Advanced Web Diagnostics Server

Installation Guide

Release 11.1

Please direct questions about Advanced Web Diagnostics Server or comments on this document to:

Technology Customer Support
Compuware Corporation
Customer Support Hotline
1-800-538-7822
FrontLine Support Web Site:
http://frontline.compuware.com

For telephone numbers in other geographies, see the list of worldwide offices at http://www.compuware.com.

Access is limited to authorized users. Use of this product is subject to the terms and conditions of the user's License Agreement with Compuware Corporation. Documentation may be reproduced by Licensee for internal use only. All copies are subject to the terms of this License Agreement. Licensee agrees to provide technical or procedural methods to prevent use of the Software and its documentation by anyone other than Licensee.

Copyright © 2009 Compuware Corporation. All rights reserved. Unpublished rights reserved under the Copyright Laws of the United States.

U.S. GOVERNMENT RIGHTS—Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in Compuware Corporation license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable. Compuware Corporation.

This product contains confidential information and trade secrets of Compuware Corporation. Use, disclosure, or reproduction is prohibited without the prior express written permission of Compuware Corporation. Access is limited to authorized users. Use of this product is subject to the terms and conditions of the user's License Agreement with Compuware Corporation.

Adobe® Reader® is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.

All other company and product names are trademarks or registered trademarks of their respective owners.

Build: October 16, 2009, 1:52

Contents

Introduction

Who Should Read This Guide

This guide is intended to be used by network engineers and system administrators installing the Advanced Web Diagnostics Server.

Organization of the Guide

The Installation Guide of Advanced Web Diagnostics Server is organized as follows:

- Advanced Web Diagnostics Server Overview [p. 11] – Describes the Advanced Web Diagnostics Server release and lists the supported protocols.
- Installation Checklist [p. 17] – Specifies how to install, license, and configure Advanced Web Diagnostics Server, with references to details in other sections of this document as required.
- System Requirements [p. 19] – Describes the minimum hardware and software requirements for Advanced Web Diagnostics Server.
- Installing Advanced Web Diagnostics Server [p. 25] – Describes how to install the Advanced Web Diagnostics Server.
- Upgrading Advanced Web Diagnostics Server [p. 33] – Describes how to upgrade the Advanced Web Diagnostics Server.
- AWDS Basic Configuration Settings [p. 41] – Describes how to configure the Advanced Web Diagnostics Server.
- Licensing ClientVantage Agentless Monitoring Products [p. 45] – Describes product licensing.
- Protocols Supported by AWDS [p. 51] – Lists protocols supported by AWDS.

Product Documentation Library

The following publications offer information on using and configuring Advanced Web Diagnostics Server.

ClientVantage Agentless Monitoring Release Notes
Summarizes new product features, known issues, and limitations, and lists last-minute information not included in other publications related to the product.

Distributed License Management – License Installation Guide
Describes how to install and administer Compuware product licensing components.

ClientVantage Agentless Monitoring Getting Started Guide
Introduces product components, release information, system requirements, licensing information, and performance estimates.

Advanced Web Diagnostics Server Installation Guide
Describes how to install the report server.

Vantage Agentless Monitoring Device Installation and Configuration Guide
Describes how to install the Agentless Monitoring Device, which collects data for the Vantage Analysis Server and Advanced Web Diagnostics Server.

ClientVantage Agentless Monitoring System Administration Guide
Describes how to configure and administer ClientVantage Agentless Monitoring.

Advanced Web Diagnostics Server on-line help
Provides on-line procedures and information to help you use the product.

Advanced Web Diagnostics Server User Guide
Guides you through the features of the report server. It describes each top-level report and many lower-level reports, shows you how to interpret the reports, how to identify problems and how to optimize your network and site operation.

ClientVantage Agentless Monitoring Web Services – Getting Started Guide for Developers
Provides data structure definitions and usage examples for CVAM Web service developers.

PDF files can be viewed with Adobe® Reader, version 7 or later. If you do not have the Reader application installed, you can download the setup file from the Adobe Web site at *http://www.adobe.com/downloads/*.

Customer Support and Online Information

Corporate Web site

To access Compuware's site on the Web, go to *http://www.compuware.com*. The Compuware site provides a variety of product and support information.

FrontLine support Web site

You can access online customer support for Compuware products via our FrontLine support site at *http://frontline.compuware.com*. FrontLine provides fast access to critical information about your Compuware products. You can read or download documentation, frequently asked

questions, and product fixes, or e-mail your questions or comments. The first time you access FrontLine, you are required to register and obtain a password. Registration is free.

Customer Support

You can contact Compuware Customer Support as follows:

- Web: via the “FrontLine Incident Reporting Form”.
- By phone: Compuware Customer Support.
  - USA and Canada customers: 1-800-538-7822 or 1-313-227-5444.
  - All other countries: please contact your local Compuware office.

All high-priority issues should be reported by phone.

Getting Help

When calling, please provide Customer Support with as much information as possible about your environment and the circumstances that led to the difficulty. You should be ready to provide:

- Client number: this number is assigned to you by Compuware and is recorded on your sales contract.
- The version number of the Agentless Monitoring Device (AMD) and the report servers.

  For the report server

  Use the report server GUI by selecting **Help → Product Information → About**, or **Tools → Diagnostics → System Status**.

  For the AMD

  Scroll down to the **Testing AMD** section. At the bottom of the diagnostic data paragraph, look for “`Version ND-RTM v.ndw.x.yy.zz`”.

- Environment information, such as the operating system and release (including service pack level) on which the product (AMD, report server) is installed, memory, hardware/network specifications, and the names and releases of other applications that were running.

  Problem description, including screenshots.
- Exact error messages, if any (screenshots recommended).
- Whether or not the problem is reproducible. If yes, include a sequence of steps for problem recreation. If not, include a description of the actions taken before the problem occurred.
- A description of the actions that may have been taken to recover from the difficulty and their results.
- Debug information as follows:

  Information from the report server

  - Log files from `http://report_server_IP/root/log/` and `watchdog.log` from the `C:\Program Files\Common Files\Compuware\Watchdog` directory.
  - Configuration file: `http://report_server_IP/ExportConfig`

- Screenshots of the problem.

Information from the AMD

Log files from `/var/log/adlex/`: `rtm.log`, `rtm.log.1`, `rtm_perf.log`, `rtm_perf.log.1`.

Information from the VCAEUE Server

- Log files from `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\log` directory.
- All files from `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\platform3.0\InstallLogs`
- All `*.log` files from `..\Documents and Settings\All Users\Application Data\Compuware\<Service Name>\workspace\log\kernel` where *<Service Name>* is Microsoft Windows Service Name associated with VCAEUE Server. By default it is `Agentless Platform 1`
- Version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\`
- Version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\eclipse`

Information from the VCAEUE Console

The installation log file:

`Vantage_Configuration_for_Agentless_End-User_Experience_11.1_InstallLog.log`

location:

`..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE`

log files located in the following directory of your VCAEUE Console installation:

`..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\eclipse\log`

and version file (`version.xml`) located in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\` and in `..\Program Files\Compuware\Vantage_Configuration_For_Agentless_EUE\cva\eclipse`.

NOTE

Please compress all the files before sending them to Customer Support.

Compuware values your comments and suggestions about the Vantage products and documentation. Your feedback is very important to us. If you have questions or suggestions for improvement, please let us know.

Conventions

The following font conventions are used throughout documentation:

This font	Indicates
Bold	Terms, commands, and references to names of screen controls and user interface elements.
Conventions [p. 9]	Links to Internet resources and linked references to titles in Compuware documentation.
`Fixed width`	Cited contents of text files, examples of code, command line inputs or system outputs. Also file and path names.
`Fixed width bold`	User input in console commands.
`Fixed width italic`	Place holders for values of strings, for example as in the command: **`cd`** *`directory_name`*
Menu → Item	Menu items.

CHAPTER 1

Advanced Web Diagnostics Server Overview

Advanced Web Diagnostics Server (AWDS) performs detailed HTTP analysis and delivers definite answers to customer problems, regarding Web site performance and errors. Faulty components can be quickly identified. Diagnosis can be extended behind the Web server, down to the particular Web application server.

AWDS is capable of transaction monitoring and can provide reports on the aggregation level, reflecting business processes instrumented by Web site applications. Performance, usage, and errors for each Web site user are mapped onto the business processes executed through Web site interaction.

AWDS can provide you with:

- Detailed HTTP analysis of every Web site user, including every single HTTP hit and page requested by the user, and recognition of individual Web forms.
- Transaction (predefined sequences of Web pages) monitoring with ready-to-use reports and drill-down capabilities.
- Problem-solving reports for Web sites that find systemic problems caused by HTTP-based application performance degradation.

AWDS Product Release Information

Table 1. Component module versions based on preceding and current release report server

Module name	Module version number in report server version		
	10.3.0	**11.0.1**	**11.1.0**
Advanced Web Diagnostics Server	10.3.0	11.0.1	11.1.0
DMI	10.3.0	11.0.1	11.1.0
RTM Base System	10.3.0	11.0.1	11.1.0

Module name	Module version number in report server version		
	10.3.0	11.0.1	11.1.0
RTM GATE	10.3.0	11.0.1	11.1.0
ND Core Base System	10.3.0	11.0.1	11.1.0

Supported Browsers and Connectivity

ClientVantage Agentless Monitoring users can access report servers through browsers with support for cookies, Java VM, JavaScript, and CSS 2. Before you start using the report server, it may be necessary to adjust JavaScript and HTTP 1.1 settings in your browser.

Compuware recommends the following browsers:

- Microsoft Internet Explorer version 6.0 or later with JavaScript and HTTP 1.1 settings enabled.

  Note that due to a different handling of the data within the HTML, Microsoft Internet Explorer may experience degradation in performance while viewing reports containing a large number of columns or reports containing a large number of tooltips.
- Mozilla Firefox version 1.5.0 or later, with JavaScript, cookie support, and HTTP 1.1 enabled.
- Other browsers with support for cookies, Java VM, JavaScript and CSS 2 may also be used, but they are not recommended.

