WebTrends Analytics

Installation and Configuration Guide

March 2006 Edition

Disclaimer

Trademarks

© 1996-2006 WebTrends Inc. All rights reserved.

Contact Information

Sales and General	Support and Services	Online Resources
WebTrends, Inc. 851 SW 6th Ave. Suite 700 Portland OR 97204 Phone: 1-503-294-7025 Fax: 1-503-294-7130 US Toll Free: 1-877-WEBTRENDS (1-877-932-8736) **Email:** marketing@webtrends.com	**Direct Technical Support:** North America and Caribbean: 1-503-223-3023 Central and South America: 1-503-223-3023 Asia Pacific, Australia, New Zealand: 1-503-223-3023 Europe, Middle East, Africa: +44 (0) 1784-463-555	**WebTrends Home Page:** http://www.webtrends.com **WebTrends Support Center:** http://www.webtrends.com/support **WebTrends Professional Services** **(Consulting and Training):** http://www.webtrends.com/services **Online Customer Center:** http://www.webtrends.com/resources

Table of Contents

Chapter 1
About This Book and the Library

This guide is intended to help the WebTrends administrator install and configure WebTrends Analytics, GeoTrends, and SmartSource Data Collector. WebTrends Analytics software and WebTrends Analytics On Demand both offer a variety of powerful analysis and reporting options. The features and reports available to you are dependent on how your company is licensed to use WebTrends. If you have questions about the WebTrends features you are licensed to use, please see your WebTrends administrator.

.

For information about	See
WebTrends Analytics software	"Basic Installation" on page 11 "Distributed Installation" on page 29 "Creating a Profile" on page 95 "Working with the Report Designer" on page 101 "WebTrends User Rights" on page 109
WebTrends Analytics On Demand	"Creating a Profile" on page 95 "Working with the Report Designer" on page 101
GeoTrends	"Installing and Using GeoTrends" on page 91
SmartSource Data Collector	"Basic Installation" on page 11 "Tagging Web Pages for SDC" on page 131 "Operating and Monitoring SDC" on page 111

Intended Audience

This book provides information for administrators who are responsible for installing and configuring WebTrends Analytics software or setting up WebTrends Analytics On Demand.

Other Information in the Library

The library provides the following information resources:

WebTrends Report User's Guide

Helps non-administrators understand and use the Reporting Console to view reports. This guide provides a brief overview of how WebTrends works, how to navigate the Reporting Console, Calendar, and Dashboards to access reports and interact with them to find the information you need.

Note

Users who only have View Reports permissions automatically use the Reporting Console instead of the Administration Console. While they can view the reports, they may not have access to any of the other controls. We recommend distributing the WebTrends Report User's Guide to these users as a introduction to navigating WebTrends reports and report data.

WebTrends Advanced Configuration Guide

A technical reference for administrators who are responsible for maintaining and configuring WebTrends software or WebTrends On Demand

WebTrends SmartView User's Guide

A guide to installing and using SmartView and configuring WebTrends to work effectively with SmartView reporting.

WebTrends Marketing Lab Programmer's Reference

Provides conceptual, procedural, and reference information that allows experienced programmers to customize the WebTrends Marketing Lab reporting environment or set up their own third-party reporting solutions based on WebTrends Marketing Lab data.

WebTrends Guide to Web Analytics

A comprehensive guide for both administrators and non-administrators providing general information and best practices for a successful WebTrends implementation. Topics covered in this guide include how to collect Web traffic data, how to get optimal performance with your Web analysis, considerations to make when setting up your organization to run Web analysis and how to configure WebTrends to give you the information you need.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Providing Feedback

Your comments are very important to us. Please take the time to let us know about your WebTrends experience by doing one of the following:

- From the Administration Console, select **Customer Center** in the left pane. Then click the **Contact Us** link and click **Submit Product Feedback** in the right pane.
- From the Reporting Console, select **Help > Feedback** from the upper right corner of the report.

The Feedback page of the WebTrends web site opens in a new browser window. You can use it to report a bug, request a feature, or give general feedback about your user experience.

The Customer Center

The WebTrends Customer Center brings together a wide variety of materials to help you learn to use WebTrends Analytics more effectively, including white papers, interactive training modules, *How Do I?* Guides, and business case studies. To access the Customer Center, click **Customer Center** in the left pane of the Administration Console.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Lucida Console`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface

Chapter 2
Licensing

In this chapter:

This chapter discusses how WebTrends Analytics software and WebTrends Analytics On Demand are licensed, how product keys are activated in software installations, and where you can view status information for your license.

How WebTrends Software Is Licensed

Your license indicates which report packs, product add-ons, and Marketing Lab Desktop modules you can use. It also determines the number of page views that WebTrends Analytics can analyze during your licensing period. These licensing concepts are described in the following sections.

Report Packs

Report packs are collections of reports that are grouped according to purpose. For example, the Commerce Report Pack includes reports about products and purchase-related visitor segments. Report packs allow you to report on the type information you need and give you the flexibility to expand your reporting with additional report packs as your needs grow.

Product Add-Ons

You can purchase features such as Custom Reporting and Advanced SmartView at a later time if they are not included in your WebTrends Analytics license. With Custom Reporting, you can create your own reports and modify preconfigured reports. Using Advanced SmartView, you view report data superimposed on your web site that includes visitor segment information, such as Buyers and Non-Buyers.

Marketing Lab Desktop Modules

If you purchased WebTrends Marketing Warehouse, your license determines which modules, such as Dashboards and Explore, your license includes.

Page Views

WebTrends Analytics is licensed according to page views analyzed per licensing period. For example, during a 12 month period, your WebTrends activation may be licensed for up to 20 million page views.

In a licensing context, a *page view* is defined as a file with a web page extension (such htm, html, asp) that is requested by a web site visitor to one of the domains being analyzed. Regardless whether WebTrends analyzes web server log files, web data stored in a WebTrends Web Data Warehouse, or SmartSource Data Collector (SDC) data generated by inserted Java Script tags on your web pages, page views are counted from one data source or the other but not both.

If log files are being analyzed and the same log file is processed at a later date by a different profile or by the same profile, the page view is not counted again. Page views are counted prior to applying any customer filters. Although multiple frames on one web page are counted as separate (multiple) page views, you can avoid this if you are using SDC by excluding the WebTrends JavaScript tag from the secondary frames.

Licensing Types

WebTrends Analytics supports two types of licenses: a trial license and a full license.

- Trial

  WebTrends Analytics is available as a 14-day, fully-functioning trial for evaluation purposes. Once this trial period expires, you can convert your installation to full mode when you purchase the fully licensed version and obtain the product license key which enables WebTrends Analytics to run.

- Full

  WebTrends Analytics runs in full mode when the product license key is entered during the installation.

Activating With License Keys

WebTrends requires a product license key to run. During the installation process, you are prompted to enter a license key. If you did not enter the license key during the installation or if you have additional keys for product maintenance, additional page views, report packs, or Marketing Lab Desktop modules, you can enter them through the Licensing dialog box.

Automatically Activating Your License Keys

If you have an Internet connection, you can activate your keys automatically.

To activate a license key automatically:

1. In the left pane of the Administration Console, select **Administration > Licensing**.
2. Select the **License Keys** tab.
3. Click **Add New Keys.** The Activate License Key dialog opens.
4. Type the new key in the **Enter license keys** text box, and click **Activate**. The key appears in the License Keys list, and the status is updated in the **General** tab. If you don't have an Internet connection, you are prompted to manually activate your license key. For more information, see "Manually Activating Your License Key" on page 7.

Manually Activating Your License Key

If you don't have an Internet connection on your WebTrends Analytics computer, you can manually activate your license. You must be able to transfer a file from the computer where WebTrends Analytics is installed to a computer that has an Internet connection.

1. Follow the steps for automatically activating your license. For more information, see "Automatically Activating Your License Keys" on page 7.
2. In the Activate License Key dialog box, right-click the **activation file** link.
3. Select **Save Target As**, and save the `license.htm` file to your computer. You can leave this dialog box open while you complete the following steps.
4. Move the `license.htm` file to a computer that has an Internet connection.
5. Open the file in Internet Explorer. The file connects to the WebTrends Activation Server.

6. When prompted, save the new file to your computer. Name the file `licensechange.txt`.
7. On the computer where WebTrends Analytics is installed save this file to the root of the WebTrends Analytics installation directory..
8. Return to Activate Product dialog box, and click **Activate**.
9. If your license key is successfully activated, the WebTrends Analytics log in page opens.

Deactivating Your License Key

If you need to move the WebTrends Analytics license key from one system to another, you must first deactivate the key. You cannot activate the key on another computer until you do.

To deactivate a key:

1. In the left pane of the Administration Console, select **Administration > Licensing**.
2. Select the **License Keys** tab.
3. Select the WebTrends license key (the first key listed).
4. Click the **Delete** icon . The Confirm Deactivation dialog box opens.
5. Click **OK**. WebTrends Analytics no longer runs until a key is activated on this or another WebTrends computer.

Checking the License Status

You can view the details about your product license in the Administration Console.

To access the Licensing dialogs:

1. In the left pane of the Administration Console, select **Administration > Licensing**.
2. Select the **General** tab.

How WebTrends On Demand Is Licensed

Your license indicates which report packs and Marketing Lab Desktop modules you can use as well as the number and type of profiles you can create. It also determines the number of page views that WebTrends On Demand collects during your licensing period before you are charged for any additional page views. These licensing concepts are described in the following sections.

Report Packs

Report packs are collections of reports that are grouped according to purpose. For example, the Commerce Report Pack includes reports about products and purchase-related visitor segments. Report packs allow you to report on the type information you need and give you the flexibility to expand your reporting with additional report packs as your needs grow.

Product Add-Ons

You can purchase features such as Custom Reporting and Advanced SmartView at a later time if they are not included in your WebTrends Analytics license. With Custom Reporting, you can create your own reports and modify preconfigured reports. Using Advanced SmartView, you view report data superimposed on your web site that includes visitor segment information, such as Buyers and Non-Buyers.

Marketing Lab Desktop Modules

If you purchased WebTrends Marketing Warehouse, your license determines which modules, such as Dashboards and Explore, your license includes.

Profiles

Your license determines the number of profiles you can create. Your total number of profiles available can be distributed to your child accounts (sub accounts within your main license).

Parent-Child profiles that you create count towards the total number of profiles you are licensed for in one of two ways. How the profile is counted depends on whether the Parent-Child profile uses Basic Analysis or Full Featured Analysis.

A Parent-Child profile using Basic Analysis with up to 10 child profiles counts as one profile. Each group of 10 additional child profiles counts as one additional licensed profile. For example, a Parent-Child profile using Basic Analysis with between 11 and 20 children counts as 2 profiles. A Parent-Child profile using Basic Analysis with between 21 and 30 children counts as 3 licensed profiles, and so on.

For a Parent-Child profile using Full Featured Analysis, each child profile counts as one profile. For example, a Parent-Child profile using Full Featured Analysis with 3 children counts as 3 licensed profiles.

Report Exports

Your license determines the number of report exports that you can use each month. Once that limit is reached, you can purchase additional report exports.

Checking the License Status

The **Edit Account** dialog box in the Account Console allows you to view the status of your profiles, custom reports, and report export limits.

To access the Edit Account dialog box:

1. From the Account Console, select **Account > Edit Account** in the left pane.
2. Select the **Settings** tab.

Checking Your Page View Balance

You can view your current page view balance in the Account Console.

To view your page view balance:

In the left pane of the Account Console, select **Account Usage > Summary**. Use this dialog to view:

- Page views collected so far during the current month
- Page views collected for the calendar year to date
- Pages views collected during the life of your account.

Chapter 3
Basic Installation

This chapter provides the information you need to install WebTrends Analytics software, WebTrends Analytics sample data, and WebTrends SmartSource Data Collector.

A basic installation installs all WebTrends Analytics software on a single computer and the optional SmartSource Data Collector on another dedicated computer. If you plan to install WebTrends Marketing Warehouse, you must perform a custom installation. For information about custom or distributed installation, see "Distributed Installation" on page 29.

Preparing for a Basic Installation

Before installing WebTrends, complete the following checklist:

- Review the hardware, operating system, and browser requirements to ensure optimum performance of WebTrends. For more information, see "Minimum System Requirements" on page 13.
- Determine your needs for storing WebTrends system data. For more information, see "Assessing Your Storage Needs" on page 12.
- Set up shares for WebTrends data. For more information, see "Setting Up Shares for Data" on page 13.
- Collect all valid license keys for the product, add-on licenses, or subscriptions.
- If anti-virus software is installed on your WebTrends-dedicated computers, decide whether you want to disable it. If the anti-virus software is activated when you install WebTrends, the installation program warns you that it may conflict with analysis. For more information, see "WebTrends and Anti-Virus Software" on page 12.

You can then choose from the following installation paths to install WebTrends, including the SmartSource Data Collector (SDC) and GeoTrends:

- "Installing WebTrends Analytics Software" on page 20 (this includes GeoTrends)
- "Installing WebTrends Sample Data" on page 25

- “SmartSource Data Collector Installation” on page 49

WebTrends and Anti-Virus Software

We recommend disabling anti-virus programs on your WebTrends computers because virus scanning can lock files that WebTrends needs. If the anti-virus program locks even a few files during a WebTrends analysis, WebTrends’ inability to write to these files can cause analysis to be incomplete and fail. Although the presence of anti-virus software does not guarantee a failure, running anti-virus and WebTrends on the same computer is not recommended.

Rather than disable virus scanning, you can configure the program not to scan log files, data files, or configuration files. (Depending on your WebTrends installation, some of these files may be located on network drives or, in a distributed installation, on other computers.) However, anti-virus software can safely scan WebTrends executables.

Although you can set your anti-virus program to run when WebTrends is not analyzing data, or to exclude the directory where WebTrends is installed, WebTrends generates alerts based on whether anti-virus is running on the same computer as WebTrends. You can use the Alert Configuration dialog box to change the default response to anti-virus scanning. For more information about managing alerts, see Help after you install WebTrends.

Assessing Your Storage Needs

Consider dedicating machines for storing your WebTrends data. As a general rule, plan on 5 GB of data per profile each year. You can store each repository on a separate machine if necessary. During the installation, you specify storage locations for the following repositories:

Analysis Data Repository
Stores the data that is processed to generate reports; accessed primarily by the Analysis engines. How much data is stored depends on a number of variables including the amount of Web site traffic, table limit settings, the quantity and complexity of your custom reports, and if you use WebTrends Visitor History feature, the amount of visitor history data that you store.

Report Data Repository
Stores the data used to display reports; is accessed by the UI Server and the Analysis engines. The size of the Report Data repository depends on the number of custom reports, your table limit settings, and the report period and storage profile settings.

Configuration Repository
Stores the settings WebTrends needs in order to run; these flat files require relatively little storage space.

Backup Repository

The backup repository contains WebTrends configuration data that can be used to restore your WebTrends installation if necessary. By default, WebTrends maintains seven daily backup archives and four weekly archives for each profile.

Setting Up Shares for Data

During the installation process, you are asked to specify the storage locations for the WebTrends data repositories discussed in the previous section. Because each path must be accessible by each machine that is part of the installation, be sure you set up these locations as shared folders before beginning the installation.

For example, to store data on the Main Application computer that has a name of “wtmain”, the shares could be:

```
\\wtmain\analysis

\\wtmain\report

\\wtmain\config

\\wtmain\backup
```

Note

WebTrends does not support administrative shares, such as `\\systemname\c$`.

Minimum System Requirements

WebTrends Analytics is a powerful application that you should install on a dedicated computer.

WebTrends Analytics Requirements

The following table shows minimum requirements for WebTrends Analytics software and provides suggestions about how to estimate the requirements for a larger implementation.

Hardware	Software	Sizing Guidelines
--Dual 2.0 GHz or higher processors --1 GB of RAM* --80 GB of usable hard disk space (7200 RPM RDE) --100 Mbps network interface card *In order to run multiple analyses on the same computer, WebTrends Analytics requires at least 3 GB of RAM and the /3GB switch in the BOOT.INI file.	**Supported Operating Systems** --Windows XP and Windows XP x64 with Service Pack 2 or higher --Windows 2003 and Windows 2003 x64 **Supported Browsers** --Microsoft Internet Explorer v6.0 or higher --Mozilla Firefox v1.5 or higher **Supported Databases** --MySQL (included) --Microsoft SQL Server 2000* with Service Pack 2 or higher (dedicated database required) --Microsoft SQL Server 2005* (dedicated database required) *If you choose to use Microsoft SQL Server, you must install it before you install WebTrends. The SQL Server installation in question must be a system dedicated to storing and supporting only WebTrends related databases. While SQL Server has the ability to maintain multiple databases, the system resource and configuration requirements of the WebTrends database server environment demand a dedicated database server environment to assure proper performance and reliability. **Note:** If you want to convert WebTrends reports to Microsoft Word or Excel format or use WebTrends SmartReports for Microsoft Excel, WebTrends also requires Office XP or Office 2003 or higher and the Sun Java Runtime Environment v1.4.2_05 or higher (v1.5.0_03 recommended).	Requirements are based on 5 profiles, 2 concurrent users, and up 100,000 daily page views. --To run GeoTrends on the same computer as WebTrends, add 1 GB of RAM. --To run GeoTrends and process more than 100,000 page views a day, add 2 GB of RAM. --Advanced reporting features require additional hardware. Contact your WebTrends account manager for more information.

WebTrends Reporting Console Requirements

The following table shows minimum requirements for the Reporting Console, which is used to view WebTrends HTML reports.

Hardware	Software
256 MB of RAM (512 MB of RAM recommended)	**Supported Operating Systems** --Windows XP and Windows XP x64 with Service Pack 2 or higher --Windows 2003 and Windows 2003 x64 --Mac OS X 10.3.9 or higher or higher with Apple's Java v1.4.2_05 or higher and Mozilla Firefox v1.5 or higher --Mac OS X 10.4.4 or higher with Apple's Java v1.4.2_05 or higher and Mozilla Firefox v1.5 or higher **Supported Browsers (Windows)** --Microsoft Internet Explorer v6.0 or higher with Sun Java Runtime Environment v1.4.2_05 or higher (v1.5.0_03 recommended). The correct version of the Java Runtime Environment is installed with WebTrends. --Mozilla Firefox v1.5 or higher **Notes** --If you want to convert WebTrends reports to Microsoft Word format, WebTrends requires Office XP or Office 2003. --If you want to convert reports to WebTrends SmartReports for Microsoft Excel, WebTrends requires Office 2003. **Supported Browsers (Mac)** --Mac OS X 10.3.9 or higher with Apple's Java v1.4.2_05 or higher and Mozilla Firefox v1.5 or higher. --Mac OS X 10.4.4 or higher with Apple's Java v1.4.2_05 or higher and Mozilla Firefox v1.5 or higher. **Notes**: --In addition, you must install the Java Embedding Plug-in. --The Reporting Console does not support report exports from Mac browsers.

WebTrends Marketing Lab Desktop Requirements

The following table shows minimum requirements for WebTrends Marketing Lab Desktop and provides suggestions about how to estimate the requirements for a larger implementation.

Hardware	Software
--1.8 GHz or higher processor --512 MB of RAM (1 GB recommended) --50 MB of usable hard disk space (7200 RPM IDE) --100 Mbps network interface card	**Supported Operating Systems** --Windows XP and Windows XP x64 with Service Pack 2 or higher --Windows 2003 and Windows 2003 x64 **Notes** --WebTrends Marketing Lab Desktop also requires Microsoft .NET Framework 1.1 Service Pack 1 or higher. --WebTrends Marketing Lab Desktop requires Macromedia Flash v7 or higher. If the required version is not detected, you are prompted to download and install the latest version.

WebTrends Marketing Warehouse Requirements

The following table shows minimum requirements for WebTrends Marketing Warehouse and provides suggestions about how to estimate the requirements for a larger implementation.

Hardware	Software
--2.4 GHz Dual Core or Dual 2.4 GHz or higher processors --6 GB of RAM --450 GB of usable hard disk space (SCSI 0+1) --100/1000 Mbps network interface card	**Supported Operating Systems** --Windows 2003 and Windows 2003 x64

SmartSource Data Collector Requirements

The following table shows minimum requirements for SmartSource Data Collector and provides suggestions about how to estimate the requirements for a larger implementation.

Hardware	Software
--Windows: 1.0GHz or higher processor --1 GB of RAM --Enough disk space to store the expected contents of your log files (7200 RPM IDE) --100 Mbps network interface card	**Supported Operating Systems** --Windows XP and Windows XP x64 with Service Pack 2 or higher --Windows 2003 and Windows 2003 x64 **Supported Browsers** --Microsoft Internet Explorer v6.0 or higher --Mozilla Firefox v1.5 or higher **Supported Web Servers** --Apache Web Server v2.0.55 --Microsoft Internet Information Server v6.0

GeoTrends Requirements

The following table shows minimum requirements for GeoTrends and provides suggestions about how to estimate the requirements for a larger implementation.

Hardware	Software
--1.0 GHz or higher processor --1 GB of RAM --30 GB of free hard disk space (7200 RPM IDE) --100 Mbps network interface card	**Supported Operating Systems** --Windows XP and Windows XPx64 with Service Pack 2 or higher --Windows 2003 and Windows 2003 x64

SmartView Requirements

The following table shows minimum requirements for SmartView.

Software	WebTrends Version
Supported Operating Systems --Windows XP with Service Pack 2 or higher --Windows 2003 **Supported Browsers** Microsoft Internet Explorer v6.0 or higher with Java 2 Platform, Standard Edition, 1.4.2_05 or higher **Note**: SmartView does not support Mozilla Firefox.	The version of SmartView that you are running must be the same version as your WebTrends Analytics version.

SmartReports Requirements

The following table shows minimum requirements for SmartReports.

Software	WebTrends Version
Supported Operating Systems --Windows XP with Service Pack 2 or higher --Windows 2003 **Required Java Version** (for exporting data only) Sun Java Runtime Environment v1.4.2_05 or higher **Required Microsoft Office Version** Microsoft Office 2003	The version of SmartReports that you are running must be the same version as your WebTrends Analytics version.

Express Viewer

The following table shows minimum requirements for Express Viewer.

