Table of Contents

Using This Guide 9

Purpose and Intended Audience 9

How to Use This Guide 9

Conventions Used in This Guide 10

Typographical Conventions 10

Admonitions 10

About Ad-Aware Client Security 11

What Is Ad-Aware Client Security? 11

Architecture and Operation 11

Ad-Aware Management Server 11

Ad-Aware Client Products 13

Ad-Aware Management Agent 14

Ad-Aware Management Console 14

Ad-Aware Deployment Tool 15

Ad-Aware Update Server 15

Supported Ad-Aware Client Products 15

Workstation Client Products 15

Ad-Aware Business Client 15

Server Client Products 15

Ad-Aware Security for Mail Servers (Windows, UNIX) 16

Ad-Aware Security for Exchange 16

Ad-Aware Security for File Servers (Windows) 16

Ad-Aware Security for Samba 16

Ad-Aware Security for SharePoint 16

Installation and Removal 17

System Requirements 17

Ad-Aware Management Server 17

Ad-Aware Management Agent 17

Ad-Aware Management Console 18

Ad-Aware Business Client 18

Ad-Aware Management Server Installed together with Ad-Aware Business Client 19
Ad-Aware Update Server 19
Before You Start the Deployment 20
Ad-Aware Client Security Basics 20
Single or Multi-Server Deployment? 20
How You Deploy a Single-Server Configuration 21
How You Deploy a Multi-Server Configuration 22
Active Directory Networks 23
Integration of the Ad-Aware Solutions for Server Systems 23
Integrating Ad-Aware Antivirus for Mac into the Centralized Reporting Platform 23
Installing Ad-Aware Management Server 24
Choosing and Preparing a Computer for Installation 24
Default Installation 25
Custom Installation (With Screenshots) 26
Installing a Slave or Master Server 38
Adding Support for Unix-based Server Security Solutions 39
Installing Components Separately 40
Installing Client Products 41
Step 1 - Prepare Computers for Deployment 41
Step 2 - Define Managed Computers 42
Step 3 - Deploy Client Products 44
Step 4 - Deploying on Offline Computers 45
Client Deployment Tools 45
Credentials Manager 46
Retry Deployment 49
Network Builder 50
Deployment Tool 56
Automatic Deployment 74
View Deployment Status 79
Upgrading 79
Considerations When Upgrading 80
Upgrading Ad-Aware Management Server 80
Upgrading Clients 81

Installation Changes 81
Changing Agent Synchronization Interval 81
Migrating Ad-Aware Management Server to another Computer 82
Migrating to a Multi-Server Configuration 84
Redirecting Clients to another Server 85
Modifying Ad-Aware Management Server Installation 86
Repairing Ad-Aware Management Server 87
Removal 87
Instructions for Complete Removal 88
Removing Clients 88
Removing Ad-Aware Management Server 90
Configuration and Management 91
Getting Started 91
Opening Management Console 91
Connecting to Ad-Aware Management Server 91
User Interface Overview 93
Changing Logon Password 96
Changing SQL Connection Password 97
Registration 98
Purchasing License Keys 98
Registering Ad-Aware Management Server 98
Configuring Proxy Settings 99
Checking the Registration Status 100
Extending or Renewing Your License 101
Registration in Master/Slave Configurations 102
The Management Dashboard 102
Monitoring Modules 102
Fixing Issues 104
Important Links 104
Configuring the Dashboard 105
Configuring E-mail Notifications 105
Computers Directory 107
Managed Computers 108

Unmanaged Computers....115
Excluded Computers....120
Policies....123
Creating New Policies....123
Current Policies....126
Exporting and Importing Policies....129
Network Tasks....135
Creating New Network Tasks....136
Current Network Tasks....138
Examples of Using Tasks....142
Network Audit....152
Configuring Network Audit....153
Creating New Network Audit Reports....156
Scheduled Network Audit Reports....158
Reporting Center....159
Creating Reports....159
Viewing and Saving Reports....161
Scheduled Reports....163
Examining the Server Activity Log....164
Setting Verbosity Level....166
Sorting Events....166
Deleting Records....166
Backup/Restore Server Configuration Tool....166
Backing Up Ad-Aware Management Server Configuration....167
Restoring Ad-Aware Management Server Configuration....170
Master-Slave Configurations....173
Master-Slave Configuration Overview....173
Feature Availability in Master Servers....174
Registering a Stand-Alone Server to a Master Server....174
Unregistering from Master Server....174
License Management....175
Tree Menu on Master Servers....175
Master/Virtual Policies....176

Master/Virtual Tasks....177
Master Reporting Center....177
Master Activity Log....177
Policy Templates....178
Ad-Aware Management Server Templates....178
Ad-Aware Management Agent Settings....178
Ad-Aware Management Agent Connection....179
Ad-Aware Business Client Templates....179
Update Request....180
Update Settings....182
Scan Policy....183
Antivirus Settings....187
Firewall Settings....192
Privacy Control....195
Anti-spam Settings....201
User Control....204
Exclusions....208
Device Detection....214
Select Main Active Modules....217
Ad-Aware Security for SharePoint Templates....218
Antivirus Settings....219
General Settings....223
Get Settings....226
Install Product Update....227
Rollback....227
Scanning Scheduled....227
Update Request....231
Update Settings....231
Ad-Aware Security for Mail Servers Templates....233
Anti-spam Filtering Settings/Rules....234
Update Request....237
Update Settings....237
Ad-Aware Security for File Servers Templates....240

Antivirus Settings 240

General Settings....245

Install Product Update 249

Rollback Product Update 249

Scan Exceptions Settings 250

Scanning Scheduled 250

Update Request 255

Update Settings 255

Ad-Aware Security for Exchange Templates 257

Anti-spam Filtering Settings/Rules 258

Antivirus Rules 264

Antivirus Settings 268

Attachment Filtering Rules 271

Content Filtering Rules 276

General Settings....281

Get Settings 285

Install Product Update 285

Rollback Product Update 285

Scanning Scheduled 286

SMTP Groups 287

Update Request 288

Update Settings 288

Ad-Aware Security for Mail Servers (Unices) Templates....290

File Logging Policy....291

Mail Alerts Policy 292

Mail Settings Policy....292

SMTP Protocol Policy....297

Update Settings Policy....298

Core Modules 299

Ad-Aware Security for Samba Templates....300

File Logging Policy....300

Mail Alerts Policy 301

Samba Protocol Policy 302

Update Settings Policy ... 303

Core Modules ... 304

Ad-Aware Update Server ... 305

What Is Ad-Aware Update Server? ... 305

Configuration and Management ... 306

Accessing Management Panel ... 306

What You Have to Do After Installation ... 307

Managing Client Products and Downloaded Updates ... 307

Configuring Settings ... 309

Changing Login Password ... 311

Cascading Configuration ... 311

Getting Help ... 312

Support ... 312

Ad-Aware Support ... 313

Ad-Aware Support Tool ... 313

Contact Information ... 316

Appendices ... 316

Available Network Tasks ... 316

Desktop Management ... 317

Processes ... 318

Files and Folders ... 318

Disk and File Systems ... 318

Computer Hardware ... 319

Operating Systems ... 320

Accounts and Domains ... 321

Computer Software ... 321

Networking ... 321

Services ... 321

WMI Service ... 322

Available Report Templates ... 322

Common Reports for Windows Products ... 322

Global Reports ... 323

Ad-Aware Management Server Reports ... 324

Ad-Aware Business Client Reports 324

Ad-Aware Antivirus for Mac Reports 326

Ad-Aware Security for File Servers Reports 326

Ad-Aware Security for Mail Servers Reports 327

Ad-Aware Security for Exchange Reports 327

Ad-Aware Security for SharePoint Reports 328

Ad-Aware Security for Samba Reports 328

Ad-Aware Security for Mail Servers (Unices) Reports 328

Default Communication Ports 329

Application Files 329

Using This Guide

Purpose and Intended Audience

This documentation is intended for all **Ad-Aware Management Server v3.5** users. The information presented herein should be easy to understand by anyone who has basic computer and networking knowledge.

This documentation shows you how Ad-Aware Management Server works, how to install it, how to use it to remotely deploy and manage the Ad-Aware protection in your network. You will learn how to get the best from Ad-Aware Management Server and the Ad-Aware business solutions.

We wish you a pleasant and useful lecture.

How to Use This Guide

This guide is organized into several major parts, making it easy to find the information you need.

About Ad-Aware Client Security

Learn about Ad-Aware Client Security, Ad-Aware Management Server and the Ad-Aware business security solutions that can be included into the centralized management platform. You are presented with basic information that provides a necessary starting point in working with Ad-Aware management Server.

Installation and Removal

This part contains everything there is to know on installing Ad-Aware Management Server and its clients. Starting with the prerequisites for a successful installation, you are guided through the whole installation process. If an older version of Ad-Aware Management Server is already installed in your network, Upgrading will show you how you can easily upgrade it to the latest version. You can also find information about various post-installation changes or how to remove the installation.

Configuration and Management

This part shows you how to use Ad-Aware Management Server and how to configure and manage network protection. Get familiar with the user interface, find out how to easily monitor the network protection status and take corrective actions, how to organize the network computers, how to run configuration policies and network management tasks, how to create network security status or audit reports.

Policy Templates

Every policy template explained in detail. Refer to this part when you cannot figure out what a specific policy setting does.

Ad-Aware Update Server

Find out how to use Ad-Aware Update Server to set up and manage a local update server for Ad-Aware updates.

Getting Help

Where to look and where to ask for help if something unexpected appears.

Appendices

Appendices provide additional information on particular topics. You can find out about the available network management tasks and report templates, as well as other useful information.

Conventions Used in This Guide

Typographical Conventions

Several text styles are used in the guide for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
Sample syntax	Syntax samples are printed in monospaced characters.
http:www.lavasoft.com	The URL link is pointing to some external location on http or ftp servers.
Filename	Files and directories are printed using monospaced font.
Option	All the product options are printed using **bold** characters.
Keyword	Important keywords or phrases are highlighted using **bold** characters.
Sample code listing	The code listing is printed with monospaced characters.

Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

Note
The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.

Important
This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

Warning
This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

About Ad-Aware Client Security

What Is Ad-Aware Client Security?

Ad-Aware Client Security is a robust and easy-to-use business security and management solution, which delivers superior proactive protection from viruses, spyware, rootkits, spam, phishing and other malware.

Ad-Aware Client Security enhances business productivity and reduces management and malware-related costs by enabling the centralized administration, protection and control of workstations inside companies' networks.

Architecture and Operation

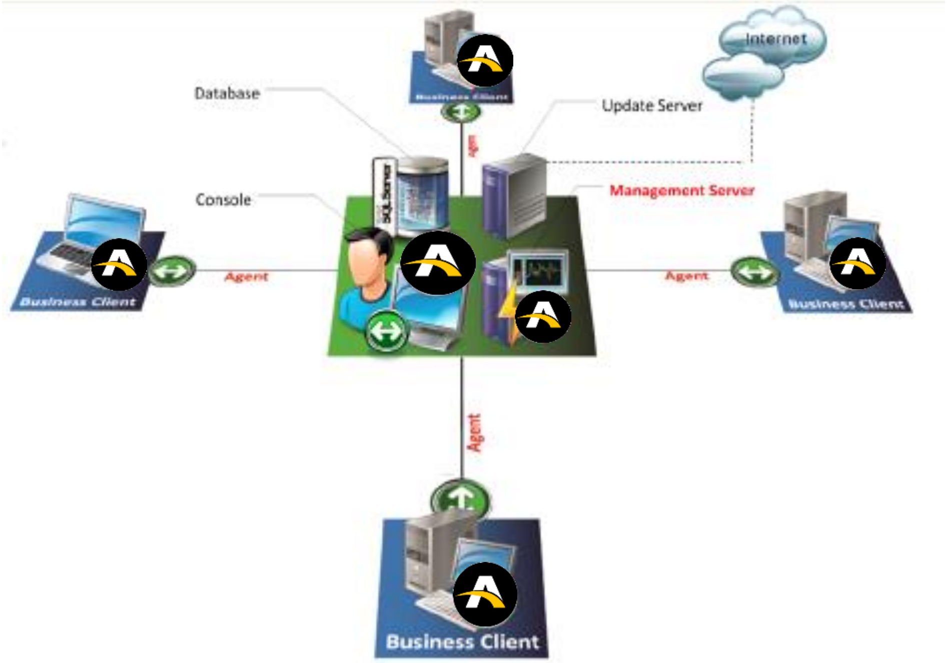
Ad-Aware Client Security includes the following components:

- Ad-Aware Management Server
- Ad-Aware client products
- Ad-Aware Management Agent
- Ad-Aware Management Console
- Ad-Aware Deployment Tool
- Ad-Aware Update Server

Ad-Aware Management Server

Ad-Aware Management Server is the main component of Ad-Aware Client Security. Its purpose is to manage all Ad-Aware security solutions inside a network based on customizable security policies.

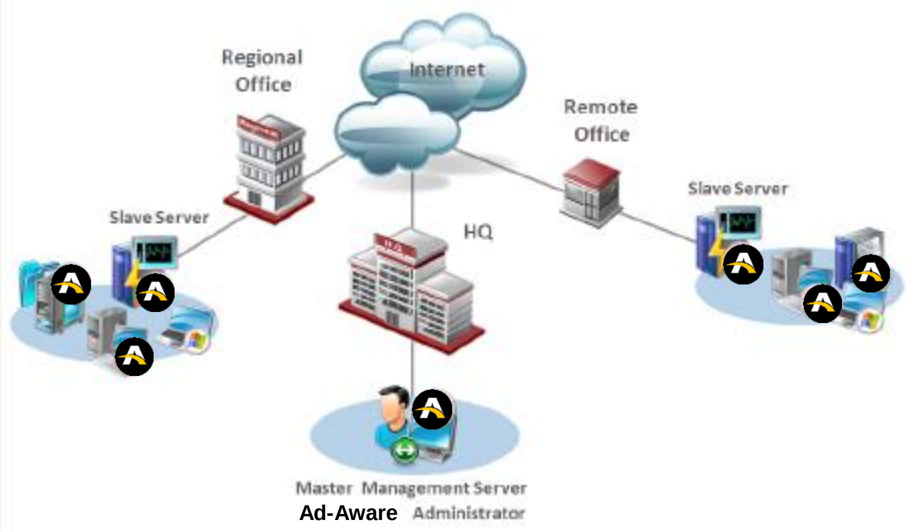
Using Ad-Aware Management Server, you can remotely install and manage Ad-Aware client products.



Remotely Install and Manage Ad-Aware Client Products

The "brain" of the product. The policies received from the user through the management console are forwarded to the workstations in order to be executed, while the information received from the workstations is processed by Ad-Aware Management Server. The information is then forwarded to the management console where it can be viewed and interpreted by the administrator. Ad-Aware Management Server can be dynamically extended to perform various other security-related policies that users may need.

Standalone or master-slave configuration. Ad-Aware Management Server can be deployed either as a stand-alone security management solution or in a master-slave architecture.



Standalone or Master-Slave Architecture

- In a stand-alone configuration, Ad-Aware Management Server manages the security of and centralizes security information about client computers.
- In a master-slave architecture, a specific instance of Ad-Aware Management Server (the master server) manages other instances of Ad-Aware Management Server (the slave servers).
    - As slave, Ad-Aware Management Server acts as stand-alone and also sends centralized information about its managed computers to the master.
    - As master, Ad-Aware Management Server does not have its own managed computers, but only those of its slave Ad-Aware Management Server. Its role is to obtain centralized results regarding the security of all computers in the organization.

Connected to Database. Ad-Aware Management Server will stay permanently connected to a database (for example MS SQL Server Database) that stores information about all product configuration files. In this way, Ad-Aware Management Server can manage a huge amount of information in the shortest possible time.

Password-protected. By default, Ad-Aware Management Server is password-protected. The default password is: admin. The password can be changed in the Ad-Aware Management Console.

Note

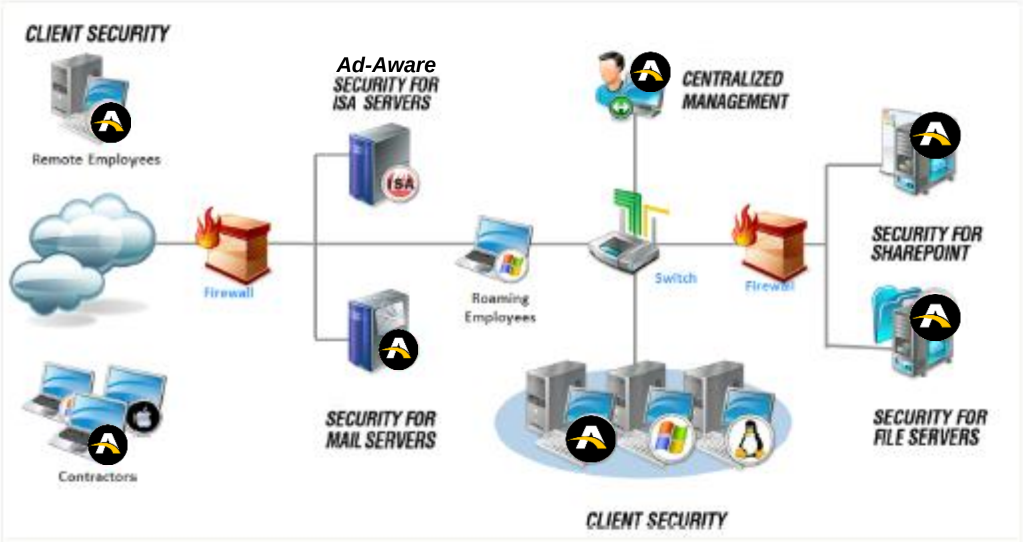
To manage the Ad-Aware clients from a workstation other than Ad-Aware Management Server, you must perform a custom installation of Ad-Aware Management Server on the respective workstation. For more information, please refer to Installing Ad-Aware Management Console on Administrator's Computer.

Ad-Aware Client Products

Ad-Aware client product is a product that Ad-Aware Management Server manages remotely, through policies.

Ad-Aware Client Security smoothly integrates with and manages:

- **Workstation Client Products**
  - Ad-Aware Business Client
- **Server Client Products (Gateway Level)**
  - Ad-Aware Security for Mail Servers (Windows, UNIX)
  - Ad-Aware Security for Exchange
- **Server Client Products (File Server Level)**
  - Ad-Aware Security for File Servers (Windows)
  - Ad-Aware Security for Samba
  - Ad-Aware Security for SharePoint



Ad-Aware Client Products

Ad-Aware Management Agent

Ad-Aware Management Agent is the component deployed on each workstation that you want to be managed by Ad-Aware Management Server. It is used to ensure communication between Ad-Aware Management Server and the Ad-Aware client products installed on a specific workstation.

It fulfills three main functions:

- Queries Ad-Aware Management Server to learn the security policies that need to be applied to the local workstation.
- Applies the security policies received from Ad-Aware Management Server.
- Sends the results of the applied policies to Ad-Aware Management Server.

Ad-Aware Management Console

Ad-Aware Management Console represents the graphical user interface (GUI), created to allow the administrator to interact with Ad-Aware Management Server.

By using the management console you can:

- Visualize the entire network (managed computers, computers that are not currently managed by Ad-Aware Management Server, computers excluded from management).
- Remotely deploy Ad-Aware Management Agent on detected network computers or on computers from Active Directory.
- Remotely deploy Ad-Aware client products on managed computers.
- Set Ad-Aware Management Server to automatically deploy Ad-Aware Management Agent and Ad-Aware Business Client on newly detected computers.
- Find out detailed information about a managed computer.
- Assign policies to managed computers or to computers from Active Directory in order to configure and even to install Ad-Aware client products.
- Run management tasks on managed computers in order to remotely perform administrative tasks.
- Check the results of the assigned policies and network management tasks.
- Configure Ad-Aware Management Server and monitor its activity.
- Obtain centralized easy-to-read reports regarding the managed computers.
- Remotely remove client products installed on managed computers.

Note

To install only the management console on a workstation you must perform a custom installation of Ad-Aware Management Server. For more information, please refer to Installing Ad-Aware Management Console on Administrator's Computer.

Ad-Aware Deployment Tool

Ad-Aware Deployment Tool is an independent component that helps you automatically install, remove or repair Ad-Aware products on remote network computers. This tool also enables you to create unattended installation packages for use on offline computers (or when remote installation fails).

> **Note**
>
> You can put it on a CD, on a shared folder, send it by e-mail or use a logon script in order to install it on workstations.

Ad-Aware Update Server

Ad-Aware Update Server is an independent component that allows you to set up an Ad-Aware update location within the local network. In this way, you can reduce Internet traffic because only one computer will connect to the Internet to download updates while the others will update from this local mirror. Moreover, updates will be performed faster and even on the computers that are not connected to the Internet.

Supported Ad-Aware Client Products

Ad-Aware Management Server smoothly integrates with and manages both Ad-Aware workstation and server security solutions.

Workstation Client Products

- Ad-Aware Business Client

Ad-Aware Business Client

Ad-Aware Business Client integrates antivirus, firewall, anti-spam and antispyware modules into one comprehensive workstation security package, tailored to meet the needs of corporate computer users worldwide.

Server Client Products

- Ad-Aware Security for Mail Servers (Windows, UNIX)
- Ad-Aware Security for Exchange
- Ad-Aware Security for File Servers (Windows)
- Ad-Aware Security for Samba
- Ad-Aware Security for SharePoint

Ad-Aware Security for Mail Servers (Windows, UNIX)

Ad-Aware Security for Mail Servers protects Windows or UNIX-based mail servers for known and unknown security threats with award winning proactive antivirus, antispyware, anti-spam, anti-phishing, content and attachment filtering technologies. The solution secures organization's email services and provides increased productivity by blocking spam and providing common centralized management tools.

Ad-Aware Security for Exchange

Ad-Aware Security for Exchange safeguard's your organizations critical messaging services to protect against email-borne viruses, spyware and spam. Integrating seamlessly with Microsoft®Exchange Server, Ad-Aware Security for Exchange combines malware protection, anti-spam, anti-phishing and content filtering technologies to increase productivity and ensure the overall integrity of your email platforms.

Ad-Aware Security for File Servers (Windows)

Ad-Aware Security for File Servers provides optimized protection of both the server operating system and data file structure for critical back-end systems. Easy to install, configure and maintain via the centralized management console, Ad-Aware for File Servers protects against viruses, spyware and rootkits to minimize the impact of malware propagation throughout the network.

Ad-Aware Security for Samba

Ad-Aware Security for Samba enables organizations to deploy antivirus and antispyware protection for their Samba network shares running on Linux, FreeBSD and Solaris systems. Deployed and maintained centrally within the network, Security for Samba scans cross-platform data structures and file stores for malware, keeping network users safe from virus infection.

Ad-Aware Security for SharePoint

Ad-Aware Security for SharePoint provides proactive protection of SQL document repositories against known and unknown viruses, spyware, Trojans and root kits. Real-time, optimized session-based scanning of uploaded, downloaded or accessed files helps to prevent Microsoft SharePoint deployments from storing and sharing of infected files within the network.

Installation and Removal

System Requirements

To fulfill its main purpose - centralized administration of all Ad-Aware security solutions in a network environment - Ad-Aware Client Security requires a TCP/IP-based computer network.

Besides this primary requirement, specific system requirements must be met in order for Ad-Aware Management Server and its client products to operate properly.

Ad-Aware Management Server

Before installing Ad-Aware Management Server, make sure that the following system requirements are met:

- **Processor**: Intel® Pentium compatible 1.6 GHz (2 GHz multi-core recommended)
- **RAM memory**:
  - 512 MB (1 GB recommended) for Windows 2000
  - 756 MB (1.5 GB recommended) for Windows XP and Windows 2003
  - 1.5 GB (3 GB recommended) for Windows Vista, Windows 2008, Windows 7
- **Hard disk space**:
  - 1.5 GB (2.5 GB recommended)
  - For installation or upgrade 3 GB are needed
- **Operating system**:
  - Windows 2000 Professional with Service Pack 4 and Update Rollup 1 Version 2
  - Windows 2000 Server with Service Pack 4 and Update Rollup 1 Version 2
  - Windows Server 2003 with Service Pack 2
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Small Business Server 2008
  - Windows XP with Service Pack 2 or Service Pack 3
  - Windows Vista with Service Pack 1 or Service Pack 2
  - Windows 7
- **Database**:
  - Microsoft SQL Server 2005 / SQL Server 2005 Express Edition (included in the installation kit)
  - Microsoft SQL Server 2008

Ad-Aware Management Agent

Before deploying Ad-Aware Management Agent on a remote computer, make sure that the following system requirements are met:

- **Processor**: Intel® Pentium compatible processor 1 GHz (1.6 GHz recommended)

- **RAM memory**:
  - 512 MB for Windows 2000, Windows XP, Windows 2003
  - 1 GB (1.5 GB recommended) for Windows Vista, Windows 2008, Windows 7
- **Hard disk space**: 100 MB (200 MB recommended)
- **Operating system**:
  - Windows 2000 Professional with Service Pack 4 and Update Rollup 1 Version 2
  - Windows 2000 Server with Service Pack 4
  - Windows XP with Service Pack 2 or Service Pack 3
  - Windows Home Server
  - Windows Server 2003 with Service Pack 2
  - Windows Vista with Service Pack 1 or Service Pack 2
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Small Business Server 2008
  - Windows 7
  - Linux 2.4.x or 2.6.x with glibc 2.3.1 or newer and libstdc++5 from gcc 3.2.2 or newer

Ad-Aware Management Console

Before installing Ad-Aware Management Console, make sure that the following system requirements are met:

- **Processor**: Intel® Pentium compatible processor 1 GHz (1.6 GHz recommended)
- **RAM memory**:
  - 512 MB (1 GB recommended) for Windows XP, Windows 2000, Windows 2003
  - 1.5 GB (2 GB recommended) for Windows Vista, Windows 2008, Windows 7
- **Hard disk space**:
  - 500 MB (1 GB recommended)
  - For installation or upgrade 2 GB are needed
- **Operating system**:
  - Windows 2000 Professional with Service Pack 4 and Update Rollup 1 Version 2
  - Windows 2000 Server with Service Pack 4 and Update Rollup 1 Version 2
  - Windows Server 2003 with Service Pack 2
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Small Business Server 2008
  - Windows XP with Service Pack 2 or Service Pack 3
  - Windows Vista with Service Pack 1 or Service Pack 2
  - Windows 7
- **Software**: Internet Explorer 6.0(+); Microsoft Management Console (MMC) 3.0(+)
- **Minimum resolution**: 1024x768 / 16 bit

Ad-Aware Business Client

Before deploying this client product, make sure that the following system requirements are met:

- **Processor:**
  - Intel® Pentium compatible processor
  - 500 MHz (800 MHz recommended) for Windows 2000
  - 800 MHz (1 GHz recommended) for Windows XP
  - 1 GHz (dual-core recommended) for Windows Vista, Windows 7
- **RAM memory:**
  - 256 MB (512 MB recommended) for Windows 2000
  - 512 MB (1 GB recommended) for Windows XP
  - 1 GB RAM (1.5 GB recommended) for Window Vista, Windows 7
- **Minimum hard disk space: 1 GB**
- **Operating system:**
  - Windows 2000 Professional with Service Pack 4 and Update Rollup 1 Version 2
  - Windows XP with Service Pack 2 or Service Pack 3
  - Windows Home Server
  - Windows Vista with Service Pack 1 or Service Pack 2
  - Windows 7

Ad-Aware Management Server Installed together with Ad-Aware Business Client

To install Ad-Aware Management Server together with Ad-Aware Business Client, make sure that the following system requirements are met:

- **Processor**: Intel® Pentium compatible 1.6 GHz (2 GHz multi-core recommended)
- **RAM memory**:
  - 756 MB (1 GB recommended) for Windows 2000 and Windows XP
  - 1 GB (3 GB recommended) for Windows Vista and Windows 7
- **Hard disk space**:
  - 1.5 GB (2 GB recommended)
  - For installation or upgrade 3 GB are needed
- **Operating system**:
  - Windows 2000 Professional with Service Pack 4 and Update Rollup 1 Version 2
  - Windows XP with Service Pack 2 or Service Pack 3
  - Windows Vista with Service Pack 1 or Service Pack 2
  - Windows 7

Ad-Aware Update Server

You can install Ad-Aware Update Server on any computer running Windows 2000 or a newer Windows operating system.

Supported browsers (for configuration and management):

- Internet Explorer 6 (+) for Windows 2000
- Internet Explorer 7 (+) for Windows operating systems newer than Windows 2000
- Mozilla Firefox 2.0 (+)

Before You Start the Deployment

Ad-Aware Client Security Basics

Ad-Aware Client Security is a network security solution aimed at all types of businesses. Four main components are of interest for the deployment:

- Ad-Aware Management Server, which allows you to centrally manage the Ad-Aware security solutions in your network.
- Ad-Aware Management Console, which is the graphical interface of Ad-Aware Management Server.
- Ad-Aware Management Agent, the local management component installed on all managed computers, which ensures communication between the managed computers and Ad-Aware Management Server.
- Ad-Aware Business Client, which protects workstations against a wide range of security threats. If you also want to protect servers and manage their protection, you must add support for the Ad-Aware server security solutions.

Ad-Aware Management Server communicates, through specific ports, with the Ad-Aware Management Agent components, Ad-Aware Management Console and with other Ad-Aware Management Server products installed in the network. These ports must not be used by any other application installed in the network. Access to them must also be allowed by the local firewalls.

These are the default communication ports:

- 7072 - The communication port between Ad-Aware Management Server and Ad-Aware Management Agent. This port must be allowed on all network computers.
- 7071 - The communication port between Ad-Aware Management Server and Ad-Aware Management Console. This port must be allowed on all Ad-Aware Management Server computers and on all computers on which you install Ad-Aware Management Console.
- 7073 - The communication port between a master and a slave instance of Ad-Aware Management Server. This port must be allowed on all Ad-Aware Management Server computers.

The default port on which Ad-Aware Update Server accepts connections from clients is 7074. The Ad-Aware Update Server port must not be used by other applications installed on the system.

Note

For detailed information on the components and operation of Ad-Aware Client Security, please refer to Architecture and Operation.

Single or Multi-Server Deployment?

The answer to this question depends on the size and complexity of your network. You must consider the following:

- A standard, single-server deployment of Ad-Aware Management Server can support up to 1,000 client computers, all managed by and reporting to the single server.

- In master-slave configuration, it is recommended to have a maximum of 3,500 clients by using up to 7 slave servers reporting to a master server, with each slave managing up to 500 computers.
- In very large networks (more than 3,500 computers), multiple master-slave deployments can be used to provide total coverage.

How You Deploy a Single-Server Configuration

These are the steps you must follow to successfully deploy Ad-Aware Client Security:

1. **Install the central management component (Ad-Aware Management Server)**. Install Ad-Aware Management Server on the desired computer using the installation CD/DVD or the installation file downloaded from the Ad-Aware website. To install the support files for Ad-Aware Windows server solutions, you must choose the custom setup type and, afterwards, select to install the corresponding add-on. For detailed information, please refer to Installing Ad-Aware Management Server.

After you install Ad-Aware Management Server, you will be able to deploy and manage workstation protection from the management console.

2. **Prerequisites**. Ensure that your network satisfies all prerequisites. This is important because if your network fails to meet some of the prerequisites, installation may fail (for example, you may not succeed in installing the Client components on some computers). For detailed information on prerequisites, please refer to Prepare Computers for Deployment.
3. **Install the local management component (Ad-Aware Management Agent)**. Deploy Ad-Aware Management Agent on workstations and servers. This is done from the management console. Ad-Aware Management Agent will handle the installation and management of the workstation security component on the workstation. For detailed information, please refer to Define Managed Computers.
4. **Install the workstation security component (Ad-Aware Business Client)**. Install the workstation security component on the client workstations. This is done from the management console. You just have to run an Ad- Aware Business Client policy on the workstations. For detailed information, please refer to Deploy Client Products.
5. **Extending protection and management to Windows servers**. To enable remote deployment and management of the Ad-Aware security solutions for Windows servers, you must install Ad-Aware Management Server together with the corresponding add-on available in the installation file. Once the add-on is installed, there are two ways to install and centrally manage the Ad-Aware security solutions for Windows servers:
   - On Windows servers with Ad-Aware Management Agent installed, you can remotely deploy the security solution using Ad-Aware Management Server. The deployment is similar to that of the workstation security component: from the management console, run a policy of the server security solution on the desired server.
   - Install the security solution on the Windows server using the Ad-Aware Security for Windows Servers installation file. If Ad-Aware Management Agent is already installed on the server, the server security solution immediately integrates with Ad-Aware Management Server. Otherwise, integration occurs as soon as you install Ad-Aware Management Agent on the server. This is useful if the Ad-Aware server security solutions are already installed on the servers.

6. **Extending protection and management to Unix-based servers**. To secure your organization's Unix-based servers with Ad-Aware solutions and to manage their protection using Ad-Aware Management Server, you must follow these steps:
   a) Install the Unix add-on on the Ad-Aware Management Server computer (either the 32-bit or the 64-bit version, depending on the computer platform).
   b) Install Ad-Aware Security for Mail Servers and Ad-Aware Security for Samba on your Unix-based servers, as needed. These security solutions cannot be remotely deployed, so you will have to install them manually.
   c) For each security solution installed, configure the integration with Ad-Aware Management Server.

For detailed information, please refer to Adding Support for Unix-based Server Security Solutions.

How You Deploy a Multi-Server Configuration

When deploying multiple instances of Ad-Aware Management Server, it is recommended to set them up in a master-slave configuration.

Ad-Aware Management Server provides great scalability through the master-slave configuration. The master-slave configuration is recommended to be used in two standard situations:

1. Your network consists of more than 1000 computers. This is the maximum number of computers that can be managed by an Ad-Aware Management Server instance. In this case, you divide the network into several sub networks and install an Ad-Aware management server for each sub network. These are called slave servers. An additional management server will be installed in order to manage all slave servers. This is the master server. A master server cannot manage client products on its own, but only the client products managed by the slave servers.
2. Several networks from different geographical areas must be managed. This is the typical case of businesses having offices in several cities or countries. In this case, you install a slave server in the network of each office. In the headquarter network, you install a slave server and a master server. The master server will manage all slave servers, including the slave server installed in the headquarter network.

Of course, a mix of these scenarios can be used. For example, the headquarter network from the second situation may be very large. In this case, you will deploy several slave servers in the headquarter network along with the master server.

The deployment of the slave servers is similar to that presented in How You Deploy a Single-Server Configuration. Repeat the respective procedure for each slave server. After you have deployed all slave servers, proceed to installing the master server. To install the master server, you must choose to perform a custom installation in the setup wizard. Once you have installed the master server, you must connect to each slave server and register it to the master server (right-click the server name in the tree menu and select Register to Master server).

Active Directory Networks

Ad-Aware Management Server integrates with Active Directory to leverage existing Windows domain structure and group policies. This makes client deployment considerably easier.

Integration with Active Directory is done through the Network Builder tool. This tool enables you to import an existing Active Directory structure (computers and groups) and deploy Ad-Aware Management Agent on all network computers. You can then assign appropriate security policies to each group.

You will consider Active Directory integration only after installing Ad-Aware Management Server (when you get to the client deployment stage). For more information, please refer to Installing Client Products.

Integration of the Ad-Aware Solutions for Server Systems

Ad-Aware Client Security is designed primarily for workstation protection and management. You can extend the Ad-Aware Management Server capabilities to include management of the Ad-Aware's server security solutions by installing add-ons. Two add-ons are available: one for the Ad-Aware Security for Windows Servers solutions and the other for Unix-based server solutions.

- The Ad-Aware Security for Windows Servers add-on is included directly in the Ad-Aware Management Server installation package. When you install Ad-Aware Management Server, you must choose the custom setup type in order to install the add-on. More information is provided in section Custom Installation (With Screenshots). To install the add-on later, you must modify the Ad-Aware Management Server installation. For more information, please refer to Modifying Ad-Aware Management Server Installation.

  Clients are installed the same way as the workstation clients or by deploying Ad-Aware Management Agent on computers on which Ad-Aware Security for Windows Servers solution is already installed. For more information, please refer to Installing Client Products.

- The add-on for Unix-based server solutions is distributed as a separate installation package. You can download it from the Ad-Aware Client Security download section (the download link is e-mailed to you after you fill in a request on the Ad-Aware website). The add-on can be installed at any time after installing Ad-Aware Management Server, without disturbing its operation. Find out how to install the add-on and clients in section Adding Support for Unix-based Server Security Solutions.

  Once the add-ons are installed, new categories of policies and reports will be available in the Ad-Aware Management Server console for the server security solutions. You can configure and manage these solutions the same way as the Windows workstation client (Ad-Aware Business Client).

Integrating Ad-Aware Antivirus for Mac into the Centralized Reporting Platform

For comprehensive information on the network security status, you can include your Mac computers into the centralized reporting platform of Ad-Aware Management Server.

All you have to do is install the business edition of Ad-Aware Antivirus for Mac on your Macs. The business edition includes a built-in agent that will report status information to Ad-Aware Management Server. The agent settings will be configured during installation.

To find out how to install the business edition of Ad-Aware Antivirus for Mac, please refer to its Administrator's Guide. Remote installation is possible using Apple Remote Desktop or a script.

An important thing to consider is that Ad-Aware Antivirus for Mac licenses are not managed by Ad-Aware Management Server. You need a separate license key to register your Ad-Aware Antivirus for Mac installations.

Installing Ad-Aware Management Server

In order to install Ad-Aware Management Server, you need a setup file or an installation CD containing the installation package.

You can download the setup file from the Ad-Aware website: http://www.bitdefender.com. Follow the links to download an evaluation version of Ad-Aware Client Security, the business security solution that integrates Ad-Aware Management Server. You will have to fill in a form and you will receive an e-mail at the address you have provided in this form. The e-mail contains a link to the download location.

Depending on the computer platform on which you install Ad-Aware Management Server, choose the 32-bit or the 64-bit version of the setup file. You must also specify if you want to manage Ad-Aware security solutions for Unix servers using Ad-Aware Management Server. To manage them, additional support files must be installed in Ad-Aware Management Server (you will be provided with an additional Server Add-on setup file).

Note
The add-on for Ad-Aware Security for Windows Servers is included in the Ad-Aware Management Server installation file.

The installation package contains the following components:

- Ad-Aware Management Server
- Ad-Aware Security for Windows Servers (Server Add-On)
- Ad-Aware Management Console
- Ad-Aware Update Server

Except for the Ad-Aware Security for Windows Servers add-on, all of these components are installed by default. If you want to install Ad-Aware Management Server together with the add-on, you must perform a custom installation.

Choosing and Preparing a Computer for Installation

You can install Ad-Aware Management Server on a dedicated computer or on one of your organization's servers. If you install Ad-Aware Management Server on a computer running a server operating system, you will have to protect that computer with a server security solution, such as Ad-Aware Security for File Servers. You will not be able to install Ad-Aware Business Client on such a computer.

Use these guidelines to choose and prepare a computer for installing Ad-Aware Management Server:

1. Make sure the computer meets the corresponding system requirements. System requirements can be found in chapter System Requirements.
2. It is recommended that the computers on which you install Ad-Aware Management Server have a static IP. Depending on whether the IP address changes or not in time, the management server identity must be configured differently when deploying Ad-Aware Management Agent. More information is provided in section Define Managed Computers.

3. **Recommendations for improved performance in large networks (with more than 500 computers).**

- For single-server deployments with more than 500 clients, it is recommended to use a more powerful system and Microsoft SQL Server's Standard or Enterprise Edition (especially if you plan to use the network audit feature intensively).
- For master-slave deployments with more than 1,000 clients, it is recommended to use a more powerful system and Microsoft SQL Server's Standard or Enterprise Edition for the master server.

Default Installation

The default installation installs a predefined configuration of Ad-Aware Management Server together with Ad-Aware Update Server. Choosing this option will install Ad-Aware Management Server as a single (stand-alone) server and an instance of Microsoft SQL Server 2005 Express Edition. The Ad-Aware Management Server components will be using the default communication ports (as displayed in the last window of the setup wizard).

⚠ **Important**

Support for the Ad-Aware Security for Windows Servers solutions is not included in the default installation. To remotely install and manage these solutions using Ad-Aware Management Server, you must perform a custom installation.

To perform a default installation:

1. Please note that you need at least 3 GB of free space on the system partition, or otherwise the installation will likely fail.
2. Locate the installation file on the computer and double-click it to start the installation wizard. If you have an installation CD/DVD insert it into the drive and follow the on-screen instructions to start installation.

   ❗ **Note**

   Before launching the setup wizard, Ad-Aware will check for newer versions of the installation package. If a newer version is available, you will be prompted to download it. Click **Yes** to download the newer version or **No** to continue installing the version then available in the setup file.
3. Click **Next**.
4. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.
5. Click **Default**.
6. **Configuration needed in rare situations**. If the default communication ports of the Ad-Aware Management Server components or of Ad-Aware Update Server are in use, you will be prompted to configure new ports. Find out more in Ad-Aware Client Security Basics. Configure requested ports and click **Next**.

Important

Please take the following into account:

- Provide port values between 1 and 65535.
- These ports must not be used by any other application installed in the network. Access to them must also be allowed by the local firewalls.
- Write down or keep a record of these port numbers. You will need them later.

7. Click **Install**.
8. Wait until the installation is completed and then click **Finish**.

Custom Installation (With Screenshots)

Custom installation is needed in particular situations or if you want to configure installation options in detail. Choose the custom installation if you require:

- Install Ad-Aware Management Server together with the add-on that provides support for remote deployment and management of the Ad-Aware security solutions for Windows servers. This add-on is not installed by default.
- Install only the management console on your administrative PC or laptop. In this way, you can remotely access Ad-Aware Management Server.
- Install Ad-Aware Management Server as a master or as a slave server in order to deploy a *master-slave architecture*.
- Configure specific communication ports for the Ad-Aware Management Server components.
- Use an existing database to manage the data needed by Ad-Aware Management Server. Supported databases: Microsoft SQL Server 2005 / SQL Server 2005 Express Edition / Microsoft SQL Server 2008.
- Install Ad-Aware Update Server separately, on a dedicated computer.

To perform a custom installation:

1. Please note that you need at least 3 GB of free space on the system partition, or otherwise the installation will likely fail.
2. Locate the installation file on the computer and double-click it to start the installation wizard. If you have an installation CD/DVD insert it into the drive and follow the on-screen instructions to start installation.

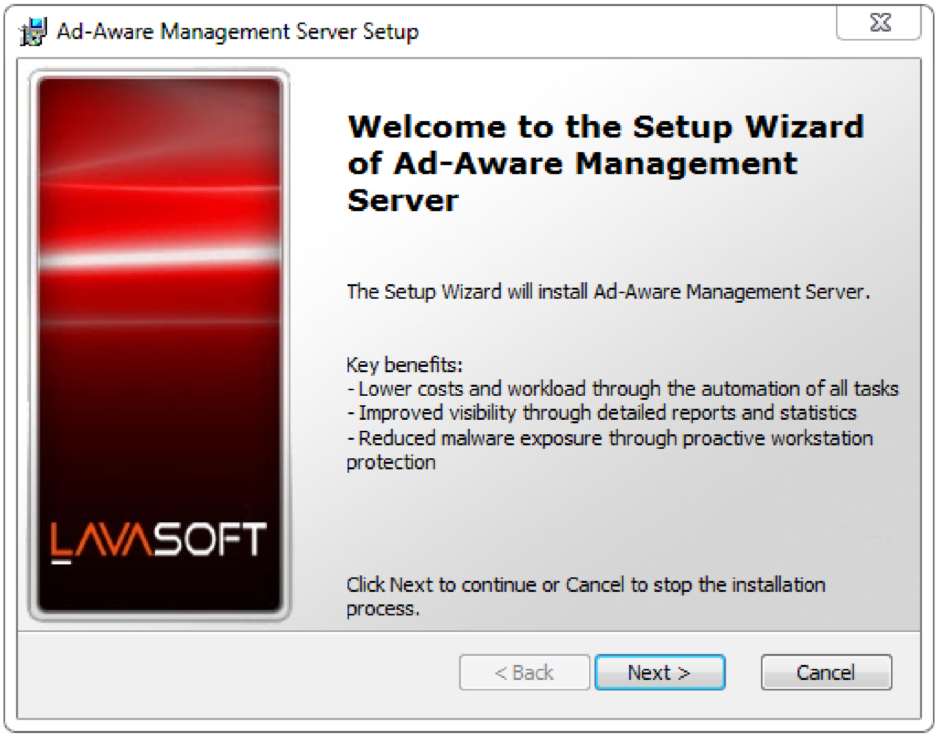
Note

Before launching the setup wizard, Ad-Aware will check for newer versions of the installation package. If a newer version is available, you will be prompted to download it. Click **Yes** to download the newer version or **No** to continue installing the version then available in the setup file.