NOTE

- Some configuration screens require a Web browser with Java™ plug-in version 1.5.0.9 or higher.
- In Java plug-in version 1.5, TLS is turned off by default. This may cause some applets not to work in your Web browser. You must turn on TLS in the Java 1.5 Control Panel to have full access to all report server features. For more information, see How to enable TLS 1.0 for Java 1.5 plug-in [p. 13].
- Without JavaScript enabled, the top menu of the report server will not be visible and you will see the following message instead: `“This product uses JavaScript. Please make sure JavaScript is enabled in your browser settings.”`

The Advanced Web Diagnostics Server and Vantage Analysis Server can be accessed using HTTP or, over secured connections, using HTTPS. We recommend secure access with a browser that supports TLS v.1. Using older versions of the protocol, such as SSL ver. 2 or SSL ver. 3, is not recommended but can be configured. For more information, see Configuring the Report Server to Communicate over HTTPS [p. 31].

How to enable JavaScript and support for HTTP 1.1 in your browser

Internet Explorer

To enable JavaScript:

1. Select **Tools** → **Internet Options** from the top menu in your browser and click the **Security** tab.
2. Choose the **Custom level...** button and enable **Active scripting** on the list of options.

To enable the HTTP 1.1:

1. Navigate to **Tools** → **Internet Options** and click the **Advanced** tab.
2. Scroll within the **Settings** list to the section titled **HTTP 1.1 settings** and make sure that the **Use HTTP 1.1** check box is selected.
3. Click **OK** and restart your browser.

Mozilla Firefox

To enable JavaScript:

1. Select **Tools** → **Options...** from the top menu in your browser and click the **Content** tab.
2. Select the **Enable JavaScript** check box.

To enable HTTP 1.1:

1. Open the browser and, in the address bar, type **`about:config`** and press `[Enter]`.

   The browser will display a list of current preferences.
2. Scroll to the **network.http.version** preference and make sure its value is `1.1`. If the value is other than `1.1` it can be changed by double clicking on the parameter name.

How to enable TLS 1.0 for Java 1.5 plug-in

TLS for Java plug-ins is turned on in **Java Control Panel**, in the **Security** settings of the **Advanced** tab.

1. Access **Java Control Panel** in one of the following ways:
   - Windows control panel:

     In Windows, click **Start** → **Settings** → **Control Panel** and select **Java** to open **Java Control Panel**. Note that **Java Control Panel** opens for the default Java installation whose number may be different than the plug-in's that you are trying to modify.
   - Java installation directory:

     Navigate to the `bin` directory where the Java version you intend to modify is installed (for example `C:\Program Files\Java\jre1.5.0_11\bin`). Click the file `javacpl.exe` to activate the configuration tool.
   - Java platform icon in system tray:

     Right-click the icon and choose **Open Control Panel** from the menu.
2. In **Java Control Panel**, click the **Advanced** tab and expand the **Security** tree.

3. Select the **Use TLS 1.0** check box.
4. Click **OK**.

Internationalization Support

Advanced Web Diagnostics Server supports international environments on both ends: report server and client browser.

Localized server support

The user interface of the report server is rendered in the following languages:

- English
- Japanese
- Korean
- Chinese simplified
- Chinese traditional.

For English, which is the default language setting, there is no need for additional configuration of the operating system or browser. To enable support for other languages, install the required font set for the target language and customize the regional options accordingly. For more information, see *Localizing the Report Server* in the *Advanced Web Diagnostics Server – User Guide*.

Character encoding support for monitored traffic

Advanced Web Diagnostics Server recognizes the following character encodings in monitored HTTP and XML traffic:

European:

- ISO-8859-1
- ISO-8859-2
- Unicode (UTF-8)

Japanese:

- Unicode (UTF-8)
- Shift_JIS
- EUC-JP

Korean:

- Unicode (UTF-8)
- EUC-KR
- ISO-2022-KR

Chinese:

- Unicode (UTF-8)

- GB18030
- Big5
- Big5-HKSCS
- EUC-TW
- ISO-2022-CN
- GB2312
- GBK
- HZ.

For more information, see *Character Encoding Support for Monitored Traffic* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

CHAPTER 2

Installation Checklist

Installation actions should be performed in this order. Follow the links for details on performing individual steps.

1. Verify hardware and software suitability.

   See System Requirements [p. 19] to make sure the hardware and software requirements are met.

2. Obtain a license for your Advanced Web Diagnostics Server installation.

   For more information, see Licensing ClientVantage Agentless Monitoring Products [p. 45].

3. Install Advanced Web Diagnostics Server.

   For new installation, see Installing Advanced Web Diagnostics Server [p. 25], for upgrade procedures, see Upgrading Advanced Web Diagnostics Server [p. 33].

4. Configure the Advanced Web Diagnostics Server.

   AWDS Basic Configuration Settings [p. 41] describes AWDS basic configuration, which has to be performed before the product can function.

   For detailed information on how to set all of the other configuration options supported by Advanced Web Diagnostics Server, please refer to *ClientVantage Agentless Monitoring System Administration Guide.*

CHAPTER 3

System Requirements

Ensure that your system meets the requirements to run ClientVantage Agentless Monitoring components.

Satisfying *minimum* requirements may not ensure the requested usability level. Choose the most appropriate hardware and system platform to achieve the best performance and optimal operation of your installation.

Recommended Hardware Platforms

Recommended hardware comes in two classes: Tier 1 and Tier 2. The table below represents specific platform support for Tier 1 and Tier 2. Although the performance between Tier 1 and Tier 2 is similar, Tier 2 hardware platforms have been designed to analyze much larger traffic data and to operate with a higher number of network interfaces. Tier 2 hardware architecture uses specific system models to support large traffic analysis and storage capabilities.

Table 2. Supported hardware platforms

Product	Tier 1	Tier 2
AMD	Dell, HP, IBM	HP, Sun, IBM
Report Server	Dell, HP, IBM, Sun	

For specific details and model numbers on Tier 1 and Tier 2 hardware configurations, please refer to a document titled *Recommended Hardware Configurations*.

Recommended Software Platform for Report Servers

The following software platform components are recommended for ClientVantage Agentless Monitoring report servers:

- Microsoft Windows Server 2008 (64-bit Edition) with the latest release, service packs, and five Client Access Licenses (CALs). Windows Server 2008 is the report server default platform.
- Microsoft Windows Server 2003 (64-bit Edition) with the latest release, service packs, and five Client Access Licenses (CALs).
- Microsoft SQL Server 2008 (64-bit Edition).
- Microsoft SQL Server 2005 (64-bit Edition).
- Adobe Reader, version 7.0.5 or higher.
- PuTTY (Telnet/SSH utility), version 0.58 or higher.
- WinSCP (Windows secure file copy utility), version 3.8.3 or higher.

The recommended minimum screen resolution on the report server machine is 1024x768, with at least 16-bit color mode.

Recommended Operating System Configuration for Report Servers

Typical preparations for a secure report server deployment require several steps to be performed on the side of the operating system. This section does not include all possible preventive measures, but it is intended to serve system administrators as a list of recommended good practices for system hardening.

1. Disable all unnecessary services.
   - Disable all unused system accounts (*for example*, Guest or SQLDebugger).
   - Disable DCOM.
   - Turn off indexing on all volumes (services).
   - Disable network protocols and bindings:

     SMB
     NetBios over TCP/IP

   - Disable the following services (if unused):

     Alerter
     Application Layer Gateway Service
     Application Management
     Automatic updates
     Background Intelligent Transfer Service (BITS)
     Computer Browser
     ClipBook
     Distributed File System
     Distributed Link Tracking Client
     Distributed Link Tracking Server
     MS Software Shadow copy Provider

DNS Server
Error Reporting Service
File replication
Help and support
HTTP SSL
Human Interface Device Access
IAS Jet Database Access
IMAPI CD Burning COM Service
Indexing Service
Intersite Messaging
Kerberos Key Distribution Center
Licence Logging Service
Messenger
Microsoft Search
NetMeeting Remote Desktop Sharing
Network DDE
Network DDE DSDM
Network Location Awareness (NLA)
Print Spooler
Remote Registry
Server
SNMP Trap Service
SQL Server FullText Search
TCP/IP NetBIOS Helper Service
Telnet
Telephony
Windows Management Instrumentation Driver Extension
WMI Performance Adapter
Windows Image Acquisition (WIA)

2. Remove all unnecessary executables and registry entries.
3. Apply restrictive permissions to files, services, end points and registry entries.
   All of these values should be created under the following registry key (if not present already):

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
   ```

   ```
   SynAttackProtect, REG_DWORD, 1
   EnableDeadGWDetect, REG_DWORD, 0
   NoNameReleaseOnDemand, REG_DWORD,1
   EnablePMTUDiscovery, REG_DWORD, 0
   KeepAliveTime, REG_DWORD (time in milliseconds), 300000
   EnableICMPRedirect, REG_DWORD, 0
   DisableIPSourceRouting, REG_DWORD, 2
   TcpMaxConnectResponseRetransmissions, REG_DWORD, 2
   TcpMaxDataRetransmissions, REG_DWORD, 3
   PerformRouterDiscovery, REG_DWORD, 0
   TcpMaxPortsExhausted, REG_DWORD, 5
   ```

   All values given above are hexadecimal.

For more information, refer to recommended reading on the Internet:

http://www.informit.com/articles/article.asp?p=371702&rl=1

http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45_gci1069540,00.html

http://support.microsoft.com/default.aspx?scid=kb;en-us;324270

MS SQL Server Setup Recommendations

The following sections provide a brief description of SQL Server 2005 setup for reliable and secure functioning with Advanced Web Diagnostics Server.

NOTE

Most of the recommendations listed here may have already been applied if the Agentless Monitoring Device was purchased as a *turnkey* solution. In cases when only Compuware software solution was chosen some of the steps may not be applicable. For more information, see *Purchase Options* in the *ClientVantage Agentless Monitoring – Getting Started Guide*.

The changes must be applied with caution so as not to affect the operation of the SQL Server or Advanced Web Diagnostics Server.

SQL Server 2005 Installation

Prior to SQL Server installation, make sure the following services are enabled (set the start to automatic) and started:

- COM+ System Application
- Distributed Transaction Coordinator

Then perform the following:

1. Start the installation of SQL Server 2005.
   Select the *Server components, tools, Books Online, and samples* install option.
2. Configure installation options.
   System configuration check may display several warnings about components needed only for Reporting Services. Because Reporting Services are not installed, the following warnings should not cause any problems with SQL Server 2005:
   - IIS Feature Requirement
   - ASP.NET Version Registration Requirement
3. Choose components to install.
   Select the following components:
   - SQL Server Database Services
   - Workstation components, Books Online, and development tools
4. Choose the instance name.
   Since it is permissible to utilize one of many MS SQL Server instances, you are permitted to use any name meaningful to you for each of the instances.
5. Define Service Account.

Select **Use the built-in system account** with **Local System** as an option.

6. Select the authentication mode.
   Choose **Mixed mode**, set *sa* password to *adlex*.
7. Define collation settings.
   Leave default Collation selection: **Dictionary order, case insensitive, for use with 1252 Character set**.
8. Disable **Error and usage Report Settings.**
   Do not send any data outside your network, clear all options.

SQL Server 2005 Configuration

After installing SQL Server 2005, perform the following configuration steps:

1. Create a new default database file location.
   Set the directory `e:\mssql\data` as **Database default locations** (for Data and Log).
2. Move the `tempdb` database to the new location.
   a) Open SQL Server Management Studio and connect to local database with administrative privileges (sa or local machine administrator). In **Object Explorer**, expand **Databases → System databases**, right click `tempdb`, and choose **New Query**.
   b) Execute the following query:

