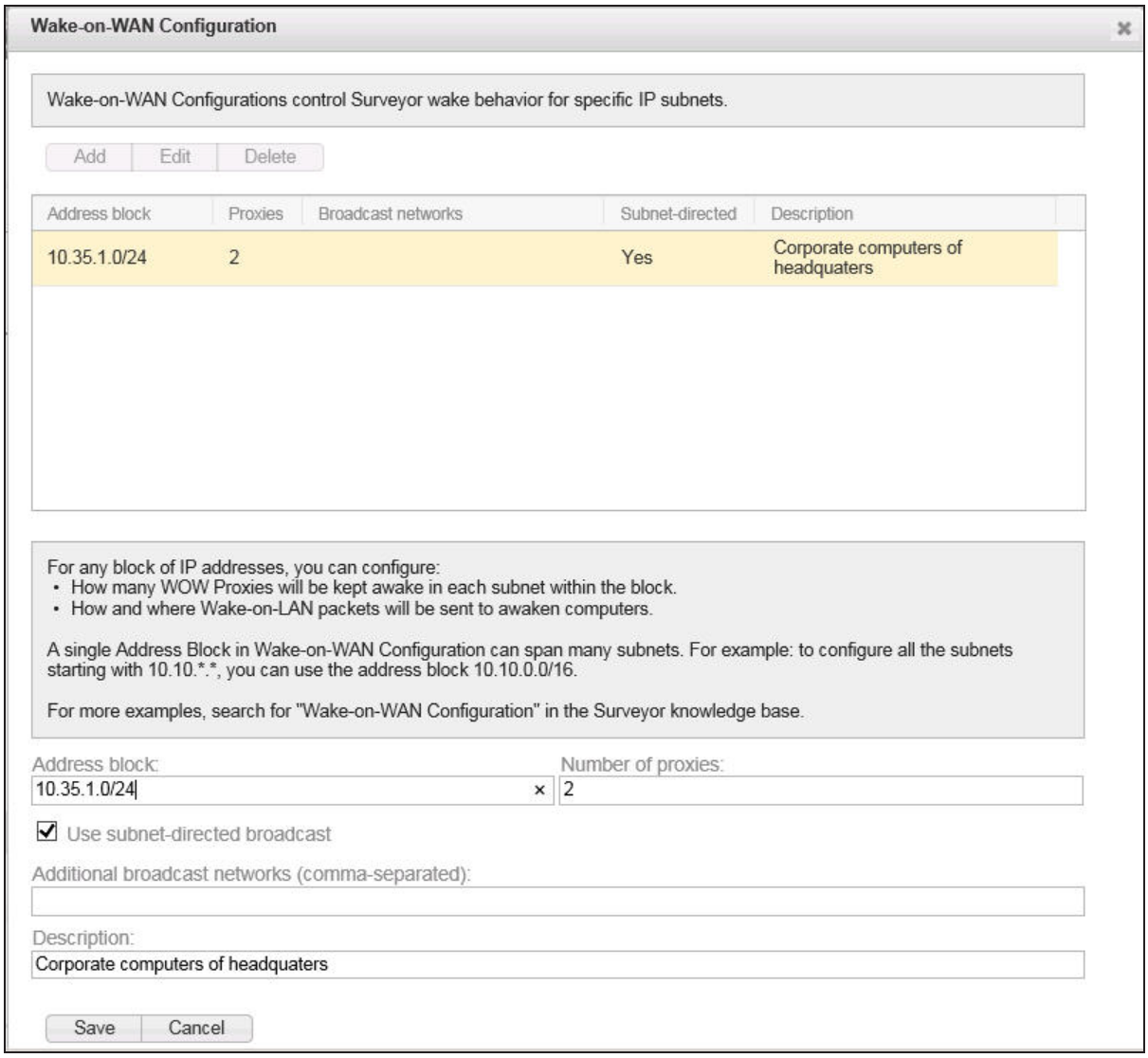
1. In the EvokeIT Administrator console, on the Configure menu, click **System Settings**, and then click **Wake-on-WAN Configuration**.



