HP WebInspect Enterprise

for the Windows® operating system

Software Version: 10.10

Implementation Guide

Document Release Date: September 2013
Software Release Date: September 2013

Legal Notices

Copyright Notice

Copyright 2013 Hewlett-Packard Development Company, L.P.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Disclaimer of Warranty

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Trademark Acknowledgements

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Other Acknowledgements

This product contains the following Apache open source component: Log4Net (**http://logging.apache.org/log4net/**). This component was modified from its original form and incorporated into this software product. To learn more about the apache software license, please visit **http://www.apache.org/licenses/LICENSE-2.0**.

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, visit the following URL:

http://h20230.www2.hp.com/selfsolve/manuals

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

For information or assistance regarding WebInspect Enterprise, contact customer support.

You can open a support case for WebInspect Enterprise via e-mail, online, or by telephone. These options are designed to provide easier access and improved customer satisfaction.

E-Mail (Preferred Method)

Send an e-mail to fortifytechsupport@hp.com describing your issue. Please include the product name so we can help you faster.

Online (Fortify Support Portal)

Access your account at the Fortify Support Portal at **https://support.fortify.com**

If you do not have an account, you forgot your username or password, or you need any assistance regarding your account, please contact us at fortifytechsupport@hp.com or (650) 735-2215.

Telephone

Call our automated processing service at (650) 735-2215. Please clearly provide your name, telephone number, the name of the product, and a brief description of the issue.

You can access the HP Application Security Community containing customer forum and blogs at:

http://h30499.www3.hp.com/t5/Application-Security-Community/ct-p/sws-AS

You can also visit the HP software support Web site at:

http://support.openview.hp.com/

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides an efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

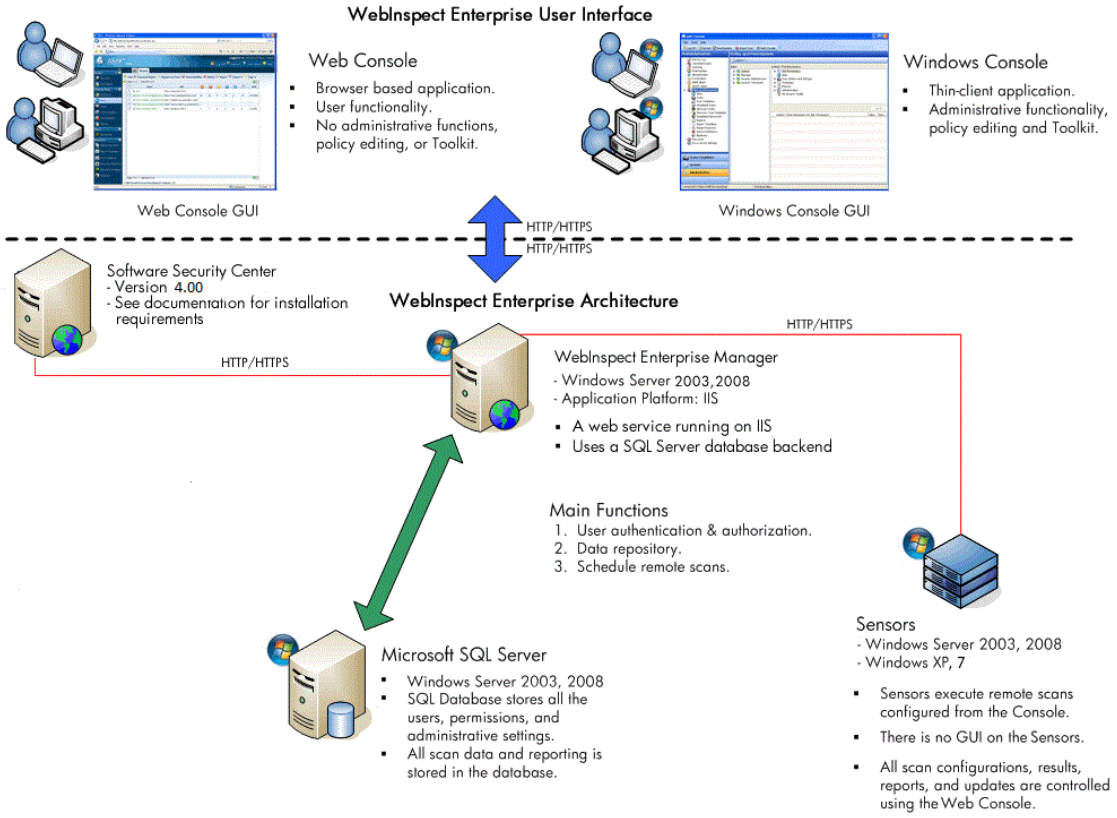
To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

WebInspect Enterprise Component Diagram

The following illustration depicts the main components of the WebInspect Enterprise System. These include the WebInspect Enterprise application, database, sensors, and users. These constitute the basis of the WebInspect Enterprise system for scheduled and remote scanning.