```
ALTER DATABASE tempdb MODIFY FILE ( NAME = tempdev , FILENAME =
'e:\mssql\data\tempdb.mdf' )
ALTER DATABASE tempdb MODIFY FILE ( NAME = templog , FILENAME =
'e:\mssql\data\templog.ldf' )
```

   c) Stop the SQLServer service.
   d) Move `tempdb.mdf` and `tempdb.ldf` from `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data` to `e:\mssql\data`
   e) Start the SQLServer Service.
   f) To verify changes in the database, execute the following query:

```
SELECT name, physical_name AS CurrentLocation, state_desc
FROM sys.master_files WHERE database_id = DB_ID(N'tempdb');
```

   A summary table like the following should appear:

Name	CurrentLocation	state_desc
tempdev	E:\mssql\data\tempdb.mdf	ONLINE
templog	E:\mssql\data\templog.ldf	ONLINE

   g) Close SQL Server Management Studio.
3. Turn off **Customer Experience Improvement Program**.

CHAPTER 4

Installing Advanced Web Diagnostics Server

Use the installation wizard to install your report server.

Note that no installation actions are performed until all of the installation information has been gathered and you have confirmed that the installation should proceed.

During the installation process:

- Click **Next** to record your selections for that step and proceed to the next step (unless errors or inconsistencies are found in the choices you specify).
- Click **Back** (if available) to go to the previous step and change settings.
- Click **Cancel** (if available) to terminate the process.

CAUTION

When installing or upgrading AWDS keep in mind that its configuration has to be synchronized with VAS, since AWDS utilizes configuration settings from VAS. As a consequence, if you had different configuration settings for AWDS and for VAS, the AWDS settings will be overridden by the VAS settings.

This is because VAS is the primary reporting engine and the whole configuration for ClientVantage Agentless Monitoring is maintained by the Vantage Configuration for Agentless End-User Experience - Console (VCAEUE Console). An AWDS can exist with a VAS only in a server farm, where the master server (VAS) populates its configuration to all slaves (AWDSes and/or VASes).

Please refer to *Backing up and Restoring Reporting Group Definitions from AWDS* in the *ClientVantage Agentless Monitoring – System Administration Guide* for information on how to save reporting groups configuration from AWDS before establishing a farm connection between servers.

Performing the Installation

You must have Administrator privileges to install Advanced Web Diagnostics Server.

CAUTION

Exit all programs before running the setup program. Some Windows programs, such as anti-virus software, may interfere with the installation process.

To install the report server:

1. Activate the installation program.

   Insert Advanced Web Diagnostics Server installation CD into the CD-ROM drive. The Vantage Setup browser should automatically appear. If it does not, navigate to the root directory of the CD and double-click the file named `setup.exe`.

   The Vantage Setup browser lists all of the products provided on the installation CD and links to product documentation and release notes.

2. Select the product to install.

   Advanced Web Diagnostics Server is available in versions for 32-bit and 64-bit platforms.

   - If you are installing it on a machine with a 32-bit architecture, click **Install Advanced Web Diagnostics Server** to install the 32-bit version.
   - If you are installing it on a machine with a 64-bit architecture and sufficient system resources, you can use either the 32-bit or the 64-bit version of Advanced Web Diagnostics Server.

     Compared with the 32-bit version, the 64-bit version of Advanced Web Diagnostics Server uses more memory to handle the same volume of traffic, but it is capable of managing much larger volumes of traffic, provided your computer is equipped with sufficient memory to support this. The recommended minimum memory size for installing the 64-bit version is 12GB. If you decide to use the 64-bit version, click **Install Advanced Web Diagnostics Server x64**.

   You may briefly see one or two messages from the InstallShield Wizard telling you that InstallShield Wizard is being prepared and initialized for the installation process. This may take a few seconds, after which a Advanced Web Diagnostics Server welcome screen displays the product release number.

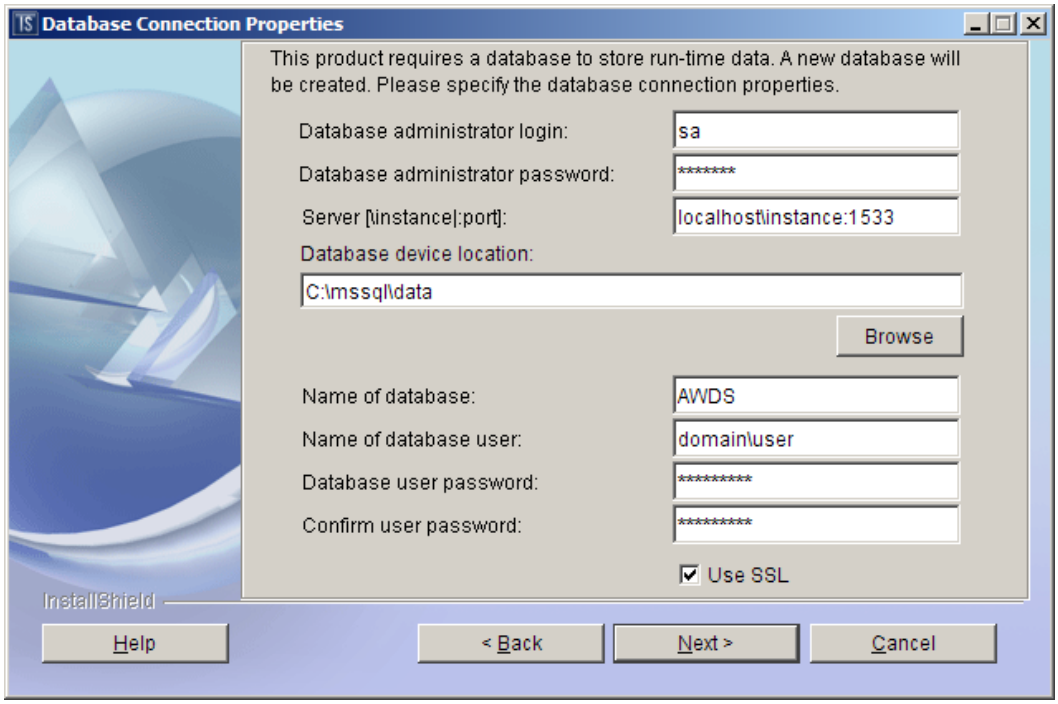
3. If a warning concerning insufficient RAM appears, click **Cancel** to abort the installation process or click **Next** to proceed with installation.
4. Click **Next** on the Advanced Web Diagnostics Server welcome screen, view the license agreement screen, and, if you agree with the terms of the license agreement, indicate your choice and click **Next** to proceed with the installation or **Cancel** to terminate the installation.
5. Type or browse for the target installation directory and click **Next**.

   If a previous installation is detected, you are offered the choice of reinstalling or upgrading your product. Refer to Upgrading Advanced Web Diagnostics Server [p. 33] for details of re-installation and upgrade procedures.

6. Define the SQL database connection properties.

   Advanced Web Diagnostics Server requires a database to store run-time data. You need to specify the information as shown on the following screen:

Figure 1. Defining SQL database connection properties



You may need to consult the database administrator to determine the correct values. If the database server is on the same machine, enter the word **`localhost`** in the **Server** field. For remote servers, enter the server name or IP address. Add the port number (preceded by a colon) if it is different from the default value of 1433. Using a "\" separator, you can indicate the SQL database instance to which you want to connect. You can also point to the SQL server instance by giving the port number only instead of the name. For more information, see Determining Microsoft SQL Server Named Instance Port Number [p. 53].

The database device location is the physical location of the database on the database server computer.

The default database username can be replaced with a local database server user or a valid domain user. Specify a domain name in the following format: **`domain\user`**.

CAUTION

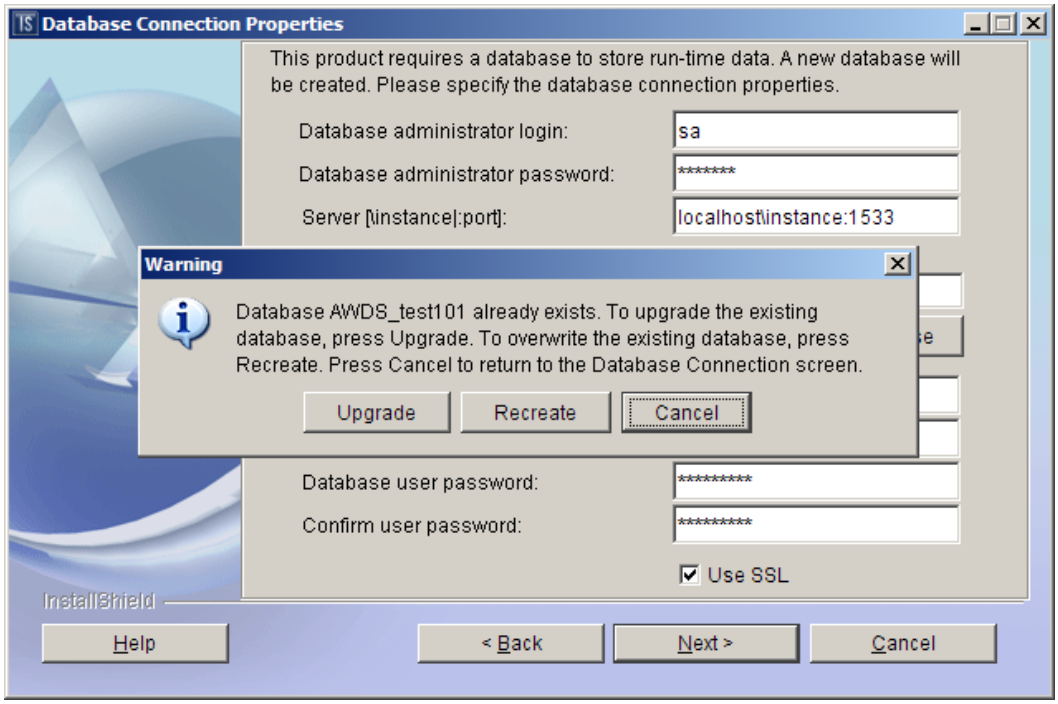
If you are going to create a database on Microsoft SQL Server 2008 and want to use a Windows domain user as the database user, you must enable this account on the SQL server prior to the report server installation. Make sure the domain user is assigned the `sysadmin` server role.

Select or clear **Use SSL** to indicate whether encryption should be used in communication with the SQL Server. Note that for this feature to work, you must also set **Force Encryption** to **Yes** in the SQL Server instance network configuration.

Click **Next** to submit your database connection choices.

7. If a database of the specified name already exists, a warning message prompts you to specify whether to **Upgrade** the existing database (and preserve the data) or **Recreate** the database (and delete all of your existing data).

Figure 2. Selecting to upgrade or recreate a database



If you want to specify another database name, click **Cancel** to go back to the previous installation screen.

8. If the **Database Size** screen appears, specify the size of the new database and then click **Next**.

   This screen is displayed if no database of the specified name already exists, or if you have selected to overwrite an existing database. The suggested size displayed on this screen is calculated to leave room for performing a backup of the database on the same disk.

9. If the **Database Server Memory Setting** screen appears, specify the maximum size of the SQL server memory and then click **Next**.

   This screen is displayed if a new database is created or if an existing database is overwritten.

   Note that for the reconfiguration to take effect, the SQL server must be restarted. If you are using a local SQL server, the installation program offers to restart it automatically. If you have specified a remote server, you are asked to restart the server manually before attempting to use the database.