2. In the **Wake-on-WAN Configuration** dialog box, 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.



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 6-8*.

1. In the Administrator console, on the EvokeIT 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 EvokeIT 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 policy. For more information about creating policies, see *Overview of Policies and Wake Management Settings on page 5-2*

7

Viewing Reports

Table 7-1 In this Chapter

Topics
Overview - Reports
Dashboard and Analytics Reports
About Data Summarization

Overview - Reports

EvokeIT reports provide views of current and summarized information about wake jobs, device status (by time, by policy, etc) and license status. This section describes the reports that are available in EvokeIT and the summarization process that is required to make report data available.

Note: EvokeIT 1.1.101 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 EvokeIT:

Report	Description
Dashboard	**Dashboard reports** are role-based dashboards that provide information on device status, power state activity, policy assignment, Agent versions, and installation and licensing. For Dashboard reports, click **Dashboard** on the menu . For details on Dashboard reports, see *Dashboard and Analytics Reports on the next page* and *Dashboard and Analytics Reports on the next page*.
Analytics	**Analytics reports** allow you to generate reports on device status, wake job status, licensing information, and other categories of interest. Analytics also allow you to dive down into the data, giving you detailed information. For Analytics reports, click **Analytics** on the EvokeIT menu . For details on Analytics reports, see *Dashboard and Analytics Reports on the next page*and *Dashboard and Analytics Reports on the next page*.
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 EvokeIT. For event reporting, click **Device Events** under Devices on the menu . For details on how to use event data for troubleshooting and optimization, see *Chapter 8: Viewing Diagnostic Information from Event Logs on page 8-1* and *Display Event Data in the Administrator Console on page 8-12*.

Data Summarization

EvokeIT provides summarized views of data in Dashboards and Analytics reports. By default, the data is summarized on an hourly basis anddaily depending on the type of report. For details, see *About Data Summarization on page 7-6*.

Dashboard and Analytics Reports

Dashboard and Analytics reports in EvokeIT provide you with views of device data from many different angles. EvokeIT'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 7-6*.

On the EvokeIT menu, when you click Dashboard, the following reports are available to you.

Status Dashboard

During deployment and ongoing operations, this view helps you to track progress device check-in and wake job status. IT can also flag devices that are underutilized and therefore possible candidates for elimination, consolidation, or virtualization. Status dashboard also gives you information on wake job status.

- **Computers by Agent Version** - Shows the versions of Verdiem agents deployed and counts of computers by version.
- **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 EvokeIT agents, including date of last summarization, actively connecting computers, computers with active policies, computers with unenforced policies, 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 when you click on data points in the report.

On the EvokeIT menu  , when you click Analytics, the following reports are available to you:

Report	Description
Operations - Computers by Agent Version	Shows the versions of Verdiem EvokeIT agents deployed and counts of computers by version.
Operations - Computers by Model	Model and manufacturer of computers reporting to Verdiem EvokeIT.
Operations - Computers by Operating System	Current Operating System of computers reporting to EvokeIT.
Operations - Device Count by Group	Shows the number of devices in each 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 EvokeIT.
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.

View and Print Dashboard Reports

1. On the EvokeIT 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 the next page*.

2. Click **Status** to view each type of dashboard.

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 EvokeIT 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 the next page*.

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 7-7*.

4. To further filter results, select 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.

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 EvokeIT dashboard and analytics reports is aggregated, summarized data.

When you install EvokeIT, 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\EvokeIT\Tools:

- **EvokeIT 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.
- **EvokeIT 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 EvokeIT data.
- **EvokeIT Resummarize All Data** - Completely resummarizes all available EvokeIT 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, **EvokeIT 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 EvokeIT 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 EvokeIT should usually be sufficient to meet your data needs for EvokeIT 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 EvokeIT 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\EvokeIT\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 EvokeIT reports:

- Device group and policy assignments
- Device family assignments

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.