Database Size and Growth Settings

The initial size for the database for installation purposes can be as small as 1GB. This is not large enough for any scan data. The recommended minimum of 20GB will provide for the installation and the initial scanning objectives. This amount of space will not be enough to keep one year's worth of scan data for most organizations.

As each application scan will vary in size and scope, an average size scan is different for each customer. The best way to establish database size and growth requirements is to monitor the database size and compare it with scan activity. The best practice is to start with the minimum 20GB size requirement and note the unused space in the database after installation. As scans are performed, keeping a weekly data set comparing the number of scans with database growth will provide the best metric for average scan size at the customer site. Comparisons of the data set showing weekly, monthly, or quarterly metrics will provide the DBA with guidelines for proper size and growth settings.

WebInspect Enterprise Manager Account Requirements

WebInspect Enterprise users (both individuals and groups) are configured as Software Security Center (SSC) users and then assigned roles in WebInspect Enterprise.

WebInspect Enterprise interacts with two administrator accounts in SSC. One of them is a general SSC administrator. The other is the WebInspect Enterprise Service, which is used to share project versions and scans between SSC and WebInspect Enterprise, and which must be given the role in SSC of WebInspect Enterprise System.

WebInspect Enterprise requires two system accounts:

- WebInspect Enterprise Manager User - Domain user account with local administrator rights on the WebInspect Enterprise Manager
- WebInspect Enterprise Sensor User - Domain user account. No other privileges are required.

In general, configuring WebInspect as a sensor is optional during WebInspect installation, but WebInspect Enterprise requires you to configure at least one connected instance of WebInspect as a sensor. The configuration process is described in the *HP WebInspect QuickStart Guide*.

The sensor is WebInspect, and in general it is referred to as a *WebInspect sensor* or, when it runs on behalf of WebInspect Enterprise, as a *WebInspect Enterprise sensor*—the terms are interchangeable (and there is only one “WebInspect Sensor” Windows service).

The SSC administrator specified during WebInspect Enterprise installation automatically becomes the first WebInspect Enterprise system administrator. If that person later becomes unavailable, no one knows his password, and he has not created other system administrators in WebInspect Enterprise, you can rerun the WebInspect Enterprise Initializer, specify a different SSC administrator, and make that person a WebInspect Enterprise system administrator. This is also useful when moving the WebInspect Enterprise application to another computer.

SQL Database Account Requirements

If you are installing WebInspect Enterprise for the first time, you must have privileges to create a database (or your database administrator must create a blank database and assign ownership to you).

WebInspect Enterprise Initialize is used for database creation and WebInspect Enterprise Manager configuration changes such as changing the user account used to access the database.

WebInspect Enterprise Manager License Components

The WebInspect Enterprise license contains the license information for each component of the WebInspect Enterprise environment.

Sensors (Fixed) - The “WebInspect Sensor” Windows service installed by the WebInspect installation connects to WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans. It receives instructions exclusively from the configurable connection to a WebInspect Enterprise Manager.

The license information for sensors and users is located in the WebInspect Enterprise Console under **Administration** → **Licensing**.

WebInspect Enterprise Manager Installation Troubleshooting

For WebInspect Enterprise installation procedures, see the *HP WebInspect Enterprise Installation Guide*.

The most common errors encountered when installing WebInspect Enterprise are shown as either a connection message error at the final phase of the WebInspect Enterprise Initialize program, or when the first connection attempt is made with a console. Most of these error messages are general in nature. Consulting the logs for either WebInspect Enterprise Initialize or WebInspect Enterprise Manager should give some indication as to the nature of the error. The suggestions below are the most common quick methods to resolving the issues.

IIS Settings and File Permissions Used by WebInspect Enterprise

** File Root Path = C:\Program Files\HP\HP WebInspect Enterprise 10.10\ManagerWS\

** IIS Virtual Directory \WIE\

Folder	IIS Authentication	Notes	File Permissions
\	Integrated		User is Network Service with 'read' access. WIE Service User must be a local administrator
\App_GlobalResources	Integrated		
\App_Themes	Integrated		
\bin	Integrated		
\ClientBin	Integrated		
\GuidedSetup	Anonymous		
\Login	Anonymous	Getting a 401 status on this page means Anonymous auth has been disabled.	
\SmartUpdateService	Anonymous	Getting a 401 status when logging in to Smart Update means Anonymous auth has been disabled.	
\WebConsole	Integrated		

SQL Login

If the installation or initialization of the database is not successful, you must set up an SQL login. Then an SQL database user in the WebInspect Enterprise database must be assigned to the role “amp_server” and associated with that login. WebInspect Enterprise Initialize can then be run to specify the SQL login for connecting to the database.