3. Follow the wizard steps. Detailed instructions with screenshots are provided hereinafter. For quick instructions on the custom installation of particular package components, please refer to Installing Components Separately.

Step 1 - Welcome Window

This welcome window describes the main benefits of using Ad-Aware Management Server.



Welcome to the Setup Wizard of Ad-Aware Management Server

The Setup Wizard will install Ad-Aware Management Server.

Key benefits:
- Lower costs and workload through the automation of all tasks
- Improved visibility through detailed reports and statistics
- Reduced malware exposure through proactive workstation protection

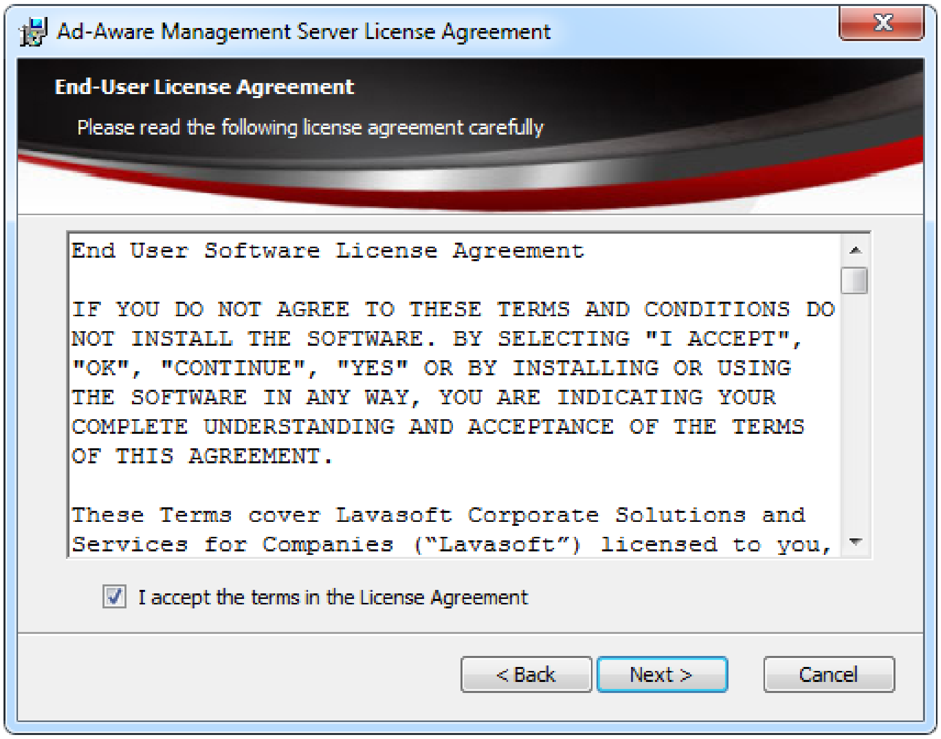
Click Next to continue or Cancel to stop the installation process.

Welcome Window

Click **Next**. A new window will appear.

Step 2 - Read the License Agreement

This window provides you with the License Agreement accompanying Ad-Aware Management Server.



End-User License Agreement

Please read the following license agreement carefully

```
End User Software License Agreement

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO
NOT INSTALL THE SOFTWARE. BY SELECTING "I ACCEPT",
"OK", "CONTINUE", "YES" OR BY INSTALLING OR USING
THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR
COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS
OF THIS AGREEMENT.

These Terms cover Lavasoft Corporate Solutions and
Services for Companies ("Lavasoft") licensed to you,
```

☑ I accept the terms in the License Agreement

License Agreement

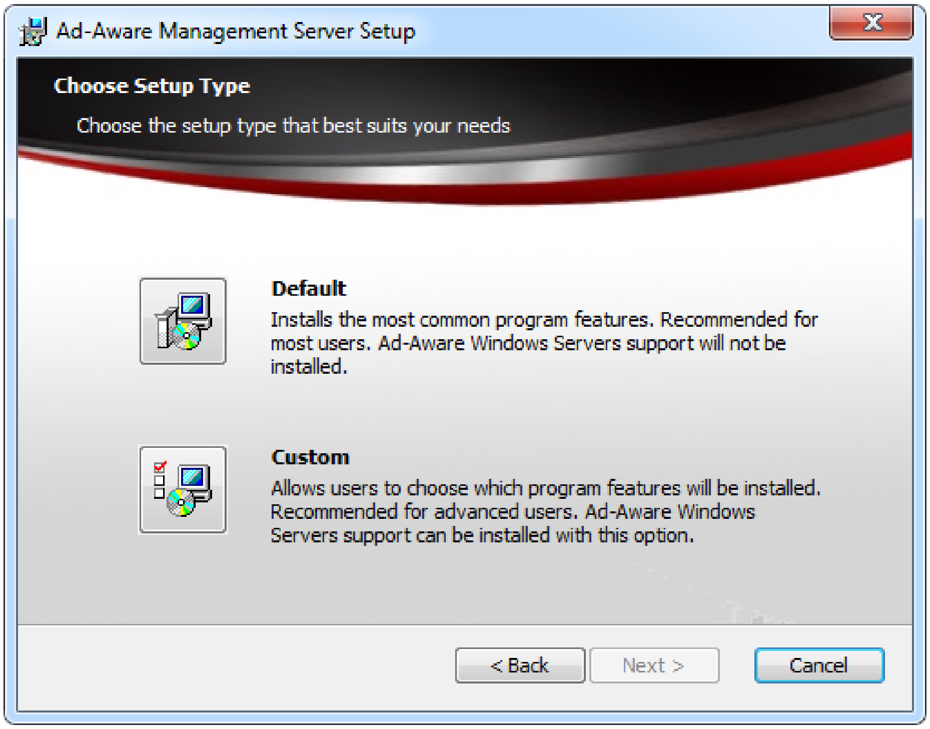
Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**. A new window will appear.

Note

If you do not agree to these terms click **Cancel**. The installation process will be abandoned and you will exit setup.

Step 3 - Choose Installation Type

This window allows you to choose the type of installation to be performed.



Ad-Aware Management Server Setup

Choose Setup Type

Choose the setup type that best suits your needs

Default

Installs the most common program features. Recommended for most users. Ad-Aware Windows Servers support will not be installed.

Custom

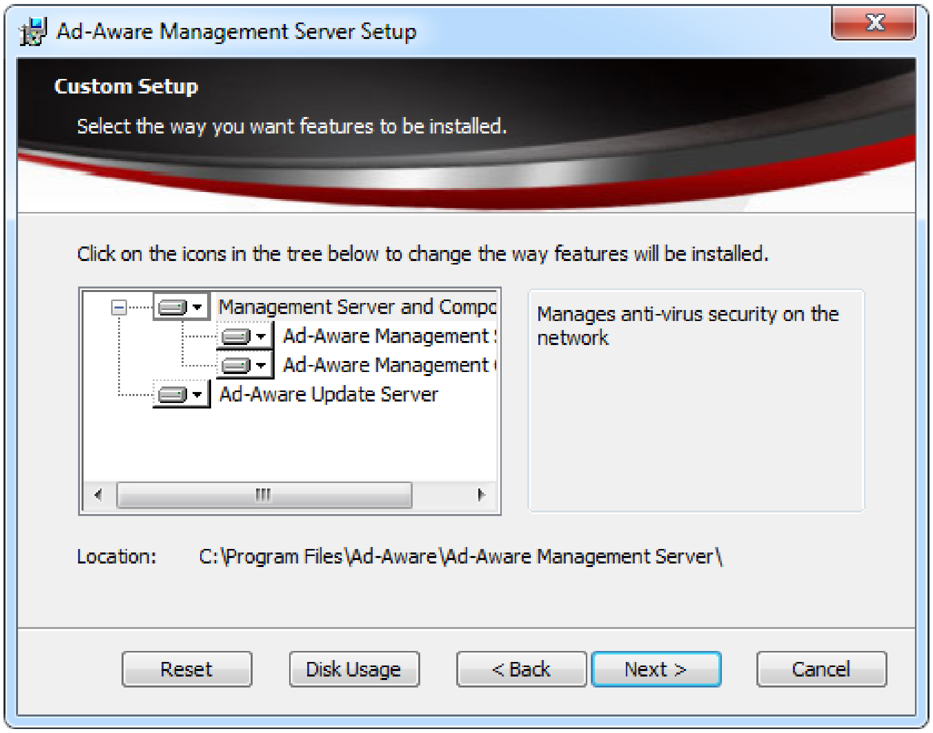
Allows users to choose which program features will be installed. Recommended for advanced users. Ad-Aware Windows Servers support can be installed with this option.

Installation Type

Click **Custom**. A new window will appear.

Step 4 - Customize Installation

This window allows you to choose which components of the installation package to be installed.



Ad-Aware Management Server Setup

Custom Setup

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

- Management Server and Compo
  - Ad-Aware Management :
  - Ad-Aware Management (
- Ad-Aware Update Server

Manages anti-virus security on the network

Location: C:\Program Files\Ad-Aware\Ad-Aware Management Server\

Custom Installation

The installation package contains the following components:

- Ad-Aware Management Server
  - Ad-Aware Security for Windows Servers (Server Add-On)
- Ad-Aware Management Console
- Ad-Aware Update Server

The components can be installed on the same computer or on separate computers.

The only restriction is to install Ad-Aware Management Server together with Ad-Aware Management Console.

Note

The computer on which you perform the installation must meet the system requirements of every component that will be installed. System requirements can be found in chapter System Requirements.

If you click any component name, a short description (including the minimum space required on the hard disk) will appear on the right side. By clicking any component icon, a menu will appear where you can choose whether to install or not the selected component.

Ad-Aware Management Server will be installed in `?:\Program Files\Ad-Aware\ Ad-Aware Management Server`.

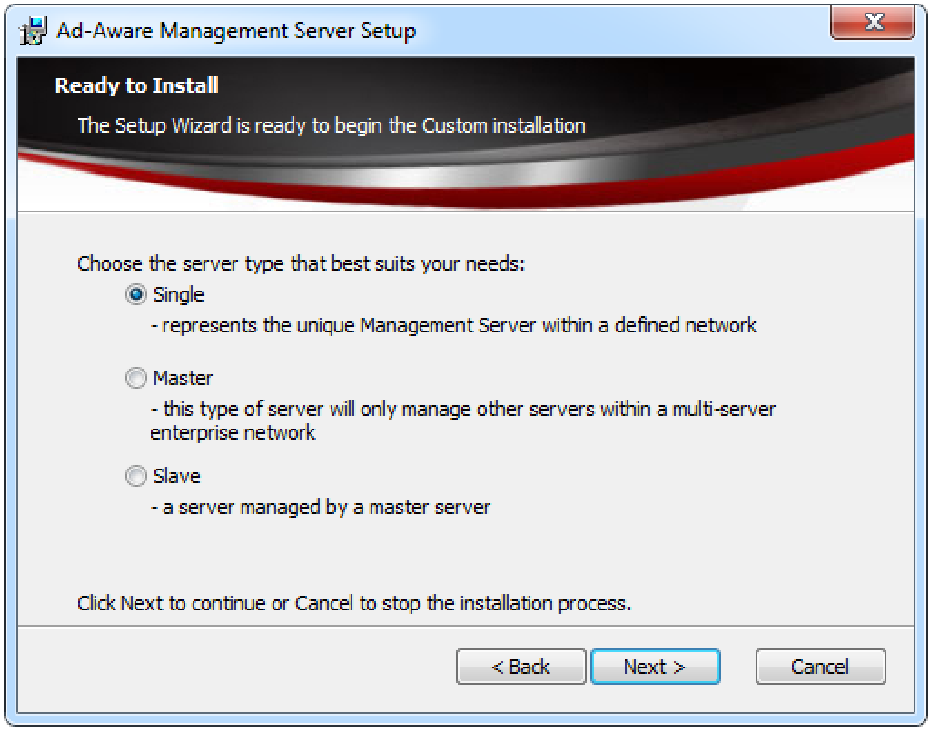
Click **Next**. A new window will appear.

Note

- If you have chosen to install only Ad-Aware Management Console, skip directly to Step 10 - Start Installation.
- If you have chosen to install only Ad-Aware Update Server, skip to Step 7 – Specify Ad-Aware Update Server Port and then to Step 10 - Start Installation.

Step 5 - Choose Server Type

This window allows you to select the server type to be installed.



Ready to Install

The Setup Wizard is ready to begin the Custom installation

Choose the server type that best suits your needs:

● Single

- represents the unique Management Server within a defined network

○ Master

- this type of server will only manage other servers within a multi-server enterprise network

○ Slave

- a server managed by a master server

Click Next to continue or Cancel to stop the installation process.

Server Type

You can select one of the following options:

- **Single** - to install a stand-alone, unique instance of Ad-Aware Management Server within the network. Such an instance of Ad-Aware Management Server manages all computers in the network.

  *** Recommended for growing businesses located in a single physical space.*

- **Master** - to install a master instance of Ad-Aware Management Server which will manage only slave instances of Ad-Aware Management Server deployed within the company's computer networks.
- **Slave** - to install a slave instance of Ad-Aware Management Server. Such an instance manages all computers within a defined network, being managed, at the same time, by a master instance of Ad-Aware Management Server. If you select this option, an edit field will appear where you must type the name or IP address of the master instance.

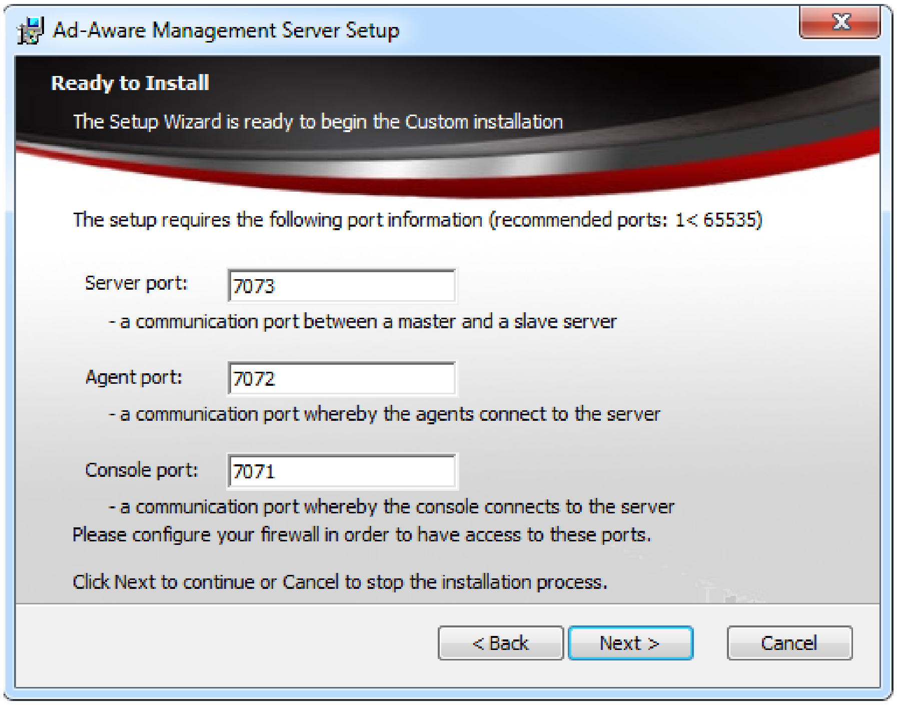
Note

For more information on the master-slave architecture, please refer to Architecture and Operation.

Click **Next.** A new window will appear.

Step 6 - Specify Communication Ports

This window allows you to change the ports used by the Ad-Aware Management Server components to communicate.



Ready to Install

The Setup Wizard is ready to begin the Custom installation

The setup requires the following port information (recommended ports: 1< 65535)

Server port: 7073
- a communication port between a master and a slave server

Agent port: 7072
- a communication port whereby the agents connect to the server

Console port: 7071
- a communication port whereby the console connects to the server

Please configure your firewall in order to have access to these ports.

Click Next to continue or Cancel to stop the installation process.

Communication Ports

You may change the default communication ports in the following fields:

- Server port - type in the port that will be used by a master instance of Ad-Aware Management Server to communicate with a slave instance. The default port is 7073.
- Agent port - type in the port that will be used by Ad-Aware Management Server to communicate with Ad-Aware Management Agent. The default port is 7072.
- Console port - type in the port that will be used by Ad-Aware Management Server to communicate with Ad-Aware Management Console. The default port is 7071.

Important

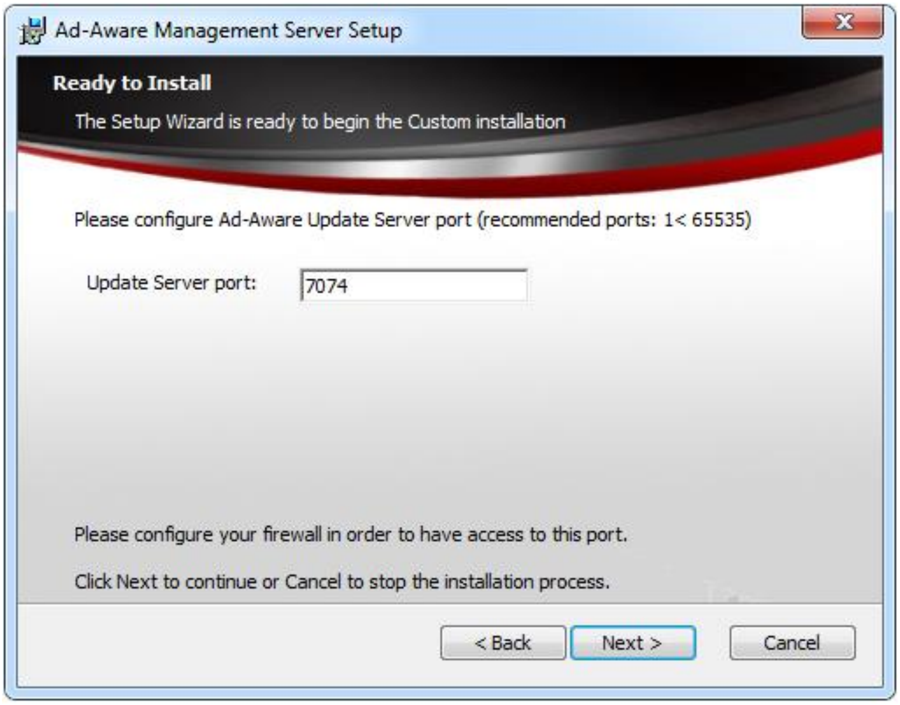
Please take the following into account:

- Provide port values between 1 and 65535 and make sure the specified ports are not used by other applications.
- Configure the local firewalls to allow these ports to be used.
- Remember the console port as you will need to provide it when connecting to Ad-Aware Management Server.

Click **Next**. A new window will appear.

Step 7 - Specify Ad-Aware Update Server Port

This window allows you to change the port used by Ad-Aware Update Server.



Ready to Install

The Setup Wizard is ready to begin the Custom installation

Please configure Ad-Aware Update Server port (recommended ports: 1< 65535)

Update Server port: 7074

Please configure your firewall in order to have access to this port.

Click Next to continue or Cancel to stop the installation process.

Ad-Aware Update Server Port

The default port is 7074. If you want to change the default port, type another value in the edit field.

The Ad-Aware Update Server port must not be used by other applications installed on the system.

Important

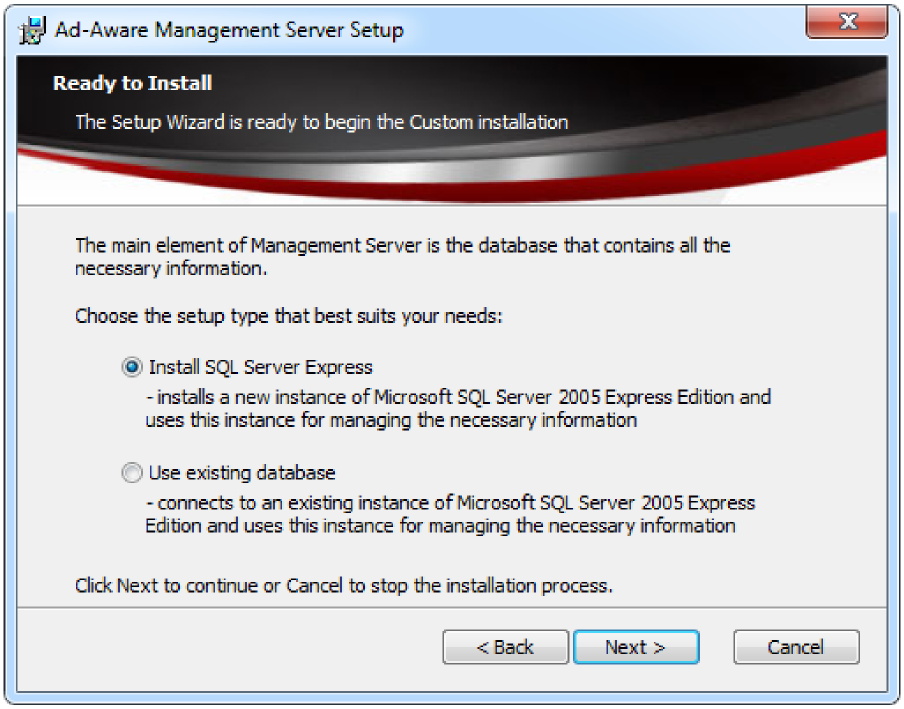
Please take the following into account:

- Provide port values between 1 and 65535.
- Configure the firewall on the computer where Ad-Aware Update Server is installed to allow this port to be used.

Click **Next**. If the port is in use, you will be prompted to set a new port. Otherwise, a new window will appear.

Step 8 - Ensure Database Support

This window allows you to install SQL Server Express or to use an existing database.



Ready to Install

The Setup Wizard is ready to begin the Custom installation

The main element of Management Server is the database that contains all the necessary information.

Choose the setup type that best suits your needs:

● Install SQL Server Express
- installs a new instance of Microsoft SQL Server 2005 Express Edition and uses this instance for managing the necessary information

○ Use existing database
- connects to an existing instance of Microsoft SQL Server 2005 Express Edition and uses this instance for managing the necessary information

Click Next to continue or Cancel to stop the installation process.

Database Support

Ad-Aware Management Server uses a dedicated database to manage all its necessary information (policies, tasks, clients and groups, network audit data, reports etc.). This helps Ad-Aware Management Server operate with large amount of data within the shortest delay possible and increase its efficiency.

Choose the option that best suits your needs:

- If you already have a working database that you want to use for Ad-Aware Management Server too, choose **Use existing database**. If Ad-Aware detects a database it can work with on the local machine, this option will be selected by default.

  Note
  Supported databases: Microsoft SQL Server 2005 / SQL Server 2005 Express Edition / Microsoft SQL Server 2008.

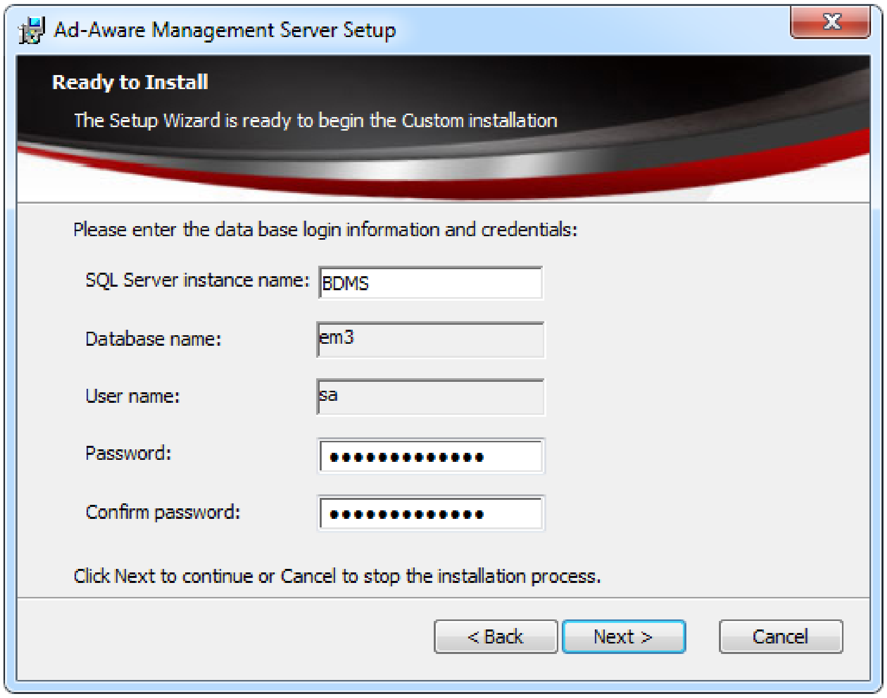
- Otherwise, choose **Install SQL Server Express** to install Microsoft SQL Server 2005 Express Edition and set up the database on the local computer.

Click **Next**. A new window will appear.

Step 9 - Connect to Database

I have chosen to install SQL Server Express

This window allows you to connect to the database.



Ready to Install

The Setup Wizard is ready to begin the Custom installation

Please enter the data base login information and credentials:

SQL Server instance name: BDMS

Database name: em3

User name: sa

Password: ••••••••••••••

Confirm password: ••••••••••••••

Click Next to continue or Cancel to stop the installation process.

Database Credentials

You can see the name of the SQL Server instance that will be installed, as well as the database name (em3) and the generic administrator username (sa).

You must specify the following:

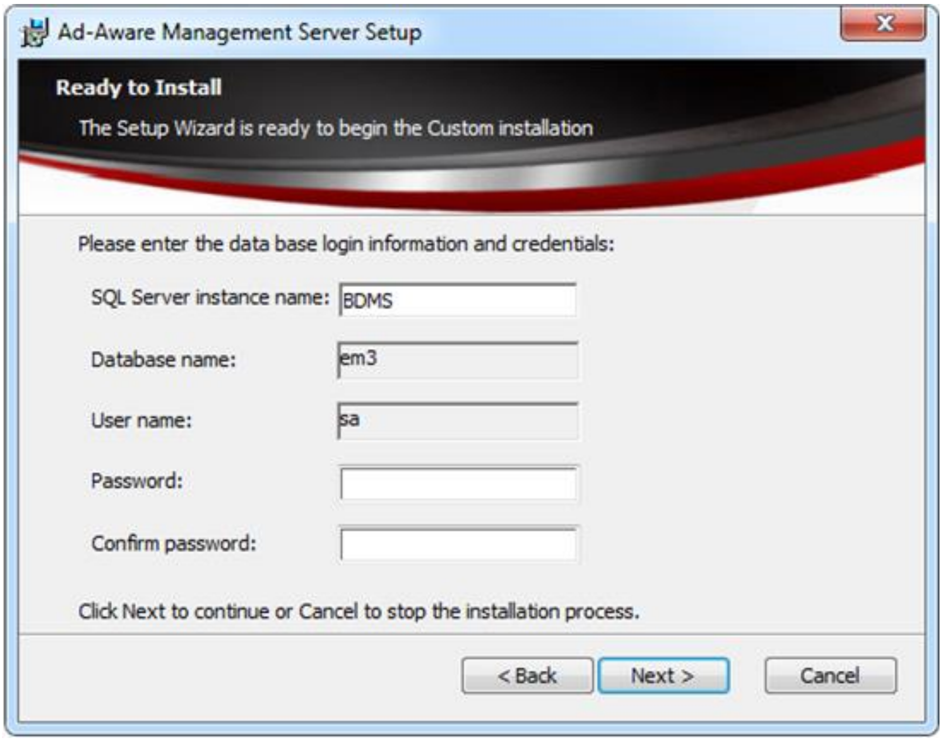
- **Password** - type in a password for the generic administrator username.
- **Confirm password** - re-type the password.

The password must be at least 7 characters long, and it must contain at least one capital letter, one small letter, one digit and one symbol.

Click **Next**. A new window will appear.

I have chosen to use an existing database

This window allows you to connect to the database.


Ad-Aware Management Server Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

Please enter the data base login information and credentials:

SQL Server instance name: BDMS

Database name: em3

User name: sa

Password:

Confirm password:

Click Next to continue or Cancel to stop the installation process.

Database Credentials

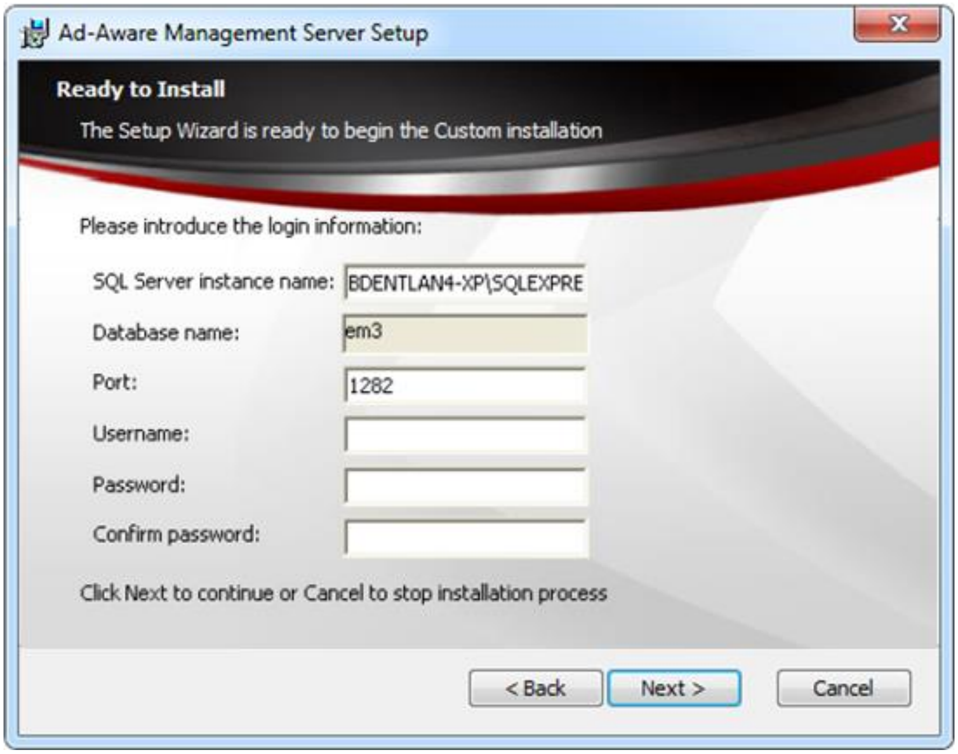
You must first provide the information used to connect to the database. The following fields must be filled in:

- **SQL Server Instance Name** - type in the name of the SQL Server instance.
- **Username** - type in a username recognized by the database.
- **Password** - type in the password of the previously specified username.
- **Confirm password** - re-type the password.

Click **Next**. A new window will appear.

Ad-Aware Management Server detected a compatible database

This window allows you to connect to a database detected on the local machine.



Ad-Aware Management Server Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

Please introduce the login information:

SQL Server instance name: BDENTLAN4-XP\SQLEXPRE

Database name: em3

Port: 1282

Username:

Password:

Confirm password:

Click Next to continue or Cancel to stop installation process

Database Credentials

You can see the name of the detected SQL Server instance and the database name (em3).

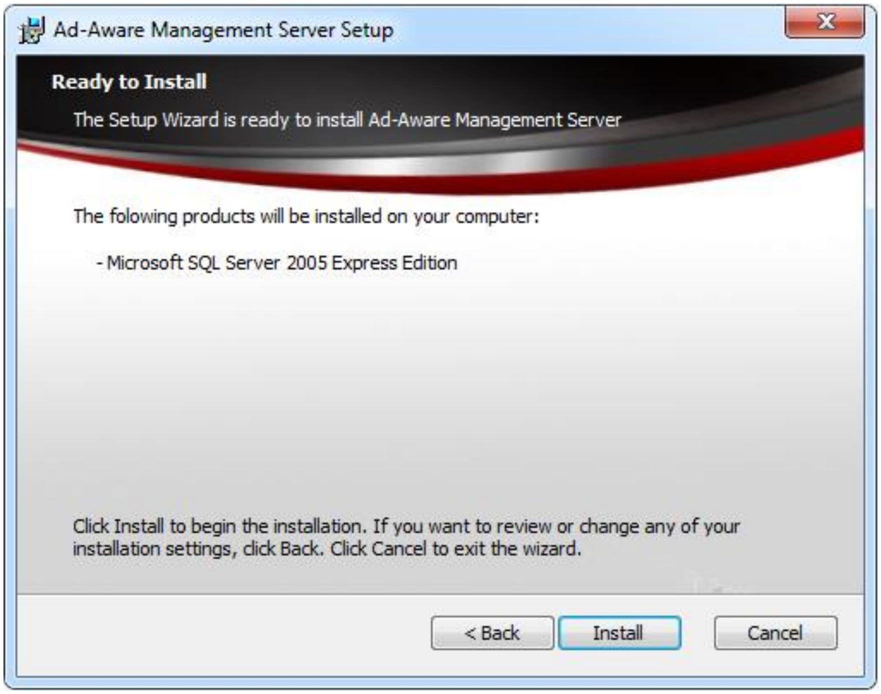
You must specify the following:

- **Username** - type in a username recognized by the database.
- **Password** - type in the password of the previously specified username.
- **Confirm password** - re-type the password.

Click **Next**. A new window will appear.

Step 10 - Start Installation

This window allows you to start installation.



Ad-Aware Management Server Setup

Ready to Install

The Setup Wizard is ready to install Ad-Aware Management Server

The folowing products will be installed on your computer:

- Microsoft SQL Server 2005 Express Edition

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Start Installation

You can see the third-party products that will be installed on your computer, if any. Depending on the components selected to be installed and on the software already installed on the local machine, the following third-party products may be installed:

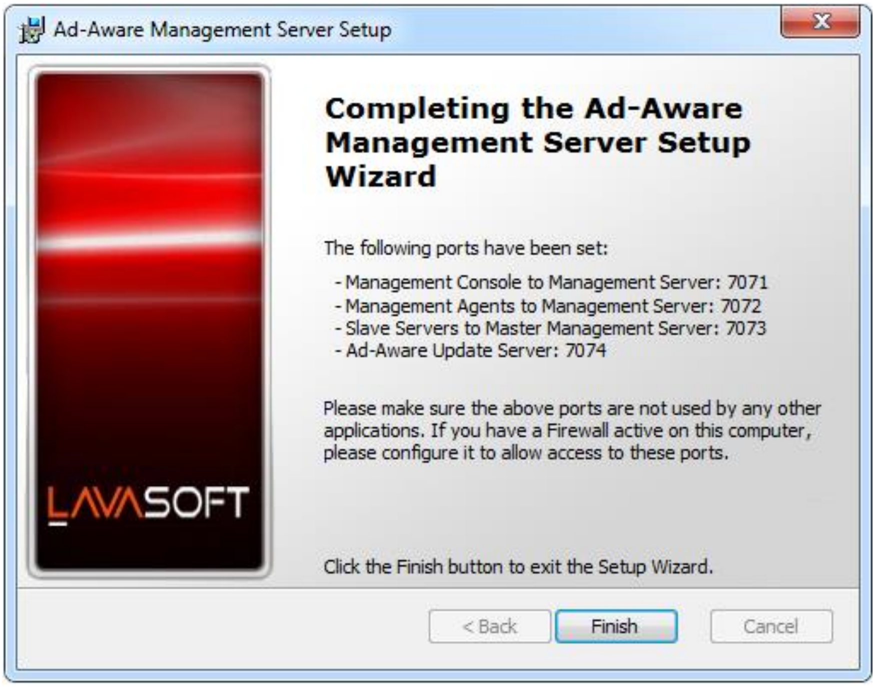
- Microsoft .Net Framework (required by Ad-Aware Management Console)
- Microsoft SQL Server 2005 Express Edition (required by Ad-Aware Management Server)

You can return to the previous steps to make any revisions if you consider this necessary.

Click **Install** in order to begin the installation of the product. Please note that the installation will take several minutes. Please wait for the installation to complete.

Step 11 - Finish Installation

At the end of the installation a new window will appear.



Completing the Ad-Aware Management Server Setup Wizard

The following ports have been set:

- Management Console to Management Server: 7071
- Management Agents to Management Server: 7072
- Slave Servers to Master Management Server: 7073
- Ad-Aware Update Server: 7074

Please make sure the above ports are not used by any other applications. If you have a Firewall active on this computer, please configure it to allow access to these ports.

Click the Finish button to exit the Setup Wizard.

Finish

You can see the communication ports configured for Ad-Aware Management Server and its components.

Reserve these ports only for Ad-Aware Management Server and make sure they are not used by other applications. If you have a firewall enabled on the local computer, you may need to configure it to allow these ports.

Click **Finish**. You may be asked to restart the computer in order to apply the changes made to the system. Please do it as soon as possible.

Once you have installed Ad-Aware Management Server, you can see in `Program Files` a new folder, named `Ad-Aware`, which contains the `Ad-Aware Management Server` subfolder.

Installing a Slave or Master Server

To install a slave or master instance of Ad-Aware Management Server, you must perform a custom installation. One of the custom installation steps enables you to set up the desired server type. All of the other installation steps are the same regardless of the selected server type. For more information, please refer to Custom Installation (With Screenshots).

It may be useful to know that you can change an Ad-Aware Management Server installation from stand-alone to slave and vice versa anytime you want. For more information, please refer to Master-Slave Configurations.

Adding Support for Unix-based Server Security Solutions

Ad-Aware security solutions for Linux, FreeBSD and Solaris servers (Ad-Aware Security for Samba, Security for Mail Servers) can be remotely managed from Ad-Aware Management Server by installing a separate add-on. The add-on can be installed at any time after installing Ad-Aware Management Server, without disturbing its operation.

Note

These security solutions cannot be remotely deployed, so you will have to install them manually.

Follow these steps to set up integration support of Ad-Aware security solutions for Unix-based servers in Ad-Aware Management Server:

1. Install the Unix add-on on the Ad-Aware Management Server computer (either the 32-bit or the 64-bit version, depending on the computer platform). To install the add-on, run the corresponding installation file and follow the wizard.

2. Install Ad-Aware Security for Mail Servers and Ad-Aware Security for Samba on your Unix-based servers, as needed. Please check with the Ad-Aware website for the list of supported distributions.

The installation procedure is quite simple. For example:

```
# sh BitDefender-Security-Mail-3.1.2-linuxgcc3x-i586.rpm.run
```

At some point, you will be asked if you want to enable integration with Ad-Aware Management Server. Type *Y* and then press *ENTER*.

3. Configure the integration with Ad-Aware Management Server.

a. Specify the Ad-Aware Management Server host:

```
# cd /opt/BitDefender/bin

# ./bdsafe bdem host <host[:port]>
```

b. Restart the product:

```
# cd /opt/BitDefender/bin

# ./bd restart
```

From this moment on, you should be able to see the installed solutions for Unix-based servers in the Ad-Aware Management Console. In the Create new policy pane, you can find new categories of policy templates.

You can disable integration with Ad-Aware Management Server at any time, using the following commands:

```
# cd /opt/BitDefender/bin

# ./bdsafe bdem enable N

# ./bd restart
```

Installing Components Separately

You can install some of the components of the installation package separately from Ad-Aware Management Server. Refer to the following topics in this section:

- Installing Ad-Aware Management Console on Administrator's Computer
- Installing Ad-Aware Update Server on a Dedicated Computer

Installing Ad-Aware Management Console on Administrator's Computer

You can install Ad-Aware Management Console on your computer and connect remotely to Ad-Aware Management Server in order to configure and manage the network security.

Connecting remotely with Ad-Aware Management Console instead of using remote desktop connection software may be more convenient in specific situations.

To install only Ad-Aware Management Console, follow these steps:

1. Locate the installation file on the computer and double-click it to start the installation wizard. Please note that you need at least 3 GB of free space on the system partition, or otherwise the installation will likely fail.
2. Click **Next**.
3. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.
4. Click **Custom**.
5. Choose to install only Ad-Aware Management Console: right-click all other components of the installation package and choose not to install them.
6. Click **Next**.
7. Click **Install**.
8. Wait until the installation is completed and then click **Finish**.
9. Configure the local firewall to allow the port on which Ad-Aware Management Server is set to accept connections from Ad-Aware Management Console. The default port is 7071.

No configuration is required if Ad-Aware Business Client is installed on the computer.

Installing Ad-Aware Update Server on a Dedicated Computer

Ad-Aware Update Server can be used to download updates for all Ad-Aware client products to a specific computer in the local network. All Ad-Aware client products installed in the network can be configured to download updates from the local update server.

In most cases, it is recommended to install Ad-Aware Update Server together with Ad-Aware Management Server, on the same computer. If your network has a large number of clients, you may consider installing it on a dedicated computer to prevent interferences with Ad-Aware Management Server.

To install Ad-Aware Update Server on a dedicated computer, follow these steps:

1. Locate the installation file on the computer and double-click it to start the installation wizard. Please note that you need at least 3 GB of free space on the system partition, or otherwise the installation will likely fail.

2. Click **Next**.
3. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.
4. Click **Custom**.
5. Choose to install only Ad-Aware Update Server: right-click all other components of the installation package and choose not to install them.
6. Click **Next**.
7. If you want to change the port on which Ad-Aware Update Server accepts connections, type a new value in the edit field. It is recommended that you use the default port (7074).

Important

Please take the following into account:

- Provide port values between 1 and 65535.
- The Ad-Aware Update Server port must not be used by other applications installed on the system.
- Keep a record of this port number. You will need to know it later, when configuring the Ad-Aware client products to download their updates from the local update server.

8. Click **Next**. If the port is in use, you will be prompted to set a new port.
9. Click **Install**.
10. Wait until the installation is completed and then click **Finish**.
11. Configure the local firewall to allow the port on which Ad-Aware Update Server is set to accept connections.

For more information, please refer to Ad-Aware Update Server.

Installing Client Products

The next logical step after installing Ad-Aware Management Server is to install the client products. Client products are Ad-Aware security solutions that can be managed remotely using Ad-Aware Management Server. You can install client products only on the network computers that are managed by Ad-Aware Management Server (client computers). Before you proceed, prepare computers for deployment to make sure it goes smoothly.

Note

For information on installing Unix-based clients, please refer to Adding Support for Unix-based Server Security Solutions. For information on Mac clients, please refer to Integrating Ad-Aware Antivirus for Mac into the Centralized Reporting Platform.

Step 1 - Prepare Computers for Deployment

Prepare the network computers for deployment as follows:

1. Make sure the network computers meet the corresponding system requirements. System requirements can be found in chapter System Requirements.

Note

Make a list of the workstations that do not meet the system requirements of Ad-Aware Business Client (mainly Windows 98 or NT workstations). Such workstations cannot be protected with Ad-Aware Business Client and must be excluded from Ad-Aware Management Server.

2. **Configuration required on the network computers.**

- Configure each Windows XP workstation that is part of a workgroup, or of a different domain than the Ad-Aware Management Server computer, NOT to use simple file sharing. Follow these steps:
  a. On the Windows Start menu, click **My Computer**.
  b. Click **Tools** > **Folder Options**, then the **View** tab.
  c. Clear the **Use simple file sharing** check box in the advanced settings list.
- On all workstations and servers you want to manage and on the Ad-Aware Management Server computers, configure the firewall to allow the communication ports used by the Ad-Aware Client Security components. Or, if you prefer, you can disable the firewalls.

  These are the default communication ports you need to allow:

  - `7072` - The communication port between Ad-Aware Management Server and Ad-Aware Management Agent. This port must be allowed on all network computers.
  - `7071` - The communication port between Ad-Aware Management Server and Ad-Aware Management Console. This port must be allowed on all Ad-Aware Management Server computers and on all computers on which you install Ad-Aware Management Console.
  - `7073` - The communication port between a master and a slave instance of Ad-Aware Management Server. This port must be allowed on all Ad-Aware Management Server computers.

These ports must not be used by any other application installed in the network. If any of these ports is used by another application, you will need to choose a new communication port and set the firewalls to allow it instead of the default port.

- It is recommended to temporarily turn off User Account Control on all computers running Windows operating systems that include this security feature (Windows Vista, Windows 7, Windows Server 2008 etc.). If the computers are in a domain, you can use a group policy to turn off User Account Control remotely.