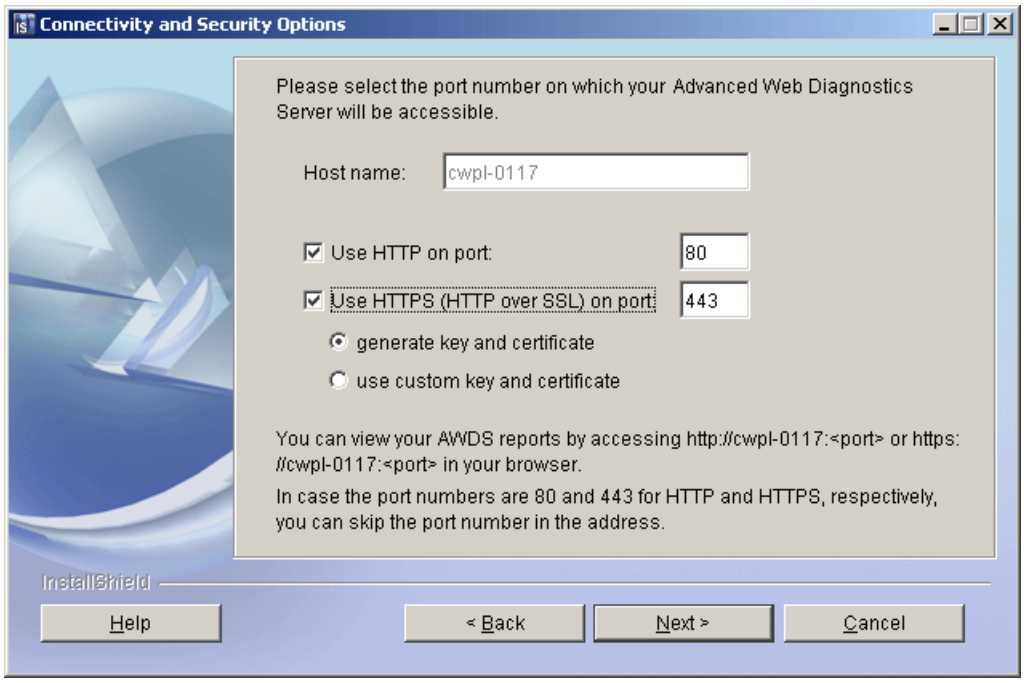
10. Configure the connectivity and security options.

    The configuration screen prompts you to specify the port number on which your Advanced Web Diagnostics Server should be accessible. The host name under which your Advanced Web Diagnostics Server will be recognized is shown on the screen for your information. You will view your Advanced Web Diagnostics Server reports by accessing this host in your browser. The host name should be followed by the port number, if the port number is not 80.

    If you need to transfer or display the reports securely across the network, you can also specify the HTTPS port number. When accessing the Advanced Web Diagnostics Server reports on a port other that 443, remember to supply the selected port number together with

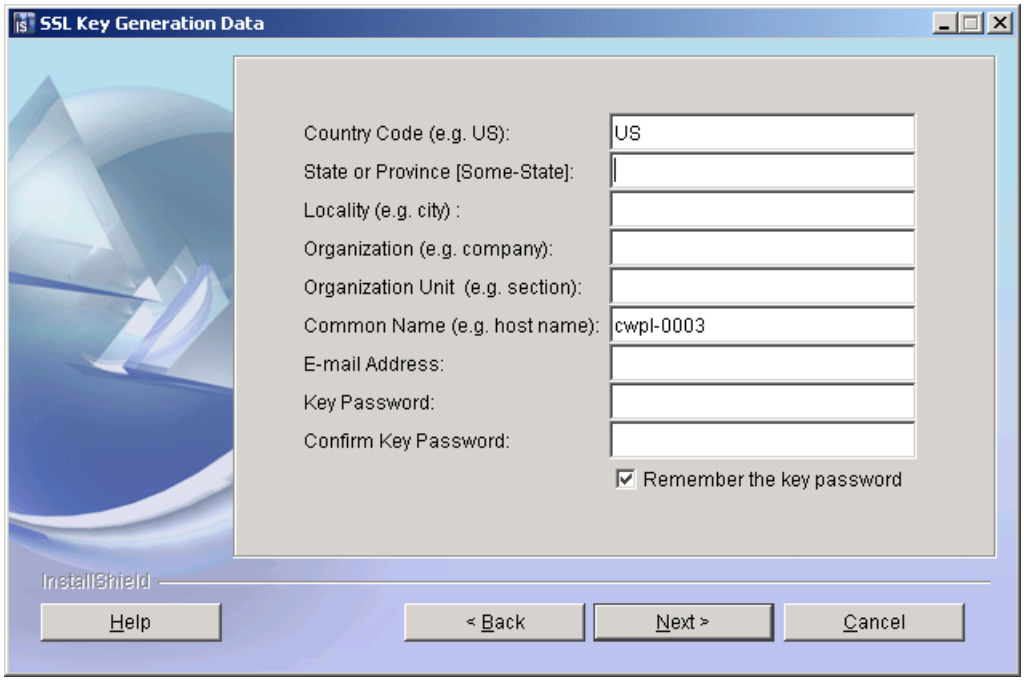
the host name in your browser. Note that HTTP/HTTPS settings can be modified by running the **Change/Remove** program from the **Add or Remove Programs** utility.

Figure 3. An example of the **Connectivity and Security Options** screen



If you select the HTTPS option, the **SSL Key Generation Data** screen enables you to either automatically generate a key and a certificate, or to use a custom encryption key. To generate the key, provide the required data, which varies depending on whether you chose automatic or custom key generation.

Figure 4. Supplying SSL key generation data



Choosing a custom encryption key requires configuring the server manually, which involves copying both the key and the certificate to the proper directory and modifying the `common.properties` file. For more information, see Configuring the Report Server to Communicate over HTTPS [p. 31].

NOTE

On the **SSL Key Generation Data** screen, there is a **Remember the key password** check box. If you decide not to store the password during the installation procedure, you can supply it on system start-up, but only if you are using a console that is directly connected to the server. Remember that the dialog box for entering the password will *not* appear if you are connected to the server using a remote console.

Also, remember that not providing a password means that the key will not be encrypted.

11. Review the summary of your installation choices and, if you are satisfied with them, click **Install**.

    If you need to change anything, use the **Back** button to retrace your steps to the appropriate configuration screen.

12. Your Advanced Web Diagnostics Server software is installed.

    The process of installing and pre-configuring software components and defining your database may take several seconds, minutes, or even hours, depending on the size of the database. A progress box shows the status of the installation action currently in progress. When all of the required actions have been completed, a final post-installation information screen is displayed.

13. Perform post-installation actions.

Depending on the operating system you are using, you may be asked at this stage whether you want to start Advanced Web Diagnostics Server. Indicate your choice in the check box provided and click **Finish**.

Configuring the Report Server to Communicate over HTTPS

You can set up your report server to use secure connections with user Web browsers, and to use automatically generated data or your own keys and certificates.

Prerequisites

It is recommended that secure access be performed using `TLSv1` (TLS version 1), which is more secure than its predecessors. Use of older versions of the protocol can be configured by setting the configuration property `connector.ssl.SSLProtocol` to `SSLv3` or `SSLv2`, as required. Note that Apache Tomcat default is `all`, with other acceptable values being `SSLv2`, `SSLv3`, `TLSv1`, and `SSLv2+SSLv3`. Leaving the `connector.ssl.SSLProtocol` parameter empty causes the Web browser negotiate the version of a secure protocol when connecting to the Web server. For more information on secure connection configuration in Apache Tomcat, refer to *http://tomcat.apache.org/tomcat-6.0-doc/apr.html#HTTPS*.

The report server implementation of SSL uses OpenSSL. This means that encryption, certification, and other operations are handled as defined in OpenSSL.

The subdirectory `tools\openssl` of the report server installation directory contains the OpenSSL tool, which can be used for SSL key and certificate generation, conversions, and management. The report server installation process uses the tools in this directory to generate a self-signed SSL certificate and a key pair for initial HTTPS server operation.

This certificate and the key pair are, by default, stored in the `wwwroot/WEB-INF/ssl` subdirectory of the report server installation directory. To change this path, modify the `connector.ssl.SSLCertificateFile` and `connector.ssl.SSLCertificateKeyFile` configuration properties in `common.properties`.

To configure your own encryption keys and register the server in the CA (certificate authority) infrastructure, the `common.properties` file has to be edited manually. Refer to the Apache Tomcat documentation: *http://tomcat.apache.org/tomcat-5.5-doc/apr.html*.

All certification procedures, such as certificate request or certificate signing, have to be handled manually by using the OpenSSL utility. For instructions on how to use the OpenSSL utility, refer to *http://www.openssl.org*.

The report server can connect to the network via standard HTTP or HTTPS (HTTP over SSL), both of which are supported by the report server installation process, or via other modes that can be configured manually.

The connectivity configuration settings are stored in the configuration file `common.properties`, in the `config` subdirectory of the report server installation directory. The names of the configuration properties in `common.properties` follow the standard names used for Tomcat

and OpenSSL. (The format of the file is different, but the names of the configuration parameters are the same.)

All of the connectivity configuration properties are set by the installation program during report server installation.

NOTE

Subsequent modifications to connectivity settings are possible but should be performed with great care. These settings require a thorough understanding of Web server connector settings and OpenSSL.

The simplest procedure for joining the server to the certification infrastructure can be summarized as follows:

1. Generate a private RSA key as described in *http://www.openssl.org/docs/HOWTO/keys.txt*.

   It is suggested that the password should be encrypted. The report server can ask for the key password every time it starts, or the password can be configured using the report server installation program.

2. Create a certificate request as described in *http://www.openssl.org/docs/HOWTO/certificates.txt* (section 3).
3. Pass the certificate to a certification authority for signing.
4. Set configuration properties.

   Configure the following settings in the `common.properties` file:

   - Point `connector.ssl.CertificateFile` to the received certificate file.
   - Point `connector.ssl.CertificateFileKey` to the generated key.
   - Point `connector.ssl.CertificateChainFile` to the chain of certificates.

5. Set the key password.

   If the key was encrypted, use the report server installation program to set the key password.

CHAPTER 5

Upgrading Advanced Web Diagnostics Server

The Advanced Web Diagnostics Server installation program will detect older versions of the product and offer to upgrade them to the current release, optionally preserving configuration information and traffic monitoring data contained in the Advanced Web Diagnostics Server database. Configuration migration is fully supported for upgrades from versions not older than two releases back. If upgrading from an earlier version, some elements of configuration migration may have to be performed manually. This applies in particular to the configuration of alarms.

CAUTION