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 EvokeIT 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 and policies**: Number of 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 EvokeIT 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\EvokeIT\Tools** folder on the EvokeIT 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\EvokeIT\Logs**.

Resummarize Data Incrementally Using a Windows Task

This topic describes the Windows tasks available to EvokeIT that handle resummarizing data incrementally.

When you install EvokeIT, the following data summarization tasks related to are automatically configured and scheduled to run in the Windows Task Scheduler:

- **EvokeIT 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\EvokeIT\Tools\AdminCommand.exe" start_summarization 1

- **EvokeIT 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 EvokeIT data.

  The corresponding command line for this task is:

  ```
  AdminCommand.exe start_summarization 30 force
  ```

  The corresponding action is:

  "C:\Program Files (x86)\Verdiem\EvokeIT\Tools\AdminCommand.exe" start_summarization 30 force

- **EvokeIT resummarize all data** -Summarizes all data incrementally at 11:50 p.m. After this task is triggered, the task runs to summarize all EvokeIT 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\EvokeIT\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 EvokeIT 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\EvokeIT\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\EvokeIT\Tools\ on same computer as the EvokeIT 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\EvokeIT\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\EvokeIT\Logs**.

8

Viewing Diagnostic Information from Event Logs

Table 8-1 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 and change power states.
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 (EvokeIT server, a third party, or an unknown trigger). Also includes display-only logs for power-state changes.
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

Category	Description
	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 wake management service; 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 EvokeIT 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\EvokeIT 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\EvokeIT Agent\Logs

Content links

Admin Actions Event Category

Includes all manual transitions to low-power states that an administrator sets on devices.

Table 8-2 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

Policy Actions Category

This category includes events that occur through power state transition manager (PSTM) rules, and other events that occur through policy schedules and change power states.

Other events recorded in this category include initial power scheme value when the client service is started, when scheme is set by the user (because the scheme is created to allow the user to override it), and so on.

Table 8-3 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

Scheduled Actions Category

Any power-state change that occurs according to the schedule set in the policy assigned to the client.

Table 8-4 Scheduled Actions Category

Event Types	Description	Normal event?
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 8-5 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

Table 8-5 Service Events Category (continued)

Event Types	Description	Normal event?
Service Stopped	The client service was stopped. All states should be considered unknown unless the subtype is Shutdown (CPU off).	no
User Activity Collection Started	Indicates start of data collection of user actions. Power states for all users go unknown.	yes
User Activity Collection Stopped	Indicates stop of data collection for user actions; power states for all users go unknown.	no
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 (EvokeIT server, a third party, or an unknown trigger). Also includes display-only logs for power-state changes.

Table 8-6 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	EvokeIT received notification from Windows that the CPU will turn off soon (user has received notification and allowed the shut down).	yes
Sleep State	EvokeIT 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	EvokeIT 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

Table 8-6 State Changes Category (continued)

Event Types	Description	Normal event?
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
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 8-7 User Actions Category

Event Types	Description	Normal event?
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 8-8 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

Changing wake settings on mouse, keyboard (including whether it's a USB device); or loading, parsing, or saving .config files.

Table 8-9 Configuration Errors Category

Event Types	Description	Normal event?
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 EvokeIT server config file.	no
Server Config ParseFailure	Failed to parse the EvokeIT server config file.	no
Server Config Save Failure	Failed to save the EvokeIT server config file.	no

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 8-10 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

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 wake management service; performance counter for the idle timer missing or failed; errors that occur while querying the user or display state.

Table 8-11 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
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

Table 8-11 Service Errors Category (continued)

Event Types	Description	Normal event?
Performance Counter Missing	A performance counter that is used with the EvokeIT idle timer is missing.	no
Performance Counter Failure	A performance counter that is used with the EvokeIT 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 8-12 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
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 8: Viewing Diagnostic Information from Event Logs on page 8-1* in the EvokeIT *Administrator Guide*.