Verify IIS Started/Running

If you cannot connect to WebInspect Enterprise using the console after installation, in Windows Administrative Tools → Services, verify that the Internet Information Services (IIS) Admin Service is running.

Account Rights and Privileges

Make sure the user logged into the machine during installation is a member of the local administrators group.

Make sure the WebInspect Enterprise Manager User is a member of the local administrators group.

If the Windows installation has been locked down, then the WebInspect Enterprise Web Service may not have sufficient rights to run. A quick test is to have the WebInspect Enterprise App Pool run as the Local System account.

Use the following procedure to set the application pool to run as another user:

1. Open the Windows Server Manager.
2. In the Server Manager window, under Server Manager (<*localhost*>), select **Roles** → **Web Server (IIS)** → **Internet Information Services (IIS) Manager**.
3. In the Internet Information Services (IIS) Manager window, expand the localhost in the Connections pane.
4. Click **Application Pools**.
5. In the list of application pools, select the WIEAppPool application pool.
6. In the Actions pane on the right, under the Edit Application Pool heading, click **Advanced Settings.**
7. In the *Advanced Settings* dialog, under the Process Model heading, click **Identity**.
8. Click the browse button to the right of the **Identity** value.
9. Change the value of the **Built-in account** field to **LocalSystem**.
10. Click **OK**.
11. Click **OK** on the *Advanced Settings* dialog.

If changing the application pool to run as the Local System account corrects the problem, start checking the permission details for the application pool user to enable appropriate permissions.

The application pool user (web service user) should have Read, Write, Read and Execute, and List Folder Contents privileges for the following directory:

Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files

The application pool user (web service user) should have Read, Read and Execute, and List Folder Contents privileges for the following directories:

\Program Files\HP\HP WebInspect Enterprise 10.10\

On Windows Server 2003:

\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA

On Windows Server 2008:

\ProgramData\Microsoft\Crypto\RSA

These are some of the more common directory permissions to research. It may be necessary to use a tool such as Procmon from Microsoft (originally produced by SysInternals) to show real-time file and registry access problems.

.NET Framework Registration

Make sure .NET extensions are allowed in IIS

Make sure the .NET 2.x and .NET 4.x extensions are marked as Allowed. For detailed information, see the *HP WebInspect Enterprise Installation Guide*.

Re-register the .NET framework with IIS

Each version of the .NET framework installed on the server includes the entire set of .NET components. The aspnet_regiis program is used to load and register the associated framework with IIS. The path below is the location of this tool for the current .NET 4.0 framework:

\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files

Using the command prompt, you can reinstall the framework and register it with IIS at the root web directory using the aspnet_regiis with the -i option.

The -i option installs this version of ASP.NET and updates scriptmaps at the IIS metabase root and for all scriptmaps below the root.

The command is formatted as: aspnet_regiis.exe -i

Restarting IIS Quick Commands

You must restart IIS during the troubleshooting steps to apply changes. Usually it is best to restart IIS whenever you make changes to the user rights for service accounts or user accounts related to the installation. The easiest method for restarting IIS is to use the following commands from the command prompt. The iisreset command will stop and start all the web sites and application pools running on the server. The additional options are self-explanatory.

- iisreset
- iisreset /stop
- iisreset /start

WebInspect Enterprise Manager Logging Customization

Use the WebInspect Enterprise logs to troubleshoot any errors that occur during the initialization process or when trying to use WebInspect Enterprise after installation. Increasing the verbosity of the logging is recommended in the event you need to send them to support for review.

The logs used for troubleshooting WebInspect Enterprise installations are:

- WebInspect Enterprise Initializer Log(s)
- WebInspect Enterprise Manager Log(s)
- WebInspect Enterprise Scheduler Service Log(s)
- WebInspect Enterprise Task Service Log(s)

These logs have a default 2MB size limitation and will keep a rolling set of five log files. Turning on debug logging is recommended for troubleshooting, but it is best to reset them to the default level of INFO after troubleshooting is complete.

WebInspect Enterprise Initializer Log Debug Settings

To increase the logging level for WebInspect Enterprise Initializer:

1. Edit the AmpInitialize.exe.logging.config file in the following directory:

   \Program Files\HP\HP WebInspect Enterprise 10.10\Initializer

2. Change the logging level from “INFO” to “DEBUG” in the following section:

```
<root>
  <level value="INFO"/>
  <appender-ref ref="RollingFile"/>
</root>
```

3. Save the file.

The logging output is located in the Initializer_trace.log in the following directory:

\Program Files\HP\HP WebInspect Enterprise 10.10\Initializer\

If additional files are created, they will be named Initializer_trace.log.1, Initializer_trace.log.2, etc.