Software	WebTrends Version
Supported Operating Systems --Windows XP with Service Pack 2 or higher --Windows 2003 **Required Java Version** Java 2 Platform, Standard Edition, 1.4.2_05 or higher	The version of Express Viewer that you are running must be the same version as your WebTrends Analytics version.

Deciding What Ports to Use

WebTrends Analytics uses ports to communicate with all the components in your installation. Review this section to make sure that other services that you plan to run on your WebTrends computers do not conflict with these ports.

During installation, you can configure the following ports:

- System Database
- User Interface Server

After installation, you can modify the following ports:

- GeoTrends Server
- Report Cache Server
- User Interface Server

For more information, see "Modifying the Ports WebTrends Uses" on page 47.

The following table shows the default port for each WebTrends component.

Component	Default Port	Configurable
GeoTrends Server	7199	Yes
Report Cache Server	7299	Yes
System Database	Microsoft SQL Server: 1433 MySQL Server: 3306	Yes
User Interface Server	Microsoft ISS/Apache port: 7099 SSL port: 9443 **Note**: The Apache port is commonly configured to use port 80 and the SSL port is commonly configured to use port 443.	Yes

In addition, WebTrends Analytics needs to be able to access the WebTrends data stored on your network. This data is stored in the repositories discussed earlier in this chapter. For more information, see "Assessing Your Storage Needs" on page 12. WebTrends runs on Windows which uses the Server Message Block (SMB) protocol to access network data. Your network administrator can tell you which port your version of Windows uses.

Installing WebTrends Analytics Software

This section describes how to install WebTrends Analytics and the optional GeoTrends component on a single computer.

- For more information about installing SmartSource Data Collector (SDC), see "SmartSource Data Collector Installation" on page 49.
- For more information about installing the optional WebTrends Analytics samples, see "Installing WebTrends Sample Data" on page 25.
- For more information about performing a custom installation and installing WebTrends components on separate computers, see "Distributed Installation" on page 29.

If you are completing these steps to upgrade your installation, you must stop the required services before installing the upgrade.

To stop the required services:

1. From the Windows Services panel, select and stop the following services:
   - WebTrends User Interface Service
   - WebTrends Schedule Agent
   - WebTrends Tomcat
2. Make sure that the WebTrends MySQL Service is started. If not, restart it before installing the upgrade.
3. Complete the steps described in the following section.

To install WebTrends:

1. ***If you downloaded your software from the WebTrends Web site:***
   a. On the computer where you want to install the WebTrends Main Application, open the downloaded installation file.
   b. Unzip the files either to the default location or to the location of your choice. When the files are unzipped, the installation program starts automatically.
2. ***Otherwise***, on the computer where you want to install the WebTrends Main Application, insert the WebTrends Analytics software CD-ROM into your CD-ROM drive. If your computer is set up to use auto-run, the installation program is automatically launched. If not, choose **Run** from the File or Start menus and type:

   ```
   X:\setup
   ```

   where `X` is the drive letter of your CD-ROM drive. The installation program starts.
3. Click **Next** to continue.
4. Before the WebTrends program files are copied to your computer, you must accept the Software License Agreement. ***If you agree to the stated terms***, select the **I accept the terms in the license agreement** option, and click **Next**. ***Otherwise***, click **Cancel** to exit the installation program without installing the software.

5. In the Add Licenses dialog box, type a valid license key in the text box and click **Add License**. Repeat this step for each license key, add-on license, and subscription license that you have. Contact WebTrends Support if you do not have a valid license key.

Note

The computer must have an Internet connection in order to automatically activate a license key. If you do not have an Internet connection on this computer, you can manually activate the license key. For more information, see "Manually Activating Your License Key" on page 7

---

6. In the Select Installation Type dialog box, select the installation method you want to use.

   a. ***If you want to install only the required components on a single computer***, select **Typical**. If you select this option, be aware that the Express Analysis Engine, GeoTrends Server, and the Marketing Warehouse components are not installed.

   b. ***If you want to install WebTrends components on a single computer and specify which components are installed***, select **Custom**. Select this option if you are installing WebTrends Marketing Warehouse.

   c. ***If you want to install the WebTrends components across multiple computers***, see "Distributed Installation" on page 29.

7. The Destination Folder dialog box opens showing the directory location where the WebTrends components are installed by default.

   a. ***If you want to accept the default installation directory***, click **Next**.

   b. ***If you want to install WebTrends in a different directory***, click **Change** and browse to your preferred location. Click **OK** to save the new location and click **Next**.

8. ***If you selected Typical for the installation type,*** in the Application Selection dialog box, specify which components you want to install on this computer:

   a. ***If you want to install the main WebTrends application***, select the **WebTrends core application** check box. The core application is the WebTrends foundation and is required for a Typical installation.

   b. ***If you want to install the GeoTrends Server***, select the **GeoTrends** check box. Select this option if you want to add geographical data about your visitors to your reports.

c. ***If you plan to use SmartSource Data Collector (SDC) to collect web traffic data***, select the **SmartSource Data Collector** check box. SDC uses JavaScript tags placed on your Web pages as an alternative method to reporting on Web server log files.

Note

Because SDC receives traffic from outside of your firewall, you should install it on a dedicated computer.

---

9. ***If you selected Custom for the installation type***, the Custom Setup dialog box opens. If you are installing WebTrends on a single computer, select the components that you want to install. If you want to install WebTrends on multiple computers see the guidelines and procedures in "Distributed Installation" on page 29.

10. In the Specify WebTrends Service Parameters dialog box, specify the type of account that WebTrends services should use.

    a. ***If you are storing WebTrends data on a network location or if you plan to schedule report exports to Microsoft Word of Excel formats,*** select **Domain User Account**. This option allows WebTrends to use resources on shared network directories. Type the user name, password, and domain for an account that has read and write permissions for any shared directories WebTrends will use. Click **Next**.

    b. ***If you are installing WebTrends on a single computer and plan to store data locally***, you can select **Local System Account**. Be aware that if you select this option, you cannot schedule Microsoft Word or Excel report exports because these programs require a domain account to run. Click **Next**.

11. ***If you selected GeoTrends in Step 8***, you are prompted to do one of the following:

    a. ***If you want WebTrends to use the latest version of the GeoTrends data file***, click **Download**. Save the file to a location accessible by the WebTrends computer.

    b. ***If you want to use the GeoTrends data file provided on your WebTrends CD-ROM***, locate the `geotrends.dat` file on the CD-ROM.

    c. Click **Next**.

12. The System Database Initialization dialog box opens showing the host, port number, and administrator information. The default port for MySQL server is 3306. Enter and confirm your database password, and click **Next**.

Note

In this dialog box, you are specifying the password for the database, not your login password for the WebTrends User Interface. If this is a subsequent WebTrends installation, only the information specified during the first installation is valid. See your WebTrends administrator if you have questions.

---

13. In the WebTrends Data and Environment Locations dialog box, specify the storage locations for each repository. For more information, see "Assessing Your Storage Needs" on page 12.

    Each path must be accessible by the WebTrends computer. If you add additional computers to your installation later, those computers need access to these shared locations. Specifying these paths using Universal Naming Convention (UNC) simplifies adding computers to your installation. For more information, see "Setting Up Shares for Data" on page 13.

    Click **Next** to continue.

14. ***If your computer does not meet the minimum system requirements***, the installation program shows which requirements were not met. Only install WebTrends Analytics on a dedicated computer that meets the minimum system requirements.

15. You are prompted to return to previous dialog boxes if you need to edit your installation choices. If you do not need to make any changes, click **Install**. The WebTrends Analytics program files are installed to your computer.

16. The Download Sample Data dialog box allows you to download the WebTrends sample files that show how to set up features and demonstrate available reports. If you want to download WebTrends sample data, click **Download Sample**. Otherwise, click **Next** and continue with Step 17.

    a. Select a sample to download.

    b. Click **Save**, and specify where you want to save the file. By default, the file is saved to your computer desktop.

    c. After the WebTrends Analytics installation program finishes, you can install the samples that you downloaded. For more information, see "Installing WebTrends Sample Data" on page 25.

17. ***If you have only chosen to install WebTrends and the optional GeoTrends data file***, you are notified that the installation is complete. You are prompted to view and read the release notes. Click **Finish** to close the installation program.

18. ***If you selected SmartSource Data Collector in Step 8***, the installation wizard for SmartSource Data Collector starts. For more information, see "SmartSource Data Collector Installation" on page 49.

Activating Your License

When you first start WebTrends Analytics, if you did not provide a valid license key during installation, you have to provide a valid license key, legacy serial numbers, or add-on keys in order to register the product. After WebTrends accepts the license key, the **Login** window opens.

You can then provide your WebTrends user name and password to log into WebTrends. (If you do not have this information, please see your WebTrends administrator.)

Installing WebTrends Sample Data

You can install WebTrends sample data from either the WebTrends CD-ROM or the WebTrends web site. Install WebTrends before installing the sample data.

To install a sample:

1. Locate the sample data using one of these methods:
   - ***If you downloaded the sample files during the WebTrends Analytics installation,*** locate the EXE file that you saved. By default, the samples are saved to your computer desktop. Continue with Step 3.
   - ***If you want to install the samples from WebTrends CD-ROM***, insert the CD-ROM, and from the window that opens, select **Miscellaneous**.
   - ***If you want to install the samples from the WebTrends web site***, log in to the WebTrends Administration Console. In the left pane select, **Install Components > Accessories**, and select **Sample Downloads**.
2. Click the link for the sample you want to download.
3. Double-click the sample executable file if you downloaded it. The installation program starts.
4. Click **Next**.

5. Before the samples are copied to your computer, you must accept the License Agreement. If you agree to the stated terms, select **I accept the terms of the license agreement**, and click **Next**. Otherwise, click **Cancel** to exit the installation program without installing the samples.
6. The Custom Setup dialog box opens. Select the samples you want to install, and click **Next**.
   - If you are unfamiliar with this type of installation program, click **Help** for details on the different selection options you can choose from.
   - If you are unclear how much storage space you have available, click **Space**. The installation program lists the available data space and requirement for each volume you have access to. (You can select the columns to sort this data.) When you are finished reviewing this information, click **OK**.
7. ***If you want to review or change any of your choices***, click **Back**. ***Otherwise***, click **Install**.
8. You are notified when the installation is complete. Click **Finish** to close the wizard.

To analyze sample data for viewing reports:

1. Log in to WebTrends Analytics.
2. In the left pane, click **Reports & Profiles**.
3. Click the **Analyze Now** icon for each of the sample profiles.

Viewing WebTrends Reports

After you install WebTrends sample data or create and run a profile, you can view reports.

To view your reports:

1. Log in to the WebTrends Administration Console.
2. In the left pane, click **Reports & Profiles**.
3. Select a profile in the list and click the profile name.

Adding Components After Installation

You can install additional WebTrends Analytics components such as GeoTrends after the main installation is complete.

To add a WebTrends component:

1. Insert the WebTrends software CD-ROM into the CD-ROM drive. If your system is set up to use auto-run, the installation program starts automatically. If not, select **Run** from the File or Start menus and `type x:\setup` where `x` is the drive letter of your CD-ROM drive.
2. The installation wizard opens. Click **Next** to continue.
3. The Program Maintenance dialog box opens. Select **Modify**, and click **Next**.
4. Click the icon next to the component that you want to install, and select **Install or maintain this component**. Click **Next** to continue.
5. Complete the steps in the installation wizard. For more information, see “Installing WebTrends Analytics Software” on page 20.

Chapter 4
Distributed Installation

This chapter provides an overview of WebTrends distributed architecture and describes how to install WebTrends Analytics software and the Marketing Warehouse in a distributed environment. Issues that involve upgrading and managing your distributed installation are discussed at the end of the chapter.

You can distribute work across multiple computers by installing WebTrends components on several machines that work together as one. You might use a distributed installation to handle many complex analysis processes, a large number of concurrent users viewing reports, or to analyze more web site traffic than a non-distributed installation can process in a single day. If you plan to use the WebTrends Marketing Warehouse, you must install WebTrends Analytics and the Marketing Warehouse on separate, dedicated systems.

Your web site traffic and your reporting needs determine the number of computers in your WebTrends installation. A distributed architecture provides the flexibility to run components in the configuration that works best for your organization, whether that means installing a multiple components on a computer or that means installing a single component (such as the Analysis component) on multiple computers. WebTrends components are discussed in detail in the following section, "Planning a Distributed Installation" on page 29.

Planning a Distributed Installation

This section describes the planning needed before you complete the distributed installation.

Understanding WebTrends Components

To plan your distributed installation, familiarize yourself with WebTrends components. This section provides general guidelines for a distributed installation. Use the WebTrends System Check Tool to help determine the number of machines you need for these components. For more information, see "Using the System Check Tool" on page 34.

Main Application

Generates and displays WebTrends reports and performs miscellaneous product housekeeping. Unless otherwise indicated by the System Check Tool or another form of needs assessment, install the Main Application and its sub-components on the same computer.

System Database

Stores data WebTrends Analytics needs in order to coordinate work for all components. For more information, see "Selecting a System Database" on page 32.

User Interface (UI) Server

A sub-component of the Main Application that generates WebTrends reports. The number of users who view reports concurrently determines the number of computers that you need running this component. You may want to install the UI Server separately so that report viewing is not affected by the work of other components such as Analysis. The System Check Tool can help you determine if you need multiple computers running the UI Server.

Analysis Engine

Performs the analysis of your web traffic data. The System Check Tool can help determine if you need multiple computers running the Analysis. The Analysis component includes a Standard Analysis engine that performs scheduled analysis of your web traffic data, and the Express Analysis engine that provides on-going analysis of your web traffic data for limited, current day only reporting. If you plan to use Express Analysis, you will need to install the Express Analysis component.

Marketing Warehouse

Prepares log files for being imported and stored in a MySQL database to allow customized data exploration. The Log File Management component pre-processes your SmartSource Data Collector log files, formatting them and making them available to the Event Database. The Event Database component includes the Event Database Server/Event Database Loader, which creates the logical MySQL database where the Event Database resides and moves event data from log files to an Event Database.

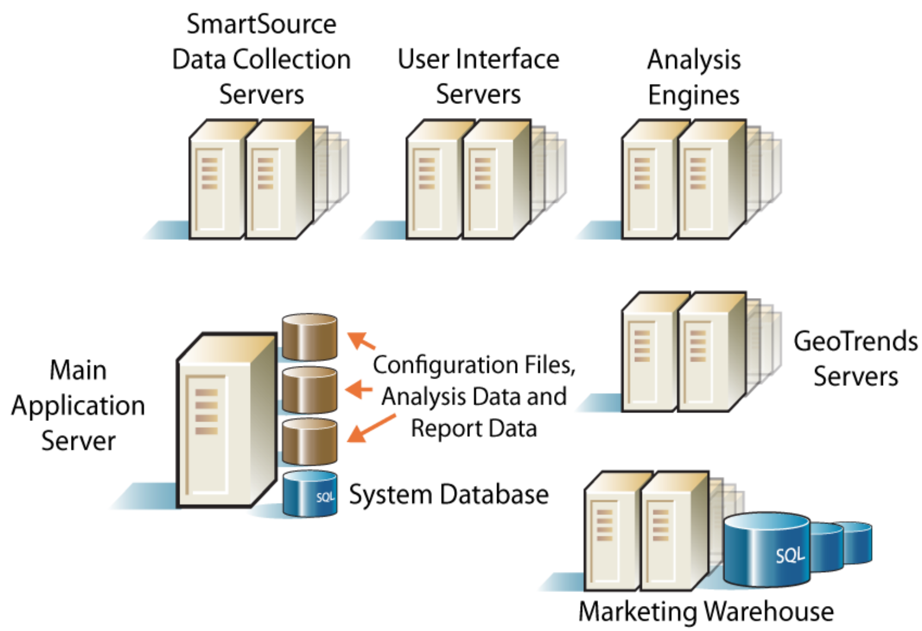
SmartSource Data Collector (SDC)

Collects web traffic data using JavaScript tags placed on your web pages. This method is an alternative to reporting on web server log files. Because SDC receives traffic from outside of your firewall, you should install it on a dedicated machine. SDC is required if you plan to use the Marketing Warehouse.

GeoTrends Server

An optional component that adds geographical data about your visitors to reports. If you want this geographic information, and your web site receives a lot of visitors, then you may want to install GeoTrends on a separate computer. Doing so allows GeoTrends to run without taking memory away from other important components. Otherwise, install GeoTrends on the machine running the Analysis Engine.

The following graphic shows WebTrends components in one possible distributed configuration:



Selecting a System Database

WebTrends Analytics uses a small database for system and configuration data. The database coordinates the work of all other components. You can use either the MySQL database that is included with WebTrends Analytics or your own Microsoft SQL Server database.

If you choose to use Microsoft SQL Server, you must install it before you install the WebTrends Main Application component. The SQL Server installation in question must be a system dedicated to storing and supporting only WebTrends related databases. While SQL Server has the ability to maintain multiple databases, the system resource and configuration requirements of the WebTrends database server environment demand a dedicated database server environment to assure proper performance and reliability. For more information, see “Preparing a Microsoft SQL Server Installation” on page 36.

Planning Your Marketing Warehouse

The WebTrends Marketing Warehouse includes two separately installable components: the Event Database Server/Event Database Loader component, which runs on a dedicated system, and the Log File Management component (consisting of the Event Database Splitter and the Log File Pre-Processor), which you can install on a separate system. The database can only be used by WebTrends Analytics for storing your event data. For information about implementing WebTrends Marketing Warehouse including tagging your web site and using the required WebTrends query parameters, see “Implementing WebTrends Marketing Warehouse” on page 65.

Planning for Log File Storage

As a best practice, you should store your log files on a network location that the WebTrends systems can access. Typically, this is accomplished by storing log files on a shared drive.

How much storage you need depends largely on your site traffic and how long you plan to store your processed log files. For more information about optimizing log file storage, see “Optimizing Your Analysis Environment” in the *WebTrends Advanced Configuration Guide*.

If you use the Marketing Warehouse, you need to consider your storage requirements for the unmodified SmartSource Data Collector (SDC) log files. Because the Log File Management component modifies the log files to prepare them for the Marketing Warehouse, you should store the SDC log files separately and copy them at regular intervals to a location where the Log File Pre-Processor can add GeoTrends and DNS data to the logs, and the Event Database Splitter can collect them and process them. By default, the Event Database Splitter deletes the processed log files after the Event Database Loader imports the event data into the Event Database. However, you can configure the Log File Management host role to keep the processed log files if you want to use them to create HTML reports. For more information, see "Configuring the Log File Management Role Settings" on page 71.

Assessing Your Data Storage Needs

Consider dedicating machines for storing your system and configuration data. As a general rule, plan on 5 GB of data per profile each year. You can store each repository on a separate system if necessary. During the installation, you specify storage locations for the following repositories:

Analysis Data Repository
: Stores the data that is processed to generate reports; accessed primarily by the Analysis engines. How much data is stored depends on a number of variables including the amount of web site traffic, table limit settings, the quantity and complexity of your custom reports, and if you use WebTrends Visitor History feature, the amount of visitor history data that you store.

Report Data Repository
: Stores the data used to display reports; is accessed by the UI Server and the Analysis engines. The size of the Report Data repository depends on the number of custom reports, your table limit settings, and the report period and storage profile settings.

Configuration Repository
: Stores the settings WebTrends needs in order to run; these flat files require relatively little storage space.

Backup Repository
: Contains WebTrends configuration data that can be used to restore your WebTrends Analytics installation if necessary. By default, WebTrends maintains seven daily backup archives and four weekly archives for each profile.

Event Database Source Directory

Contains your SmartSource Data Collector log files, which are the source for your Marketing Warehouse profiles. Marketing Warehouse components process the log files located in this directory and import them into your Marketing Warehouse. For more information, see "Planning for Log File Storage" on page 32.

Using the System Check Tool

The WebTrends System Check Tool can help determine the hardware requirements for your distributed installation. You provide information about how you plan to use WebTrends, and the System Check Tool provides the minimum system requirements for each type of computer it recommends. The more familiar you are with WebTrends concepts, the better the results it provides. You can then use this information to plan how the software is distributed over your machines.

To access this tool:

- WebTrends CD-ROM
- http://product.webtrends.com/ptw.aspx?action=42&prodtype=wrc

When answering the System Check Tool questions, consider not only your immediate needs but also how they might change as your web site and your reporting requirements grow.

Deciding Which Ports to Use

WebTrends uses ports to communicate with all the components in your installation. Review this section to make sure that other services that you plan to run on your WebTrends computers do not conflict with these ports.

During installation, you can configure the following ports:

- Event Database Server (Marketing Warehouse installations only)
- System Database
- User Interface Server

After installation, you can modify the following ports:

- GeoTrends Server
- Report Cache Server

- User Interface Server

For more information, see “Modifying the Ports WebTrends Uses” on page 47.

The following table shows the default port for each WebTrends component.

Component	Default Port	Configurable After Installation
Event Database Server	3307	No
GeoTrends Server	7199	Yes
Report Cache Server	7299	Yes
System Database	Microsoft SQL Server: 1433 MySQL Server: 3306	Yes
User Interface Server	Microsoft IIS/Apache port: 7099 SSL port: 9443 **Note**: The Apache port is commonly configured to use port 80 and the SSL port is commonly configured to use port 443.	Yes

In addition, WebTrends needs to be able to access the WebTrends data stored on your network. This data is stored in the repositories discussed earlier in this chapter. For more information, see “Assessing Your Data Storage Needs” on page 33. WebTrends runs on Windows which uses the Server Message Block (SMB) protocol to access network data. Your network administrator can tell you which port your version of Windows uses.

Preparing for a Distributed Installation

Once you have completed your plan for the WebTrends installation, prepare the system database and configure file sharing for the computers that you are using for WebTrends.

WebTrends and Anti-Virus Software

We recommend disabling anti-virus programs on your WebTrends computers because virus scanning can lock files that WebTrends needs. If the anti-virus program locks even a few files during a WebTrends analysis, WebTrends' inability to write to these files can cause analysis to be incomplete and fail. Although the presence of anti-virus software does not guarantee a failure, running anti-virus and WebTrends on the same computer is not recommended.

