

HP Assessment Management Platform

for the Windows[®] operating system

Software Version: 8.10

Implementation Guide

Document Release Date: May 2010

Software Release Date: May 2010



Legal Notices

Warranty

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.

The information contained herein is subject to change without notice.

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.

Copyright Notice

Copyright 2010 Hewlett-Packard Development Company, L.P.

Trademark Acknowledgements

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

Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

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 AMP, contact customer support.

You can open a support case for Application Security Center products either online or by telephone.

Online (preferred)

- 1 Browse to URL <http://support.openview.hp.com/>.
- 2 Log in. If you have not registered before, you will need to do so and provide your Service Agreement ID (SAID) number. If you do not have an SAID number, there is an option on the page to declare yourself a "trusted customer" and enter a case.
- 3 Select your HP product and report the issue.

Telephone (voice recognition system)

- 1 Call 1-800-633-3600.
- 2 Say "Software."
- 3 Say "WebInspect" or "Assessment Management Platform" or "QAInspect" or "DevInspect."
- 4 Say or type your SAID.

You can access the HP Application Security Center customer forum and blogs at

<http://www.communities.hp.com/securitysoftware/>

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 find more information about access levels and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

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

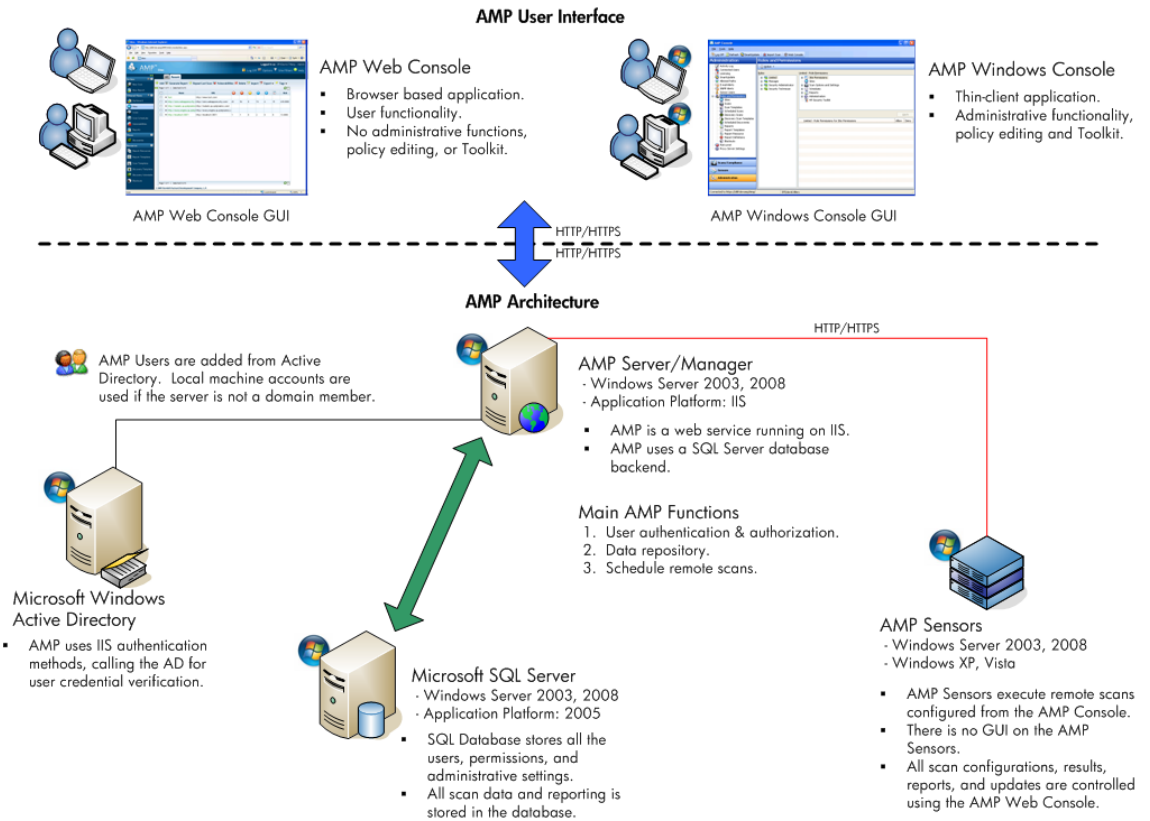
Contents

AMP Component Diagram	1
AMP Client Application Diagram	2
Hardware and Software Requirements	3
Database Size and Growth Settings	4
AMP Manager Account Requirements	5
SQL Database Account Requirements	5
AMP Manager License Components	5
AMP Manager Installation Troubleshooting	6
IIS Settings and File Permissions Used by AMP	6
SQL Login	6
Verify IIS Started/Running	7
Account Rights and Privileges	7
.NET Framework Registration	8
Restarting IIS Quick Commands	8
AMP Manager Logging Customization	8
AMP Manager Log Debug Settings	9
AMP Initialize Log Debug Settings	9
AMP Reporting Service Log Debug Settings	10
AMP Scheduler Service Log Debug Settings	10
AMP Task Service Log Debug Settings	11
AMP Quality Center Service Log Debug Settings	11
Failure to Install SSL Certificate on 64-Bit OS	12
AMP Manager Data Path Customization	14
Modifying the Web.config File (Moving the Storage Folders)	14
Modifying the Web.logging.config File (Moving Logging Locations)	15
Encrypting the Communication between AMP and SQL 2005	16
Enabling AMP to Use SSL	16
Editing the Encrypted SQL Connection String Section of web.config	16
Encrypt Connection String in the AmpReportingService.exe.config File after Modifying the web.config File	16
Encrypt Connection String in the AmpTaskService.exe.config File after Modifying the web.config File	17
AMP Sensor Installation	17
AMP Sensor Remote SQL Server Standard Edition Connectivity	18
AMP Sensor Logging	20
AMP Sensor Scan Logs	20
AMP Sensor Directory Path Customization	20
Modifying the SharedSettings.config File	20
Retaining Copies of Scan Data on the AMP Sensor	21
General Database Settings for AMP (SQL Server 2005)	21

Database Maintenance for AMP (SQL Server 2005)	21
Check Database Integrity Task	22
Database Fragmentation Maintenance	23
Rebuild Index	23
Reorganize Index	24
Update Statistics Task	25

