EVOKEIT

Installation 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

Overview of EvokeIT

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

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 to endpoints 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 transition** (PC and Mac only) that specify the amount of time of user inactivity before a device transitions to a lower power state. Each power transition can have a unique schedule.

- **Wake up settings** for PC and Mac clients.
- **Logging and data collection settings** for PC and Mac clients.

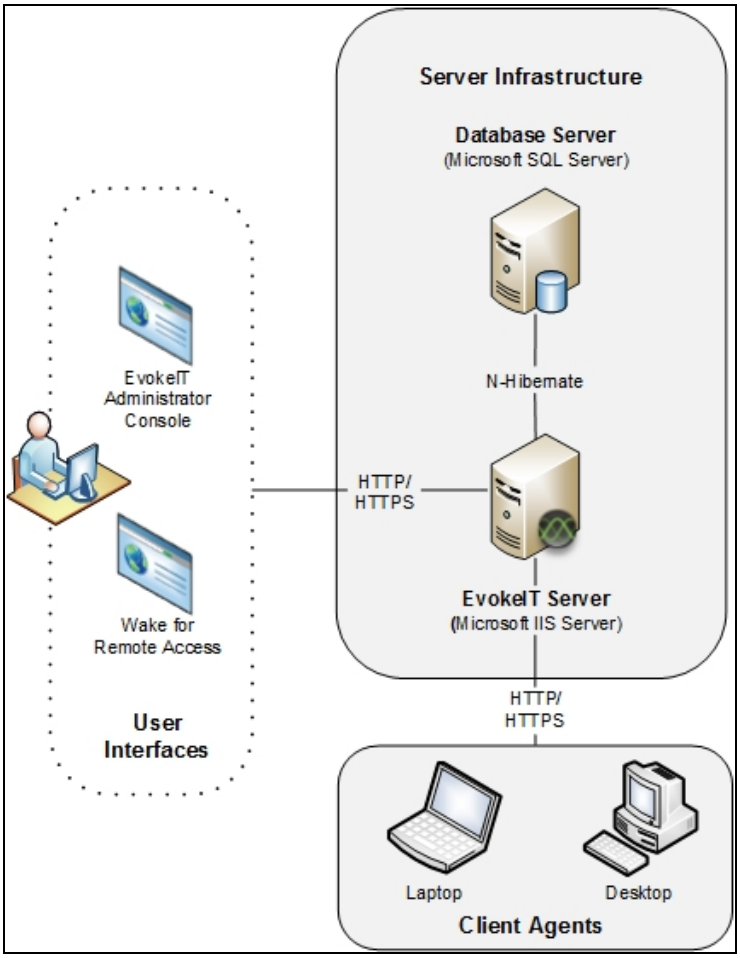
EvokeIT assigns policies manually or through assignment rules that you create. Each device can have only one policy assigned to it, but each policy can contain multiple power level changes, each with its own schedule.

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 wake management" in the *EvokeIT Administrator Guide*.

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.
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 EvokeITserver.

2

Preparing for the EvokeIT Server Installation

Table 2-1 In this Chapter

Topics
System Requirements
Server Installation Options and Prerequisite Software
Prepare the Environment for the Server Installation
Setting up the Database Environment

System Requirements

This section provides steps to take to get your system ready for server installation. A typical installation includes the EvokeIT server and database, Wake for Remote Access.

Review the following prerequisites and system requirements before beginning installation.

This section lists supported hardware, operating system, database, and software required for installing and running the EvokeIT system. Latest patches are assumed throughout.

Note: For a single-server installation, supported versions of the operating system, IIS, and SQL Server software should be installed on the dedicated EvokeIT Server.

With sufficient hardware, a single wake management server can manage up to 70,000 devices.

System Size and Scalability

Best practice is to dedicate the wake management server to EvokeIT and not to any additional critical services.

EvokeIT Wake Management Server Components

The following table lists the supported system components for the EvokeIT wake management service, administrator console, and queue service.

Required components that are not already installed on the computer will be installed automatically as part of the server installation.

Operating system	Microsoft Windows Server 2016 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2008 R2 **Note:** Windows Server 2008 (non-R2) is not supported.
Web server	Microsoft Internet Information Services (IIS) 7.x must be enabled in Windows Server.
Software required for wake management services	Microsoft .Net Framework 4.6.2 ActiveMQ 5.13.4
Java	• Java 7 • Java 8 **Note:** If no version of Java is found during installation, Java 8 is installed by default. If Java 7 is found, the

	installation continues with Java 7.
Administrator console, Advanced Reporting, Wake for Remote Access web site	· Adobe Flash Player 10 or later · Internet Explorer 8 or later OR Mozilla Firefox (current version) OR Google Chrome (current version) OR Apple Safari (current version) OR Edge **Note:** If you use a supported 64-bit operating system, you will need to use the 32-bit version of IE to run Adobe Flash Player.

Database Requirements

The wake management server communicates with a Microsoft SQL Server database to store and retrieve client and power-state transition data for reporting.

Supported versions	Microsoft SQL Server 2016 Microsoft SQL Server 2014 Microsoft SQL Server 2012 Microsoft SQL Server 2008 R2 Microsoft SQL Server 2014 R2 Express Edition (For evaluations only) **Note:** Windows Installer 4.5 should already be installed on the server computer if you are planning to run a basic installation that uses SQL Server Express.
Database location	The database can reside locally on the EvokeIT server computer or remotely on a separate computer.
Database storage space	5 GB of hard drive storage space per 1,000 clients per year.
Features required to be enabled in the SQL server	• Database Engine Services • Reporting Services - Native • Management Tools

EvokeIT Client Agent

The EvokeIT client agent is supported on any of following operating systems.

- Windows 10 (x86 and x64)
- Windows 8.1 (x86 and x64)
- Windows 7 (x86 and x64)
- Apple Mac OS X versions 10.11 (El Capitan), 10.10 (Yosemite), 10.9 (Mavericks), and 10.12 (Sierra)

Server Installation Options and Prerequisite Software

When you run the EvokeIT setup program, you can select a Basic or Advanced installation.

- *Install and Set up Server Components (Basic Installation) on page 3-2* installs all components required for the EvokeIT server on a single computer. In addition to the EvokeIT server and database components, a basic installation includes Wake for Remote Access.

  Components are installed in standard default locations; for example, Program Files\Verdiem\EvokeIT on the local computer. The default port 80 is assigned for http communications.

  A basic installation best suits typical small- to medium-sized networks with centralized administration.

- The *Install and Set up Server Components (Advanced Installation) on page 3-4* provides options for you to specify or confirm location and service account details for the EvokeIT server and database.

  The advanced installation gives more flexibility in enterprise-level networks, in which you want to host any of the EvokeIT components on separate computers, or connect to a remote database.

  Installing components on separate computers may require some manual post-installation configuration. The topic*Install and Set up Server Components (Advanced Installation) on page 3-4* indicates where this configuration is needed.

Prerequisite Software

In addition to the standard system requirements, some EvokeIT server components require additional software, all of which are included in the installation process (if not detected).

- The Microsoft .Net 4 Framework (Full Version) and Java 7 update 67. The Administrator console requires Microsoft .Net 4 Framework (Full Version) and IIS 7.0 running on Windows Server 2008, IIS 7.5 running on Windows Server 2008 R2, or IIS 8 and above running on Windows Server 2012 R2.
- Microsoft SQL Server 2016, 2014, 2012, or 2008 R2. If Microsoft SQL Server is not already installed, the installation automatically installs Microsoft SQL Server 2014 Express.
- Adobe Flash Player 10 or later must be installed on a computer that will run the Administrator console. This does not have to be the server.
- ActiveMQ 5.13.4 is required for the wake management service, administrator, and enterprise IT management processor components.

Adobe Flash Player 10 must be installed on a computer that will run the Administrator console. The Flash player is not automatically installed; however, a link to install the player is displayed in the Administrator console home page if it is not present.

Additional Server Configuration Requirements

If Windows Firewall is enabled on the EvokeIT server computer, and you will use web-based components, such as the Wake for Remote Access, you may need to configure the firewall to allow those components to access it.

For information, see *Configure Windows Firewall to Allow Web Components to Access the Server on page 3-10* .

Server Installation Components

The following table lists the components that are part of the server installation process, along with the names of the Windows or web services that are installed with each component.

For more information about permissions required and information needed for the installation program, see *Permissions Required for Installation and Deployment on page 1*.

Component	Service name & type	Description
Wake management service	ITMService (web)	Service that communicates wake management activity between managed devices and the database, and between devices and server.
EvokeIT database	SQL Server database (outside of EvokeIT)	Database that stores power-state and user-activity data. Requires SQL Server 2016, 2014, 2012, or 2008 R2. Advanced installation options prompt for database server, name, instance, and authentication method. Windows Installer 4.5 is required on the server computer if you are planning to run a basic installation that uses Microsoft SQL Server Express. For additional database requirements, see *Setting up the Database Environment on page 2-9*.
Administrator API and Administrator console	Admin (web) AdminUI (web)	The web server API and administrator console that runs on top of it. Requires Microsoft .Net Framework 4.0 (Full Version) and IIS. The browser-based user interface requires Adobe Flash Player 10.
Enterprise IT management processor	EvokeIT Task Processor (Windows)	Windows service that performs many critical wake management server functions. This is required if you install the IT Management Service(ITM).
Wake	Verdiem	Enables asynchronous messaging between the Administrator API

Component	Service name & type	Description
management queue service	ActiveMQ (Windows)	and the ITM (essentially between server and clients). Requires ActiveMQ 5.13.4, which is installed if it isn't detected.
Analytics reporting engine	SQL Server Reporting Services (SSRS)	The SSRS Server processes the data queries which the Advanced Reporting Web Services then turns into charts, graphs, PDFs, and other results visible in Dashboards and Analytics reports.