When installing or upgrading AWDS keep in mind that its configuration has to be synchronized with VAS, since AWDS utilizes configuration settings from VAS. As a consequence, if you had different configuration settings for AWDS and for VAS, the AWDS settings will be overridden by the VAS settings.

This is because VAS is the primary reporting engine and the whole configuration for ClientVantage Agentless Monitoring is maintained by the Vantage Configuration for Agentless End-User Experience - Console (VCAEUE Console). An AWDS can exist with a VAS only in a server farm, where the master server (VAS) populates its configuration to all slaves (AWDSes and/or VASes).

Please refer to *Backing up and Restoring Reporting Group Definitions from AWDS* in the *ClientVantage Agentless Monitoring – System Administration Guide* for information on how to save reporting groups configuration from AWDS before establishing a farm connection between servers.

Navigating the Upgrade Process

- Click **Next** to record your selections for that step and proceed to the next step (unless errors or inconsistencies are found in the choices you specify).
- Click **Back** (if available) to go to the previous step and change settings.
- Click **Cancel** (if available) to terminate the process.

Performing a Report Server Upgrade

You must have administrative privileges to upgrade Advanced Web Diagnostics Server.

CAUTION

Exit all programs before running the setup program. Some Windows programs, such as anti-virus software, may interfere with the upgrade process.

To upgrade Advanced Web Diagnostics Server (to install a newer version over an existing version):

1. Stop the currently running server.

   In Windows, click **Start → Programs → Advanced Web Diagnostics Server → Server → Stop**.

2. Activate the installation program.

   Insert the Advanced Web Diagnostics Server installation CD into the CD-ROM drive. The Vantage CD browser should automatically appear. If it does not, navigate to the root directory of the CD and double-click the file named `Autostart.exe`.

   The Vantage CD browser lists all of the products and documentation provided on the installation CD.

3. Specify whether to install the 32-bit version or the 64-bit version of the product.

   Advanced Web Diagnostics Server is available in two versions:

   - For a machine with a 32-bit architecture, click **Install Advanced Web Diagnostics Server** to install the standard 32-bit version.
   - For a machine with a 64-bit architecture, you can use either the 32-bit version (as above) or you can click **Install Advanced Web Diagnostics Server x64** to install the 64-bit version of Advanced Web Diagnostics Server.

     You should choose based on the available memory and the volume of traffic you need to monitor. Compared with the 32-bit version, the 64-bit version of Advanced Web Diagnostics Server uses more memory to handle the same volume of traffic, but it is capable of managing much larger volumes of traffic, provided your computer is equipped with sufficient memory to support this. The recommended minimum memory size for installing the 64-bit version is 12GB.

   NOTE

   Upgrade from a 32-bit version to a 64-bit version is not supported. If you need to perform such an upgrade, you must save your 32-bit configuration settings manually (this pertains only to new server configuration files added after the 32-bit installation) and uninstall the 32-bit version of the product, while preserving the database. You should then install the 64-bit version as a new installation, not an upgrade, and perform a manual migration of configuration settings. Note that those settings that are maintained in the database will be migrated together with the database. For more information, see Migrating the Report Server to 64-bit Version [p. 39].

When you select the version, you may briefly see one or two messages from the InstallShield wizard telling you that InstallShield Wizard is being prepared and initialized for the installation process, after which the welcome screen displays product release number information and the amount of physical memory available is checked.

4. If the detected amount of physical memory (RAM) on the target machine is lower than the recommended amount, you will see a warning message.

   Click **Cancel** to abort the installation and perhaps upgrade the machine's RAM before restarting the installation process, or click **Next** (not recommended) to continue this installation with less than the recommended amount of RAM.

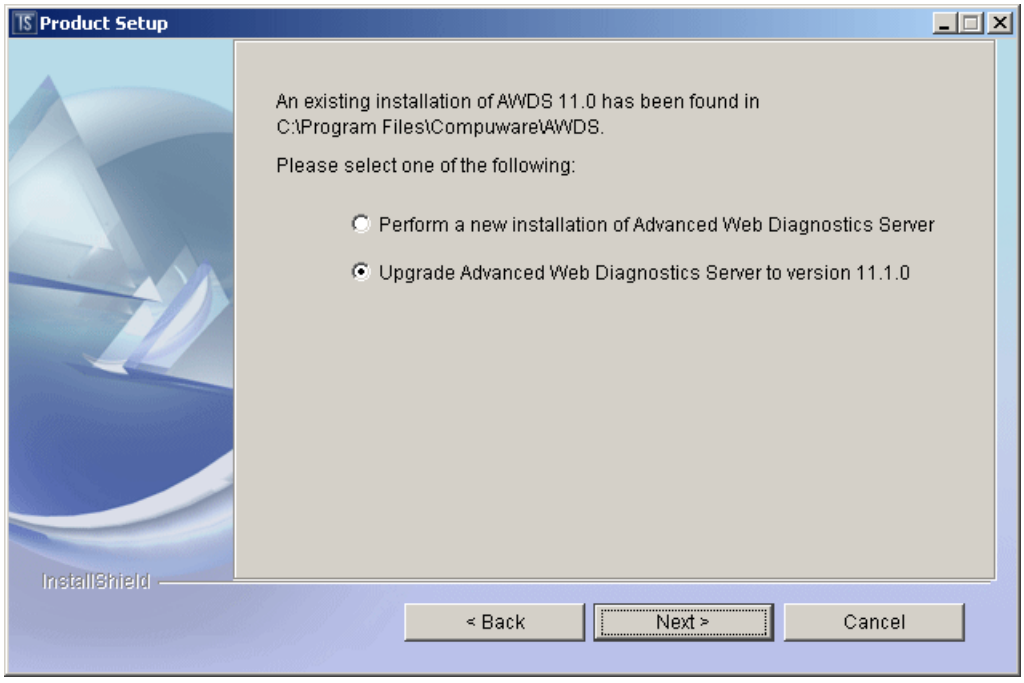
5. Click **Next** on the welcome screen and view the license agreement screen.
6. If you agree with the terms of the license agreement, select the appropriate radio button and click **Next** to proceed with the installation.

   If you do not accept the terms of the license agreement, click **Cancel** to terminate the installation process.

7. Choose whether to perform a new installation or an upgrade to the current installation.

   When an existing version of the software is detected, you are given the option to either perform a fresh installation of the current version of the product, or to upgrade, while optionally preserving configuration settings and/or database contents:

Figure 5. Choosing between a new installation and an upgrade



Note that configuration migration is fully supported for upgrades from versions 1.6 or later. (Version 1.6 of Advanced Web Diagnostics Server was distributed together with version 4.6.3 of the Vantage Analysis Server.) If upgrading from an earlier version, some elements of configuration migration may have to be performed manually.

After you select an option (new installation or upgrade), click **Next** to proceed with the new installation or upgrade. Note that Advanced Web Diagnostics Server component services will be stopped before the installation or upgrade can be performed.

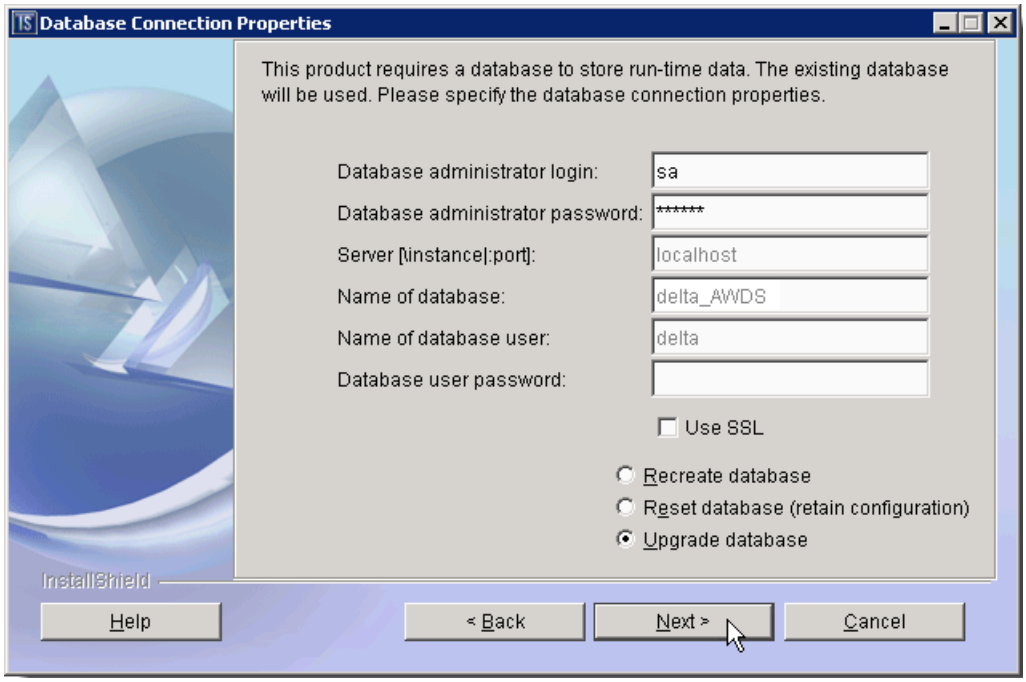
IMPORTANT

- If you chose to perform a new installation, you should stop reading this procedure and now refer to Step 5 [p. 26] of Installing Advanced Web Diagnostics Server [p. 25].
- If you chose to perform an upgrade, continue with the next step of this procedure.

8. Confirm SQL database connection properties.

   Advanced Web Diagnostics Server requires a database to store run-time data. When you are upgrading an existing installation, the current database connection properties are displayed, allowing you to modify the database administrator login name and password:

Figure 6. Database Connection Properties



Select or clear the **Use SSL** check box to indicate whether SSL should be used in communication with a report server.

Use the radio buttons to specify what to do with the database:

Recreate database

This option deletes the database and creates a new database of the same name. All the information contained in the database is lost.

Reset database

This option purges traffic monitoring data from the database but preserves the product configuration settings.

Upgrade database

This option preserves all traffic monitoring data and product configuration settings.

Click **Next** to submit your database connection choices.

9. *Optional:* Modify HTTP/HTTPS settings.

During the upgrade procedure, you cannot change connectivity and security settings. However, you can do so at any time after the upgrade by running the **Change/Remove** program from the **Add or Remove Programs** utility located in the Windows **Control Panel**. Each time, during the server upgrade to 11.1 version, a screen will appear to remind you about it.

Figure 7. The **HTTP Connection Info** screen

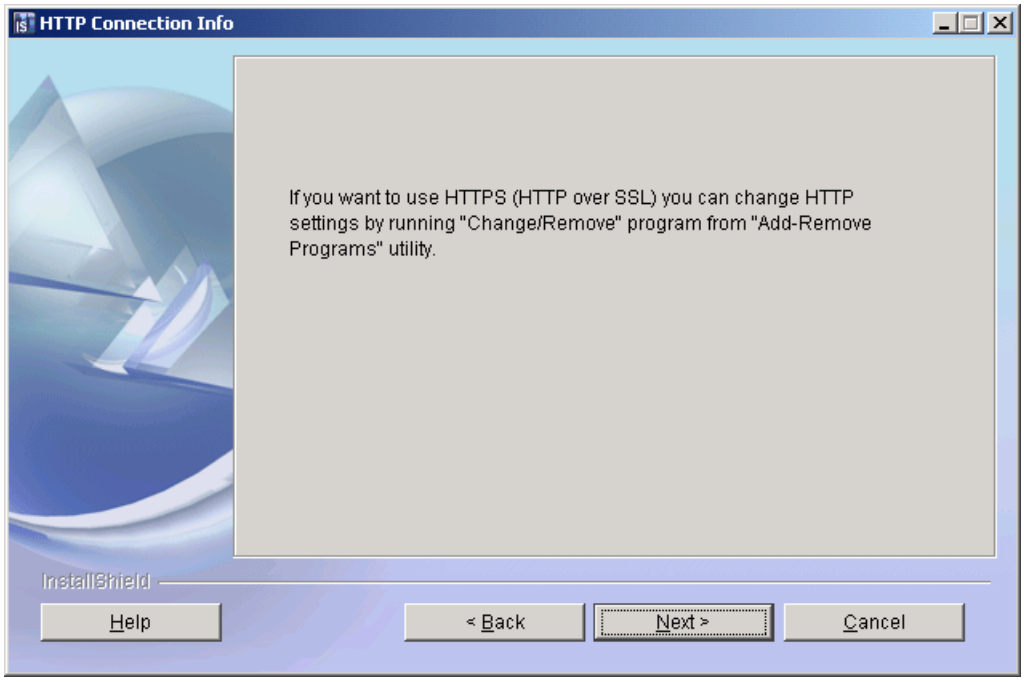
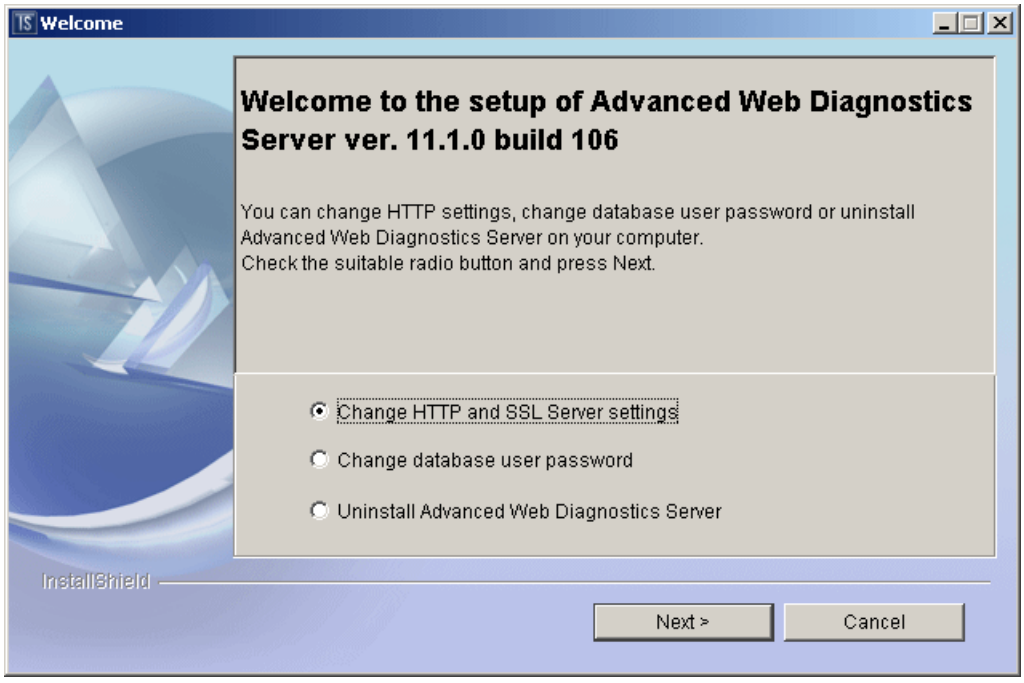


Figure 8. Modifying the HTTPS settings on the **Change/Remove** screen



For more information on how to configure HTTPS settings, refer to the Step 10 [p. 28] of the Advanced Web Diagnostics Server installation procedure, and to Configuring the Report Server to Communicate over HTTPS [p. 31].

10. Review the summary of installation choices.

    Before the actual upgrade commences, a summary screen displays all of the choices you have made. Review them carefully and, if you need to change any of them, use the **Back** button to retrace your steps to the appropriate configuration screen.