3. Before you deploy Ad-Aware Business Client on the managed workstations, REMOVE any third-party security software installed on the managed workstations. Failing to do so may result in failure to deploy Ad-Aware Business Client and in system instability.

Note

You can fulfill this prerequisite easier AFTER defining the managed computers (by deploying Ad-Aware Management Agent on them). Ad-Aware Management Server provides a built-in task named *`List Installed Software`* that you can run on all managed computers to identify and remove installed security software. For more information, please refer to Network Tasks.

Step 2 - Define Managed Computers

In order to manage a workstation remotely, Ad-Aware Management Agent must be installed on that workstation. You deploy Ad-Aware Management Agent from the Ad-Aware Management Console - the user interface of Ad-Aware Management Server.

To deploy Ad-Aware Management Agent on the network computers, follow these steps:

1. Provide the administrative credentials.

2. Deploy Ad-Aware Management Agent.

There are several deployment methods, each appropriate for a specific situation.

- **Using the Network Builder tool**. Network Builder is recommended to be used for the initial deployment of Ad-Aware Management Agent in the network and for major network reorganization operations.
- **Using the Automatic Deployment tool**. Automatic Deployment is used to keep Ad-Aware Management Server up-to-date with the network changes after the initial deployment. Using Automatic Deployment, Ad-Aware Management Agent can be automatically deployed on the newly detected computers.
- **From the Unmanaged Computers group, using the contextual menu**. The Unmanaged Computers group displays the network computers automatically detected by Ad-Aware Management Server. You can easily deploy Ad-Aware Management Agent on any computer, by right-clicking the computer and selecting Deploy Ad-Aware this computer.
- **Using Deployment Tool**. Deployment Tool is to be used when the other deployment methods fail.

You will find out how to use these methods as you go through section Step 2 – Deploy Ad-Aware Management Agent.

⚠ **Important**

Each time you deploy Ad-Aware Management Agent you will be prompted to configure the deployment options. Pay special attention when configuring the management server identity. Ad-Aware Management Agent communicates with Ad-Aware Management Server using either the IP address or the name of the computer Ad-Aware Management Server is installed on. To prevent communication issues, configure the management server identity as follows:

- Use the IP address of the Ad-Aware Management Server computer if it does not change in time (static or reserved IP address).
- Use the server name when the IP address is dynamically assigned by DHCP (no MAC address-based IP reservation).

Step 1 - Provide Administrative Credentials

In order to remotely deploy Ad-Aware Management Agent, Ad-Aware Management Server requires a set of credentials for authentication on the remote computer.

Use the Credentials Manager to store the authentication credentials: open the management console and click **Tools > Credentials Manager**. You can provide the user name and password of the administrator of an Active Directory domain or the credentials of the local user accounts. For more information, please refer to Credentials Manager.

Step 2 - Deploy Ad-Aware Management Agent

These are the recommended steps to be followed when you initially deploy Ad-Aware Management Agent:

1. **Organize the network computers and deploy Ad-Aware Management Agent using Network Builder**. Network Builder helps you easily organize the network computers into a manageable structure and deploy Ad-Aware Management Agent on selected computers. This tool is designed to be used during the initial deployment of Ad-Aware Management Agent and when reorganizing the managed network.

   To use the Network Builder open the management console and click **Tools > Network Builder**.

   You can create managed computers groups into which you will then drag & drop the detected network computers. If you use Active Directory to manage network users and resources, you can directly import the existing Active Directory structure. For more information, please refer to Network Builder.

2. **Use Deployment Tool to deploy Ad-Aware Management Agent on the computers on which deployment with Network Builder failed**. Deployment Tool helps you automatically install, remove or repair Ad-Aware products on remote network computers. This tool also enables you to create unattended installation packages for use on offline computers (or when remote installation fails).

   You typically resort to the Deployment Tool when other deployment methods fail (you cannot successfully ping a target computer). In such cases, create unattended installation packages, then copy and execute them on the inaccessible network computers. For more information, please refer to Deployment Tool.

3. **Keep Ad-Aware Management Server up-to-date with the network changes**. Once you have created and organized the managed computers network, you can configure the Automatic Deployment tool. This tool enables you to deploy Ad-Aware Management Agent and Ad-Aware Business Client automatically on newly detected computers.

   To configure Automatic Deployment open the management console, click **Tools > Automatic Deployment**. For more information, please refer to Automatic Deployment.

   As an alternative to Automatic Deployment, you can periodically check the dashboard in the management console (just click the server name in the tree menu). If there are unmanaged computers, go to **Computers Directory** > **Unmanaged Computers**. Right-click the computers you want to manage and select **Deploy on this computer**.

Step 3 - Deploy Client Products

After defining and organizing managed computers into groups, you can start deploying the client products. You do not have to actually install them. Just create a policy corresponding to a client product and assign it to run on managed computers or on entire groups of managed computers. If the product is not already installed on the managed computer, it will automatically be installed before the policy is applied.

For more information about policies, please refer to Policies.

Do not apply Ad-Aware Business Client policies on the company servers! Ad-Aware Business Client is a security solution designed to protect workstations only and it will not install on Windows Server operating systems. To protect the company servers, use Ad-Aware Security for File Servers.

Note

To remotely manage a Ad-Aware server product already installed on a server, you only need to define that server as a managed computer (by deploying Ad-Aware Management Agent). The integration is made automatically without having to remove and reinstall the product.

Step 4 - Deploying on Offline Computers

To deploy Ad-Aware Management Agent or Ad-Aware Business Client on offline computers:

1. Create unattended installation packages using Deployment Tool. For more information, please refer to Deployment Tool.
2. Transfer the installation packages to the offline computers and install them. Install Ad-Aware Management Agent first, and then Ad-Aware Business Client.

Client Deployment Tools

Ad-Aware Management Server comes with several built-in tools that help you easily deploy the Ad-Aware clients across the entire network, manage deployments and check deployment status and result.

Credentials Manager

Credentials Manager allows you to save the credentials used by Ad-Aware Management Server for authentication when deploying Ad-Aware Management Agent.

Note

These credentials are used only when deploying Ad-Aware Management Agent directly on unmanaged computers or by using Network Builder or Automatic Deployment. If you use Deployment Tool, you will have to provide the appropriate credentials separately, when you configure the deployment options.

Retry Deployment

If this option is enabled, failed deployments will run again automatically. This may be more convenient than reviewing every failed deployment and then reinitiating it manually.

Network Builder

Network Builder helps you easily organize the network computers into a manageable structure and deploy Ad-Aware Management Agent on selected computers. This tool enables you to import an existing Active Directory structure (computers and groups) and deploy Ad-Aware Management Agent on all network computers.

Deployment Tool

Deployment Tool helps you automatically install, remove or repair Ad-Aware products on remote network computers. This tool also enables you to create unattended installation packages for use on offline computers (or when remote installation fails).

Automatic Deployment

Automatic Deployment allows Ad-Aware Management Server to automatically deploy Ad-Aware Management Agent and Ad-Aware Business Client on newly detected computers.

Deployment Status

The Deployment Status window provides information on the status of all initiated, in progress or finished deployment processes, regardless of the deployment method.

Credentials Manager

In order to remotely deploy Ad-Aware Management Agent, Ad-Aware Management Server requires a set of credentials for authentication on the remote computer:

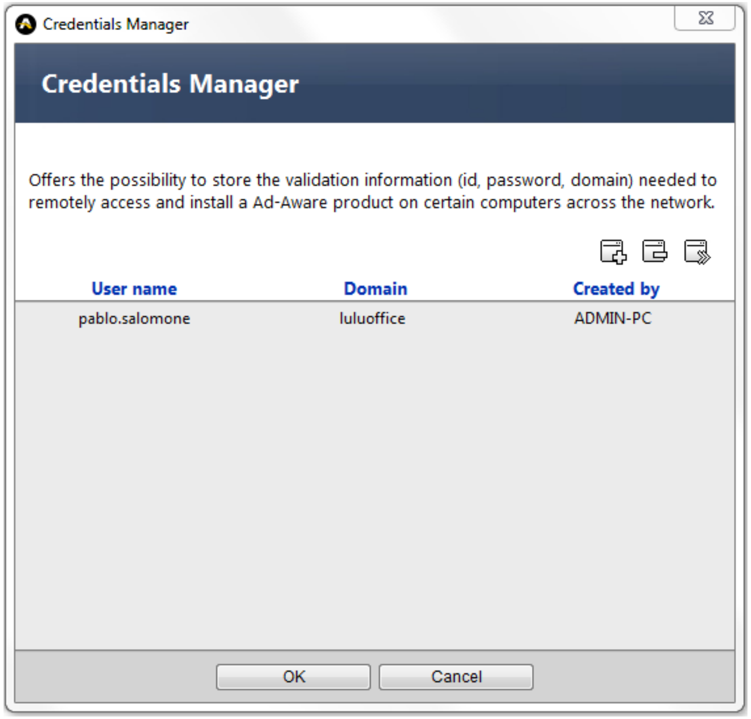
- The username of a user account with administrative rights on the remote computer.
- The password of the specified user account.
- For a domain administrator account, the domain to which it belongs.
- For a local administrator account (on a stand-alone or workgroup computer), the computer name.

Credentials Manager allows you to save the credentials used by Ad-Aware Management Server for authentication when deploying Ad-Aware Management Agent.

Note

These credentials are used only when deploying Ad-Aware Management Agent directly on unmanaged computers or by using Network Builder or Automatic Deployment. If you use Deployment Tool, you will have to provide the appropriate credentials separately, when you configure the deployment options.

To open the Credentials Manager window, open the management console; click **Tools** and then **Credentials Manager** on the menu.


Credentials Manager

Offers the possibility to store the validation information (id, password, domain) needed to remotely access and install a Ad-Aware product on certain computers across the network.

User name	Domain	Created by
pablo.salomone	luluoffice	ADMIN-PC

Credentials Manager

You can see all of the credentials saved by Credentials Manager. For security reasons, the password is not displayed in the Credentials Manager window, neither in clear, nor masked.

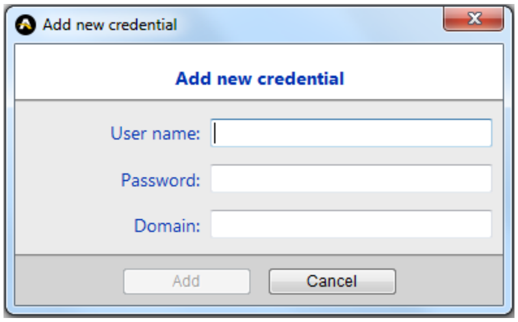
When deploying Ad-Aware Management Agent on a remote computer, Ad-Aware Management Server will try the credentials sets in the list one by one until authentication is successful. If authentication fails, Ad-Aware Management Agent will not be deployed on the remote computer.

Note

You can check deployment status and history by clicking the Tools menu in the management console and choosing **View Deployment Status**. Use the last deployment status to find out which deployments failed because of missing credentials.

Adding New Credentials

You can add up to 100 sets of credentials. To add a new set of credentials, click the **Add** button. A new window will appear.



Adding New Credentials

You must fill the required information in the following fields:

- **Username** - type the username of a user account with administrative rights.
- **Password** - type the password of the previously specified username.

Note

The provided password is encrypted in order to avoid a potential security threat.

- **Domain** - if you specified a domain user account, type the respective domain; otherwise, type the computer name.

Click **Add** to add the new credentials. If you want to quit, just click **Cancel**.

When finished adding credentials, click **OK** to save the changes and close the window.

Adding Credentials for Windows Server (Active Directory) Domains

For the network computers that are within an Active Directory domain, you will only have to provide the credentials of the domain administrator.

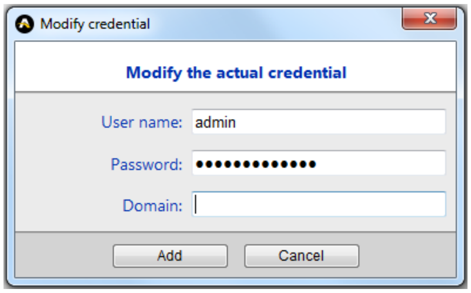
Adding Credentials for Windows Workgroups or Stand-alone Computers

In the case of network computers grouped into Windows workgroups, you will have to provide administrative credentials for each computer. This also applies to stand-alone computers.

If the same username and password are configured on all computers in a workgroup, you can provide only these credentials, leaving the **Domain** field blank.

Editing Existing Credentials

To edit an existing set of credentials, click the **Edit** button. A new window will appear.



Modify credential

Modify the actual credential

User name: admin

Password: •••••••••••••

Domain:

Editing Existing Credentials

Make the desired changes and click **OK** to save them. If you want to quit, just click **Cancel**.

When finished editing credentials, click **OK** to save the changes and close the window

Deleting Existing Credentials

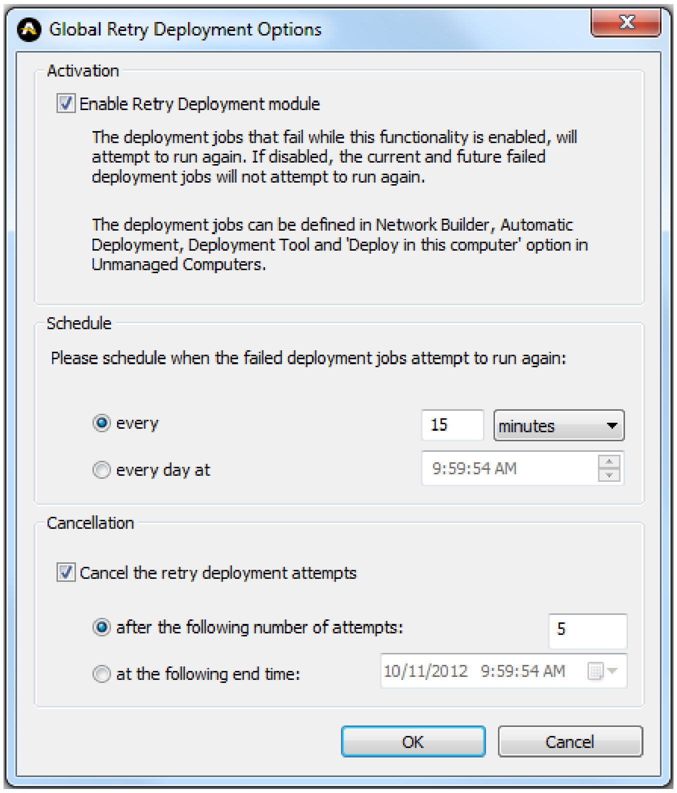
To delete an existing set of credentials, select the corresponding user from the list and click the **Delete** button. You will have to confirm your action by clicking **Yes**.

Click **OK** to save the changes and close the window.

Retry Deployment

If you want the failed deployments to run again automatically, you must configure the Retry Deployment option. This may be more convenient than reviewing every failed deployment and then reinitiating it manually.

To open the window where you can configure the global Retry Deployment options, click **Tools** in the management console and then **Retry Deployment** on the menu.



Global Retry Deployment Options

Activation

☑ Enable Retry Deployment module

The deployment jobs that fail while this functionality is enabled, will attempt to run again. If disabled, the current and future failed deployment jobs will not attempt to run again.

The deployment jobs can be defined in Network Builder, Automatic Deployment, Deployment Tool and 'Deploy in this computer' option in Unmanaged Computers.

Schedule

Please schedule when the failed deployment jobs attempt to run again:

● every 15 minutes

○ every day at 9:59:54 AM

Cancellation

☑ Cancel the retry deployment attempts

● after the following number of attempts: 5

○ at the following end time: 10/11/2012 9:59:54 AM

Retry Deployment

To automatically rerun the deployments that failed, select **Enable Retry Deployment module**. By default, the current and future deployments that failed are retried every 15 minutes, but no more than 5 times.

The retry options can be configured as needed. You can set the failed deployments to be rerun either after a desired number of minutes/hours/days or at a specific time of the day. To limit the number of attempts, select **Cancel the retry deployment attempts** and set either a limited number of attempts or a specific deadline.

Note
Deployments cannot be retried more often than every 5 minutes.

Network Builder

Network Builder helps you easily organize the network computers into a manageable structure and deploy Ad-Aware Management Agent on selected computers.

Note
You should use Network Builder immediately after deploying Ad-Aware Management Server.

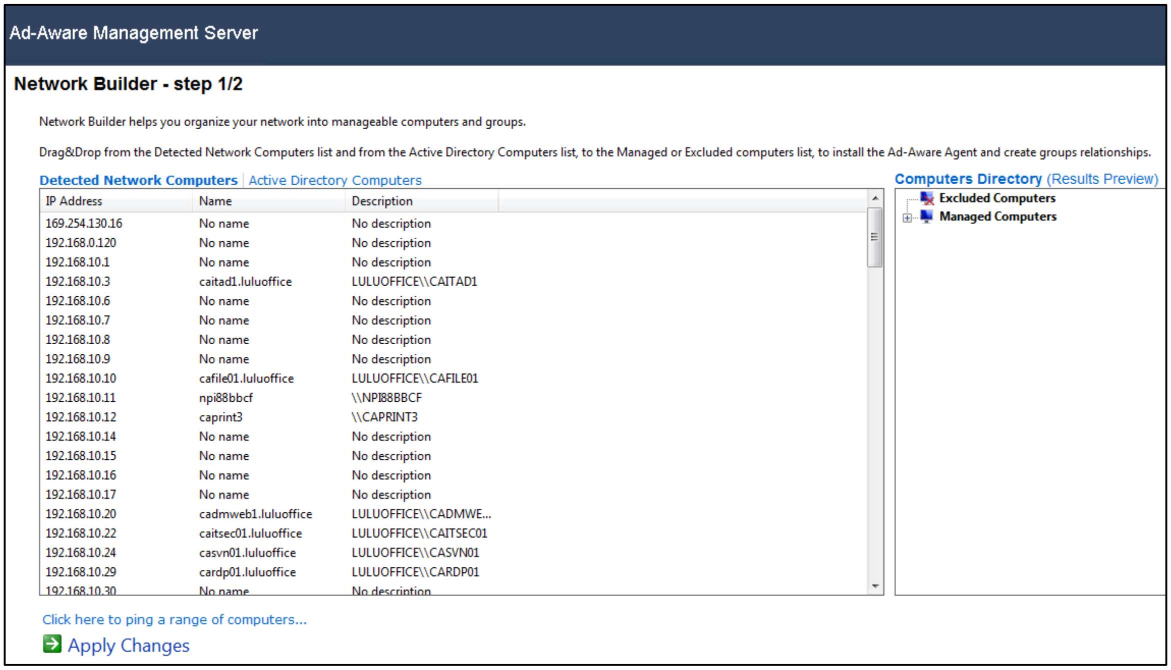
Using Network Builder, you can drag & drop the detected network computers (those displayed in the Unmanaged Computers group) or the computers imported from Active Directory in the Excluded Computers or Managed Computers group. After organizing the network computers, you can apply changes and deploy Ad-Aware Management Agent on the computers that you have moved into the Managed Computers group.

To display the Network Builder pane, click **Tools** in the management console and then **Network Builder** on the menu.

Note
If connected to more than one instance of Ad-Aware Management Server in the management console, you must first select the specific instance to use the tool for.

You must follow a two-step procedure.

Step 1/2 - Organize Computers



Ad-Aware Management Server

Network Builder - step 1/2

Network Builder helps you organize your network into manageable computers and groups.

Drag&Drop from the Detected Network Computers list and from the Active Directory Computers list, to the Managed or Excluded computers list, to install the Ad-Aware Agent and create groups relationships.

Detected Network Computers
Active Directory Computers
Computers Directory (Results Preview)
Excluded Computers
Managed Computers

IP Address	Name	Description
169.254.130.16	No name	No description
192.168.0.120	No name	No description
192.168.10.1	No name	No description
192.168.10.3	caitad1.luluoffice	LULUOFFICE\\CAITAD1
192.168.10.6	No name	No description
192.168.10.7	No name	No description
192.168.10.8	No name	No description
192.168.10.9	No name	No description
192.168.10.10	cafile01.luluoffice	LULUOFFICE\\CAFILE01
192.168.10.11	npi88bbcf	\\NPI88BBCF
192.168.10.12	caprint3	\\CAPRINT3
192.168.10.14	No name	No description
192.168.10.15	No name	No description
192.168.10.16	No name	No description
192.168.10.17	No name	No description
192.168.10.20	cadmweb1.luluoffice	LULUOFFICE\\CADMWE...
192.168.10.22	caitsec01.luluoffice	LULUOFFICE\\CAITSEC01
192.168.10.24	casvn01.luluoffice	LULUOFFICE\\CASVN01
192.168.10.29	cardp01.luluoffice	LULUOFFICE\\CARDP01
192.168.10.30	No name	No description

Detected Network Computers

On the left side of the **Network Builder** pane, you can see the detected network computers. These computers are not managed by Ad-Aware Management Server and can be found in the Unmanaged Computers group. You can click **Active Directory Computers** to import and display the computers from Active Directory instead of the unmanaged computers. On the right side, you can see the Excluded Computers and Managed Computers groups from Computers Directory.

To organize the network computers, follow these guidelines:

1. Drag&Drop in Excluded Computers all network devices that will not be managed by Ad-Aware Management Server. For more information, please refer to Excluding Computers from Management.
2. If an Active Directory structure is already in place, click **Active Directory Computers** and drag & drop the structure directly in Managed Computers.
3. If no Active Directory structure is available, organize the detected network computers as follows:
   a) Create groups in Managed Computers. For example, you can create separate groups for your Quality Assurance, Online, Sales and Administrative departments (teams). This will help you manage network computers more easily and enforce policies based on user category.
   b) Drag&drop the computers to be managed by Ad-Aware Management Server into the appropriate groups. Do not place servers and workstations in the same group.

Pinging Computers

Ad-Aware Management Server detects network computers by listening to the network traffic. Therefore, network discovery is a process that takes some time and does not fully reflect the network state. Some network computers may be online, but Ad-Aware Management Server may not have detected them yet.

You can detect new network computers by pinging ranges of IP addresses. Click the provided link, type the lower and upper limit of the IP range and click **Start**. All new computers that respond to the ping are automatically displayed as detected network computers. They are highlighted as follows:

- Computers on which Ad-Aware Management Agent is already installed (managed computers) are highlighted in green.
- Unmanaged computers are highlighted in red.

Creating New Groups

You can create sub-groups in the Managed Computers group in order to organize the computers managed by Ad-Aware Management Server according to the company's structure.

To create a new sub-group in Managed Computers or in one of its sub-groups, right-click the parent group and select **Create new group**. Type an appropriate name for the newly created group.

Deleting Groups

To delete a sub-group of the Managed Computers group, right-click it and select **Delete group**.

Removing Computers from Groups

To remove a computer from the Excluded Computers or Managed Computers group, right-click it and select **Remove computer from group**.

Deleting Detected Computers

To delete a computer both from the group it is placed in and from the list of detected network computers, right-click it and select **Delete computer**.

Note

If you delete an unmanaged computer while it is still connected to the network, Ad-Aware will eventually detect its activity and restore it in the Unmanaged Computers group.

Excluding Computers from Management

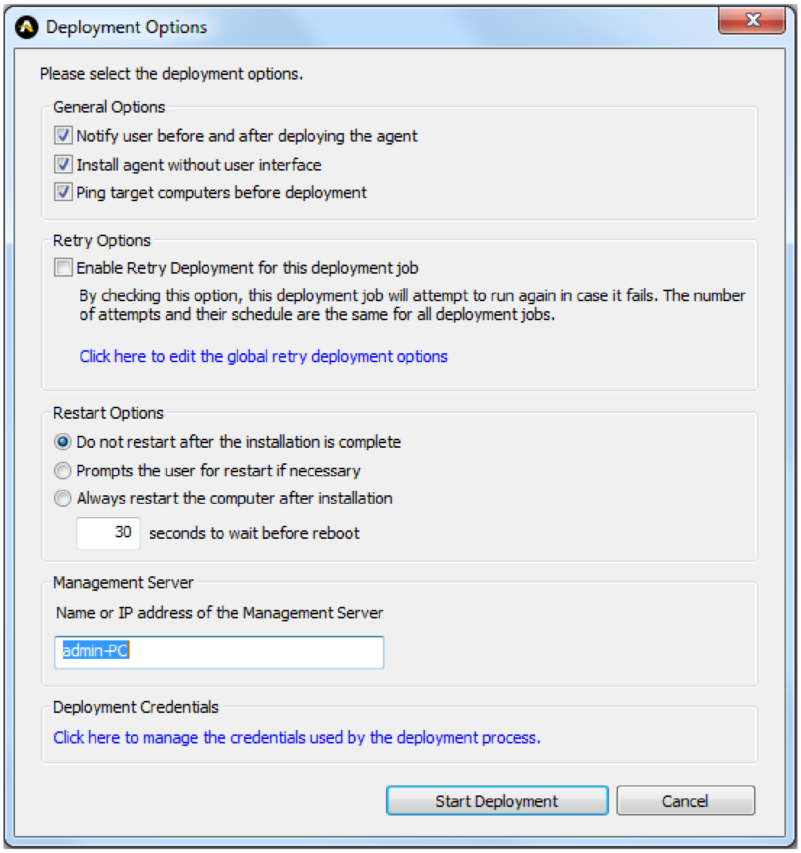
If you do not want specific computers to be managed by Ad-Aware Management Server, you just have to exclude them from management. For example, you might want to exclude your own computer, the computers of your IT team or the computers of the Quality Assurance team.

You should also exclude the router interfaces and management switches detected by Ad-Aware Management Server in the broadcast domain. You should make a list of such devices in your network, find them in the Unmanaged Computers group and exclude them.

To exclude a computer or a group of computers from management, move them by drag&drop in the **Excluded Computers** group.

Step 2/2 - Deploy Ad-Aware Management Agent

To save the changes made to the way network computers are organized, click **Apply changes**. A new window will appear.



Deployment Options

Please select the deployment options.

General Options

☑ Notify user before and after deploying the agent

☑ Install agent without user interface

☑ Ping target computers before deployment

Retry Options

☐ Enable Retry Deployment for this deployment job

By checking this option, this deployment job will attempt to run again in case it fails. The number of attempts and their schedule are the same for all deployment jobs.

Click here to edit the global retry deployment options

Restart Options

● Do not restart after the installation is complete

○ Prompts the user for restart if necessary

○ Always restart the computer after installation

30 seconds to wait before reboot

Management Server

Name or IP address of the Management Server

admin-PC

Deployment Credentials

Click here to manage the credentials used by the deployment process.

Deployment Options

You must specify the deployment options before initiating the deployment of Ad-Aware Management Agent

To configure and initiate the deployment of Ad-Aware Management Agent, follow these steps:

Step 1 - Configure General Options

You can specify the deployment behavior on the remote computer using the options in the **General Options** category.

Check **Notify user before and after deploying the agent** if you want the user logged on the remote computer to be briefly informed about the deployment process. Two dialogs will appear on the user's screen, before and after the deployment process.

Check **Install agent without user interface** if you want the deployment process to be performed silently in the background. If you do not check this option, the Windows Installer interface will appear on the user's screen.

Select **Ping target computers before deployment** to find out immediately if and which of the target computers are disconnected from the network. If the ping to a target computer fails, Ad-Aware Management Server will not proceed with the deployment on that computer.

Step 2 - Configure Retry Options

By selecting Enable Retry Deployment for this job, if the deployment fails the first time, it will run again automatically. To configure the retry options, click the provided link.

Note

For more information, please refer to Retry Deployment.

Step 3 - Specify Restart Method

To specify how to restart the remote computer, select one of the options in the **Restart Options** category. If you select:

- **Do not restart after the installation is completed** - the remote computer will not be restarted once the installation is completed. Ad-Aware Management Agent does not require a restart to complete the installation, so you can safely select the first option.
- **Prompt the user for restart if necessary** - the user logged on the remote computer will be prompted to restart the computer, if it is necessary.

Note

The user must confirm or suspend computer restart within 30 seconds, otherwise the remote computer will be restarted automatically.

- **Always restart the computer after installation** - the remote computer is restarted immediately after the installation is completed, without alerting the user.

Step 4 - Specify Management Server

Ad-Aware Management Agent communicates with Ad-Aware Management Server using either the IP address or the name of the computer Ad-Aware Management Server is installed on. To prevent communication issues, configure the management server identity as follows:

- If the IP address of the Ad-Aware Management Server computer does not change in time (static or reserved IP address), type the IP address.
- Otherwise, if the IP address is dynamically assigned by DHCP (no MAC address-based IP reservation), type the computer name.

By default, Ad-Aware Management Agent will be managed by the specific instance of Ad-Aware Management Server that deploys it. If you want Ad-Aware Management Agent to be managed by another instance of it

Defender Management Server, provide the name or IP address of the computer it is installed on in the corresponding field.

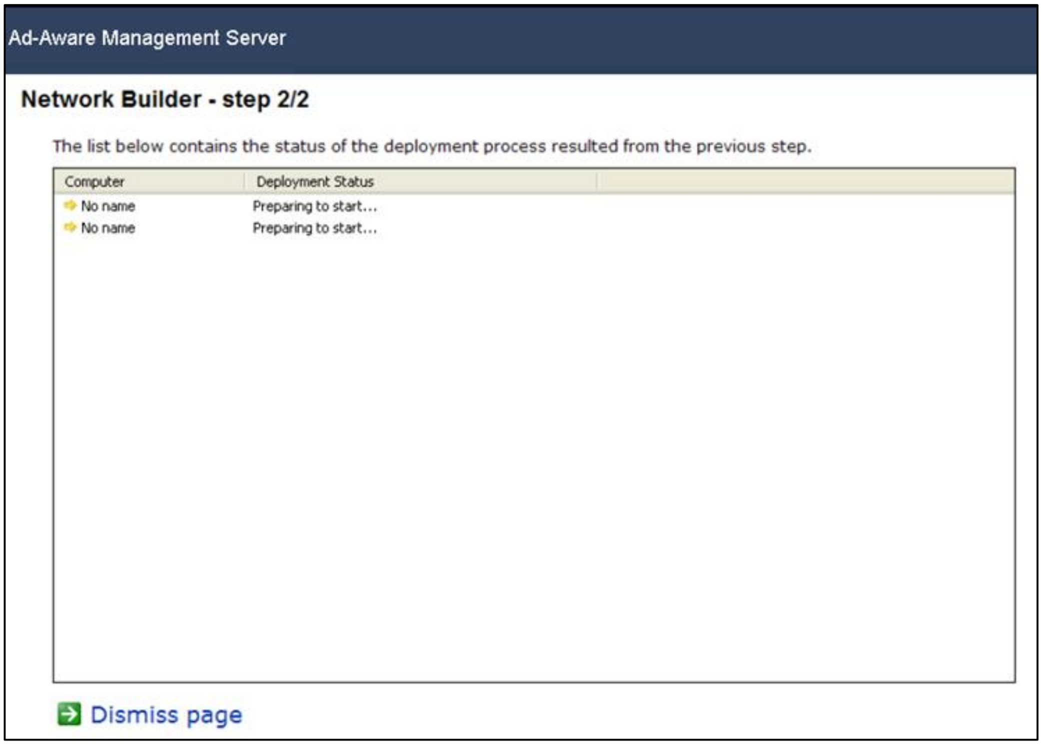
Step 5 - Provide Administrative Credentials

In order to remotely deploy Ad-Aware Management Agent, Ad-Aware Management Server requires administrative credentials to authenticate on the remote computer. Use Credentials Manager to manage these credentials. To open the Credentials Manager window, click the provided link.

Note
For more information, please refer to Credentials Manager.

Step 6 - Start Deployment

Click **Start Deployment** to initiate the deployment process. A new pane will be displayed.



Ad-Aware Management Server

Network Builder - step 2/2

The list below contains the status of the deployment process resulted from the previous step.

Computer	Deployment Status
No name	Preparing to start...
No name	Preparing to start...

Deployment Status

You can see the status of the deployment process for each computer moved into the Managed Computers group.

Click **Dismiss page** to close this pane.

Deployment Tool

Deployment Tool helps you automatically install, remove or repair Ad-Aware products on remote network computers. This tool also enables you to create unattended installation packages for use on offline computers (or when remote installation fails).

You will need to use *Deployment Tool* in the following situations:

- To remotely deploy Ad-Aware Management Agent (or an Ad-Aware client product) on the network computers that are not automatically detected by Ad-Aware Management Server

  Note
  Only the computers in the same broadcast domain as the Ad-Aware Management Server computer are automatically detected.

- To automatically repair or remove Ad-Aware Management Agent or Ad-Aware client products installed on remote network computers
- To create unattended installation packages which will be used to install Ad-Aware Management Agent and Ad-Aware client products on offline computers (or when remote installation fails)

Launching Deployment Tool

You can launch Deployment Tool in one of the following ways:

- Open the management console click **Tools** and then **Deployment Tool** on the menu.
- On the Windows Start menu, follow the path: **Start** - **Programs** - Ad-Aware Management Server **- Ad-Aware Deployment Tool**.

A wizard will appear and guide you through the deployment process.

Note
The wizard steps and use instructions of Deployment Tool will be discussed in the following sections.

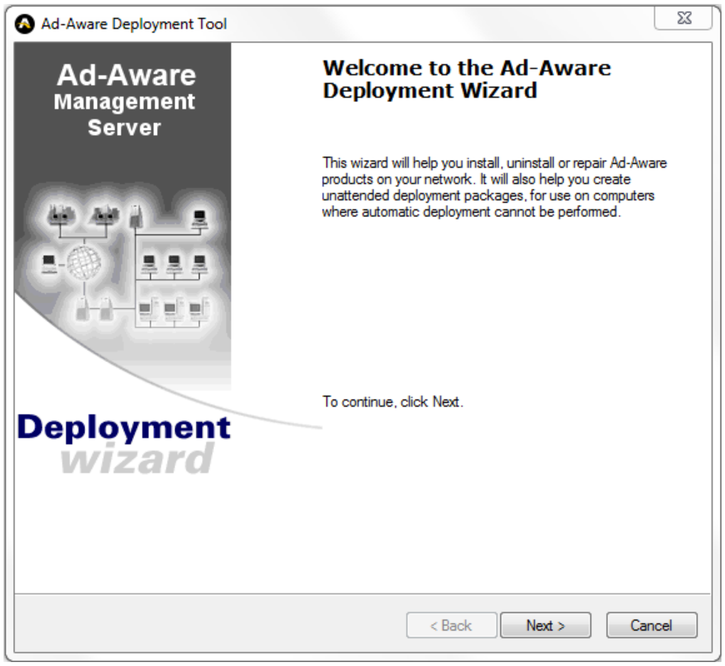
Automatically Installing, Repairing or Removing Products

To automatically install, remove or repair Ad-Aware products on remote network computers, launch Deployment Tool and follow the wizard steps.

Note
You must choose Automatically Install / Uninstall / Repair a product in the second step of the wizard.

Step 1/8 - Welcome Window

When you launch Deployment Tool, a welcome window will appear.


Ad-Aware Deployment Tool

Welcome to the Ad-Aware Deployment Wizard

This wizard will help you install, uninstall or repair Ad-Aware products on your network. It will also help you create unattended deployment packages, for use on computers where automatic deployment cannot be performed.

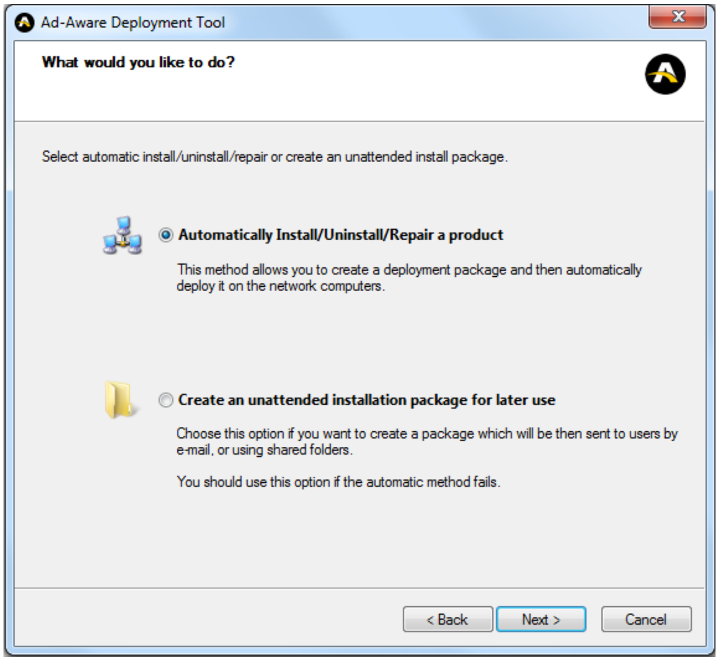
To continue, click Next.

Welcome Window

Click **Next.** A new window will appear.

Step 2/8 - Select Deployment Method

This window allows you to select the deployment method you want to use.


Ad-Aware Deployment Tool

What would you like to do?

Select automatic install/uninstall/repair or create an unattended install package.

● **Automatically Install/Uninstall/Repair a product**

This method allows you to create a deployment package and then automatically deploy it on the network computers.

○ **Create an unattended installation package for later use**

Choose this option if you want to create a package which will be then sent to users by e-mail, or using shared folders.

You should use this option if the automatic method fails.

Deployment Method

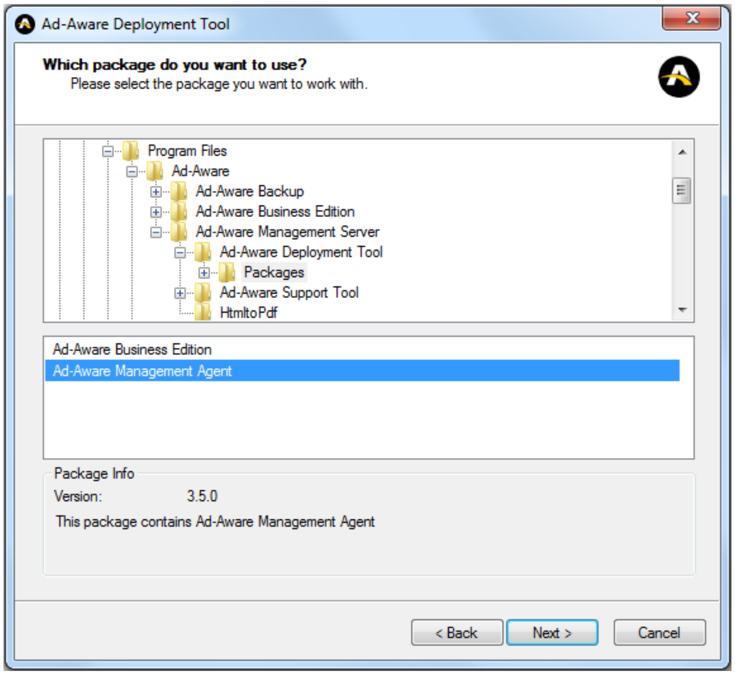
The following options are available:

- **Automatically Install / Uninstall / Repair a product** - to automatically install, remove or repair Ad-Aware products on remote network computers.
- **Create an unattended installation package for later use** - to create an installation package which can be used to manually install Ad-Aware Management Agent or the Ad-Aware client products.

Select the first option and click **Next**. A new window will appear.

Step 3/8 - Select Package

This window allows you to select the package you want to use.



Ad-Aware Deployment Tool

Which package do you want to use?
Please select the package you want to work with.

Ad-Aware Business Edition
Ad-Aware Management Agent

Package Info
Version: 3.5.0
This package contains Ad-Aware Management Agent

Packages

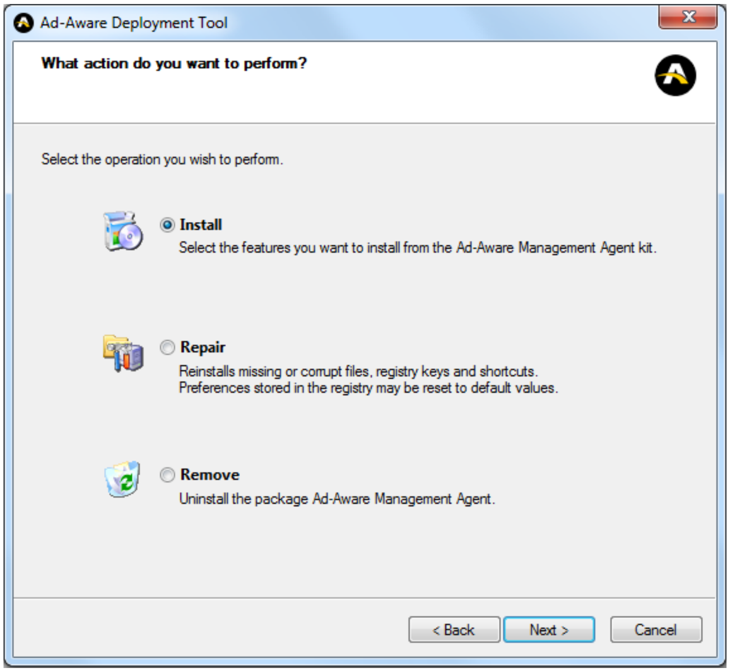
You can see the list of available installation packages:

- **Ad-Aware Business Client**
- **Ad-Aware Management Agent**
- **Ad-Aware Security for Windows Servers** (only available if the corresponding add-on is installed)

Select the package you want to use and click **Next**. A new window will appear.

Step 4/8 - Select Operation

This window allows you to select what operation to perform.



What action do you want to perform?

Select the operation you wish to perform.

● Install
Select the features you want to install from the Ad-Aware Management Agent kit.

○ Repair
Reinstalls missing or corrupt files, registry keys and shortcuts.
Preferences stored in the registry may be reset to default values.

○ Remove
Uninstall the package Ad-Aware Management Agent.

Operations

You can choose to automatically install, repair or remove the previously selected package on remote network computers.

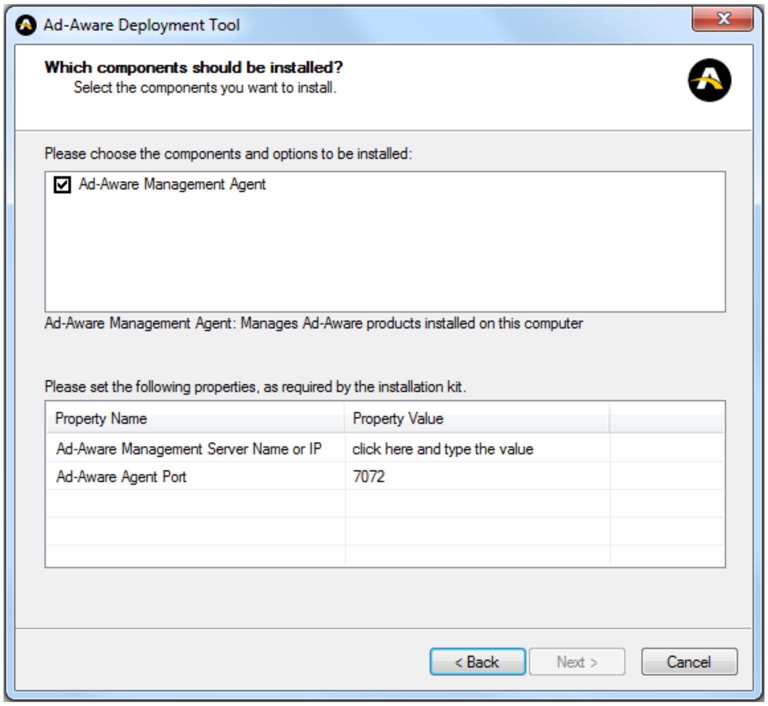
Note

If you choose Repair or Remove, you will skip the next step.

Select the operation you want to perform and click **Next**. A new window will appear.

Step 5/8 - Configure Package

This window allows you to specify which package components to install and package-specific installation settings.



Ad-Aware Deployment Tool

Which components should be installed?

Select the components you want to install.

Please choose the components and options to be installed:

☑ Ad-Aware Management Agent

Ad-Aware Management Agent: Manages Ad-Aware products installed on this computer

Please set the following properties, as required by the installation kit.

Property Name	Property Value
Ad-Aware Management Server Name or IP	click here and type the value
Ad-Aware Agent Port	7072

Package Components

Depending on the installation package selected, you may have to provide package-specific installation information. You can see the required information, if any, in the lower part of the window.