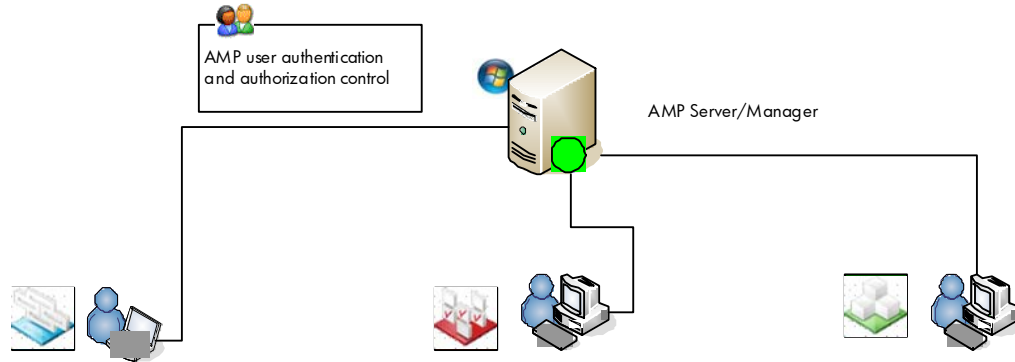
AMP Component Diagram

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



AMP Client Application Diagram

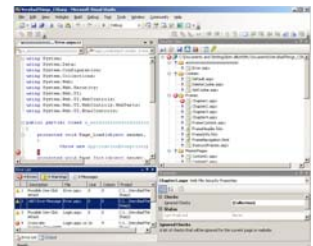
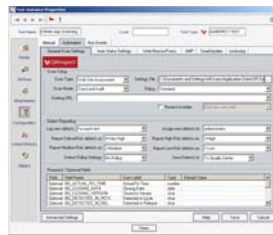
The following illustration depicts the Client connections to the AMP System. WebInspect, QAInspect, and DevInspect are all run on user machines with connectivity to AMP enabled via the chosen licensing model.



- Stand-alone application .
- Permissions controlled via AMP.
- Data is sent to AMP when scan is complete .
- Policies are pulled from AMP .
- Updates are pulled from AMP .
- Scans can be downloaded locally from AMP .
- Advanced Toolkit includes SQL Injector , Web Brute, Cookie Cruncher, Web Fuzzer

- Integrates with Quality Center client as the GUI .
- Data is sent to AMP and Quality Center
- Vulnerabilities are mapped as defects in Quality Center .
- Auto-status change for recursive scans .
- Permissions controlled via AMP .
- Policies & Updates are pulled from AMP .
- Standard Toolkit is included .

- Integrates with Visual Studio or Eclipse as an add-on to the IDE .
- Data is sent to AMP and defects can be logged into TFS .
- Combines static scan and dynamic scan capabilities .
- Provides code level fixes via Smart Objects .
- Permissions controlled via AMP .
- Policies & Updates are pulled from AMP .
- Standard Toolkit is included .



Hardware and Software Requirements

All AMP machines (excluding the database) require the following:

- Microsoft Internet Explorer 7.0 or later, or Mozilla FireFox 2.0 or later
- An active Internet connection

AMP Server (Manager)	Minimum Requirements	Recommended
Processor	2.5 GHz - Single	3.0+ GHz Multi-core
RAM	2 GB (remote database)	4 GB
Available Disk Space	5 GB (for remote database) 20 GB (for local database)	20 GB (local database)
OS and Software	Windows Server 2003 SP1 or Windows Server 2008 .NET 3.5 SP1 IIS 6.0	Windows Server 2003 SP2 or Windows Server 2008

The default locations for downloaded updates (including client binary updates) are under the All Users profile. Organizations using smaller boot partitions (below 20GB) can encounter problems from a lack of storage space for these updates, as well as the space required for scan uploads from the sensors. See [AMP Manager Data Path Customization](#) on page 16 for instructions to modify these default locations.

AMP Sensor	Minimum Requirements	Recommended
Processor	1.5 GHz - Single	3.0+ GHz Multi-core
RAM	2 GB	4 GB
Available Disk Space ¹	2 GB	20 GB
OS and Software	Windows XP Professional SP2/SP3 (32-bit), Windows Server 2003 Standard SP1/SP2 (32-bit), Windows Vista SP1 (32- or 64-bit) .NET 3.5 SQL Server 2005 Standard or Express Edition SP3 SQL Server 2008 Standard or Express Edition SP1 ²	Windows 2003 SP2 SQL Server Express Edition SP3 or SQL Server 2005 SP3
Screen Resolution ³	1024 x 768	1280 x 1024

¹ All scans run from the sensor are uploaded to AMP and removed from the sensor by default. A custom setting can be used to keep a local copy of scans on the sensors. See [Retaining Copies of Scan Data on the AMP Sensor](#) on page 23 for instructions to modify the default behavior. In the case where the customer is using WebInspect on the sensor, the disk space requirements are increased in order to download scans from AMP and also for WebInspect scan storage.

- ² The AMP Sensor requires either SQL Server Express Edition 2005/2008 or SQL Server Standard Edition 2005/2008 for temporary scan storage.
- ³ The screen resolution recommendations are provided for using WebInspect on the AMP Sensor. The AMP Sensor does not have an interactive GUI for scanning purposes.

AMP Console	Minimum Requirements
Processor	1.5 GHz - Single
RAM	1 GB
Available Disk Space	2 GB
OS and Software	Windows XP SP2 or Windows Server 2003 SP1 or Windows Server 2008 or Windows Vista .NET 3.5 Microsoft Silverlight (required only if you want to use the Scan Linkage Analyzer) Microsoft SQL Server 2005/2008 Express Edition (required only if you want to edit policies, compliance templates, or audit inputs)

AMP Database	Minimum Requirements	Recommended
Processor	2.0 GHz - Single	3.0+ GHz Multi-core
RAM	2 GB	4 GB
Available Disk Space*	20 GB	100 GB
OS and Software	Windows Server 2003/2008 SQL Server 2005/2008 Standard Edition	Windows 2003 SP2

* Disk space requirements will vary greatly for each organization. See [Database Size and Growth Settings](#) on page 4 for additional suggestions regarding the space requirements.

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.

AMP Manager Account Requirements

AMP uses Windows Active Directory for account management, including user credentials validation. Installations for workgroups use local accounts on the AMP server and AMP Database machines as a substitute for Active Directory accounts.