Website Files and Virtual Directories

The installer creates the following IIS virtual directories for the components that you install:

- Admin: Administrator API
- AdminUI: Administrator console
- Dashboard: Dashboard reports
- ITMService: IT Management Service
- WRA: Wake for Remote Access

Permissions Required for Installation and Deployment

To install and run the EvokeIT system, you need to confirm the necessary user accounts and permissions for the services that are installed.

Creating User Accounts for EvokeIT

Each service installed with EvokeIT runs under a user account. The permissions for the user account must be configured to allow the service to access other components of the EvokeIT system.

In general, EvokeIT services require local administrator permissions on the computer on which they're installed. However, instead of using the computer's local system account or an administrator account that is also someone's personal account, it is more secure and useful for troubleshooting to create a user specifically for running EvokeIT components.

Services Installed with the Server Setup Program

The EvokeIT setup program installs a number of services. Two of these are Windows services that run on the wake management server; the others are web services that run through IIS. Frequently the wake management and web servers will be hosted on the same computer, as is the case if you choose the Typical installation path in the EvokeIT setup program.

For the Typical installation path, default options are used, and all components are installed on the same computer. The EvokeIT IIS application pool runs under the network account, the Enterprise IT Management Processor runs under the local system account, and the IIS default web site is used with all of its default settings. The web services (ITMService and Admin) run under the identity of the application pool.

If you select the Advanced path, you can install individual components and specify users that run the services.

The following table lists the services installed and the permissions needed for each.

Service	Permissions Needed
Admin web service	• The equivalent of local administrator permissions on the server, as well as on the computers that run the Administrator console. • Additional administrative permissions for performing wake management tasks on client agents are configured in roles in the EvokeIT Administrator console.
EvokeIT Task Processor (background wake management processor)	Permission to run as a Windows service.
ITMService (wake management processor web service)	• The equivalent of local administrator permissions on the wake management and web servers. • The equivalent of local administrator permissions on the wake management and web servers. • data_reader and data_writer permissions on the wake management database in SQL Server.
Verdiem ActiveMQ (message queueing) service user	Permission to run as a Windows service.

Permissions Required for Wake for Remote Access

Service	Permissions Needed
WRA (Wake for Remote Access web service)	Must be a member of a EvokeIT security role that has **Change Device State** and **Wake** permissions on all relevant security groups that are set up in the Administrator console.

Prepare the Environment for the Server Installation

Before you run the EvokeIT server installation program, take these steps to make sure software pre-requisites are met and the installation itself can run smoothly.

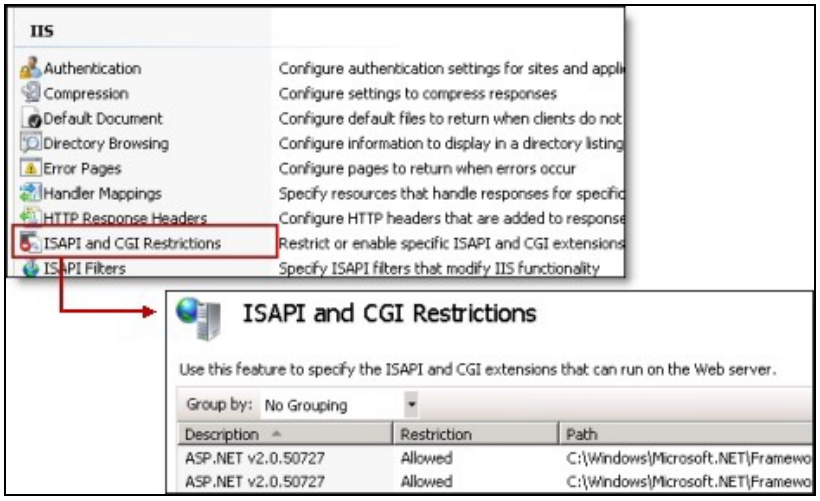
1. Identify the dedicated computer or VM you are planning to use for the server, and confirm that it is configured to meet installation requirements.

   - Minimum 4GB of RAM, 80GB of free hard disk space with a reasonably fast processor (ideally with a minimum of 2 processors or cores).
   - Supported operating system, web server, and SQL Server software.

     SQL Server 2014 Express Edition is supported for evaluations. Production use of EvokeIT requires SQL Server Standard Edition or other licensed editions.

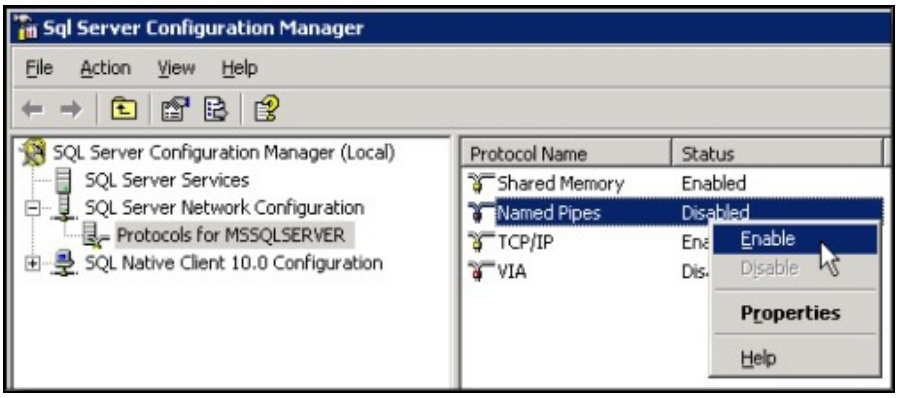
2. Log in to the EvokeIT server computer as a user that is a member of the Local Administrator group.
3. Windows Server 2008 systems: Add the appropriate Windows components for IIS 7 and ASP.NET, as described in Deploying an ASP.NET Server (IIS 7) on Microsoft TechNet.s
4. Open IIS Manager, and allow ASP.NET v2.0.50727.

   IIS 7: Select the server home, double-click **ISAPI and CGI Restrictions**, and then allow **ASP.NET v2.0.50727**.



5. Enable named pipes on the database server:

   a. Open the SQL Server Configuration Manager, navigate to Protocols for **MSSQLSERVER**, and enable **Named Pipes**.



b. Restart the SQL Server from the command line:

   net stop mssqlserver and net start mssqlserver

6. If Windows Firewall is enabled on the server, add an exception to allow incoming traffic from EvokeIT components.

   - In the Control Panel / Windows Firewall, click the **Exceptions** tab, and add TCP port 80 for wake management components.

     For detailed steps, refer to the Microsoft TechNet topic Add a Port to the Firewall Rules List.

Setting up the Database Environment

This topic describes common wake management database configurations and suggestions for when to use each.

To start, you need to decide where to host the database. If your overall deployment is relatively compact, you might put it on the same computer as the server. More commonly, though, the database resides on a separate server maintained by a database administrator.

Using a Local Database

If the server will host both the database and the EvokeIT server, the most straightforward option is to log in as a local administrator, and have the EvokeIT installer create the database during installation.

However, if you decide to create a user for EvokeIT, make sure that the user has the appropriate database permissions. See *Using a remote database* for more information.

Using a Remote Database

You can host the wake management database on a separate computer, either on the same domain or across domains. If you will be using a remote database, you can create and configure the database independently before or after you install EvokeIT, or the installer can create the database during installation.

- Creating the database during installation

  The database administrator (DBA) grants permissions on the SQL server to allow the user running the EvokeIT installation program to create a new database. During installation, the account that is specified with access to the database must have sys_admin rights to the database server. After installation, the DBA can reduce permissions for that user to db_owner for ongoing administration.

  Required permissions: The user must be a member of the **dbcreator** role during installation. After installation, the minimum permissions required are db_datareader and db_datawriter. To create a dbcreator role, refer

- Creating the database independently of installation

  If a DBA creates the database separately, use either of these options to configure it:

  - Create it before installation, and the user installing EvokeIT points to it during installation. The setup program then creates and configures the database tables for EvokeIT.

    Required permissions: During the installation/upgrade, the account used to access the database must have db_owner and sys_admin rights. The sysadmin rights can be removed after the install. The db_owner rights can be limited to the EvokeIT database.

  - The DBA creates and configures the database before or after the installation, so that the installer does not touch the database server. During installation, database credentials are entered so that the installation program can write the proper settings to the configuration files.

    The required SQL script for creating the tables for EvokeIT is included in the distribution package.

Important: If you choose to have your DBA pre-create the database prior to installing EvokeIT, the DBA will need to run the EnterpriseWakeDB.sql against the new database. This script is located in the distribution package in the EvokeIT6xx\EvokeIT Server\Resources\Database folder. You will see three SQL scripts in this folder, however only the EnterpriseWakeDB.sql needs to be run.

3

Installing and Managing the EvokeIT Server Components

Table 3-1 In this Chapter

Topics
Install and Set up Server Components (Basic Installation)
Install and Set up Server Components (Advanced Installation)
Manually Deploy Reports
System Settings and Descriptions
Reporting Settings
Uninstall or Change the Server Configuration
Configure Windows Firewall to Allow Web Components to Access the Server

Install and Set up Server Components (Basic Installation)

When you run the EvokeIT setup program, you can select a default or custom installation. This section gives an overview of the components that you can choose to install with the EvokeIT system and the prerequisites for installation. It also steps through the installation process itself.