Ad-Aware Business Client

If you have selected to install Ad-Aware Business Client, you must set the following properties:

- **Scan computer for malware before installation**... - select the corresponding check box if you want to scan the target computer for malware before installing the program. If the target computer is infected, the infecting malware may block or corrupt the Ad-Aware Business Client installation.
- **Client Mode** - set the user privileges by choosing an appropriate option from the menu.
  - In the restricted user mode, the user cannot configure the product, but only perform basic tasks, such as launching a default scan task, updating Ad-Aware or backing up data. This is the recommended setting.
  - In the power user mode, the user has full control over Ad-Aware Business Client.
- **Components** - configure the installation options of the main components of Ad-Aware Business Client (Antivirus, Firewall, Anti-spam, Privacy Control, Anti-phishing, User Control, Update, Backup).
  - The Antivirus and Update components will be installed automatically. Select the **Enabled** check box if you want any of these components to be enabled.
  - If you want the Backup component to be available in the user interface, select the Active check box.
  - For the other components, choose the appropriate option from the menu:

Action	Description
Active and Enabled	The component will be installed and it will be enabled at installation time.

Active and Disabled	The component will be installed, but it will be kept disabled.
Inactive	The component will not be installed.

- **Administrative password** - type an administrative password to protect the program from unauthorized access. Users will have to provide this password in order to change the program settings or to remove the program. You must confirm the password in the **Re-type administrative password** field.

Ad-Aware Management Agent

If you have selected to install Ad-Aware Management Agent, you must set the following properties:

- **Ad-Aware Management Server Name or IP** - type the name or the IP address of the Ad-Aware Management Server in the corresponding field. If the Ad-Aware Management Server computer does not respond to ping, you will be prompted to confirm that it is connected to the network.

Important

Ad-Aware Management Agent communicates with Ad-Aware Management Server using either the IP address or the name of the computer Ad-Aware Management Server is installed on. To prevent communication issues, configure the management server identity as follows:

- If the IP address of the Ad-Aware Management Server computer does not change in time (static or reserved IP address), type the IP address.
- Otherwise, if the IP address is dynamically assigned by DHCP (no MAC address-based IP reservation), type the computer name.

- **Ad-Aware Management Agent Port** - type the communication port used by the Ad-Aware Management Agent in the corresponding field. By default, the port set during the installation of Ad-Aware Management Server is used automatically.

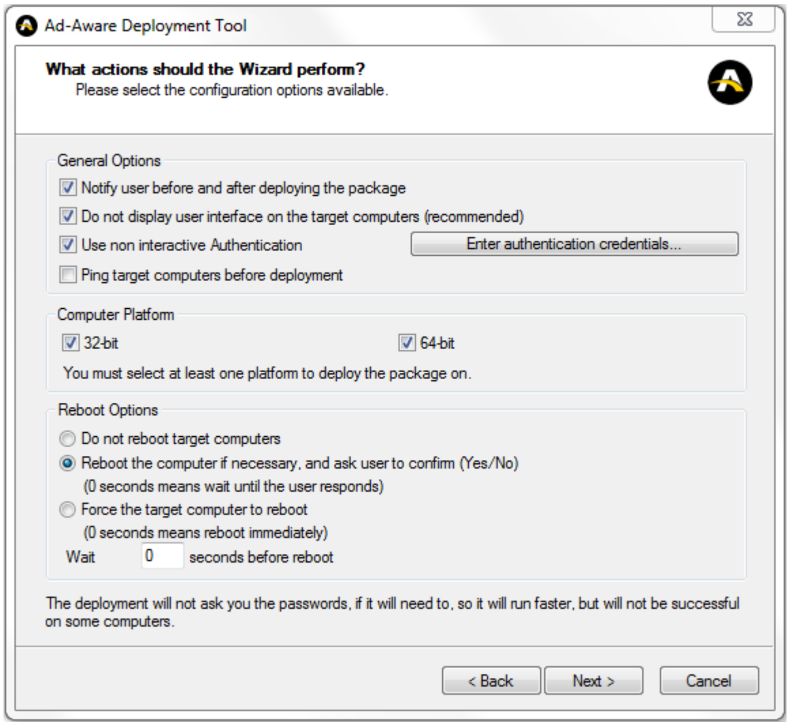
Ad-Aware Security for Windows Servers

If you have selected to install Ad-Aware Security for Windows Servers, select the check boxes corresponding to the specific security solutions that you want to install.

Click **Next**. A new window will appear.

Step 6/8 - Configure Deployment Options

This window allows you to configure the deployment options.



Ad-Aware Deployment Tool

What actions should the Wizard perform?
Please select the configuration options available.

General Options
☑ Notify user before and after deploying the package
☑ Do not display user interface on the target computers (recommended)
☑ Use non interactive Authentication [Enter authentication credentials...]
☐ Ping target computers before deployment

Computer Platform
☑ 32-bit ☑ 64-bit
You must select at least one platform to deploy the package on.

Reboot Options
○ Do not reboot target computers
● Reboot the computer if necessary, and ask user to confirm (Yes/No)
(0 seconds means wait until the user responds)
○ Force the target computer to reboot
(0 seconds means reboot immediately)
Wait 0 seconds before reboot

The deployment will not ask you the passwords, if it will need to, so it will run faster, but will not be successful on some computers.

Deployment Options

The deployment options are grouped into two categories:

General Options

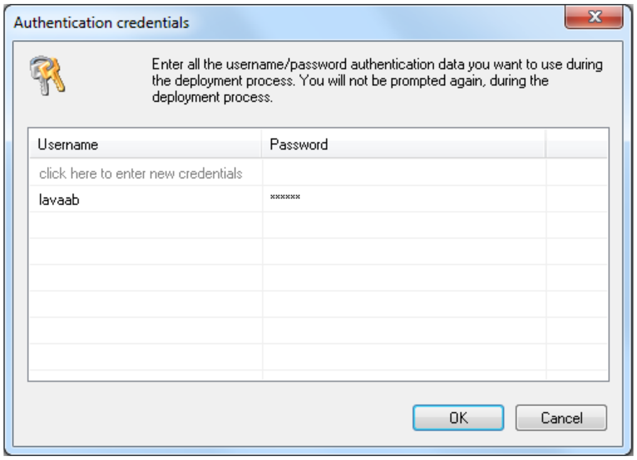
The options in the **General Options** category allow you to specify the deployment behavior on the target computers. You can select:

- **Notify user before and after deploying the package** - to alert the user logged on the target computers about the deployment process. Two dialogs will appear on the user's screen, before and after the deployment process.
- **Do not display user interface on the target computers (recommended)** – to install the package silently in the background. The Windows Installer interface will not be displayed on target computers.
- **Use non interactive Authentication** - to provide the administrative credentials (username and password) that will be used to authenticate on the target computers. For the network computers that are within an Active Directory domain, you will only have to provide the credentials of the domain administrator.

Important

If you do not provide the authentication credentials now, you will have to provide them separately for each target computer during the deployment. Therefore, using this option may save you time.
Reboot Options

To provide the credentials, click **Enter authentication credentials**. A new window will appear.
Type the usernames required for authentication and their respective passwords in the corresponding fields.
Click **OK**. The provided credentials are saved automatically for future deployments.


Authentication credentials

Enter all the username/password authentication data you want to use during the deployment process. You will not be prompted again, during the deployment process.

Username	Password
click here to enter new credentials	
lavaab	******

Credentials

- **Ping target computers before deployment** - to check, before starting the deployment, if the target computers respond to ping requests. If the ping to a target computer fails, a message in the deployment status column will indicate that the computer is disconnected. The deployment on that computer will be cancelled. For such computers, you will have to reinitiate deployment at a later time or to clear this check box before starting the deployment.

Note
The ping may fail for other reasons. For example, the firewall installed on the target computer may prevent the computer from responding to ping.

Computer Platform

The options in the **Computer Platform** category allow you to specify the target computer platforms. If you do not want to deploy the package on a particular platform (either 32-bit or 64-bit) clear the corresponding check box.

Reboot Options

Usually, after the deployment is completed, the target computers must be restarted. The options in the **Reboot Options** category allow you to specify how to restart the target computers. If you select:

- **Do not reboot target computers** - the target computers will not be restarted, even if necessary. Ad-Aware will wait for a user to restart them.
- **Reboot the computer if necessary, and ask the user to confirm** - the user will be prompted to restart the computer, if necessary. If no user response is received within the specified time interval, the computer is automatically restarted. To specify the time interval until restart, type the number of seconds in the edit field.

Note
By default, the target computers will be automatically restarted after 30 seconds.

- **Force the target computer to reboot** - the target computers will be restarted after the specified time interval. To specify the time interval until restart, type the number of seconds in the edit field. If you want to restart the target computers immediately, type 0.

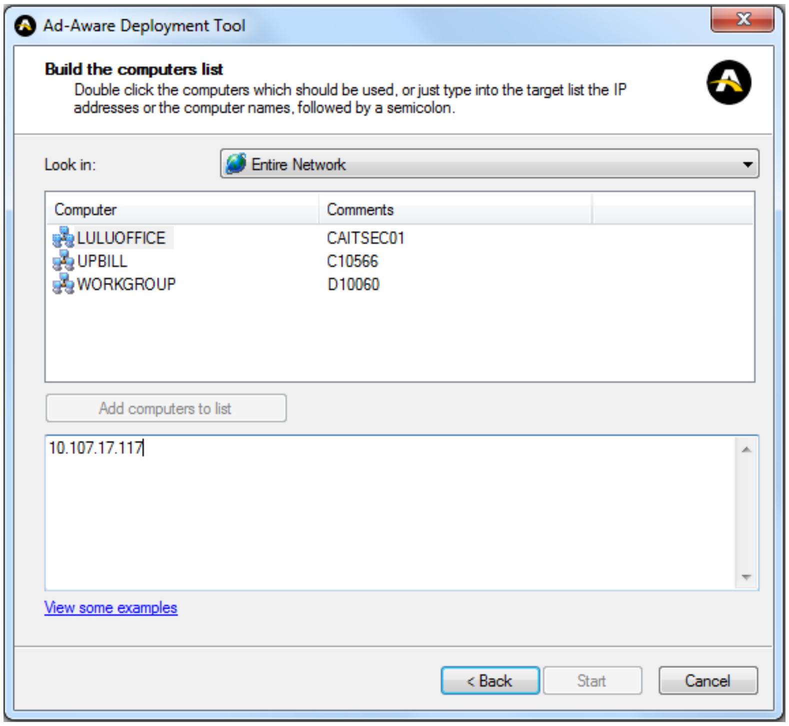
Note

By default, the target computers will be automatically restarted after 30 seconds.

Click **Next**. A new window will appear.

Step 7/8 - Save Installation Package

This window allows you to specify the computers on which the package will be deployed.



Ad-Aware Deployment Tool

Build the computers list

Double click the computers which should be used, or just type into the target list the IP addresses or the computer names, followed by a semicolon.

Look in: Entire Network

Computer	Comments
LULUOFFICE	CAITSEC01
UPBILL	C10566
WORKGROUP	D10060

10.107.17.117

Target Computers

You can easily browse the entire **Microsoft Windows Network** and see all domains and workgroups in your network.

To specify the target computers, use one the following methods:

- **Browse the network to find target computers**. You must follow the next steps:
  1. Double-click a domain or workgroup in the **Entire Network** list (or select it from the menu) to see the computers it contains.
  2. Double-click the computers you want to add to the target list (or select them and click **Add computers to list**).

  Note

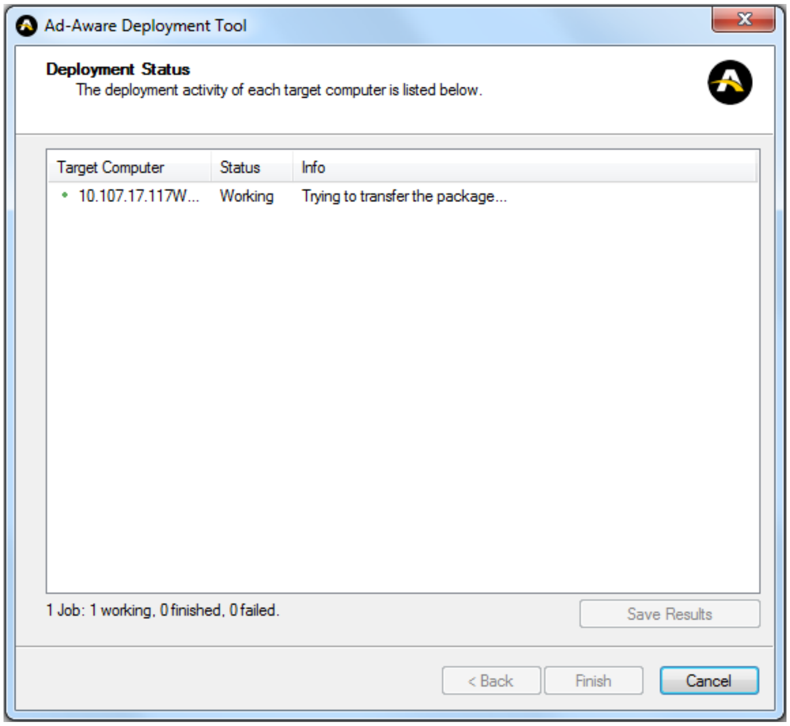
  To select all computers in the list, click one of them and then press CTRL+A.

- **Type the name or IP address of the target computers directly into the target list, separated by semicolons ";"**.
- To learn about the syntax you must use, click **View some examples**. A new window will appear providing you with examples of valid and wrong syntax.

Click **Start** to initiate the deployment process. A new window will appear.

Step 8/8 – View Deployment Status

This window shows you the deployment status.



Deployment Status

The deployment activity of each target computer is listed below.

Target Computer	Status	Info
10.107.17.117W...	Working	Trying to transfer the package...

1 Job: 1 working, 0 finished, 0 failed.

Results

You can see the deployment status on each target computer. Wait until all deployment processes are finished.

You may be prompted to provide authentication credentials for part or all of the target computers (if you have not provided them when configuring the deployment options).

Type in the corresponding fields the username and password of an administrative user account to authenticate on the target computer. Click **OK** to continue the deployment.

If you do not provide the required credentials within 60 seconds, the deployment on that computer will fail.

Note

If the deployment process fails, you can see the returned error message explained in detail.

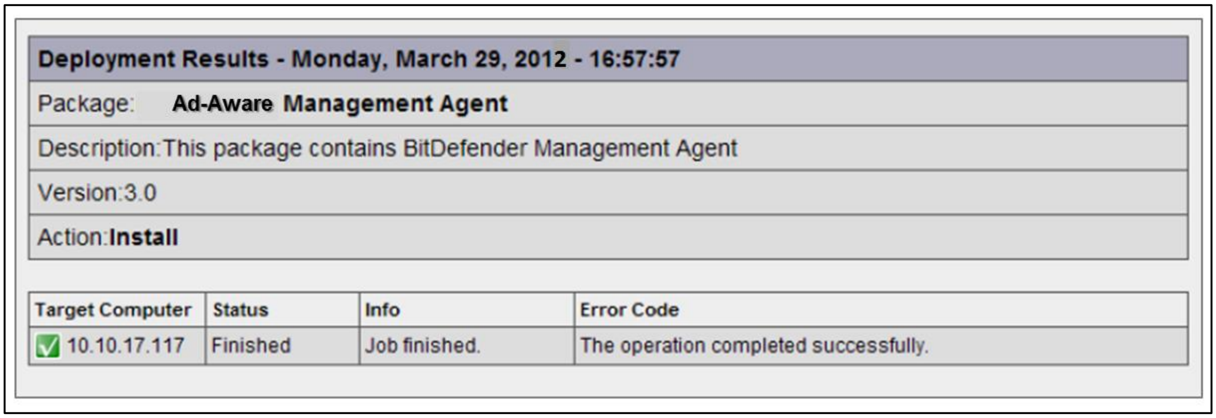
If you want to save the results in a `HTML` or a `txt` file, click **Save Results**.
Click **Finish** to close the window.

Examining Deployment Results

You can easily examine the results of the automatic deployment performed on the remote computers. You just have to save them in a HTML or a txt file in the last step of the wizard.

Note
This is very useful when troubleshooting errors that occurred during deployment.

The following picture presents the deployment results saved in HTML format:



Deployment Results - Monday, March 29, 2012 - 16:57:57
Package: **Ad-Aware Management Agent**
Description:This package contains BitDefender Management Agent
Version:3.0
Action:**Install**

Target Computer	**Status**	**Info**	**Error Code**
✓ 10.10.17.117	Finished	Job finished.	The operation completed successfully.

Deployment Results in HTML Format

You can see:

- when the operation was performed
- information about the deployed package
- what operation was performed
- the status of and additional information on the deployment process for each target computer, as well as detailed information about the error, if any

Creating Unattended Installation Packages

The unattended installation packages enable you to install Ad-Aware Management Agent or Ad-Aware client products on offline computers (or when remote installation fails).

An unattended installation package is an executable archive (an installer) which contains:

- the installation package of Ad-Aware Management Agent or of an Ad-Aware client product
- the installation settings, which specify:
  - what product components to be installed
  - the product-related installation settings, if any
  - how to interact with the user during installation
  - the reboot procedure after the installation is completed

You can do one of the following with this package:

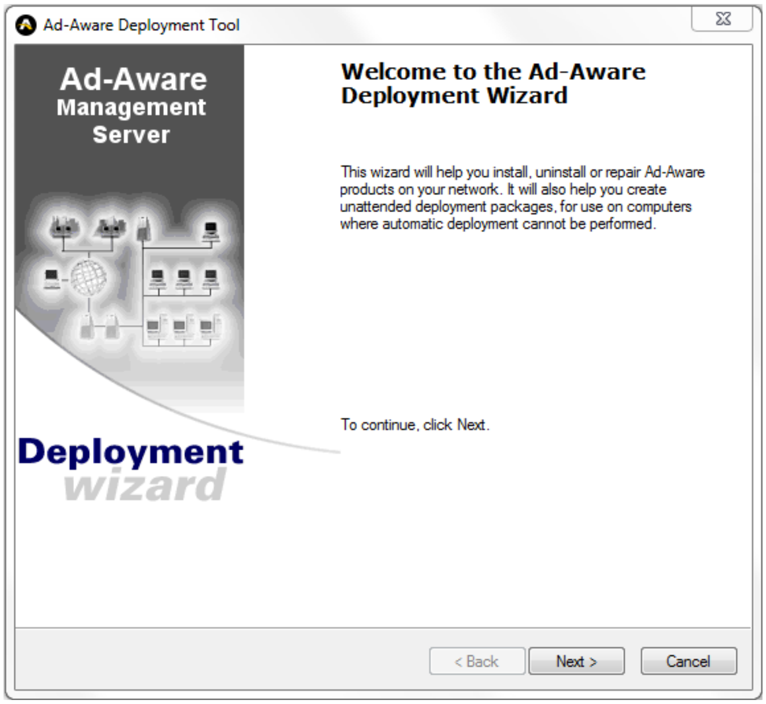
- Put it on a removable storage device (CD, DVD, USB stick) and then copy it on network computers
- Send it by e-mail to a certain user
- Transfer it in a shared folder, so that it can be read from any other workstation
- Use a logon script to automatically install it after the login procedure

To create an unattended installation package, launch Deployment Tool and follow the wizard steps.

Note
You must choose **Create an unattended installation package for later use** in the second step of the wizard.

Step 1/7 - Welcome Window

When you launch Deployment Tool, a welcome window will appear.



Welcome to the Ad-Aware Deployment Wizard

This wizard will help you install, uninstall or repair Ad-Aware products on your network. It will also help you create unattended deployment packages, for use on computers where automatic deployment cannot be performed.

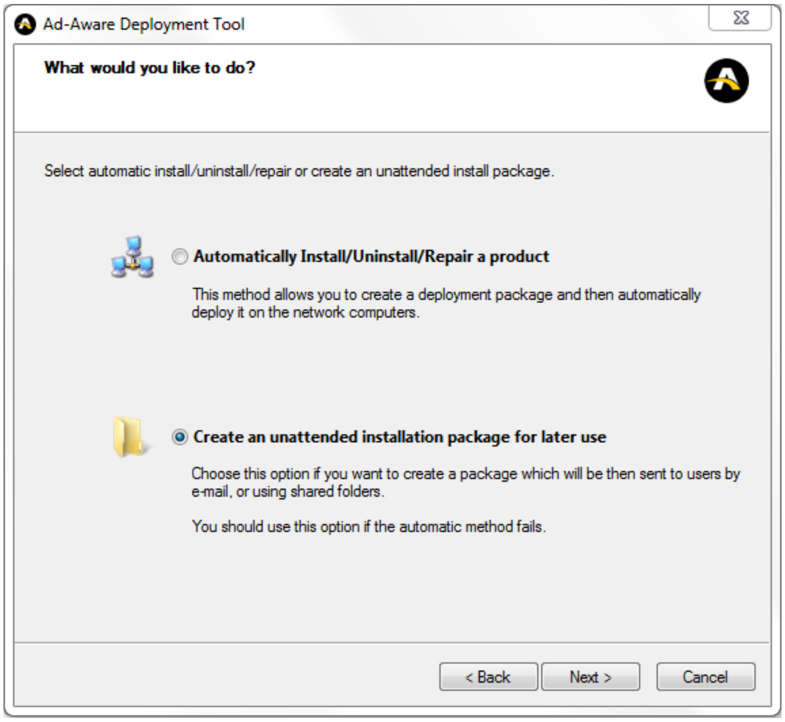
To continue, click Next.

Welcome Window

Click **Next**. A new window will appear.

Step 2/7 - Select Deployment Method

This window allows you to select the deployment method you want to use.



Ad-Aware Deployment Tool

What would you like to do?

Select automatic install/uninstall/repair or create an unattended install package.

○ **Automatically Install/Uninstall/Repair a product**

This method allows you to create a deployment package and then automatically deploy it on the network computers.

● **Create an unattended installation package for later use**

Choose this option if you want to create a package which will be then sent to users by e-mail, or using shared folders.

You should use this option if the automatic method fails.

Deployment Method

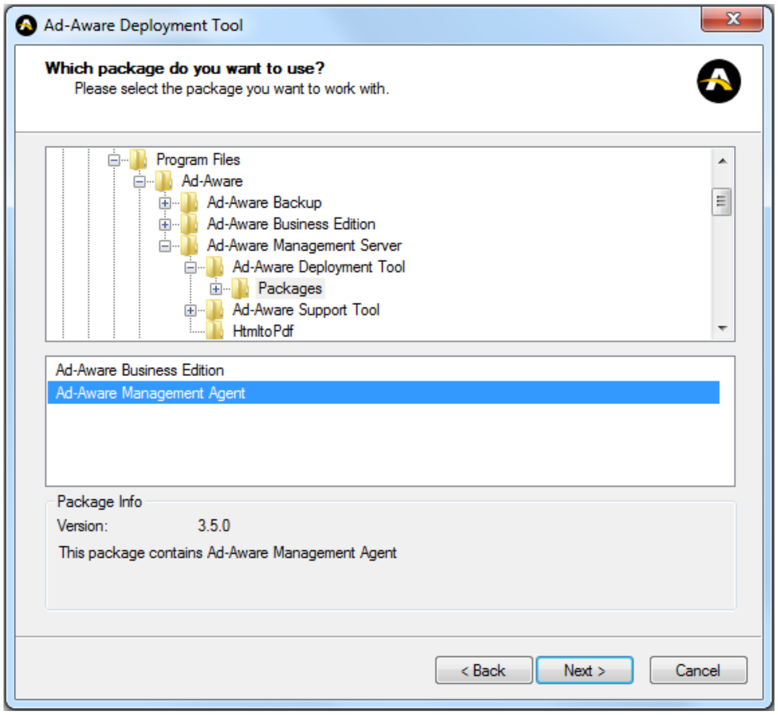
The following options are available:

- **Automatically Install / Uninstall / Repair a product** - to automatically install, remove or repair Ad-Aware products on remote network computers.
- **Create an unattended installation package for later use** - to create an installation package which can be used to manually install Ad-Aware Management Agent or the Ad-Aware client products.

Select the second option and click **Next**. A new window will appear.

Step 3/7 - Select Package

This window allows you to select the package you want to use.



Ad-Aware Deployment Tool

Which package do you want to use?

Please select the package you want to work with.

Ad-Aware Business Edition

Ad-Aware Management Agent

Package Info

Version: 3.5.0

This package contains Ad-Aware Management Agent

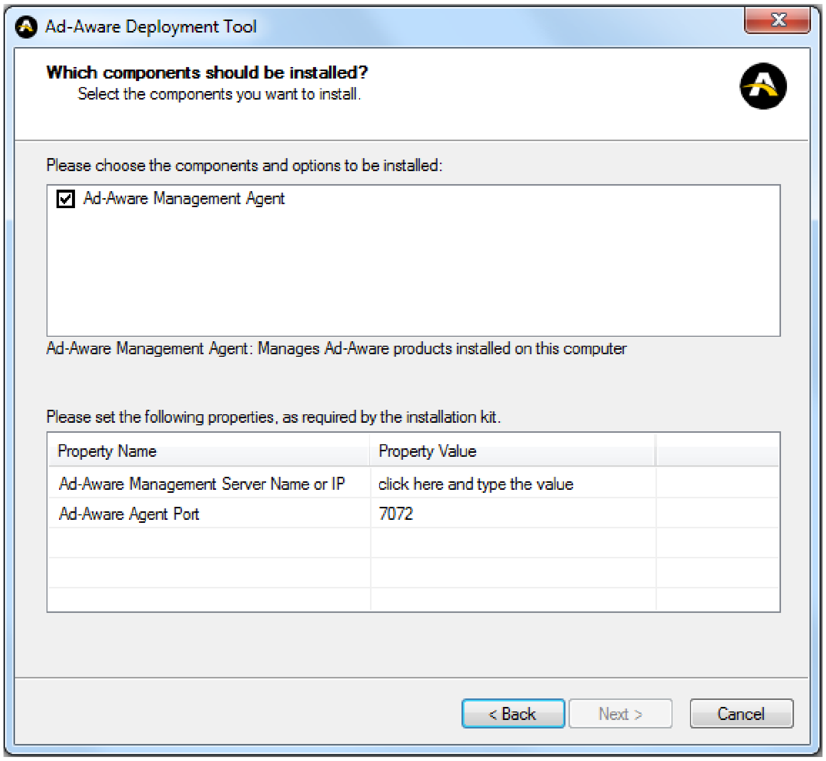
Packages

- **Ad-Aware Business Client**
- **Ad-Aware Management Agent**
- **Ad-Aware Security for Windows Servers** (only available if the corresponding add-on is installed)

Select the package you want to use and click **Next**. A new window will appear.

Step 4/7 - Configure Package

This window allows you to specify which package components to install and package-specific installation settings.



Ad-Aware Deployment Tool

Which components should be installed?
Select the components you want to install.

Please choose the components and options to be installed:

☑ Ad-Aware Management Agent

Ad-Aware Management Agent: Manages Ad-Aware products installed on this computer

Please set the following properties, as required by the installation kit.

Property Name	Property Value
Ad-Aware Management Server Name or IP	click here and type the value
Ad-Aware Agent Port	7072

Package Components

Depending on the installation package selected, you may have to provide package-specific installation information. You can see the required information, if any, in the lower part of the window.

Ad-Aware Business Client

If you have selected to install Ad-Aware Business Client, you must set the following properties:

- **Scan computer for malware before installation**... - select the corresponding check box if you want to scan the target computer for malware before installing the program. If the target computer is infected, the infecting malware may block or corrupt the Ad-Aware Business Client installation.
- **Client Mode** - set the user privileges by choosing an appropriate option from the menu.
  - In the restricted user mode, the user cannot configure the product, but only perform basic tasks, such as launching a default scan task, updating Ad-Aware or backing up data. This is the recommended setting.
  - In the power user mode, the user has full control over Ad-Aware Business Client.
- **Components** - configure the installation options of the main components of Ad-Aware Business Client (Antivirus, Firewall, Antispam, Privacy Control, Antiphishing, User Control, Update, Backup).
  - The Antivirus and Update components will be installed automatically. Select the **Enabled** check box if you want any of these components to be enabled.
  - If you want the Backup component to be available in the user interface, select the **Active** check box.
  - For the other components, choose the appropriate option from the menu:

Action	Description
Active and Enabled	The component will be installed and it will be enabled at installation time.
Active and Disabled	The component will be installed, but it will be kept disabled.
Inactive	The component will not be installed.

- **Administrative password** - type an administrative password to protect the program from unauthorized access. Users will have to provide this password in order to change the program settings or to remove the program. You must confirm the password in the Re-type administrative password field.

Ad-Aware Management Agent

If you have selected to install Ad-Aware Management Agent, you must set the following properties:

- Ad-Aware Management Server Name or IP - type the name or the IP address of the Ad-Aware Management Server in the corresponding field. If the Ad-Aware Management Server computer does not respond to ping, you will be prompted to confirm that it is connected to the network.

> **Important**
>
> Ad-Aware Management Agent communicates with Ad-Aware Management Server using either the IP address or the name of the computer Ad-Aware Management Server is installed on. To prevent communication issues, configure the management server identity as follows:
>
> - If the IP address of the Ad-Aware Management Server computer does not change in time (static or reserved IP address), type the IP address.
> - Otherwise, if the IP address is dynamically assigned by DHCP (no MAC address-based IP reservation), type the computer name.

- Ad-Aware Management Agent Port - type the communication port used by the Ad-Aware Management Agent in the corresponding field. By default, the port set during the installation of Ad-Aware Management Server is used automatically.

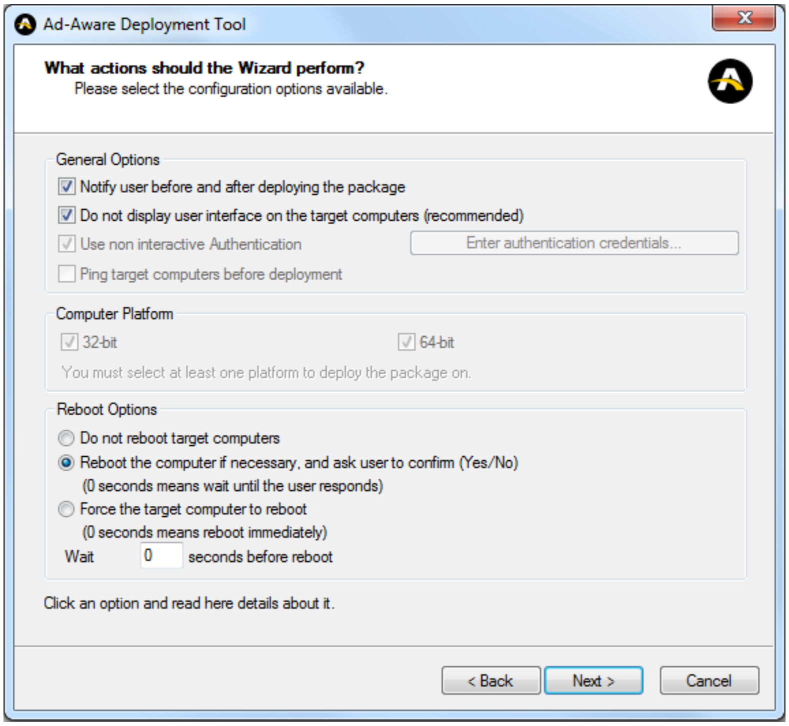
Ad-Aware Security for Windows Servers

If you have selected to install Ad-Aware Security for Windows Servers, select the check boxes corresponding to the specific security solutions that you want to install.

Click **Next**. A new window will appear.

Step 5/7 - Configure Deployment Options

This window allows you to configure the deployment options.



Ad-Aware Deployment Tool

What actions should the Wizard perform?
Please select the configuration options available.

General Options

☑ Notify user before and after deploying the package
☑ Do not display user interface on the target computers (recommended)
☑ Use non interactive Authentication
□ Ping target computers before deployment

Computer Platform

☑ 32-bit ☑ 64-bit
You must select at least one platform to deploy the package on.

Reboot Options

○ Do not reboot target computers
● Reboot the computer if necessary, and ask user to confirm (Yes/No)
(0 seconds means wait until the user responds)
○ Force the target computer to reboot
(0 seconds means reboot immediately)
Wait 0 seconds before reboot

Click an option and read here details about it.

Deployment Options

The deployment options are grouped into two categories:

General Options

The options in the **General Options** category allow you to specify the deployment behavior on the target computers. You can select:

- **Notify user before and after deploying the package** - to alert the user logged on the target computers about the deployment process. Two dialogs will appear on the user's screen, before and after the deployment process.
- **Do not display user interface on the target computers** (recommended) – to install the package silently in the background. The Windows Installer interface will not be displayed on target computers.

Reboot Options

Usually, after the deployment is completed, the target computers must be restarted.

The options in the **Reboot Options** category allow you to specify how to restart the target computers. If you select:

- **Do not reboot target computers** - the target computers will not be restarted, even if necessary. Ad-Aware will wait for a user to restart them.
- **Reboot the computer if necessary, and ask the user to confirm** - the user will be prompted to restart the computer, if necessary. If no user response is received within the specified time interval, the computer is automatically restarted. To specify the time interval until restart, type the number of seconds in the edit field.

Note

By default, the target computers will be automatically restarted after 30 seconds.

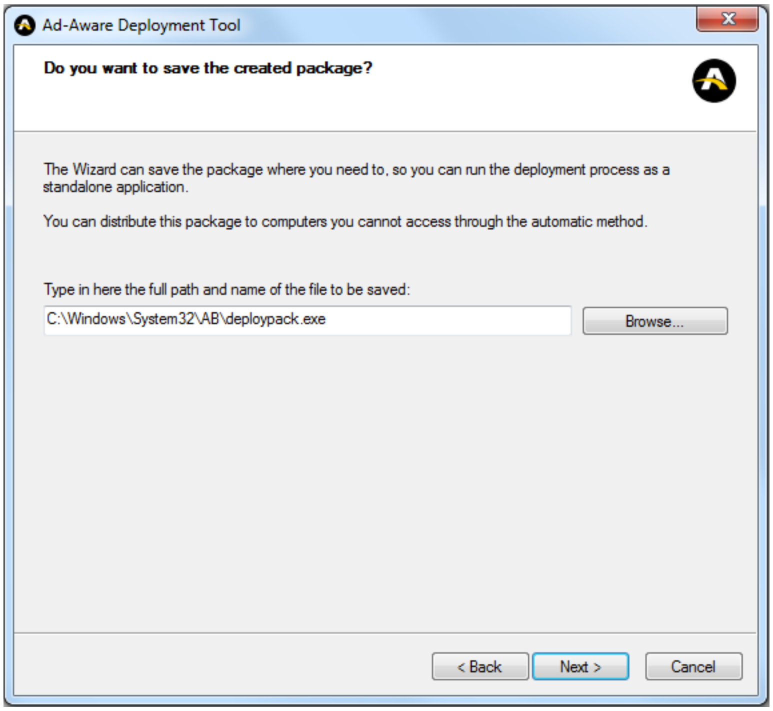
- **Force the target computer to reboot** - the target computers will be restarted after the specified time interval. To specify the time interval until restart, type the number of seconds in the edit field. If you want to restart the target computers immediately, type 0.

Note
By default, the target computers will be automatically restarted after 30 seconds.

Click **Next**. A new window will appear.

Step 6/7 - Save Installation Package

This window allows you to create and save the unattended installation package.



Do you want to save the created package?

The Wizard can save the package where you need to, so you can run the deployment process as a standalone application.

You can distribute this package to computers you cannot access through the automatic method.

Type in here the full path and name of the file to be saved:

C:\Windows\System32\AB\deploypack.exe

Saving Options

You can make any changes you want by returning to the previous steps (click Back).

To specify the package name and where to save it, follow the next steps:

1. Click **Browse**.
2. Select the location where to save the file. You can save it on the local machine or on a network share.
3. Save the file with the desired name. The default filename is deploypack.exe.

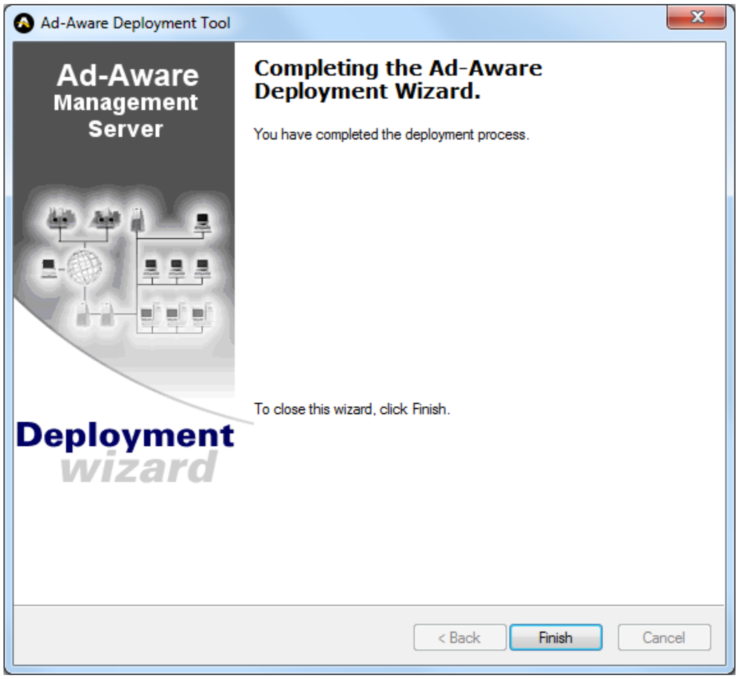
Note
We recommend that you choose an explicit filename, such as deploypack_aaagent.exe.

You can also type the full path and name of the installation package directly in the edit field.

Click **Next** to create and save the unattended installation package. A new window will appear.

Step 7/7 - Close Window

This window shows you the results.



Completing the Ad-Aware Deployment Wizard.

You have completed the deployment process.

To close this wizard, click Finish.

Results

Click **Finish** to close the window.

You can find the unattended installation package at the location where you chose to save it. Next, you will have to copy the file on the target computers and run it with administrative privileges. The installation file works both on 32-bit and 64-bit platforms.

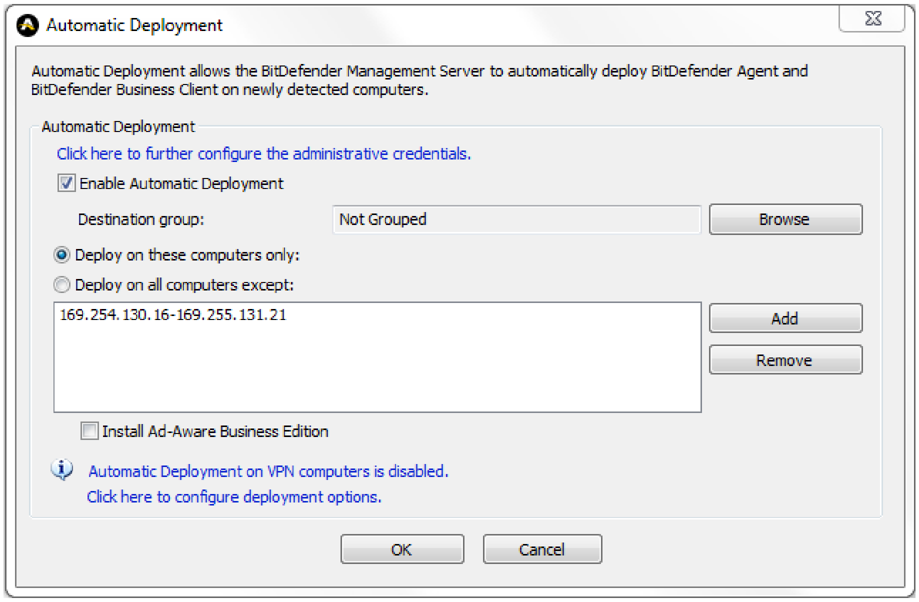
Automatic Deployment

Automatic Deployment allows Ad-Aware Management Server to automatically deploy Ad-Aware Management Agent and Ad-Aware Business Client on newly detected computers. This tool is very useful in keeping the network managed by Ad-Aware Management Server up to date with the changes in the physical network, after the initial deployment and configuration.

Note

By default, Automatic Deployment is disabled. Ad-Aware Management Agent will be deployed only on the computers detected after enabling Automatic Deployment.

To open the Automatic Deployment configuration window, open the management console click **Tools** and then **Automatic Deployment** on the menu.



Automatic Deployment allows the BitDefender Management Server to automatically deploy BitDefender Agent and BitDefender Business Client on newly detected computers.

Automatic Deployment

Click here to further configure the administrative credentials.

☑ Enable Automatic Deployment

Destination group: Not Grouped

● Deploy on these computers only:

○ Deploy on all computers except:

169.254.130.16-169.255.131.21

□ Install Ad-Aware Business Edition

Automatic Deployment on VPN computers is disabled.
Click here to configure deployment options.

Automatic Deployment

Here you can find the following information:

- If Automatic Deployment is enabled.
- The IP addresses of the computers on which Ad-Aware Management Agent can be deployed or, on the contrary, those expressly excepted from the management of Ad-Aware Management Server.
- If Ad-Aware Business Client is deployed along with Ad-Aware Management Agent.
- Whether automatic deployment is performed on computers in Virtual Private Networks (VPNs).

To remove IP addresses from the list, select them and click **Remove**. You will have to confirm your action by clicking **Yes**.

Configuring Automatic Deployment

In order to configure Automatic Deployment, follow the next steps:

Step 1/5 - Provide Administrative Credentials

In order to remotely deploy Ad-Aware Management Agent, Ad-Aware Management Server requires administrative credentials to authenticate on the remote computer. Use Credentials Manager to manage these credentials. To open the Credentials Manager window, click the provided link.

Note
For more information, please refer to Credentials Manager.

Step 2/5 - Enable Automatic Deployment

Check **Enable Automatic Deployment** to enable Automatic Deployment. Please note that Automatic Deployment will be immediately disabled if, later on, you delete all the authentication credentials saved by Credentials Manager.

Note

Ad-Aware Management Agent will not be automatically deployed only by enabling Automatic Deployment. You will have to follow the next configuration steps in order for Automatic Deployment to work properly.

If you also want Ad-Aware Business Client to be automatically deployed along with Ad-Aware Management Agent, check **Install Ad-Aware Business Client**.

Step 3/5 - Select Destination Group

After automatic deployment, the newly managed computers are placed in **Managed Computers>Not grouped** by default. If you want to place these computers in another group, click **Browse**, select the desired group and click **OK.**

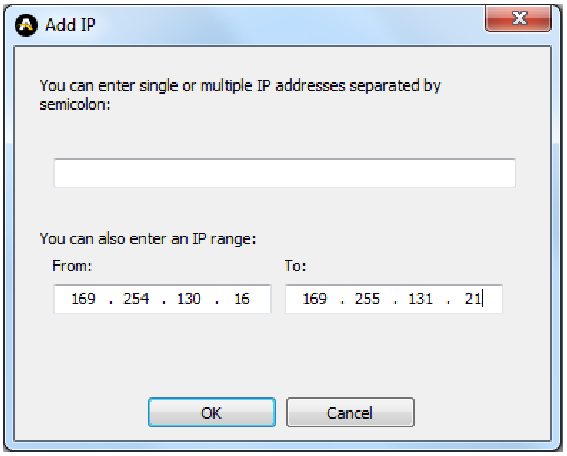
Step 4/5 - Specify Allowed or Restricted IP Addresses

You must specify the IP addresses on which Ad-Aware Management Server is allowed or not to deploy Ad-Aware Management Agent. Choose either **Deploy on these computers only** or **Deploy on all computers except** and provide the IP addresses.

Note

- If you have specific IP addresses assigned to router interfaces, management switches or some computers that you do not want to be managed by Ad-Aware Management Server, choose **Deploy on all computers except** and provide the excepted IP addresses.
- If you have a range of IP addresses assigned to computers that you want to be managed by Ad-Aware Management Server, choose Deploy on these computers only and provide these IP addresses.

To add IP addresses, click **Add**. A new window will appear.



Add IP

You can enter single or multiple IP addresses separated by semicolon:

You can also enter an IP range:

From: 169 . 254 . 130 . 16

To: 169 . 255 . 131 . 21

Add IP addresses

Type the IP addresses in the upper edit field, separating them by semicolons (";"). If you want to add a range of IP addresses, type the lower and upper range limit in the corresponding fields.

Click **OK** to save the changes and close the window.