WebInspect Enterprise Manager Log Debug Settings

To increase the logging level for the WebInspect Enterprise Manager:

1. Edit the Web.logging.config file in the following directory:

   \Program Files\HP\HP WebInspect Enterprise 10.10\ManagerWS\

2. Change the logging level from “INFO” to “DEBUG” in the following section:

```
<root>
  <level value="INFO"/>
  <appender-ref ref="ASPNetOut"/>
  <appender-ref ref="RollingFile"/>
</root>
```

3. Save the file.

The logging output is located in the ManagerWS_trace.log in the following directory:

On Windows Server 2003

\Documents and Settings\All Users\Application Data\HP\WIE\Manager\

On Windows Server 2008

\ProgramData\HP\WIE\Manager\

If additional files are created, they will be named ManagerWS_trace.log.1, ManagerWS_trace.log.2, etc.

WebInspect Enterprise Scheduler Service Log Debug Settings

To increase the logging level for the WebInspect Enterprise Scheduler Service:

1. Edit the AmpScheduler.exe.logging.config file in the following directory:

   \Program Files\HP\HP WebInspect Enterprise 10.10\Scheduler

2 Change the logging level from “INFO” to “DEBUG” in the following section:

```
<root>
  <level value="INFO"/>
  <appender-ref ref="RollingFile"/>
</root>
```

3 Save the file.

The logging output is located in the Scheduler_trace.log in the following directory:

On Windows Server 2003

\Documents and Settings\All Users\Application Data\HP\WIE\Scheduler

On Windows Server 2008

\ProgramData\HP\WIE\Scheduler

If additional files are created, they will be named Scheduler_trace.log.1, Scheduler_trace.log.2, etc.

WebInspect Enterprise Task Service Log Debug Settings

To increase the logging level for the WebInspect Enterprise Task Service:

1 Edit the AmpTaskService.exe.logging.config file in the following directory:

\Program Files\HP\HP WebInspect Enterprise 10.10\Task Service

2 Change the logging level from “INFO” to “DEBUG” in the following section:

```
<root>
  <level value="INFO"/>
  <appender-ref ref="RollingFile"/>
</root>
```

3 Save the file.

The logging output is located in the TaskService_trace.log in the following directory:

On Windows Server 2003

\Documents and Settings\All Users\Application Data\HP\WIE\TaskService

On Windows Server 2008

\ProgramData\HP\WIE\TaskService

If additional files are created, they will be named TaskService_trace.log.1, TaskService_trace.log.2, etc.

WebInspect Enterprise Manager Data Path Customization

By default, the WebInspect Enterprise Manager uses the All Users profile path as the SmartUpdate download, sensor upload, and WebInspect Enterprise Manager logging repository. Some installations may have limited space on the boot partition, which will require the redirection of these files and folders. Changes need to be made to both the web.config file and the Web.logging.config file to move both the logging and repository folders. The instructions for modifying each file are detailed below.

Modifying the web.config File (Moving the Storage Folders)

The web.config file for WebInspect Enterprise is located in the following directory:

\Program Files\HP\HP WebInspect Enterprise 10.10\ManagerWS

To change the data paths used by the WebInspect Enterprise Manager, add the following lines inside the <appSettings> element in the web.config file.

<add key="Manager.TempPath" value="D:\WIEData\temp" />

<add key=" Manager.BaseDataPath" value="D:\WIEData" />

Note: Instead of using the Manager.BaseDataPath key, you could add the following five lines to provide greater granularity.

<add key="Manager.ScanUploadsPath" value="D:\WIEData\ScanUploads" />

<add key="Manager.ScanImportPath" value="D:\WIEData\ScanImports" />

<add key="Manager.SensorUploadsPath" value="D:\WIEData\SensorUploads" />

<add key="SmartUpdate.ProductsFilePath" value="D:\WIEData\SmartUpdatePatches" />

<add key="Manager.PimCachePath" value="D:\WIEData\PimCache" />

If you do not want to change all of the paths, then you can comment out the appropriate lines.

Modifying the Web.logging.config File (Moving Logging Locations)

The log files are controlled by the Web.logging.config file. The configuration specifies an “appender” that is used to write the log entries to a file, and each appender has properties such as the log file path.

The default appender configuration uses the following settings:

<appender name="RollingFile"
type="SPI.Diagnostics.Logging.Appender.AppDataRollingFileAppender">

<file value="HP\WIE\Manager\ManagerWS_trace.log/”>

<appDataLocation value="AllUsers"/>

…

</appender>

This defines a log file where the path is relative to the “Documents and Settings\All Users\Application Data” directory if running Windows 2003 and the “\ProgramData\” directory if running Windows 2008. This works because the appender type is set to AppDataRollingFileAppender. If you want to change the configuration to use an absolute path for the log file, you must change the appender type to RollingFileAppender and replace the relative path with the absolute path. The appDataLocation setting will no longer be needed, so you can comment it out or delete it. The updated config section should look similar to the following:

<appender name="RollingFile" type="SPI.Diagnostics.Logging.Appender.RollingFileAppender">

<file value="D:\WIEData\logs\ManagerWS_trace.log/”>

…

</appender>

This same change can be made to the WebInspect Enterprise Scheduler Service and the WebInspect Enterprise Task Service logging configuration files.