Applies to

Product

Display Event Data in the Administrator Console

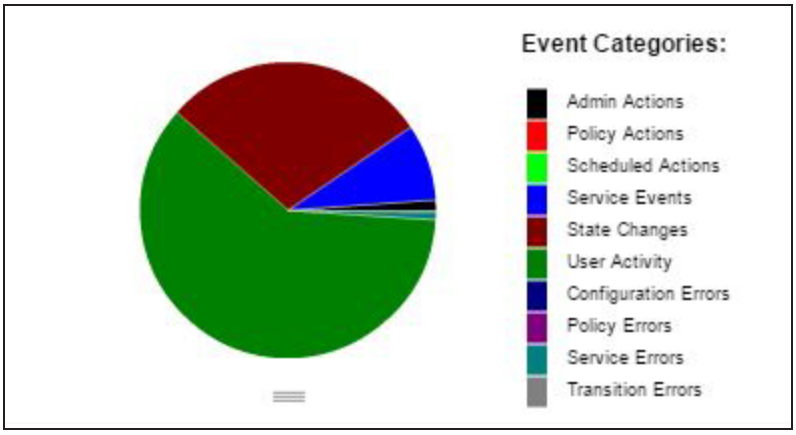
You can view client agent activity in a summary report, or view a list of devices by event or events by event type.

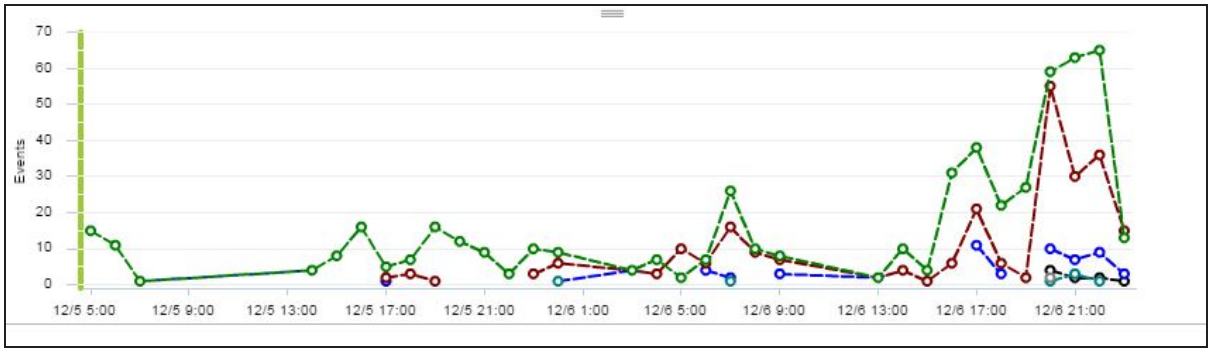
In addition, you can use search filters to fine-tune the data. For example, view events only in a particular administration group, events to which a particular policy is assigned, and so on.

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 EvokeIT 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. • 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. 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.
- EvokeIT 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 4-13*.

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, EvokeIT 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 EvokeIT.

To access these settings in an individual policy, on the EvokeIT menu, click **Policy Schedules**, 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 EvokeIT 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\EvokeIT\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, ITMWebService.*yyyy.mm.dd*.log. The most current log takes the base file name.

Server component	Path to log files
ITM Web Service	`C:\Program Files\Verdiem\EvokeIT\Logs\ ITM WebService.log`
Enterprise Wake Management Service	`C:\Program Files\Verdiem\EvokeIT\Logs\PowerManagementProcessor.log`
Administrator web service	`C:\Program Files\Verdiem\EvokeIT\Logs\AdminWebService.log`
Data Summarization	`C:\Program Files\Verdiem\EvokeIT\logs\Summarization.log`
Wake for Remote Access	`C:\Program Files\Verdiem\EvokeIT\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\EvokeIT\activemq-5.13.4\bin\win32\wrapper.log`
IIS	`C:\inetpubs\logs\logfiles`
Analytics and Dashboard	`C:\Program Files\Verdiem\EvokeIT\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 EvokeIT data logged in the IIS log file to the last 30 days.