An EvokeIT installation includes the EvokeIT server and database, SSRS (for Advanced Reporting), Wake for Remote Access, all installed on the same computer. All required components that are not already installed on the computer will be installed automatically as part of the server installation.

! **Important:** Ensure SQL Server Reporting Services (SSRS) is configured before you begin EvokeIT installation. For information about SSRS configuration, see the *EvokeIT Reports Configuration Guide*.

---

1. Log on to the server computer as a user that is a member of the Local Administrator group, and then navigate to the distribution folder.
2. Run **EvokeITServerSetup.exe**.

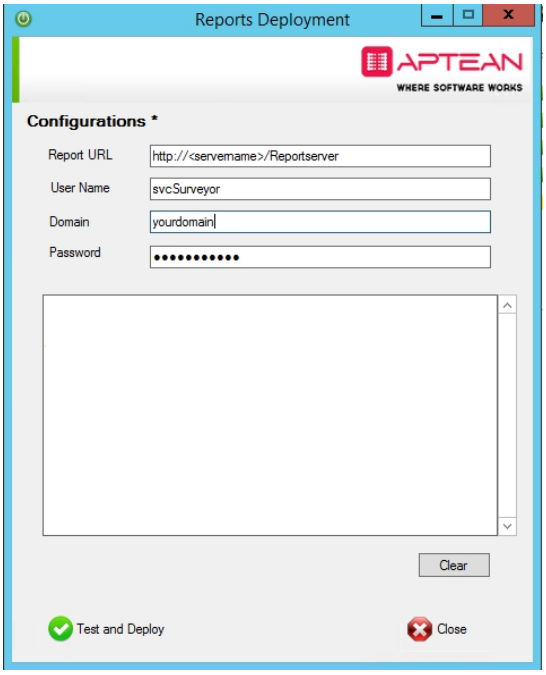
   If an existing version of the EvokeIT server is detected, the installation will indicate the components to be upgraded. Click Upgrade **EvokeIT Server**, accept the end user license agreement, and then click **Begin Upgrade** to proceed. If you are upgrading, you won't need to follow the rest of the steps in this topic.
3. Click **Continue with Basic Install**.
4. Proceed through accepting the license agreement, and then click **Begin Install**.

   For other details about the Default installation settings, see *Server Installation Options and Prerequisite Software on page 2-4*.
5. Do one of the following:
   - If an existing report deployment is found, the installer will automatically update the reports. Go to step 9.
   - If there is no existing report deployment, the reports need to be manually deployed. Go to step 6.
6. After installation completes, click **Manually Deploy Reports in SSRS Server**.

   The **Reports Deployment** window opens.
7. Enter the following information in the **Reports Deployment** window.
   - **Report URL**: URL of the report server
   - **Username**: A user name of the reporting server with appropriate access permissions.

- **Domain**: Domain of the reporting server.
- **Password**: Password associated with the user name of the reporting server.

The following is an image of the **Reports Deployment** window.



8. Click **Test and Deploy**.

After testing and deploying reports, the **Reports Deployment** window closes.

Note: If you need to deploy reports manually, see *Manually Deploy Reports on page 3-6*.

Note: You may have a server setup where the EvokeIT database and SQL Server Reporting Services (SSRS) are hosted on two different servers. If this is the case, see *Advanced Reports Deployment on page 13*.

9. Click **Close Setup Wizard and Open the EvokeIT Administrator Console** and begin configuring EvokeIT.

Note: Check the logs to verify if the installation is successful.

Install and Set up Server Components (Advanced Installation)

The advanced options for installing EvokeIT provide options for remote administration.

This procedure assumes the following:

- You have followed the steps appropriate for your organization in *Prepare the Environment for the Server Installation on page 2-7*, and you have the web site and database connection information.
- You have created any user accounts you need to run the EvokeIT services.
- You have configured SQL Server Reporting Services (SSRS). For information about configuring SSRS, see the *EvokeIT Reports Configuration Guide.*

Note: If you install all of the components on one computer, you do not need to perform these extra configuration steps manually, because they are completed by the setup program.

1. Log on to the server computer as a user that is a member of the Local Administrator group, and then navigate to the EvokeIT distribution folder.
2. Run **EvokeITServerSetup.exe**.

   If an existing version of the EvokeIT server is detected, the installation will indicate the components to be upgraded. Click **Upgrade EvokeIT Server**, accept the end user license agreement, and then click **Begin Upgrade** to proceed. If you are upgrading, you won't need to follow the rest of the steps in this topic.
3. Click **Set Advanced Install Options**.
4. Select the service account and database connection, and then click **Continue with Advanced Install Options**.
5. Select the installation path, and then click **Continue with End User License Agreements**.
6. Read and accept the agreements for the EvokeIT server and then click **Begin Install**.

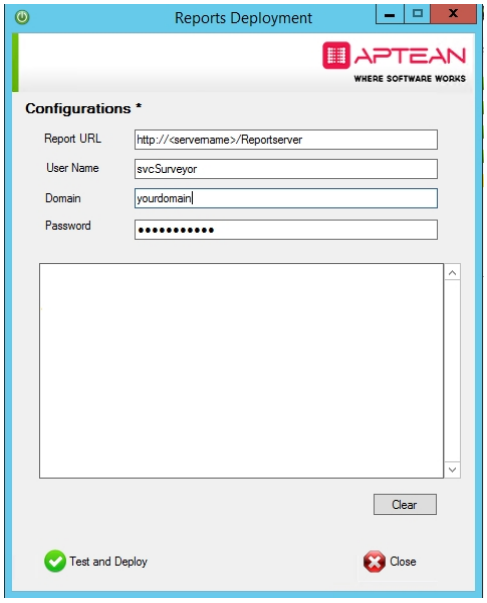
   A full EvokeIT installation includes the EvokeIT server and database, SSRS (for Advanced Reporting), Wake for Remote Access, all installed on the same computer. All required components that are not already installed on the computer are also installed automatically.
7. Do one of the following:
   - If an existing report deployment is found, the installer will automatically update the reports. Go to step 11.
   - If there is no existing report deployment, go to step 8.
8. After installation completes, click **Manually Deploy Reports in SSRS Server**.

The **Reports Deployment** window opens.

9. Enter the following information in the **Reports Depoloyment** window.

   - **Report URL**: URL of the report server.
   - **Username**: A user name of the reporting server with appropriate access permissions.
   - **Domain**: Domain of the reporting server.
   - **Password**: Password associated with the user name of the reporting server.

   The following is an image of the **Reports Deployment** window.



10. Click **Test and Deploy**.

    After testing the connection and deploying reports, the **Reports Deployment** window closes.

> **Note:** If you need to deploy reports manually, see *Manually Deploy Reports on the next page*.

> **Note:** You may have a server setup where the EvokeIT database and SQL Server Reporting Services (SSRS) are hosted on two different servers. If this is the case, see *Advanced Reports Deployment on page 13*.

11. Click **Close Setup Wizard and Open the EvokeIT Administrator Console** and begin configuring EvokeIT.

> **Note:** Check the logs to verify if the installation is successful.

Note: If the administrator console does not open, you may need to enable ASP.NET in IIS. For details, see Administrator console does not open in the browser.

Note: To open the EvokeIT administrator console: From the Windows Start menu, click All Programs > Verdiem > EvokeIT Administrator.

If you have granted db_creator or equivalent permissions to the user running the EvokeIT installer, you can reduce those permissions. If the user is also the user that will run the service, minimum required permissions are db_datareader and db_datawriter.

In addition, if you install individual server components on separate computers, you need to do some additional manual configuration.

Manually Deploy Reports

This section contains information about manually deploying reports. This can be done using two different methods.

- **Deploy**: The existing reports are removed and a fresh deployment is done. For information about deploying reports, see *Deploy reports below*.
- **Upgrade**: The existing credentials and connection details are retained and the reports are re-deployed. For information about upgrading reports, see *Upgrade Reports on page 1.*

Deploy reports

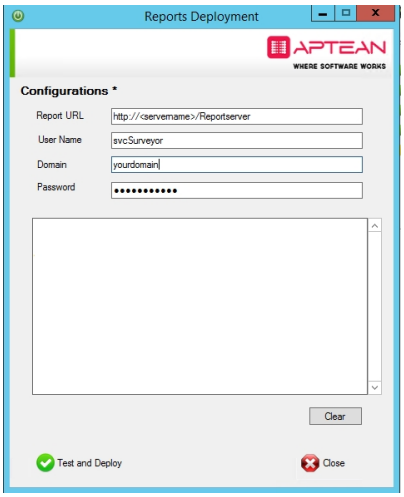
This section contains information about deploying reports.

To deploy reports

1. Go to **C:\Program Files (x86)\Verdiem\EvokeIT\Reports**
2. Run the **DeployReports** application.

   The **Reports Deployment** window opens.
3. Provide URL and credentials for the SQL server reporting service.
4. Enter the following information in the **Reports Deployment** window.
   - **Report URL**: URL of the report server.
   - **Username**: A user name of the reporting server with appropriate access permissions.
   - **Domain**: Domain of the reporting server.
   - **Password**: Password associated with the user name of the reporting server.

   The following is an image of the **Reports Deployment** window.