11. Upgrade Advanced Web Diagnostics Server

    On the summary screen, click **Install** to commence the actual process of upgrading and pre-configuring software components and defining your database. The amount of time this takes depends on the size of the database and may be anything between several seconds and, for large databases, several hours. A progress box shows the status of the installation action currently in progress. When all of the required actions have been completed, a final post-upgrade information screen is displayed.

12. Perform post-installation actions.

    Depending on the operating system you are using, you may be asked at this stage whether you want to start Advanced Web Diagnostics Server. Indicate your choice in the check box provided and click **Finish**. There is no such choice for Windows 2000, which requires re-booting before the Advanced Web Diagnostics Server can function. In case of Windows 2000, after clicking **Finish** on the post-installation information screen, you will be asked, in a separate message box, if you wish to re-boot the system now or later.

    It is possible to change the database user password during the upgrade procedure (see Step 8 [p. 36]) or at any time after the installation or upgrade by running the **Change/Remove**

program from the **Add or Remove Programs** utility located in the **Control Panel** (Figure 8. Modifying the HTTPS settings on the Change/Remove screen [p. 38]).

After selecting the option **Change database user password** choose **Next** and enter a new password in the following screen.

Migrating the Report Server to 64-bit Version

Prerequisites

A working installation of a 32-bit version with a database attached, is required in order to upgrade to a 64-bit version. Make note of the `sa` database password and path to the database.

The path for upgrading to a 64-bit version of AWDS requires uninstalling of the current 32-bit version, and installation of a new 64-bit version. This process requires a manual transfer of custom settings from one version to the other. The majority of report server configurations and settings are stored in the attached database. Only the configuration files that were created after the default installation need to be transferred manually. These include alarm configuration files located in `C:\Program Files\Compuware\AWDS\config` folder and custom SQL scripts that are located in the `C:\Program Files\Compuware\AWDS\config\sql\ms\def` folder.

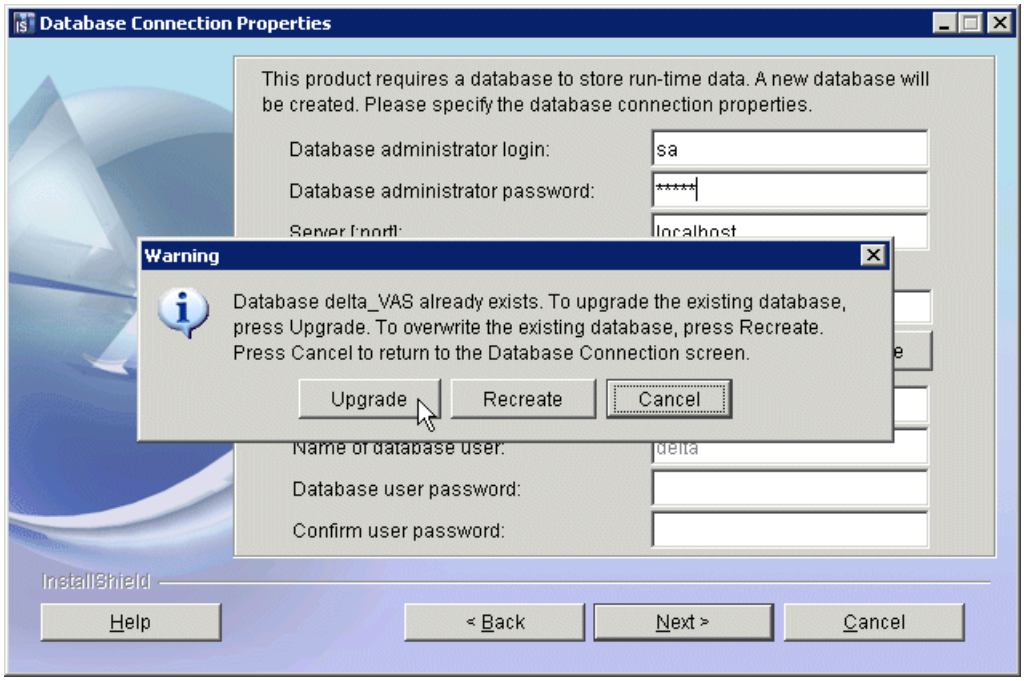
- Files starting with `alarm-` in their filename located in the `C:\Program Files\Compuware\AWDS\config` folder should be copied to a repository folder outside of the current VAS installation path.
- The SQL script files located in the `C:\Program Files\Compuware\AWDS\config\sql\ms\def` folder should be copied to the repository folder.
- The current 32-bit version of VAS should be uninstalled preserving the database.
- The new 64-bit version should be installed using default installation path and the **upgrade** option for the database installation.
- All of the configuration files should be moved back to their respective paths within a new installation.

1. Create a temporary repository folder.
2. Navigate to `C:\Program Files\Compuware\AWDS\config` and copy all files starting with `alarm-` to the repository folder.
3. Navigate to `C:\Program Files\Compuware\AWDS\config\sql\ms\def` and copy all of the SQL scripts to the repository folder.
   The repository folder should now contain all of the alarm XML files and all of the SQL script files.
4. Uninstall the current 32-bit version using **Add or Remove Programs** in the **Start** → **Settings** → **Control Panel**.
5. Install the AWDS 64-bit version using the same installation procedures and information used for the 32-bit version.

CAUTION

Make sure that during the installation process, the **Upgrade** option is chosen when the existing database is detected.

Figure 9. Database upgrade



6. Copy all the `alarm-` files from the repository to the `C:\Program Files\Compuware\AWDS\config` folder.
7. Examine and compare the `C:\Program Files\Compuware\AWDS\config\sql\ms\def` folder contents with the repository and copy the missing SQL scripts from the repository into the new installation.

The new 64-bit installation will now contain the configuration read from the upgraded database and all of the custom alarm and SQL scripts created in the 32-bit version.

It is recommended to confirm that the new installation contains the proper settings before removing the temporary repository.

CHAPTER 6

AWDS Basic Configuration Settings

When you use Advanced Web Diagnostics Server for the first time, you are asked to specify basic configuration options that must be specified before Advanced Web Diagnostics Server starts to function. You must have administrative privileges to make these settings.

The scalability options allow you to configure your Advanced Web Diagnostics Server to handle the volume of traffic you expect to monitor.

NOTE

Recommended hardware comes in two classes: Tier 1 and Tier 2. For more details on Tier 1 and Tier 2 hardware configurations, see Recommended Hardware Platforms [p. 19].

Small Web site

When you select **Small Web site**, you can collect detailed information about a small number of page loads per day—approximately 2 million on Tier 1 equipment.

Page Elements
When you select **Small Web site**, **Page Elements** are stored in a database.[1]

Page Headers
By default, page headers are stored on the AMD. To store all page headers in the database, select **Store page headers in DB**. This will increase the size of the database (approximately 6 to 7 times larger than the original size).

[1] For XML and SOAP, **Page Elements** data is identical to **Page Analysis** data, so, to avoid unnecessarily keeping the duplicates in the database, a `VDATA_FILTER_XMLSOAP` filter is set to `true` by default. Keeping this filter set to `true` saves disk space but, because the XML and SOAP entries are filtered out, it makes reporting on the Page Elements level (elements or headers) impossible.

To change the value of `VDATA_FILTER_XMLSOAP` property in `userpropertiesadmin`, type **`http://AWDS_server/userpropertiesadmin`** in the Web browser's **Address** bar and press `[Enter]`, change the filter's property value, and click **Set value** to accept the change. To access this screen, you need to have administrative privileges for the report server.

NOTE

Storing page headers on the AMD introduces certain limitations to the Page Elements data view. If header data is stored on the AMD, and if you use page header-related dimensions in your report—including Request header, Request parameters (from URL), POST data, POST data (raw) and Request cookie in the **HTTP request** section, and Response header, Response cookie in **HTTP response** section—you also have to apply an *Operation ID* or *Hit ID* filter in this report.

The data daily storage default limit for a small Web site is 2M pages per day. By default, data is still written to the database if the daily storage limit is exceeded, and only an alert is issued. However, this behavior, as well as the limit itself, can be changed by a user with administrative privileges. For more information, see Scalability-related configuration properties [p. 43].

Large Web site

When you select **Large Web site**, you can collect aggregated information about a large number of page loads per day, approximately 10 million on Tier 1 equipment. The efficiency of Tier 2 is from 30% to 50% higher than that of Tier 1.

The data daily storage default limit for a large Web site is 10 million pages per day. By default, data is still written to the database if the daily storage limit is exceeded, and only an alert is issued. However, this behavior, as well as the limit itself, can be changed by a user with administrative privileges. For more information, see Scalability-related configuration properties [p. 43].

Page Elements

The **Page Elements** data view is limited in its report generation capability by the fact that traffic monitoring data is stored on the AMDs and not in the report server's database.[1]