Reduce the Amount of Data Being Logged

In EvokeIT 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

The EvokeITdownload installation package includes the script **DeleteIISLogs.ren** (in the **..\EvokeIT_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 EvokeIT client computers, log files are saved in the following locations:

EvokeIT Client Logs: C:\Program Files\Verdiem\EvokeIT 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\EvokeIT\Logs**

The files are named PwrMgrUserSession.log.n, where n is a positive integer.

Macintosh Clients:

~\library\logs\verdiem

The files are named surveyorsession.log.n, where n is a positive integer.

Macintosh clients:

~\library\logs\verdiem

9

Using Wake for Remote Access

Table 9-1 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

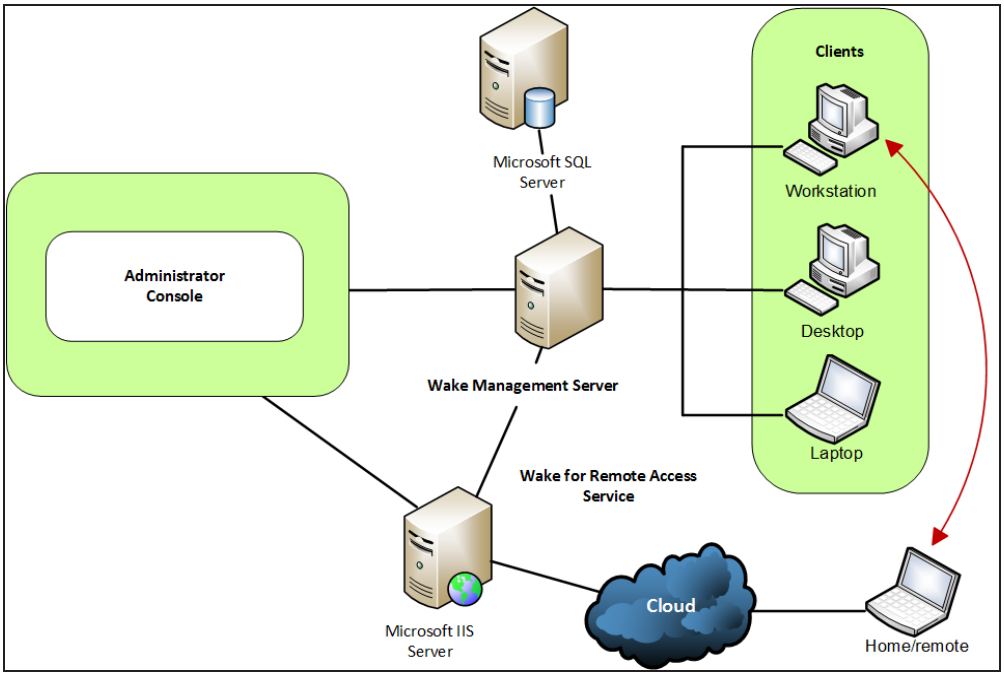
This section contains information about customizing Wake for Remote Access. You can do this both on the server side, modifying IIS application settings, and on the client side, changing the styles and layout for the browser pages that end users visit to wake their computers.

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 EvokeIT system, it does this through the unique EvokeIT 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 EvokeIT wake 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 EvokeIT 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 EvokeIT Knowledge Base.

  Note: If Windows Firewall is enabled on the EvokeIT 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 10-4*.

- (Optionally) In your web browser, enter the URL for the local web site on the computer where you installed the EvokeIT server, such as **http://hostname/WRA/** where *hostname* = EvokeIT wake 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 EvokeIT.

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 EvokeIT Administration Guide.

For Technical Support contact information or to log on to the portal, visit the Support page on aptean.com.