AMP requires two service accounts:

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

AMP users will need to be added to AMP in the Administration → Roles and Permissions section of the AMP Console after installation is complete. The user performing the installation is added to the AMP System Administrator role automatically. Also, rerunning AMP Initialize will add the person running the application to the AMP System Administrator's role. This is useful when moving the AMP Server to another computer.

SQL Database Account Requirements

If you are installing AMP 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).

AMP Initialize is used for the database creation and AMP Server configuration changes such as changing the user account used to access the database.

AMP Manager License Components

The AMP license contains the license information for each component of the AMP environment:

Sensors (Fixed) - The "AMP Sensor for WebInspect" Windows Service installed by the WebInspect installation that connects to AMP for the purpose of performing remotely scheduled or requested scans. It receives instructions exclusively from the configurable connection to an AMP Manager.

Users (Concurrent) - Users are any accounts connected to AMP using the AMP Console, the AMP Web Console, or any HP ASC scanner (WebInspect, QAInspect, or DevInspect). When configured, HP ASC Scanners connect to AMP to receive license, permissions, updates, and scan data. They present a user interface through which scans may be conducted. AMP controls permissions for the application and also provides the policies and compliance templates. HP ASC scanners can be configured to upload scan results to AMP automatically at the completion of the scan or only when specifically instructed by the user.

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

AMP Manager Installation Troubleshooting

The most common errors encountered when installing AMP are shown as either a connection message error at the final phase of the AMP 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 AMP Initialize or AMP 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 AMP

** File Root Path = C:\Program Files\HP\HP AMP 8.0 Server\AmpManagerWS\

** IIS Virtual Directory \AMP\

Folder	IIS Authentication	Notes	File Permissions
\	Integrated		User is Network Service with 'read' access. AMP Service User must be a local administrator with 'read' access.
\App_GlobalResources	Integrated		
\App_Themes	Integrated		
\bin	Integrated		
\Dashboard	Integrated		
\Login	Anonymous	Getting a 401 status on this page means Anonymous auth has been disabled	
\Reports	Integrated		
\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 doesn't work, you must set up a SQL login. Then a SQL database user in the AMP database must be assigned to the role "amp_server" and associated with that login. AMP Initialize can then be run to specify the SQL login for connecting to the database.

Verify IIS Started/Running

If you cannot connect to AMP using the console after installation, first verify that the AMP web service is started by accessing the main service of AMP via the URL in a browser. The default location of the service is:

```
http(s)://<hostname>/AMP/managerservice.asmx
```

If an error page is returned, the AMP web service is not running due to an IIS configuration or permissions issue. Refer to the following sections for help in resolving these issues.

If this page is returned, then the AMP web service is running and you should consult the AMP Manager Logs for any errors. See [AMP Manager Logging Customization](#) on page 8 for log locations and instructions.

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 AMP Manager User is a member of the local administrators group.

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

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

- 1 Right-click My Computer → Manage → Services and Applications → Internet Information Services (IIS) Manager → Application Pools → AmpAppPool → Identity.
- 2 Change the user from “Network Service” to “Local System” in the drop-down menu.

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 (Network Service by default) to enable appropriate permissions.

The application pool user (web service user) should have Read, Write, Read and Execute, 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\AMP 8.0 Server\
```

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 permitted in IIS

- 1 Right-click My Computer → Manage → Services and Applications → Internet Information Services (IIS) Manager → Web Service Extensions
- 2 Make sure the .NET 2.x extensions are marked as permitted.

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 2.0 framework:

```
\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe
```

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

The -i option will install this version of ASP.NET and update 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

AMP Manager Logging Customization

Use the AMP logs to troubleshoot any errors that occur during the initialization process or when trying to use AMP 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 AMP installations are:

- AMP Initialize Log(s)
- AMP Manager Log(s)
- AMP Reporting Service Log(s)
- AMP Scheduler Service Log(s)
- AMP Task Service Log(s)
- AMP Quality Center 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.

AMP Manager Log Debug Settings

Increasing the logging level for the AMP Manager.

- 1 Edit the Web.logging.config file in the following directory:
 \Program Files\HP\AMP 8.0 Server\AmpManagerWS\
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 AmpManagerWS_trace.log in the following directory:

On Windows Server 2003

 \Documents and Settings\All Users\Application Data\HP\AMP\8.0\Manager\
On Windows Server 2008

 \ProgramData\HP\AMP\8.0\Manager\
If additional files are created, they will be named AmpManagerWS_trace.log.1,
AmpManagerWS_trace.log.2, etc.

AMP Initialize Log Debug Settings

Increase the logging level for AMP Initialize

- 1 Edit the AmpInitialize.exe.logging.config file in the following directory:
 \Program Files\HP\AMP 8.0 Server\AmpInitialize\
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 AmpInitialize_trace.log in the following directory:

 \Program Files\HP\AMP 8.0 Server\AmpInitialize\

AMP Reporting Service Log Debug Settings

To increase the logging level for the AMP Reporting Service:

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

\Program Files\HP\HP AMP 8.0 Server\AmpReportingService

- 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 AmpReportingService_trace.log in the following directory:

On Windows Server 2003

\Documents and Settings\All Users\Application
Data\HP\AMP\8.0\AmpReportingService

On Windows Server 2008

\ProgramData\HP\AMP\8.0\AmpReportingService

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

AMP Scheduler Service Log Debug Settings

To increase the logging level for the AMP Scheduler Service:

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

\Program Files\HP\HP AMP 8.0 Server\AmpScheduler