Rather than disable virus scanning, you can configure the program not to scan log files, data files, or configuration files. (Depending on your WebTrends installation, some of these files may be located on network drives or, in a distributed installation, on other computers.) However, anti-virus software can safely scan WebTrends executables.

Although you can set your anti-virus program to run when WebTrends is not analyzing data, or to exclude the directory where WebTrends is installed, WebTrends generates alerts based on whether anti-virus is running on the same computer as WebTrends. You can use the Alert Configuration dialog box to change the default response to anti-virus scanning. For more information about managing alerts, see Help after you install WebTrends.

Preparing a MySQL Database Installation

If you plan to use MySQL for your WebTrends database, no special preparation is required. The database is installed when you install the WebTrends software. The installation program provides the host name and associated port number for you, and automatically loads MySQL onto your system. You can install the System Database component on the system running the Main Application or on a separate system.

Preparing a Microsoft SQL Server Installation

If you plan to use Microsoft SQL Server for your WebTrends database, you must install the server before beginning the WebTrends installation. When setting up the server:

- Create two empty SQL server databases. Name one of them `wtMaster` and the other `wt_Sched`.
- Configure a login account using SQL Server Authentication. The login account must be a member of the `sysadmins` server role.

- Make a note of the host name of your SQL Server and the password for your login account. You will need this information in order to complete the WebTrends installation.

Note

Because of issues with mixing languages, WebTrends only supports SQL Servers that have the SQL_Latin1_General_CP1_CI_AS (case-insensitive) collation installed at the server level. The databases should then be configured with that same SQL_Latin1_General_CP1_CI_AS collation.

Setting Up Shares for Data

During the installation process, you are asked to specify the storage locations for the WebTrends data repositories discussed in "Assessing Your Data Storage Needs" on page 33. Because each path must be accessible by each machine that is part of the distributed installation, be sure you set up these locations as shared folders before beginning the distributed installation.

For example, to store data on the Main Application computer that has a name of "wtmain", the shares could be:

```
\\wtmain\storage\analysis

\\wtmain\storage\report

\\wtmain\storage\config

\\wtmain\storage\backup
```

If you plan to use WebTrends Marketing Warehouse, you need to set up two shared directories, one for the unmodified SmartSource Data Collector (SDC) log files, and another for your log files after the Log File Pre-Processor and the Event Database Splitter have modified them.

```
\\wtmain\modules\logpreproc\logsrc

\\wtmain\modules\eventdatabase\src
```

If you plan to use the Express Analysis feature, you also need to set up two shared directories, one for Express Analysis log file data and one for Express Analysis report data. The following example shows two data shares created on a computer that has a name of “expressanalysis”:

```
\\wtexpressanalysis\logfiles

\\wtexpressanalysis\reports
```

Note

WebTrends does not support administrative shares, such as \\systemname\c$.

Performing the Distributed Installation

After all the computers designated for WebTrends are configured, you can proceed with the installation.

Notes

- If you are using Microsoft SQL Server for your WebTrends database, make sure that it is installed and set up before installing WebTrends. For more information, see “Preparing a Microsoft SQL Server Installation” on page 36.
- If anti-virus software is installed on your WebTrends-dedicated computers, decide whether you want to disable it. If the anti-virus software is activated when you install WebTrends, the installation program warns you that it may conflict with analysis. For more information, see “WebTrends and Anti-Virus Software” on page 36.

If you want to upgrade your installation to a newer version, see “Upgrading Your Distributed Installation” on page 45.

Installing the Main Application

When you install WebTrends Analytics components in a distributed configuration, you begin by installing the Main Application and other components that you want to run on the Main Application system.

To perform a distributed installation:

1. If you downloaded your software from the WebTrends web site:

   a. Beginning with the system you have designated for your Main Application, open the downloaded installation file.

   b. Unzip the files either to the default location or to the location of your choice. When the files are unzipped, the installation program starts automatically.

2. ***Otherwise,*** beginning with the system you have designated for your Main Application, insert the WebTrends software CD-ROM into your CD-ROM drive. If your computer is set up to use auto-run, the installation program starts automatically. If not, choose **Run** from the File or Start menus and type `x:setup` where *x* is the letter of your CD-ROM drive.

3. The installation wizard starts. Click **Next** to continue.

4. Before the WebTrends program files are copied to your computer, you must accept the Software License Agreement. ***If you agree to the stated terms***, select the **I accept the terms in the license agreement** option, and click **Next**. ***Otherwise***, click **Cancel** to exit the installation program without installing the software.

5. Type a valid license key, and click **Add License**. Repeat this step for each license key, Add-On license, and subscription license that you have. See your WebTrends administrator if you do not have a valid license key.

   Note

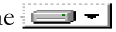
   You must have Internet connectivity to automatically activate a license key. If you do not have an Internet connection on this computer, you can manually activate the license key. For more information, see "Manually Activating Your License Key" on page 7.

6. The Select Install Type dialog box opens. Select **Custom**, and click **Next**.

7. The Destination Folder dialog box opens. The default installation folder is `x:\Program Files\WebTrends\` where x refers to the hard drive you are installing to.

   a. ***If you want to accept the default installation directory***, click **Next**.

   b. ***If you want to install in a different directory***, click **Change** and browse to your preferred location. Click **OK** to save the new location and click **Next**.

8. The Custom Setup dialog box opens. The  icon indicates which components will be installed on this computer. Expand the list to view all available components.You must install the Main Application component on this computer, but you can specify any sub-components, such as the UI Server, that you want to run on some other computer by selecting the component and clicking **Do not install this component**.

Note

You must install the Marketing Warehouse components on a dedicated computer. They cannot run on the same system as the Main Application components.

---

9. Select all the components that you want to install on this computer. You can get a description for each component by selecting it in the list and viewing the description on the right. Click **Next**.

10. In the Specify WebTrends Service Parameters dialog box, accept **Domain User Account** as the type of account that WebTrends services should use. This option allows WebTrends to use resources on shared network directories. Type the user name, password, and domain for an account that has read and write permissions for any shared directories WebTrends will use. Click **Next**.

11. ***If you selected the GeoTrends Server component***, do one of the following:

    - Click **Download** to download the latest available version of the GeoTrends data file from the WebTrends web site.
    - Locate the GeoTrends data file on the WebTrends CD-ROM.

12. The UI Server Parameters dialog box opens. WebTrends recommends that you use the default settings, but you may want to identify the host by IP Address rather than domain name or modify the port the UI Server uses. The default port is 7099. For more information about ports, see “Deciding Which Ports to Use” on page 34. Click **Next**.

13. The Select Database Type dialog box opens. Select the database type you want WebTrends to use for the system database. **MySQL** database is included with WebTrends and is automatically installed if you select this option. If you want to use **Microsoft SQL Server** for the system database, you must install it on a dedicated computer before you start the WebTrends installation procedure. For more information, see “Preparing a Microsoft SQL Server Installation” on page 36.

14. The System Database Initialization dialog box opens showing the host, port number, and administrator information. The default port for MySQL Servers is 3306. The default port for Microsoft SQL Server is 1433. For more information about ports, see "Deciding Which Ports to Use" on page 34. Type your password, confirm it, and click **Next**.

Note

You are specifying the password for the database, not for the WebTrends program. Also, if this is an upgrade WebTrends installation, only the information used during the first installation is valid here. See your WebTrends administrator if you have questions.

---

15. The Specify WebTrends Data and Environment Locations dialog box opens. As a best practice, you should specify the paths to shared directories that you created before beginning the installation. For more information, see "Setting Up Shares for Data" on page 37. You must specify directories for the following:

- Specify the location for storing analysis data in the **Analysis Data Repository** field
- Specify the location for storing report data in the **Report Data Repository** field
- Specify the location for WebTrends configuration data in the **Configuration Repository** field
- Specify the location for configuration data that you can use to restore your installation in the **Backup Repository** field

Click **Next** to continue.

16. ***If you selected Express Analysis***, the Specify Express Analysis dialog box opens where you can:

- Specify the location where your Express Analysis data is available for processing in the **Express Analysis Log Source** field
- Specify the location where the results of the Express Analysis are stored in the **Express Analysis Report Data Repository** field

You should specify paths to shared directories that you created before beginning the installation. Click **Next** to continue.

17. A confirmation window opens, reminding you to use shared folders for the storage locations. Click **Yes** to accept the directory locations you specified.

18. ***If your computer does not meet the minimum system requirements***, the **System Integrity Check Results Window** shows which requirements were not met. Only install WebTrends Analytics on a dedicated computer that meets the minimum system requirements.

19. A **Ready to Install the Program** window opens. Click **Install**. The WebTrends program files are installed to the computer.

20. The **Download Sample Data** dialog box allows you to download the WebTrends sample files that show how to set up features and demonstrate available reports. If you want to download WebTrends sample data, click **Download**. Otherwise, click **Next** and continue with step 21.

    a. Select a sample to download.

    b. Click **Save**, and specify where you want to save the file. By default, the file is saved to your computer desktop.

    c. Download any other samples that you want to use. After WebTrends is installed, you can install the samples that you downloaded. For more information, see “Installing WebTrends Sample Data” on page 44.

21. ***If you have only chosen to install WebTrends and the optional GeoTrends data file***, you are notified that the installation is complete.

    a. Select the **View Release Notes** check box to read important information about WebTrends including new features, identified issues, and summary of your installation.

    b. Make a note of your WebTrends log in information.

    c. Click **Finish** to close the Installation program.

You can install the remaining components on your other WebTrends-designated computers in the order that you choose.

Installing the Marketing Warehouse

You must install the Marketing Warehouse components on a system separate from the WebTrends Main Application. You can install all Marketing Warehouse components on one computer or you can install the Event Database Server and Event Database Loader components on one computer and the Log File Management component on a separate computer.

To install the Event Database Server, Event Database Loader, and (optional) Log File Management components:

1. Run the installation executable on the system you have designated for the Event Database Server/Event Database Loader components.

2. Select **Modify Installation**.

3. Select **Marketing Warehouse** in the list, and select **Install or maintain this component**.

4. ***If you want to install the Log File Management component*** on the same system running the Event Database Server/Event Database Loader components, select **Log File Management** and select **Install or maintain this component**. The Log File Management component (which includes the Log File Pre-Processor and the Event Database Splitter) is required for the Marketing Warehouse, but you can install it on a separate system. Click **Next**.

5. The Event Database Server Parameters dialog box opens. ***If you want to accept the default settings***, in the **Password** text box, type the password you want to use to log in to the Event Database Server.

6. Otherwise, you can change the default settings.

   a. In the **Host** text box, you can identify the Event Database Server host by IP Address rather than the domain name.

   b. In the **Port** text box, specify the port number that you want the Event Database Server to use.

   c. In the **Username** text box, specify the user name you want to use to log in to the Event Database Server.

   d. In the Password text box, specify the password you want to use to log in to the Event Database Server. You can specify the password you use for the WebTrends Analytics UI Server or use another password.

7. Click **Finish** to close the Installation program.

Notes

After you install the Log File Management component, you must specify the UNC path to your log file storage location in the host role settings if you installed the Log File Management component on more than one computer or if you created a shared directory for your log file storage. For information about specifying this location, see "Specifying the SDC Log File Source Location" on page 44.

To install the Log File Management component on a separate system:

1. Run the installation executable on the computer you have designated for the Log File Management component.

2. Select **Modify Installation**.

3. Select **Log File Management** in the list, and select **Install or maintain this component**. Click **Next**.

4. Click **Finish** to close the Installation program.

Specifying the SDC Log File Source Location

After you install the Log File Management component, you must specify the UNC path to your log file storage location. For more information about configuring this storage location, see “Setting Up Shares for Data” on page 37.

To specify the log file source location:

1. In the left pane of the WebTrends Analytics Administration console, click **Administration > System Management > Hosts**.

2. Select the **Log File Management** role.

3. In the Log File Source Directory text box, specify the path to the data share you created for storing your unmodified SDC log files.

Installing WebTrends Sample Data

You can install WebTrends sample data from either the WebTrends CD-ROM or the WebTrends web site. Install WebTrends before installing the sample data.

To install a sample:

1. Locate the sample data using one of these methods:

   - ***If you downloaded the sample files during the WebTrends installation,*** locate the files that you saved. By default, the samples are saved to your computer desktop. Continue with step 3.
   - ***If you want to install the samples from WebTrends CD-ROM***, insert the CD-ROM, and from the window that opens, select **Miscellaneous**.
   - ***If you want to install the samples from the WebTrends web site***, log in to the WebTrends Administration Console. In the left pane select, **Components > Accessories**, and select **Sample Downloads**.

2. Select from the select one of the following samples:

   - ZedescoSDCSample.exe
   - ZedescoSample.exe

- StreamingMediaSample.exe

3. Double-click the sample executable file, or select **Run** from the Windows Start menu to launch the installation wizard. Click **Next**.
4. Before the samples are copied to your computer, you must accept the License Agreement. If you agree to the stated terms, select **I accept the terms of the license agreement**, and click **Next**. Otherwise, click **Cancel** to exit the installation program without installing the samples.
5. The **Custom Setup** dialog box opens. Select the samples you want to install, and click **Next**.
   - If you are unfamiliar with this type of installation program, click **Help** for details on the different selection options you can choose from.
   - If you are unclear how much storage space you have available, click **Space.** The installation program lists the available data space and requirement for each volume you have access to. (You can select the columns to sort this data.) When you are finished reviewing this information, click **OK**.
6. ***If you want to review or change any of your choices***, click **Back**. ***Otherwise***, click **Install**.
7. You are notified when the installation is complete. Click **Finish** to close the wizard.

To analyze sample data for viewing reports:

1. Log in to WebTrends Administration Console.
2. Click **Reports & Profiles**.
3. Click the **Analyze Now** icon for each of the sample profiles.

Upgrading Your Distributed Installation

If you are completing these steps to upgrade your installation, you must stop the required services before installing the upgrade.

To stop the required services:

1. On your WebTrends Main Application computer, stop the following WebTrends services on every computer in the distributed installation:
   – WebTrends GeoTrends Server
   – WebTrends User Interface Service

– WebTrends Apache
– WebTrends Scheduler Agent
– WebTrends System Monitor Service
– WebTrends Tomcat

Make sure you stop these services on all computers.

2. Make sure your WebTrends system database is still running.

   a. ***If you are running MySQL for your WebTrends system database***, make sure that the WebTrends MySQL Service is started. If not, restart it before installing the upgrade.

   b. ***If you are running Microsoft SQL Server for your WebTrends system database,*** make sure the service for Microsoft SQL Server, MSSQLSERVER, is started.

3. Beginning with the computer that contains the WebTrends Analytics system database, run the upgrade installation program.

4. When the upgrade installation on the Main Application computer is finished, continue to run the installation program on the computers where WebTrends components are installed. For example, the computers running the UI Server, the GeoTrends Server, SmartSource Data Collector (SDC), and the Analysis Engine. As a best practice, we suggest that you upgrade the Analysis Engine computers last.

5. Restart the WebTrends services on all computers, and the upgraded version starts.

6. You can use the Topology dialog box to make sure that all computers in the installation are recognized. In the left pane of the Administration Console select **Administration** > **Monitoring** > **Topology**.
   If you suspect that one of the WebTrends component computers was not upgraded, check the status logs on each computer in your distributed installation for a "version incompatibility error." This message is logged when one of the WebTrends components does not match the version of the database. For example, if you cannot view the WebTrends UI or if there is no new report data since the upgrade, one of the computers may not have been upgraded. Status logs are located in the *`WebTrends Installation Directory`*`\logs` directory.

Managing Your Distributed Installation

WebTrends provides several features for managing the computers in your installation which are discussed in this section.

Viewing Available Resources

The Topology dialog box shows all the hosts, or computers, in your installation, the roles assigned to each host, and the available resources for each computer. A *role* is a function that the host performs according to the modules you installed on that computer. A *group* is a designation that you create primarily for the purpose of distributing work.

To view the computers in your installation:

In the left pane of the Administration Console select **Administration** > **Monitoring** > **Topology**.

Using Groups to Distribute Work

WebTrends allows you to create groups and assign the computers in your installation to those groups. For example, if you have multiple hosts that have the Standard Analysis Engine Role, you can use Host Groups to make sure that the computers that have sufficient system resources analyze your largest web activity data files. You could then assign profiles that process large data sets to this group.

To work with host groups:

1. In the left pane of the Administration Console, select **Scheduler** > **Options** > **Host Groups**.
2. Select **New Host Group** to begin creating a new host group or edit an existing host group.

Monitoring Hosts in Your Installation

For troubleshooting purposes, you may need to check the status of the WebTrends services. The Service Health dialog box allows you manage all the WebTrends services in your installation through the Administration Console.

To manage WebTrends services, in the left pane of the Administration Console, select **Administration** > **Monitoring** > **Service Health**.

Modifying the Ports WebTrends Uses

You may need to change the ports that WebTrends components use if they are used by other services.

To modify ports after installation:

1. In the left pane of the Administration Console, select **Administration > System Management > Hosts**.
2. Click **Use local settings**.
3. Select the server whose port you want to change.

Chapter 5

SmartSource Data Collector Installation

Preparing to Install SDC

Before installing SDC, review this section for special considerations.

- If you are installing WebTrends SmartSource Data Collector (SDC) on Apache, and you have a version of Apache earlier than v2.0.55 installed on the SDC dedicated system, you must remove it before installing SDC. When you install SDC, a later version of Apache is installed. For information about removing an existing version of Apache, see "Uninstalling SDC on Windows" on page 62.
- You must remove any pre-existing SDC installation before installing this version. For information about upgrading SDC, see "Upgrading SDC" on page 52.
- You must install a supported version of IIS before installing the IIS-based SDC software. For more information about compatible versions of IIS software, see "Preparing for a Basic Installation" on page 11.

Network Considerations

SDC is a specialized Web server. It receives HTTP requests from Web clients, processes the requests, and appropriately responds to the Web clients. The connections established between the clients and the server use TCP/IP. To make the required connection, the Web server must be listening on a predetermined port associated with a known IP address. The client must have knowledge of the IP address and connectivity to the Web server.

Before installing SDC, consider the issues related to the configuration of your network that enable the TCP/IP communication between the Web server and Web clients. Most importantly, keep in mind that the SDC server is a Web server that must be available for Web clients to make HTTP requests.

Load Balancer Considerations

If you plan to install SDC on multiple computers behind a load balancer, there are additional network and operations considerations.

- Install the same version on each SDC computer. When you install upgrade versions, you need to install the new version on each before you bring any of them back on line.
- Configure each SDC computer the same way so that they are mirror images of each other. Any differences in configuration could cause problems during analysis, particularly for settings such as cookies.
- Implement a method of gathering the log files from each SDC computer and moving them to a location accessible by WebTrends Analytics. After you install SDC, you will create a WebTrends profile that specifies the collection of log files to use for reporting.
- Make sure that the client IP logged is not the IP address of the load balancer. Some load balancers are configured to overwrite the client IP address resulting in reports that show all traffic coming from one visitor.
- Make sure that the load balancer is not configured to track visitor sessions, because hits from SDC contain all the data needed that enable WebTrends to identify visitor sessions. Configuring the load balancer to identify hits throughout the session slows the web server needlessly.
- As a best practice, you should configure the load balancer to host the SSL certificates if you want to use SSL. Hosting the certificates on each SDC server would put unnecessary burden on the server degrading performance.

Security Considerations

Because external clients make requests to the SDC server, carefully consider the security of your server before installing SDC. The SDC server is a specialized Web server, but the security issues related to the SDC server are common to the security issues of standard Web servers.

Many types of threats are related to Web server operations:

- Unauthorized access to confidential data
- Data corruption
- Web site disruption
- Denial of Service (DOS) and other types of attacks

One approach to a secure configuration of the SDC server employs a “deny all” model. This approach begins with all services disabled, and enables only those services necessary for the operation of the SDC server. Specifically, do not enable services (daemons) such as telnet, mail, and finger. For the SDC server, the only TCP/IP link to the Internet required is port 80. (Port 443 is required if you use secure connections using SSL.)

Firewalls are often used to protect Web servers and internal corporate networks. You can select from many types of firewalls and numerous ways to configure them and their corresponding networks. To use a firewall (which can be composed of routers, network segments, and host computers), you need to determine the location of your SDC server relative to the firewall in your network. You can put the SDC server outside or inside of the firewall. If you place the Web server outside of the firewall, it is more susceptible to malicious attacks. However, if an attacker breaks in, only the boundaries of the SDC server will have been breached and not the entire corporate network.

The details about the types of security breaches and the methods for preventing these attacks are beyond the scope of this document. However, it is highly recommended that you address the security concerns before exposing the SDC server to external users.

Installing SmartSource Data Collector

To use SDC you need to:

1. Install SDC. For more information, see “Installing IIS-Based SDC” on page 54 or “Installing Apache-Based SDC” on page 56.
2. Create an SmartSource Data Collector data source and generate SmartSource Site IDs. For more information, see “Defining an SDC Data Source” on page 59.
3. Configure the SDC site map file. For more information see, “Configuring an SDC Site Map” on page 60.
4. Start the SDC server. For more information, see “Starting SDC” on page 61.
5. Insert the WebTrends JavaScript tag on your Web site. For more information, see “Tagging Web Pages for SDC” in the *WebTrends Installation and Configuration Guide*“Tagging Web Pages for SDC” on page 131.

Upgrading SDC

Understanding Standard Model, Hosted Model, Service Model

Before v7.5a, you may have configured SDC for Standard Model or Hosted Model. Standard Model collects Web activity data for one domain, and the request from your Web site to the SDC is `http://`*`hostname`*`/dcs.gif`. Because Standard Model doesn't include a SmartSource Site ID (DCSID) in the JavaScript tag and consequently, the request to SDC, when you upgrade you will create a SmartSource data source, and in the process, generate a SmartSource Site ID.

Hosted Model collects Web activity data for multiple domains or sections of a site using a SmartSource Site ID (DCSID) for each domain that you want to track in isolation. You can continue to use existing SmartSource IDs, and you will also configure the SDC site map file to recognize them.