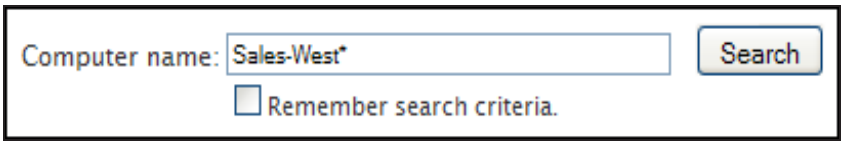
Application Settings that You Can Customize in IIS Manager

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 9-12*.

Note: Search results return only computers on which a licensed EvokeIT client agent is installed. (Unlicensed agents are not returned.)

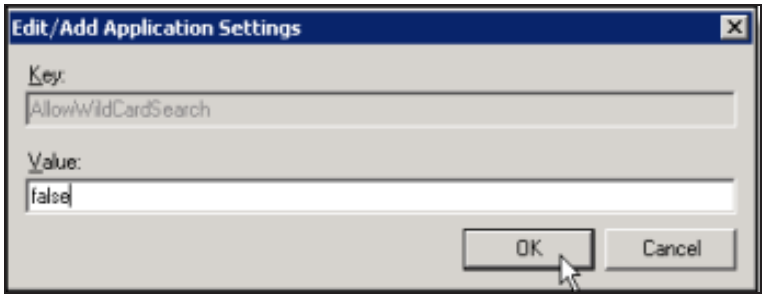
How to Customize Application Settings in IIS Manager

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.

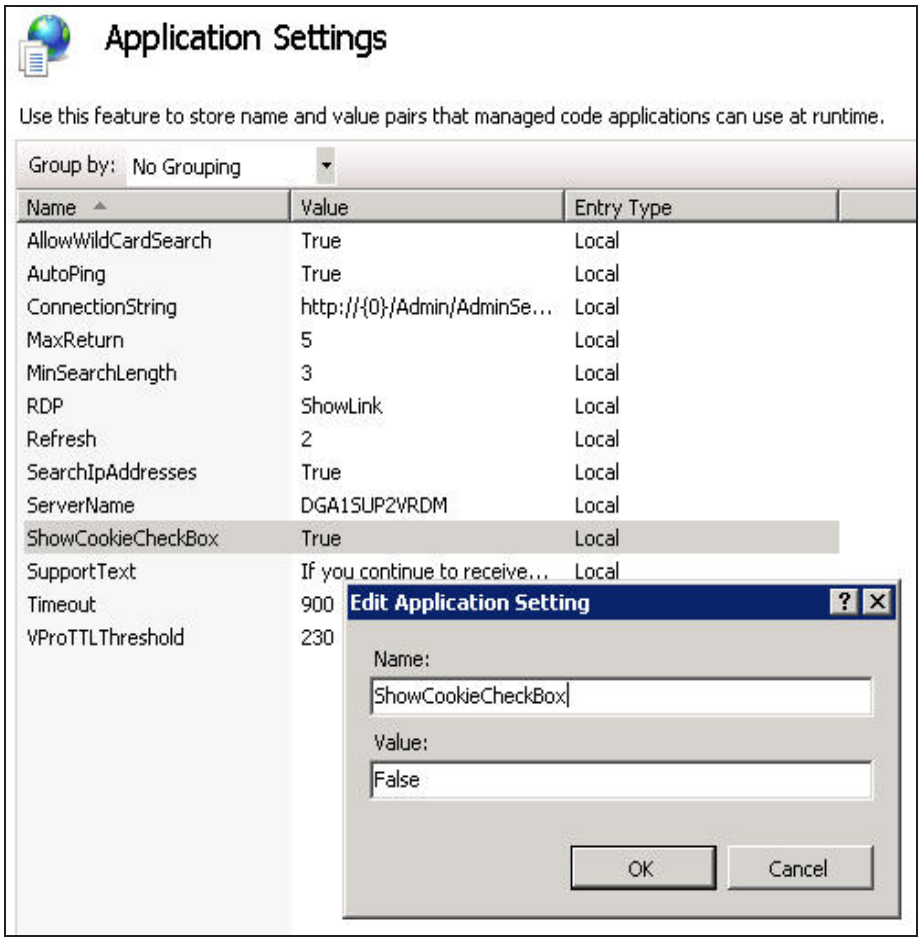
   For descriptions, see *Wake for Remote Access (WRA) Application Settings and Descriptions on page 9-10*.