Step 5/5 - Save Changes

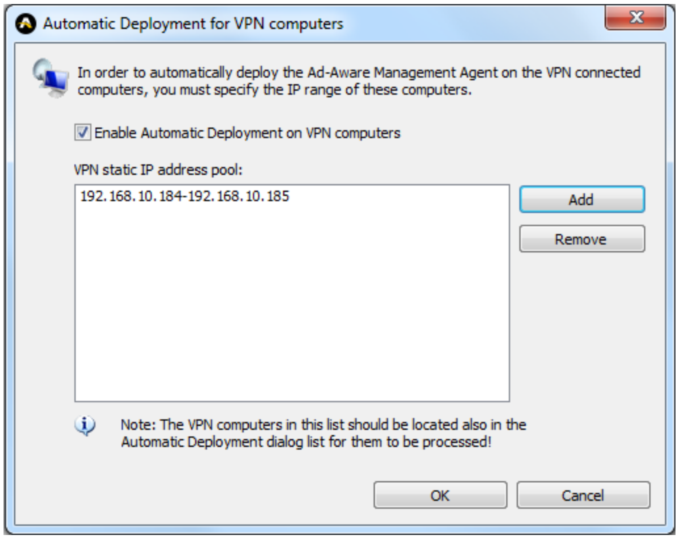
Click **OK** to save the changes and close the window.

Configuring Automatic Deployment for VPN Computers

To configure automatic deployment for VPN computers, follow these steps:

1. Configure Automatic Deployment.

2. Click the link that informs you about the automatic deployment on VPN computers. A new configuration window will appear.



Automatic Deployment for VPN computers

In order to automatically deploy the Ad-Aware Management Agent on the VPN connected computers, you must specify the IP range of these computers.

☑ Enable Automatic Deployment on VPN computers

VPN static IP address pool:

192.168.10.184-192.168.10.185

Note: The VPN computers in this list should be located also in the Automatic Deployment dialog list for them to be processed!

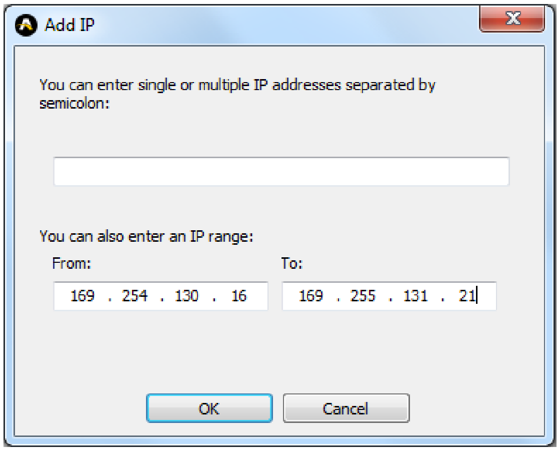
Automatic Deployment for VPN Compute

3. Select Enable Automatic Deployment on VPN computers.

4. Specify the IP addresses belonging to the VPN computers.

Important
In order to perform automatic deployment on the specified VPN computers, their IP addresses must be either explicitly allowed or not restricted in the Automatic Deployment configuration window.

- To add IP addresses to the list, click Add. A new window will appear.



You can enter single or multiple IP addresses separated by semicolon:

You can also enter an IP range:

From: 169 . 254 . 130 . 16

To: 169 . 255 . 131 . 21

Add IP addresses

Type the IP addresses in the upper edit field, separating them by semicolons (";"). If you want to add a range of IP addresses, type the lower and upper range limit in the corresponding fields.

Click **OK** to add the specified IP addresses to the list.

- To remove an entry from the list, select it and click **Remove**.

5. Click **OK** to save the changes and close the window.

Deploying Ad-Aware Business Client Automatically

By default, when Automatic Deployment is enabled, only Ad-Aware Management Agent is automatically deployed. If you also want Ad-Aware Business Client to be automatically deployed along with Ad-Aware Management Agent, check **Install Ad-Aware Business Client**.

Important

Make sure that the IP addresses configured for automatic deployment are not assigned to file servers or mail servers. Ad-Aware Business Client is designed to protect only user workstations and must not be installed on servers.

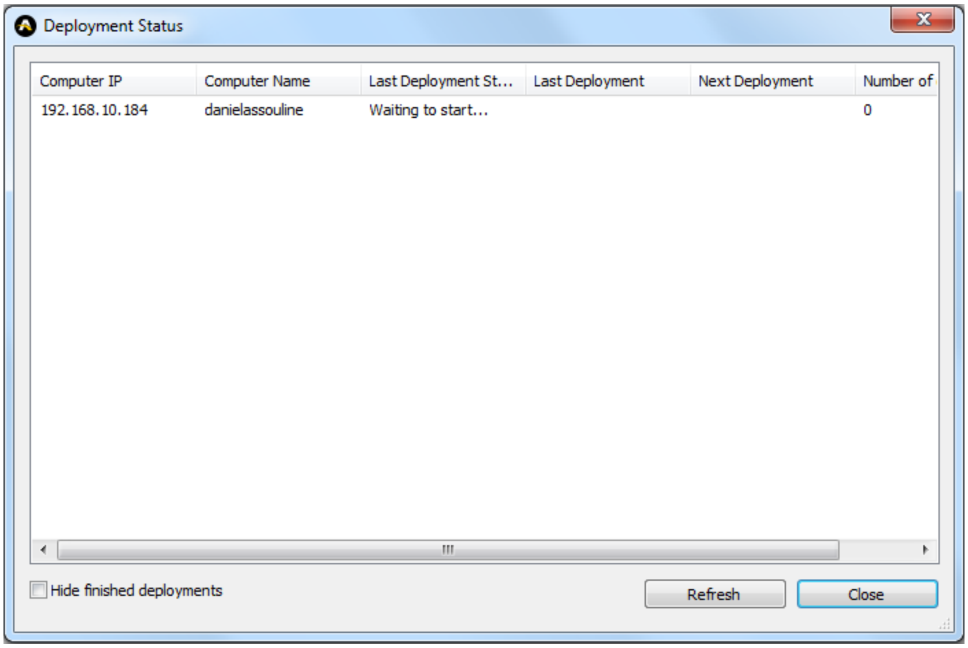
Click **OK** to save the changes and close the window.

Disabling Automatic Deployment

To disable Automatic Deployment, just clear the check box corresponding to **Enable Automatic Deployment**. Click **OK** to save the changes and close the window.

View Deployment Status

To view the status information of all the deployments initiated, click Tools in the management console and then View Deployment Status on the menu. A new window will appear.



Computer IP	Computer Name	Last Deployment St...	Last Deployment	Next Deployment	Number of
192.168.10.184	danielassouline	Waiting to start...			0

Deployment Status

You can see all the deployments initiated so far. The table provides useful information about the deployment:

- The IP address and the name of the computer on which the deployment has been or is being run.
- The status of the last deployment.
- When the deployment was last run.
- When a failed deployment is going to run next, if the retry option is enabled.
- How many times deployment has been attempted.

To see only the failed deployments, select **Hyde finished deployments**.

To delete the records about a deployment job, right-click it and select **Delete**. To delete the records about several deployment jobs, select the jobs, right-click one of them and then select **Delete**.

To update the records, click **Refresh**.

To close the window, click **Close**.

Upgrading

If an older version of Ad-Aware Client Security is already installed in your network, you can easily upgrade it to version 3.5. The things to consider before you upgrade are presented hereinafter.

Upgrade will be performed in two steps:

1. Upgrade the older version of Ad-Aware Management Server to version 3.5. For more information, please refer to Upgrading Ad-Aware Management Server.

2. From the Ad-Aware Management Server 3.5 dashboard, upgrade the outdated agents and client products in your network. For more information, please refer to Upgrading Clients.

Considerations When Upgrading

Ad-Aware Management Server version 3.5 comes with many improvements and changes. Therefore, when upgrading, some of the data, features and settings in your current deployment will not be preserved.

This is what you should consider before the upgrade:

- The Management Dashboard has been completely redesigned.
- The new version replaces old report templates with many new ones (over 20 templates for Ad-Aware Business Client), which will help you obtain more detailed information. Existing scheduled reports will be lost.
- WMI scripts have been renamed as Network Tasks. You can find them, grouped together with the new Network Audit feature, under Network Tools.
- Custom policy and WMI script templates are no longer supported. Existing custom templates will be lost.
- Some of the old policy templates have been redesigned or split into several templates in the new version. As a consequence, the following policies will be lost:
  - Update Scheduled policies for Ad-Aware Business Client (new Update Settings policy is now available)
  - Antivirus Settings policies for Ad-Aware Security for Exchange
  - Antivirus Settings and Filters Settings policies for Ad-Aware Security for Mail Servers

Upgrading Ad-Aware Management Server

You can upgrade an older Ad-Aware Management Server installation to version 3.5 in two ways:

Directly install the new version over the older installation. Most of the Ad-Aware Management Server settings will be preserved during the upgrade. Remove the older installation first, and then install the new version. No settings will be preserved.

To directly install over an older installation:

1. Copy or download the installation file to the computer on which Ad-Aware Management Server is installed. Please note that you need at least 3 GB of free space on the system partition, or otherwise the installation will likely fail.
2. Double-click the installation file to start the installation wizard.
3. Click **Next**.
4. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.

> **Note**
>
> If you do not agree to these terms click **Cancel**. The installation process will be abandoned and you will exit setup.

5. Click **Upgrade** to replace the older version with the newer one.
6. Wait until the upgrade is completed and then click **Finish**.

Upgrading Clients

When upgrading clients make sure to first upgrade the agents and only then the client products.

To upgrade the outdated clients:

1. Open the management console and connect to Ad-Aware Management Server.

   The default password is `admin`.

2. In the new management dashboard, look for the **Updates Status** section.
3. Click the **Outdated agents** issue and follow the instructions to upgrade outdated agents to version 3.5. This operation may take a while.
4. Wait until all agents have been upgraded.
5. Return to the management dashboard, the same section.
6. Click the **Update available** issue and follow the instructions to upgrade outdated client products to version 3.5. This operation may take a while.

Installation Changes

This chapter describes some installation changes that you may need to perform at some point after the initial deployment.

- Changing Agent Synchronization Interval
- Migrating Ad-Aware Management Server to Another Computer
- Migrating to a Multi-Server Configuration
- Redirecting Clients to Another Server
- Modifying Ad-Aware Management Server Installation
- Repairing Ad-Aware Management Server

Changing Agent Synchronization Interval

Ad-Aware Management Agent is preconfigured to synchronize with Ad-Aware Management Server as follows:

- Every 5 minutes in LAN networks.
- Every hour over a VPN connection.

The default settings are suitable only for deployments with up to 100 clients. To accommodate a larger number of clients, the synchronization interval must be adjusted properly.

Use these guidelines to choose a synchronization interval that is appropriate for your LAN network:

- For few hundred clients (100-300 clients), set the synchronization interval recommended for medium-sized networks (10 minutes). For 400-500 clients, a larger interval is recommended.
- If the number of existing clients is large (over 500 clients), set the synchronization interval recommended for large networks (2 hours).
- The synchronization interval must also take into account the traffic between clients and Ad-Aware Management Server. For networks with intense activity (for example, hundreds of thousands of malware

alerts, anti-spam alerts etc.), a larger synchronization interval is recommended for increased performance. As a rule of thumb, if you notice poor performance, try increasing the synchronization interval.

The default synchronization interval for VPN connections should not be changed, unless you have more than 100 clients connecting through VPN.

You can reconfigure Ad-Aware Management Agent with a new synchronization interval using an **Ad-Aware Management Agent Settings** policy.

Follow these steps:

1. Connect to Ad-Aware Management Server using the management console.
2. In the tree menu, go to **Policies > Create New Policy**.
3. Select **Ad-Aware Management Server Templates** from the menu above the table.
4. Double-click the **Ad-Aware Management Agent Settings** template (or select it and click **Next**).
5. Change the synchronization interval according to your situation.
6. Click **Next**.
7. Select the check box corresponding to the server's name to reconfigure all clients.
8. Click **Next**.
9. Click **Save Policy** to create the policy. The new policy will appear in the Current Policies pane, where you can manage it and check the results.

Note

The change becomes effective as soon as the agent synchronizes with Ad-Aware Management Server (by default, within maximum 5 minutes in LAN networks or 1 hour over a VPN connection). It might take a while until all clients synchronize (some of them might be offline).

Migrating Ad-Aware Management Server to another Computer

In this section you can find out how to migrate Ad-Aware Management Server v3.5 installation and its clients to a different computer. To learn how you can migrate an older installation of Ad-Aware Management Server to version 3.5, please refer to Upgrading**.**

- Migrating a Stand-Alone Installation
- Migrating a Slave or Master Installation

Migrating a Stand-Alone Installation

Depending on how clients connect to Ad-Aware Management Server, there are two different migration procedures:

- **Situation A. Clients connect to Ad-Aware Management Server using server's IP address. The new server will use the same IP address as the old server.**

1. Install Ad-Aware Management Server on the new server. For more information, please refer to Installing Ad-Aware Management Server.
2. Back up the configuration of the existing Ad-Aware Management Server installation. For more information, please refer to Backing Up Ad-Aware Management Server Configuration.
3. Transfer the configuration backup file to the new server and then restore (import) the Ad-Aware Management Server configuration. For more information, please refer to Restoring Ad-Aware Management Server Configuration.
4. Register the new Ad-Aware Management Server instance with the license key you used on the old server. For more information, please refer to Registering Ad-Aware Management Server.
5. Remove Ad-Aware Management Server from the old server as described in Removing Ad-Aware Management Server.

- **Situation B.**
  1) Clients connect to Ad-Aware Management Server using server's IP address. The new server will use a different IP address than the old server.
  2) Clients connect to Ad-Aware Management Server using server's name.

  1. Install Ad-Aware Management Server on the new server. For more information, please refer to Installing Ad-Aware Management Server.
  2. Back up the configuration of the existing Ad-Aware Management Server installation. For more information, please refer to Backing up Ad-Aware Management Server Configuration.
  3. Transfer the configuration backup file to the new server and then restore (import) the Ad-Aware Management Server configuration. For more information, please refer to Restoring Ad-Aware Management Server Configuration.
  4. Migrate existing clients to the new server by reconfiguring the Ad-Aware Management Agent connection settings. For more information, please refer to Redirecting Clients to Another Server.

     Important
     Leave the old server in place for a while as clients that are offline will need to synchronize once with the old server. Otherwise, they will still report to the old server after it has been demoted. Remember that the default synchronization period is 5 minutes for LAN networks and one hour for VPN connections.

  5. Register the new Ad-Aware Management Server instance with the license key you used on the old server. For more information, please refer to Registering Ad-Aware Management Server.
  6. After all clients have synchronized with the new server, you can remove Ad-Aware Management Server from the old server as described in Removing Ad-Aware Management Server.

Migrating a Slave or Master Installation

To migrate a slave installation of Ad-Aware Management Server to another computer, follow the same steps as for a stand-alone installation. The only difference is that you must install Ad-Aware Management Server as slave of the designated master server. You can install Ad-Aware Management Server directly as slave of the designated master server by performing a custom installation. You can also install it as a stand-alone instance and then register it to the master server after the installation. For more information, please refer to Installing a Slave or Master Server.

To migrate a master installation of Ad-Aware Management Server to another computer:

1. Install the new master instance of Ad-Aware Management Server on the designated computer. You must perform a custom installation as described in Custom Installation (With Screenshots).
2. Back up the configuration of the existing Ad-Aware Management Server installation. For more information, please refer to Backing up Ad-Aware Management Server Configuration.
3. Transfer the configuration backup file to the new server and then restore (import) the Ad-Aware Management Server configuration. For more information, please refer to Restoring Ad-Aware Management Server Configuration.
4. Switch the slave servers to the new master server. Repeat the following steps for each slave server:

   Connect to the slave instance of Ad-Aware Management Server using the management console.

   a. Right-click the server name in the tree menu and select **Unregister from Master Server**. This action will remove registration as slave of the current master server.
   b. Right-click the server name again and select **Register to Master Server**.
   c. Type the IP address or name of the new master server and the server communication port. The default port is 7073.
   d. Click **OK** to save changes.
5. Remove Ad-Aware Management Server from the old server as described in Removing Ad-Aware Management Server.

Migrating to a Multi-Server Configuration

If your network has grown very large, or if your organization started opening local or international offices, it is time to migrate your Ad-Aware Management Server deployment from the current single-server configuration to a multi-server configuration. You can install the additional instances of Ad-Aware Management Server either as stand-alone or in a master-slave configuration (recommended).

A master-slave configuration consists of several Ad-Aware Management Server instances that manage the network computers (the slave servers) and a central Ad-Aware Management Server instance that only manages the other instances (the master server).

This information is important when considering a multi-server configuration:

- A standard deployment using a single Ad-Aware Management Server instance has a maximum of 1,000 client computers, all managed by and reporting to the single server.
- In master-slave configuration, it is recommended to have a maximum of 3,500 clients by using up to 7 slave servers reporting to a master server, with each slave managing up to 500 computers.
- In very large networks (more than 3,500 computers), multiple master-slave deployments can be used to provide total coverage.

Migrating to a master-slave configuration is fairly easy.

Just follow these steps:

1. Install the master instance of Ad-Aware Management Server in the main network (in geographically-distributed networks, this is usually the headquarters network). You must perform a custom installation as described in Custom Installation (With Screenshots).
2. Register the initial stand-alone instance of Ad-Aware Management Server to the master server. For more information, please refer to Registering a Stand-Alone Server to a Master Server.
3. Install additional slave instances of Ad-Aware Management Server, as needed:
   - If new offices have opened; install a slave server in the network of each office.
   - If the network has become larger than supported; install an additional slave server in the network.

   Afterwards, redirect part of the clients of the initial stand-alone server to this slave server. For more information, please refer to Redirecting Clients to Another Server.

You can install Ad-Aware Management Server directly as slave of the designated master server by performing a custom installation. You can also install it as a stand-alone instance and then register it to the master server after the installation. For more information, please refer to Installing a Slave or Master Server.

Redirecting Clients to another Server

There are two specific situations that require redirecting clients to another Ad-Aware Management Server instance:

- When migrating an Ad-Aware Management Server installation to another computer (only if the new computer will use a different IP address than the old one).
- In large complex networks, when installing additional Ad-Aware Management Server instances (load balancing).

Note

The procedure presented hereinafter must also be followed when you need to change the server's IP address if clients are configured to use it.

Client redirection can be performed using an **Ad-Aware Management Agent Connection** policy. Follow these steps:

1. Connect to Ad-Aware Management Server using the management console.
2. In the tree menu, go to **Policies > Create New Policy**.
3. Select **Ad-Aware Management Server Templates** from the menu above the table.
4. Double-click the **Ad-Aware Management Agent Connection** template (or select it and click **Next**).
5. Enter the new connection settings (corresponding to the new Ad-Aware Management Server instance). **Follow these guidelines:**
   - Use the IP address of the Ad-Aware Management Server computer if it does not change in time (static or reserved IP address).
   - Use the server name when the IP address is dynamically assigned by DHCP (no MAC address-based IP reservation).

   The default port is 7072.
6. Click **Next**.

7. Select the target computers depending on the situation:
    - **When migrating an installation to a new computer**. Select the check box corresponding to the server's name to reconfigure all clients.
    - **When load balancing**. To redirect specific computer groups only, select the check box corresponding to each such group.
8. Click **Next**.
9. Click **Save Policy** to create the policy. The new policy will appear in the Current Policies pane, where you can manage it and check the results.

Note
The change becomes effective as soon as the agent synchronizes with Ad-Aware Management Server (by default, within maximum 5 minutes in LAN networks or 1 hour over a VPN connection). It might take a while until all clients synchronize (some of them might be offline).

If Ad-Aware Management Agent does not manage to connect to Ad-Aware Management Server using the new settings, it will use the previous settings to connect to the former Ad-Aware Management Server. Ad-Aware Management Agent will automatically connect to the new Ad-Aware Management Server once this is available.

Modifying Ad-Aware Management Server Installation

You can modify the Ad-Aware Management Server installation by adding or removing components.

The installation package contains the following components:

- Ad-Aware Management Server
- Ad-Aware Security for Windows Servers (Server Add-On)
- Ad-Aware Management Console
- Ad-Aware Update Server

To modify the Ad-Aware Management Server installation:

1. You must log on to the computer with an administrator account.
2. On the Windows Start menu, go to **All Programs** - **Ad-Aware Management Server** - **Modify**, **Repair** or **Remove**.
3. Click **Next**.
4. Click the button corresponding to the **Modify** option.
5. The **Custom Setup** installation window will appear. This is where you can change which components to be installed. By clicking any component icon, a menu will appear where you can choose whether to install or not the selected component.

Note
Removing a component will not affect the other components in any way.

6. Click **Next**.

7. Click **Install** to modify the current installation and wait for the operation to complete.
8. Click **Finish**. A system restart may be required.

Repairing Ad-Aware Management Server

The Ad-Aware Management Server installation package offers the option to repair the installation in case a major malfunction occurs. Installation repair consists of reinstalling all of the currently installed components, using the installation options of the previous installation. This operation will fix missing or corrupt registry entries, files and shortcuts.

You will be able to choose to preserve the settings and data from the Ad-Aware Management Server database.

Important
Use of the installation repair option is not recommended, but it may be useful if you need to get Ad-Aware Management Server up and running as soon as possible.

To repair the Ad-Aware Management Server installation:

1. You must log on to the computer with an administrator account.
2. On the Windows Start menu, go to **All Programs** - **Ad-Aware Management Server – Modify, Repair** or **Remove**.
3. Click **Next**.
4. If you want to preserve your current settings and data, select **I want to keep my settings**. The Ad-Aware Management Server database will not be removed in this case.
5. Scheduled reports and e-mail settings will be lost even if you select this option.

Important
It is recommended that you first try to repair installation without removing the database.

6. Click the button corresponding to the **Repair** option.
7. Click **Repair** and wait for the operation to complete.
8. Click **Finish**. A system restart may be required.

Removal

This is where you can find out how to remove clients, Ad-Aware Management Server or the entire Ad-Aware Client Security installation.

Refer to the topic of your interest:

- Instructions for Complete Removal
- Removing Clients
- Removing Ad-Aware Management Server

Instructions for Complete Removal

To completely remove Ad-Aware Client Security from the network:

1. **Considerations for multi-server configurations**. If a multi-server configuration is deployed in the network, repeat the following steps for each stand-alone or slave instance of Ad-Aware Management Server. Afterwards, remove master instances as described in Removing Ad-Aware Management Server.
2. Remove all the clients managed by Ad-Aware Management Server as described in Removing Clients.
3. Check that all clients have been removed: in the management console, go to **Computers Directory > Managed Computers** and make sure removal was successful (all computers should have disappeared).
4. Remove Ad-Aware Management Server as described in Removing Ad-Aware Management Server.

Removing Clients

There are several ways to remove clients:

- From the Managed Computers Pane
- Using Deployment Tool
- Local Removal

Make sure to always remove Ad-Aware Business Client first and then Ad-Aware Management Agent

Note

Unix-based clients cannot be remotely removed from the Ad-Aware Management Server console. Please refer to the documentation of the specific Ad-Aware solution for removal instructions.

From the Managed Computers Pane

Clients can be very easily removed from the management console, the **Managed Computers** pane. For detailed information, please refer to these topics:

- Removing Client Products
- Removing Clients

Using Deployment Tool

This is an alternative method to remove Ad-Aware clients from the network.

You will run Deployment Tool two times: first, to remove Ad-Aware Business Client (or Ad-Aware Security for Windows Servers) and then Ad-Aware Management Agent.

Follow these steps:

1. Click **Next**.

2. Select the first option and click **Next**.
3. Select the Ad-Aware product you want to remove. Click **Next**.
4. Select **Remove**, then click **Next**.
5. You can leave the default deployment options unchanged. Click **Next**.
6. Specify the clients that you want to remove, using one the following methods:
   - **Browse the network to find target computers**. You must follow the next steps:

     a. Double-click a domain or workgroup in the **Entire Network** list (or select it from the menu) to see the computers it contains.

     b. Double-click the computers you want to add to the target list (or select them and click **Add computers to list**). To select all computers in the list, click one of them and then press CTRL+A
   - **Type the name or IP address of the target computers directly into the target list, separated by semicolons ";".**

   To learn about the syntax you must use, click View some examples. A new window will appear providing you with examples of valid and wrong syntax.
7. Click **Start** and wait for the operation to complete.
8. Check that removal succeeded on all selected clients. If the deployment process fails, you can see the returned error message explained in detail.

   If you want to save the results in a HTML or a txt file, click **Save Results**.

Click **Finish** to close the window.

Local Removal

To remove Ad-Aware Business Client locally:

1. Ad-Aware Business Client must operate in the power user mode. Otherwise, you need the administrative password. If the administrative password is not set, you cannot remove the program.
2. You must log on to the computer with an administrator account.
3. On the Windows Start menu, go to **All Programs** - **Ad-Aware Business Client** - **Modify**, **Repair** or **Uninstall**.
4. Click **Next**.
5. Click the button corresponding to the **Uninstall** option.
6. Click **Uninstall** and wait for the operation to complete.
7. Click **Finish**. A system restart may be required.

To remove Ad-Aware Management Agent from the client:

1. On the Windows Start menu, go to **Control Panel** - **Add or Remove Programs** (or **Programs and Features** on Windows Vista and Windows 7).
2. Find Ad-Aware Management Agent in the list of currently installed programs and select it.
3. Click **Remove** and wait for the operation to complete.
4. Click **Finish**. A system restart may be required.

Checking That Clients Have Been Removed

To find out if the selected clients have been removed:

1. Connect to Ad-Aware Management Server using the management console.
2. Go to **Computers Directory > Managed Computers**.
3. Search for the computers in the Managed Computers list.
   - If you have removed both the Ad-Aware client product and Ad-Aware Management Agent, the computer should not appear in the list.
   - If you have removed only the Ad-Aware client product, the computers should appear in the list, but with no product installed.

Removing Ad-Aware Management Server

The removal procedure is the same for all types of Ad-Aware Management Server installations (stand-alone, slave or master). Before you remove a stand-alone or slave instance of Ad-Aware Management Server, remember that you must first remove its clients (except when you want to reinstall it).

To remove Ad-Aware Management Server:

1. You must log on to the computer with an administrator account.
2. On the Windows Start menu, go to **All Programs** - **Ad-Aware Management Server** - **Modify**, **Repair** or **Remove**.
3. Click **Next**.
4. Click the button corresponding to the **Remove** option.
5. If you do not plan to reinstall Ad-Aware Management Server, select **I want to uninstall SQL**.
6. Click **Remove** and wait for the operation to complete.
7. Click **Finish**. A system restart may be required.

After the removal process is over, we recommend that you delete the `Ad-Aware` folder from `Program Files`.

If you have not chosen to automatically remove the SQL database instance, you can manually remove it as follows:

1. On the Windows Start menu, go to **All Programs** - **Ad-Aware Management Server** - **Remove SQL Server Instance**.
2. Click **Yes** to confirm removing the database and wait until the removal is completed.

Configuration and Management

Getting Started

Ad-Aware Management Server and its client products can be configured and managed through a graphical user interface named Ad-Aware Management Console. The new MMC-based management console was designed with the network administrator's needs in mind and focusing on improving user experience.

By using the management console you can:

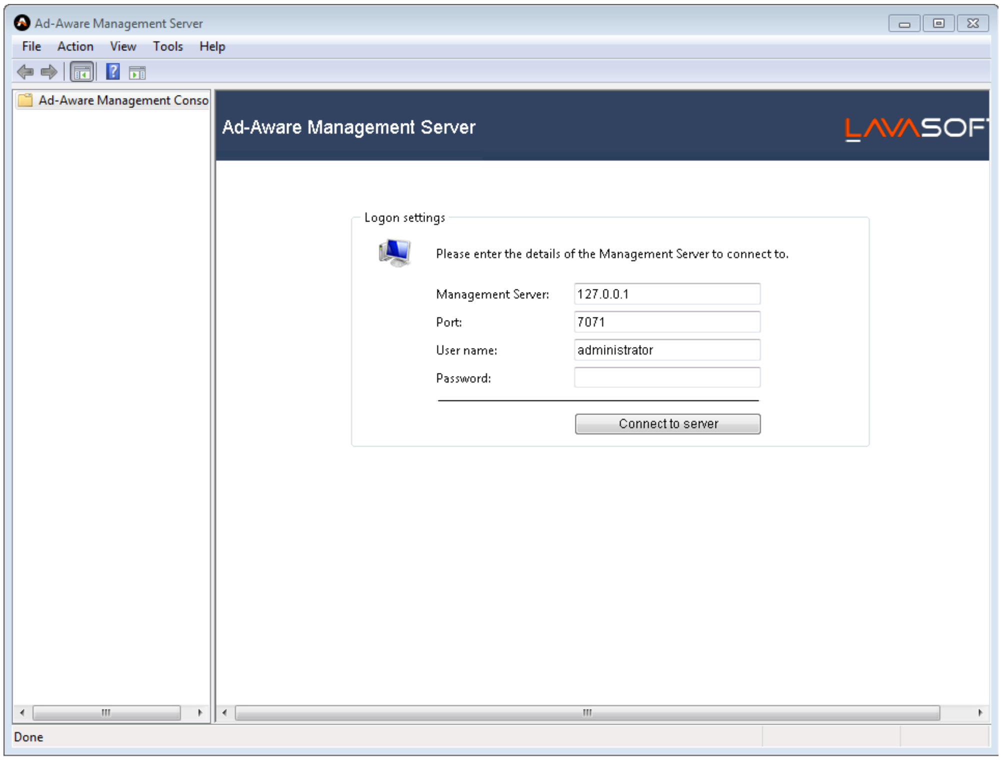
- Visualize the entire network (managed computers, computers that are not currently managed by Ad-Aware Management Server, computers excluded from management).
- Remotely deploy Ad-Aware Management Agent on detected network computers or on computers from Active Directory.
- Remotely deploy Ad-Aware client products on managed computers.
- Set Ad-Aware Management Server to automatically deploy Ad-Aware Management Agent and Ad-Aware Business Client on newly detected computers.
- Find out detailed information about a managed computer.
- Assign policies to managed computers or to computers from Active Directory in order to configure and even to install Ad-Aware client products.
- Run management tasks on managed computers in order to remotely perform administrative tasks.
- Check the results of the assigned policies and network management tasks.
- Configure Ad-Aware Management Server and monitor its activity.
- Obtain centralized easy-to-read reports regarding the managed computers.
- Remotely remove client products installed on managed computers.

Opening Management Console

To open the management console, use the Windows Start menu, by following the path: **Start – Programs** - **Ad-Aware Management Server** - **Ad-Aware Management Console**.

Connecting to Ad-Aware Management Server

Whenever you open the management console, you must provide the logon information of the Ad-Aware Management Server instance you want to connect to. You can connect to the local Ad-Aware Management Server instance or, remotely, to an instance installed on another computer.


Ad-Aware Management Server
File Action View Tools Help
Ad-Aware Management Conso
Ad-Aware Management Server
LAVASOFT
Logon settings
Connect to server
Done

Please enter the details of the Management Server to connect to.

Management Server: 127.0.0.1

Port: 7071

User name: administrator

Password:

Logon Settings

To connect to Ad-Aware Management Server, fill in the following fields:

- **Management Server** - type in the IP address of the Ad-Aware Management Server instance you want to connect to.

  Note

  If the instance of Ad-Aware Management Server is on the local machine, you can type `127.0.0.1` or `Localhost`.

- **Port** - type in the port used by the management console to communicate with the respective instance of Ad-Aware Management Server.

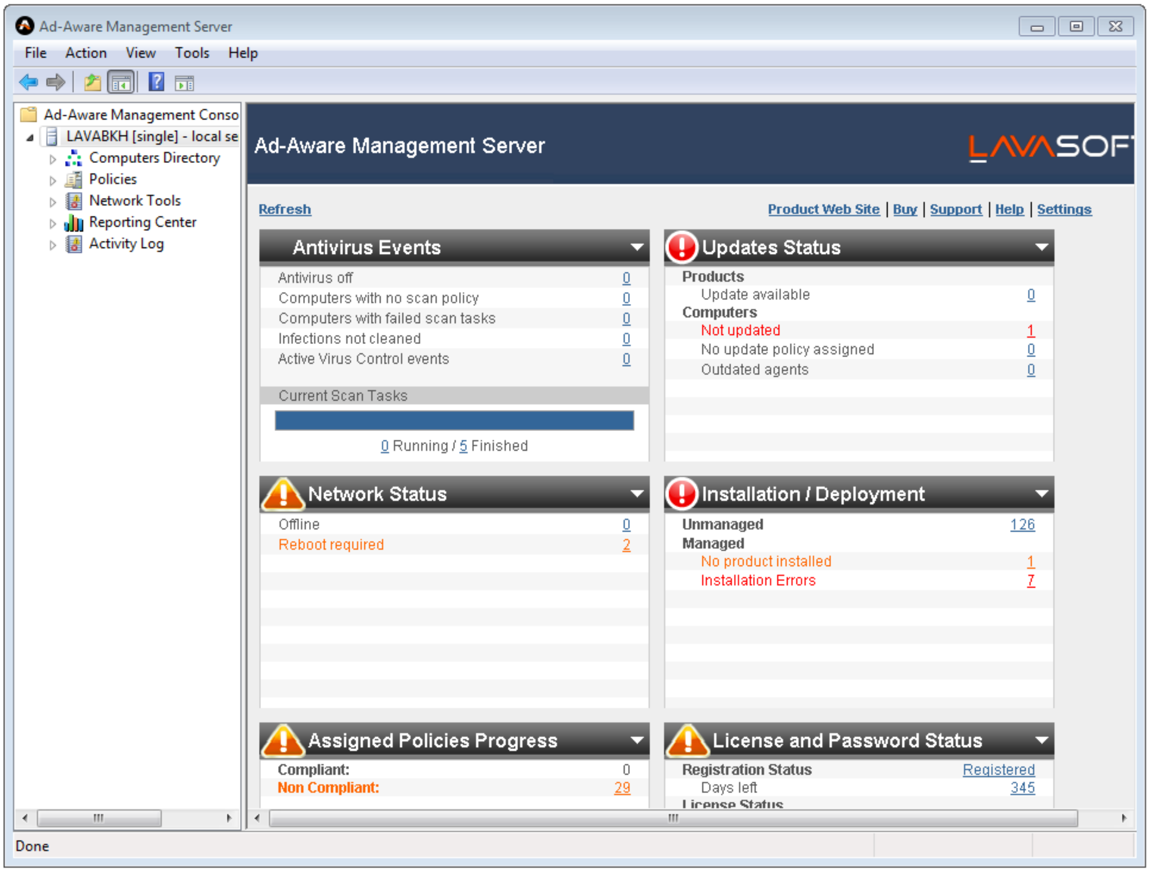
  Note

  This port was specified during the installation of Ad-Aware Management Server. If you did not change the default value, type `7071`.

- **Username** - type in a recognized username. The default username is `administrator`.
- **Password** - type in the password of the previously specified username. The default password is `admin`.

User Interface Overview

When you connect to an Ad-Aware Management Server instance, its name and all objects will appear in the tree menu on the left, while the dashboard will be displayed on the right side of the management console window.


Ad-Aware Management Server
File Action View Tools Help
Ad-Aware Management Conso
LAVABKH [single] - local se
Computers Directory
Policies
Network Tools
Reporting Center
Activity Log
Ad-Aware Management Server
LAVASOF
Refresh
Product Web Site | Buy | Support | Help | Settings
Done

Antivirus Events

Antivirus off	0
Computers with no scan policy	0
Computers with failed scan tasks	0
Infections not cleaned	0
Active Virus Control events	0

Current Scan Tasks

0 Running / 5 Finished

Updates Status

Products	
Update available	0
Computers	
Not updated	1
No update policy assigned	0
Outdated agents	0

Network Status

Offline	0
Reboot required	2

Installation / Deployment

Unmanaged	126
Managed	
No product installed	1
Installation Errors	7

Assigned Policies Progress

Compliant:	0
Non Compliant:	29

License and Password Status

Registration Status	Registered
Days left	345
License Status	

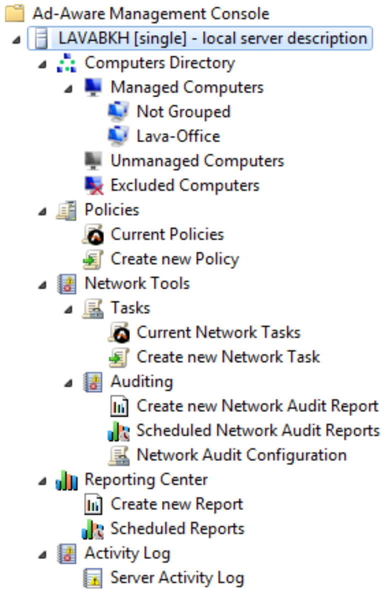
Management Console

The management console window consists of two panes. In the pane on the left, you can see the tree menu containing the Ad-Aware Management Server instances you are connected to and their related objects. The right pane displays the selected object from the tree menu.

At the top of the window, you can see the classic MMC menu bar and toolbar.

Tree Menu

In the pane on the left, you can see the tree menu.



Tree Menu

The tree menu consists of several containers, each container with its specific objects.

The root container is **Ad-Aware Management Console**. If you right-click it, a shortcut menu will appear. You can select:

- **Add server** - to connect to an additional instance of Ad-Aware Management Server.
- **Disconnect all** - to disconnect from all Ad-Aware Management Server instances.

Under the root container, you can see all of the instances of Ad-Aware Management Server you are connected to. If you right-click such an instance, a shortcut menu will appear. The following options are available:

Option	Description
Register to Master server	Opens a window where you can type the IP address or name of a master instance of Ad-Aware Management Server that will manage this instance.
Disconnect	Disconnects the management console from the Ad-Aware Management Server instance.
Refresh	Refreshes the Ad-Aware Management Server *dashboard*.
Change Password	Opens a *window* where you can change the logon password of the Ad-Aware Management Server instance.
Help	Opens the help file.

Each Ad-Aware Management Server instance in the tree menu contains the following objects:

- **Computers Directory** - contains the computers managed by Ad-Aware Management Server and those automatically detected by Ad-Aware Management Server in the broadcast domain.
  - *Managed Computers* - displays the computers managed by Ad-Aware Management Server.

    - *Unmanaged Computers* - displays the detected network computers that are not managed by Ad-Aware Management Server.
    - *Excluded Computers* - displays the network computers that will not be managed by Ad-Aware Management Server.
- **Policies** - allows managing the Ad-Aware client products installed on managed computers.
    - *Current Policies* - displays current policies and allows managing them.
    - *Create New Policy* - displays policy templates and allows creating new policies.
- **Network Tools** - this is where you can run network management tasks and create network audit reports.
    - *Tasks* - allows performing administrative tasks on managed computers.
        - Current Network Tasks - displays current tasks and allows managing them.
        - Create New Network Task - displays available tasks and enables you to run them on managed computers.
    - *Auditing* - enables you to configure the network audit feature and to create network audit reports.
        - Create New Network Audit Report - allows creating various types of network audit reports using built-in templates.
        - Scheduled Network Audit Reports - displays and enables you to manage the scheduled network audit reports you have created.
        - Network Audit Configuration - this is where you can configure the network audit options.
- **Reporting Center** - allows obtaining centralized reports regarding the network security status.
    - *Create New Report* - allows creating new reports.
    - *Scheduled Reports* - displays and allows managing the scheduled reports you have created.
- **Activity Log** - logs all operations of Ad-Aware Management Server, including error codes and debug messages.
    - *Server Activity* - displays events regarding the activity of Ad-Aware Management Server.

Tools Menu

The menu bar contains the menus provided by the MMC framework. The Tools menu allows access to the tools provided by Ad-Aware Management Server. The following options are available:

Registration

Opens the Registration Information window where you can see the license status and register Ad-Aware Management Server.

Credentials Manager

Opens Credentials Manager where you can save the credentials used for authentication when deploying Ad-Aware Management Agent on remote computers.

Change SQL Connection Password

Allows changing the password that the local Ad-Aware Management Server instance uses to connect to its database. Use this option after you have changed the password of the SQL user.

Deployment Tool

Launches Deployment Tool. Deployment Tool helps you automatically install, remove or repair Ad-Aware products on remote network computers. This tool also allows you to create unattended installation packages for use on offline computers (or when remote installation fails).

Network Builder

Launches Network Builder. Network Builder helps you easily organize the network computers into a manageable structure and deploy Ad-Aware Management Agent on selected computers.

Automatic Deployment

Opens the Automatic Deployment configuration window. Automatic Deployment allows Ad-Aware Management Server to automatically deploy Ad-Aware Management Agent and Ad-Aware Business Client on newly detected computers.

Retry Deployment

Opens a window where you can configure Ad-Aware Management Server to automatically retry deployment on computers where it failed initially.

View Deployment Status

Opens the Deployment Status window, which provides information on the status of all initiated, in progress or finished deployment processes, regardless of the deployment method.

E-mail Settings

Opens the E-mail Settings window where you can configure the e-mail settings required to send e-mail alerts.

Export/Import Policies Tool

Allows you to replicate the current policies configured on a specific Ad-Aware Management Server instance on other Ad-Aware Management Server instances.

Backup/Restore Server Configuration Tool

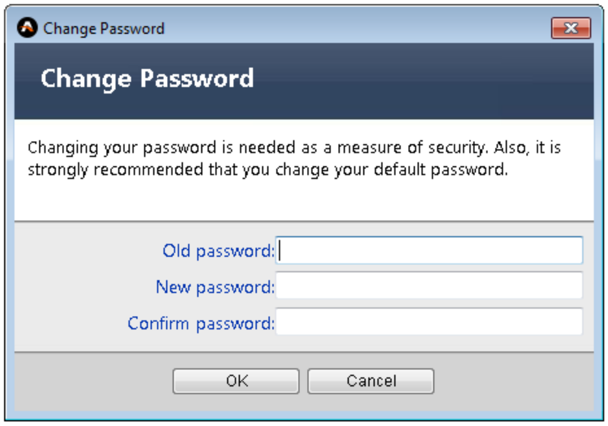
Opens Backup/Restore Server Configuration Tool. This tool helps you save the Ad-Aware Management Server configuration to a backup file or restore a previously saved configuration of Ad-Aware Management Server.

Note

If connected to more than one instance of Ad-Aware Management Server in the management console, you must first select the specific instance to use these tools for.

Changing Logon Password

To change the logon password for a specific Ad-Aware Management Server instance right-click it in the tree menu and select **Change Password**. The following window will open:



Changing your password is needed as a measure of security. Also, it is strongly recommended that you change your default password.

Change Password

You must fill in the following fields:

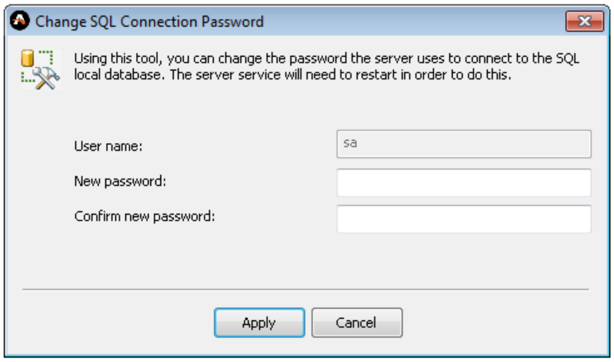
- **Old password** - type in the old password.
- **New password** - type in the new password.
- **Confirm password** - type in the new password again.

Click **OK** to change the password.

Changing SQL Connection Password

The security policies of your organization may require changing the passwords of the SQL users periodically. This implies changing the password of the username that Ad-Aware Management Server uses to connect to its database. In such cases, you must indicate to Ad-Aware Management Server the change of this password.

To change the password that the local Ad-Aware Management Server uses to connect to its database, click **Tools** and then **Change SQL Connection Password** on the menu. A new window will appear.



Using this tool, you can change the password the server uses to connect to the SQL local database. The server service will need to restart in order to do this.

User name: sa

SQL Connection Password

You must type the new password in the corresponding fields.

Click **Apply** to change the password.

Registration

Ad-Aware Client Security comes with a trial period of 30 days. During the trial period, the solution is fully functional and you can test it to see if it meets your expectations. You can use Ad-Aware Management Server to manage any number of Ad-Aware products (even the solutions designed to protect server systems).

Before the trial period is over, you must register Ad-Aware Management Server with a license key to keep your network protected.