5. Click **Test and Deploy**.

   A success message appears after the reports are successfully deployed.

Note: You may have a server setup where the EvokeIT database and SQL Server Reporting Services (SSRS) are hosted on two different servers. If this is the case, see *Advanced Reports Deployment on page 13*.

Upgrade reports

This section contains information about upgrading reports.

To upgrade reports

1. Open command prompt.
2. Type `<installed location>\Verdiem\ EvokeIT\Reports`.

   For example: C:\Program Files (x86)\Verdiem\Surveyor\Reports

2. Run the command `DeployReportsConsole.exe update`.

Note: If the deployment fails, details of the deployment failure can be found under **C:\Users\<user>\AppData\Local\Verdiem Corporation\Server Install Logs\Reports_Deploy.log**.

System Settings and Descriptions

The table in this topic contains settings from Configure Server 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 0 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.

Uninstall or Change the Server Configuration

Use **Add or Remove Programs** in the Windows Control Panel to uninstall or change EvokeIT server components.

This starts the setup .msi file and gives you the appropriate options for the components installed. Run this process on each computer that hosts a EvokeIT component that you want to uninstall or change.

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 is added to the exceptions list. If an SSL connection is used, enable port 443.

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.

   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

EvokeIT Client Distribution

Table 4-1 In this Chapter

Topics
Install the EvokeIT Windows Client Agent from the Setup Program
Install or Uninstall EvokeIT Windows Agent from the Command Line
Install EvokeIT Mac Agent
Distribute the EvokeIT Windows Client Agent by Disk Image
Deploy the EvokeIT Windows Client Agent using Group Policy
Distribute the EvokeIT Windows Client Agent through a Microsoft ConfigMgr Package
Managing Client Agent Software Upgrades

Install the EvokeIT Windows Client Agent from the Setup Program

This section contains information for command-window installation of the client agent and some common ways to distribute the EvokeIT Windows client software to a large number of computers. If you use a management system that is not covered here and would like some help, feel free to contact Technical Support

To use the setup program, you need to know the address of the EvokeIT server computer and have access to the EvokeIT distribution media.

This procedure describes how to run the installation program on the Windows client computer directly. When you want to use your standard software distribution process, use the procedure for running a silent installation. For information, see *Install or Uninstall EvokeIT Windows Agent from the Command Line on page 1*.

1. On the client computer, log in as a local administrator and copy the EvokeIT client distribution files from the distribution media to the client computer.
2. Run the setup file **EvokeITAgentSetup.exe** and follow the instructions in the installation wizard. In the wizard pages, note the following:
   a. On the Installation Configuration page, you must replace <*servername*> with the correct address of the EvokeIT server.
   b. On the same page, leave the **Add Aptean as a trusted publisher** check box selected.
3. Click **Install** to continue.

Install or Uninstall EvokeIT Windows Agent from the Command Line

This topic provides the command line parameters for installing or uninstalling the agent software for Windows clients.

Installation Process

This procedure describes how to run the silent installation on the client computer directly. You can use this same command with your standard software distribution process to push the client agent to multiple computers.

1. Copy the files for the client distribution to a location on the client computer.
2. To run the silent installation, open a command window, change to the directory that contains the setup file, and then type the following command:

```
EvokeITAgentSetup.exe /s /v"/qn PMP_
URL=http://EvokeITWebServerName/ITMService/ITMService.svc/PMP"
```

Note: There is no space between the /v parameter and the opening quotation mark. Adding one will cause the installation to fail.
If you are creating a SCCM ConfigMgr package for the agent installation, there is a limitation of 171 characters in the command line argument. As a workaround, you can create a BAT file for the SCCM package to reference.

Or, use the .msi file directly:

```
Msiexec.exe /i [PATH TO EvokeIT Agent.msi FILE] /qn PMP_
URL="http://<SERVERNAME>/ITMService/ITMService.svc/PMP"
```

3. If you want to create an installation log file, add the **/log** parameter with the **/qn** parameter and specify the location. For example:

   ```
   EvokeITAgentSetup.exe /s /v"/qn [other parameters] /log setup_
   log.txt"
   ```

   A reliable location for setup_log.txt is the same directory as the setup file. However, you can add the path to another location and file name. Either way, the directory that you specify must exist on the client computer.

Confirming Client Distribution Success

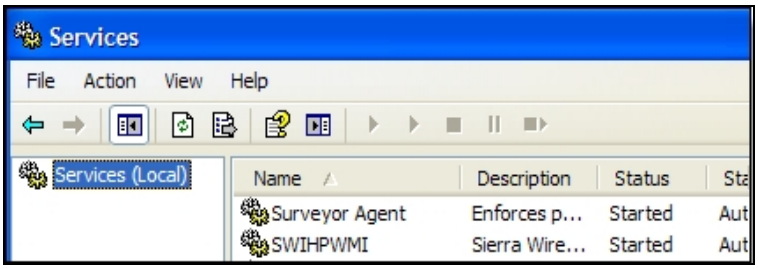
If you installed the client agent by sending a distribution package from your desktop management system to a large number of computers, verifying its success is usually a two-phase process:

- After the package runs, you can check the reports in the desktop management system to confirm that it ran successfully.
- After a week or two, use the EvokeIT Administrator console to view the number of computers that are checking in with the server and the number of licenses that are used.

Troubleshooting Windows-Based Clients

If it looks as if a computer is not checking in properly, check that the client agent is running on that computer:

1. On the client computer, open the Windows Services console: **Click Start menu / Run**, and type *services.msc*.
2. Confirm that the status of the EvokeIT Agent shows **Started**.



Parameters and Descriptions

For a standard silent installation, common parameters include:

- **/s —** silences the setup.exe file.
- **/v"[attributes]" —** passes everything inside the quotations to the setup application.

Important: There is no space between the /v parameter and the opening quotation mark. Adding one will cause the installation to fail.

- **/qn —** used inside the quotations of the /v parameter to silence the .msi application. You can pass additional attributes, including:

  INSTALLDIR=\"[path]" — specifies the parent directory in which you want to install the client application files on the client computer. The default is C:\Program Files\Verdiem\EvokeIT Agent. **Optional parameter**.

  INSTALLCERTIFICATE=yes — sets Aptean as a trusted publisher. **Optional parameter**. The default is yes.

  PMP_URL=[url] — specifies the web address to the ITM service on the EvokeIT server. **Required parameter**.

  DATA_COLLECTION_DIR=\"[path]" — specifies the directory where historical data and service logs should be stored (if you need it to be different than default). **Optional parameter**.

Uninstalling the Windows Client Agent

You can uninstall the agent from the Add/Remove Programs component of the Windows Control Panel on the client computer, or you can use the following command from the client's distribution directory:

```
msiexec /q /x "EvokeIT Agent.msi"
```

If you did not copy the distribution files to the client, you can run a silent uninstall by using the product code in the registry instead the .msi file name.

For example:

```
mxiexec /q /x {F3466B4E-A738-4D12-92C5-4CD3E06447B8}
```

In this example the x characters represent the product code.

Command Line Parameters Available for EvokeIT Agent Installation

When running a command line install the following properties can be passed in via the /qn switch.

Note: INSTALLDIR and path names with spaces must be delimited by \"\".

Property	Description
INSTALLDIR	The parent directory for the install. The default is *C:\Program Files\Verdiem\EvokeIT Agent*. **Optional**
INSTALLCERTIFICATE	If Yes, Aptean is added as a trusted publisher. Useful if you are planning to use PSTM scripts. Default is Yes. **Optional**
DATA_COLLECTION_DIR	Specifies the directory where historical data and service logs should be stored (if you need it to be different than default). **Optional**
PMP_MAX_BACKOFF	The maximum back off time in minutes used when the agent cannot reach its ITM server. The default is 15 minutes.
PMP_URL	The URL for the ITM web service; for example, *http://<yourserver>/ITMService/ITMService.svc/PMP*. **Required**
REINSTALL	A Microsoft property used for upgrade installs. **Optional**
REINSTALLMODE	A Microsoft property used for upgrade installs. **Optional**

Install EvokeIT Mac Agent

This topic provides an overview and step-by-step descriptions of commands you use to install the EvokeIT agent package (**EvokeITAgent.pkg**) and update the **serverconfig** file. You can use these steps in the command window or within an installation script that you create.

The procedures here assume you have read *Installation Files for the EvokeIT Mac Client on page 4-7* and that you have Administrator-level permissions on the Mac client computers.

Use the included **updateinstallerconfig.pl** script to recreate the package with customized **serverconfig** information.

Note: The EvokeITAgent.pkg can be installed on Mac OS X 10.12, 10.11, 10.10, and 10.9. The updateinstallerconfig.pl script runs only on Mac OS X 10.12, 10.11, 10.10, and 10.9.

Install the Mac Agent Using the updateinstallerconfig.pl Script

For this procedure, you open the package, insert the server hostname into the **serverconfig** file, re-create the package, and then install it.

Note: The **updateinstallerconfig.pl** script runs only on Mac OS X 10.12, 10.11, 10.10, and 10.9.

Command Overview

```
sudo perl ~/Desktop/updateinstallerconfig.pl --hostname yourserver --package ~/Desktop/EvokeITAgent.pkg
```

```
sudo installer -pkg ~/Desktop/EvokeITAgent.pkg -target /
```

where *yourserver* is the hostname of the EvokeIT server.

Note: */Desktop* can be whatever location you have copied **updateinstallerconfig.pl** to.