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 9-10*.


Application Settings
Use this feature to store name and value pairs that managed code applications can use at runtime.
Group by: No Grouping
Name
Value
Entry Type
AllowWildCardSearch True Local
AutoPing True Local
ConnectionString http://{0}/Admin/AdminSe... Local
MaxReturn 5 Local
MinSearchLength 3 Local
RDP ShowLink Local
Refresh 2 Local
SearchIpAddresses True Local
ServerName DGA1SUP2VRDM Local
ShowCookieCheckBox True Local
SupportText If you continue to receive... Local
Timeout 900
VProTTLThreshold 230
Edit Application Setting
Name:
ShowCookieCheckBox
Value:
False
OK
Cancel

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. 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 9-13*.
AutoPing	True	Pings the computer the user wants to wake before sending the wake request, to determine whether the computer is already awake. 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. This excludes the page load time, so the actual result can take a few seconds longer than the value specified.
ServerName	Your EvokeIT server name	A text string that displays the name of the wake 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. 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 EvokeIT server when a user searches for a computer. This can occur, for example, if the server is offline, or the server name setting is not correct in the IIS Manager.

Setting Name	Default Value	Description
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 EvokeIT 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\EvokeIT\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.

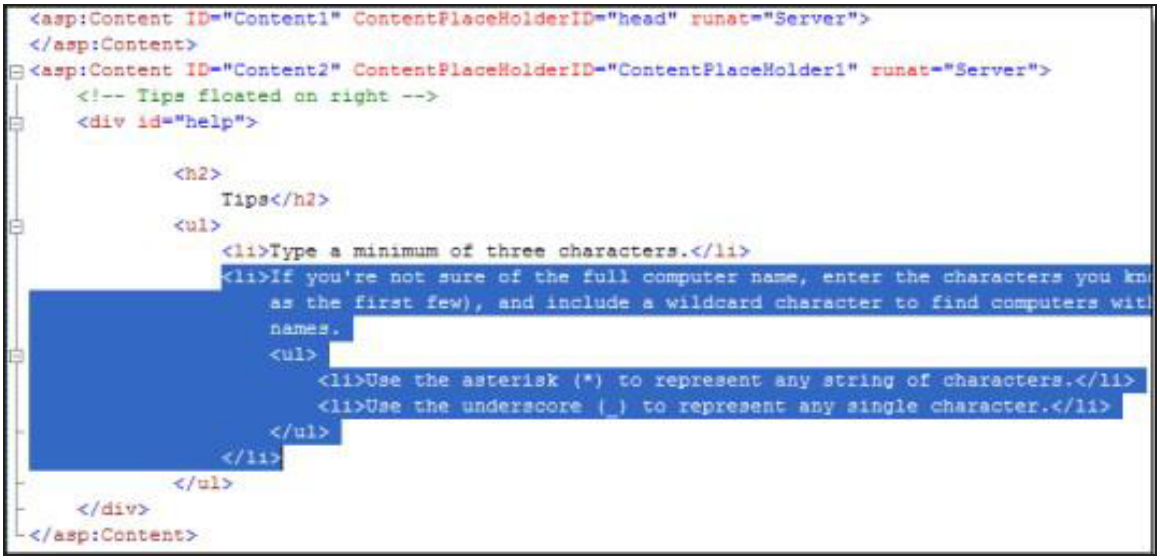
Caution: Before you edit the .aspx, .master, and .css files, create backup copies. Edit them at your own risk. Verdiem Technical Support cannot troubleshoot errors you receive after customizing these pages.

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\EvokeIT\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\EvokeIT\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\EvokeIT\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.

10

Troubleshooting

Table 10-1 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 EvokeIT 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 EvokeIT 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 10-5*.