Refer to the topic of your interest:

- Purchasing License Keys
- Registering Ad-Aware Management Server
- Checking the Registration Status
- Extending or Renewing Your License
- Registration in Master/Slave Configurations

Purchasing License Keys

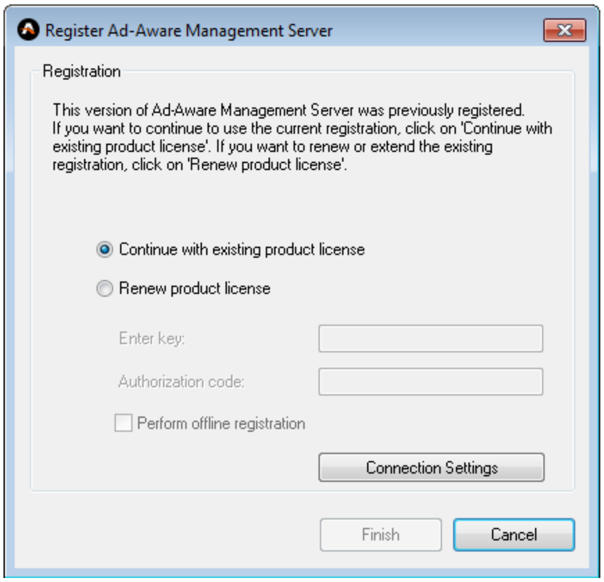
To purchase a license key, contact Lavasoft's Ad-Aware Business solutions @ sales@lavasoft.com. You will be assisted in finding the best solution for you and your business.

Registering Ad-Aware Management Server

You can register Ad-Aware Management Server over the Internet or offline. If you want to register offline, you will need an authorization code (besides the purchased license key). To get an authorization code, contact your Ad-Aware sales representative.

To register Ad-Aware Management Server:

1. Open the management console and connect to Ad-Aware Management Server.
2. Click the **Tools** menu and then click **Registration**. A new window will appear.
3. Click **Register**. A new window will appear.


Register Ad-Aware Management Server

Registration

This version of Ad-Aware Management Server was previously registered.
If you want to continue to use the current registration, click on 'Continue with existing product license'. If you want to renew or extend the existing registration, click on 'Renew product license'.

● Continue with existing product license

○ Renew product license

Enter key:

Authorization code:

□ Perform offline registration

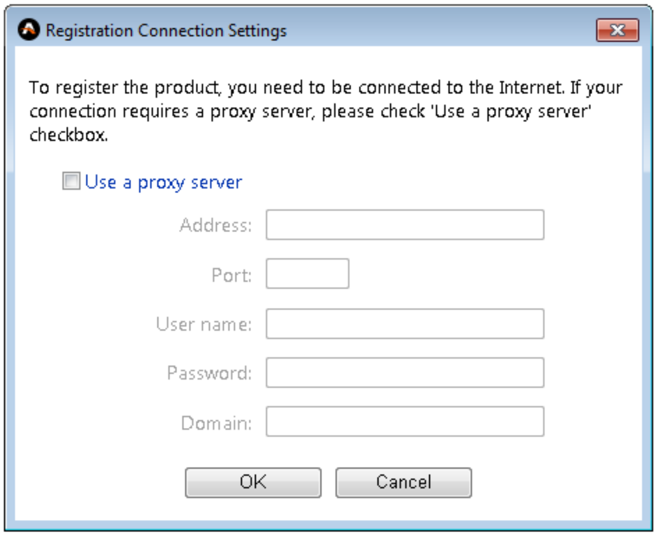
Registration

4. Select **Register this product**. If the product has been registered before, the option is **Renew product license**.
5. Type the license key in the **Enter key** field.
6. Particular situations:
   - If you want to register the product offline, select **Perform offline registration** and type the authorization code in the **Authorization Code** field.
   - To register online via a proxy connection, click **Connection Settings** and configure the proxy settings. For more information, please refer to Configuring Proxy Settings.
7. Click **Finish**.

You can see the new information regarding your license in the **Registration Information** window.

Configuring Proxy Settings

If your company connects to the Internet through a proxy, you must configure the proxy settings in order to perform online registration. Click **Connection Settings** to open the window where you can configure the proxy settings.



To register the product, you need to be connected to the Internet. If your connection requires a proxy server, please check 'Use a proxy server' checkbox.

□ Use a proxy server

Address:

Port:

User name:

Password:

Domain:

Proxy Settings

Select **Use a proxy** server and fill in the fields with the required information.

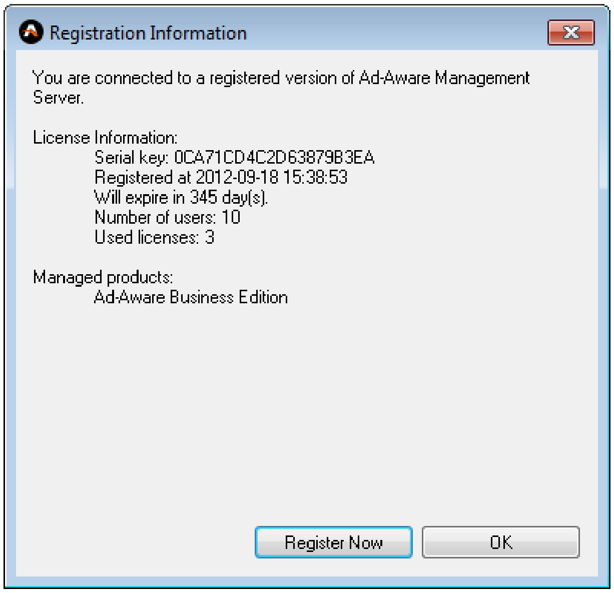
- **Proxy Address** - type in the IP address of the proxy server.
- **Port** - type in the port Ad-Aware uses to connect to the proxy server.
- **Username** - type in a user name recognized by the proxy.
- **Password** - type in the valid password of the previously specified user.
- **Domain** - type in the NTLM domain if you use NTLM domain authentication inside the network. Otherwise, leave this field blank.

Click **OK** to save the changes.

Checking the Registration Status

To check the Ad-Aware Management Server registration status:

1. Open the management console and connect to Ad-Aware Management Server.
2. Click the Tools menu and then click Registration. A new window will appear.



You are connected to a registered version of Ad-Aware Management Server.

License Information:
Serial key: 0CA71CD4C2D63879B3EA
Registered at 2012-09-18 15:38:53
Will expire in 345 day(s).
Number of users: 10
Used licenses: 3

Managed products:
Ad-Aware Business Edition

Registration Information

You can see whether the Ad-Aware Management Server instance is a trial version or a registered version. For registered versions, you are provided with detailed information about the license, including:

- The number of days until the license expires.
- The number of users covered by the license, which is actually the number of licensed Ad-Aware Business Client installations. If the license key also covers specific Ad-Aware server security solutions, this number also indicates how many users can be protected by each such solution.
- The number of Ad-Aware Business Client installations currently managed by Ad-Aware Management Server.
- What Ad-Aware products can be managed by Ad-Aware Management Server (displayed under **Managed products**). These are the Ad-Aware products supported by your license key.

Click **OK** to close the window.

Extending or Renewing Your License

If you want to extend the licensing period or the number of users covered by your license, contact your Ad-Aware sales representative (an authorized distributor, partner or reseller). You will be assisted in finding the best solution for you and with your purchase.

After you have purchased a license renewal or additional users:

- In most cases, your current license will be extended automatically, without you having to enter a new license key. Please note that the changes may take a few days to go into effect.
- In some cases, you will receive a new license key to register Ad-Aware Management Server with. This usually happens when you want to add other Ad-Aware solutions to the centralized management platform. Enter the new license key as described in Registering Ad-Aware Management Server.

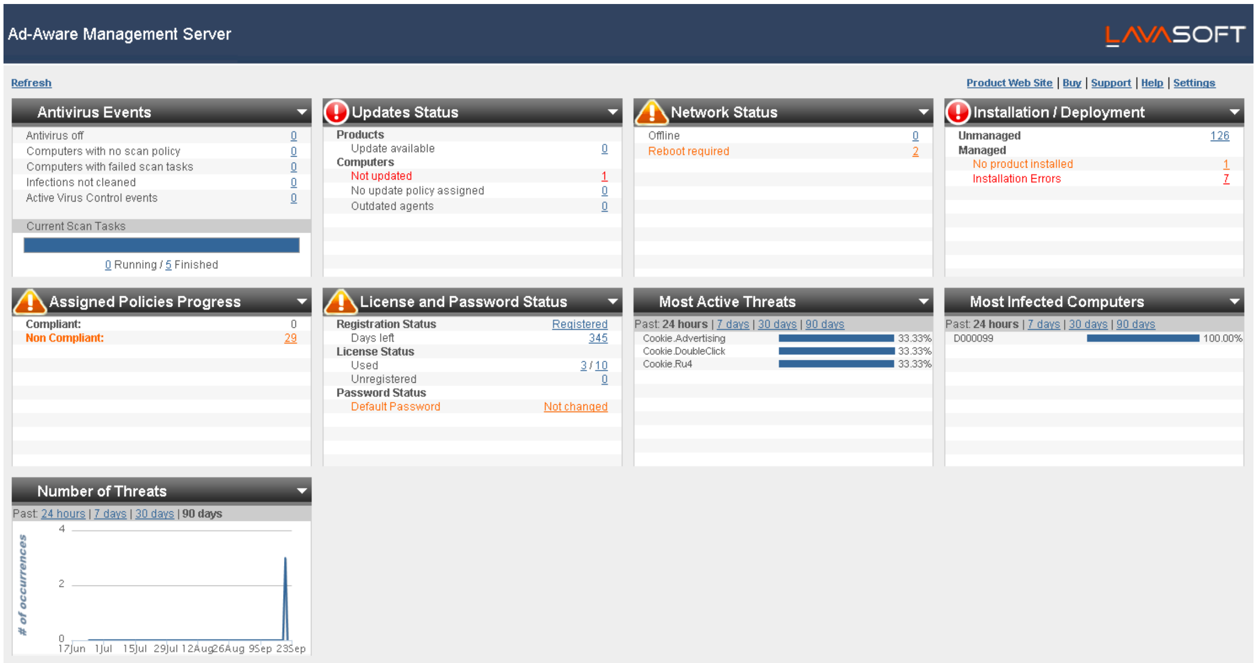
Registration in Master/Slave Configurations

If you have deployed a master/slave configuration, you must register each slave instance of Ad-Aware Management Server with a license key. You cannot and do not need to enter a license key on the master server.

Your Ad-Aware sales representative can provide you with detailed information on this topic. If you do have problems with the registration, you can contact us for assistance at Business Support.

The Management Dashboard

Each time you connect to Ad-Aware Management Server using the management console, or click the server's name in the tree menu, a status pane is displayed. This status pane is referred to as the dashboard.


Ad-Aware Management Server
LAVASOFT
Refresh
Product Web Site | Buy | Support | Help | Settings
# of occurrences
4
2
0
17Jun
1Jul
15Jul
29Jul
12Aug
26Aug
9Sep
23Sep

Antivirus Events

Antivirus off	0
Computers with no scan policy	0
Computers with failed scan tasks	0
Infections not cleaned	0
Active Virus Control events	0

Current Scan Tasks

0 Running / 5 Finished

Updates Status

Products	
Update available	0
Computers	
Not updated	1
No update policy assigned	0
Outdated agents	0

Network Status

Offline	0
Reboot required	2

Installation / Deployment

Unmanaged	126
Managed	
No product installed	1
Installation Errors	7

Assigned Policies Progress

Compliant:	0
Non Compliant:	29

License and Password Status

Registration Status	Registered
Days left	345
License Status	
Used	3 / 10
Unregistered	0
Password Status	
Default Password	Not changed

Most Active Threats

Past: **24 hours** | 7 days | 30 days | 90 days

Cookie.Advertising	33.33%
Cookie.DoubleClick	33.33%
Cookie.Ru4	33.33%

Most Infected Computers

Past: **24 hours** | 7 days | 30 days | 90 days

D000099	100.00%

Number of Threats

Past: 24 hours | 7 days | 30 days | **90 days**

The Management Dashboard

The dashboard provides you with useful information on the network security status and helps you easily solve the issues that require your attention. You should check the dashboard frequently in order to quickly identify and solve the issues affecting Ad-Aware Management Server or the network security.

Monitoring Modules

The dashboard is organized into several monitoring modules, which inform you about different network security aspects and help you fix related issues. Only some modules are displayed by default. You can choose which monitoring modules to display and how they are arranged as described in Configuring the Dashboard.

Monitored issues are systematically organized and easy to follow. You can find out more details about a specific issue by clicking it. For more information, please refer to Fixing Issues.

This is the entire list of monitoring modules:

Antivirus Events

This is where you can monitor any issue concerning your network's antivirus protection.

You can check if and which computers have real-time antivirus protection turned off or have no scan policy. You can run appropriate configuration policies to fix detected issues.

You are also informed about infected computers or computers with failed scan tasks so as to quickly fix these security issues. Furthermore, you can check applications detected by Active Virus Control and decide on the best course of action.

The status of the currently running or recently finished scan tasks is provided for quick overview.

E-mail Filters

This module informs you if there are any configuration issues with the Ad-Aware e-mail filters installed on your mail servers. You can run appropriate configuration policies to fix detected issues.

Updates Status

This module helps you get a complete picture of the update status of all managed Ad-Aware clients.

The **Products** subcategory informs you when new product updates are available. You can find out detailed information about available product updates and schedule their installation at a convenient time.

The **Computers** subcategory alerts you about computers with outdated malware signatures, with no policy assigned or with outdated agents. You can find out detailed information about detected problems and take corrective actions.

Network Status

Find out which computers are offline or need a reboot.

- A computer is considered offline or inactive if it has not synchronized for more than 1 day (by default). Such computers may be disconnected from the network (mobile employees, telecommuters) or a firewall may block their synchronization with the server.

  You can change the inactivity period to best meet your organization's specific needs. Click the arrow in the upper-right corner of the section and select **Edit Settings**.

- A computer may need a reboot after a Ad-Aware product, or another application, has been installed or updated. You can find out why a reboot is necessary and schedule it at a convenient time.

Installation / Deployment

Find out more about the unmanaged computers in your network and about the managed computers with no Ad-Aware product installed or with installation errors.

Assigned Policies Progress

This is where you can quickly check the progress and status of assigned policies. Check non-compliant computers to see whether assigned policies failed to apply or if they are scheduled to apply later.

License and Password Status

Provides detailed information about your registration, license and password status. The default logon password must be changed to prevent unauthorized access. Click the link to set a new password.

Most Active Threats

Shows the most active threats detected in the network in the last 24 hours; 7 days, 30 days or 90 days.

Most Infected Computers

Shows the most infected computers in the network in the last 24 hours; 7 days, 30 days or 90 days.

Number of Threats

Shows a graphic representation of the number of detected malware threats in the last 24 hours; 7, 30 or 90 days. A spike may indicate a potential security issue.

Number of Spam

Shows a graphic representation of the number of detected spam e-mails in the last 24 hours, 7, 30 or 90 days. A spike may indicate a potential security issue.

Number of Phishing Attempts

Shows a graphic representation of the number of detected phishing attempts in the last 24 hours; 7, 30 or 90 days. A spike may indicate a potential security issue.

Fixing Issues

The dashboard helps you easily fix potential or existing network security issues. When you open the dashboard, you can immediately notice where the problem areas are.

Categories in which issues have been detected are marked with a warning icon. The following warning icons are used:

⚠ A **triangle with an exclamation mark** indicates the existence of issues that pose medium security risks.

❗ A **circle with an exclamation mark** indicates the existence of issues that pose high security risks.

Moreover, monitored items change their color when issues are detected. Orange or red items indicate medium or high network security issues.

Click such items to find out more information. Follow the instructions provided in order to fix the respective issue. Some messages can be marked as read if you do not consider them to be important.

To go back to the dashboard, click the link in the upper-left corner of the pane.

Important Links

At the top of the dashboard there are several useful links.

Link	Description
Product Web Site	Opens the product website.
Buy	Opens a web page where you can buy a license key.
Support	Opens the Ad-Aware support page for business products.
About	Opens a window where you can see details about the product.

Help	Opens the help file.
Settings	Opens a window where you can configure monitoring options.

Configuring the Dashboard

The dashboard can be customized to better suit your needs.

To choose which monitoring modules to display:

1. In the tree menu, click the server's name to display the dashboard.
2. Click the **Settings** link in the upper-right corner of the dashboard.
3. Under **Display Modules**, select the modules you want to see on the dashboard.
4. Click the x button in the upper-right corner of the window to save the changes.

To organize the modules on the dashboard, drag & drop them to the desired position.

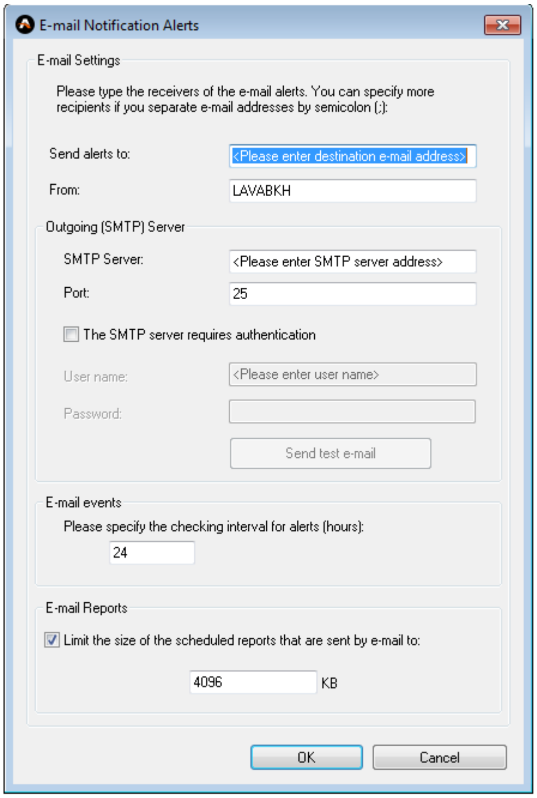
Configuring E-mail Notifications

Ad-Aware Management Server can notify you through e-mail about important issues affecting the network security. The e-mail notifications may help you block threats to the network security in a timely manner.

If you configure e-mail notifications, Ad-Aware Management Server will check for the selected security issues regularly, based on the configured checking interval. If new security issues have occurred since the last check, you will receive an e-mail regarding the status of each issue. For example, if the checking interval is set to 1 hour, every hour you will receive e-mail alerts about the issues that occurred during the past hour. Alerts regarding the registration status (trial or expired) are sent only once a day.

Step 1 - Configure the E-mail Settings

In order to receive e-mail notifications, you must first configure the e-mail settings. To this purpose, click **Tools** and then **E-mail Settings** on the menu. A new window will appear.



E-mail Notification Alerts

E-mail Settings

Please type the receivers of the e-mail alerts. You can specify more recipients if you separate e-mail addresses by semicolon (;):

Send alerts to: <Please enter destination e-mail address>

From: LAVABKH

Outgoing (SMTP) Server

SMTP Server: <Please enter SMTP server address>

Port: 25

☐ The SMTP server requires authentication

User name: <Please enter user name>

Password:

E-mail events

Please specify the checking interval for alerts (hours):

24

E-mail Reports

☑ Limit the size of the scheduled reports that are sent by e-mail to:

4096 KB

E-mail Settings

You must configure the following settings:

- **Send alerts to** - type in the e-mail address where to send the alerts. If you want to specify several recipients, separate their e-mail addresses by semicolon (;).
- **From** - if several instances of Ad-Aware Management Server are deployed within the organization, type in a text to identify the sender of the alerts.
- **SMTP Server** - type in the name or IP address of the mail server used to send the alerts.
- **Port** - type in the port used to connect to the mail server.
- If the SMTP server uses authentication, select The **SMTP server requires authentication** and provide the credentials required to authenticate with the mail server.
  - **User name** - type in a user name / e-mail address recognized by the mail server.
  - **Password** - type in the password of the previously specified user.

You can test the e-mail settings by sending a test e-mail (click **Send a test mail**). If the settings are correct, you can find the test e-mail when you check your e-mail address.

E-mail Events. By default, Ad-Aware Management Server will check for and alert you about new issues every hour. If you want to modify the checking interval, select a different interval from the menu.

E-mail Reports. In the *Create New Report* pane, you can create scheduled reports and choose to send them by e-mail. Reports can sometimes be quite large. This is why e-mailed reports are by default limited to the first 4096 bytes. To view the entire reports, you must open the management console and connect to the management server.

In the E-mail Reports section, you can modify or remove the report size limit. To modify the size limit, type the new value in the edit field. To remove the size limit, clear the check box.

Click **OK** to save the changes.

Step 2 - Choose the Alerts

To specify for which issues to receive e-mail notifications, follow these steps:

1. In the tree menu, click the server's name to display the dashboard.

2. Click the **Settings** link in the upper-right corner of the dashboard.

3. Under **E-mail Alerts**, select the issues that you want to be notified about through e-mail.

4. Click the x button in the upper-right corner of the window to save the changes.

Computers Directory

Computers Directory contains the network computers managed by Ad-Aware Management Server and other computers within the same subnet.

Ad-Aware Management Server automatically detects all online network devices within the broadcast domain that have a configured network interface. Most of these detected devices are computers; however, management switches and router interfaces are also detected.

The network computers are organized into three main groups:

- Managed Computers - contains the computers managed by Ad-Aware Management Server, namely those on which Ad-Aware Management Agent has already been installed. One or more Ad-Aware client products may also be installed on these computers.

  Note
  Computers will be referred to as managed or under the management of Ad-Aware Management Server if they have Ad-Aware Management Agent installed.

- Unmanaged Computers - contains the detected network computers on which Ad-Aware Management Agent has not been deployed yet and which have not been excluded from the management of Ad-Aware Management Server.

  Note
  The first time you connect to a server, you will find all detected network computers in this group.

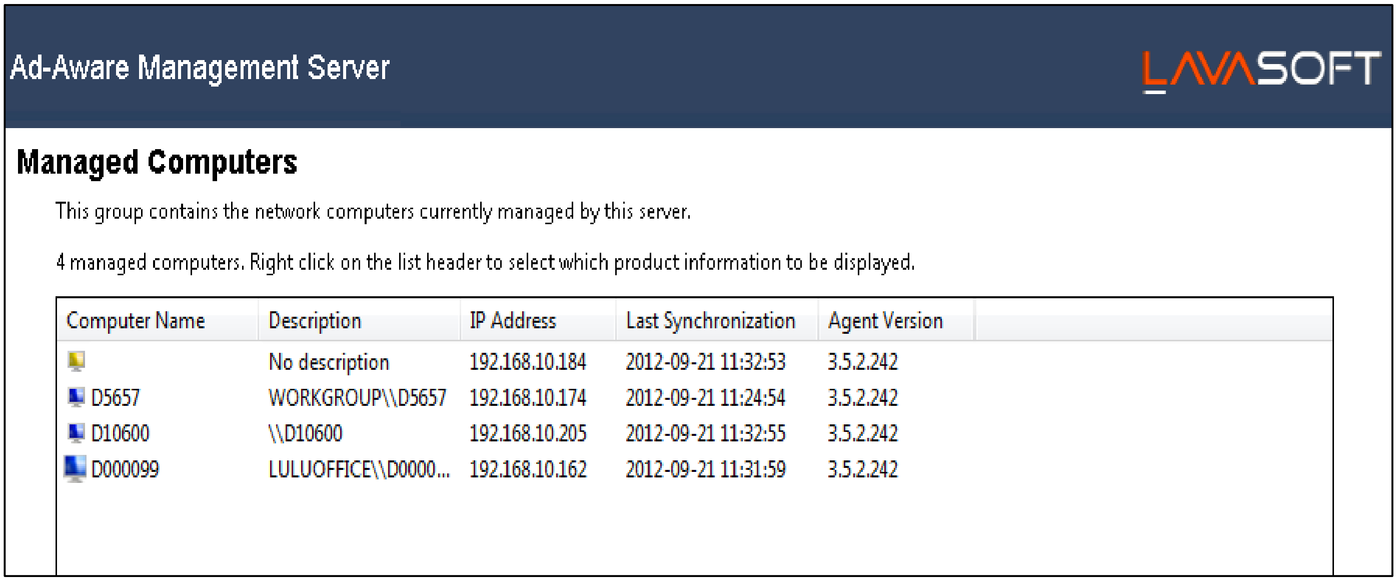
- Excluded Computers - contains the network computers which are not monitored at all by Ad-Aware Management Server. In this group you can find all network computers excluded from the Unmanaged Computers or Managed Computers group.

Managed Computers

The Managed Computers group contains all the computers managed by Ad-Aware Management Server. Ad-Aware Management Agent was previously deployed on these computers.

To display this group, do one of the following:

- In the tree menu, go to **Computers Directory > Managed Computers**.
- In the Computers Directory pane, click the corresponding link.



Managed Computers

This group contains the network computers currently managed by this server.

4 managed computers. Right click on the list header to select which product information to be displayed.

Computer Name	Description	IP Address	Last Synchronization	Agent Version
	No description	192.168.10.184	2012-09-21 11:32:53	3.5.2.242
D5657	WORKGROUP\\D5657	192.168.10.174	2012-09-21 11:24:54	3.5.2.242
D10600	\\D10600	192.168.10.205	2012-09-21 11:32:55	3.5.2.242
D000099	LULUOFFICE\\D0000...	192.168.10.162	2012-09-21 11:31:59	3.5.2.242

Managed Computers

You can see all the computers managed by Ad-Aware Management Server listed in the table. The table columns provide you with useful information about the listed computers:

- **Computer Name** - the name of the computer.
- **Description** - the computer description.
- **IP Address** - the IP address of the detected computer.
- **Last Synchronization** - the last time Ad-Aware Management Agent synchronized with Ad-Aware Management Server.

Note

It is important to monitor the Last Synchronization field as long inactivity periods might indicate a communication issue or a disconnected computer. The dashboard will inform you about the managed computers that have not synchronized with Ad-Aware Management Server for more than 24 hours.

- Agent Version - the Ad-Aware Management Agent version installed on the managed computer.

The icon next to the name of each managed computer quickly informs you about that computer:

Managed computer with no client products (only Ad-Aware Management Agent is installed)

Managed computer with Ad-Aware Business Client installed operating in the restricted user mode. In the restricted user mode, the user cannot configure the product, but only perform basic tasks, such as launching a default scan task, updating Ad-Aware or backing up data

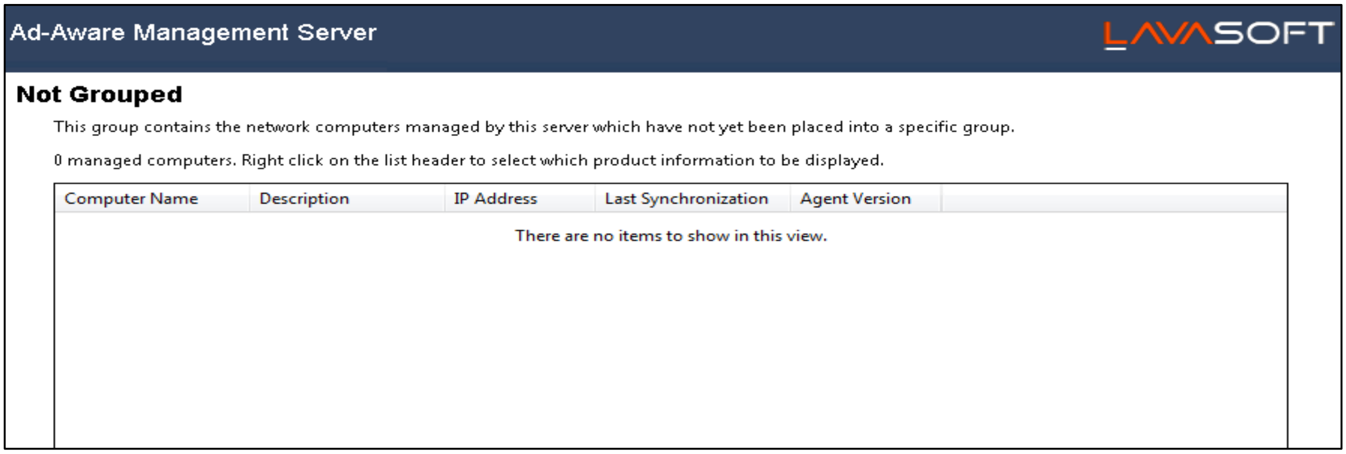
Managed computer with Ad-Aware Business Client installed operating in the power user mode. In the power user mode, the user has full control over Ad-Aware Business Client

Managed computer on which one or more Ad-Aware server security solutions are installed

Computer Groups

You can organize managed computers by creating specific groups according to the structure of your organization. In the tree menu, you can see all the groups included in the Managed Computers group.

Initially, managed computers are placed in a default group, called **Not Grouped**. To display this group, click **Not Grouped** in the tree menu.



Not Grouped

This group contains the network computers managed by this server which have not yet been placed into a specific group.

0 managed computers. Right click on the list header to select which product information to be displayed.

Computer Name	Description	IP Address	Last Synchronization	Agent Version

There are no items to show in this view.

Not Grouped Computers

You can see the managed computers which have not yet been placed in a specific group.

Different from the custom groups, you cannot rename or delete this group. You cannot create a new sub-group or move an existing group in this group either.

Creating Groups

To create a new sub-group in the Managed Computers group or in a custom group, follow these steps:

1. Right-click the group into which the new sub-group is to be included and select **Create group**. A new group (named **New Group**) will appear under the parent group in the tree menu.
2. Rename the newly created group.

Renaming Groups

To rename a group, right-click it, select **Rename** and type the new name.

Moving Groups

To move a sub-group from one group to another, follow these steps:

1. Right-click the sub-group you want to move and select **Cut**.

2. Right-click the group into which the sub-group is to be moved and select Paste.

If you are reorganizing the Managed Computers group, we recommend that you use the Network Builder.

Moving Computers to Another Group

To move computers from the current group to another group, follow these steps:

1. Select the computers from the list (use the Ctrl and Shift keys for multiple selections).

2. Right-click the selection and choose **Copy to group** or **Cut to group**.

3. In the tree menu right-click the group to move computers to and choose **Paste Client(s).**

Deleting Groups

To delete a specific group, right-click it and select **Delete**. You will have to confirm your action by clicking **Yes**.

Refreshing Computer List

To refresh the computer list, either press the F5 key or right-click the group in the tree menu and select **Refresh** from the shortcut menu.

Sorting through Computer List

You can sort computers by:

- name
- description
- IP address
- the time when the agent last synchronized with Ad-Aware Management Server
- agent version

To sort computers by one of the previously mentioned criteria, just click the corresponding column heading in the table.

For example, if you want to order computers by name click the **Computer Name** heading. If you click the heading again, the computers will be displayed in reverse order.

Searching for Computers

You can easily find a specific computer by its name using the keyboard. First, select a computer from the table and then press the key corresponding to the first letter of the computer name until the respective computer is displayed.

Another method to find a specific computer is to sort through the computer list and scroll up or down in the list to find the respective computer. In this way, you can search for computers using various criteria, such as name, IP address or activity.

Assigning Policies

You can assign policies to specific clients or to entire client groups (even to the entire Managed Computers group). You can choose to assign an existing policy or to create and assign a new policy.

- To assign a policy to a specific client, right-click the client and choose either **Assign new Policy** or **Assign existing Policy.**
- To assign a policy to an entire client group, right-click the group in the tree menu and choose either **Assign new Policy** or **Assign existing Policy**.

If you choose to assign a new policy, you must follow the wizard to create and configure the new policy. You will skip the computer selection step. For more information, please refer to Creating New Policies.

If you choose to assign an existing policy, you must select the desired policy from the list and click **Assign**.

Assigning Tasks

You can assign tasks to specific clients or to entire client groups (even to the entire Managed Computers group).

- To assign a task to a specific client, right-click the client and choose either **Assign new Network Task** or **Assign existing Network Task**.
- To assign a task to an entire client group, right-click the group in the tree menu and choose either **Assign new Network Task** or **Assign existing Network Task**.

If you choose to assign a new task, you must follow the wizard to create and configure the new task. You will skip the computer selection step. For more information, please refer to Creating New Network Tasks.

If you choose to assign an existing task, you must select the desired task from the list and click **Assign**.

Viewing Assigned Policies

You can view all the policies assigned to specific clients or client groups.

To view the policies assigned to a specific client, right-click it and select **View policies**. To view the policies assigned to a specific client group, right-click the respective group in the tree menu and select **View policies**. In both cases, a new pane will open and it will display the current policies.

Viewing Assigned Tasks

You can view all the tasks assigned to specific clients or client groups.

To view the tasks assigned to a specific client, right-click it and select **View Network Tasks**. To view the tasks assigned to a specific client group, right-click the respective group in the tree menu and select **View Network Tasks**. In both cases, a new pane will open and it will display the assigned tasks.

Checking Client Details and Status

You can easily get information about a specific computer and the status of the Ad-Aware products installed.

Right-click the computer and select **More details**. You can see information about the system and the status of Ad-Aware Management Agent. Information about the Ad-Aware client products installed on the computer is available on separate tabs.

Monitoring Client Products Status

If you want an overview of the security status of all managed computers, you can choose to display additional columns providing such information. Follow these steps:

1. Right-click any column header.
2. Point to the name of the desired client product.
3. Select the information you want to be displayed about that client product.

The table will be refreshed and you will notice the new column.

To hide a column providing general information, follow these steps:

1. Right-click any column header.
2. Point to **General Information**.
3. Clear the check mark next to the column you want to hide.

Filtering managed computers based on the client product installed. By default, all managed computers in a group are displayed in the table, regardless of the client product installed. You can apply filters to only view the managed computers with a specific client product installed. Follow these steps:

1. Right-click any column header.
2. Point to **Filters**.
3. Select which managed computers to be displayed based on the client product installed. For example, you can select to show only the computers with Ad-Aware Business Client installed.

Switching between Restricted and Power User

Ad-Aware Business Client can operate in two modes: restricted user and power user.

In the restricted user mode, the user cannot configure the product, but only perform basic tasks, such as launching a default scan task, updating Ad-Aware or backing up data. In the power user mode, the user has full control over Ad-Aware Business Client.

By default, after deployment, Ad-Aware Business Client will operate in the restricted user mode. If you want the Ad-Aware Business Client installed on a specific computer to operate in the power user mode right-click the respective client in the list and select **Switch to power desktop**. To go back to the restricted user mode, just right-click the client again and select **Switch to restricted desktop**.

Note

The change becomes effective as soon as the agent synchronizes with Ad-Aware Management Server (by default, within maximum 5 minutes in LAN networks or 1 hour over a VPN connection). Ad-Aware Business Client will immediately switch to the other operating mode if the product interface is closed. Otherwise, the user will be prompted to restart the interface for the changes to take effect.

Removing Client Products

Client products can be easily removed from a managed computer. Simply right-click on the computer you would like to remove and select **Uninstall Ad-Aware Client Products**.

To remove the Ad-Aware client products from several computers at once:

1. Select the computers from the list (use the Ctrl and Shift keys for multiple selection).
2. Right-click the selection and choose **Uninstall Ad-Aware Client Products**.

Important

In order to assign a new policy and re-install Ad-Aware Business Client, you must first restart the computer. You can use a *task* to automatically restart managed computers.

Removing Clients

If you no longer want to manage a specific computer, you must first remove any client product installed. After removing the client product, right-click the computer and select **Uninstall Ad-Aware Management Agent**.

Once Ad-Aware Management Agent is removed, the computer automatically disappears from the Managed Computers list. Eventually, it may be detected and displayed in the Unmanaged Computers group.

To remove several clients at once:

1. Select the computers from the list (use the Ctrl and Shift keys for multiple selection).
2. Right-click the selection and choose Uninstall Ad-Aware Management Agent. If you see the **Uninstall Ad-Aware Client Products** option instead, your selection contains at least one computer with an Ad-Aware client product installed.

Deleting Computers from Table

You can delete any computer listed in the table. In this way, you can remove from the database the computers that are no longer part of the network.

To delete a computer from the database, right-click it and select **Delete** from the menu You will have to confirm your action by clicking **Yes**.

To delete several computers from the database, select them, right-click the selection and then select **Delete items** from the menu. You will have to confirm your action by clicking **Yes**.

> **Note**
> If you delete a managed computer while it is still connected to the network, Ad-Aware will eventually detect its activity and restore it in the **Managed Computers > Not Grouped** group.

Excluding Computers from Management

To exclude a computer from management, just right-click it and select **Exclude** from the menu. You will have to confirm your action by clicking **Yes**.

To exclude several computers from management, select them, right-click the selection and then select **Exclude items** from the menu. You will have to confirm your action by clicking **Yes**.

> **Note**
> The excluded computers will be moved in the **Excluded Computers** group.

Changing Displayed Information

You can change the displayed information by adding or removing columns from the table or by changing their order. By default, all available columns are displayed.

Right-click the table header to choose which columns to display. To change their order, drag & drop the column header to the desired position.

Exporting Computer List

You can export the list of the computers in the group to an HTML, XML, text or comma-separated values (CSV) file. This is very useful if you need printed statistics. To export the computer list:

1. In the tree menu, right-click the group.
2. Select **Export groups/clients** to a file from the menu. A new window will appear.

3. If you want to include information about subgroups, select the **Include Subgroups** check box.
4. Click **Browse**.
5. Save the file under the desired name and type.
6. Click **OK**.

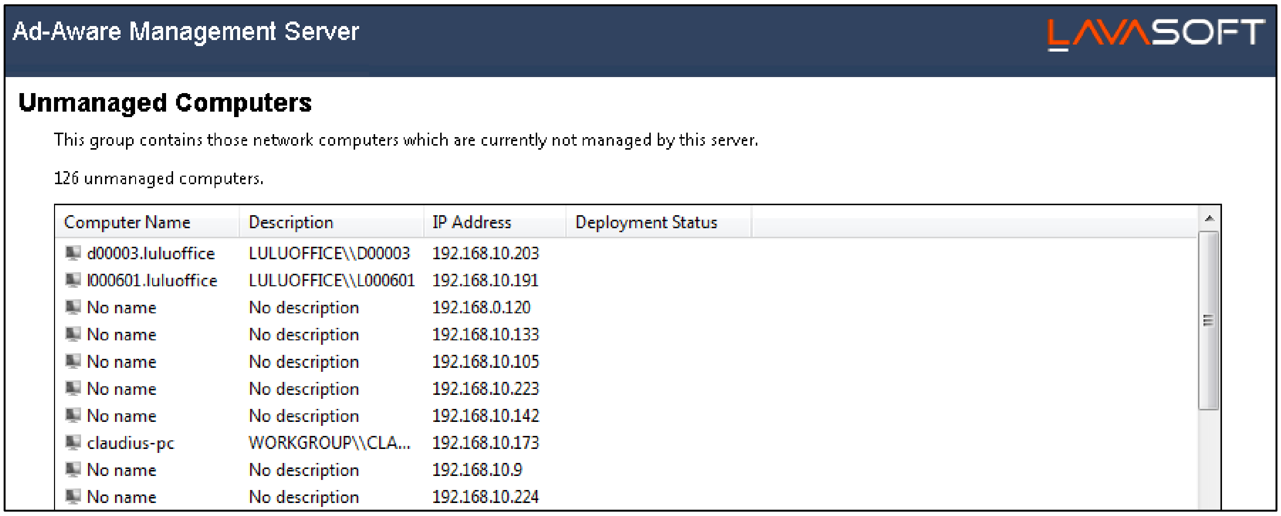
Unmanaged Computers

The Unmanaged Computers group contains the detected network computers on which Ad-Aware Management Agent has not yet been deployed and which have not been excluded from the management of Ad-Aware Management Server.

Note
The first time you connect to an instance of Ad-Aware Management Server, you will find all detected network computers in this group.

To display this group, do one of the following:

- In the tree menu, go to **Computers Directory > Unmanaged Computers**.
- In the Computers Directory pane, click the corresponding link.



Unmanaged Computers

This group contains those network computers which are currently not managed by this server.

126 unmanaged computers.

Computer Name	Description	IP Address	Deployment Status
d00003.luluoffice	LULUOFFICE\\D00003	192.168.10.203	
l000601.luluoffice	LULUOFFICE\\L000601	192.168.10.191	
No name	No description	192.168.0.120	
No name	No description	192.168.10.133	
No name	No description	192.168.10.105	
No name	No description	192.168.10.223	
No name	No description	192.168.10.142	
claudius-pc	WORKGROUP\\CLA...	192.168.10.173	
No name	No description	192.168.10.9	
No name	No description	192.168.10.224	

Unmanaged Computers

You can see the unmanaged computers listed in the table. The table columns provide you with useful information about the listed computers:

- **Computer Name** - the name of the computer.

Note
If **No Name** is displayed under this column, the respective computer may be a management switch or a router interface.

- **Description** - the computer description.

- **IP Address** - the IP address of the computer.
- **Deployment Status** - the deployment status, when deploying Ad-Aware Management Agent on the remote computer.

Refreshing Computer List

To refresh the computer list, either Press the F5 key or right-click the group in the tree menu and select **Refresh** from the shortcut menu.

Sorting through Computer List

You can sort computers by:

- name
- description
- IP address
- deployment status

To sort computers by one of the previously mentioned criteria, just click the corresponding column heading in the table.

For example, if you want to order computers by name click the **Computer Name** heading. If you click the heading again, the computers will be displayed in reverse order.

Searching for Computers

You can easily find a specific computer by its name using the keyboard. First, select a computer from the table and then press the key corresponding to the first letter of the computer name until the respective computer is displayed.

Another method to find a specific computer is to sort through the computer list and scroll up or down in the list to find the respective computer. In this way, you can search for computers using various criteria, such as name, IP address or activity.

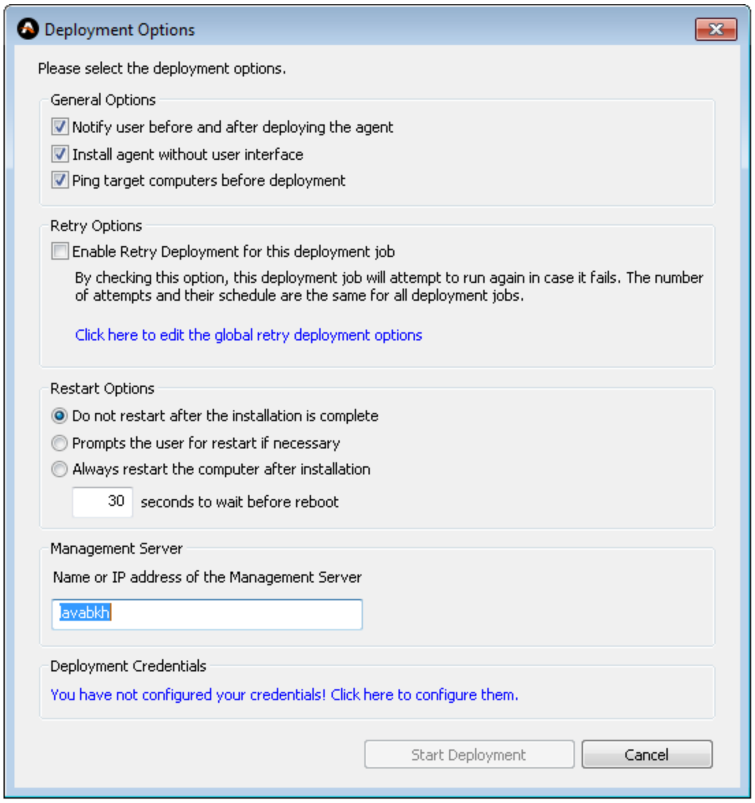
Deploying Ad-Aware Management Agent

In order to manage a remote computer using Ad-Aware Management Server, you must first deploy Ad-Aware Management Agent on the respective computer. You can do that directly from the **Unmanaged Computers** group.

Note

When deploying Ad-Aware Management Agent in the network for the first time, it is recommended to use Network Builder. To automatically deploy Ad-Aware Management Agent on newly detected computers, use Automatic Deployment.

To deploy Ad-Aware Management Agent on a specific computer, just right-click it and select **Deploy on this computer.** To deploy Ad-Aware Management Agent simultaneously on several computers, select them, right-click the selection and then select **Deploy on these items**. In both situations, a new window will appear, allowing you to configure the deployment options and initiate the deployment process.



Deployment Options

Please select the deployment options.

General Options

☑ Notify user before and after deploying the agent

☑ Install agent without user interface

☑ Ping target computers before deployment

Retry Options

☐ Enable Retry Deployment for this deployment job

By checking this option, this deployment job will attempt to run again in case it fails. The number of attempts and their schedule are the same for all deployment jobs.

Click here to edit the global retry deployment options

Restart Options

● Do not restart after the installation is complete

○ Prompts the user for restart if necessary

○ Always restart the computer after installation

30 seconds to wait before reboot

Management Server

Name or IP address of the Management Server

avabkh

Deployment Credentials

You have not configured your credentials! Click here to configure them.