- For the WebInspect Enterprise Scheduler Service, edit the AmpScheduler.exe.logging.config file in the directory \Program Files\HP\HP WebInspect Enterprise 10.10\Scheduler.
- For the WebInspect Enterprise Task Service, edit the AmpTaskService.exe.logging.config file in the directory \Program Files\HP\HP WebInspect Enterprise 10.10\TaskService.

Encrypting the Communication between WebInspect Enterprise and SQL 2005

Some customers may require the communication between the WebInspect Enterprise Web Service and the SQL Server to be encrypted. Standard Microsoft instructions for enabling SSL communication between these two components are available on the internet. The instructions are focused on configuring the WebInspect Enterprise web service to use the enabled SSL encryption after the Windows configuration is complete.

The steps below detail how to configure WebInspect Enterprise to use SSL encryption *after* configuring a certificate on the SQL Server machine *and* configuring the WebInspect Enterprise manager (SQL Client) to use the encryption. Details on setting up this configuration can be found in the following kb from Microsoft:

"How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console" - **http://support.microsoft.com/default.aspx/kb/316898**

Enabling WebInspect Enterprise to Use SSL

The instructions below detail how to modify the web.config file to use encrypted communication (SSL) after you have configured both machines as detailed in the Microsoft KB 316898 article.

After configuring the encryption on SQL 2005 and configuring the WebInspect Enterprise manager to use the encryption, you additionally need to modify the web.config file for the WebInspect Enterprise web service to utilize the encryption. The connection string is encrypted by default, which requires the steps below to decrypt the string, perform the necessary modifications, and then re-encrypt the string in the web.config file. Also, if you rerun WebInspect Enterprise Initialize, then you will need to redo this process, or keep a backup copy of the encrypted connection string.

Editing the Encrypted SQL Connection String Section of web.config

In the IIS Manager, go to Properties on the WebInspect Enterprise virtual directory, click the ASP.NET tab, and click Edit Configuration. Append "Encrypt=Yes" to the end of the connection string. This will handle decrypting and encrypting the connection string.

Note: This is not applicable to Windows Server 2008.

Encrypt Connection String in the TaskService.exe.config File after Modifying the web.config File

1. Stop the WebInspect Enterprise Task Service. At a command line, enter:

   net stop "WebInspect Enterprise 10.10 Task Service"

2 Locate the connectionStrings element in the web.config file. See below. Copy the data inside the "<CipherValue>…</CipherValue>" section and paste the data in the exact same section in the AmpTaskService.exe.config file.

```
<connectionStrings configProtectionProvider="DataProtectionConfigurationProvider">
  <EncryptedData>
   <CipherData>
    <CipherValue>M5KyPhzm+=</CipherValue>
   </CipherData>
  </EncryptedData>
</connectionStrings>
```

3 Restart the WebInspect Enterprise Task Service. At a command line, enter:

net start "WebInspect Enterprise 10.10 Task Service"

WebInspect Enterprise Sensor Installation

A user who installs a sensor must be a local administrator on that WebInspect machine. A sensor is part of the WebInspect installation package and it does not require its own license. The WebInspect Enterprise license contains the license information required to activate WebInspect sensors.

During WebInspect Enterprise installation, there are two alternative procedures for installing WebInspect sensors on behalf of WebInspect Enterprise. One procedure allows you to do either or both of the following:

- Test the sensor username and password credentials before starting the service
- Specify sensor connectivity to a remote SQL Server

Both procedures are described in the *HP WebInspect Enterprise Installation Guide*.

WebInspect Enterprise Sensor Remote SQL Server Standard Edition Connectivity

When configuring the WebInspect Enterprise sensor to write to a remote SQL Server Standard Edition instead of a local SQL Server Express Edition, observe the following considerations:

- The database for the Sensor must be created using the Sensor configuration. The user logged into the Sensor machine must have at least temporary rights to create a database on the SQL Server.
- The WebInspect Sensor service on the Sensor machine must use an account that can access the remote SQL database. This account needs read/write access to the SQL database created for the Sensor. By default, this service runs as the local system, which will not have access to a remote database if you choose Windows Authentication when configuring the database connection information. To use Windows Authentication, you must change how the service logs on, as follows:

  1 Right-click the HP Fortify Monitor icon in the task tray and select **Configure Sensor**.

  2 On the *Configure Sensor* window, in the Service Account section, select the option to Log on as **This account**.

  3 Enter a user name in the box next to **This account**.

4 Enter the account's password in the **Password** and **Confirm Password** boxes.

5 Click **Start**.

The user performing this action must have rights to create a database on this SQL server (or instance) or an equivalent SQL Server authentication account.