Step-by-Step Description

1. On the Mac client, open a command window and type the command to open the package and insert the EvokeIT server name:

   ```
   sudo perl ~/Desktop/updateinstallerconfig.pl--hostname yourserver --package ~/Desktop/EvokeITAgent.pkg
   ```

   For example:

   ```
   sudo perl ~/Desktop/updateinstallerconfig.pl--hostname lab.verdiem.local --package ~/Desktop/EvokeITAgent.pkg
   ```

   For Mac agents, use the following command line to configure the package for HTTPS:

   ```
   sudo perl ~/Desktop/updateinstallerconfig.pl --hostname
   ```

   ```
   yourserver --https --package ~/Desktop/EvokeITAgent.pkg
   ```

2. Next, install the package:

```
sudo installer -pkg ~/Desktop/EvokeITAgent.pkg -target /
```

Important: You must specify the system root as the target as shown here, because the EvokeIT agent is installed relative to the root.

After you complete this procedure once, the **serverconfig** file in the installation package contains the server hostname, and for subsequent installations, you can simply run the package as in step 2.

Manually Configure Serverconfig and Restart the Client

In cases where manual configuration of the client **serverconfig** file is required, follow these steps.

1. Stop the daemon. At the command line type:

   ```
   sudo launchctl unload
   /Library/LaunchDaemons/com.verdiem.pwrmgrdaemon.plist
   ```

2. Edit the *hostname* in the **serverconfig** located at **/Library/Application Support/Verdiem/Data** (requires sudo). Note that codepage (UTF-8) must be respected for the **serverconfig** file.
3. Restart the daemon:

   ```
   sudo launchctl load
   /Library/LaunchDaemons/com.verdiem.pwrmgrdaemon.plist
   ```

Installation Files for the EvokeIT Mac Client

This topic describes the contents of the EvokeIT agent package file and configuration involved in Mac client installation.

Updating the Serverconfig File with Your Server URL

A required step of the installation process is to enter the hostname of your EvokeIT server into the appropriate **serverconfig** setting, so that clients know where to report their power-state activity.

For details, see *Install EvokeIT Mac Agent on page 4-5*. You can also update **serverconfig** file manually.

The EvokeIT Agent Package File

EvokeITAgent.pkg is a flat package file that contains the installation components, which it installs into the following locations.

Note: Macintosh OS X 10.9 (or later) is required to install the **EvokeITAgent.pkg**.

Component and installed location	Description
/Library/Application Support/ Verdiem/SurveyorPowerManagement.app	The application bundle.
/Library/StartupItems/ PwrMgrDetection/PwrMgrDetection	The application that detects and dispatches power-state events.
/Library/StartupItems/PwrMgrDetection /StartupParameters.plist	Registration description plist for startup items.
/Library/LaunchDaemons/com .verdiem.pwrmgrdaemon.plist	A plist used for launchctl, which handles the way that the EvokeIT daemon is run and launched.
/Library/Application Support /Verdiem/Data/serverconfig	An empty serverconfig file in which you will need to enter the hostname the EvokeIT server computer, either manually or by using an included script.
/Library/Application Support/Verdiem/Data/ updateinstallerconfig.pl	A Perl script that inserts the hostname of the EvokeIT server into the serverconfig file and restarts the EvokeIT daemon. **Note:** Macintosh OS X 10.9 is required to run this script.
/Library/PreferencePanes/ EvokeIT.prefPane	The EvokeIT preferences panel that appears under System Preferences.
/Library/LaunchAgents/ com.verdiem. pollingagentstchnagent.plist	A plist used to launch notification dialog whenever power transition happens through Verdiem.

EvokeITAgent.pkg also includes the following scripts that unload and load the daemon.

- **preinstall:** Stops the EvokeIT daemon if it's running.
- **postflight:** Starts the EvokeIT daemon, sets file permissions correctly on files in the bundle and other files listed above.

Note: These scripts are used only by the installer; they are not installed on the client computer.

Confirm Mac Client Connectivity to the EvokeIT Server

This topic provides instructions for determining that a Mac client is connecting to the EvokeIT server.

1. Determine that the client agent is installed and running:
   a. On the Mac client, click **Applications > Utilities > Activity Monitor**, and verify that PwrMgrDaemon appears in the list of processes running on the computer.
   b. On the Mac client, on the Apple menu > **System Preferences**. You should see the EvokeIT application logo
2. Confirm that the client is connected in EvokeIT.
   a. In the EvokeIT Administrator console on the Devices page, select the groups that contain the Mac agent client computers.
   b. Confirm that the Mac clients appear in the device list and that they each show the following status settings:
      - Last Connected: *today's* date
      - Licensed: Yes
      - Status Summary: Current
      - Policy Status: Delivered
3. Determine that the client is connected in the Mac console:
   a. On the Mac client, click **Applications > Utilities > Console**.
   b. On the **File** menu, click **Open Recent**, and then select **PwrMgrService.log**.

Uninstall a Mac Client

To uninstall a Mac client, you will need to stop the EvokeIT daemon and then delete several files and directories.

1. Stop the daemon. At the command line type:

```
sudo launchctl unload
/Library/LaunchDaemons/com.verdiem.pwrmgrdaemon.plist
```

2. Stop the agent. At the command line type:

   ```
   Sudo launchctl unload
   /Library/LaunchAgents/com.verdiem.pollingagentstchnagent.plist
   ```

3. Delete the following files and directories:

   ```
   /Library/LaunchDaemons/com.verdiem.pwrmgrdaemon.plist
   /Library/Application Support/Verdiem/SurveyorPowerManagement.app
   /Library/StartupItems/PwrMgrDetection/PwrMgrDetection
   /Library/StartupItems/PwrMgrDetection/StartupParameters.plist
   /Library/Application Support/Verdiem/Data/
   /Library/LaunchAgents/com.verdiem.pollingagentstchnagent.plist
   ```

Distribute the EvokeIT Windows Client Agent by Disk Image

This topic describes how to prepare a prototype Windows computer for distributing the client agent by copying its disk image to the other computers.

Note: This topic applies only to the Windows PC client.

1. On the computer you want to use as the image, install the client agent from the setup program (EvokeITAgentSetup.exe).
2. Verify that the client connects to the EvokeIT server.
3. In the Windows Services console, stop the EvokeIT Agent service:
   a. Right-click **My Computer** and choose **Manage**.
   b. In the Computer Management console, expand **Services and Applications**.
   c. Under Services, right-click **EvokeIT Agent** and choose **Stop**.
4. In the **Program Files** or `Program Files (x86)\Verdiem\EvokeIT Agent\Data` folder, delete the following files:
   - eventstore: contains power state and event history
   - policy: contains wake management instructions

   When you transfer the image to new computers, you want them to begin with a clean history and no policy, so that they receive instructions only from the server.
5. In the **Data** folder:

This enables a new unique ID to be assigned to each computer when the agent is installed.

6. In the **serverconfig** file (all versions), confirm that the path to your EvokeIT wake management service is correct. It looks something like this:

   {"serverURL":"http:\/server_name.local\/ITMService\/ITMService.svc\/PMP"}

7. In the **Logs** folder:

   Delete all files from the **Logs** folder (but do not delete the folder itself) .

Additional Information

After you prepare the prototype computer, you can copy its image to the other client computers.

To prevent collisions among EvokeIT clients when they connect to the server, each computer that receives the disk image must have:

- a unique DNS name.
- a unique MAC address.

For more information about completing the image installation, refer to the documentation provided by your imaging software.

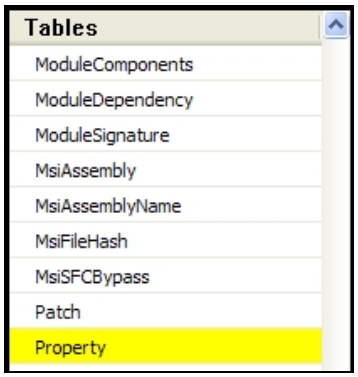
Deploy the EvokeIT Windows Client Agent using Group Policy

This process involves two separate procedures: create the transform file from the client installer package (.msi); then add the transform and package to a Group Policy object. This procedure applies to the Windows agent only.

To create the transform file, you need a transform editor. The procedure provided here uses Orca, although you can use any transform editor.

Orca is a database table editor for creating and editing Windows Installer packages and merge modules. It is available in the Windows Installer SDK, which you can download from the Microsoft Download Center.

1. Start Orca, and in the client agent folder of your EvokeIT distribution, open EvokeIT Agent.msi.
2. From the **Transform** menu, choose **New Transform**.
3. In the **Tables** column, select **Property**.



4. Confirm the following properties and values:

   - PMP_URL: The address of the wake management web server that hosts the ITM service.

   Note: You must add this property.

   Specifies the web address to the ITM service on the EvokeIT server. For example: http://<*servername*>/ITMService/ITMService.svc/PMP.

   - SERVER_PORT: the port number you will use for the deployment (http port 80 by default).

5. From the **Transform** menu choose **Generate Transform**.
6. Enter a name for the transform file (.mst), save it, and then exit Orca.

Create the Group Policy Object for EvokeIT Windows Client Installation

After you create a transform file from the EvokeIT client installer package, you can add it and the package to a Group Policy object to install the Windows client software.

Before you can perform this procedure, use the steps on the previous page to create the transform file that you'll use in this procedure.

Note: This procedure is from the Group Policy Object Editor Help and modified to include the information specific to EvokeIT.