Page Headers

Page header data is stored on the AMDs. (This is mandatory for large Web sites.)

NOTE

Because of Page Elements view limitations resulting from storing page headers on the AMD, if you use page header-related dimensions on a report—including Request header, Request parameters (from URL), POST data, POST data (raw) and Request cookie in the **HTTP request** section, and Response header, Response cookie in **HTTP response** section—you must also filter report data by **Operation ID**.

If no page header-related dimensions are used, you can choose to filter the report either by **Operation ID** or—provided the report interval limit is equal to or less than one hour—by **User name**.

Data aggregation performed for large Web site mode does not affect the accuracy of the predefined reports, but it may influence reports you create using the DMI report generation tool.

- The following AWDS reports are not available in large Web site mode:

Page Design Problem Overview
Largest Page Elements
Most Popular Page Elements

The following AWDS reports are unavailable when accessed from VAS:

Load Sequence – Stepchart
HTTP Response by Page Element

Scalability-related configuration properties

If you have administrative privileges, you can modify the default configurations described above using options on the **User Properties** screen. To access this screen, in the Web browser's **Address** bar, type:

`http://`*`AWDS_server`*`/userpropertiesadmin`

Configurable properties include:

`FDI_SAVE_ONLY_SLOW_PAGES`
When this is set to `TRUE`, the server will store only slow pages in the database.

`FV_THR_SMALL_SITE`
Determines the daily storage limit for small Web site mode, which by default is 2 million pages per day.

`FV_THR_LARGE_SITE`
Determines the daily storage limit for large Web site mode, which by default is 10 million pages per day.

`FV_THR_APPLY_PAGES_LIMIT`
When this is set to `1`, data is not written to the database if the daily storage limit is exceeded.

`FDI_ADD_CLIENT_TO_AGGR`
When this is set to `TRUE`, client information (client IP, user name, tier client IP) is added to aggregation.

Modifying AWDS Basic Configuration Settings

After AWDS has been accessed for the first time and configured, the basic configuration screen does not appear automatically when the server is started. However, it can always be accessed by selecting **Settings → Advanced Web Diagnostics Server → Scalability Settings**.

CAUTION

Selecting the **Store page headers in DB** check box under **Small Web site** will increase the size of the database required for data storage. If database size is of concern, it is best to leave this setting as default (not selected).

The scalability settings do not affect historical data, and you do not need to purge the report server database when changing the scalability settings. However, note that the collected data can vary depending on the scalability configuration. *For example*, in the large Web site mode, client IP addresses and user names are not stored. This means that if you change the settings to the small Web site mode, this information will not appear on the reports covering older data, that is, the period of time when large Web site was selected.

Configuring Other AWDS Settings

For detailed information on how to set all of the other configuration options supported by Advanced Web Diagnostics Server, please refer to *ClientVantage Agentless Monitoring—System Administration Manual*. Sections referring exclusively to Advanced Web Diagnostics Server are marked “(AWDS)”; sections referring to all of the ClientVantage Agentless Monitoring report servers, including Advanced Web Diagnostics Server, have no applicability annotations in titles.

CHAPTER 7

Licensing ClientVantage Agentless Monitoring Products

Vantage products are protected by a license management system called Compuware Distributed License Management (DLM).

DLM uses the following components to help manage product licensing:

License File

DLM authorizes you to use Compuware products through a license file, which is a text file that contains information about the component options purchased with the product, including information for the product's features and the number and types of licenses that were purchased.

Compuware License Service (`cpwr.exe`)

An application (invoked by the DLM application or executed from the command line) that manages and services requests for the licenses of your Compuware products. The Compuware License Service can be installed on Windows and UNIX platforms. In many cases, it is recommended that you co-locate the Compuware License Service with the server-based components of one of the Compuware products you are installing.

License types

DLM offers several different types of licenses as described in the table below. Each Compuware product may support different combinations of these license types.

Table 3. DLM license types

License type	Description	Obtained by...
Trial License	A trial license ships with some Compuware products. This license type lets you evaluate the product. The default evaluation period is two weeks, after which time the trial license expires.	Installing the product.

License type	Description	Obtained by...
Temporary License	A temporary license has a fixed expiration date from the time that it is installed on your system. You must run the DLM to install this license type.	Requesting the license from Compuware, not shipped with the product.
Permanent Node-Locked License	A Permanent Node-Locked license is a client-based single-user license and does not have an expiration date. A Node-Locked license is identified by the HOSTID keyword in the license file and must always run on the same machine (same *node*, and hence the license is "node-locked") as it was originally installed. If you change workstations or *NIC* cards, you must contact Compuware to obtain a new license.	Running the DLM to determine your node identifier and providing the information to Compuware. Compuware will e-mail you a license file based on the node identifier. Vantage licenses will only recognize the first NIC address identified during system startup. If you have a multi-homed system, you will need to obtain a license based on your disk serial number.
Permanent Concurrent (Floating) License	A Permanent Concurrent license is server-based and allows you to purchase a specific number of licenses without assigning them to a particular workstation. When all available licenses are checked out from the License Manager, no additional users can run the product until a license is checked back in. This type of license has a license file with SERVER and DAEMON lines.	Running the DLM on the server for the License Manager to obtain the node identifier and providing the information to Compuware. The License Manager software and the license files must be installed on the server. Use the DLM from the client machines to connect them to the License Manager.
Borrowed License	A borrowed license is a license that the user checks out of the borrow proxy server and later checks back in. This enables the user to detach from the network and still use the Compuware product.	License must be requested from Compuware. Requires the Borrow License Client application to be installed in the same directory as the DLM.

Licensing Report Server Features

Compuware recommends that you back up the license information (license file) before installing the license with the Compuware Distributed License Management (DLM).

If, on the computer on which you are installing the report server, DLM is not already installed, it will be installed automatically as part of the report server installation.

NOTE

A stand-alone installation of DLM can also be found on the report server installation CD. For a 32-bit version of the report server, use the DLM version in the subdirectory named `win32`; for a 64-bit version of the report server, use the DLM version in the `x64` subdirectory.