WebInspect Enterprise Sensor Logging

The WebInspect Enterprise Sensor log is in the following locations:

On Windows XP and Windows Server 2003:

\Documents and Settings\All Users\Application Data\HP\HP WebInspect\Amp\logs

On Windows Server 2008:

\ProgramData\HP\HP WebInspect\Amp\logs\

The file is named AMPSensorWI_trace.log. If additional files are created, they will be named AMPSensorWI_trace.log.1, AMPSensorWI_trace.log.2, etc. The name can be changed in the AmpSensorWI.exe.logging.config file located at Program Files(x86)\HP\HP WebInspect.

WebInspect Enterprise Sensor Scan Logs

Information regarding the scans performed by the WebInspect Enterprise sensor can be found in the same HP\HP WebInspect directory as described above for your operating system, but in the EnterpriseServer\logs\ subdirectory (rather than the Amp\logs\ subdirectory), and with the scan GUID as the further subdirectory name for each particular scan.

WebInspect Enterprise Sensor Directory Path Customization

By default, the WebInspect Enterprise Sensor uses the All Users profile path as the update download and sensor scan upload repository. Some installations may have small boot partitions that require the redirection of these repository folders. Changes need to be made to the SharedSettings.config file in the WebInspect folder to redirect the WebInspect Enterprise data path. This will modify all of the paths for the WebInspect Enterprise sensor, including both scan logs and scan data (if set to keep a local copy).

Keep in mind that this does not modify the locations for WebInspect data files. The WebInspect path settings are configured using the WebInspect interface.

Modifying the SharedSettings.config File

1 Stop the WebInspect Sensor service.

2 Edit the SharedSettings.config file in the following directory:

On Windows XP and Windows Server 2003:

\Documents and Settings\All Users\Application Data\HP\HP WebInspect

On Windows Server 2008:

\ProgramData\HP\HP WebInspect

3 Change the “AmpDirectory” value to point to the new location as shown below:

```
</setting>
  <setting name="AmpDirectory" serializeAs="String">
  <value>D:\Put_new_path_here</value>
</setting>
```

4 Save the file and restart the WebInspect Sensor service.

Retaining Copies of Scan Data on the WebInspect Enterprise Sensor

By default, the WebInspect Enterprise sensor deletes all locally stored scan data after the data has been uploaded to WebInspect Enterprise. If customers want to keep a copy of the scan data on the sensor, use the following procedure.

1 Stop the WebInspect Sensor service.

2 Create a file named AmpSensorWI.user.config in the following directory:

C:\Program Files\HP\HP WebInspect Enterprise 10.10

The file should contain the following:

```
<?xml version="1.0" encoding="utf-8"?>
<appSettings>
 <add key="KeepAllScanFiles" value="true"/>
     OR
<add key="KeepFailedScanFiles" value="true"/>  [Note: To keep scans with a status of "failed."]
</appSettings>
```

3 Save the file and restart the WebInspect Sensor service.

Scans run by the WebInspect Enterprise Sensor will store a local copy on the sensor machine, as well as uploading the data to the WebInspect Enterprise database.

General Database Settings for WebInspect Enterprise (SQL Server 2005)

The options for the database can be found by right-clicking the database and using the Properties menu. Some considerations for the WebInspect Enterprise database are listed below:

- Database files and transaction log files should be stored on different disks or partitions for better performance.
- The size of the database file should be set to the largest amount available on the system. Setting this value low and then allowing the database option to auto-grow the file will decrease performance once the size limit is reached. Some DBAs suggest turning off the auto-grow option and monitoring the file size, increasing the size of the database as it becomes larger. The logic is that once a database is full, and it starts to auto-grow, it will most likely do so during periods when the database is being used, which will cause system performance to degrade.
- If the database is performing poorly, turning off the auto-update statistics option may increase performance, as it may be running continuously on databases that are incurring large amounts of activity. If you turn off this option, you should run the Update Statistics Maintenance Task.