Service Model Features

With SDC v7.5a and higher, the installation configures SDC for Service Model. Service Model allows you to analyze activity for all SmartSource Site IDs (DCSIDs) by providing the account rollup data source. WebTrends creates the account rollup data source automatically when all data sources in your installation are SmartSource data sources. If your data sources are a mix of SmartSource data sources and other types of data sources, the account rollup data source is not automatically created. Service Model is also required for those using WebTrends Marketing Warehouse and those using the Express Analysis feature for WebTrends software which provides constantly updatable reporting based on your SDC log files. For more information, see "Setting up Express Analysis" in the *WebTrends Advanced Configuration Guide*.

Upgrading Best Practices

Use the following guidelines when upgrade to a new version of SmartSource Data Collector (SDC):

- When upgrading to new version of (SDC), you should regenerate your WebTrends JavaScript tag and replace all existing tags for all your domains and subdomains with the new tag. Older versions of the tag cannot coexist with the new tag.

  Note
  Although your new version of SDC works with JavaScript tags generated with prior versions, WebTrends Analytics relies on new JavaScript tags for analysis.

- Make sure that each Web page contains only one instance of the JavaScript tag. SDC does not support double-tagging.
- Coordinate tagging your Web pages with the new WebTrends JavaScript tag as closely as possible to installing the SDC upgrade to avoid missing data collected from your Web site. SDC cannot collect data until all your pages are tagged with the new tag and the SDC upgrade is installed.
- After implementing your new tag, purge your Web server cache to clear cached pages that contain older versions of your tag.
- Perform the upgrade during your site's least active time period.
- *If you are upgrading from SDC v7.5 or earlier*, note that the log file naming scheme has changed. If you have custom scripts or other processes that are dependent on the names previously used, you will need to modify them to support the new names. For more information about the log file format, see "SDC Log File Name" on page 127.

Note
Be aware that when you first implement a new JavaScript tag, caches that contain pages with the older version of your tag will continue to return these pages until the browser cache is refreshed. Mixing versions of the JavaScript tag is not supported and could cause slightly skewed visitor and visit counts until all browser caches are refreshed.

To install the SDC upgrade:

1. Create a backup copy of the entire SDC installation directory.
2. Remove the previous version. For more information, see "Uninstalling SmartSource Data Collector" on page 62.
3. Install the new version of SDC. For more information about the installation, see "Installing IIS-Based SDC" on page 54 or "Installing Apache-Based SDC" on page 56.

4. ***If you are moving from Standard Model to Service Model***, we recommend that at this point, you create a copy of the new `dcs.cfg` file, save it to another location, and replace it with the `dcs.cfg` file located in the backup SDC installation directory you created in step 1. Run the new SDC version for 48 hours or until you determine that it is running as expected. Then complete the remaining steps in this procedure.

5. Compare the `dcs.cfg` file included in the installation with your backup copy using a text editor. Alternatively, you can print copies of each file and manually compare them. Determine which settings you customized in your previous version. Be sure to set the following settings to `true`:

   – sitewidecookie

   – hostedmodel

   – servicemodel

6. ***If you are upgrading a Standard Model SDC to a Service Model SDC***, in the WebTrends Administration Console, edit your existing data sources and generate a SmartSource Site ID. The new tag supports account rollup visitor session tracking and first-party cookie tracking. For more information about modifying the data source, see "Defining an SDC Data Source" on page 59.

7. Save the new JavaScript tag.

8. Modify the SDC site map file with your SmartSource Site IDs (DCSIDs). For more information, see "Configuring an SDC Site Map" on page 60.

9. ***If you plan to track first-party cookies using your WebTrends JavaScript tag***, you need to make additional changes to your JavaScript tag and the session tracking definitions your profiles use. For more information, see "Using Cookies to Track Visitor Sessions" in the *WebTrends Advanced Configuration Guide*.

10. Tag your Web site with the JavaScript tag. For more information about tagging your site, see "Inserting the SDC JavaScript Tag" on page 135.

Installing IIS-Based SDC

You must install a supported version of IIS before installing the IIS-based SDC software. For more information about compatible versions of IIS software, see "Preparing for a Basic Installation" on page 11.

To install IIS-based SDC:

1. Insert the WebTrends CD-ROM into your CD-ROM drive.
   - If your system is set up to use auto-run, the setup program is automatically launched.
   - If not, click **Start** > **Run** to open the **Run** dialog box, and type `d:\setup` where `d:` is the letter of your CD-ROM drive.
2. Review the contents of the InstallShield Wizard Welcome dialog box and click **Next**.
3. Review the SmartSource Data Collector License Agreement.
   - If you agree to the terms of the Agreement, select **I accept the terms in the license agreement**, and then click **Next**.
   - Otherwise, click **Cancel** to exit the installation.

Note

Click **Cancel** at any time to exit the installation.

---

4. ***If you want to accept the default directory***, click **Next**.
5. ***Otherwise***, click **Change**. Browse to the location you want or type the location in the **Folder name** text box. Click **OK**. In the Destination Folder dialog box, click **Next**.
6. Click **Install** to begin the installation. An Installing WebTrends SmartSource Data Collector dialog box opens and the installation process begins.
7. Select **Internet Information Server (IIS)**, and click **Next**.
8. Click **Finish**. The SDC installation is complete.

Note

If you use IIS 6, before you start using SDC, you need to configure the logging directory to have the necessary rights.

Configuring Log File Directory Security Permissions for IIS 6

If you use Microsoft IIS 6, you need to configure the directory that SDC uses for storing its log files to have at least modify rights. When SDC creates a log file, it saves the file with a `dcsbusy` file extension. When it completes the log file, it saves the file with a `log` file extension. The SERVICE group needs to have rights to Modify in order to save the log file with the new extension.

To configure the log file directory:

1. On the computer where you installed SDC, navigate to the directory SDC uses to write log files. The default directory is *`SDC installation directory`*`\weblog`. If you want SDC to store its log files in another directory, navigate to that directory.
2. Right-click on the file, and select **Properties**.
3. Select the **Security** tab.
4. Select the SERVICE group. If you don't see this group in the list, you need to add it. Select the **Modify** check box.
5. ***If you are not using the default log file directory***, open the `dcs.cfg` file which is located in the *`SDC installation directory`*`\cfg` directory.
6. Change the value for the `logfiledir` setting to the complete path to the directory you want to use for logging.

Installing Apache-Based SDC

If you select SmartSource Data Collector during the WebTrends Analytics installation, an Installation wizard for SmartSource Data Collector opens after the WebTrends Analytics installation is complete. If a version of Apache earlier than v2.0.55 is installed, remove it before installing SDC.

To install the Apache Web server and SDC:

1. After the main WebTrends installation has completed, the SmartSource Data Collector Installation wizard launches. Click **Next** to continue.
2. Review the SmartSource Data Collector License Agreement.
   - ***If you agree to the terms of the Agreement***, select **I accept the terms in the license agreement**, and click **Next**. You cannot continue the installation unless you accept the terms of the licsense agreement.
   - ***Otherwise***, click **Cancel** to exit the installation.
3. ***If you want to accept the default directory***, click **Next**.
4. ***Otherwise***, click **Change** and browse to the location where you want to install SDC or type the location in the **Folder name** text box. Click **OK**. In the Destination Folder dialog box, click **Next**.
5. Click **Install**. An Installing WebTrends SmartSource Data Collector dialog box opens and the installation process begins.
6. A Server Type dialog box opens. Select **Apache** as your Web server, and click **Next**.
7. The message, **This product requires the use of Apache Web Server 2.0.55. Would you like to install it now?** is displayed.

Note

As a best practice to insure ease of use and full SDC functionality, you should uninstall and then re-install the Apache Web server.

   - ***If you want to install the Apache Web server***, click **Yes**. Go to step 8.
   - ***If you have already installed the required version of Apache***, click **No** and skip the Apache portion of the installation. Go to step 21.
8. The Apache httpd server installation wizard Welcome page opens. Click **Next.**
9. Review the Apache Software License Agreement.
   a. ***If you agree to the terms of the Agreement***, select **I accept the terms in the license agreement**, then click **Next**.
   b. ***Otherwise***, click **Cancel** to exit the installation.
10. Review the Read This First message. Click **Next** and the Server Information dialog box opens.
11. In the **Network domain** text box, specify the domain for the SDC server.

12. In the **Server name** text box, specify the registered DNS name or IP address for the SDC host. This setting allows you to configure a host name which is sent back to clients to identify your server if the host name is different than the one the program would get otherwise. The server name you enter is used to modify the `httpd.conf` file.

13. In the **Administrator's email address** text box, specify the address where problems with the server are to be sent.

14. Specify how you want to install Apache HTTP Server 2.0 programs and shortcuts.

    - ***If you want to run Apache as a service***, select **For All Users, on Port 80, as a Service**.
    - ***If you want to start Apache manually***, select **Only for the Current User, on Port 8080**.

    Click **Next**.

15. ***If you want to install all of the Apache software***, select **Typical**, and click **Next**.

16. ***Otherwise, if you want to install only one or more features***, select **Custom** and click **Next**. The Custom Setup dialog opens.

17. In the Destination Folder dialog box specify the installation directory. *If you want to accept the default installation directory*, click **Next**. *Otherwise*, click **Change** to specify a different installation directory. Browse to the new location or type the folder name in the **Folder name** text box. Click **OK**. Then in the Destination Folder dialog box, click **Next**.

18. The Ready to Install dialog box opens. To set up a custom installation, select the Apache components to install by clicking the icons and choosing a component installation option.

    a. Click **Space** to see a list of your drives, drive sizes, available space for each drive, and the required space for the selected features.

    b. ***If you want to accept the default destination folder***, click **Next**.

    c. ***Otherwise***, click **Change** to specify a different destination folder. Browse to the new folder or type the folder name in the **Folder name** text box. Click **OK** and then in the Custom Setup dialog box, click **Next**.

19. Click **Install** and the Apache installation begins.

Note

If a web server or another application is already running on port 80 or another port that you specified for SDC, you receive the following error message:

```
Only one usage of each socket address <protocol/network address/
port> is normally permitted. : make_sock: could not bind to address
0.0.0.0:80 no listening sockets available, shutting down. Unable to
open logs.
```

Open your management console (On your desktop right-click **My Computer** icon **>** **Manage** > **Services and Applications** > **Internet Information Services**) and stop the server or application that is running on port 80.

---

20. The Installation Wizard Completed dialog box opens, indicating that Apache is installed. Click **Finish**.

21. To complete the SDC configuration, your Web server must be stopped and restarted. Click **Yes** to do so at this time. Click **No** to postpone this step and the configuration.

22. Click **Finish**. The SDC installation is complete.

Defining an SDC Data Source

If you are installing SDC for the first time, you need to create an SDC data source in the WebTrends Administration Console. The data source generates a JavaScript tag containing the unique DCSID for your site. If you have multiple domains and you want to report traffic for those sites separately, create a data source for each domain.

If you have already defined an SDC data source, and you know your DCSID, you can skip this step. If you have defined an SDC data source and you need to know your DCSID, you can look at the data source in Edit mode in the Administration Console to find the DCSID.

To create an SDC data source:

1. In the left pane of the WebTrends Administration Console, select **Administration > Data Sources**.
2. Click **New Data Source**.
3. In the Data Source Type dialog box, select **Web: SmartSource Data Files**.
4. Identify the location of your SmartSource Data Collector log files.

5. Provide information about the time zone for the log file.
6. In the SmartSource Site ID dialog box, click **Generate a new SmartSource Site ID** and specify the IP address of the SmartSource Data Collector computer.
7. In the SmartSource Data Collector dialog box, copy the WebTrends JavaScript tag, or click **Download this tag** to save it in a text file.
8. Save the data source.

Configuring an SDC Site Map

To run SDC version 7.5a or higher, you need to configure a site map file that contains the DCSID for each of your data sources. The site map file allows you to track visitors across multiple domains using first-party cookies. It also allows you to analyze traffic for all your domains using the account roll-up data source and use Express Analysis. For more information, see "Setting Up Express Analysis" in the *WebTrends Advanced Configuration Guide*.

To configure the SDC site map:

1. Open the `webtrendssites.lst` file located in the *`SDC installation directory`*`\cfg` directory.

   Copy the first line of code for each data source that you want to track. For example,
   `dcs5w0txb10000wocrvqy1nqm_6n1p, -5, 1, NULL, 1, 1`

   Note
   Each line of code represents a single data source. All fields are required. For more information about each field, see "SDC Configuration" in the *WebTrends Advanced Configuration Guide*.

   ---

2. Replace dcs5w0txb10000wocrvqy1nqm_6n1p with the DSCID for your SDC data source. You can use an existing DSCID or generate a new one. For more information, see "Defining an SDC Data Source" on page 59.
3. Replace `-5` with the time zone of your Web server. Specify a value between -12 and 12 that corresponds to the GMT offset of your Web server. For example, the time zone for Pacific Standard Time is `-8`.

4. Increment the value of the third field for each DCSID you specify. For example, if you have two DCSIDs, you would modify the third field in the following manner:

```
DCSID1, TIMEZONE, 1, NULL, 1, 1
DCSID2, TIMEZONE, 2, NULL, 1, 1
```

Note

Do not modify the `NULL` value unless you are setting up SDC for Express Analysis. If you configuring the data source for Express Analysis, change `NULL` to `'express'`. For more information see “Setting Up Express Analysis” in the *WebTrends Advanced Configuration Guide*.

---

5. *If you want to prevent SDC from setting cookies for a specific data source*, change the fifth field value to `0`. You can use this setting to override the global setting that disables cookies in the SDC configuration file, `dcs.cfg`. By default, cookies are enabled, which is specified by a value of `1`. You should only disable cookies if your organization’s policy does not allow visitors to be identified using cookies.
6. *If you want to configure session only cookies for a specific data source*, change the sixth field value to `2`. You can use this setting to override the global setting that configures cookie persistence in the SDC configuration file, `dcs.cfg`. By default, cookies generated by SDC are persistent specified by a value of `1`.

Starting SDC

The installation program creates a fully configured Web site named *SmartSource Data Collector*. You can restart IIS to activate SDC by entering the following commands at a command prompt:

```
net stop iisadmin /y

net start w3svc
```

The SDC server is now configured and listening for instrumented hits on Port 80.

Notes

- Before SDC can collect traffic about your Web site, you must insert the JavaScript tag on your Web pages. For more information, see "Tagging Web Pages for SDC" on page 131.
- For more information about configuring SmartSource Data Collector and the `dcs.cfg` file, see "SDC Configuration" in *WebTrends Advanced Configuration Guide*.
- For information about enabling secure communication from Web clients to SDC using the Secure Sockets Layer protocol, see "Secure Socket Layer (SSL)" in the *WebTrends Advanced Configuration Guide*.

Uninstalling SmartSource Data Collector

This section describes the procedures for removing an installation of SmartSource Data Collector (SDC). If you are installing an upgrade of SDC, you must remove any previous installation of SDC before installing the upgrade.

Uninstalling SDC on Windows

Uninstalling Apache on Windows

Complete the following steps:

1. Stop Apache-based SDC.
   - Open a command prompt type the following command:

     ```
     net stop apache 2
     ```
2. From the Windows Control Panel, select **Add/Remove Programs**.
3. Under **Currently installed programs**, select the **Apache httpd Server** and click **Remove**.
4. If you plan to install the SDC-provided Apache in the same directory as the previous installation of Apache, you may have to remove the Apache folder with the `conf` and `logs` subfolders to completely remove Apache.

Uninstalling Windows-Based SDC

Complete the following steps:

1. If you want to preserve your SDC settings, create a backup file of the SDC configuration file located in the `SDC installation directory\cfg\dcs.cfg`. You might also want to create a backup file of the SDC site map file, `webtrendssites.lst`. If you are using `cookieversion=2`, you might want to preserve your cookie validation private key (MagicCode).
2. From the Windows Control Panel, select **Add/Remove Programs**.
3. Under **Currently installed programs**, select **WebTrends SmartSource Data Collector**, and click **Remove**.
4. Click **Yes** in the confirmation dialog box.
5. Close the Add/Remove Programs window.

Upgrading Apache Web Server

Periodically, the Apache Software Foundation (www.apache.org) releases new versions of Apache 2.0. Typically, these releases are minor ones that fix bugs or respond to security vulnerabilities. As long as the new Apache 2.0 release maintains binary compatibility, you are free to upgrade to it.

The method used to upgrade Apache 2.0 varies according to the operating system you are using. We recommend that you back up your existing Apache installation before upgrading. The following subsections describe how to upgrade for each supported operating system.

Upgrading on Windows

You should install the Apache 2.0 upgrade in the same directory as the previous installation.

To upgrade Apache on Windows:

1. Download the Apache 2.0 Win32 Binary upgrade from www.apache.org.
2. Stop Apache from the command line by typing `net stop apache2`.
3. Uninstall the existing Apache 2.0 by selecting **Settings > Control Panel > Add/Remove Programs > Apache HTTP Server 2.0.***x* from the Start menu.

4. Install the Apache 2.0 upgrade in the same directory as the previous installation. Doing so preserves your *Apache Installation Directory*\logs and *Apache Installation Directory*\conf directories. To install the upgrade, execute the following command:

```
apache_2.0.x-win32-x86-no_ssl.msi
```

where *x* specifies the 2-digit minor version.

Binary Compatibility

If you attempt to use SDC with a version of Apache 2.0 that is incompatible, you will see a message similar to the following in your Apache error log at startup:

```
httpd: module "inc/apachelogserver.h" is not compatible with this
version of Apache.
Please contact the vendor for the correct version.
```

If you get this error message, contact WebTrends support for a compatible version of SDC.

Chapter 6

Implementing WebTrends Marketing Warehouse

WebTrends Marketing Warehouse includes the Marketing Warehouse, which is a collection of marketing-related databases, and the Marketing Lab Desktop, which gives you access to the customer and business event data captured in the Marketing Warehouse. Before you can use WebTrends Marketing Warehouse, a WebTrends administrator must configure WebTrends Analytics, deploy a v8 or higher JavaScript tag on the web site, and implement the required query parameters.

This chapter describes how WebTrends administrators create profiles and configure user rights in preparation for using WebTrends Marketing Warehouse.

Preparing to Use WebTrends Marketing Warehouse

Before you can use WebTrends Marketing Warehouse, you must complete the following steps:

1. *If you use the software version of WebTrends Analytics,* install WebTrends Analytics including WebTrends Marketing Warehouse components and the GeoTrends Server. For more information, see "Installing the Marketing Warehouse" on page 42.
2. *If you use WebTrends Analytics software,* configure the Log File Management Role settings. For more information, see "Configuring the Log File Management Role Settings" on page 71.
3. *If you use WebTrends Analytics software*, install and configure SmartSource Data Collector. Marketing Warehouse profiles require log files from SmartSource Data Collector v8 or higher. For more information, see "SmartSource Data Collector Installation" on page 49.
4. Implement the WebTrends JavaScript tag on your web site. For more information, "Client Side Integration" in the *WebTrends Advanced Configuration Guide*.

5. Configure your web site to use the required WebTrends query parameters. For more information, see "Tagging for Marketing Warehouse" on page 67.
6. Configure user rights for Marketing Lab Desktop. For more information, see "Identifying Visits and Visitors for Marketing Warehouse" on page 66.
7. Create a Marketing Warehouse profile. For more information, see "Creating a Marketing Warehouse Profile" on page 74.

Identifying Visits and Visitors for Marketing Warehouse

Marketing Warehouse relies on first-party cookies supplied by the WebTrends JavaScript tag or by WebTrends third-party cookies (`WEBTRENDS_ID`) for identifying visits and visitors. For the most accurate identification of visitors, your WebTrends JavaScript tag should be configured for first-party cookie tracking. By default, first-party cookie tracking is enabled when you create a SmartSource data source. You can configure the tag use the cookie tracking method of your choice. The tag can generate a first-party cookie for you, use your company's first-party cookie (or your method of uniquely identifying visitors), or use the cookie generated by the WebTrends Cookie Plug-in. For more information, see "Using Cookies to Track Visitor Sessions" in the *WebTrends Advanced Configuration Guide*.

Note

If you used a version of WebTrends prior to v8, you need to edit your SmartSource data sources and update your WebTrends JavaScript tag. For more information, see "Defining an SDC Data Source" on page 59.

Without cookie tracking, the Marketing Warehouse tracks events only. Visitors without cookies are considered "unknown visitors."

Marketing Warehouse also recognizes the `WT.dcsvid` parameter which identifies visitors using a value generated and maintained by your web server. The Marketing Warehouse uses this query parameter to populate the `ExternalVisitorID` field of the Visitor table, which links to external visitor data in the Modules Database.

Tagging for Marketing Warehouse

In order to populate the Marketing Warehouse with the event data required for Marketing Lab Desktop, you need to implement a WebTrends JavaScript tag. You can create a WebTrends JavaScript tag by creating a SmartSource data source in WebTrends Analytics software or by creating a data source in WebTrends On Demand. Marketing Warehouse requires a tag created using WebTrends Analytics software or On Demand v8 or higher. For information about implementing the tag on your web site, "Implementing the WebTrends JavaScript tag on Your Web Site" in the Administration Console help.

Marketing Warehouse also requires the presence of certain WebTrends query parameters in your SmartSource Data Collector log files. For more information about the complete set of WebTrends query parameters, see "WebTrends Query Parameters" in the *WebTrends Advanced Configuration Guide*.

Campaign Events

The Marketing Warehouse requires the following query parameter values to be present for campaigns in order to populate the `CampaignEvent` table:

`WT.mc_id`

`WT.mc_id=`*`Campaign ID`*

Identifies a specific marketing campaign. Pass this query parameter to pages that you want to associate with a specific campaign. You can specify a numeric or string value.

`WT.mc_ev`

`WT.mc_ev=`*`EmailOpen/click`*

Identifies the campaign event type. Marketing Warehouse associates hits with the `click` value as a campaign clickthrough event.

Marketing Warehouse associates hits with the `emailopen` value as email campaigns that resulted in an email open event.

Content Group Events

The Marketing Warehouse uses the following query parameter values to populate the `ContentGroupEvent` table:

`WT.cg_n`

`WT.cg_n=`*`Name[;…]`*

Identifies the name of a content group. The maximum length for each ***`Name`*** is 64 bytes.

`WT.cg_s`

Identifies the name of a sub-content group. The maximum length is for each *`SubName`* is 64 bytes.

External Visitors

The Marketing Warehouse uses this query parameter to populate the `ExternalVisitorID` field of the Visitor table, which links to external visitor data in the Modules Database.