When the report server is first installed, a two-week trial license is installed with the product. The trial license allows you to use both of the configurable personalities of the product as well as all of the licensable features. To continue using the product past the trial period, contact Compuware to obtain a license suited to your requirements.

If you are using multiple Compuware products, merge the license files with the DLM to easily manage the licenses.

You can run the licensing utility by selecting **Start → Programs → Compuware → Distributed License Management**.

Refer to the License Manager documentation for instructions on using the DLM to install a new or trial license.

NOTE

The report server checks for new licenses every few minutes. Therefore, it may take a number of minutes before a newly applied license is recognized by the server.

Features are usually licensed on the report servers, with the feature-specific functionality being enabled on the AMD , but if the AMD is a standalone product with no report server available, it is also possible to license a feature on the AMD itself.

Post-licensing actions

After installation of a new license on the report server, re-application of the license to AMDs is performed automatically. AMDs are able to accept a new license without restart. Note, however, that if the new license extends the current functionality of the product, this new functionality has to be configured before it can be used. For example, if the new license allows you to monitor a new protocol, this protocol has to be added to the list of monitored protocols by specifying it in the configuration settings.

Licensed Features Supported by VAS, AWDS, and AMD

Vantage Analysis Server (VAS) and Advanced Web Diagnostics Server (AWDS) are licensed per module, which mean that for each of the analysis options you use (such as Web, Enterprise, Database analyzer, or Oracle Forms), you must purchase a license. Compuware does not limit the usage of the report servers; any number of users can access VAS and AWDS reports.

The following separately licensable features are supported by VAS, AWDS, and Agentless Monitoring Device (AMD):

Table 4. ClientVantage Agentless Monitoring and Agentless Monitoring Device licensable features

Feature name	Description	VAS	AWDS	AMD
`VAS_Web`	VAS – Web personality	YES	—	YES

Feature name	Description	VAS	AWDS	AMD
VAS_Enterprise	VAS – Enterprise personality	YES	—	YES
VAS_EUE	VAS – End-User Experience	YES	YES	YES
AMD_VFC	License to connect AMDs	YES	YES	—
AM_OracleApplications	Enables “packaged” definitions for Oracle Applications	YES	YES	YES
AM_Siebel	Enables “packaged” definitions for Siebel CRM suite	YES	YES	YES
AM_SSL_Decryption	SSL support	YES	YES	YES
AMD_ClientVantage [2]	Enables ClientVantage integration.	YES	YES	YES
AWDS	AWDS	—	YES	YES
VAS_Citrix	Thin Client (Citrix Presentation Server and Windows Terminal Server) analysis	YES	—	YES
VAS_DB_DRDA	DRDA (DB2) analysis	YES	—	YES
VAS_DB_Informix	Informix Database analysis	YES	—	YES
VAS_DB_Oracle	Oracle Database analysis	YES	—	YES
VAS_DB_TDS	TDS (Sybase and MS SQL) analysis	YES	—	YES
VAS_DNS	DNS analysis	YES	—	YES
VAS_Exchange	MS Exchange analysis	YES	—	YES
VAS_FIX	FIX transaction analysis	YES	—	YES
VAS_Mail	SMTP analysis	YES	—	YES
VAS_MQ	IBM MQ analysis	YES	—	YES
VAS_OracleForms	Oracle Forms analysis	YES	—	YES
VAS_SAP	SAP GUI monitoring	YES	YES	YES
VAS_Tuxedo	Tuxedo/Jolt analysis	YES	—	YES
VAS_VPN	VPN support	YES	—	YES
VAS_XML	XML and SOAP transaction analysis, including XML over MQ	YES	YES	YES

[2] This feature is licensed on the report server, but the feature-specific functionality is enabled on the AMD.

NOTE

- If you purchased `VAS_Enterprise` and used the HTTP analysis in the past, after upgrade to the release 11.1 you need to purchase the `VAS_Web` feature to continue the HTTP analysis. This feature has been removed from the `VAS_Enterprise` in version 11.0.1.
- VAS can read data from AMDs even if you do not have the `VAS_Web` or `VAS_Enterprise` features installed. In such cases, your setup will be able to monitor transactions only.

APPENDIX A

Protocols Supported by AWDS

Table 5. Supported protocols in this release

Analyzer	Protocol	Version	Limitations / example application
HTTP	HTTP	1.0, 1.1 (RFC 2616)	Advanced analysis for GET/POST methods. For all other methods, including WebDAV, every hit is reported separately. No pipelining.
Oracle Applications over HTTP[3]	HTTP	1.1, 1.0 (RFC 2616)	Oracle E-Business Suite 11i Oracle E-Business Suite 12
Oracle Applications over HTTPS[3]	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	
Oracle Forms (over HTTP) Oracle Forms (over TCP) Oracle Forms (over SSL) Oracle Forms (over HTTPS)	Oracle Forms	6i, 10.1	Oracle Forms 6i Oracle Application Server 9i, 10i, 10g R2 Transactions not supported.

[3] Monitoring applications using HTTP protocol may register excessive traffic. For more information, see *Supported Packaged Applications* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

Analyzer	Protocol	Version	Limitations / example application
SAP GUI	SAP GUI protocol (DIAG)	6.40, 7.10	No errors detection. SAP GUI for Java 7.10rev8, Windows SAP GUI v.7.10, SAP GUI Console
Siebel over HTTP[4] Siebel over HTTPS[4]	HTTP	1.1, 1.0 (RFC 2616)	Siebel CRM 7.8.2.0
Siebel over HTTPS[4]	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	
SSL (with decryption)	HTTPS	HTTP 1.1 encapsulated in SSL, SSL 3.0, TLS1.0 (RFC 2246)	56-bit DES is not supported. Only RSA Key Exchange Algorithm supported. GET/POST methods only; no pipelining.

[4] A special parameter configuration is recommended for analyzing Siebel applications. For more information, see *Global Settings for Recognition and Parsing of URLs* in the *ClientVantage Agentless Monitoring – System Administration Guide*.

APPENDIX B

Determining Microsoft SQL Server Named Instance Port Number

When you perform a named instance installation of Microsoft SQL Server, the port is chosen dynamically at the time of installation. You can determine your SQL Server named instance in several ways; using **SQL Server Configuration Manager** is the most appropriate one.

Prerequisites

You need physical or remote access to the operating system where Microsoft SQL Server instance is installed.

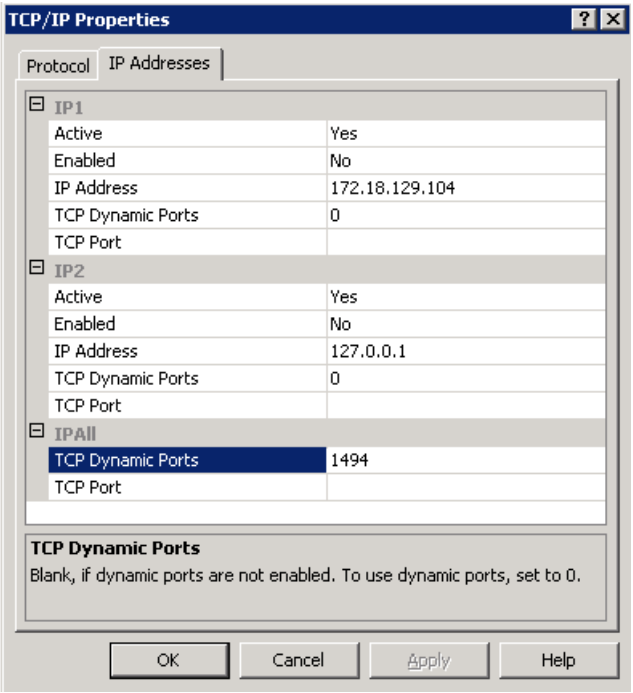
If enabled, the default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances of the Database Engine are configured for dynamic ports. This means they select an available port when the SQL Server service is started.

In general, you should refer to your SQL Server named instances by name so that you always address the valid instance (the port number may change but the instance name does not). If, during installation of the report server, you are unable to use the instance name and are forced to give a port number, you can check its value:

1. Log into the system either remotely (via Remote Desktop, for example) or locally.
2. In Windows, go to **Programs** → **Microsoft SQL Server** ***<server_version>*** → **Configuration Tools** and choose **SQL Server Configuration Manager**.
3. Select **Protocols for** ***<instance name>*** and then double-click **TCP/IP** to inspect the instance TCP/IP settings.
4. In the **TCP/IP Properties** dialog box, on the **IP Addresses** tab, determine the currently assigned port number.

   If the **TCP Dynamic Ports** dialog box contains 0, this indicates that the Database Engine is listening on dynamic ports. The **IPAll** dialog contains the port number used by the SQL Server named instance you selected.

Figure 10. TCP/IP Properties for the SQL Server named instance



5. Click **Cancel** to close **TCP/IP Properties**.
6. *Optional:* Repeat steps Step 3 [p. 53]–Step 5 [p. 54] for each instance you need to verify.
7. *Optional:* You can validate port number discovery using **`netstat`** program.

   Connect to the Database Engine with **SQL Server Management Studio** from a remote machine. On the machine hosting SQL Server, issue the **`netstat`** command and inspect the **Local Address** and **Foreign Address** columns. Find a matching pair (or pairs) of addresses that represents your remote connection to the SQL Server. The **Local Address** column contains the port number associated with the local machine (separated by a colon from the IP address).

Index