- 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 AmpScheduler_trace.log in the following directory:

On Windows Server 2003

\Documents and Settings\All Users\Application Data\HP\AMP\8.0\Scheduler

On Windows Server 2008

\ProgramData\HP\AMP\8.0\Scheduler

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

AMP Task Service Log Debug Settings

To increase the logging level for the AMP Task Service:

- 1 Edit the AmpTaskService.exe.logging.config file in the following directory:
 \Program Files\HP\HP AMP 8.0 Server\AmpTaskService
- 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 AmpTaskService_trace.log in the following directory:

On Windows Server 2003

 \Documents and Settings\All Users\Application Data\HP\AMP\8.0\TaskService

On Windows Server 2008

 \ProgramData\HP\AMP\8.0\TaskService

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

AMP Quality Center Service Log Debug Settings

This section is applicable only if the Quality Center Service has been installed separately.

To increase the logging level for the Quality Center Service:

- 1 Edit the Amp.Services.QC.Service.exe.logging.config file in the following directory:
 \Program Files\Common Files\HP AMP Quality Center 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 AmpQCService_trace.log in the following directory:

On Windows Server 2003

 \Documents and Settings\All Users\Application
 Data\HP\AMP\8.0\QualityCenterService

On Windows Server 2008

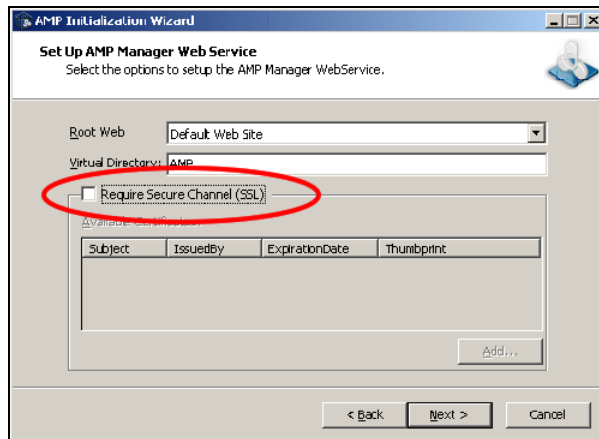
 \ProgramData\HP\AMP\8.0\QualityCenterService

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

Failure to Install SSL Certificate on 64-Bit OS

When initializing the AMP Manager (Server) under a 64-bit operating system, the AMP Initialize program may display an error message indicating that it “could not add SSL.” Although the program generated a certificate and placed it in the store, the program did not attach the certificate to IIS.

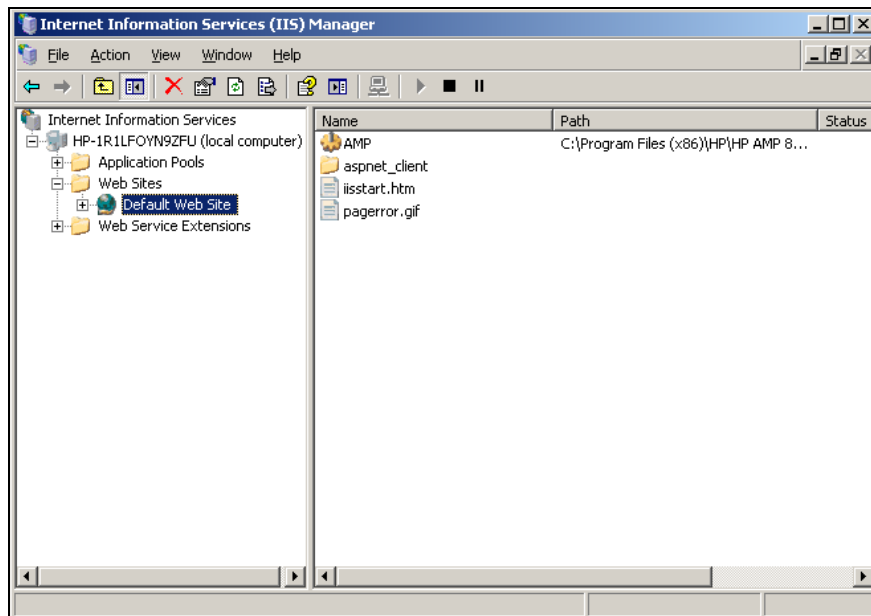
You must restart the AMP Initialize program and proceed as usual until the program displays the *Set Up AMP Manager Web Service* dialog. At this point, make sure the **Require Secure Channel (SSL)** option is not selected and then continue.



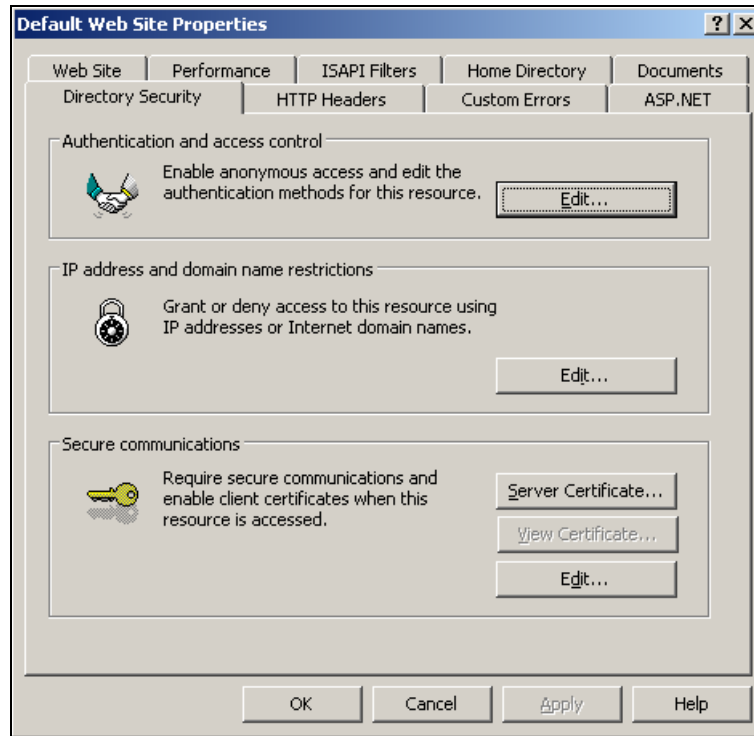
After the AMP Initialize program completes successfully, use the following procedure to attach the certificate.

Windows Server 2003

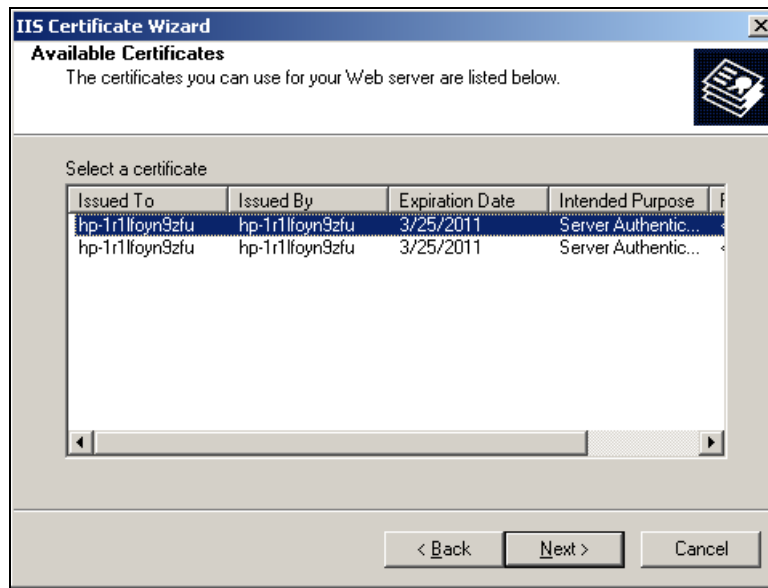