Database Maintenance for WebInspect Enterprise (SQL Server 2005)

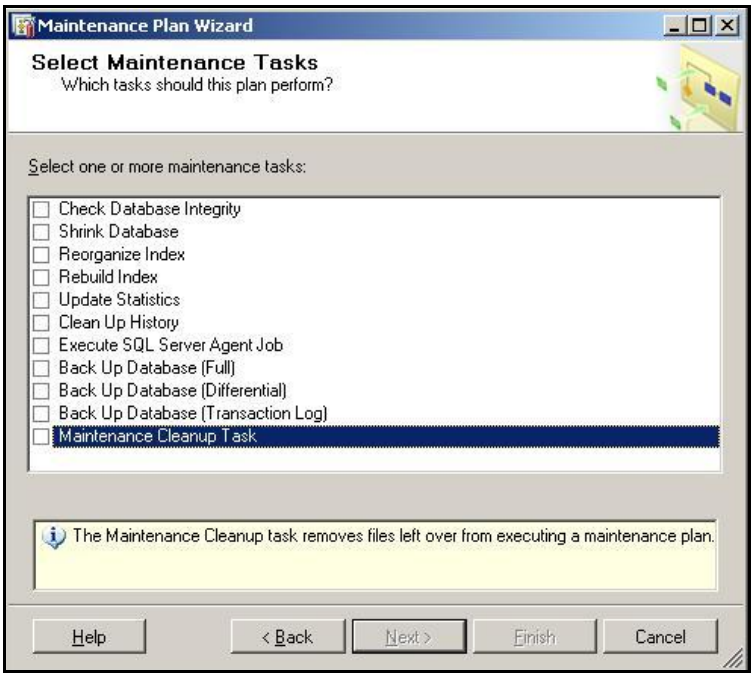
The descriptions included in this document cover only the most important maintenance tasks associated with database performance issues and are intended for customers that do not have a DBA on staff.

Note: With tasks that have multiple options, the recommended setting for the WebInspect Enterprise database is noted by the WebInspect Enterprise Recommended Options.

In SQL Server 2005, the Maintenance Plan Wizard guides you through a series of steps that request several bits of information for a complete plan that are saved as an SQL Server Integration Services package. This plan is executed by the SQL Server Agent Service. This service must be running in order for the Maintenance Plan to initiate.

The steps are listed in a logical order of progression for the tasks to be performed. Each option important for the WebInspect Enterprise database is listed followed by the general description of the selected maintenance task. Keep in mind that these are general suggestions for customers that do not have a DBA resource on staff.

The Maintenance Plan Wizard is located in SQL Server Management Studio. From **Management**, right-click **Maintenance Plan Wizard**. Multiple maintenance plans can be created and run on different schedules. It is generally recommended to run separate maintenance plans for the system databases (master, model, msdb) and user databases (the WebInspect Enterprise database).



WebInspect Enterprise Recommended Options

The maintenance plan should be scheduled to run during a non-peak time. It can be run daily, weekly, or monthly at the customer's discretion. Each should be configured to write the results to a common log directory and should be reviewed frequently to monitor the health of the database.

Check Database Integrity Task

The Check Database Integrity task checks the allocation and structural integrity of all the objects in the specified database. The task can check a single database or multiple databases, and you can choose whether to also check the database indexes.

Note: You can repair errors with the DBCC CHECKDB Transact-SQL command. Using a repair option with this command requires the database to be in single-user mode, which will take the database and WebInspect Enterprise application offline.

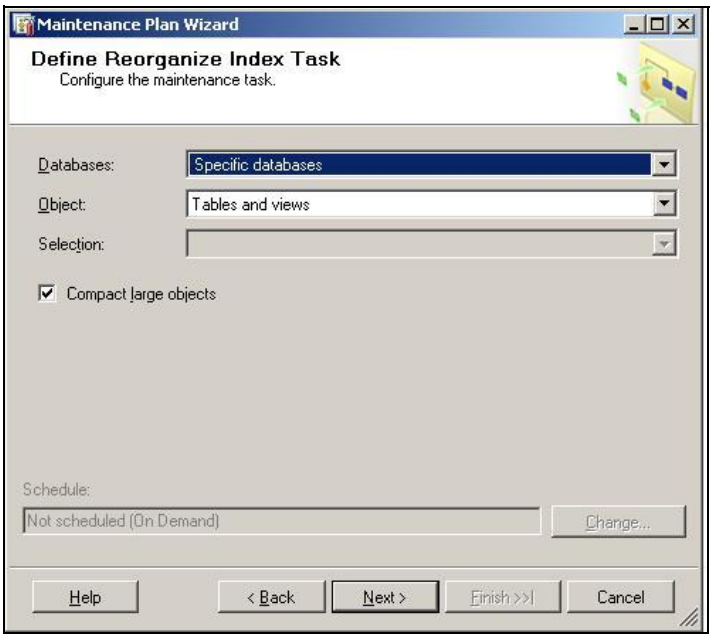
Database Fragmentation Maintenance

The Reorganize Index, Rebuild Index, and Update Statistics maintenance tasks come under the subject of fragmentation.

The SQL Server 2005 Database Engine automatically maintains indexes whenever insert, update, or delete operations are made to the underlying data. Over time, these modifications can cause the information in the index to become scattered in the database (fragmented). Fragmentation exists when indexes have pages in which the logical ordering, based on the key value, does not match the physical ordering inside the data file. Heavily fragmented indexes can degrade query performance and cause the application to respond slowly.