`WT.dcsvid`

`WT.dcsvid=`*`anystring`*

This parameter identifies visitors using the unique visitor ID you assign to your visitors.

Product View Events

The Marketing Warehouse uses the query parameters values in this section to populate the `ProductViewEvent` table:

Use the following query parameters to populate the Viewed SKU attribute:

`WT.pn_sku`

`WT.pn_sku=`*`productSKU[;…]`*

Identifies the SKU (a unique numeric identifier) of the product.

`WT.tx_e=v`

Identifies a product view.

Both parameters must be present in the hit in order for the Marketing Warehouse to recognize the hit as a product view.

Note
Marketing Warehouse assumes that `WT.tx_u` has a value of 1 (units) when passed in a hit with `WT.tx_e`.

Purchase Events

The Marketing Warehouse uses the query parameters in this section to populate the `PurchaseEvent` table, the `PurchaseEventOrderType` table, and the `PurchaseLineItemEvent` table:

`WT.pn_sku`

`WT.pn_sku=`*`productSKU[;…]`*

Identifies the SKU (a unique numeric identifier) of the product. When multiple values are passed, the order of the values is important because they correlate to the number of units passed in the `WT.tx_u` parameter.

`WT.tx_e=p`

Identifies a product purchase.

`WT.tx_i`

`WT.tx_i=`*`InvoiceNumber`*

Identifies the invoice number for the purchase.

`WT.tx_s`

`WT.tx_s=`*`Subtotal[;…]`*

Identifies the total cost for each product in the order. Do not include a currency symbol and be sure pass the value in *dollars.cents* format. If an order contains multiple products, separate the totals for each product using a semi-colon.

`WT.tx_u`

`WT.tx_u=`*`Units[;…]`*

Identifies the quantity in the transaction. Pass a positive integer for this value. If an order contains multiple products, separate the numbers of units for each product using a semi-colon. When multiple values are passed, the order of the values is important because they correlate to the number of units passed in the `WT.pn_sku` parameter.

Registered Visitors

The Marketing Warehouse uses this query parameter to set the `IsRegistered` column in the `Visitor` table.

`WT.rv`

`WT.rv=1`

Your web server should pass this parameter with a value of 1 on a hit when a visitor completes a registration process.

Scenario Events

The Marketing Warehouse uses the query parameters in this section to populate the `ScenarioEvent` table.

`WT.si_n`

`WT.si_n=`*`Name[;…]`*

Identifies the name of the Scenario Analysis. The maximum length for each *`Name`* is 64 bytes.

`WT.si_x`

`WT.si_x=`*`StepPosition[;…]`*

Identifies the Scenario Analysis step by number.

`WT.si_cs`

`WT.si_sc=1/0[;]`

A value of 1 identifies that a conversion has occurred. In most cases, this page coincides with the last step of your Scenario.

Shopping Cart Events

The Marketing Warehouse uses the query parameters in this section to populate the `CartEvent` table:

`WT.tx_e=a/r`

A value of `a` identifies an addition to a shopping cart. A value of `r` identifies a removal from a shopping cart.

`WT.tx_cartid`

`WT.tx_cartid=`*`CartIdentifier`*

Pass a unique value to identify a visitor's cart. The Marketing Warehouse uses this parameter to identify events associated with a specific cart.

`WT.pn_sku`

`WT.pn_sku=`*`productSKU[;…]`*

Identifies the SKU (a unique numeric identifier) of the product.

`WT.tx_u`

`WT.tx_u=`*`Units[;…]`*

Identifies the quantity in the transaction. Note that the values for WT.pn_sku and WT.tx_u are tied together item-for-item in sequential order.

`WT.tx_e=a`

Identifies an addition to a shopping cart.

Search Events

Search events, which are populated in the SearchEvent table are determined by inspecting the referrer on the first page view for a visit. The parameters in this section help to characterize the search event.

`WT.srch`

`WT.srch=`*`SearchEngineType`*

Categorizes the search event as either "paid" (if `WT.srch=1`) or "organic" (`WT.srch` is not supplied or empty).

Configuring the Log File Management Role Settings

The Log File Management Role settings allow you to configure Log File Pre-Processor settings. The Log File Pre-Processor collects SmartSource Data Collector (SDC) log files from the location you specify, add GeoTrends and DNS data to the log files, and makes them available to the WebTrends Marketing Warehouse components.

To configure the Log File Management Role:

1. In the left pane of the WebTrends Analytics Administration Console, select **Administration > System Management > Role Settings**.
2. Select **Log File Management**.
3. In the **Log File Source Directory** text box, specify the location of your SDC log files. Because the Event Database Splitter prepares the log files for the Event Database Loader, modifying the original format, you should create a batch process that copies your SDC log files from the SDC storage location to the location you specify here.
4. In the **Log File Extension** text box, specify the SDC log file extension. Use a comma or a semi-colon to separate multiple extensions.
5. *If you want to add geographical data (state and country) to the SDC log files specified in the **Log File Source Directory** text box*, select the **Enable GeoTrends Lookups** check box. The GeoTrends Server must be installed if you enable this setting or the profile processing stalls.
6. *If you want to add resolved domain names to the SDC log files specified in the **Log File Source Directory** text box*, select the **Enable DNS Lookups** check box.
7. *If you want to specify a DNS server for the Log File Pre-Processor to use*, specify the domain name or IP Address of that server in the **Override DNS Server** text box.
8. *If you want the Log File Pre-Processor to save the processed log files after they are prepared for the Marketing Warehouse*, clear the **Delete Processed Logs** check box. You should only clear this check box if you plan to use the log files as the data source for a WebTrends Analytics profile (such as an Express Analysis profile). If you decide to save the log files, you should create a batch process that moves the log files to another storage location at regular intervals because the log files consume a large amount of disk space.

Configuring User Rights for WebTrends Marketing Warehouse

If you are a WebTrends administrator, you must give users the necessary user rights for using the WebTrends Marketing Warehouse components: the WebTrends Marketing Lab Desktop and the Marketing Warehouse.

To configure user rights:

1. In the left pane of the WebTrends Analytics Administration Console, select **Administration > Users**.
2. Edit a user, and give the user the appropriate level of access to WebTrends Marketing Warehouse components and features. The following table describes these rights:

User Right	Description
Event Database Free Form Queries	Specifies whether the user can run free-form SQL queries against Event Database data in your Marketing Warehouse.
Event Database Full Named Query Access	Specifies whether the user has access to confidential external data such as financial and user information when using Named Queries to query Event Databases in your Marketing Warehouse.
Explore	Specifies whether the user has access to WebTrends Explore in the Marketing Lab Desktop. Explore is used to interactively view data in an Event Database.
Goals	Specifies whether the user can create Goals for Marketing Lab Desktop Performs Dashboards.
Marketing Lab Desktop	Specifies whether the user can access the Marketing Lab Desktop installation program from the Install Components page of the WebTrends Analytics Administration Console. The Marketing Lab Desktop allows you to install and use Marketing Lab modules such as WebTrends Explore and Performance Dashboards.

User Right	Description
Marketing Warehouse Profiles	Specifies the user's rights to create, view, edit, and delete Marketing Warehouse profiles. Marketing Warehouse profiles specify the information needed to generate reports from your Marketing Warehouse. They define the location of a data source and specify the database location.
ODBC Driver	Specifies whether the user can install and use the WebTrends ODBC Driver. The WebTrends ODBC Driver allows you to query WebTrends data, including Marketing Warehouse and Report database data
Segment	Specifies the user's rights to create or apply segments to data in the Marketing Lab Desktop.

Creating a Marketing Warehouse Profile

When you create a Marketing Warehouse profile, WebTrends Analytics creates a MySQL-based Marketing Warehouse that allows custom querying of web activity data. As a best practice, deploy your new JavaScript tag and create and enable your profile as close together as possible. Also, consider creating and enabling your profile to coincide with a time frame boundary, such as the first day of the week, or the first day of the month. Doing so helps reduce differences between visitor counts for larger time frames that occur when you deploy the JavaScript tag days/weeks/months before creating the profile.

To create a Marketing Warehouse profile:

1. In the left pane of the WebTrends Analytics Administration Console, select **Web Analysis > Reports & Profiles**.
2. In the Profiles dialog box, click **New Profile**.
3. In the **Profile Name** text box, type a name to identify your profile in the User Interface.
4. In the **Web Site Domain Name** text box, type the home page of your web site.

5. *If you use WebTrends Analytics On Demand*, specify the time zone you want to use for displaying reports. For most users, this is the local time zone. WebTrends uses time zone information when counting traffic to your site to determine when days begin and end.

6. Select the **Advanced Profile Options** check box. Click **Next**.

7. In the Profile Class dialog box, select **Marketing Warehouse**. Click **Next.**

8. *If you use WebTrends Analytics software*, in the General dialog box, choose whether to use the Windows time zone and Daylight Savings Time offset used for report time, or click Specify Time Zone/DST Overrides to specify different time zone or DST offset settings. Click **Next**.

9. In the Data Source dialog box, select the data source you have defined for your Event Database data. If you have not yet defined a data source, click the Data Source link and define one. *If you use WebTrends Analytics software*, you can only select from SmartSource data sources. Click **Next**.

10. The Database Location dialog box provides default names for the Event and Module Databases. Unless you prefer an alternative naming convention, simply accept the default names. At least one Database Location (the one created during installation) is available for you to select. If you have installed additional MySQL databases for storing Marketing Warehouse data and those locations are not available in the Database Location list, you need to define the additional locations by clicking the Database Locations link. Click **Next**.

11. In the URL Rebuilding dialog box, select the URL Rebuilding definition to be applied to this profile. URL Rebuilding determines which query parameters to include when constructing a page (for example, when constructing entry pages). In most cases, you should use the same URL Rebuilding definition that you use for your WebTrends Analytics profiles. Click **Next**.

12. In the summary dialog, review the profile details, click **Save**. By default, the profile is configured to start analyzing data immediately. If you choose not to start analysis when you save the profile, you can start it at any time by editing the profile and selecting **Analysis Enabled** on the **Event Analysis** tab.

Chapter 6

Using the On Demand Account Console

In this chapter:

Setting Up WebTrends Analytics On Demand

This section describes how to set up a new WebTrends Analytics On Demand account after you have signed up for the service. Setting up your account involves the following steps:

- Logging in to WebTrends On Demand
- Creating a data source
- Creating a profile
- Viewing your reports

Logging in to WebTrends On Demand

To log in to your account:

1. You receive confirmation of your registration by email. The email contains your Account Name, User Name and Validation Key. The Validation Key is necessary for the first time you log in to WebTrends On Demand. You will need to know your password and navigate to `http://ondemand.webtrends.com`.
2. Log in to WebTrends On Demand with your Account Name, User Name, Password. You will then be prompted to re-enter your Password and to enter the Validation Key. Note that the information you enter is case sensitive.
3. Check your account settings. Click **Edit Account** to view information on the following:
   - **Account Information** shows your contact information.
   - **Billing Information** shows your cost information.
   - **Settings** shows information about your current usage of some settings and your contracted limit.

To continue setting up a new WebTrends On Demand account, see “Creating a Data Source”.

Creating a Data Source

To set up your WebTrends On Demand account, you specify a data source that will be associated with your profile.

1. From the Account Console, click **Administration Console**.
2. In the left pane, click **Administration > Data Sources**.
3. Click **New Data Source** and select the appropriate time zone.
4. Type a name for the data source in the **Data Source Name** text box.
5. Click **Tracking** to Generate any additional tracking tags you might need or want
6. Click **Download this tag**. Note that the tag is created from the information you provided in your settings. The tag directs information about the activity on your web site to WebTrends Analytics On Demand.

7. Click **Save** to add this new data source to the list of data sources.
8. Implement the WebTrends JavaScript tag on all of the web pages you want to track. For more information see "Implementing the JavaScript Tag on Your Web Pages" in the Administration Console Help.

To continue setting up your WebTrends On Demand Account, see "Creating a Profile".

Creating a Profile

Part of setting up your WebTrends account is creating a profile that identifies the web site activity that you want to report on. Your data is collected, analyzed, and displayed in your WebTrends On Demand reports.

1. In the left pane of the Administration Console, click **Web Analysis** > **Reports & Profiles**.
2. Click **New Profile** to define your profile. You associate a data source with your new profile while completing the New Profile Wizard.
3. At the end of the New Profile Wizard, you can review a summary of your selections for your profile. Click **Save** to accept the settings for the profile or define the advanced settings that you want.

   If you want to define more settings to further customize your profile, click **Advanced Settings**. Included in the tabs for these settings are tabs representing the dialog boxes that you completed in the New Profile Wizard. The additional tabs you see depend on choices you made in the New Profile Wizard.

   For more information on configuring Advanced Settings, see **Help**.
4. Click **OK** to close the confirmation message.
5. Click **Account Console** in the left pane to return to the Account Console.
6. Click **log out** to exit WebTrends On Demand.

WebTrends generates your first reports within a few hours.

Using the Account Console

The Account Console provides access to all features of WebTrends On Demand. When you first log in, a list of all accounts associated with your main account is displayed in the account list. The following section describes the components of the Account Console.

Administration Console

Allows you to create profiles and reports in order to analyze your web traffic activity, fine-tune user settings, and manage data sources.

Log Out

Logs you out of the WebTrends On Demand service.

Help

Opens the online Help system.

Accounts

Create Account/Create Subaccount

Allows you to create an account if you have administrator rights for a reseller or master account, or have licensed the ability to create sub-accounts within your account.

Edit Account

Allows you to modify settings for the selected account. Edit Account settings contains contact information, billing information, and other account settings information.

Delete Account

Allows you to delete the selected account if you have administrator rights.

Account History

Shows a list of significant events for the account selected, such as the creation of a profile. You can sort the list by date, action, or event details. Select an event, and click **View Item** for details.

Account Usage

Provides a summary of licensing statistics about the account selected, such as the number of profiles and custom reports used. For more information, see "Checking the License Status" on page 8.

FTP Access

If your account is licensed for features such as the Log File Delivery Service that require access to the WebTrends FTP server, this option allows you to log in to transfer files.

Email Branding

If you have a master or reseller account, this option allows you to customize the content of automated email message that WebTrends On Demand sends to your customers.

Product Branding

Allows you to customize the links and images shown in the WebTrends Account Console, Reporting Console, and Administration Console.

Request Report Update

Allows you to submit a request to reanalyze past data for a profile when you change configuration settings that affect the consistency of reporting data. You can request a Live Report Update for data up to 90 days old.

Users

Allows you to manage user rights for each account in the Account List.

Select an account in the list to work with that account's users and associated rights. You can also edit, remove, and add user rights if you have administrator rights for your account.

My Settings

Contact Information

Lets you review and change your contact information.

Change Password

Lets you change your password.

Mailing Lists

Lets you review and change your mailing list preferences.

Toolbar Commands

Feedback

Lets you provide general product feedback, report a problem, or request a feature.

Help (for this page)

Opens the online Help system.

Working with User Settings

From the Account Console, you can manage the users associated with each account listed by adding users, modifying access rights, and removing users from the account.

Adding a User

Note

To fine-tune these access rights settings, select **Administration > Users** in the Administration Console.

To add a user:

1. Select the account from the Account Console that you want to work with.
2. Click **Users** in the left pane, and the users who are currently members of the account are displayed.
3. Click **Add User**, and the New User dialog box opens.
4. In the **Login Username** text box, type a username that contains 4-30 alphanumeric characters. It must not contain spaces.
5. In the **Email** text box, type a valid email address for the user. The new user receives a welcome email that provides information needed to log in to WebTrends.
6. In the **First Name** text box, type the user’s first name.
7. In the **Last Name** text box, type the user’s last name.
8. In the **Company** text box, type the organization or business this user belongs to.

9. In the **Password** text box, select Auto-Generate Password to have a password automatically created for the user, or select Specify Password to define a custom password for the user.
10. Select the rights for the new user in the **Step 2 of 2** dialog box. See Help for a description of each user right.
11. Click **Apply Changes**.

Creating Multiple Users at Once

If you have a master or reseller account, you can create multiple user accounts at once by specifying them in comma-delimited text format.

To create multiple users at once:

1. Select the account from the Account Console that you want to work with.
2. Click **Users** in the left-hand menu, and then select **Add Multiple Users**.
3. Enter each user on a separate line in the User List dialog box in the following format:

   ```
   Username,User E-Mail,First Name,Last Name,Right IDs
   ```

   For example:

   ```
   Sue,Sue@Mail.com,Sue,Miller,1 5
   ```

   To view a list of right IDs, select the **Click Here to View List of Valid Right IDs** link in the dialog box.

   Note
   You can generate this user list from an external database, and copy and paste that data in the User List dialog box.

Changing Account Information

You can update contact information for your account in the **Edit Account** dialog.

To modify account information:

1. Select the account from the Account Console that you want to work with.

2. Click **Edit Account** in the left-hand menu. For more information about these settings, see Help.

   Your licensing agreement determines the maximum number available. Fore more information, see "How WebTrends On Demand Is Licensed" on page 9.

   Note
   You may be able to adjust the maximum values if you have a master or reseller type of account.

Viewing Account History

You can view activity data for your account in the Account History dialog box. This dialog displays the date of the event, actions taken, and event details. This information can be very helpful for administering the account. For example, if you need to find out who deleted a profile or received a specific report, you could find those details here.

Note
The Account History list can be sorted by Date, Action, and Details.

To view account history:

1. Select the account from the Account Console that you want to work with.
2. Click **Account History**, and a list of events is displayed.
3. Select an item in the list, and click **View Item** in the left-hand menu to show event details.

Creating an Account

If you are a reseller of WebTrends On Demand, you have multiple accounts under one main account for billing and administrative purposes. As a reseller, you have one main reseller account that contains all your customer accounts and within those accounts, it is possible to have sub-accounts.

If you have licensed sub-accounts for your account, you can also create accounts.

To create a new account:

1. Log in to WebTrends On Demand.
2. From the Account Console, click **Create Account/Create Subaccount**.
3. The **New Account Creation** dialog box indicates the account that you are logged into. Be sure that this is the account that you want associated with the new account.
   - ***If you have a master type of account***, you can select **Add New Reseller Account** to add a reseller account. Reseller accounts contain customer accounts which you can administer.
   - ***If you have a master or reseller type of account***, you can select **Add New Customer Account** to create an account associated with the reseller account selected. A single company may have a single customer account and multiple sub accounts within the account for each division, department, product, or other segment that requires separate reporting.
   - ***If you want to create an account for the select customer account***, click **Add a Sub-Account to An Existing Customer Account**. Sub-accounts share the resources of the account such as profiles and custom reports.
4. Click **Next Step**, and the **Account Information** dialog box opens. Enter the required information, and click **Next Step**.
5. If you are creating a new reseller account, the **Account Service Settings for New Reseller Account** dialog box opens. Enter the maximum number of child accounts, custom profiles, custom reports, and report exports that this new account should have. The dialog box displays the quantities available to be distributed from the master account to the reseller account.
6. Click **Next Step**, and the **User Information** dialog box opens. Enter the required information in the text boxes.
7. Click **Next Step** to review settings for the account, and click **Submit Registration** if you are satisfied. Otherwise, click **Back** to make changes.

Setting Up WebTrends On Demand Small Business

WebTrends On Demand Small Business maintains all of your log files and makes sure that these files are associated with the profiles that you create.

Setting up your account involves the following steps:

- Logging in to WebTrends On Demand
- Creating a profile
- Viewing your reports

Logging in to Your Account

1. Click the URL provided in the confirmation email from WebTrends.
2. Log in to WebTrends On Demand with your user name, account name, password, and license key. Note that the information you enter is case sensitive.
3. Click **Edit Account** so that you can check your account information. Here you can review the following:
   - **Contact Information** shows your contact information.
   - **Billing Information** shows your cost information.
   - **Shows** information about your current usage of some settings and your contracted limit.

Creating a Profile

Part of setting up your WebTrends account is creating a profile that identifies the web site activity that you want to report on. Your data is collected, analyzed, and displayed in your WebTrends On Demand reports.

To create a profile:

1. Click **Profiles & Reports** to identify a named group of settings with which you identify the visitor activity data on your web pages. The information about this activity will be collected and stored on the WebTrends servers and then analyzed and finally displayed in your WebTrends On Demand reports.
2. Click **Add Profile**.
   a. Type a name for the profile in the **Profile Name** text box.
   b. Specify the location of the Web page you want to analyze in the **URL** text box.
   c. Specify the time zone you want reflected in your reports in the **Time Zone** text box.

d. Use the arrows to specify the users who have access to this profile in the **User Access** text box.

e. Specify the day of the week that should be considered the first for reports in the **First Day of Week** setting.

f. If there are visitors that you do not want to include in the analysis for this profile, enter the IP Address for that activity in the **IP Exclude Filter** text box. For example, you might not want to count visitors from your own company.

3. Click **Add Profile**. The **JavaScript** tab is highlighted and WebTrends JavaScript tag is displayed.

   Note that the tag directs information about the activity on your web site to files that log the information. The files "log" the activity.

4. Copy the WebTrends JavaScript tag.

5. Paste the tag between the <body> and </body> tags on all of the web pages you want WebTrends On Demand to track.

   As soon as you have pasted the WebTrends JavaScript tag to your deployed Web pages, your Web site traffic data is collected by WebTrends servers. Comprehensive reports on your site activity will be ready for viewing within the next 24 hours.

Generating Reports

After you create a profile and copy the JavaScript code to your Web pages, you can log in to WebTrends On Demand to view your reports. It typically takes up to 24 hours after tagging your pages before report data starts showing.

To test your configuration, we recommend generating approximately 30 hits to your test pages. Wait an hour and generate a similar number of hits. This procedure is not required for profiles associated with live web sites, because these sites typically already receive a steady stream of traffic.

Using the Account Console Small Business Edition

The Account Console provides access to all features of WebTrends Analytics On Demand. This section describes the features and settings available from the Account Console.

Reports & Profiles

You can use the Reports & Profiles module to manage profiles in order to analyze your web site activity and create reports. A profile defines how data from an associated data source should be analyzed and reported.

Accounts

You can use the Accounts module to manage your account settings, to view a log of significant events, and a summary of statistics about your account.