- 1 Navigate to Administrative Tools and run the IIS Manager.
- 2 Expand the computer node and the Web Sites folder. You should see a Default Web Site item, as depicted in the following illustration.



- 3 Right-click **Default Web Site** and select **Properties**.
- 4 On the *Default Web Site Properties* dialog, select the **Directory Security** tab and click **Server Certificate**.

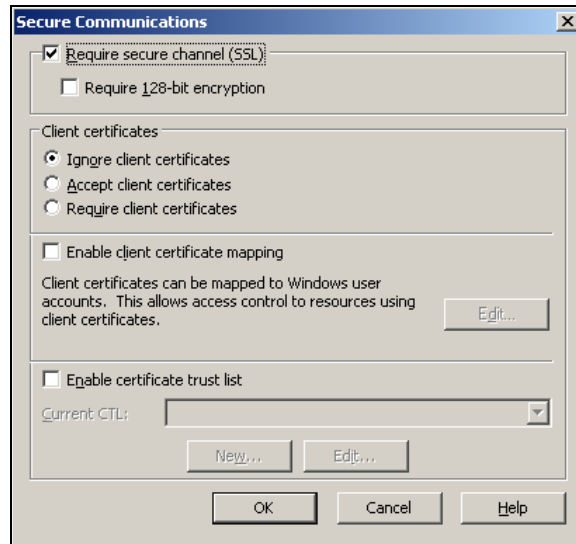


- 5 On the first page of the Certificate Wizard, click **Next**.
- 6 Select **Assign an existing certificate** and click **Next**.
- 7 You should see the certificate that was generated during the AMP Initialize that you did not use in the certificate list.



- 8 Select the certificate and click **Next**.

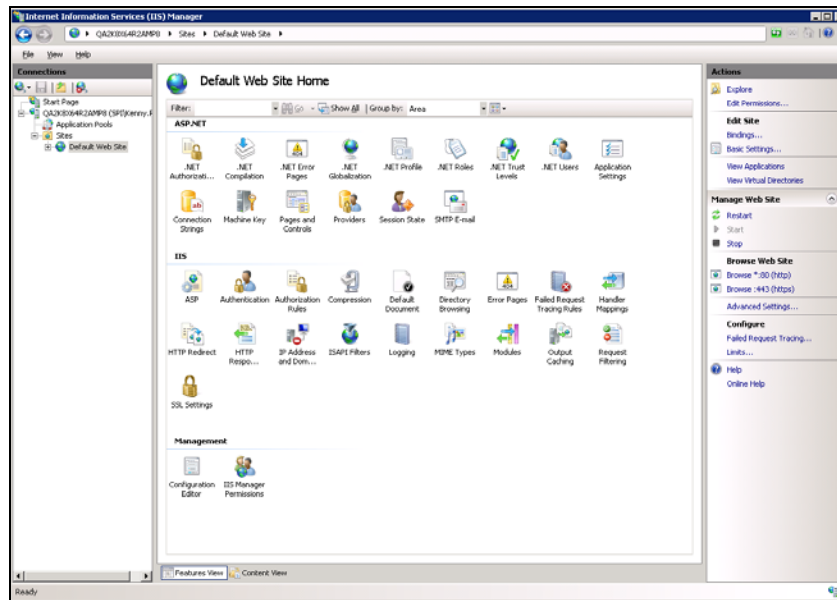
- 9 Click **Next** without changing the SSL port.
- 10 Click **Next**. Click the Finish button.
- 11 On the Summary page of the Wizard, click **Next**. This should return you to the *Default Web Site Properties* dialog.
- 12 In the **Secure Communications** group, click **Edit**.
- 13 Select **Require Secure Channel (SSL)** and click **OK**.



- 14 Click **OK** to close the *Default Web Server Properties* dialog and finalize your changes.

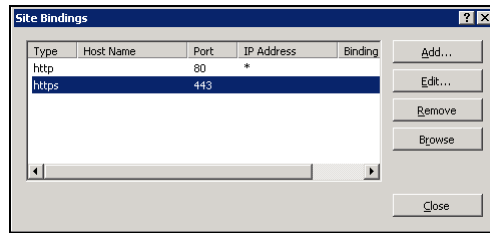
Windows Server 2008

- 1 Navigate to Administrative Tools and run the IIS Manager.
- 2 Expand the computer node and the Web Sites folder. You should see a Default Web Site item, as depicted in the following illustration.

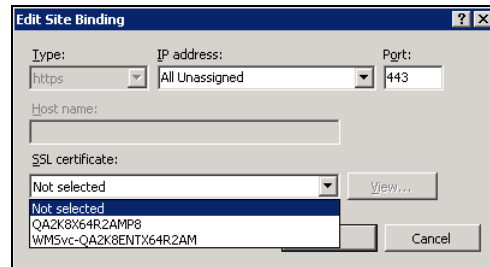


- 3 In the Actions panel on the right side, under Edit Site, click **Bindings**.

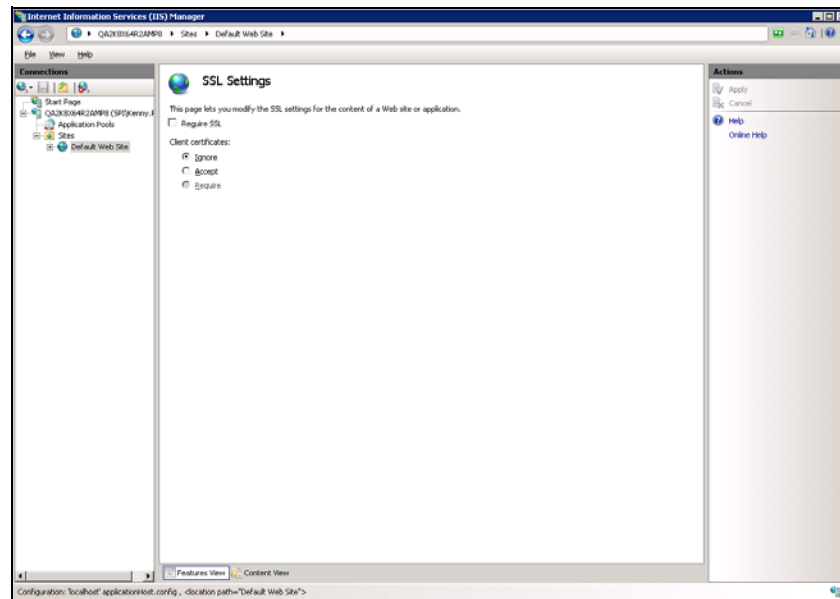
- 4 If the *Site Bindings* dialog contains an entry for https, select it and click **Edit**. Otherwise, click **Add** and select https from the **Type** list.



- 5 You should see the certificate that was generated by the AMP Initialize program in the **SSL Certificate** list.



- 6 Select the certificate and click **OK**.
- 7 Close the *Site Bindings* dialog.
- 8 On the IIS Manager window, double-click the SSL Settings icon (under the IIS group).
- 9 On the Features view, select **Require SSL** and click **Apply** (in the Action panel).



AMP Manager Data Path Customization

By default, the AMP Manager uses the All Users profile path as the SmartUpdate download, sensor upload, and AMP 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 AMP is located in the following directory:

```
\Program Files\HP\AMP 8.0 Server\AmpManagerWS\
```

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

```
<add key="Manager.TempPath" value="D:\AmpData\temp" />
<add key="Manager.BaseDataPath" value="D:\AmpData" />
```

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

```
<add key="Manager.ScanUploadsPath" value="D:\AmpData\ScanUploads" />
<add key="Manager.ScanImportPath" value="D:\AmpData\ScanImports" />
<add key="Manager.SensorUploadsPath" value="D:\AmpData\SensorUploads" />
<add key="SmartUpdate.ProductsFilePath" value="D:\AmpData\SmartUpdatePatches" />
<add key="Manager.PimCachePath" value="D:\AmpData\PimCache" />
```

If you don't 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\AMP\8.0\Manager\AmpManagerWS_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 something like this:

```
<appender name="RollingFile"
type="SPI.Diagnostics.Logging.Appender.RollingFileAppender">
  <file value="D:\AmpData\logs\AmpManagerWS_trace.log"/>
  ...
</appender>
```

This same change can be made to the AMP Reporting Service, AMP Scheduler Service, AMP Task Service, and AMP Quality Center Service logging configuration files.

- For the AMP Reporting Service, edit the AmpReportingService.exe.logging.config file in the following directory: \Program Files\HP\HP AMP 8.0 Server\AmpReportingService.
- For the AMP Scheduler Service, edit the AmpScheduler.exe.logging.config file in the following directory: \Program Files\HP\HP AMP 8.0 Server\AmpScheduler.
- For the AMP Task Service, edit the AmpTaskService.exe.logging.config file in the following directory: \Program Files\HP\HP AMP 8.0 Server\AmpTaskService.
- For the AMP Quality Center Service, edit the Amp.Services.QC.Service.exe.logging.config file in the following directory: \Program Files\Common Files\HP AMP Quality Center Service.

Encrypting the Communication between AMP and SQL 2005

Some customers may require the communication between the AMP 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 AMP web service to use the enabled SSL encryption after the Windows configuration is complete.

The steps below detail how to configure AMP to use SSL encryption AFTER configuring a certificate on the SQL Server machine AND configuring the AMP Server (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 AMP to Use SSL

The instructions below detail how to modify the web.config file of AMP 8.1 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 AMP Server to use the encryption, you additionally need to modify the web.config file for the AMP web service to utilize the encryption. The connection string is encrypted by default, which requires the steps below to decrypt the sting, perform the necessary modifications, and then re-encrypt the string in the web.config file. Also, if you rerun AMP 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 AMP 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 AmpReportingService.exe.config File after Modifying the web.config File

- 1 Stop the AMP Reporting Service. At a command line, enter “net stop Amp8ReportingService.”
- 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 AmpReportingService.exe.config file.

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

- 3 Restart the AMP Reporting Service. At a command line, enter “net start Amp8ReportingService.”

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

- 1 Stop the AMP Task Service. At a command line, enter “net stop AmpTaskService.”
- 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 AMP Task Service. At a command line, enter “net start AmpTaskService.”

AMP Sensor Installation

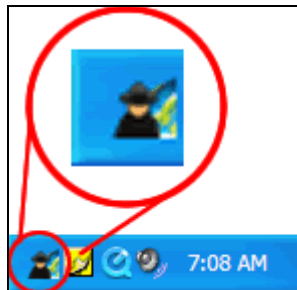
The user installing the AMP Sensor must be a local administrator on the Sensor machine. The installation package for the AMP Sensor is contained within the WebInspect installation. An AMP Sensor is a subset of the WebInspect package that does not require a WebInspect license for activation. All the license information for AMP Sensors is contained in the AMP License.

During the installation of WebInspect, there is a screen that will allow you configure the package as an AMP Sensor. The best practice is to bypass setting up the Sensor at this screen and perform the Sensor configuration via the HP ASC Monitor after the installation wizard is complete. There are two reasons for this:

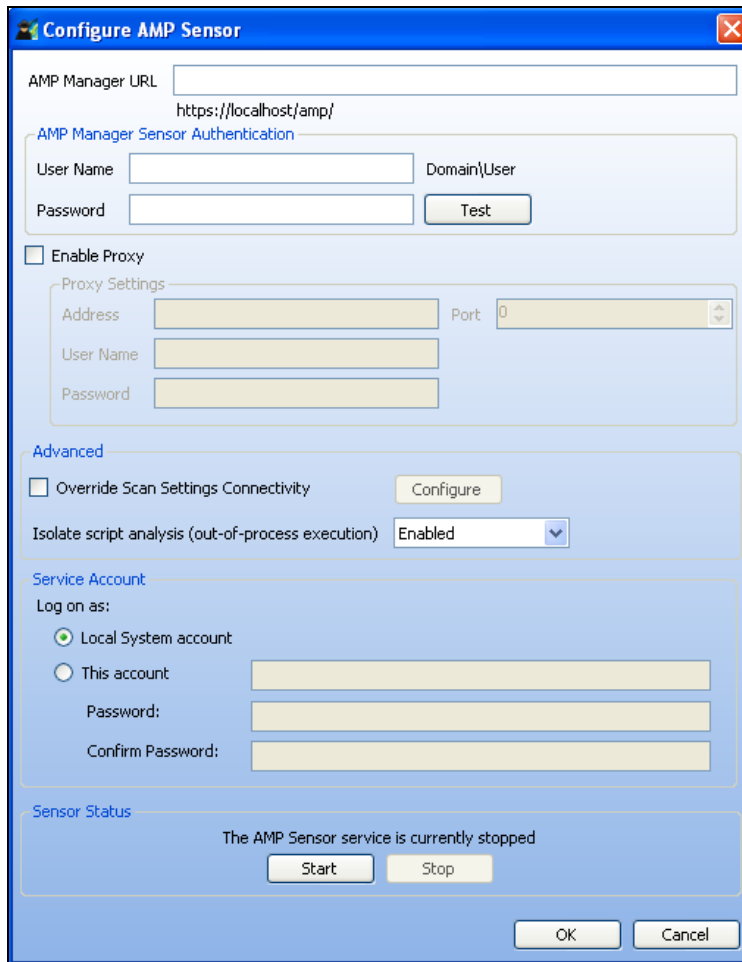
- The ASC Monitor Sensor configuration allows the user to test the Sensor username/ password credentials prior to starting the service.
- The ASC Monitor Sensor configuration allows the user to specify Sensor connectivity to a remote SQL Server.

Configuration of the AMP Sensor is performed via the HP ASC Monitor program. This should be launched automatically and resides in the task tray. You can manually launch it via the Start menu for HP WebInspect.

Right-click the HP Application Security Center icon in the task tray and select **Configure AMP Sensor**.



As shown below, the *Configure AMP Sensor* window includes the ability to test the Sensor authentication credentials and configure a remote SQL Server (**Override Scan Settings Connectivity** option).



AMP Sensor Remote SQL Server Standard Edition Connectivity

When configuring the AMP 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 via 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 AMP 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. To do so, use the following procedure.

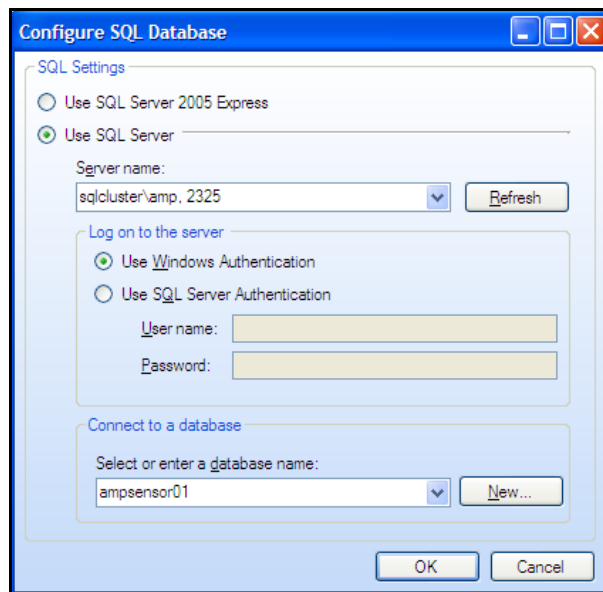
- 1 Right-click the HP Application Security Center icon in the task tray and select **Configure AMP Sensor**.

- 2 On the *Configure AMP Sensor* window, under Service Account - Log on as, select **This account**. See illustration on page 18.
- 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**.

In the example below, the information for the remote SQL database is as follows:

- SQL Server name: sqlcluster
- SQL Instance name: amp
- SQL Server listening port: 2325
- AMP Sensor database: ampsensor01

The ampsensor01 database has been previously created using the New button shown in the illustration. 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.



AMP Sensor Logging

The AMP Sensor log is in the following locations:

On Windows XP and Windows Server 2003