Note: To perform the installation, user needs 'Domain Computers' permission only and the folder where client package is placed must have 'Read and Execute' permissions allowed to computers.

1. Open the Group Policy Object Editor by choosing *Start menu / Run*, and typing *gpedit.msc.*
2. Navigate to and select **Computer Configuration / Software Settings / Software Installation**.
3. Right-click in the details pane and click **New / Package**.

4. In the Open dialog box, from the EvokeIT distribution folder, browse to **EvokeIT Agent / EvokeIT Agent.msi**, and then click **Open**.
5. In the Deploy Software dialog box, click **Advanced**, and then click **OK**.
6. In the properties dialog box for the package, in the **Modifications** tab, click **Add**.
7. In the Open dialog box, browse to the transform file you created for the EvokeIT client installer, and then click **Open**.
8. Make sure you are done configuring modifications, and then in the EvokeIT Client Agent Properties window, click **OK**.

Note: The package is assigned or published immediately when you click OK. If the modifications are not properly configured, you will have to uninstall the package or upgrade the package with a correctly configured version.

9. Close the Group Policy Object Editor.
10. To put the Group Policy updates into effect, either restart the computers or run the command gpupdate /force to refresh the Group Policy settings.

Note: If you get an error that validation of the installer package has failed, try editing the default language properties of the package. To do this, right-click the package and choose **Properties**. On the **Deployment** tab, click **Advanced**, and then select the **Ignore language when deploying this package** check box.

Distribute the EvokeIT Windows Client Agent through a Microsoft ConfigMgr Package

Distributing the EvokeIT Windows client agent through Microsoft Systems Center Configuration Manager 2007 involves three phases.

1. *Create a ConfigMgr Package for the EvokeIT Window Client Agent Installation below*
2. *Create an Advertisement to Distribute a EvokeIT Windows Client Package on the next page*
3. *Validate EvokeIT Windows Client Installation through ConfigMgr on page 4-15*

Create a ConfigMgr Package for the EvokeIT Window Client Agent Installation

This procedure covers the first of three phases of distributing the EvokeIT Windows client agent through Configuration Manager: the settings that you use in the New Package Wizard.

1. From the EvokeIT distribution, copy the Windows client agent folder to a Configuration Manager site server or to a shared network folder.

2. Open the Configuration Manager console, navigate to **Site Database / Computer Management / Software Distribution / Packages**.
3. Right-click **Packages** and choose **New / Package**.
4. Follow the instructions in the New Package Wizard:
   a. On the **General** page, enter a name for the package, and complete any additional fields you want.
   b. On the **Data Source** page, select **This package contains source files**, and click **Set**. In the Set Source Directory dialog box, under **Source directory location**, click the type of connection, enter the source directory, and then click **OK**.
   c. On the Distribution Settings page, for **Sending Priority**, select **High**.
5. When you complete the remaining wizard steps, click **Close**.

   The package appears under the **Packages** node of the site tree in the Configuration Manager console.
6. Expand the package, right-click **Distribution Points**, and choose **New Distribution Points**.
7. Select the check box beside the name of each server you want to make distribution points, and then click **Next**.

   The wizard creates the distribution points and completes.
8. Click **Close** to return to the site tree.
9. Right-click **Programs**, choose **New / Program**, and follow the instructions in the New Program wizard, noting the following specific setting for this program:
   - On the General page, For **Command line**, enter the command with the parameters you want to install the client agent.

     For a sample command and list of available parameters, see*Install or Uninstall EvokeIT Windows Agent from the Command Line on page 4-2*.

After you create the package, select distribution points, and create the program for running the package, you set up an advertisement to distribute it.

Create an Advertisement to Distribute a EvokeIT Windows Client Package

This task is the second phase of distributing the EvokeIT Windows client agent through Configuration Manager. You do this after you create the installation package, select distribution points, and create the program that runs the installer.

If you have not created the package for the EvokeIT Windows client agent, see *Create a ConfigMgr Package for the EvokeIT Window Client Agent Installation on the previous page*

1. In the Configuration Manager console, set up a collection of clients that you want to target for the EvokeIT client agent distribution.

   You can base the collection on a query or direct membership rules.

2. Right-click the collection, and then choose **Distribute / Software**.
3. Follow the instructions in the Distribute Software to Collection Wizard:

   a. On the Package page, select **Select an existing package**, click **Browse**, and then select the EvokeIT installation package you created.

   b. On the Advertise Program page, indicate that you want to advertise a program from this package.

   c. On the Select Program page, click the program you created for this distribution.

   d. On the Advertisement pages, configure the settings for the name, any subcollections to advertise to, and the schedule.

   e. On the Assign Program page, select **Yes, assign the program**.

   f. Complete the wizard.

After the advertisement goes out to the collection, and the installation has completed, you can validate the installation.

Validate EvokeIT Windows Client Installation through ConfigMgr

After you distribute the EvokeIT client agent through Configuration Manager, you use the EvokeIT Administrator console to confirm that it was successful.

If you have not yet distributed the EvokeIT client agent to a collection, see *Create a ConfigMgr Package for the EvokeIT Window Client Agent Installation on page 4-13*.

1. On the EvokeIT server computer, open the EvokeIT Administrator console in a browser.
2. On the Devices page, use the device filters to select the groups in the PC device family that represent the computers that received the Configuration Manager distribution.
3. Confirm that the PC clients appear in the device list and that they each show the following status settings:

   - Last Connected: Today
   - Licensed: Yes
   - Status Summary: Current
   - Policy Status: Delivered

Note: If the total number of PCs that match your search criteria exceeds the number that are displayed in the device list, you will need to refine the search to view all of them.

5

Licensing Devices

Table 5-1 In this Chapter

Topics
About Device Licenses
Viewing License Information
Add or Remove a License File
Reclaim Licenses for Inactive Devices

About Device Licenses

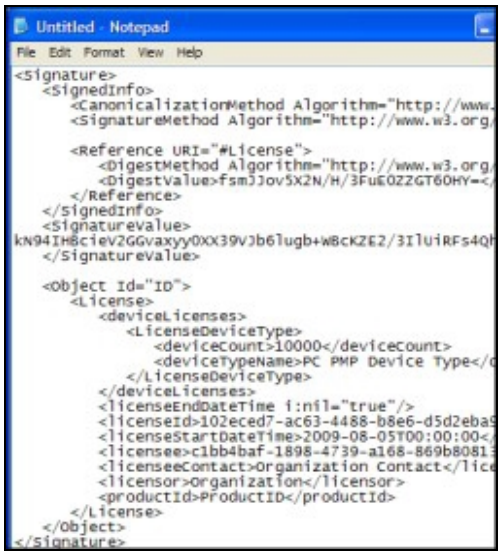
After you install the client agent, you license the devices in your system. This section describes the process.

This topic provides an overview of the license file, license types, and viewing license information in your system through the EvokeIT Administrator console.

How the License File Works

Device licenses are stored in an XML file. You import the file into the system through the Administrator console. The server apply policies only on devices that are licensed.

The license file includes information such as product and license id, number of devices in the EvokeIT system, effective dates, and other information that helps the server recognize which devices to measure or manage.



How You Obtain License Files

During the evaluation period, your Verdiem representative works with you to determine the number of devices you want to license. After you decide to deploy EvokeIT, the Verdiem representative goes through a process to generate a single license file that contains the number of licenses determined, the license types, and other required data.

When you receive the file, you complete just a few simple steps in the Administrator console to apply the license to client devices.

Viewing License Information

In the server settings of the Administrator console, you can view all licenses applied to an instance of EvokeIT, as well as the following status information:

- Dates for when the license became active and when it expires.
- Device families covered by the license and number of devices in each family.

> **Note:** The device type **PC ITM** represents both Windows and Mac computers. ITM refers to the EvokeIT wake management protocol.

- Number of total licenses available and in use.
- Licensee (your organization name), licensor's organization and individual contact names.
- License unique id.

In addition, when you view a list of devices on the License Management page, you can display a column that indicates whether each device is licensed.

Viewing License Information

In addition to viewing the license status of devices, you can also see information about the license file itself. For example, when it expires or how many devices it covers.

License Management Page

The Manage Licenses page is where you can add or remove license files and monitor license allocation.

The following table describes each of the settings on the **License Management page** (on the Configure menu , click **License Management**.

Setting	Description
Device	The type of device that is licensed under the selected license file. **Device types PC ITM:** PC or Mac Computers on which the client agent is installed, and on which you enforce policies. ITM stands for IT management.
Total Licenses	The number of devices that are allowed to be licensed through the selected license file.
Total Allocated / Total Remaining	The number of licenses in the selected license file that are in use, and the number that can still be used.
Start / End	The start and end dates during which the selected license file is valid.

Setting	Description
Licensee	The organization to whom the license is issued.
Contact	The person or organization to contact to renew the license or change its conditions.
Licensor	The organization that issued the license.
ID	The globally unique string used to identify and verify the license file, automatically generated when the file is created by the Licensor.

Add or Remove a License File

To license devices, you obtain a license file from your Verdiem representative and then activate it though the Administrator console.

This task describes how to add or remove a license file that you have already obtained for the number of device licenses you need. Also see *Reclaim Licenses for Inactive Devices on the next page*.

1. Log on to the server computer.
2. You'll have one of the following options for saving the license file to the server's local drive:
   - Save the file attachment from email.
   - Download the file from the customer portal address you were given.
3. The license file is an XML file. If you obtained a .zip file, extract it and confirm that the license file shows the .xml extension.