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
```

Configure Windows Firewall to Allow Web Components to Access the Server

If you use EvokeIT 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 EvokeIT. 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 wake 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.

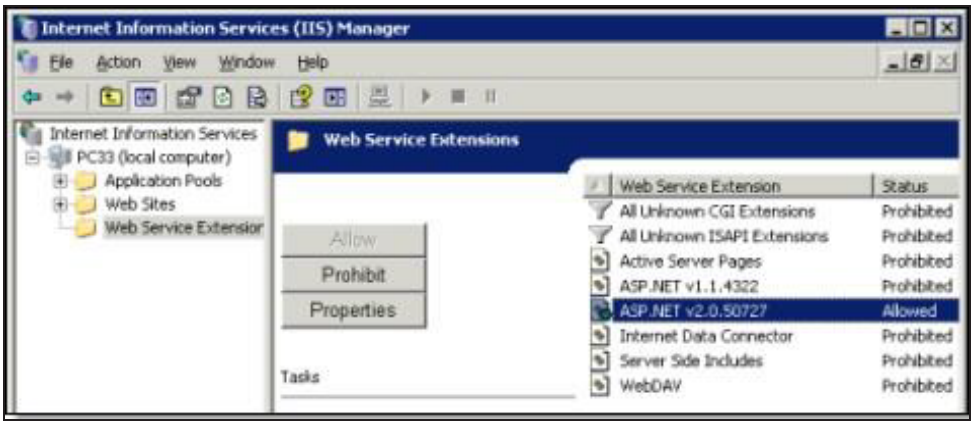
For additional information, refer to the Microsoft TechNet topic Add a Port to the Firewall Rules List.

Configure the web server to allow ASP.NET v.2.0.50727 applications

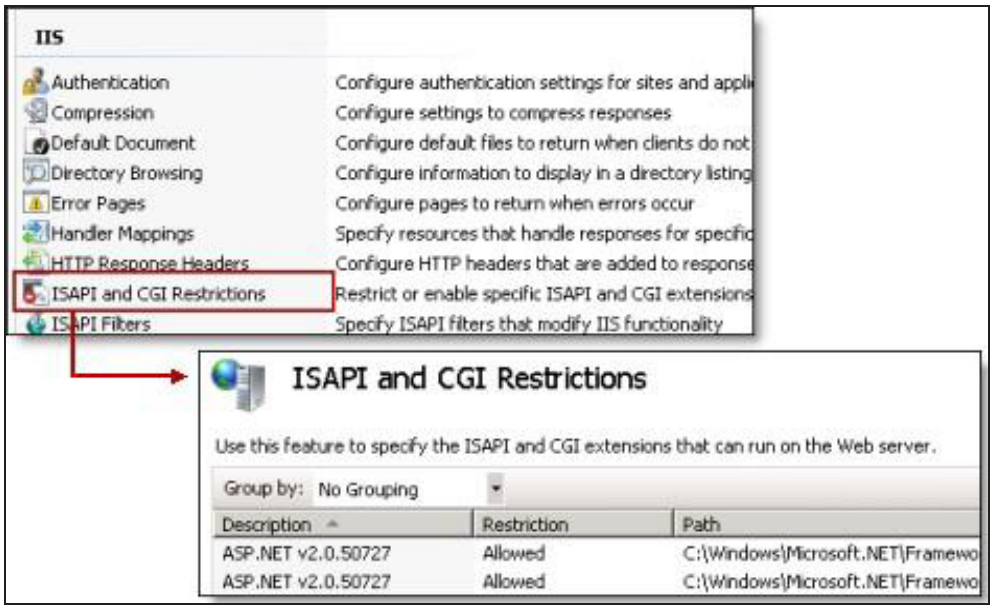
The correct version of ASP.NET must be allowed on any computer that hosts the EvokeIT server or Wake for Remote Access.

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 9-10* 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 EvokeIT.

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 EvokeIT, 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\EvokeIT\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 wake 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 wake management server, but the current user does not have the required permissions on the wake 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\EvokeIT\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**".