```
\Documents and Settings\All Users\Application Data\SPI  
Dynamics\WebInspect\7.0\Amp\logs
```

On Windows Server 2008 and Vista

```
\ProgramData\SPI Dynamics\WebInspect\7.0\Amp\logs\
```

The file is named AMPSensorWI_trace.log. The name can be changed in AmpSensorWI.exe.logging.config.

AMP Sensor Scan Logs

Information regarding the scans performed by the AMP sensor can be found in the same directory as above, with the scan GUID as the folder name for each particular scan.

AMP Sensor Directory Path Customization

By default, the AMP 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 AMP data path. This will modify all of the paths for the AMP 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 AMP 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\SPI Dynamics\WebInspect\7.0
```


On Windows Server 2008 and Vista:

```
\ProgramData\SPI Dynamics\WebInspect\7.0
```
- 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 AMP Sensor Service.

Retaining Copies of Scan Data on the AMP Sensor

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

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

C:\Program Files\SPI Dynamics\WebInspect 7.0

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: Scans with a status of "failed."]
```

```
</appSettings>
```

- 2 Save the file and restart the AMP Sensor Service.

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

General Database Settings for AMP (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 AMP 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 AMP (SQL Server 2005)

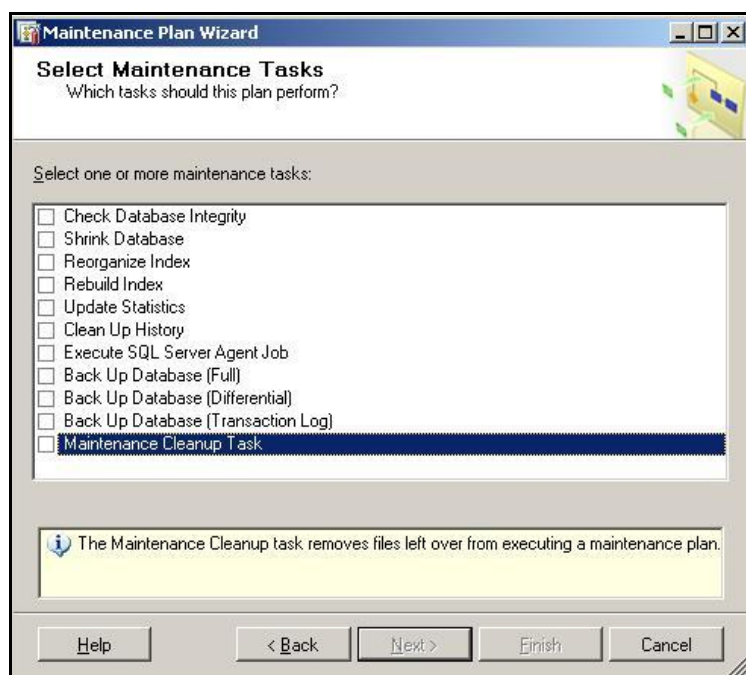
The descriptions included in this document cover only the most important maintenance tasks associated with database performance issues and are intended for customers that do not have a DBA on staff.

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

In SQL Server 2005, the Maintenance Wizard guides you through a series of steps that request several bits of information for a complete plan that are saved as a 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 AMP database is listed following the general description of each 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 the SQL Management Studio under **Management** → **Maintenance**. 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 AMP database).



AMP 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: Repairing errors can be done 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 AMP application offline.

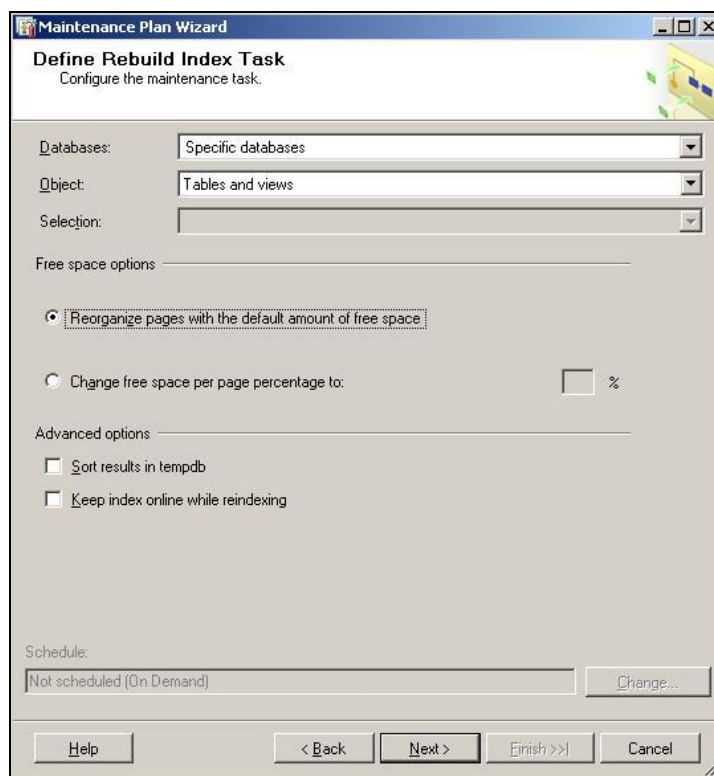
Database Fragmentation Maintenance

The following options can all be encompassed under the fragmentation subject (Rebuild Indexes, Reorganize Indexes, Update Statistics).

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.

Rebuild Index

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.

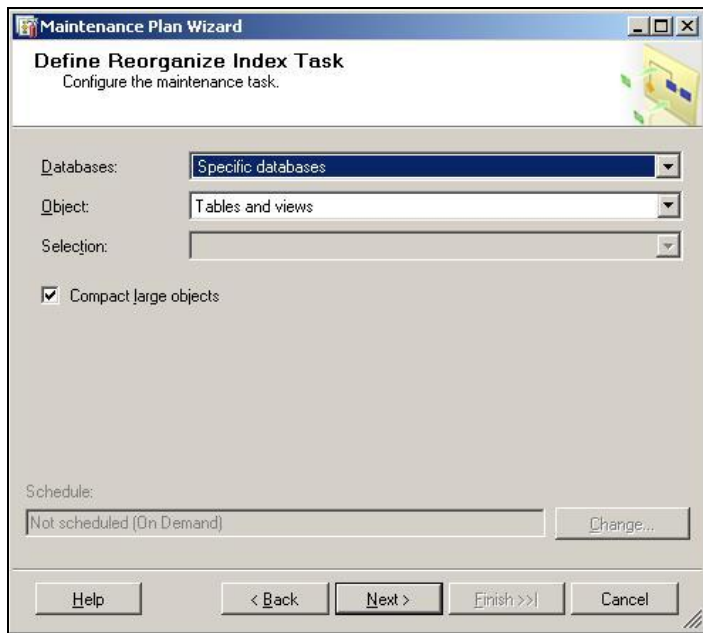


AMP Recommended Options

Select All Tables and Views and Reorganize pages with the default amount of free space.

Reorganize Index

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

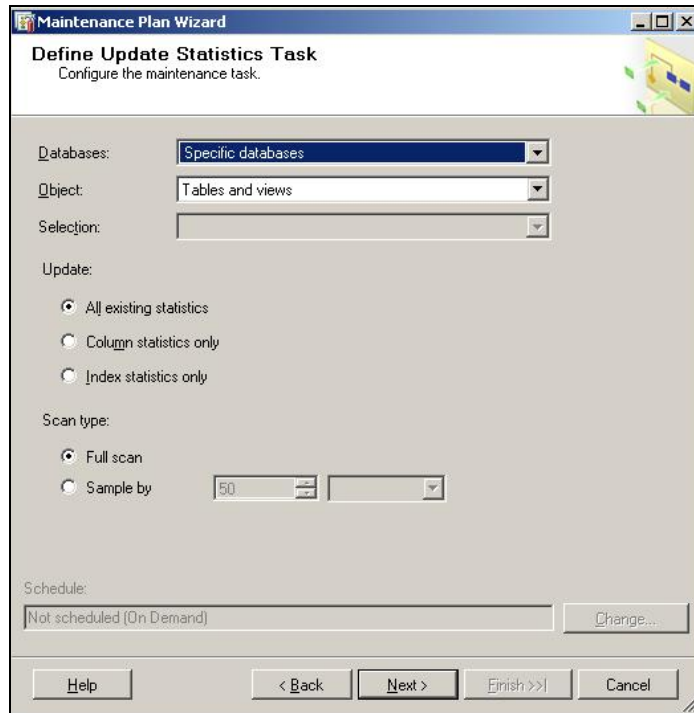


AMP Recommended Options

Select All Tables and Views and Compact Large Objects.

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.



AMP Recommended Options

Select All Tables and Views, All Existing Statistics, and Full Scan.