   Note: If the file does not show the .xml extension, open it in Notepad to confirm that it's an XML file, close it, and change or add the extension. If that does not work or the file is not an XML file, you will need to contact your Verdiem representative to resolve the problem.

4. Open the Administrator console, on the Configure menu, click **License Management**.
5. Click **Add License File**, and do the following:
   a. For Files of type, replace type **Text** by manually typing *.* to show all files.
   b. Navigate to your license file location, select the file, and click **Open**.
      If you want to remove an existing license, select the file, and click **Delete**.

If you add a license file, its information is displayed in the Administrator console, indicating the number of licenses, where the license came from, and so on. Devices are licensed immediately (you do not need to restart the service).

When you remove a license file, devices that are associated with it become unlicensed. At that point, power use on those devices is no longer managed or measured.

Reclaim Licenses for Inactive Devices

Rather than removing licences 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**.

6

Configuring and Running Data Summarization

Table 6-1 In this Chapter

Topics
About Data Summarization

About Data Summarization

This section describes data summarization, and how and when to configure, schedule, run, and check the status of it.

This topic describes how to configure, schedule, run, and check the status of the summarization process.

The data displayed in higher level EvokeIT 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**.

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 *Resummarize Data Incrementally Using a Windows Task on page 6-4*.

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 *Resummarize Data Incrementally Using the AdminCommand.exe Tool on the next page*.

For details on resummarizing all data, see *Resummarize All Data on page 6-6*.

To View the Results of the Summarization Task:

- Open the **summarization** log file in **C:\Program Files\Verdiem\EvokeIT\Logs**.

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 and 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.

Note: Avoid running a full re-summarization whenever possible.

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

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 Resummarize Current Day or EvokeIT Resummarize Past 30 Days** 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**.

Resummarize All Data

This topic describes how to reset summarization data for cases where you might want to resummarize data completely, from scratch.

You can resummarize data by clicking the **Resummarize All Data** button on the Device Power Draws page in the EvokeIT Administrator console, or by running the **EvokeIT Resummarize All Data** Windows task which uses the AdminCommand.exe start_summarization force command.

Note: Do not click **Resummarize All Data** unless you are certain that you want to resummarize data. If you are interested in keeping the historical data in some form, back up the EvokeIT database before resummarizing all of the data.
Any system settings that have changed since the previous summarization process has run will be applied to all historical data in the database. This includes changes to policies and groups.
If you are running the summarization process on the EvokeIT server computer (recommended), be sure to run the process when the EvokeIT server is not required to be active.

To completely resummarize all EvokeIT data:

1. In the EvokeIT Administrator console, on the Configure menu, click **Device Power Draws**.
2. Click the **Resummarize All Data** button.

   Optionally, you can trigger the **EvokeIT Resummarize All Data** task in the Windows Task Scheduler.

   Or, manually resummarize all data by running AdminCommand.exe start_summarization force from the command prompt as an administrator from **C:\Program Files\Verdiem\EvokeIT\Tools** on the EvokeIT server.

To View the Results of the Summarization Task:

- Open the **summarization** log file in **C:\Program Files\Verdiem\EvokeIT\Logs**.

7

Troubleshooting

Table 7-1 In this Chapter

Topics
Administrator Console does not Open in Browser
Configure the Web Server to Allow ASP.NET v.2.0.50727 Applications
Wake for Remote Access Troubleshooting
Timeouts During the Wake Process
Wake for Remote Access Issues Related to the IIS Application
Duplicate Computer Names Returned in Search Results
Using the Wake for Remote Access (WRA) Test Files for Troubleshooting
Advanced Reports Deployment

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:

- *IIS is not Configured to Allow ASP.NET v.2.0.50727 Applications below*
- *ASP.NET is not Registered in IIS below*
- *Multiple Versions of ASP.NET Registered in IIS on the next page*
- *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 the next page*

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.

- Unregister ASP.NET 4.0:

  ```
  C:WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe /u
  ```

- Re-register ASP.NET 2.0:

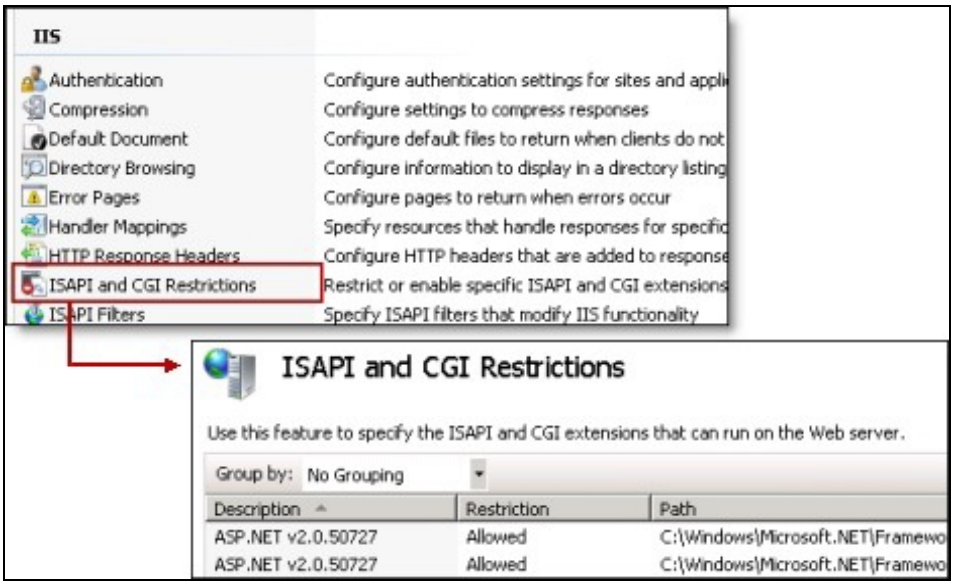
  ```
  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe /i
  ```

Configure 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 7** and above: 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.

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 *AutoPing application settingThe following table lists and defines the WRA application settings that you can customize in IIS Manager*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 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://"font-style: italic;letter-spacing: -1pt;">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.

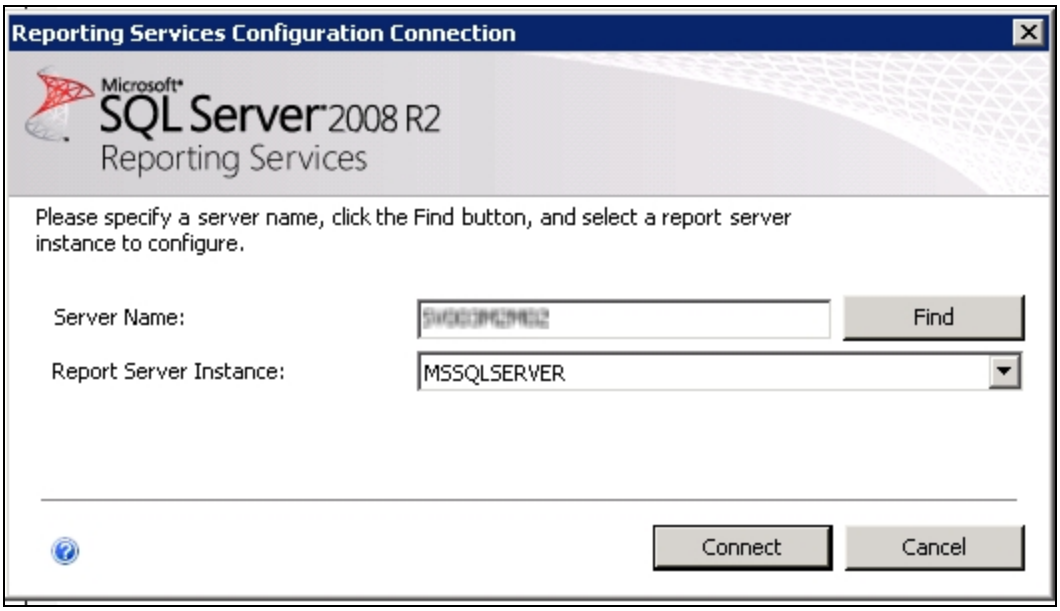
Advanced Reports Deployment

You may have a server setup where the EvokeIT database and SQL Server Reporting Services (SSRS) are hosted on 2 different servers. In such instances, the SSRS may not be able to communicate with the EvokeIT database due to credential issues. Also, there may be instances where the EvokeIT database and SSRS are hosted on the same server, but SSRS may not be able to access the EvokeIT database due to credential issues.

To test EvokeIT database-SSRS connection and restore connection:

1. Click **Start** > **All Programs** > **<Your SQL Server>**> **Configuration Tools** > **Reporting Service Configuration Manager**.

   The **Reporting Services Configuration Connection** window is displayed as seen in the following image.