Deployment Options

To configure and initiate the deployment of Ad-Aware Management Agent, follow these steps:

Step 1 - Configure General Options

You can specify the deployment behavior on the remote computer using the options in the **General Options** category.

Check **Notify user before and after deploying the agent** if you want the user logged on the remote computer to be briefly informed about the deployment process. Two dialogs will appear on the user's screen, before and after the deployment process.

Check **Install agent without user interface** if you want the deployment process to be performed silently in the background. If you do not check this option, the Windows Installer interface will appear on the user's screen.

Select **Ping target computers before deployment** to immediately find out if and which of the target computers may be disconnected from the network. If the ping to a target computer fails, a message in the deployment status column will indicate that the computer is disconnected. Ad-Aware Management Server will not proceed with the deployment. For such computers, you will have to reinitiate deployment at a later time or to clear this check box before starting the deployment.

Note

The ping may fail for other reasons. For example, the firewall installed on the target computer may prevent the computer from responding to ping.

Step 2 - Configure Retry Options

By selecting **Enable Retry Deployment for this job**, if the deployment fails the first time, it will run again automatically. To configure the retry options, click the provided link.

Note

For more information, please refer to Retry Deployment.

Step 3 - Specify Restart Method

To specify how to restart the remote computer, select one of the options in the **Restart Options** category. If you select:

- **Do not restart after the installation is completed** - the remote computer will not be restarted once the installation is completed. Ad-Aware Management Agent does not require a restart to complete the installation, so you can safely select the first option.
- **Prompt the user for restart if necessary** - the user logged on the remote computer will be prompted to restart the computer, if it is necessary.

Note

The user must confirm or suspend computer restart within 30 seconds, otherwise the remote computer will be restarted automatically.

- **Always restart the computer after installation** - the remote computer is restarted immediately after the installation is completed, without alerting the user.

Step 4 - Specify Management Server

Ad-Aware Management Agent communicates with Ad-Aware Management Server using either the IP address or the name of the computer Ad-Aware Management Server is installed on. To prevent communication issues, configure the management server identity as follows:

- If the IP address of the Ad-Aware Management Server computer does not change in time (static or reserved IP address), type the IP address.
- Otherwise, if the IP address is dynamically assigned by DHCP (no MAC address-based IP reservation), type the computer name.

By default, Ad-Aware Management Agent will be managed by the specific instance of Ad-Aware Management Server that deploys it. If you want Ad-Aware Management Agent to be managed by another instance of Ad-Aware Management Server, provide the name or IP address of the computer it is installed on in the corresponding field.

Step 5 - Specify Deployment Credentials

In order to remotely deploy Ad-Aware Management Agent, Ad-Aware Management Server requires administrative credentials to authenticate on the remote computer. Use Credentials Manager to manage these credentials. To open the Credentials Manager window, click the provided link.

Note

For more information, please refer to Credentials Manager.

Step 6 - Start Deployment

Click **Start Deployment** to initiate the deployment process. You can see the deployment status in the **Deployment Status** field.

Excluding Computers from Management

If you do not want specific computers to be managed by Ad-Aware Management Server, you just have to exclude them from management. For example, you might want to exclude your own computer, the computers of your IT team or the computers of the Quality Assurance team.

You should also exclude the router interfaces and management switches detected by Ad-Aware Management Server in the broadcast domain. You should make a list of such devices in your network, find them in the Unmanaged Computers group and exclude them.

To exclude a computer from management, just right-click it and select **Exclude** from the menu. You will have to confirm your action by clicking **Yes**.

To exclude several computers from management, select them, right-click the selection and then select Exclude items from the menu. You will have to confirm your action by clicking **Yes.**

Note

The excluded computers will be moved in the **Excluded Computers** group.

Deleting Computers from Table

You can delete any computer listed in the table. In this way, you can remove from the database the computers that are no longer part of the network.

To delete a computer from the database, right-click it and select **Delete** from the menu You will have to confirm your action by clicking **Yes**.

To delete several computers from the database, select them, right-click the selection and then select **Delete items** from the menu. You will have to confirm your action by clicking **Yes**.

Note

If you delete an unmanaged computer while it is still connected to the network, Ad-Aware will eventually detect its activity and restore it in the Unmanaged Computers group.

Changing Displayed Information

You can change the displayed information by adding or removing columns from the table or by changing their order. By default, all available columns are displayed.

Right-click the table header to choose which columns to display. To change their order, drag&drop the column header to the desired position.

Exporting Computer List

You can export the list of the computers in the group to an HTML, XML, text or comma-separated values (CSV) file. This is very useful if you need printed statistics.

To export the computer list:

1. In the tree menu, right-click the group.
2. Select **Export groups/clients to a file** from the menu. A new window will appear.
3. Click **Browse**.
4. Save the file under the desired name and type.
5. Click **OK**.

Excluded Computers

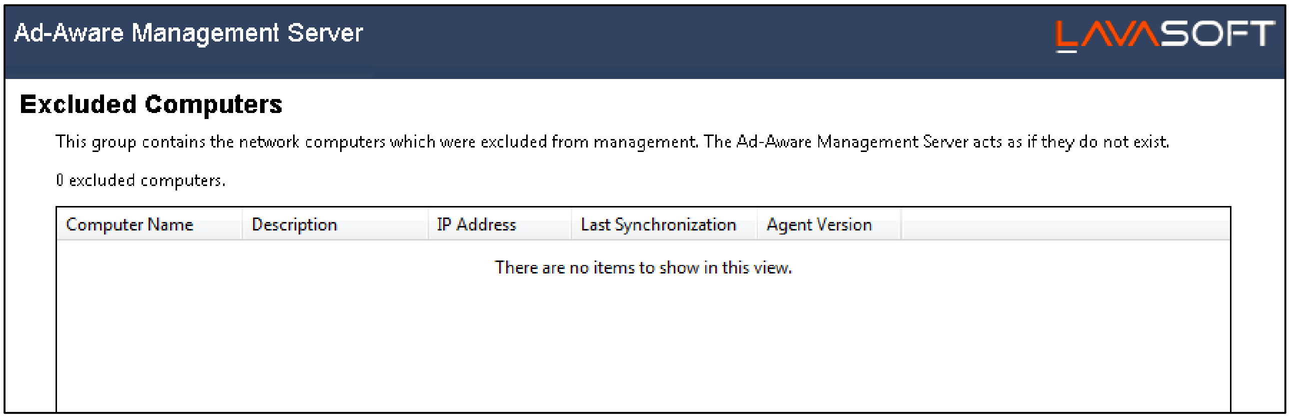
The Excluded Computers group contains the network computers that were excluded from the management of Ad-Aware Management Server. These computers are not monitored at all by Ad-Aware Management Server.

Note

Computers can be excluded both from the Unmanaged Computers and from the Managed Computers group. As a rule, exclude the management switches and router interfaces automatically detected by Ad-Aware in the broadcast domain as well as the computers that you do not want to be managed by Ad-Aware Management Server.

To display this group, do one of the following:

- In the tree menu, go to **Computers Directory > Excluded Computers**.
- In the Computers Directory pane, click the corresponding link.



Ad-Aware Management Server

Excluded Computers

This group contains the network computers which were excluded from management. The Ad-Aware Management Server acts as if they do not exist.

0 excluded computers.

Computer Name	Description	IP Address	Last Synchronization	Agent Version

There are no items to show in this view.

Excluded Computers

You can see the excluded computers listed in the table. The table columns provide you with useful information about the listed computers:

- **Computer Name** - the name of the computer.

Note

If No Name is displayed under this column, the respective computer may be a management switch or a router interface.

- **Description** - the computer description.
- **IP Address** - the IP address of the detected computer.
- **Last Synchronization** - the last time the computer was detected.
- **Agent Version** - if Ad-Aware Management Agent is installed on the computer, you can see its version.

Refreshing Computer List

To refresh the computer list, either press the F5 key or right-click the group in the tree menu and select **Refresh** from the shortcut menu.

Sorting through Computer List

You can sort computers by:

- name
- description
- IP address
- the time when they were last detected

To sort computers by one of the previously mentioned criteria, just click the corresponding column heading in the table.

For example, if you want to order computers by name click the **Computer Name** heading. If you click the heading again, the computers will be displayed in reverse order.

Searching for Computers

You can easily find a specific computer by its name using the keyboard. First, select a computer from the table and then press the key corresponding to the first letter of the computer name until the respective computer is displayed.

Another method to find a specific computer is to sort through the computer list and scroll up or down in the list to find the respective computer. In this way, you can search for computers using various criteria, such as name, IP address or activity.

Deleting Computers from Table

You can delete any computer listed in the table. In this way, you can remove from the database the computers that are no longer part of the network.

To delete a computer from the database, right-click it and select **Delete** from the menu. You will have to confirm your action by clicking **Yes**.

To delete several computers from the database, select them, right-click the selection and then select **Delete items** from the menu. You will have to confirm your action by clicking **Yes**.

Note

If you delete a computer while it is still connected to the network, Ad-Aware will eventually detect its activity. The following situations may occur:

- If Ad-Aware Management Agent is installed on the computer, then the computer will appear in the **Managed Computers > Not Grouped** group.
- Otherwise, the computer will appear in the **Unmanaged Computers** group.

Restoring Excluded Computers

You cannot directly restore an excluded computer to its original group.

The only method that you can use to restore an excluded computer is to delete it from the table. This works however only for the main groups. If the computer was excluded from a sub-group within the Managed Computers group, after Ad-Aware Management Agent contacts the server, the respective computer will be placed in the Not Grouped group.

Note

For more information, please refer to Deleting Computers from Table.

Changing Displayed Information

You can change the displayed information by adding or removing columns from the table or by changing their order. By default, all available columns are displayed.

Right-click the table header to choose which columns to display. To change their order, drag & drop the column header to the desired position.

Exporting Computer List

You can export the list of the computers in the group to an HTML, XML, text or comma-separated values (CSV) file. This is very useful if you need printed statistics.

To export the computer list:

1. In the tree menu, right-click the group.
2. Select **Export groups/clients** to a file from the menu. A new window will appear.
3. Click **Browse**.
4. Save the file under the desired name and type.
5. Click **OK**.

Policies

Ad-Aware client products can be managed remotely through policies. A policy defines a set of security rules a client computer must comply with.

Policies are sent by Ad-Aware Management Server to Ad-Aware Management Agent, which applies them to the local Ad-Aware client product. Once a policy has been successfully transmitted to Ad-Aware Management Agent, it will be applied to the local Ad-Aware client product no matter if communication with Ad-Aware Management Server fails.

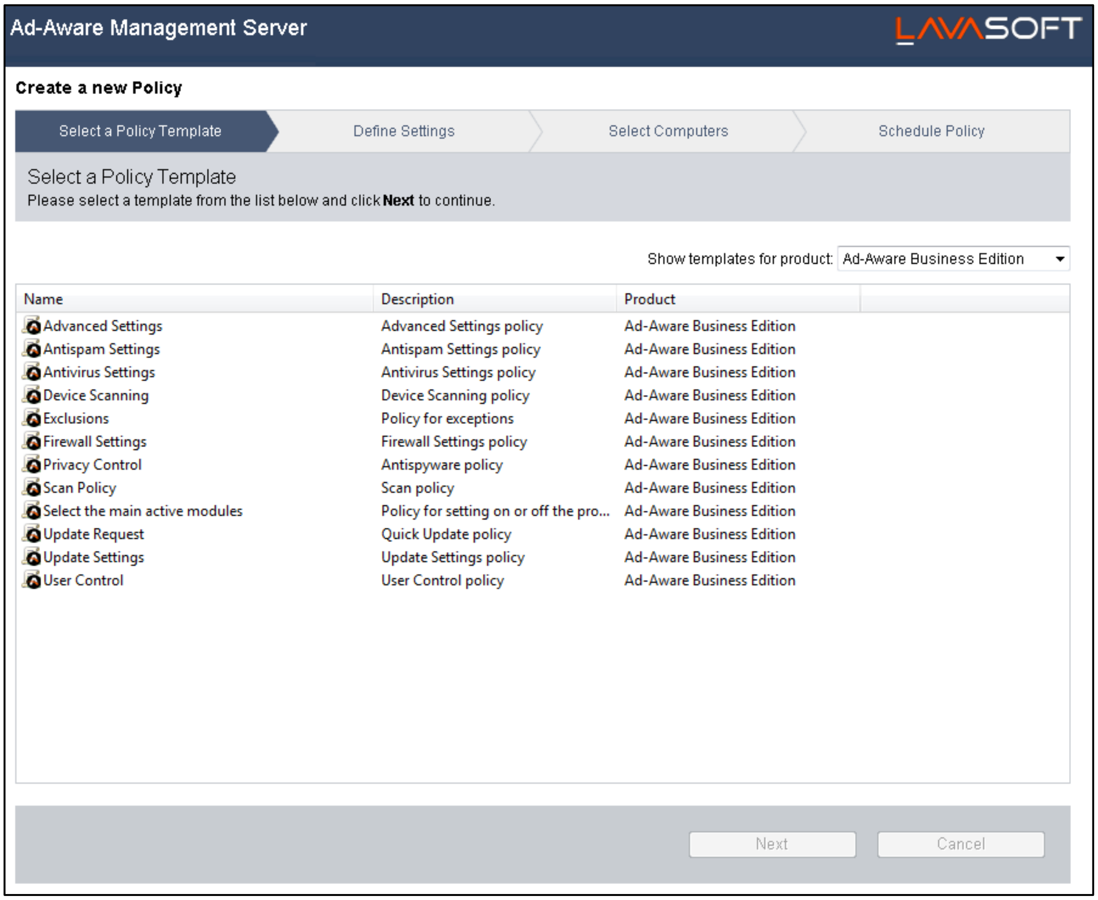
Policies can be assigned to individual clients or to entire groups of clients. You can also assign policies to local or network (Active Directory) users.

Creating New Policies

Policies are created based on built-in policy templates. A policy template contains a predefined set of options that allow you to configure a specific feature of a Ad-Aware product. Policy templates are product dependent, meaning that you can use them to create policies only for a specific product.

You can create and assign new policies in the Create New Policy pane. To display this pane, do one of the following:

- In the tree menu, go to **Policies > Create New Policy**.
- In the Policies pane, click the corresponding link.



Create a new Policy

Select a Policy Template

Please select a template from the list below and click **Next** to continue.

Show templates for product: Ad-Aware Business Edition

Name	Description	Product
Advanced Settings	Advanced Settings policy	Ad-Aware Business Edition
Antispam Settings	Antispam Settings policy	Ad-Aware Business Edition
Antivirus Settings	Antivirus Settings policy	Ad-Aware Business Edition
Device Scanning	Device Scanning policy	Ad-Aware Business Edition
Exclusions	Policy for exceptions	Ad-Aware Business Edition
Firewall Settings	Firewall Settings policy	Ad-Aware Business Edition
Privacy Control	Antispyware policy	Ad-Aware Business Edition
Scan Policy	Scan policy	Ad-Aware Business Edition
Select the main active modules	Policy for setting on or off the pro...	Ad-Aware Business Edition
Update Request	Quick Update policy	Ad-Aware Business Edition
Update Settings	Update Settings policy	Ad-Aware Business Edition
User Control	User Control policy	Ad-Aware Business Edition

Create New Policy Pane

Policy templates are grouped by product. You can choose which policy templates to view from the menu above the table. For detailed information on the options of each template and how to configure them, please refer to Policy Templates.

To create and assign a new policy, follow the wizard steps:

1. **Select a policy template**.
   a. Select the product you want to create the policy for from the menu. To view all policy templates available (of all Ad-Aware products), choose the corresponding option.
   b. Double-click the policy template you want to use (or select it and click **Next**).
2. **Define settings**.

   Configure the policy settings as needed and click **Next**. For detailed information on the options of each template and how to configure them, please refer to Policy Templates.
3. **Select the target computers**.

   You can choose one of the following options:

   - **Network computer**

     Select this option if you want to assign the policy to individual or groups of managed computers. The policy will be enforced for all users who log on to the target computers, regardless if they are local or network (Active Directory) users.

Note

User policies have priority over computer policies. If a different policy is configured for a specific user, the user policy will be applied when the user logs on instead of the computer policy.

You can choose specific computers, groups of managed computers or all managed computers. To view the managed computers as a list, select **Show list of network computers**.

By selecting a group, the policy will apply to any computer that is later added to the group (provided that the schedule you configure in the next step does not specify an end time).

- **Network users and groups**

  Select this option if you have an Active Directory domain and you want to assign the policy to specific network users or user groups. The policy will be enforced for selected users, regardless of the managed computer they log on to.

- **Local users**

  Select this option when you want to define special policies for local user accounts configured on the network computers (such as the built-in Administrator or Guest accounts). You must enter the name of the user account you want the policy to apply to (you cannot specify more than one user account).

  The policy will be applied on any managed computer when the specified user logs on.

Click **Next**.

4. **Schedule and save the policy.**

a) By default, the policy is applied as soon as possible (within a maximum of 5 minutes on LAN network computers or 1 hour over a VPN connection). Depending on the situation, you may want to change the default schedule.

- To run the policy at a later time, select the **Starting** check box and set the time as needed.
- To specify an end time after which the policy will no longer run, select the **Ending** check box and set the time as needed.

Note

The policy settings on the computers or user accounts on which the policy already ran will remain unchanged until a new policy is run.

- To run the policy on a regular basis, choose a convenient option from the **Schedule** menu and set the frequency using the second menu. You can specify when to start and when to end the schedule by selecting the **Starting** and **Ending** check boxes.

Note

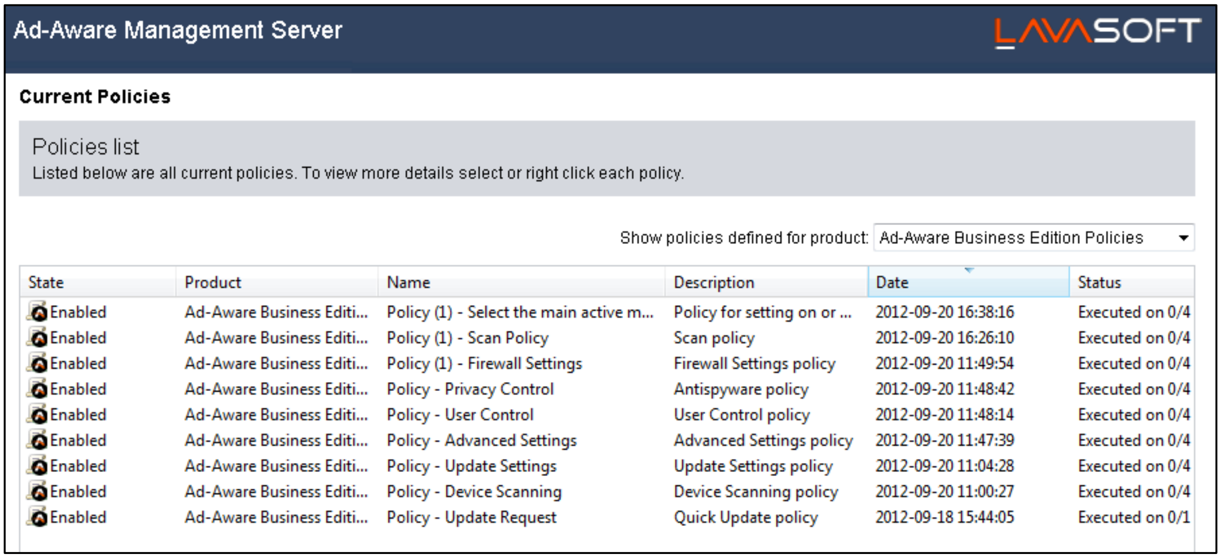
Update and scan policies will normally be configured to run regularly. For other policies, a one-time only execution schedule should be suited in most situations.

b) Click **Save Policy** to create the policy. The new policy will appear in the Current Policies pane, where you can manage it and check the results.

Current Policies

You can see and manage the active policies in the Current Policies pane. To display this pane, do one of the following:

- In the tree menu, go to **Policies > Current Policies**.
- In the Policies pane, click the corresponding link.



Current Policies

Policies list

Listed below are all current policies. To view more details select or right click each policy.

Show policies defined for product: Ad-Aware Business Edition Policies

State	Product	Name	Description	Date	Status
Enabled	Ad-Aware Business Editi...	Policy (1) - Select the main active m...	Policy for setting on or ...	2012-09-20 16:38:16	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy (1) - Scan Policy	Scan policy	2012-09-20 16:26:10	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy (1) - Firewall Settings	Firewall Settings policy	2012-09-20 11:49:54	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy - Privacy Control	Antispyware policy	2012-09-20 11:48:42	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy - User Control	User Control policy	2012-09-20 11:48:14	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy - Advanced Settings	Advanced Settings policy	2012-09-20 11:47:39	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy - Update Settings	Update Settings policy	2012-09-20 11:04:28	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy - Device Scanning	Device Scanning policy	2012-09-20 11:00:27	Executed on 0/4
Enabled	Ad-Aware Business Editi...	Policy - Update Request	Quick Update policy	2012-09-18 15:44:05	Executed on 0/1

Current Policies Pane

The current policies are grouped by product. You can see the policies of the selected category in the table. The table columns provide general information about each policy, including the execution status.

Policies can be managed using options from the shortcut menu.

"No Data Available" Status

The **No Data Available** status indicates that currently there are no computers or users available to apply the policy to.

This status is displayed in one of the following situations:

- The policy has been configured to run on a group that currently does not contain any computer.
- The policy has been configured to apply to a local user or to network users who have not logged on yet to a computer managed by Ad-Aware Management Server.
- The policy has run on the target computers, but the Ad-Aware client product has been removed from the respective computers afterwards.
- You have just imported policies from a policies file. You must assign imported policies to computers or users managed by this Ad-Aware Management Server instance.

Monitoring Policy Execution

To monitor the execution of a policy, right-click it and select **More details**. A new pane is displayed.

In this pane you can view summary information about the policy and a table with all computers on which it has been assigned to run. The table columns provide useful information about the policy execution status on computers (the last time the policy ran and the last synchronization time).

You can click a column header to sort information by that column. Click the column header again to change the sorting order.

To find out details for a specific computer, just click the corresponding table entry. Details will be displayed in a new section under the table.

Viewing and Editing Policy Settings

A policy allows configuring the same settings as the template based on which it was created. For detailed information on the options of each template, please refer to Policy Templates.

To view the settings of a specific policy, right-click the policy and select **View settings**. The settings will be displayed in a new pane. You can see the policy name and how its settings are configured. Click Close to return to the previous pane.

To edit the settings of a specific policy:

1. Right-click the policy and select **Edit settings**. A new pane, where you can modify the policy settings, will be displayed.
2. Make the desired changes by selecting new settings or providing other parameters.
3. If you want to, you can change the computers or users the policy will apply to (go to the **Select Computers** tab).
4. Go to the **Scheduler** tab and configure the schedule as needed. To run the policy as soon as possible, set the schedule to **One time** with no start time.
5. Click **Save** to save the changes and to return to the Current Network Tasks pane. The modified policy will apply to selected computers or users according to the schedule.

If you want to go back without saving any changes, click **Cancel**.

Changing Policy Schedule

In some situations, you may want to change the current policy execution schedule. For example when the configured end time has passed or if the regular schedule is no longer suited. The policy will run on selected computers or user accounts according to the new schedule.

To change the current schedule of a policy:

1. Right-click the policy and select **Edit settings**.
2. Click the **Scheduler** tab.

3. Change the policy schedule as needed. To run the policy as soon as possible, set the schedule to **One time** with no start time.
4. Click **Save** to save the changes and to return to the Current Policies pane.

Checking and Changing Policy Assignments

To check what computers and users the policy is assigned to apply to and to change current assignments:

1. Right-click the policy and select **Edit settings**. A new pane, where you can modify the policy settings, will be displayed.
2. Click the **Select Computers** tab. You can see the computers, groups or users the policy is assigned to.
3. If you want to go back without saving any changes, click **Cancel**. To change the current assignments, follow the next steps.
4. Select the check boxes corresponding to the computers or computer groups you want the policy to apply to. To assign the policy to network users, select **Network users and groups** and choose the desired users and groups. To assign the policy to local users, select **Local users** and enter the name of the user account.
5. Go to the **Scheduler** tab and configure the schedule as needed. To run the policy as soon as possible, set the schedule to **One time** with no start time.
6. Click **Save** to save the changes and to return to the Current Policies pane.

Renaming Policies and Changing Their Description

When you create more than one instance of the same policy, additional instances will have a number in front of their name. This number indicates the order in which they were created. You should consider renaming instances of the same policy and change their description so that you can quickly identify them.

To rename a policy, follow these steps:

1. Right-click the policy and select **Change name**.
2. Type a new name in the edit field.
3. Press ENTER.

To change the description of a policy, follow these steps:

1. Right-click the policy and select **Change description**.
2. Type a new description in the edit field.
3. Press ENTER.

Deleting Policies

If you no longer need a policy and its details, you can delete it.

To delete a policy, right-click it and select **Delete**. You will have to confirm your action by clicking **Yes**.

Enabling/Disabling Policies

Active policies, which have not run on all selected computers or which are set to run regularly, can be disabled anytime you want, for as long as needed. When disabled, a policy cannot be applied to assigned computers. To disable an active policy, right-click it and select **Disable**. To activate a disabled policy, right-click it and select **Enable**.

Note

The change becomes effective as soon as the agent synchronizes with Ad-Aware Management Server (by default, within maximum 5 minutes in LAN networks or 1 hour over a VPN connection).

Exporting and Importing Policies

If you use several Ad-Aware Management Server instances to manage the network, you do not have to configure the security policies separately for each of them. Once you have configured all the necessary policies on a particular Ad-Aware Management Server instance, you can use Export/Import Policies Tool to replicate policies on the other Ad-Aware Management Server instances.

Export/Import Policies Tool helps you export the policies configured on a specific Ad-Aware Management Server instance and import them on other Ad-Aware Management Server instances. Only the policy settings are saved, not the client computers and groups they apply to.

Note

This tool is not intended to be used as a fail-safe option in case the Ad-Aware Management Server configuration is corrupted. To be prepared for such extreme situations, you can periodically back up all product configuration data (including current policies and their assignment) using the Backup/Restore Server Configuration Tool. For more information, please refer to Backup/Restore Server Configuration Tool.

The policy replication process consists of these main steps:

1. Export current policies configured on a specific Ad-Aware Management Server instance to a policies file.
2. Transfer the policies file to the Ad-Aware Management Server computers on which you want to replicate the saved policies. You can also copy the policies file to a network share available to these computers.
3. Import the policies from the policies file to the other Ad-Aware Management Server instances.
4. Assign the imported policies to managed computers and groups, as needed.

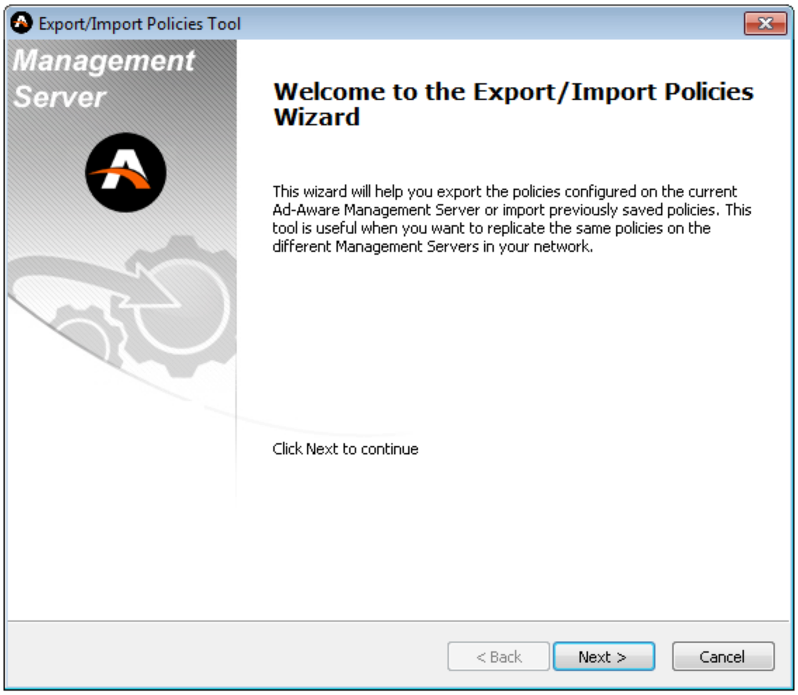
Exporting Policies

To export the current policies of Ad-Aware Management Server:

1. Open the management console and connect to Ad-Aware Management Server.
2. On the **Tools** menu, click **Export/Import Policies Tool**. A wizard will appear.

3. Complete the wizard. You must select **Export Policies** in the second step of the wizard.

Step 1/4 - Welcome Window



Welcome to the Export/Import Policies Wizard

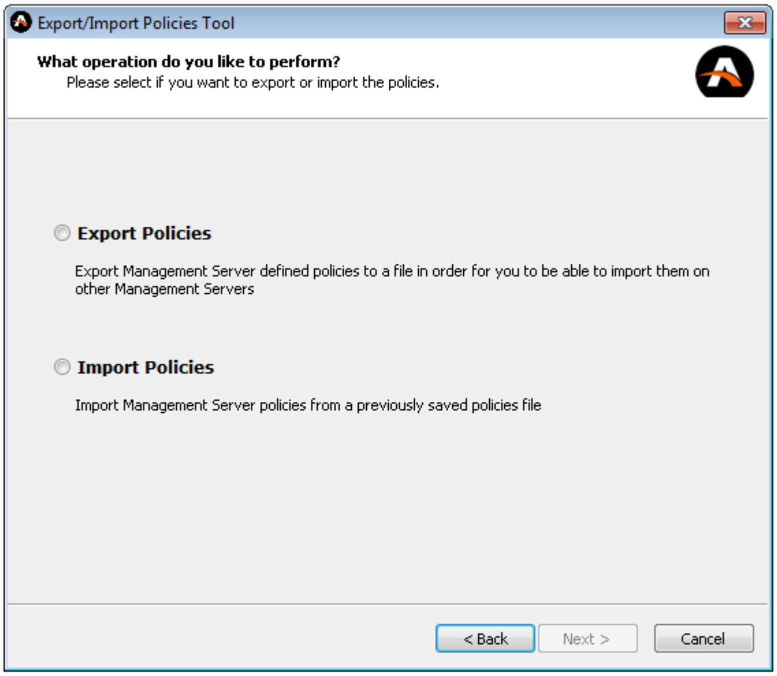
This wizard will help you export the policies configured on the current Ad-Aware Management Server or import previously saved policies. This tool is useful when you want to replicate the same policies on the different Management Servers in your network.

Click Next to continue

Welcome Window

Click **Next**.

Step 2/4 - Select Export Policies



What operation do you like to perform?
Please select if you want to export or import the policies.

○ **Export Policies**

Export Management Server defined policies to a file in order for you to be able to import them on other Management Servers

○ **Import Policies**

Import Management Server policies from a previously saved policies file

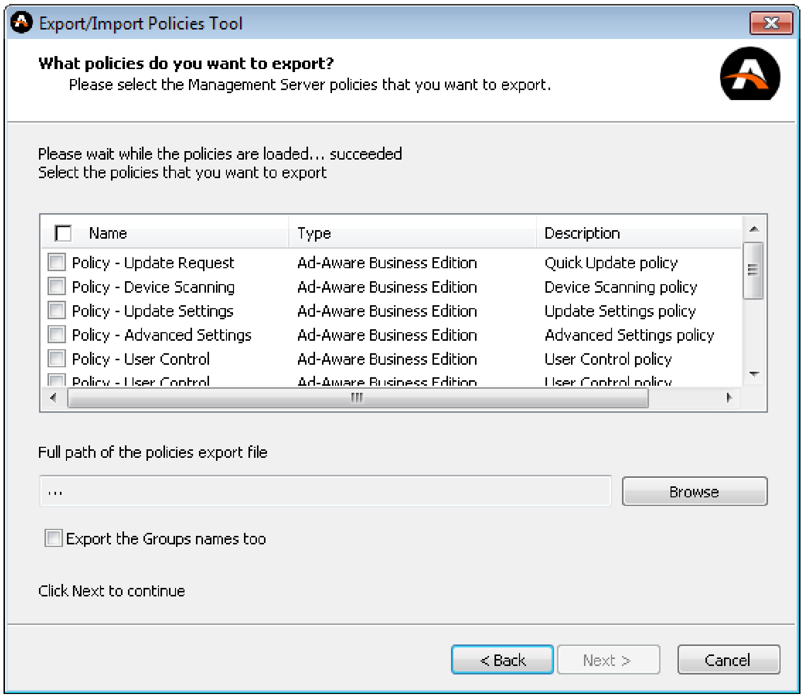
Select Export Policies

The following options are available:

- **Export Policies** - to save the current policies configured on Ad-Aware Management Server to a policies file.
- **Import Policies** - to import policies from a policies file.

Select the first option and click **Next.**

Step 3/4 - Configure Export Options



Export/Import Policies Tool

What policies do you want to export?

Please select the Management Server policies that you want to export.

Please wait while the policies are loaded... succeeded
Select the policies that you want to export

□ Name	Type	Description
□ Policy - Update Request	Ad-Aware Business Edition	Quick Update policy
□ Policy - Device Scanning	Ad-Aware Business Edition	Device Scanning policy
□ Policy - Update Settings	Ad-Aware Business Edition	Update Settings policy
□ Policy - Advanced Settings	Ad-Aware Business Edition	Advanced Settings policy
□ Policy - User Control	Ad-Aware Business Edition	User Control policy
□ Policy - User Control	Ad-Aware Business Edition	User Control policy

Full path of the policies export file

...

□ Export the Groups names too

Click Next to continue

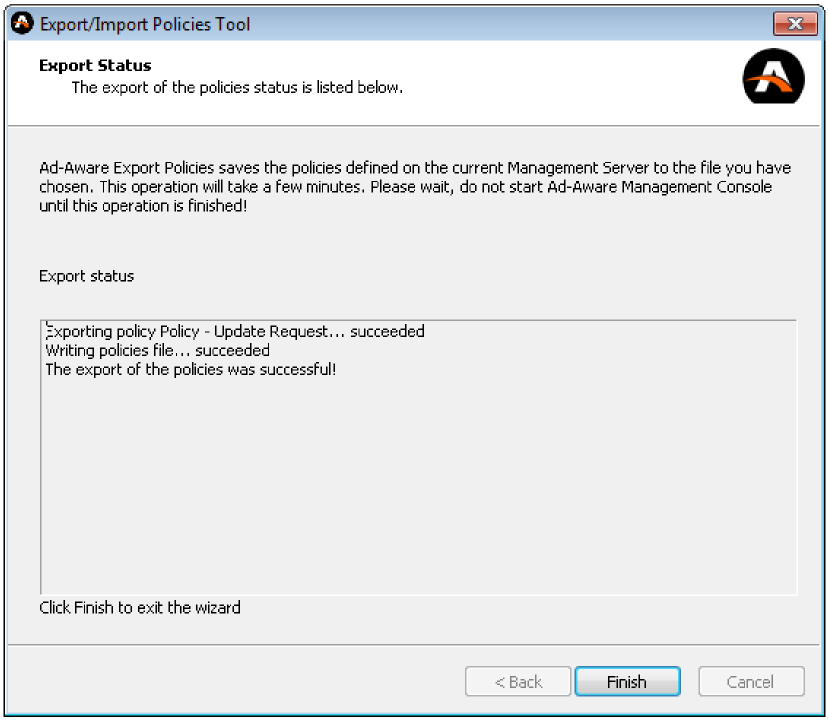
Configure Export Options

You can see the current policies defined on Ad-Aware Management Server. Select the policies to be exported. To export all policies, select the check box next to the **Name** column header.

You must also specify where the selected policies should be saved. Click **Browse** and choose where and under what name to save the policies file. The files containing the exported Ad-Aware Management Server policies have the .pce extension.

Click **Next** to export the selected policies.

Step 4/4 – Finish



Export Status

The export of the policies status is listed below.

Ad-Aware Export Policies saves the policies defined on the current Management Server to the file you have chosen. This operation will take a few minutes. Please wait, do not start Ad-Aware Management Console until this operation is finished!

Export status

```
Exporting policy Policy - Update Request... succeeded
Writing policies file... succeeded
The export of the policies was successful!
```

Click Finish to exit the wizard

Finish

Wait until the policies are exported, then click **Finish**.

You must transfer the policies file to the other Ad-Aware Management Server computers on which you want to import the policies.

Importing Policies

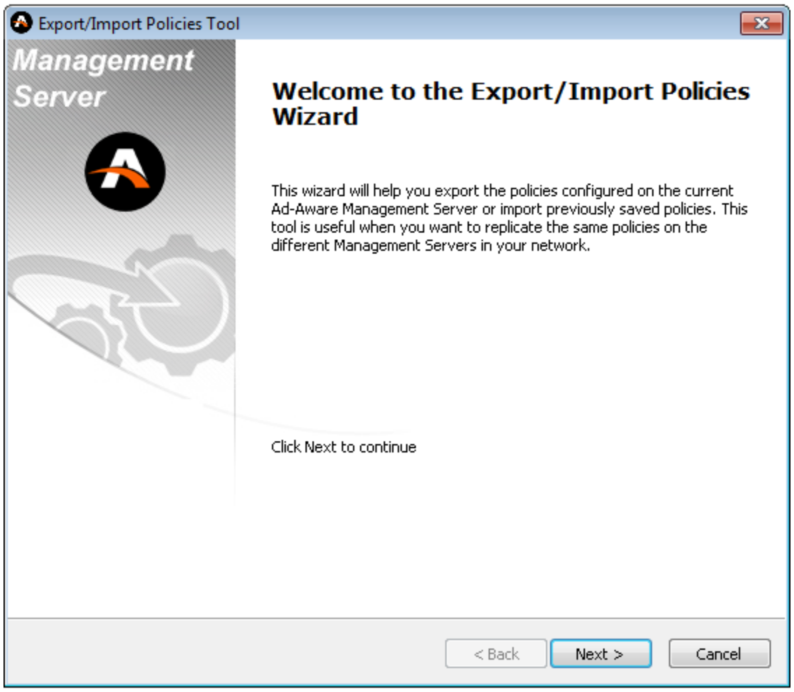
To import policies to Ad-Aware Management Server, follow these steps:

1. Open the management console and connect to Ad-Aware Management Server.
2. On the **Tools** menu, **click Export/Import Policies Tool**. A wizard will appear.
3. Complete the wizard. You must select **Import Policies** in the second step of the wizard.

Note

The imported policies will merge with (but will not replace) the policies already defined on Ad-Aware Management Server. If a current policy has the same name as one of the imported policies, the imported policy will be named differently.

Step 1/4 - Welcome Window



Welcome to the Export/Import Policies Wizard

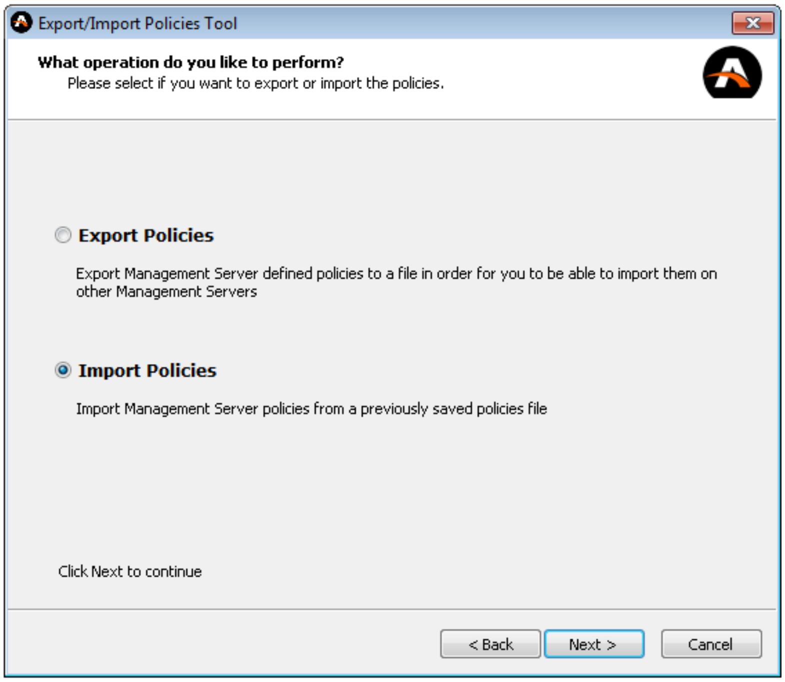
This wizard will help you export the policies configured on the current Ad-Aware Management Server or import previously saved policies. This tool is useful when you want to replicate the same policies on the different Management Servers in your network.

Click Next to continue

Welcome Window

Click **Next**.

Step 2/4 - Select Import Policies



What operation do you like to perform?
Please select if you want to export or import the policies.

○ **Export Policies**

Export Management Server defined policies to a file in order for you to be able to import them on other Management Servers

● **Import Policies**

Import Management Server policies from a previously saved policies file

Click Next to continue

Select Import Policies

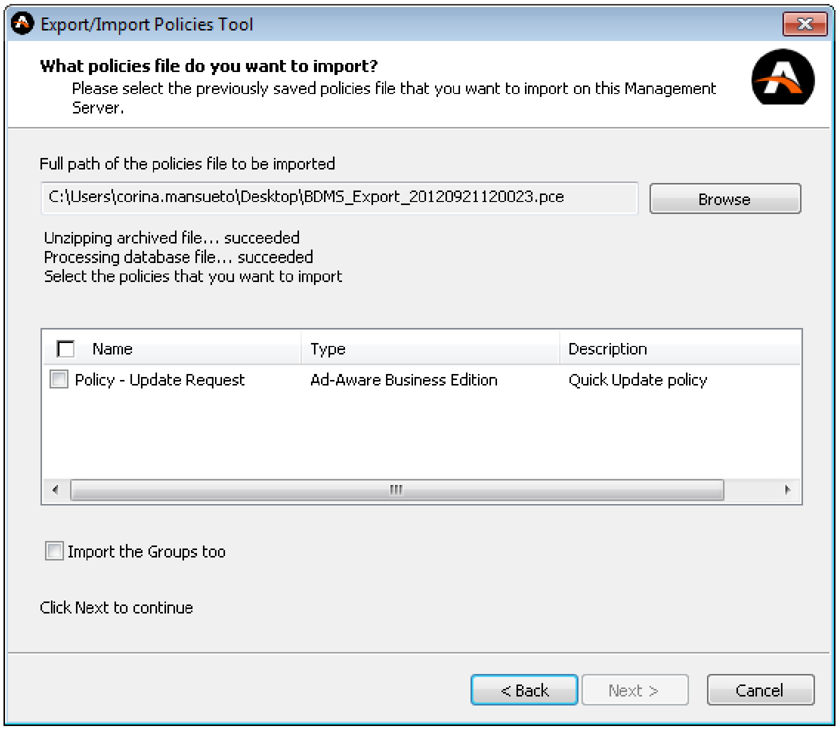
The following options are available:

- **Export Policies** - to save the current policies configured on Ad-Aware Management Server to a policies file.

- **Import Policies** - to import policies from a policies file.

Select the second option and click **Next**.

Step 3/4 - Select Policies File


Export/Import Policies Tool

What policies file do you want to import?

Please select the previously saved policies file that you want to import on this Management Server.

Full path of the policies file to be imported

C:\Users\corina.mansueto\Desktop\BDMS_Export_20120921120023.pce

Unzipping archived file... succeeded
Processing database file... succeeded
Select the policies that you want to import

□ Name	Type	Description
□ Policy - Update Request	Ad-Aware Business Edition	Quick Update policy

□ Import the Groups too

Click Next to continue

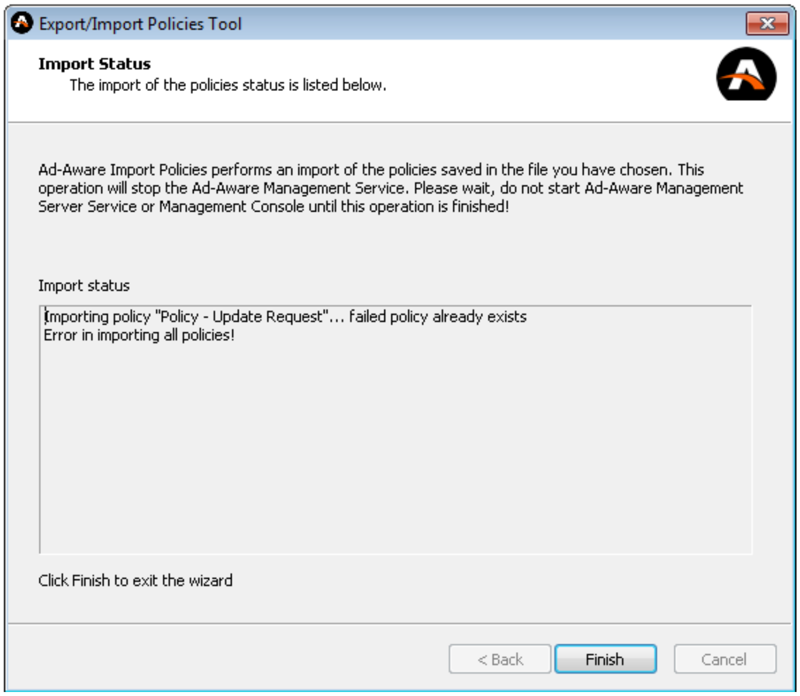
Select Policies File

You must specify the location of the file containing the policies you want to import. Click **Browse**, locate and open the policies file. The files containing the exported Ad-Aware Management Server policies have the . pce extension.