Users

You can use the Users module to manage account users and their rights. You can also edit, remove, and add user rights if you have administrator rights for your account.

My Settings

You can use the My Settings module to update your contact information, change your password, and subscribe to WebTrends mailing lists.

Log Out

You can click **Log Out** to exit your On Demand account.

Help

You can click **Help** to activate the online Help system.

Viewing WebTrends Reports

After you have completed the set up procedures described earlier in this chapter and your web site activity has been analyzed, you can view reports.

To view your reports:

1. Log into WebTrends On Demand.
2. In the left pane, click **Reports & Profiles**.
3. Select a profile in the list and click the profile name.

Chapter 7
Installing and Using GeoTrends

This chapter describes how to install and use GeoTrends. GeoTrends enhances both pre-defined and custom reports with demographic and marketing data by using the client machine's IP address to look up information such as area code, region, country, city, state, and market segmentation information. In pre-defined reports, the main differences when using GeoTrends are reflected in several visitor-related reports, especially those reports under the Geography heading.

For an example of how WebTrends uses GeoTrends data, look at the Countries report in the **Visitors > Geography** reports folder. This report shows the top countries of the visitors to your site. Without GeoTrends, the report shows only one country category called **Unknown Origin**. When creating custom reports, GeoTrends dimensions (listed and described in the following section) are always available. However, you need to install GeoTrends to get meaningful information for these dimensions.

Note

GeoTrends is not available for WebTrends Analytics On Demand Small Business Edition, and GeoTrends data does not appear in reports for Basic Parent-Child profiles in either WebTrends software or On Demand.

Information GeoTrends Provides

All WebTrends users receive the Basic GeoTrends software, which delivers base-level reporting. For more detailed reporting, you can purchase licensing options to receive Advanced GeoTrends.

Basic GeoTrends

Basic GeoTrends provides the following information:

Geography Dashboard

Key graphs and tables that provide an overview of geographic information of the visitors.

City

The city associated with the client machine's IP address.

Country

The country associated with the client machine's IP address.

Region

The world geographic region associated with the client computer's IP address.

State, Province, Territory

The state (of the United States of America), province (of Canada), or territory (of Australia, Brazil, Germany, Great Britain, Japan) associated with the client machine's IP address. Note that for Japan, you may receive a code that coordinates with a Prefecture. In some cases, such as Australia, GeoTrends provides an abbreviation of the federal state or territory.

Advanced GeoTrends

Advanced GeoTrends provides the following information:

Geography Drilldown

Report format that allows you to drill down to more geographic information about visitors.

Area code

The area code associated with the client machine's IP address. Note that the area code covers only IP addresses in the United States and Puerto Rico.

DMA (Designated Market Area)

A DMA consists of all counties whose largest viewing share is given to stations of that same market area. Non-overlapping DMAs cover the entire continental United States, Hawaii and parts of Alaska. There are currently 210 DMAs throughout the U.S.

MSA (Metropolitan Statistical Area)

MSAs are relatively freestanding Metropolitan Areas and are not closely associated with other Metropolitan Areas. These areas typically are surrounded by non-metropolitan counties. A Metropolitan Area (MA) is defined as one of a large population nucleus, together with adjacent communities that have a high degree of economic and social integration with that nucleus. Some MAs are defined around two or more nuclei. Each MA must contain either a place with a minimum population of 50,000 or a Census Bureau-defined urbanized area and a total MA population of at least 100,000 (75,000 in New England).

PMSA (Primary Metropolitan Statistical Area)

If an area that qualifies as a metropolitan area has more than one million people, PMSAs may be defined within it. PMSAs consist of a large urbanized county or cluster of counties that demonstrates very strong internal economic and social links, in addition to close ties to other portions of the larger area..

Note

Because GeoTrends relies on IP addresses to look up data in the database, it is recommended that you do not select Resolve Mode in the Domain Name/IP Resolution Mode drop-down list of the Internet Resolution dialog box. Also, ensure that your web server is not configured to perform DNS lookups for IP addresses as it creates the log file. In both instances, you will have to resolve domain names back into IP addresses before you can benefit from the GeoTrends data.

Installing GeoTrends

GeoTrends is an optional component that can be installed during the standard WebTrends installation. You can also add it to your installation as described in “Adding Components After Installation” on page 27. If your WebTrends installation CD-ROM is not available, you can download the GeoTrends database through the Administration Console by selecting **Install Components** in the left pane and **Accessories** in the right pane. Click the GeoTrends link.

You can install GeoTrends on the same computer as the core WebTrends application, or you can install it on a different computer. If you install GeoTrends on a separate computer, the installation updates the WebTrends database with the location of GeoTrends.

Activating GeoTrends

In order to activate GeoTrends after you install it, you must stop and restart the WebTrends Services to activate your GeoTrends installation.

Determining if GeoTrends Is Installed

To confirm that GeoTrends is installed:

1. In the left pane of the Administration Console, select **Administration > System Management Hosts**.
2. If GeoTrends is installed, the list of components includes GeoTrends Server.

Getting Updates

You can check for updated versions of GeoTrends through the WebTrends Administration Console.

To get updates:

1. In the left pane of the Administration Console, select **Install Components**.
2. Click **Check For New Components**.
3. WebTrends looks for updated versions on the WebTrends Web site. If a newer version is available, the dialog box includes a link to download the new version.
4. Click **Update GeoTrends Data**.
5. Save the installation program to a computer running WebTrends, and run the installation program from the saved location.
6. GeoTrends is updated automatically once a day, or you can run the `geotrendsupdate.exe` to update it immediately. The `geotrendsupdate.exe` is located in *`WebTrends Installation Directory`*`\common\lib\` on the computer where GeoTrends is installed.

Chapter 8

Creating a Profile

This chapter describes the kind of information stored in report profiles and provides instructions for creating a profile using the Basic and Advanced profile wizards. For more information about using each dialog in the profile wizards, see the Administration Console Help.

How Profiles Work

Profiles specify all of the information needed to generate reports from a web data file. They define the location of your web server data and how it should be analyzed. For example, profiles can specify information such as:

- The type of web data WebTrends analyzes and where to find it
- Whether your web site resides on a single server or on multiple servers
- The location of your home page
- Whether to apply data filters
- Which users can access the profile
- Which reports to create
- When to update reports

Each profile is associated with a set of log files from which it draws data and one or more templates, which determine the set of reports that can be rendered from the analyzed data. When you analyze a profile, WebTrends creates a set of Report databases. You can use the WebTrends Reporting Console to view reports for a specified profile and template based on the data in the Report databases.

Profile Creation

To begin creating a profile, log into the Administration Console, select **Web Analysis > Reports & Profiles**, and click **New Profile**.

Using the Profile Wizard

WebTrends allows you to create profiles in two modes. In the Basic mode of profile creation, WebTrends uses the most common settings to produce reports quickly with minimum configuration. The Basic mode creates a Standard Full-Featured Analysis profile. You can also use the Advanced Profile settings to customize your profile by providing more information about your web data, your site configuration, and your reporting preferences.

To create a profile using the standard wizard:

1. In the Profile Name dialog box, provide a name for your profile and specify the web site domain name.
2. If you are a WebTrends On Demand user, specify the time zone you want to use when displaying your reports.
3. In the Data Source dialog box, specify a data source (if you have already configured one, or if you are a WebTrends On Demand user) or create a new one by specifying the location of your log file. If you are using WebTrends On Demand or your own Smart Data Collection server, you can use this dialog box to download the SDC tracking code that WebTrends uses to identify your web site.
4. In the Report Packs dialog box, specify the licensed report packs you want to use with the current profile. Report Packs determine what kinds of reports WebTrends creates, and thus the type of data included in reports for this profile.
5. In the Session Tracking dialog box, specify how to identify user sessions for the profile.
6. In the Summary dialog box, review your settings.

Advanced Profile Settings

Use the Advanced Profile settings if you want to configure special WebTrends features such as:

- Advanced SmartView reports
- Profile analysis scheduling (WebTrends software users only)
- Advanced reporting features including:
  - Campaign and Scenario Analysis
  - Content Group Analysis
  - Hit and Visit Filters
  - URL Parameter Analysis
  - URL Search and Replace

  Click **Additional Settings** in the last wizard dialog box to access these advanced settings.

You should also use Advanced Profile settings if you want to create special types of profiles such as Parent-Child profiles. For more information about configuring these specialized profile types, see the Help and the *WebTrends Advanced Configuration Guide*.

To create a profile using the Advanced Profile settings:

1. In the Profile Name dialog box, provide a name for your profile and specify the web site domain name.
2. If you are a WebTrends On Demand user, specify the time zone you want to use when displaying your reports.
3. Select the **Advanced profile options** check box. You see the Advanced Profile Options dialog boxes in the wizard listed in the left column.
4. Click **Next** to complete the dialog boxes. For detailed information about each setting, click the **Help** icon. To configure more profile options than the wizard provides, click **Additional Settings** in the Summary dialog box.

Advanced Profile Dialog Boxes

The following dialog boxes are included in the Advanced Profile wizard. For detailed information about how to complete each dialog box, see the Help. Dialog boxes marked with an asterisk (*****) may not be displayed depending on the wizard settings you choose.

Profile Name
: Specifies the name of the profile, the site domain name (used to identify the SmartView domain and the web site URL) and (for WebTrends On Demand users) the time zone.

Profile Class
: Specifies the type of web data to use and whether to create a standard, Advanced SmartView, Event Database, or Parent-Child report.

Site Configuration*
: Specifies whether your web data is stored in logs or a WebTrends Warehouse, and whether the web server resides on one server or multiple servers.

General
: Specifies the portion of the log to analyze, whether to retrieve HTML page titles, whether to enable Express Analysis, and time zone behavior.

Parent Child*
: Specifies the settings used to create a Parent-Child profile.

Data Sources
: Specifies the location of the web data file.

Home
: Specifies the location of the site home page.

SmartView
: Specifies whether to enable SmartView reporting. For advanced SmartView profiles, specifies whether to analyze the home page domain or another domain.

Page File Types*
: Specifies which file types WebTrends counts as page views.

URL Rebuilding*
: Specifies whether to apply settings that modify URLs before analysis to provide more accurate reporting.

Session Tracking*
: Specifies whether to apply profile-specific settings for tracking user sessions.

Schedule
: Specifies when analysis should occur.

Host Binding*
Specifies whether analysis should run only on certain computers or groups of computers.

Pre-Analysis*
Specifies whether any programs should run immediately before analysis.

Post-Analysis*
Specifies whether any programs should run immediately after analysis.

Chapter 9

Working with the Report Designer

This chapter provides information about how to use the WebTrends Report Designer to create and modify templates and dashboards. It also discusses how to set global options for reports.

Note

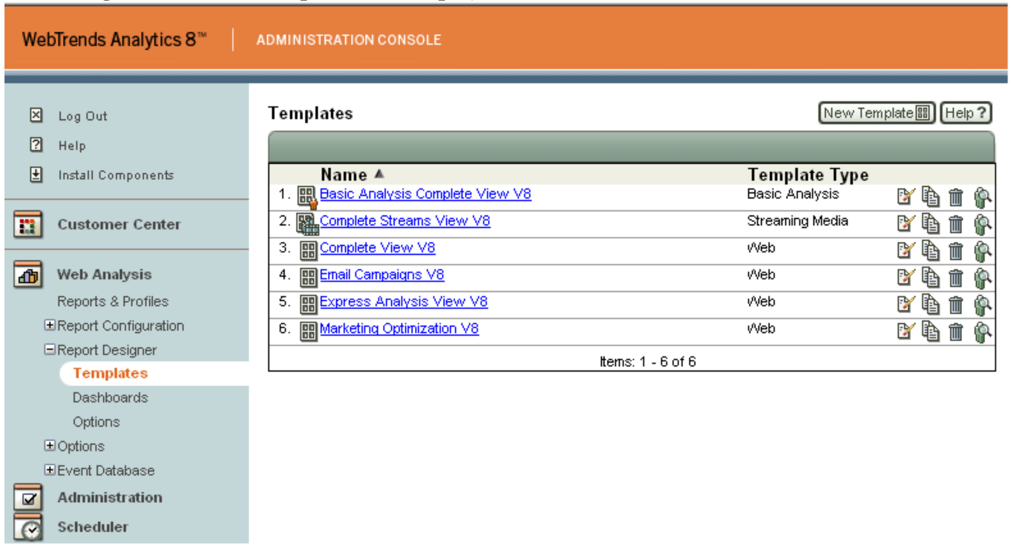
This feature is not available for WebTrends Analytics On Demand Small Business Edition.

Report Templates

Specify the appearance of your reports using report templates. A report template defines the content and layout of the report, including the tables, graphs, and language used. You can start with a blank template or modify one of the report templates that WebTrends provides to create new ones. Click **New Template** to configure a new template. If you choose to edit a report, you will note that the template settings are contained on tabs.

Template Settings

Select **Report Designer > Templates** from the left pane of the Administration Console. A list of available templates opens to the right. The following graphic shows the Report Designer with the Templates list displayed.



The icon preceding the name of the template indicates the template's type, and each type is listed in the Template Type column. Click the template name to view its settings. The icons at the end of each template are commands for **Edit**, **Copy**, **Delete**, and **Show Uses**. The **Show Uses** icon lists the reports or report components that currently use a configured object.

The template settings are described in the following sections.

General Tab

Use the General dialog box to name your template and specify its type.

Template Name

Type a name that identifies this template.

Templates are listed in the **Web Analysis > Report Designer > Templates** list and in the **Report Templates** list in **Reports & Profiles >** edit a profile **> Reports**.

Template Type

Specify this template's type. If you are editing a template, this control is disabled.

Content Tab

The left side of the tab displays the Table of Contents for the selected template; select any item in it, and the selected report or dashboard appears to the right. The following list describes the buttons available in this dialog box:

New Chapter

Adds a chapter to the item you select on the left. Enter a description you want to use for the chapter in the text box that opens. If you are editing a template, click **Save** at the bottom. If you are creating a new template, click on the TOC to add the new chapter name, and then click **Next**.

Delete

Removes the item you select the from this template. When editing, click **Save** at the bottom of the window. When creating new, click **Next**.

Move up, Move down

Moves the item you select up or down in the order of the reports in this template.

Add Report

Adds reports and dashboards to the folder you select on the left. Click **Done** to save your changes.

Add External Link

Specifies a Web page or image to be included in the report. The linked information is displayed in the report in a space that is the same size as the other dashboard items. Click **Done** save your changes to this template.

Express Viewer

Use this tab to select dashboards that are compatible with the Express Viewer. The list shows the available Express Viewer compatible dashboards for this template.

Language/Style Tab

Use this tab to specify the report layout, format, and default language for this template.

Default Language

Select the default language to use for this template. If desired, users can change the language while viewing reports.

Word Wrap

Select if you want to wrap long strings of text in reports or cut them off. Wrapping the text provides more information while trimming long strings makes for a shorter, cleaner report.

Report Graphs

Select this check box to include graphs in reports using this template. You can select the next check box to specify that the graphs should be minimized by default. If the length of your reports is an issue, you might not want to include graphs to limit their size.

Report Tables

Select this check box if you want to include tables in the reports using this template. You can also specify the default number of rows for the tables.

Help Cards

Select this check box to include help cards in reports using this template. Help cards explain the information in the report tables and describe how to use it. The information in the Help cards is relative to the data being shown in the report.

Template Access

Use this tab to define which users have View, Edit, and Delete rights to this template. You can use **Select All** or **Select None** for shortcuts to these check boxes if you have many users to work with.

Applying Templates

You apply templates in the Options section of the Report Designer. For more information, see "Report Templates" on page 108.

Note
For information about how to add, edit, and delete templates, see the Help.

Report Dashboards

Use dashboards to specify the graphs and summary tables relevant to your needs. These items are displayed in the report as clickable summaries that you can open to view a detailed report.

If you do not find a dashboard that contains what you need, you can either build a new Dashboard, or copy one you like and modify it.

Dashboard Settings

Select **Report Designer > Dashboards** in the left pane of the Administration Console. The Dashboards dialog box displays a list of pre-configured dashboards that you can include in your reports.

Dashboards are listed in groups of twenty. Click the **10** or **50** tabs to change the size of the list.

Use the links, such as **Go Forward 1**, **Next 20,** or **Last 20** in the bottom right and left corners of the list to navigate the dashboards.

Dashboard settings appear in two tabbed views described in the following sections.

General Tab

Name

Specify the unique name of this dashboard. It is used in the report table of contents and as the title of the dashboard in the report.

Title

Explains what type of information this dashboard contains. This description appears in the report just under the title for this dashboard.

Short Description

Explains what type of information this dashboard contains. This description appears in the report just under the title for this dashboard.

Note

Some Dashboard Descriptions that come loaded with WebTrends contain strings surrounded by `%%`. These strings are used as tokens that refer to localized text. If you change these tokens, the localized text function does not work. Also, the tokens are specific to the dashboard descriptions that use them. If you copy a dashboard description containing a token, replace the token with your own text.

Type Of Dashboard

Specifies the type of profile this dashboard is used with. For more information about different profile types, see Help. If you are editing a dashboard, this option is not available.

Express Viewer Compatibility

Specifies whether the dashboard can be used for Express Viewer reports. To make a dashboard compatible with Express Viewer, it can only include graphs. If you are editing a dashboard and any tables are configured in the **Content** tab, this setting is not available. Once you remove the tables, you can select this option.

Content Tab

You can modify the contents of a dashboard using this tab.

The **Content** tab opens showing the current elements included this dashboard. You can edit the presentation of each individual dashboard element or add additional reports or external links to your dashboard.

To add elements:

- Click **Add External Link** to link a URL to this dashboard. You configure the URL to show up as an image and when you click on this thumbnail, you are taken to the URL.

  Note

  You can link an image located on a Web server, a Web page, or a file such as a PDF or a spreadsheet that is stored on a Web server or a network drive. Use external links to provide information relevant to the report. For example, you can link a Web page that contains daily sales information and use the macros to present the appropriate data for the day that you generate the report.

- Click **Add Item To Dashboard** to add tables and graphs to this dashboard. You can select from a list of items that are categorized.

To edit how an individual report appears in the dashboard

- Click the top banner of the thumbnails to drag them where you want them to be displayed within the dashboard.
- Use the tabs near the top of the thumbnails to specify the type of graph to use.
- Click the edit icon at the top of a graph, table, or presentation to change included measures as well as display properties such as legends and value labels, or to specify the path to a background image.
- Quickly edit external links.
- Click the trash can icon to delete unwanted thumbnails.

Report Options

The Report Options settings enable you to configure default report settings for new profiles.

To edit individual reports themselves, make your changes to each profile using the profile editor.

Note

From the Administration Console, select **Web Analysis > Reports & Profiles**. Click the **Edit profile** icon to open the profile editor.

Reports

Use the **Report Periods** tab to define which reports you want enabled by default when you create a new profile. Because disk space and memory are needed to maintain the report data, only select the reports you need.

Generated Report Types
: Select the check boxes for the reports that you want created by default for each new profile.

Report Week Starts On
: Select the day of the week to start your reports.

Each time a profile is analyzed, WebTrends updates each of the report types selected. Because the data for each report interval consumes disk space and memory, you should only select the reports you need.

Report Templates

Templates are applied to profiles to format reports. Use this tab to define the default Report Template assigned when creating profiles. To add a report template to any of these groups, go to **Report Designer > Templates.** For more information, see the Administration Console Help or "Report Templates" on page 101.

Web
: Select the default template for new web server profiles.

Streaming Media
: Select the default template for new streaming media server profiles.

Basic Analysis
: Select the default template for profiles that report on SmartSource Data.

Chapter 10
WebTrends User Rights

This chapter describes how to assign user rights to various features of WebTrends Analytics. When you define users, you can specify the features they can access, their default profile settings, and the dialog boxes they see. You can also set up authentication within WebTrends, so users log in using user names and passwords you specify.

Note

If your web server is configured for Operating System Authentication, users must be given rights on the local machine or have a domain account. (If you choose not to set up a local user account, use WebTrends authentication.) For full details on setting up a local user, please refer to your operating system's documentation.

Adding Users

To add a user:

1. In the left pane of the Administration Console, click **Administration > Users.** A list of the current administrators and users opens.
2. Click **New User** 

. The Adding User dialog box opens.
3. In the **Login Name** text box, type the log in name for the user. If the **Password** and **Confirm Password** text boxes are displayed, type the password for the user.

   Note

   The password field appears only if Custom Authentication is enabled.

   ---

4. Type a descriptive name in the **User Name** text box. WebTrends uses this description in user lists elsewhere in the program.

5. In the **User Password** section, choose one of the following options:
    - Select your system to authenticate this user's password
    - Select WebTrends software to do the authentication. If you choose WebTrends software, enter the password and confirm it in the accompanying text boxes so that the WebTrends software recognizes the user.
6. If at any time you need to disable this user's WebTrends access, select the **Disable User** check box here. Disabling access does not delete or remove the user from WebTrends, it just suspends the ability to log in and use WebTrends. Click **Next**.
7. In the User Rights dialog box, set WebTrends privileges for this user. For more information, see Help. Click **Next**.
8. In the Preferences dialog box, specify this user's time zone, so that all WebTrends events are displayed in the user's local time.
9. Specify the session time out for this user. This setting determines how long this user can remain inactive before WebTrends automatically ends the session.
10. Under Start Page, specify the dialog box or report that you want WebTrends to display first when the user logs in. Click **Next**.
11. The **Summary** tab lists the current settings for the user you are adding. To save these settings, click **OK**. The user is added to the **Users** list.

    To log in to the WebTrends software as a different user, close both the Administration Console dialog box and the initial **Log In** dialog box before relaunching the WebTrends software.

About View Only Permissions

Users who have no other permissions than View Reports automatically use the Reporting Console instead of the Administration Console. While they can view the reports, they do not have access to any of the other controls.

The *WebTrends Report User's Guide* is available to help orient view-only users to the Reporting Console. You can download this guide from the WebTrends Customer Center

Chapter 11

Operating and Monitoring SDC

This chapter describes how to operate Apache-based SmartSource Data Collector (SDC) or Microsoft IIS-based SDC on a Web server that is running on Windows 2003/XP. If your Web server is installed on Windows, you can keep track of installation events by examining the Audit Log file and the Event Viewer, both of which are discussed in this chapter.