Reorganize Index Task

The Reorganize Index task reorganizes indexes in SQL Server database tables and views. Use the *Define Reorganize Index Task* dialog to move index pages into a more efficient search order. Having the pages in order improves index-scanning performance.

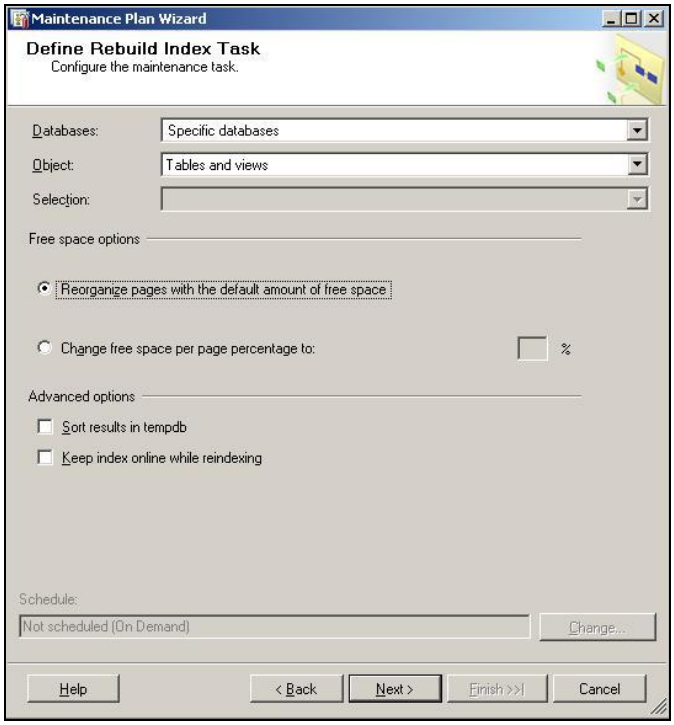


WebInspect Enterprise Recommended Options

Select the **Tables and views** object and the **Compact large objects** check box.

Rebuild Index Task

The Rebuild Index task rebuilds indexes in SQL Server database tables and views. Rebuilding an index drops the index and creates a new one. In doing this, fragmentation is removed, disk space is reclaimed by compacting the pages using the specified or existing fill factor setting, and the index rows are reordered in contiguous pages (allocating new pages as needed). This can improve disk performance by reducing the number of page reads required to obtain the requested data.

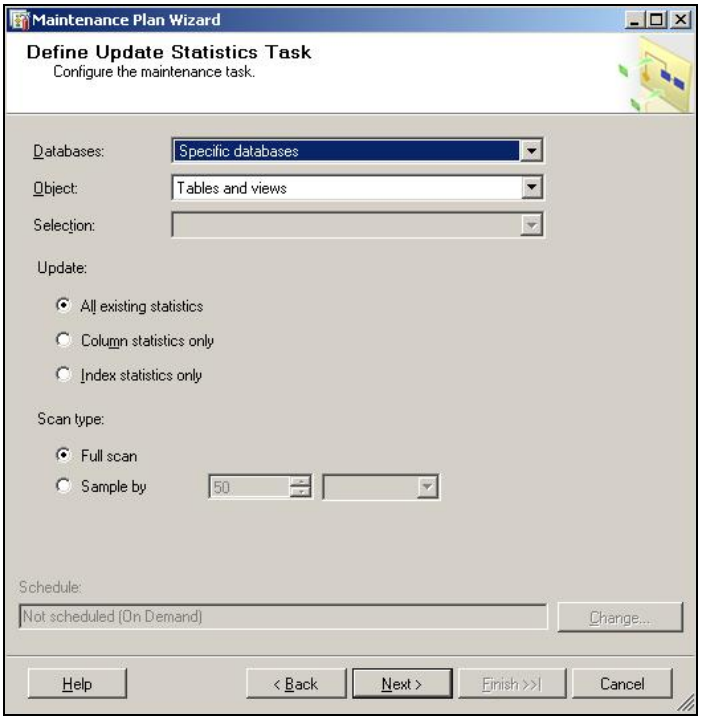


WebInspect Enterprise Recommended Options

Select the **Tables and views** object and the **Reorganize pages with the default amount of free space** option.

Update Statistics Task

The Update Statistics task updates information about the distribution of key values for one or more statistics groups (collections) in the specified table or indexed view. SQL Server 2005 allows for statistical information to be created regarding the distribution of values in a column. The query optimizer uses this statistical information to determine the optimal query plan by estimating the cost of using an index to evaluate the query.



WebInspect Enterprise Recommended Options

Select the **Tables and views** object, the **All existing statistics** option, and the **Full scan** option.