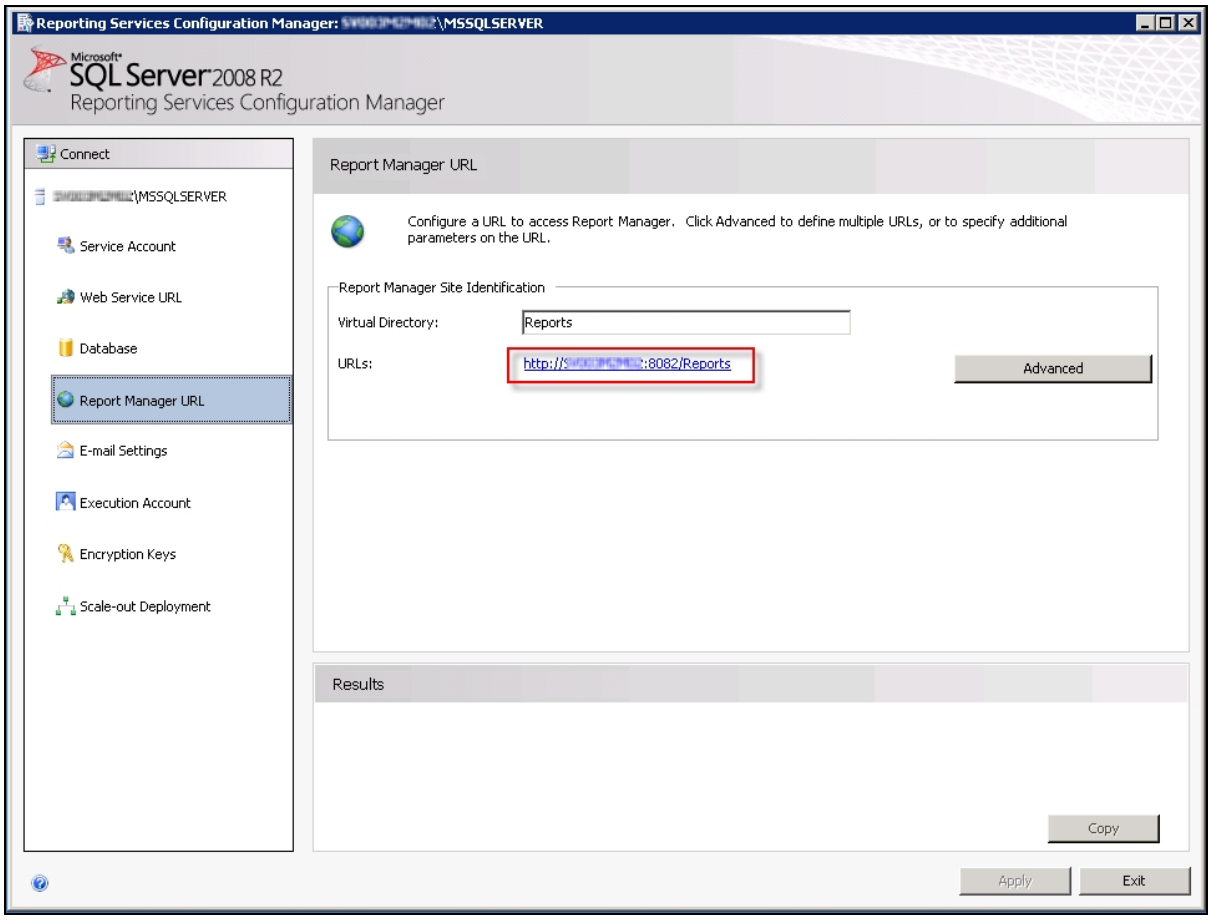
2. Use the following steps to open the **Reporting Services Configuration Manager** window.

   a. In the **Server Name** field, enter your report server name, if the server name displayed is not your report server name.

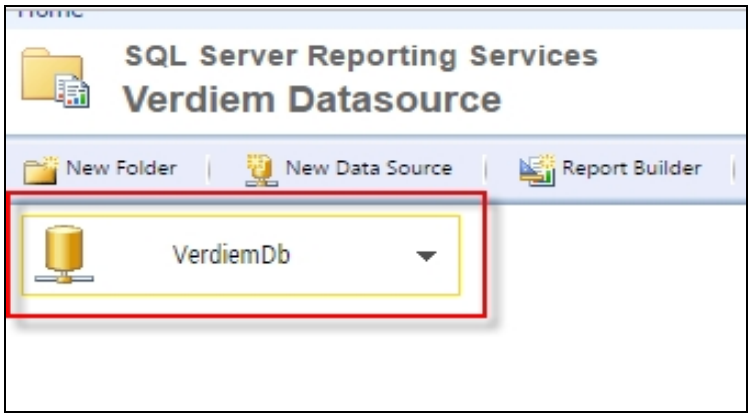
   b. Click **Find** and select the report server instance that you want to configure.

   c. Click **Connect**.

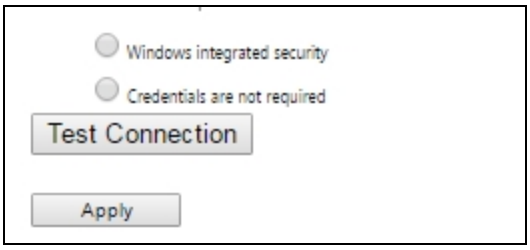
3. In the **Connect** pane, click **Report Manager URL** to open the **Web Service URL** pane.
4. Click the URL in the **Report Manager Site Identification** area as shown in the following image to access the **SQL Server Reporting Services Home** page.



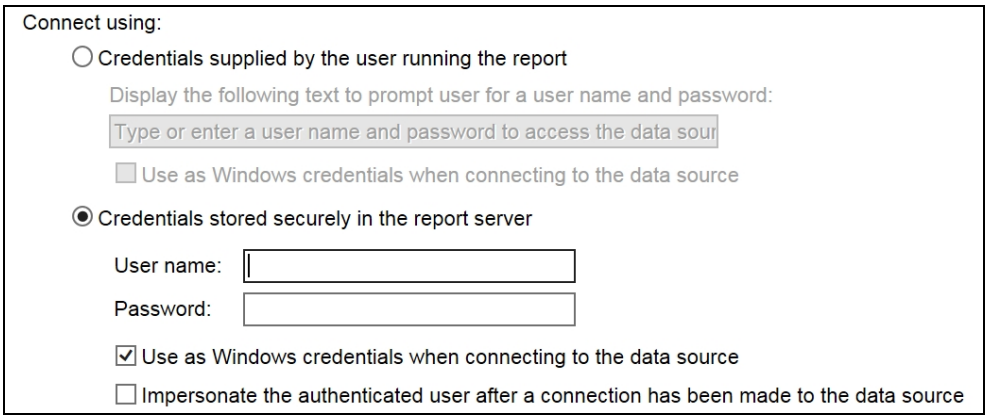
5. Click the **Verdiem Datasource** folder to open the folder.
6. Click **VerdiemDb** to open the **Properties** pane.



7. Click **Test Connection**.



8. Do one of the following:
   - If the connection is successful, your EvokeIT database is connected to SSRS.
   - If the error reads **Login failed for user 'NTAUTHORITY\ANONYMOUS LOGON'**, proceed to the next step.
9. In the **Connect using** area, select **Credentials stored securely in the report server**.



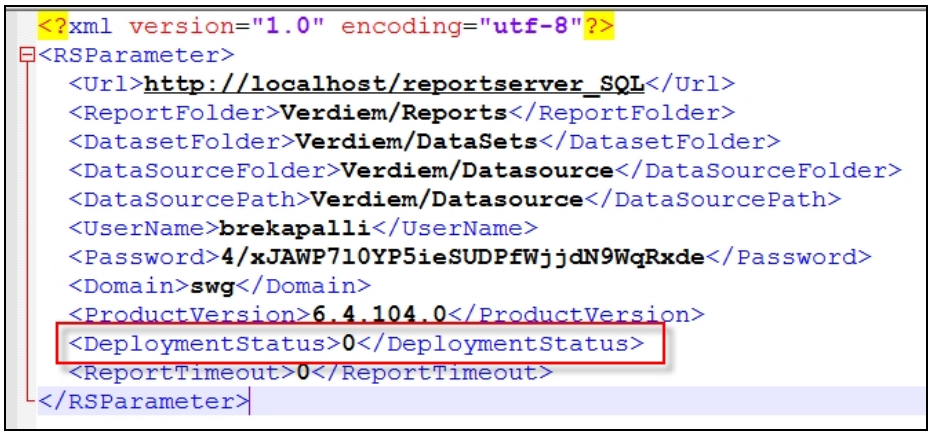
9. Provide valid credentials.
10. Click **Test Connection**.
11. If the connection is successful, click **Apply**.

Exit Codes for Report Deployment

This section contains information about exit code numbers and the meaning of exit codes for report deployment. These exit codes give the status of report deployment. The exit codes are found in the **DepoyReportsConfig.xml** file which is in the following location.

<InstalledLocation>/EvokeIT/Reports

The exit codes are found in the `<DeploymentStatus>` tag as shown in the following image.



The following table contains the exit code numbers and their meaning.

Exit Code Number	Meaning
0	Success
1	SuccessfullyMovedDatasource
2	SuccessfullyDeletedFolders
3	SuccessfullyCreatedFolders
4	SuccessfullyCreatedDataSource
5	SuccessfullyCreatedDataSet
6	SuccessfullyPublishedReports
7	SuccessfullyPublishedImages
8	SuccessfullyUpdatedDataSources
9	SuccessfullyUpdatedDataSets
10	SuccessfullyDeployed
11	Failed
12	RSConnectionFailed
13	IncorrectUriFormat
14	ServiceInitializationFailed
15	FolderNotFound
16	NotAbleToMoveDatasource
17	UnableToDeleteFolder
18	FolderNameIsNull

Exit Code Number	Meaning
19	UnableToCreateFolders
20	ErrorInCreatingDataSource
21	ErrorInCreatingDataSet
22	ErrorInPublishingReports
23	ErrorInPublishingImages
24	ErrorInReadingFiles
25	ErrorInUpdatingDataSources
26	ErrorInUpdatingDataSets
27	InvalidOperation