This chapter also describes how to monitor SDC and determine the general health of the Web server.

Operating SDC

Note
For more information about monitoring, see "Monitoring SDC" on page 125.

Setting Environment Variables for Windows

Before you start or stop SDC, make sure that your environment variables are set correctly.

For your SDC-enabled Web server to start, `WT_ROOT` must be set. You can set `WT_ROOT` as an environment variable or as a registry entry. The registry key is located in:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\WebTrends Corporation\SmartSource
Data Collector
```

The entry is stored in the `WT_ROOT` registry value. Note that the environment variable always takes precedence over the registry value.

Note
The necessary registry entry is made during installation.

Running Apache-Based SDC

Starting and Stopping SDC for Windows

You can start and stop your SDC-enabled Apache server using one of the following methods:

- Open the Control Panel, select **Services**, and start or stop the Apache service as needed.
- Open a command prompt and enter the following commands:

  `net start apache2` – Starts the Apache server.
  `net stop apache2` – Stops the Apache server.

Note
If you are running the SSL-enabled version of the web server, refer to "Uninstalling Smart-Source Data Collector" on page 62 for issues related to starting and stopping the server.

Error Reporting for Windows 2000/2003/XP

To verify that your Apache server started, use the Windows Task Manager to view the process list. You should see two Apache processes running.

If the Apache server did not start correctly, you can examine the error log file located in *`Apache installation directory/`*`logs/error.log`.

Additional errors may be logged in the application log of the Windows Event Viewer. The problem is most likely be due to an error in the `httpd.conf` file.

SDC Log File Location

The `logfiledir` setting in the `[logrotation]` section determines the storage location of SDC log files. You can configure these settings in the `dcs.cfg` file. If this directory does not exist, SDC creates it.

The SDC Audit log contains errors related to the `lfm_rotate` utility. If the utility is unable to log the errors in the SDC Audit Log, the errors are logged in the Apache error log.

Testing Your Log File

If you are unsure that your log file is receiving information correctly, follow these steps to test it.

1. Open a Web browser.
2. Type and execute the following command in the URL address field:

   `http://`*`SDC domain`*`/dcs.gif?dcsuri=/test.html&dcsref=xxx`

3. Open the SDC-generated log file and see if it contains a hit with `xxx` in the cs(Referer) field.

Viewing Apache Statistical Information

Apache contains a module that you can use to obtain statistical information for your Web server.

To enable this feature:

1. Verify that the `status_module` is enabled. This includes uncommenting the following to the `httpd.conf` file:

   Windows 2003/XP

   ```
   LoadModule status_module modules/mod_status.so
   ```

   Note
   Remove the # sign before each entry in order to uncomment the line.

2. Uncomment the following lines to the end of your `httpd.conf` file (applies to Windows 2003/XP:

   ```
   <Location /server-status>
   SetHandler server-status
   Order Deny,allow
   Deny from all
   Allow from .mysite.com
   </Location>
   ```

   where `.mysite.com` is your domain.

   Note
   Remove the # sign before each entry in order to uncomment the line.

3. Stop and start Apache.

4. You can access your Apache statistics using

```
http://<your.server.name>/server-status
```

Note

Hits to /server-status are not logged in your log file but are reported as invalid hits in the SDC log file. Because of this, enabling this module increases on the load on the SDC server.

Running IIS-Based SDC

Starting and Stopping SDC

You can start or stop your SDC-enabled IIS web server using one of the following methods:

- Open the **Control Panel**, select **Services**, and start or stop the **World Wide Web Publishing Service** as needed.
- Open a command prompt and enter the following commands:

  `net start w3svc` – Start the IIS web service

  `net stop w3svc` – Stop the IIS web service

  If you have made any SDC configuration changes, you must stop and start the IIS Admin Service for the changes to take effect. Stopping/starting the IIS Admin Service can be accomplished by executing the following from a command prompt:

  ```
  net stop iisadmin /y
  ```

  ```
  net start w3svc
  ```

SDC Log File Location

The `logfile` directory setting in the `[logrotation]` section determines the location of the SDC log files. You can configure these settings in the `dcs.cfg` file. If this directory does not exist, SDC creates it.

Testing Your Log File

If you are unsure that your log file is receiving information correctly, test your log file.

To test the log file:

1. Open a Web browser.
2. Type and execute the following command in the URL address field:

   `http://`*`SDC web server domain`*`/dcs.gif?dcsuri=/test.html&dcsref=xxx`

3. Open the SDC-generated log file and see if it contains a hit with `xxx` in the cs(Referer) field.

SDC Audit Log

SmartSource Data Collector records significant events in an audit log file. Additionally, SDC can record the events in the Event Viewer under Windows 2000/2003/XP. This allows SDC to log to a centralized system log. The `[auditlog]` section of the SDC configuration file contains settings used to configure where to log information, and level of log information to write. For more information about configuring audit file logging see the "SDC Configuration" chapter of the *WebTrends Advanced Configuration Guide*. Changes to the configuration file (`dcs.cfg`) become effective after the Web server is stopped and started.

Audit Log Location

The audit log file is located in the following directory:

`SDC installation directory``\log\dcs.audit` (Windows 2000/2003/XP)

The entries in the `dcs.audit` file have the following format:

```
Date: ####
Message
```

Information logged in the audit log file ranges from critical errors to debug information. The `debuglevel` parameter in the configuration file dictates what level of messages are logged in the audit log. You may log errors, warnings, or both.

If your operating system uses a FAT32 file system, you can keep the audit log file from growing beyond the operating system limits by truncating or rotating the file.

The `dcs.cfg` file contains the following parameters that control logging.

- The `auditlimitbysize` parameter file enables audit log file truncation or audit log rotation.
- The `auditmaxsize` parameter determines how large the audit file grows before being truncated or rotated.
- The `auditlimitbysizemethod` parameter determines whether the audit log is truncated in place or rotated to a new file name.
- If you are truncating the audit log, the `audittrimsize` parameter determines how much of the audit log file is retained prior to truncation. Therefore, you can retain only the most recently written information.
- If you are rotating the auditlog, when the audit log reaches the `auditmaxsize`, it is rotated (copied) to a new name. The format of the file name is:

  `prefix-YYYY-MM-DD-HH-0mmss-hostname.ext`

  Where:

  > *`prefix`* is the auditlog specified in the `auditfilenameprefix` setting located in the `[auditlog]` section. The default is `dcs`.
  >
  > *`YYYY`* is the four-digit year of the first hit in the file.
  >
  > *`MM`* is the two-digit month of the first hit in the file.
  >
  > *`DD`* is the two-digit day of the first hit in the file.
  >
  > *`HH`* is the two-digit hour of the first hit in the file.
  >
  > *`0mmss`* is the five-digit number that is a combination of zero plus minutes plus seconds of the first hit in the file.
  >
  > *`hostname`* is the machine name of the SDC server that created the file.
  >
  > *`ext`* is the `auditfilenameext` setting located in the `[auditlog]` section.

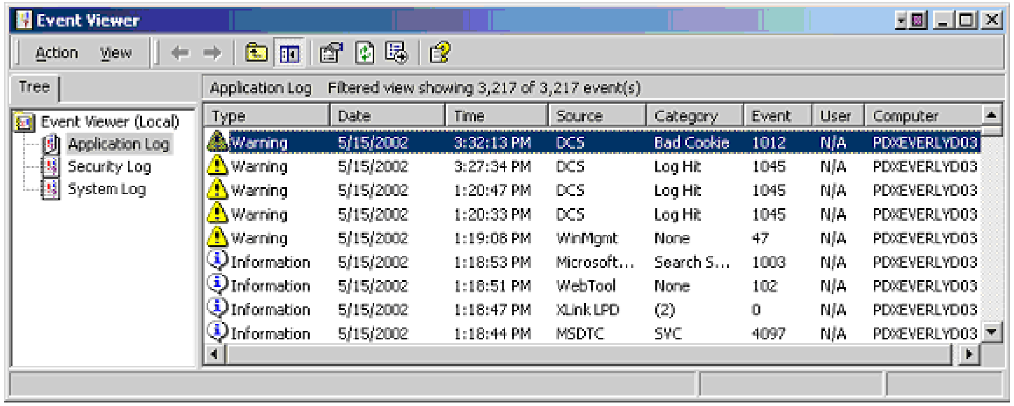
  Example:

  ```
  dcs-2004-02-10-00-05330-sdcd03.audit
  ```

Using the Event Viewer (Windows 2000/2003/XP)

You can configure SDC to write error and warning messages to the application log in the Event Viewer. In the event header, the event Source column must contain SDC as the identifier. The event Category gives a broad indication of the type of error or warning that occurred. The event Description contains the same text that is found in the SDC audit log file. Refer to your operating system's documentation for specific details related to the Event Viewer.

The following graphic shows SDC warning messages that have been written to the Event Viewer:



Hit Count Tracking

Note
Hit count tracking is supported only on IIS-based installations.

Once SDC is up and running, you may want to monitor the number of hits being processed. You could wait until the SDC-generated logs have been analyzed by WebTrends and then view the reports. Or you could simply monitor the size of the SDC-generated log files. A better method is to use the hit count tracking feature that is built into SDC. When hit count tracking is enabled, SDC writes hourly hit count information to the hit count log file (HCLF).

The hit count flush rate dictates the timing of writes to the HCLF. When the flush rate interval expires, the HCLF is opened, written to, and closed. The HCLF is typically created when the first flush occurs. Thereafter, hit count data is appended to the HCLF. If the HCLF is deleted underneath a running SDC, another is created at the time of the next flush.

Naming of Hit Count Log File

By default, the Hit Count Log File resides under the `SDC installation directory/log`. The name of the HCLF reflects its creation time, and the machine it is running on. The naming convention is:

Server_CreationTime.hclf

Where

Server The machine name of the computer where SDC is running.

CreationTime GMT time when HCLF was created. Format is of the form *yyyy_mm_dd_sssss* where

`yyyy` The four-digit year

`mm` The two-digit month

`dd` The two-digit day

`sssss` The five-digit number of seconds since midnight (padded with leading zeros) and ranges from 0 to 86,398.

You can configure the location of the HCLF using the `hitcountlogfiledir` setting in the `[logserver]` section.

You can configure the file name extension of the HCLF using the `hitcountlogfileext` in the `[logserver]` section.

For example, if you selected the default SDC installation folder, your IIS-based SDC machine name is `dcs01`, and the HCLF was created on `Thu Feb 14 11:09:00 2002`, then the HCLF file name would be:

```
C:\Program Files\WebTrends\SmartSource Data Collector\log\
dcs01_2002_02_14_68940.hclf
```

Contents of Hit Count Log File

The HCLF is an ASCII file. The first line in the file contains a header that describes the format of the hit count records. The remaining lines contain the hit count data in comma separated format.

The header syntax is as follows:

```
#entry,flush-time,interval-time,id,raw-count,proc-count,type,
server,agent,firsthit-time,lasthit-time
```

The following table provides description of each field within a HCLF record:

Field	Type	Description
`entry`	*Numeric*	Entry number for the record (line). Each record is sequentially numbered, starting with 1 up to a maximum value of 2^{64}. When a new HCLF is created, the `entry` value starts over again with the value of 1.
`flush-time`	*Numeric*	Time when data was written. Represented as the number of seconds since the epoch (UTC).
`interval-time`	*Numeric*	Hourly interval (bucket) in which the hits occurred. Represented as the number of seconds since the epoch (UTC). Will always be the beginning of an hour.
`id`	*Alphanumeric*	The DCSID. The following two DCSIDs are special cases: `0` represents the sum of all successful hits for the interval. `1000000` represents the sum of all unsuccessful hits for the interval.
`raw-count`	*Numeric*	The total number of hits. This is a number ranging from 1 to 2^{32}. If no hits are received for a given `ID` during the time period, then no record is written to the HCLF.
`proc-count`	*Numeric*	Same as `raw-count` field.
`type`	*Alphanumeric*	This field is always `DCS`.

Field	Type	Description
`server`	*Alphanumeric*	The machine name of the computer (for example, pdxdcs01) where SDC is running. Maximum length is 260 (including null terminator).
`agent`	*Alphanumeric*	Same as `server` field.
`firsthit-time`	*Numeric*	Time of first hit for a given record. Represented as number of seconds since the epoch (UTC).
`lasthit-time`	*Numeric*	Time of last hit for a given record. Represented as number of seconds since the epoch (UTC).

When a flush occurs, SDC writes out a record that contains the total number of hits during the interval. If no hits were received, then no record is written. If invalid hits occurred during the interval, an additional record containing the total number of invalid hits is written. If Hosted-Model SDC is enabled, non-zero hit count totals for each DCSID are also written. The `id` field serves to distinguish between a total hit count record (`id=0`), an invalid hit count record (`id=1000000`), and a DCSID-specific hit record (`id=`*`DCSID`*).

Examples

If you ran hosted-SDC on `dcs01` and did the following:

- Started SDC on Thursday, Feb 14, 2002 at 11:09:00 (1013713740 seconds since the epoch)
- Set the flush interval to 20 minutes
- Tracked the following DCSIDs: dcsknjb24gsu7s61pxz9uww73_7x5i, dcss5zx2u60f7xe4o8qw25a73_5q5w, and dcs4r3tysgsu7sq4d2prrhq73_4y1j

Therefore, the current `interval-time` is `Thu Feb 14 11:00:00 2002` (1013713200 seconds since the epoch). Note that for this example, hits between 11:00:00 and 11:08:59 are not counted.

At 11:20:00 (1013714400 seconds since the epoch), the first flush would occur. If the successful hit counts were:

DCSID	Hit Count
dcsknjb24gsu7s61pxz9uww73_7x5i	542
dcss5zx2u60f7xe4o8qw25a73_5q5w	26
dcs4r3tysgsu7sq4d2prrhq73_4y1j	1029

the records would look like this:

```
1,1013714400,1013713200,dcsknjb24gsu7s61pxz9uww73_7x5i,542,542,
DCS,dcs01,dcs01
2,1013714400,1013713200,dcss5zx2u60f7xe4o8qw25a73_5q5w,26,26,DC
S,dcs01,dcs01
3,1013714400,1013713200,dcs4r3tysgsu7sq4d2prrhq73_4y1j,1029,102
9,DCS,dcs01,dcs01
4,1013714400,1013713200,0,1597,1597,DCS,dcs01,dcs01
```

At 11:40:00 (1013715600 seconds since the epoch), the second flush would occur. If the successful hit counts were:

DCSID	Hit Count
dcsknjb24gsu7s61pxz9uww73_7x5i	3227
dcss5zx2u60f7xe4o8qw25a73_5q5w	877
dcs4r3tysgsu7sq4d2prrhq73_4y1j	665

the records would look like this:

```
5,1013715600,1013713200,dcsknjb24gsu7s61pxz9uww73_7x5i,3227,322
7,DCS,dcs01,dcs01
6,1013715600,1013713200,dcss5zx2u60f7xe4o8qw25a73_5q5w,877,877,
DCS,dcs01,dcs01
7,1013715600,1013713200,dcs4r3tysgsu7sq4d2prrhq73_4y1j,665,655,
DCS,dcs01,dcs01
8,1013715600,1013713200,0,4769,4796,DCS,dcs01,dcs01
```

At 12:00:00 (1013716800 seconds since the epoch), the third flush would occur. If the successful hit counts were:

DCSID	Hit Count
dcsknjb24gsu7s61pxz9uww73_7x5i	809
dcss5zx2u60f7xe4o8qw25a73_5q5w	1165
dcs4r3tysgsu7sq4d2prrhq73_4y1j	6244

and there were 4 invalid hit counts. The records would look like this:

```
9,1013716800,1013713200,dcsknjb24gsu7s61pxz9uww73_7x5i,809,809,
DCS,dcs01,dcs01
10,1013716800,1013713200,dcss5zx2u60f7xe4o8qw25a73_5q5w,1165,1165
,DCS,dcs01,dcs01
11,1013716800,1013713200,dcs4r3tysgsu7sq4d2prrhq73_4y1j,6244,6244,DC
S,dcs01,dcs01
12,1013716800,1013713200,0,8218,8218,DCS,dcs01,dcs01
13,1013716800,1013713200,1000000,4,4,DCS,dcs01,dcs01
```

At 12:20:00 (1013718000 seconds since the epoch), the third flush would occur. If the successful hit counts were:

DCSID	Hit Count
dcsknjb24gsu7s61pxz9uww73_7x5i	0

DCSID	Hit Count
dcss5zx2u60f7xe4o8qw25a73_5q5w	901
dcs4r3tysgsu7sq4d2prrhq73_4y1j	622

the records would look like this:

```
14,1013718000,1013716800,dcss5zx2u60f7xe4o8qw25a73_5q5w,901,901,D
CS,dcs01,dcs01
15,1013718000,1013716800,dcs4r3tysgsu7sq4d2prrhq73_4y1j,622,622,DCS,
dcs01,dcs01
16,1013718000,1013716800,0,1523,1523,DCS,dcs01,dcs01
```

Note that there is no record for `DCSID dcsknjb24gsu7s61pxz9uww73_7x5i` because its hit count was zero.

Configuring the Hit Count Log File

Configure the HCLF by modifying HCLF-related settings in the SDC configuration file, `dcs.cfg`.

Enable Hit Count Tracking

`trackhitcount [logserver section]`

Boolean that determines if hit count tracking is enabled. The default value for this setting is false.

Configure Rotation

The HCLF may be rotated by size and/or by number of times flushed. For flush-rate-based rotation, set `hitcountrotatebyflush=true` and set `hitcountflushesperrotation` to the number of flushes performed before the file is rotated. Note that flushes occur periodically based on the `hitcountflushrate` setting.

`hitcountrotatebyflush [logserver section]`

Boolean used to indicate if flush-based rotation is enabled. The default is false.

`hitcountflushesperrotation [logserver section]`

Integer that determines the number of flushes that occur before an HCLF is rotated. Only applies if `hitcountrotatebyflush` is true. The default is 3.

For size-based rotation, set `hitcountlimitbysize=true` and set `hitcountmzxsize` to the maximum size of the file (in MBs).

`hitcountlimitbysize [logserver section]`

Boolean used to indicate if size-based rotation is enabled. Only applies if `trackhitcount` is true. The default is false.

`hitcountmaxsize [logserver section]`

Integer that determines the maximum size (in megabytes) of the HCLF. Only applies if `hitcountlimitbysize` is true. The default is 1.

Advanced Configuration

While the default settings provide an operational SDC with hit count tracking, the hit count tracking settings listed below may need to be modified for your installation. Note that changes to the dcs.cfg file are not recognized until the web server is stopped and started.

`hitcountflushrate [logserver section]`

The number of minutes to elapse between hit count log file writes. Valid values are: 2, 3, 5, 6, 10, 12, 20, 30. The default and value for this setting is 20. This ensures that no more than 20 minutes of hit count data would be lost as a result of a catastrophic event.

Monitoring SDC

The environment in which SDC operates is a critical component of a successful installation. To reduce the risks of data loss, SDC must be deployed in an environment that provides high availability. This includes, but is not limited to, items such as incorporating the appropriate redundancy and alerting and monitoring.

While the configuration and setup of an environment that provides high availability is outside the scope of this document (and the SDC product), the following list identifies several of the key SDC-related items that should be monitored:

- The system resources on the computer hosting SDC (for example, CPU, memory, disk space)

- The SDC plug-in (to determine if it is installed)
- The health of the Web server hosting SDC, including the ability of the Web server to correctly respond to an HTTP request
- The SDC log file

You can use commonly available tools such as Perfmon along with specific characteristics of SDC to monitor system resources.

Regarding all other SDC-related items, you can use commonly available tools in combination with the following SDC characteristics to aid in the monitoring process:

- The content returned to a Web client in response to a valid SDC request is generated by a URL re-mapping process. Hits to the `dcs.gif` file are remapped to `wt_dcs.gif`. The SDC plug-in performs the re-mapping. If the SDC plug-in is installed and the Web server is functioning, hits to `dcs.gif` produce an HTTP response with a successful status code.
- Valid hits to the SDC are logged in a log file, which is found in a configurable location.

Installation Monitoring

To determine if the SDC plug-in is installed and to ascertain the general health of the Web server, a configuration may include the use of an external monitoring agent that periodically sends valid http requests to the SDC. If the SDC returns a valid response with a successful http status code, there is a high likelihood that the Web server is in a good state and the SDC is properly installed. This determination is based on the URL re-mapping process performed by SDC and the general nature of HTTP Web servers.

Log File Monitoring

The most important aspect of monitoring SDC is ensuring it continues to create a log file. All valid hits to SDC should be written to the SDC log file. Before describing a suggested monitoring configuration, however, the behavior of SDC logging mechanism must be understood. The following subsections describe this behavior.

Hit Validation

All hits to SDC are validated. In most cases, invalid hits are not recorded in the SDC log file.

The following list describes several types of validation:

- The uri-stem of the hit to SDC must tail-match a valid logging file name. The valid logging file names are determined by the values of the `loggingfilename/noscriptfilename` settings found in the `dcs.cfg` file. These values are typically `dcs.gif` and `njs.gif`.
- The DCSID is validated. The `dcsidbacktoversion` setting in the `dcs.cfg` file setting determines which version(s) of DCSIDs are valid. For more information, see "SDC Configuration" in *WebTrends Advanced Configuration Guide*.
- If SDC cookies are enabled and cookie validation enabled, the contents of the SDC cookies are validated. Note that SDC can still record hits associated with invalid cookies if the logging of invalid hits is enabled.
- The required parameters in the hit to SDC are present. The `DCS_URI` (typically `dcsuri`) is the only parameter that must be in the hit to SDC. Others parameters can be required by configuring SDC.

SDC Log File Name

This section describes the naming convention used for SDC log files.

The base portion of log file name is made up of pieces of information about the log file contents. The following example shows the base log file name syntax:

```
[REALTIMEID-]dcs-YYYYY-MM-DD-HH-0mmss-hostname
```

where

`[REALTIMEID-]` is the `realtime` field of the site map file if Express Analysis is configured (optional).

`DCS` indicates that SDC created the log file. This piece is always present and does not change.

`YYYY` is the four-digit year of the first hit in the log file.

`MM` is the two-digit month of the first hit in the log file.

`DD` is the two-digit day of the first hit in the log file.

`HH` is the two-digit hour of the first hit in the log file.

`0mmss` is the five-digit number that is a combination of zero plus minutes plus seconds of the first hit in the log file.

`hostname` is the name of the SDC server that created the hits in the log file.

For example, if Service Model SDC is enabled and Express Analysis is configured, the following file is generated on February 25, 2005:

```
express-dcs-2005-02-25-02253-sdcserver.log
```

Log File Extension

When SDC first creates the log file, the file has a `.dcsbusy` file extension. This extension indicates that SDC is actively writing to the file. After the log file is rotated, it is renamed to `.log`.

Log File Rotation

Log file rotation is the process of recording log hits in different files based on specific criteria. SDC uses the `rotationratestandardlag` setting in the `dcs.cfg` file to determine when log files should be rotated.

Logging Behavior

The behavior of the logging component of SDC is important when monitoring the resultant log file. The most critical issue to consider is the time when the hit information is actually written to disk. This varies based on the hosting Web server.

SDC has its own logging component. You can configure the behavior of this component based on setting found in the `dcs.cfg` file. The configuration covers the following:

- Buffered writes vs. non-buffered writes
- If buffered writes, the size of the buffer
- The amount of time between flushes, allowing you to limit the time hit data remains in the internal buffer before it is flushed to disk.

As hits are processed by SDC, they are passed to the log file controller. Based on SDC configuration, the hits are either immediately written to disk or placed in an internal buffer. If buffered writes are enabled, the internal buffer grows until the buffer reaches a configurable size. At that time, the hit data is written to disk. Periodically (as specified by the `heartbeatrate` and `bufferflushrate` settings), a check is made for buffers that have data in them but have not been flushed in a time exceeding the buffer flush rate. If this situation is detected, the buffer is flushed to disk.

Suggested Monitoring Configuration

With an understanding of the behavior of your SDC log files, you can use one of many commonly available monitoring tools to monitor the logging component. While the configuration varies depending on the monitoring tool you choose, the following example provides a high-level overview of a potential setup.

The sample setup includes an agent that makes HTTP requests to SDC and another agent that monitors the size of the data in the SDC log file. The HTTP agent periodically sends valid requests to SDC. At a rate greater than or equal to the rate of the HTTP requests, the other monitoring agent verifies that the SDC log file has grown. This size-monitoring agent must also take into consideration the issues associated with buffered vs. non-buffered writes. If the log file does not grow as expected, the monitoring agent must take the action appropriate for your SDC installation. This may be as simple as generating an alert to removing the particular machine from a farm of SDC servers.

When implementing a log file monitor, the following key issues should be considered:

- The agent must be aware of the log file naming conventions.
- The agent must be able to recognize SDC log file rotation.
- The agent must be aware of the SDC logging behavior.
- The agent must not interfere with SDC.
- A single valid DCSID should be used for the monitoring component. The external agent must send hits to SDC using the appropriate DCSID. The monitoring agent then needs to monitor the growth of the log file associated with the appropriate DCSID.

Chapter 12
Tagging Web Pages for SDC

This chapter describes how users of the SmartSource Data Collector (SDC) must tag their Web sites with the WebTrends JavaScript tag so that hits from their Web site are sent to SDC. It also provides information about customizing the tag.

- For more information about using the JavaScript tag, see "SDC JavaScript Tags" on page 131.
- For more information about using the VBScript tag, see "SDC VBScript Tags" on page 136.
- For more information about how META tags interact with SDC, see "Understanding META Tags for SDC" on page 140.

Note
If you use WebTrends On Demand, see the "Client-Side Integration for WebTrends On Demand" chapter in *WebTrends Advanced Configuration Guide* for information about tagging your Web pages.

SDC JavaScript Tags

About the JavaScript Tag

The tag records information about the hit to your tagged Web site and the subsequent forwarding of that information to SDC. SDC reconstructs the original hit from the query parameters and records it in a log file.

The tag is JavaScript v1.1 compatible and includes a tracking function that generates a series of Image objects. The creation of the Image object causes a hit to SDC. Through the use of an array of Image objects, many hits to SDC from a single Web page can be made in rapid succession. Particularly, it is well-suited for use with Flash applications. It should be noted that some versions of IE3 do not track the hits using this tag, because of incomplete support of JavaScript v1.1 – specifically the lack of support for the Image object.

Because the tag is a script, only Web pages that result in the execution of a script (such as `.html`, `.htm`, and `.asp`) can be instrumented using this method.

Finding the JavaScript Tag

If you use SDC, you can download the tag through the Administration Console.

To download the tag:

1. In the left pane of the Administration Console, click **Administration > Data Sources**.
2. Add or edit a SmartSource data source.
3. Select the **SmartSource Data Collector** tab.
4. Click **Download this tag**.

Modifying the JavaScript Tag

Note
Modify the JavaScript tag file in a way that preserves the integrity of the file and does not add any special formatting character or to any character conversion.

Tracking Multiple Domains

By default, the JavaScript tag is configured to pass the content domain. This is done by assigning a value to the `dcssip` parameter as follows:

```
DCS.dcssip=window.location.hostname;
```

This sets the domain from the URL address entered into the browser. For example, a request to `http://www.abcxyz.com` logs a domain of `www.abcxyz.com` while a request to `http://abcxyz.com` logs a domain of `abxcyz.com`.

An alternative to using `window.location.hostname` as the value is to "hard code" the domain name when assigning a value to `dcssip`. This ensures consistent results. Do this by modifying the following line:

```
DCS.dcssip=ContentDomain;
```

where *`ContentDomain`* represents the domain of the Web site you want to track.

For example, suppose you have two Web sites, `abcxyz.com` and `123.com`, and you want to track them using a single SDC. Insert your WebTrends JavaScript tag containing the `dcssip` parameter set to the appropriate domain on all pages on both Web sites. For example, on `abcxyc.com` pages, your tag contains the following line:

```
DCS.dcssip="abcxyz.com";
```

On `123.com` pages, your tag contains the following line:

```
DCS.dcssip="123.com";
```

Configuring By Hit

You can configure SDC through the settings stored in the `dcs.cfg` configuration file. Changes to settings come into effect after the Web server is stopped and started. You can override some settings on a per hit basis using the tag.

To configure SDC on a per hit basis:

1. Enable configure by hit. In the `dcs.cfg` file, set the `cfgbyhit` setting to true in the `[logserver]` section.
2. Determine the identifier that corresponds with the settings you want to override.

   To override a configuration file setting, you need an identifier. The identifier is a 8-digit hexadecimal value that is interpreted by SDC. Identifiers are listed in the following table:

Setting to Override	Identifier
Disable cookie processing	`00000001`
Disable first time cookie detection	`00000002`
Enable session cookies	00000004

   To override multiple settings, perform a bitwise AND of the individual identifier values.
3. Include the identifier in your JavaScript tag.
4. Configure your tag to pass the setting override for a given resource by enabling the `dcscfg` parameter.

To enable configure by hit, add a line to the `dcsVar( )` function:

```
DCS.dcscfg=identifier;
```

where

`identifier` represents the configuration settings to override. The identifier is an 8-digit hexadecimal value that is interpreted by SDC, and affects runtime behavior.

The following example shows how to disable cookie processing:

```
DCS.dcscfg=1;
```

5. In addition, you must configure the `<NOSCRIPT>` section by modifying

```
SRC=http://localhost/njs.gif?dcsuri=/nojavascript
```

to

```
SRC=http://localhost/njs.gif?dcsuri=/nojavascript
&dcscfg=identifier
```

Issuing Per-Hit P3P Headers

To issue per-hit P3P headers with SDC, you must configure your JavaScript tag to pass the compact policy and/or policyref. You can do this by enabling the dcsp3p parameters.

For more information on configuring SDC to issue per hit P3P headers, see the "P3P and SDC" section of the SDC Configuration Reference chapter in the *WebTrends Advanced Configuration Guide*.

Preventing Caching

To prevent caching, the Web client's current time is included as a URL parameter to the hit targeted at SDC. Each hit to the SDC server changes with time such that caching is prevented. Note that the time parameter sent to SDC is discarded and, therefore, not included in the SDC log file.

To accomplish this, a JavaScript Date object is constructed. The `getTime()` method is used to retrieve the number of milliseconds since 1970. This is then added as a parameter to SDC effectively preventing millisecond to millisecond caching.

Inserting the SDC JavaScript Tag

You can insert the JavaScript tag anywhere on your Web page between the `<BODY>` `</BODY>` tags. The advantage of placing the tag at the top of your Web pages lies in how the cancelled pages are handled. If a page begins to load and the page load is cancelled by clicking the **STOP** button on the browser, the page hit may not be sent to the SmartSource Data Collector (SDC) if the JavaScript code resides at the bottom of your Web page.

You can use one of the following methods to insert the tag into your Web site:

- Include file (see page 135)
- Inline script (see page 136)
- Dynamic pages (see page 136).

We recommend using the include file method.

Using an Include File

When you want to add the same code to numerous pages, you can use an include file that contains your JavaScript tag. Using an include file has an advantage when you must modify or upgrade the code. When you modify the code in the include file, it is automatically updated to all pages that have the include statement. You may implement the include from the client-side or from the server-side.

Client-Side Method

In JavaScript 1.1 and later, you can include the contents of an external file on every page of your web site. The SRC attribute of the `<SCRIPT>` tag lets you specify a file as the JavaScript source.

To implement this method, save the tag to a file, which is accessible to every page of your site, and then reference the file in the SRC attribute in each Web page. For example, suppose you saved your tag to a file named dcs_tag.js and placed it in the directory named `common`, which is located off of the document root. To include this file, add the following line to your Web pages:

```
<SCRIPT LANGUAGE="JavaScript1.1" SRC="/common/dcs_tag.js">
</SCRIPT>
```

External JavaScript files cannot contain any HTML tags; they must contain only JavaScript statements and function definitions.

Server-Side Method

Server-side includes (SSI) are enabled by default for Microsoft Internet Information Server and Apache Web servers. You can either configure the server to run SSI on all files with the extensions you use for your Web pages, such as `.htm` and `.html`, or you may need to change your page extensions, `.stm`, `.shtm`, and `.shtml`). Because additional processing is required when SSI is enabled, server performance may be adversely affected.

To implement this method, save the tag to a file that is accessible to every page of your Web site, and then reference the file in the `<!--#include…-->` statement in each Web page. For example, suppose you saved your tag in a file named `dcs_tag.js`, and placed it in the directory named `common` off of the document root. To include this file, add the following line to your Web pages:

```
<!--#include virtual="/common/dcs_tag.js"-->
```

Using an Inline Script

You can insert the JavaScript tag by adding the entire tag to each Web page (inline script). To implement this method, use an HTML editor or Notepad to insert the script.

Using Dynamic Pages

Uploading common code or text on every page of a Web site is one of the main reasons to use dynamic-database-driven Web tools. Most of these tools support the concept of a "template" which inserts common code automatically. Use the built-in method provided by your tool.

SDC VBScript Tags

About the VBScript Tag

The tag lets you record information about the hit to your Web site and subsequently forwards that information to SDC. SDC reconstructs the original hit from the query parameters and records it in a log file.

This tag is compatible with Internet Explorer 5.0 and includes a tracking function that generates an inline image. Use of this tag is not recommended with Flash applications (or any other situation that involves many tracking hits to the SDC from a single Web page.)

Because the tag is a script, only Web pages that result in the execution of a script (such as `.html`, `.htm`, and `.asp`) can be instrumented using this method.

Locating the VBScript Tag

If you use SmartSource Data Collector (SDC), the VBScript tag file is located in one of the following directories:

Unix

SDC Installation Directory`/util/vbscript/dcs_tag.vbs`

Windows 2000/2003/XP

SDC Installation Directory`\util\vbscript\dcs_tag.vbs`

Modifying the VBScript Tag

Specifying the SDC Domain

Before implementing the VBScript tag, you must first modify the script to match your SDC installation.

To prepare your VBScript tag, complete these steps:

1. Replace the two occurrences of `@@DOMAIN@@` string with the domain name or IP address of your SDC server.

   a. Look for the first occurrence between the `<SCRIPT> </SCRIPT>` tags. This instances handles cases in which the client is using a VBScript-enabled browser:

   ```
   strURL = strURL & "://@@DOMAIN@@/dcs.gif?".
   ```

   b. The second reference (between the `<NOSCRIPT> </NOSCRIPT>` tags) handles cases in which the browser is not Internet Explorer version 5.0 or greater:

   ```
   document.write "<IMG BORDER='0' NAME='DCSIMG' WIDTH='1'
   HEIGHT='1' SRC='http://@@DOMAIN@@/njs.gif?dcsuri=/novbscript'>"
   ```

Important
Modify the VBScript tag file in a way that preserves the integrity of the file and does not add any special formatting character or to any character conversion.

Tracking Multiple Domains

To track multiple domains with SDC, you must configure your VBScript tag to pass the content domain either by configuring the `dcssip` parameter or by using the `windows.location.hostname` function. We recommend that you use the `dcssip` parameter method.

To use the dcssip parameter:

1. Edit your VBScript tag file.
2. Change the following line:

   ```
   strURL = strURL & "&dcssip=yourdomain"
   ```

   to

   ```
   strURL = strURL & "&dcssip=contentdomain"
   ```

   where *`contentdomain`* represents the domain of the Web site you want to track.

For example, suppose you have two Web sites, `abcxyz.com` and `123.com`, and you want to track them using a single SDC. Insert your WebTrends JavaScript tag containing the `dcssip` parameter set to the appropriate domain on all pages on both Web sites. For example, on `abcxyc.com` pages, your tag contains the following line:

```
strURL = strURL & "&dcssip=abcxyz.com"
```

On `123.com` pages, your tag contains the following line:

```
strURL = strURL & "&dcssip=123.com"
```

To use the windows.location.hostname function:

1. Edit your VBScript tag file.
2. Change the following line:

   ```
   strURL = strURL & "&dcssip=yourdomain"
   ```

   to

   ```
   strURL = strURL & "&dcssip=" & Escape(window.location.hostname)
   ```

   This method sets the domain from the URL address entered in the browser. For example, a request to `http://www.abcxyz.com` logs a domain of `www.abcxyz.com` while a request to `http://abcxyz.com` logs a domain of `abxcyz.com`.

Configuring by Hit

You can configure SDC through the settings stored in the dcs.cfg configuration file. Changes to settings come into effect after the Web server is stopped and started. Certain settings may be overridden on a per hit basis with the SDC tag.

To configure SDC on a per hit basis:

1. Enable configure by hit.

   Set the `cfgbyhit` setting to true in the `[logserver]` section of the dcs.cfg file.

2. Determine the identifier that corresponds with the settings to override (currently, you can disable only cookie processing).

   To override a configuration file setting, you need an identifier. The identifier is a 8-digit hexadecimal value that is interpreted by SDC. Identifiers are listed in the following table:

Setting to Override	Identifier
Disable cookie processing	`00000001`

   To override multiple settings, perform a bitwise AND of the individual identifier values.

3. Include identifier in the VBScript tag.

   Configure your SDC VBScript tag to pass the setting override for a given resource by enabling the `dcscfg` parameter.

   To enable configure by hit, modify the line

   ```
   'strURL = strURL & "&dcscfg=yourcfg"
   ```

   to

   ```
   strURL = strURL & "&dcscfg=identifier"
   ```

   where

   `identifier` represents the configuration settings to override. The identifier is an 8-digit hexadecimal value that is interpreted by SDC, and affects runtime behavior. Currently, only `00000001` is supported (disable cookie processing).

The following example shows how to disable cookie processing:

```
strURL = strURL & "&dcscfg=00000001"
```

Issuing Per-Hit P3P Headers

To issue per-hit P3P headers with SDC, you must configure your VBScript tag to pass the compact policy and/or policyref. You can do this by enabling the `dcsp3p` parameters. For more information, see to the “P3P and SDC” section of the *WebTrends Advanced Configuration Guide’s* SDC Configuration chapter.

Preventing Caching

To prevent caching, the Web client's current time is included as a URL parameter to the hit targeted at the SDC. Each hit to the SDC server changes with time such that caching is prevented. Note that the time parameter sent to the SDC is discarded and, thus, not included in the SDC log file.

To accomplish this, a VBScript Date function is called. The `Timer()` function is used to retrieve the number of seconds since midnight. This is then added as a parameter to the SDC – effectively preventing second to second caching.

Inserting the VBScript Tag

You can insert the VBScript tag anywhere on your Web page between the `<BODY> </BODY>` tags. The advantage of placing the tag at the top of your Web pages lies in how the cancelled pages are handled. If a page begins to load and the page load is cancelled by clicking the **Stop** button on the browser, the page hit may not be sent to the SmartSource Data Collector if the VBScript code resides at the bottom of your Web page.

Understanding META Tags for SDC

The JavaScript tag supports the use of HTML `META` tags as a means of extending the collected data. By adding supported `META` tags to your Web pages, you can capture meta-data describing your Web content.

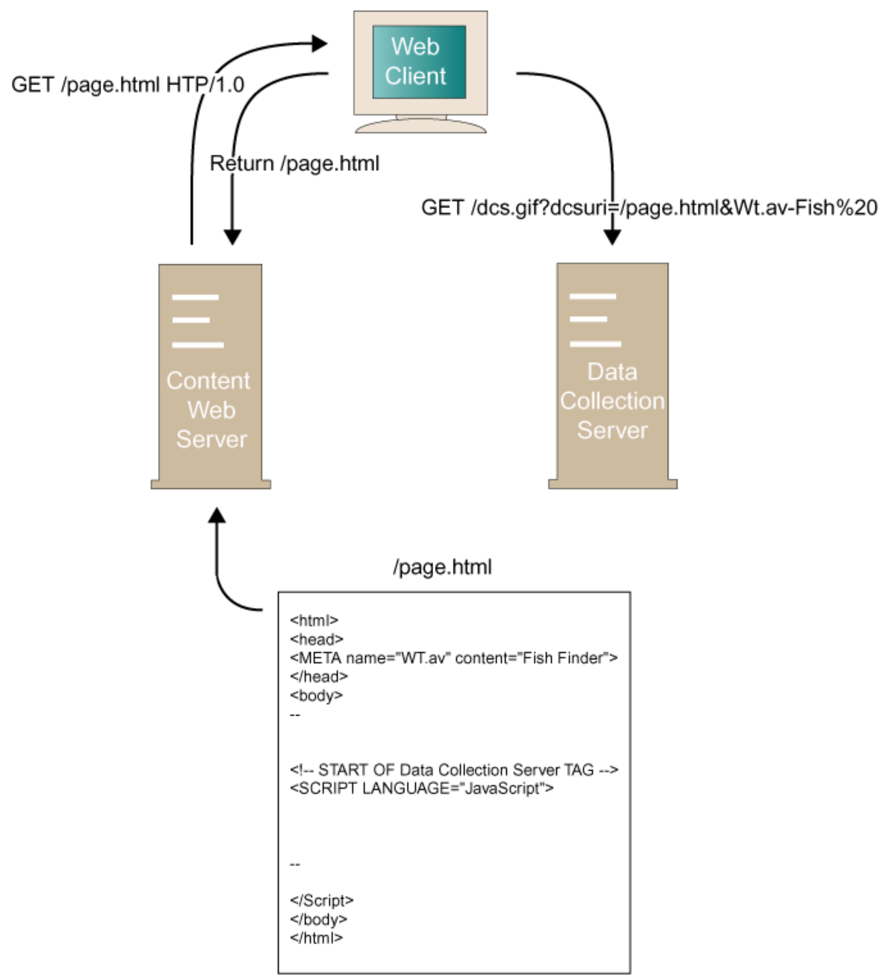
The tag takes advantage of Web browsers support of the Document Object Model (DOM) to capture the meta-data. When found, the meta-data is added to the SDC hits in the form of WebTrends query parameters. These query parameters are then used by WebTrends during the analysis process. For more information about supported parameters, see the "WebTrends Query Parameters" chapter in the *WebTrends Advanced Configuration Guide*.

Note

SDC support for `META` tags is limited to browsers that parse and make available the entire HTML document. For browsers without the appropriate support, which include browsers earlier than Microsoft Internet Explorer 4.*x*, Netscape Navigator 6.*x*, and Opera 6.*x*, the hit to the SDC is not augmented with data found in `META` tags.

In the following illustration, the Web client makes an HTTP request for `/page.html` from the Content Web Server. `/page.html` contains the JavaScript tag along with a WebTrends `META` tag.

```
<META NAME="WT.av"  CONTENT="Fish Finder">
```



When `/page.html` is received by the Web client, the JavaScript tag executes. This includes searching for WebTrends `META` tags and if found, adding the information to the hit to SDC. The query parameters added in this example are:

```
&WT.av=Fish%20Finder
```

Notice that the JavaScript tag escapes the value of the `CONTENT` attribute.

The instrumented hit is received by SDC, processed and logged. The logged hit looks like this:

```
2005-03-05 00:06:39 192.168.17.213 - - GET /page.html
WT.av=Fish%20Finder …
```

META Tag Syntax

The general syntax of the SDC-supported `META` tag is as follows:

```
<META NAME="name" CONTENT="content">
```

You must insert the `META` tag within the `<HEAD></HEAD>` tags.

The *`name`* represents the parameter name.

The *`content`* represents the parameter value. It should be noted that the length of the hit to the SDC is limited in size. In modern browsers, this is limited to 2k bytes. Since the `content` is included as a SDC hit parameter, its length is limited in size.

The additional parameters from the `META` tags are added to the query parameter list in the following fashion:

```
"&"+name+"="+URL-encoded content
```

Tagging Best Practices

Web Page Editor Issues

A number of HTML editors actually modify your HTML code and can break JavaScripts. Make sure that your HTML editor does not modify your HTML or the tag in any way.

Specify Character Sets On Tagged Pages

As a best practice, you should include a character set META tag on the pages that have your WebTrends JavaScript tag. For example, `<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">`.

If you don't specify the character set, a browser may use the character set defined on the previously viewed Web site. If that character set does not match the one you intend to be used on your own, your tags may not be consistently encoded. The resulting reports would show a single Web page as several different Web pages, and the text for the pages that were not encoded correctly may not be properly displayed.

Index

E

F

G

H

I

J

L

M

P

R

S