Once you open the file, you can see the policies it contains. Select the policies you want to import. To import all policies, select the check box next to the **Name** column header.

Click **Next** to import the selected policies.

Step 4/4 – Finish



Import Status

The import of the policies status is listed below.

Ad-Aware Import Policies performs an import of the policies saved in the file you have chosen. This operation will stop the Ad-Aware Management Service. Please wait, do not start Ad-Aware Management Server Service or Management Console until this operation is finished!

Import status

```
Importing policy "Policy - Update Request"... failed policy already exists
Error in importing all policies!
```

Click Finish to exit the wizard

Finish

Wait until the policies are imported, then click **Finish**.

Next, go to the Current Policies pane and assign the imported policies to managed computers and groups, as needed.

Network Tasks

Ad-Aware Management Server provides you with a series of useful network management tasks designed to facilitate administrative control over the network. The tasks are based on Windows Management Instrumentation (WMI) and on the Ad-Aware policy technology. In earlier versions, they were known as WMI scripts.

Note

Windows® Management Instrumentation (WMI) is the Microsoft® implementation of Web-Based Enterprise Management (WBEM), an initiative to establish standards for accessing and sharing management information over an enterprise network. WMI is WBEM-compliant and provides integrated support for Common Information Model (CIM), the data model that describes the objects that exist in a management environment.

You can run network tasks on remote network computers managed by Ad-Aware Management Server, in order to:

- Find out useful information about the network computers, such as system information, installed software, startup programs, free disk space and so on.
- Remove software installed on the network computers.

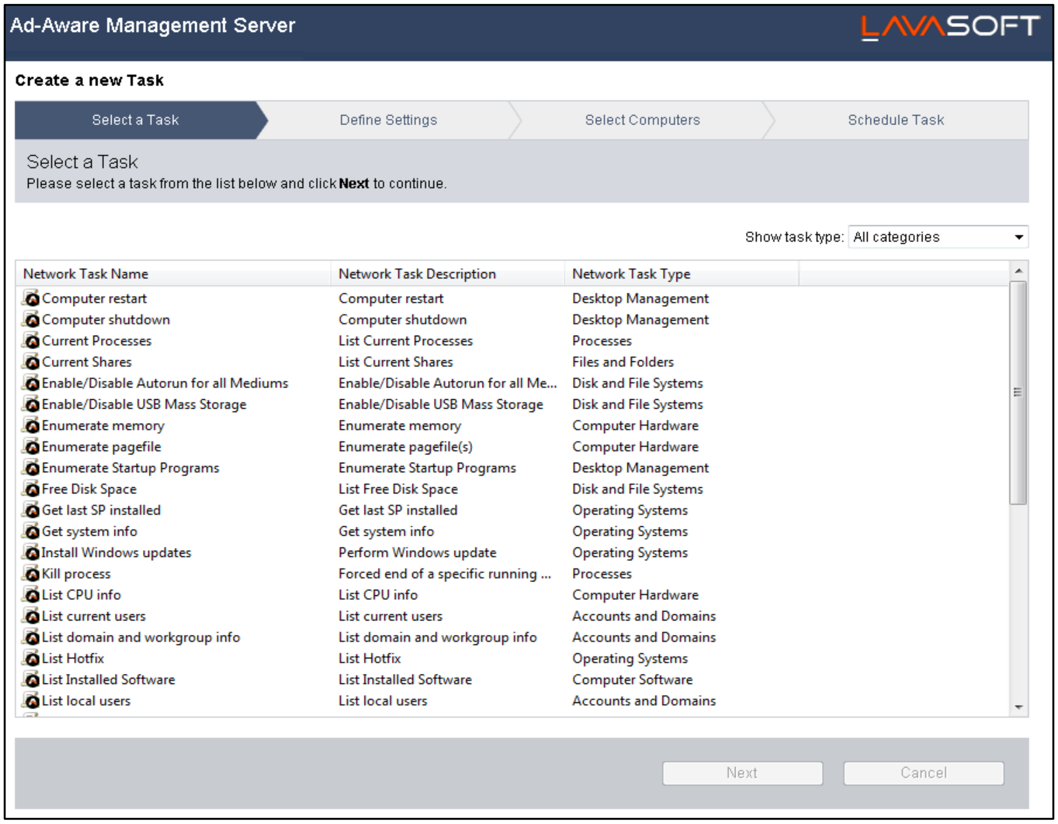
- Kill specific processes running on the network computers.
- Restart or shutdown the network computers.
- Log off the user logged on the network computers.
- install available Windows updates or configure Windows Automatic Updates on the
- Network computers.
- Enable/disable autorun or USB storage devices on the network computers.
- Change the Remote Desktop Connection settings on the network computers.
- Inform users about administrative tasks that are going to be performed on their computer.

Creating New Network Tasks

You can create and run new network tasks from the Create New Network Task pane.

To display this pane, do one of the following:

- In the tree menu, go to **Network Tools** > **Tasks** > **Create New Network Task**.
- In the Network Tools pane, click the corresponding link.



Create a new Task

Select a Task

Please select a task from the list below and click **Next** to continue.

Show task type: All categories

Network Task Name	Network Task Description	Network Task Type
Computer restart	Computer restart	Desktop Management
Computer shutdown	Computer shutdown	Desktop Management
Current Processes	List Current Processes	Processes
Current Shares	List Current Shares	Files and Folders
Enable/Disable Autorun for all Mediums	Enable/Disable Autorun for all Me...	Disk and File Systems
Enable/Disable USB Mass Storage	Enable/Disable USB Mass Storage	Disk and File Systems
Enumerate memory	Enumerate memory	Computer Hardware
Enumerate pagefile	Enumerate pagefile(s)	Computer Hardware
Enumerate Startup Programs	Enumerate Startup Programs	Desktop Management
Free Disk Space	List Free Disk Space	Disk and File Systems
Get last SP installed	Get last SP installed	Operating Systems
Get system info	Get system info	Operating Systems
Install Windows updates	Perform Windows update	Operating Systems
Kill process	Forced end of a specific running ...	Processes
List CPU info	List CPU info	Computer Hardware
List current users	List current users	Accounts and Domains
List domain and workgroup info	List domain and workgroup info	Accounts and Domains
List Hotfix	List Hotfix	Operating Systems
List Installed Software	List Installed Software	Computer Software
List local users	List local users	Accounts and Domains

Create New Network Task Pane

You can see the available network management tasks in the table. You can run these tasks in order to find out more information about the managed computers and to perform administrative tasks. Check appendix Available Network Tasks for a detailed description of each network task.

Tasks are grouped into several categories. You can filter displayed tasks by choosing a task category from the menu above the table.

To create and run a new task, follow the wizard steps:

1. **Select a task**.

   Double-click the task you want to use (or select it and click **Next**).

2. **Define settings**.

   Configure the task settings (if any) and click **Next**.

   Note

   Only the following tasks have configurable settings:

   - Enable/Disable autorun for all drives
   - Enable/Disable USB mass storage
   - Install Windows updates
   - Kill process
   - List installed software
   - Remote Desktop Connection
   - Remove software
   - Run program
   - Send message
   - Windows automatic updating

   For more information, please refer to Examples of Using Tasks.

3. **Select the target computers.**
   You can choose one of the following options:

   - **Network computer**

     Select this option if you want to run the task on individual or groups of managed computers. You can choose specific computers, groups of managed computers or all managed computers. To view the managed computers as a list, select **Show list of network computers**.

     By selecting a group, the task will also run on any computer that is later added to the group (provided that the schedule you configure in the next step does not specify an end time).

   - **Network users and groups**

     Select this option if you have an Active Directory domain and you want the task to run when specific network users are logged on to a managed computer.

   - **Local users**

     Select this option if you want the task to run when a specific local user is logged on to a managed computer (such as the built-in Administrator or Guest accounts). You must enter the name of the user account (you cannot specify more than one user account).

Click **Next**.

4. **Schedule and save the task**.

a) By default, the task will run as soon as possible (within a maximum of 5 minutes after the task assignment). Depending on the situation, you may want to change the default schedule.

- To run the task at a later time, select the **Starting** check box and set the time as needed.
- To run the task on a regular basis, choose a convenient option from the **Schedule** menu and set the frequency using the second menu. You can specify when to start and when to end the schedule by selecting the Starting and **Ending** check boxes.

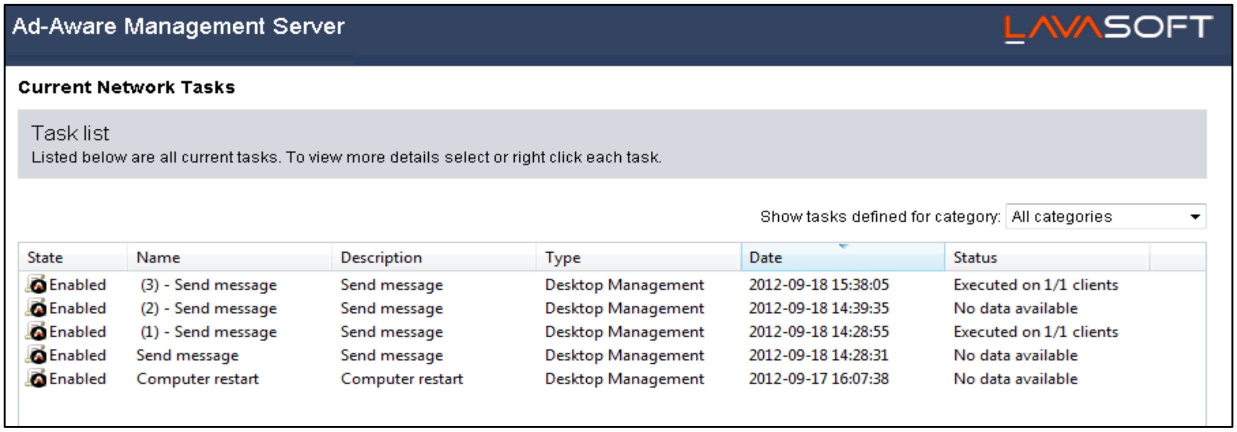
> **Note**
>
> You will set most tasks to run one-time only (occasionally with a fixed end date). In rare situations, you may want to run the task on a regular basis (for example, to automatically shut down network computers or log off users at the end of the working hours).

b) **Click Save Task** to create and run the task. The new task will appear in the Current Network Tasks pane, where you can manage it and check the results.

Current Network Tasks

You can check task results and manage your tasks in the Current Network Tasks pane. To display this pane, do one of the following:

- In the tree menu, go to **Network Tools** > **Tasks** > **Current Network Tasks**.
- In the Network Tools pane, click the corresponding link.



Current Network Tasks

Task list

Listed below are all current tasks. To view more details select or right click each task.

Show tasks defined for category: All categories

State	Name	Description	Type	Date	Status
Enabled	(3) - Send message	Send message	Desktop Management	2012-09-18 15:38:05	Executed on 1/1 clients
Enabled	(2) - Send message	Send message	Desktop Management	2012-09-18 14:39:35	No data available
Enabled	(1) - Send message	Send message	Desktop Management	2012-09-18 14:28:55	Executed on 1/1 clients
Enabled	Send message	Send message	Desktop Management	2012-09-18 14:28:31	No data available
Enabled	Computer restart	Computer restart	Desktop Management	2012-09-17 16:07:38	No data available

Current Network Tasks Pane

The current network tasks (task instances you have created and configured to run on network computers) are displayed in the table. The table columns provide general information about each task, including the execution status. You can filter displayed tasks by choosing a task category from the menu above the table.

To check task results or manage a task, right-click it and use the options from the shortcut menu.

"No Data Available" Status

The No Data Available status indicates that currently there are no computers available to run the task on.

This status is displayed in one of the following situations:

- The task has been configured to run on a group that currently does not contain any computers.
- The task has been configured to run under a local or network user account that has not been used yet on any computer managed by Ad-Aware Management Server.
- Ad-Aware Management Server no longer manages the computers the task has been configured to run on.

Checking Task Results

To check the results of a current task, right-click it and select **More details**. A new pane is displayed.

In this pane you can view summary information about the task and a table with all computers on which it has been assigned to run. The table columns provide useful information about the task's execution status on computers (the last time the task ran and the last synchronization time).

You can click a column header to sort information by that column. Click the column header again to change the sorting order.

To find out details for a specific computer, just click the corresponding table entry. Details will be displayed in a new section under the table.

Note

For the List installed software task, you can see a link above the table. Click the link if you want to remove undesired software installed on the managed computers. For more information, please refer to Application Control.

Viewing and Editing Task Settings

Only the following tasks have configurable settings:

- Enable/Disable autorun for all drives
- Enable/Disable USB mass storage
- Install Windows updates
- Kill process
- List installed software
- Remote Desktop Connection
- Remove software
- Run program
- Send message
- Windows automatic updating

To view the settings of a task right-click the task and select **View settings**. The template settings will be displayed in a new pane. Click **Close** to return to the previous pane.

To edit the settings of a task:

1. Right-click the task and select **Edit settings**. A new pane will be displayed.

2. Configure each task as follows:
   - **Enable/Disable autorun for all drives**. Select whether to enable or disable the Windows autorun feature for all drives.
   - **Enable/Disable USB mass storage**. Select whether to allow or block USB storage devices.
   - **Install Windows updates**. Select to find out information about the available Windows updates or to install Windows updates.
   - **Kill process**. Type the name of the process you want to terminate.
   - **List installed software**. If you also need information about the Microsoft and Windows updates installed on the client computers, select **Show updates**.
   - **Remote Desktop Connection**. Select whether to allow or block incoming Remote Desktop connections.
   - **Remove software**. In the edit field, type the name of the software you want to be removed.
   - **Run program**. Specify the path to the application you want to run and additional parameters.
   - **Send message**. In the edit field, type the message you want to send.
   - **Windows automatic updating**. Configure the Windows Automatic Updates options as needed.

Note

For more information, please refer to Examples of Using Tasks.

3. If you want to, you can change the computers the task will run on (go to the **Select Computers** tab).
4. Go to the **Scheduler** tab and configure the schedule as needed. To run the task as soon as possible, set the schedule to **One time** with no start time.
5. Click **Save** to save the changes and to return to the Current Network Tasks pane.

The modified task will run on selected computers according to the schedule.

Important

Existing task results will be lost after saving changes. If you want to keep the task results, click Cancel.

Running a Task Again

If you run a current task again, existing task results will be lost.

To run a current task again:

1. Right-click the task and select **Edit settings**.
2. If you want to, you can change the task settings (if any) or the computers the task will run on (go to the **Select Computers** tab).
3. Click the **Scheduler** tab.
4. To run the task as soon as possible, set the schedule to **One time** with no start time. Or, you can configure a schedule that suits you better.
5. Click **Save** to save the changes and to return to the Current Network Tasks pane.

The modified task will run on selected computers according to the schedule.

Changing Task Schedule

In some situations, you may want to change the current task execution schedule. For example when the configured end time has passed or if the regular schedule is no longer suited. the task will run on selected computers according to the new schedule.

Existing task results will be lost.

To change the current schedule of a task:

1. Right-click the task and select **Edit settings**.
2. Click the **Scheduler** tab.
3. Change the task schedule as needed. To run the task as soon as possible, set the schedule to **One time** with no start time.
4. Click **Save** to save the changes and to return to the Current Network Tasks pane.

Running Tasks on Other Computers

If you choose to run a current task on other computers, existing task results will be lost.

To run a task on other computers:

1. Right-click the task and select **Edit settings**.
2. Click the **Select Computers** tab.
3. Select the check boxes corresponding to the computers or computer groups you want the task to run on. To run the task on all managed computers, select the check box corresponding to the server's name.
4. Go to the **Scheduler** tab and configure the schedule as needed. To run the task as soon as possible, set the schedule to **One time** with no start time.
5. Click **Save** to save the changes and to return to the Current Network Tasks pane.

The modified task will run on selected computers according to the schedule.

Renaming Tasks and Changing Their Description

When you create more than one instance of the same task, additional instances will have a number in front of their name. This number indicates the order in which they were created. You should consider renaming instances of the same task and change their description so that you can quickly identify them.

To rename a task, follow these steps:

1. Right-click the task and select **Change name**.
2. Type a new name in the edit field.
3. Press ENTER.

To change the description of a task, follow these steps:

1. Right-click the task and select **Change description**.
2. Type a new description in the edit field.

3. Press ENTER.

Deleting Tasks

When you no longer need the results of a task, you should delete it.

To delete a task, right-click it and select **Delete**. You will have to confirm your action by clicking **Yes**.

Enabling/Disabling Tasks

Active tasks, which have not run on all selected computers or which are set to run regularly, can be disabled anytime you want, for as long as needed. When disabled a task cannot be executed on the assigned computers.

To disable an active task, right-click it and select **Disable**. To activate a disabled task, right-click it and select **Enable**.

Note

The change becomes effective as soon as the agent synchronizes with Ad-Aware Management Server (by default, within maximum 5 minutes in LAN networks or 1 hour over a VPN connection).

Examples of Using Tasks

Here are some examples of how you can use the network management tasks provided by Ad-Aware Management Server:

- Gathering Information about Client Workstations
- Application Control
- Monitoring Processes Running on Client Workstations
- Changing Remote Desktop Connection Settings
- Sending Messages to Client Workstations
- Running Programs on Client Workstations
- Configuring Windows Automatic Updates on Client Workstations
- Updating Windows on Client Workstations
- Enabling/Disabling Autorun or USB Storage Devices on Client Workstations

Gathering Information about Client Workstations

The network management tasks can be successfully used in the troubleshooting process. You can remotely run specific tasks to obtain preliminary information about client workstations having issues. Based on this information, you can better assess the problem and find potential quick fixes.

Note

You can find a detailed description of each network task in appendix Available Network Tasks.

The **Get system info** task, for example, provides useful information about client workstations, such as:

- Operating system information
- System name, model and manufacturer
- Total RAM memory
- Processor
- BIOS version

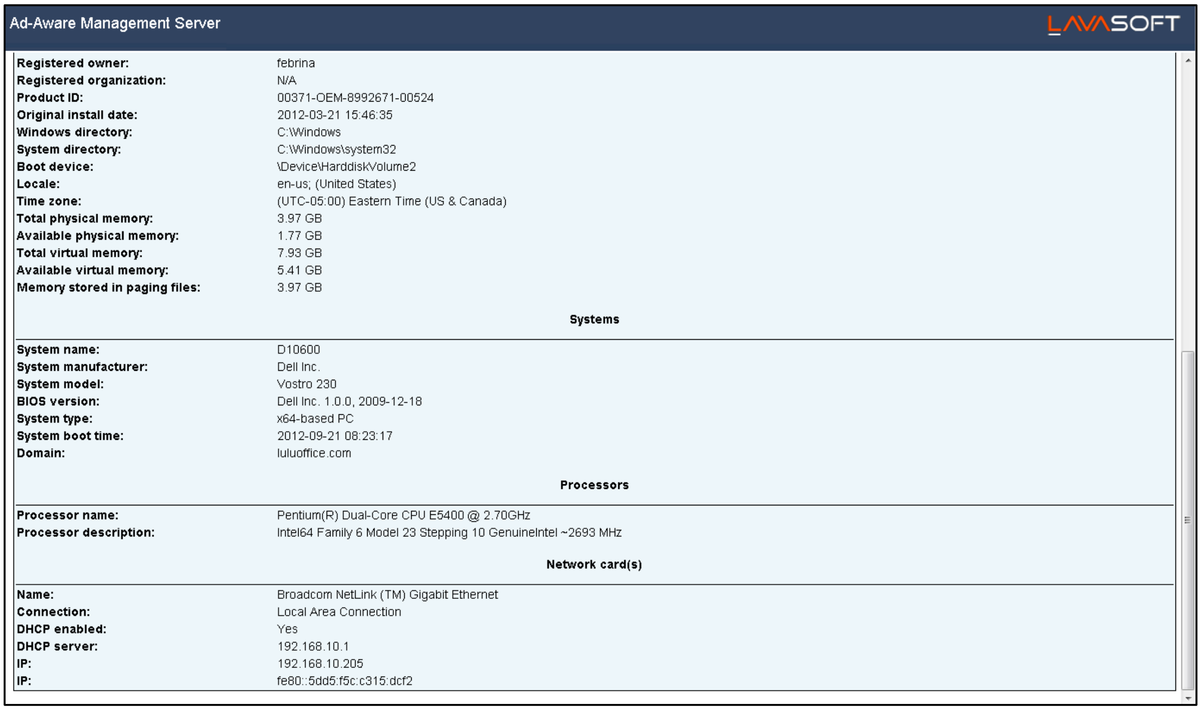
To create and run a Get system info task, follow these steps:

1. In the Create New Network Task pane, double-click the **Get system info** task (or select it and click **Next**).
2. Select the check boxes corresponding to the computers or computer groups you want the task to run on. To run the task on all managed computers, select the check box corresponding to the server's name.

   Note

   You can also choose to run the task on the managed computers on which specific network (Active Directory) or local users are logged on. However, this assignment method is uncommon for tasks used for gathering information.
3. Click **Next**.
4. By default, the task is executed on a selected client the next time that client synchronizes with Ad-Aware Management Server (within a maximum of 5 minutes after the task assignment).
5. Click **Save Task** to create and run the task. The new task will appear in the Current Network Tasks pane.

Once the task is executed, you can check the results in the Current Network Tasks pane by double-clicking the task. The following image provides an example of such results for a client workstation:



```
Registered owner:                febrina
Registered organization:         N/A
Product ID:                      00371-OEM-8992671-00524
Original install date:           2012-03-21 15:46:35
Windows directory:               C:\Windows
System directory:                C:\Windows\system32
Boot device:                     \Device\HarddiskVolume2
Locale:                          en-us; (United States)
Time zone:                       (UTC-05:00) Eastern Time (US & Canada)
Total physical memory:           3.97 GB
Available physical memory:       1.77 GB
Total virtual memory:            7.93 GB
Available virtual memory:        5.41 GB
Memory stored in paging files:   3.97 GB

                                        Systems

System name:                     D10600
System manufacturer:             Dell Inc.
System model:                    Vostro 230
BIOS version:                    Dell Inc. 1.0.0, 2009-12-18
System type:                     x64-based PC
System boot time:                2012-09-21 08:23:17
Domain:                          luluoffice.com

                                        Processors

Processor name:                  Pentium(R) Dual-Core CPU E5400 @ 2.70GHz
Processor description:           Intel64 Family 6 Model 23 Stepping 10 GenuineIntel ~2693 MHz

                                        Network card(s)

Name:                            Broadcom NetLink (TM) Gigabit Ethernet
Connection:                      Local Area Connection
DHCP enabled:                    Yes
DHCP server:                     192.168.10.1
IP:                              192.168.10.205
IP:                              fe80::5dd5:f5c:c315:dcf2
```

Get System Info

Application Control

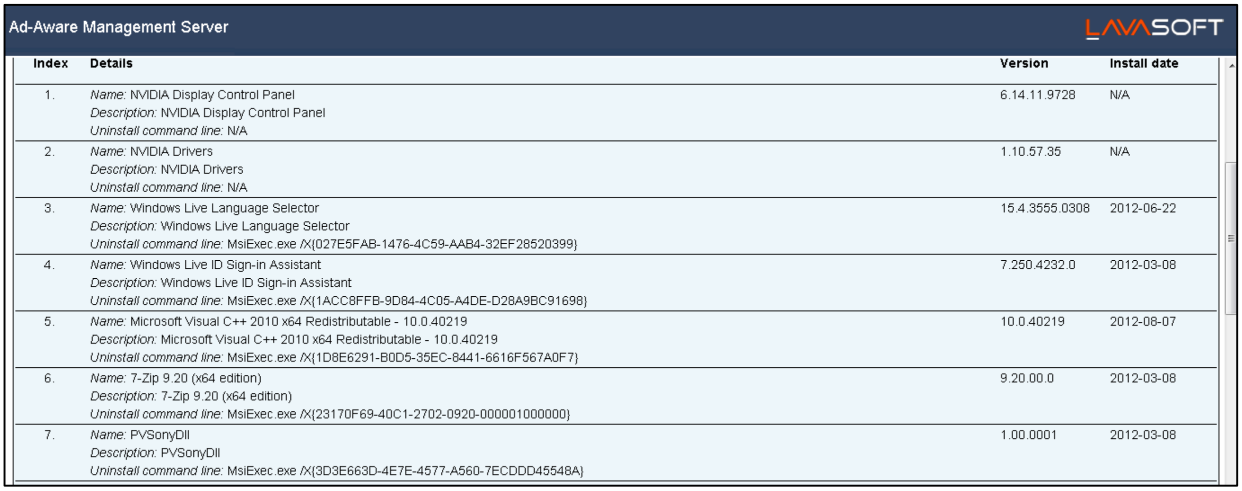
A number of tasks help maintain compliance with the organization's policies regarding the use of applications. Using only the Ad-Aware Management Console, you can easily find out what software is installed on client workstations and remove any undesired application.

Step 1 - Verifying Installed Applications

To verify the applications installed on client workstations, you can use the **List installed software** task. This task can be used to obtain the list of all the applications installed on client workstations, including Microsoft and Windows updates.

Run the task on the desired workstations. Once the task is executed, you can check the results in the Current Network Tasks pane by double-clicking the task.

The following image provides an example of such results for a client workstation:



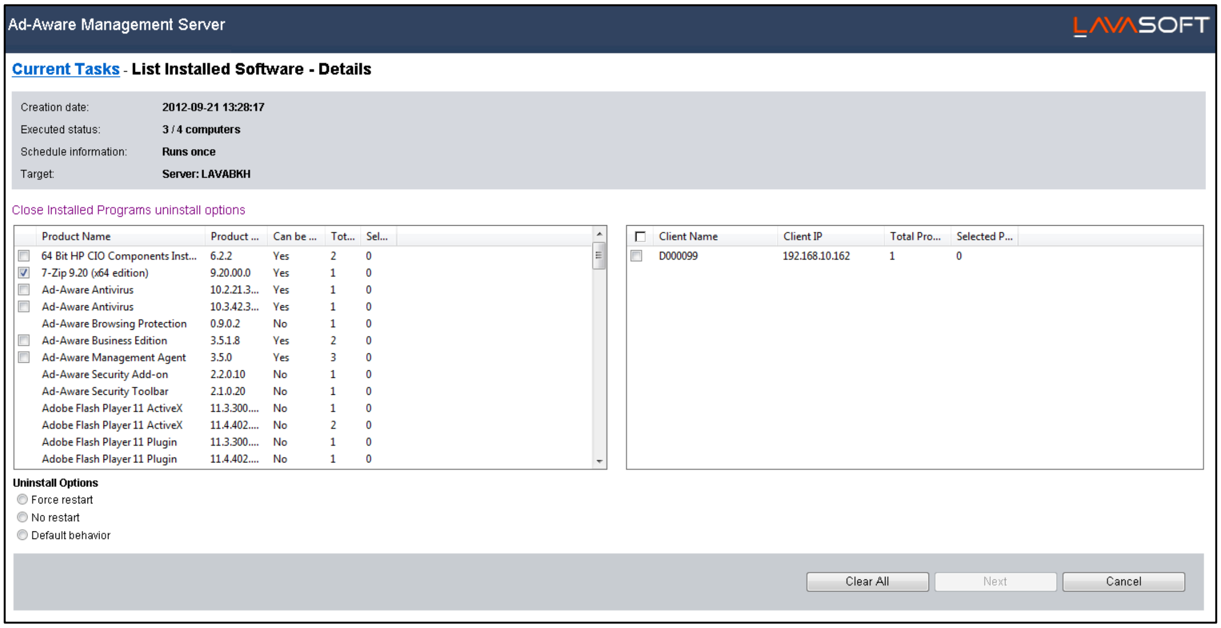
Index	Details	Version	Install date
1.	*Name:* NVIDIA Display Control Panel *Description:* NVIDIA Display Control Panel *Uninstall command line:* N/A	6.14.11.9728	N/A
2.	*Name:* NVIDIA Drivers *Description:* NVIDIA Drivers *Uninstall command line:* N/A	1.10.57.35	N/A
3.	*Name:* Windows Live Language Selector *Description:* Windows Live Language Selector *Uninstall command line:* MsiExec.exe /X{027E5FAB-1476-4C59-AAB4-32EF28520399}	15.4.3555.0308	2012-06-22
4.	*Name:* Windows Live ID Sign-in Assistant *Description:* Windows Live ID Sign-in Assistant *Uninstall command line:* MsiExec.exe /X{1ACC8FFB-9D84-4C05-A4DE-D28A9BC91698}	7.250.4232.0	2012-03-08
5.	*Name:* Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 *Description:* Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 *Uninstall command line:* MsiExec.exe /X{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	10.0.40219	2012-08-07
6.	*Name:* 7-Zip 9.20 (x64 edition) *Description:* 7-Zip 9.20 (x64 edition) *Uninstall command line:* MsiExec.exe /X{23170F69-40C1-2702-0920-000001000000}	9.20.00.0	2012-03-08
7.	*Name:* PVSonyDll *Description:* PVSonyDll *Uninstall command line:* MsiExec.exe /X{3D3E663D-4E7E-4577-A560-7ECDDD45548A}	1.00.0001	2012-03-08

List Installed Software

Step 2 - Removing Unwanted Applications

If an application installed on a client workstation does not comply with the application use policies, you can easily remove it from the results section of the **List installed software** task. This is what you have to do:

- Click the link above the results table. A new pane is displayed.



Current Tasks - List Installed Software - Details

Creation date: 2012-09-21 13:28:17
Executed status: 3 / 4 computers
Schedule information: Runs once
Target: Server: LAVABKH

Close Installed Programs uninstall options

	Product Name	Product ...	Can be ...	Tot...	Sel...
☐	64 Bit HP CIO Components Inst...	6.2.2	Yes	2	0
☑	7-Zip 9.20 (x64 edition)	9.20.00.0	Yes	1	0
☐	Ad-Aware Antivirus	10.2.21.3...	Yes	1	0
☐	Ad-Aware Antivirus	10.3.42.3...	Yes	1	0
	Ad-Aware Browsing Protection	0.9.0.2	No	1	0
☐	Ad-Aware Business Edition	3.5.1.8	Yes	2	0
☐	Ad-Aware Management Agent	3.5.0	Yes	3	0
	Ad-Aware Security Add-on	2.2.0.10	No	1	0
	Ad-Aware Security Toolbar	2.1.0.20	No	1	0
	Adobe Flash Player 11 ActiveX	11.3.300....	No	1	0
	Adobe Flash Player 11 ActiveX	11.4.402....	No	2	0
	Adobe Flash Player 11 Plugin	11.3.300....	No	1	0
	Adobe Flash Player 11 Plugin	11.4.402....	No	1	0

☐	Client Name	Client IP	Total Pro...	Selected P...
☐	D000099	192.168.10.162	1	0

Uninstall Options

○ Force restart
○ No restart
○ Default behavior

Uninstall Options

You can see two tables:

- The left-side table displays all applications installed on the client workstations the script has run on.
- The right-side table displays all client workstations on which a selected application is installed.

Select the application you want to remove. Only applications installed using the MSI installer are removable.

Note

You can select several applications for removal.

If you want to remove the application from all the workstations it is installed on, select the check box in the **Client name** column header. If you want to remove it only from specific workstations, select only the corresponding check boxes.

A computer restart may be required to completely remove the selected application.

Select one of the available restart options:

- **Force restart** - to automatically restart the target computer after the application is removed.
- **No restart** - to wait for the user to restart the computer.
- **Default behavior** - to restart the target computer only if required.

Click **Next**.

Click **Uninstall** and then **Yes** to remove the application from the selected computers. An **Uninstall Software** task is automatically created and assigned to the selected computers to remove the application. Once the task is executed, you can check the results in the Current Network Tasks pane by double-clicking the task.

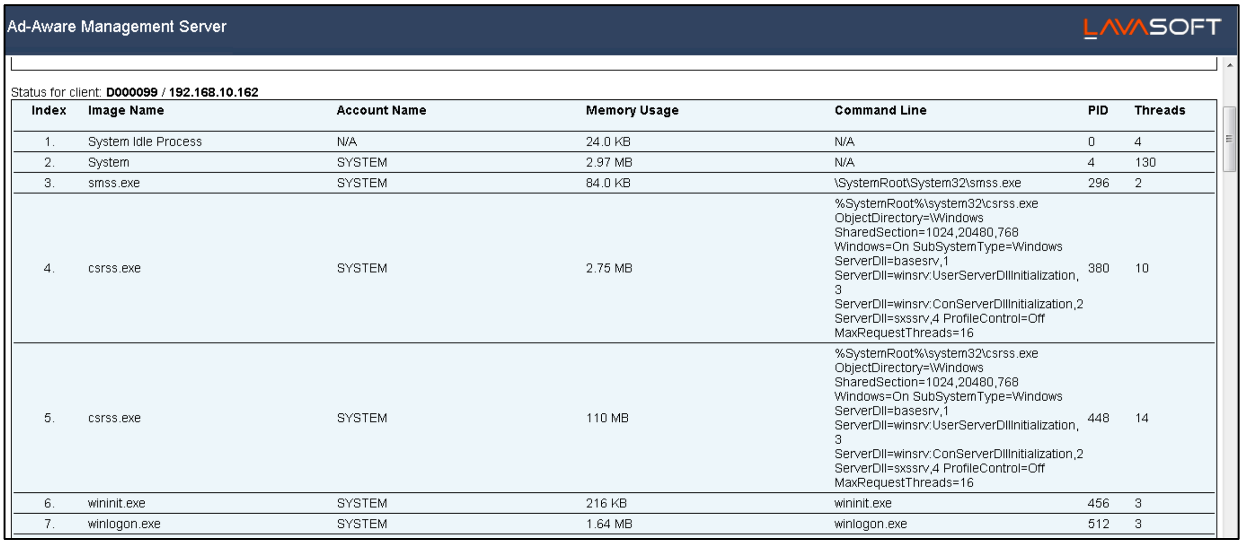
Monitoring Processes Running on Client Workstations

Users may complain that their computer performs poorly. In this case, you should check whether there are processes that eat up CPU. By terminating any such processes, you can quickly close non-responsive applications or restore computer functionality.

Step 1 - Check Running Processes

The **Current Processes** task can be used to obtain information on the processes currently running on client workstations. Run the task on the desired workstations. Once the task is executed, you can check the results in the Current Network Tasks pane by double-clicking the task.

The following image provides an example of such results for a client workstation:



Status for client: **D000099 / 192.168.10.162**

Index	Image Name	Account Name	Memory Usage	Command Line	PID	Threads
1.	System Idle Process	N/A	24.0 KB	N/A	0	4
2.	System	SYSTEM	2.97 MB	N/A	4	130
3.	smss.exe	SYSTEM	84.0 KB	\SystemRoot\System32\smss.exe	296	2
4.	csrss.exe	SYSTEM	2.75 MB	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	380	10
5.	csrss.exe	SYSTEM	110 MB	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	448	14
6.	wininit.exe	SYSTEM	216 KB	wininit.exe	456	3
7.	winlogon.exe	SYSTEM	1.64 MB	winlogon.exe	512	3

Current Processes

You can search the Internet for information about the running processes. Your findings may lead to a high CPU consumer or they may confirm the existence of spyware or of a virus.

Important

If you suspect you are dealing with a virus or other malware, follow these steps:
1. Terminate the suspect process immediately using a *Kill process* task.
2. Update the virus definitions of Ad-Aware Business Client using an *update request policy*.
3. Scan the client workstation comprehensively using an Ad-Aware Business Client scan policy.

Step 2 - Terminate Unwanted Processes

If you identify an unwanted process running on a client workstation, you can easily terminate it using a **Kill process** task. Before creating such a task, copy or write down the name or ID of the unwanted process from the results of the **Current processes** task.

To remotely terminate a process running on a client workstation, follow these steps:

1. In the Create New Network Task pane, double-click the **Kill process** task (or select it and click **Next**).
2. Type in the name of the process you want to terminate (as displayed by the **Current processes** task). Alternatively, you can select **Process identifier (PID)** and type the process identifier.
3. Click **Next**.
4. Search for the computer in the **Managed Computers** groups and select its check box. Alternatively, you can select **Show list of network computers**, search for the computer in the list and click it.
5. Click **Next**.
6. By default, the task will run as soon as possible (within a maximum of 5 minutes after the task assignment). To make sure the process will be terminated if it starts again, you may set the task to run regularly (with a fixed end time).
7. Click **Save Task** to create and run the task. The new task will appear in the Current Network Tasks pane.

Changing Remote Desktop Connection Settings

Remote Desktop Connection (also known as Remote Desktop) is a software provided by Windows operating systems to allow users to connect remotely to another computer. Mobile workers and telecommuters commonly use Remote Desktop to access resources on their workstation (or on company servers) from a remote location. Also, IT administrators sometimes connect with Remote Desktop to network computers to troubleshoot issues or install applications.

Windows provides a setting that can be used to allow or block incoming Remote Desktop connections (on Windows XP, **Allow users to connect remotely to this computer**). This setting can be changed only by users that are members of the Administrator group.

The **Remote Desktop Connection** tasks changes Windows settings on client workstations to control incoming connections through Remote Desktop Connection. You can run the task once and configure Windows on all managed computers to allow or block incoming Remote Desktop connections. This comes in handy especially when you administer hundreds of computers.

> **Note**
>
> You typically control Remote Desktop connections using a firewall (for example, apply an *Ad-Aware Business Client firewall policy*). If you use Remote Desktop to manage network workstations remotely, it may be convenient to configure the firewall to allow incoming Remote Desktop connections, but control them from Windows. This is very efficient if users log on to restricted (limited) Windows user accounts.

To create and assign a Remote Desktop Connection task, follow these steps:

1. In the Create New Network Task pane, double-click the **Remote Desktop Connection** task (or select it and click **Next**).
2. Select the option corresponding to the operation to be performed on the assigned client workstations:
   - **Enable Remote Desktop Connection** - to allow incoming Remote Desktop connections and disable the Windows Firewall (if available).
   - **Disable Remote Desktop Connection** - to block incoming Remote Desktop connections.
3. Click **Next**.

4. Select the check boxes corresponding to the computers or computer groups you want the task to run on. To run the task on all managed computers, select the check box corresponding to the server's name.
5. Click **Next**.
6. By default, the task is executed on a selected client the next time that client synchronizes with Ad-Aware Management Server (within a maximum of 5 minutes after the task assignment).
7. Click **Save Task** to create and run the task. The new task will appear in the Current Network Tasks pane.

Sending Messages to Client Workstations

There are situations when you need to notify users about administrative tasks that are going to be performed. You can use **Send message** tasks to send messages to client computers. The message is displayed in a dialog box and requires the user to click **OK** to acknowledge its receipt.

Note

For Windows 2000 workstations, the task uses the net send command and requires the **Messenger** service to be started (default setting). For other Windows workstations, the task uses the `msg` command and requires the **Terminal Services** service to be started (default setting).

To create and assign a Send message task, follow these steps:

1. In the Create New Network Task pane, double-click the **Send message** task (or select it and click **Next**).
2. Type in the edit box the message you want to be displayed on client workstations.

   For example, if you plan to perform an administrative task, type a text similar to this one:

An administrative task is going to be performed at 7 AM. Please be sure to close all applications and leave your computer turned on.

3. Click **Next**.
4. You will configure the assignment options according to the situation. For example:
   - If you want to send a message to users logged on to a local account, select **Local users** and enter the account name. To send a message to specific network (Active Directory) users when they log on to a managed computer, select **Networks users and groups** and then select them from the list.
   - To send a message to users logged on to specific computers, search for these computers in the **Managed Computers** groups and select the corresponding check boxes. When you want to send a message to all users who are logged on, select the check box corresponding to the server's name.
5. Click **Next**.
6. By default, the task will run as soon as possible (within a maximum of 5 minutes after the task assignment). Depending on the situation, you may want to change the default schedule.
   - To run the task at a later time, select the **Starting** check box and set the time as needed.
   - To run the task on a regular basis, choose a convenient option from the **Schedule** menu and set the frequency using the second menu. You can specify when to start and when to end the schedule by selecting the **Starting** and **Ending** check boxes.
7. Click **Save Task** to create and run the task. The new task will appear in the *Current Network Tasks* pane.

Running Programs on Client Workstations

You can use **Run program** tasks to run applications or scripts on client computers.

To create and assign Run program tasks, follow these steps:

1. In the Create New Network Task pane, double-click the Run program task (or select it and click Next).
2. Select to run an application located on the client workstation or on the local computer.
3. Provide the path to the application:
   - If you chose to run an application from the local machine, you can click **Browse** and select the application.
   - If you chose to run an application from the client workstation, you must type the path to the application in the edit field. You can use the following system variables:

System Variable	Description
`%PROGRAMFILES%`	The Program Files folder. A typical path is `C:\Program Files`.
`%SYSTEM%`	The Windows System folder. A typical path is `C:\Windows\System32`.
`%WINDOWS%`	The Windows directory or SYSROOT. A typical path is `C:\Windows`.

4. Configure additional settings as follows:
   - **Parameters** - to provide the parameters required to run the application. You must type these parameters in the edit field that appears.
   - **Destination Folder** - to copy the script on the client computers. You must type the path to the destination folder in the edit field that appears.
   - **Display application output** - to include the results returned by the application in the task results. You need to configure how long to wait for the results by selecting an appropriate time interval from the menu. If the application running time exceeds this limit, no application results will appear in the results window of the task.
   - **Operating system architecture** - select the check box corresponding to the supported operating system architecture.
   - **Run as current user** - to run the application under the current user privileges.

     ⚠ **Important**

     If you plan to run applications requiring user input on Windows Server 2008 or on Windows Vista computers, it is recommended to select this option. Otherwise, the application may fail to run.

   - **Run as system** - to run the application under system user privileges.
5. Click **Next**.
6. Select the check boxes corresponding to the computers or computer groups you want the task to run on. To run the task on all managed computers, select the check box corresponding to the server's name.
7. Click **Next**.
8. By default, the task is executed on a selected client the next time that client synchronizes with Ad-Aware Management Server (within a maximum of 5 minutes after the task assignment). Depending on the situation, you may want to change the default schedule.

- To run the task at a later time, select the **Starting** check box and set the time as needed.
- To run the script on a regular basis, choose a convenient option from the **Schedule** menu and set the frequency using the second menu. You can specify when to start and when to end the schedule by selecting the **Starting** and **Ending** check boxes.

9. Click **Save Task** to create and run the task. The new task will appear in the Current Network Tasks pane.

Configuring Windows Automatic Updates on Client Workstations

Windows Automatic Updates helps users keep their operating system up-to-date. An up-to-date operating system may greatly reduce the number of malware that can compromise its security. You can configure Windows Automatic Updates consistently across the network (on all network computers) using the **Windows automatic updating** task.

To create and assign Windows automatic updating tasks, follow these steps:

1. In the Create New Network Task pane, double-click the **Windows automatic updating** task (or select it and click **Next**).
2. Select one of the available options to configure Windows Automatic Updates on client workstations. The options are similar to those of Windows Automatic Updates.
   - **Automatically download recommended updates and install them**. This option may be appropriate for users who are not so familiarized with computers (users you expect not to know how to install Windows updates). Configure the update frequency and time using the menus.
   - **Download updates, but let the user choose when to install them**.
   - **Notify the user when new updates are available**.
   - **Turn off Automatic Updates**. This option is not recommended. If Windows is not updated regularly, the system will be more vulnerable to viruses and hackers.

   > **Note**
   >
   > If you turn off Automatic Updates, you can manually update Windows on client computers using the **Install Windows updates task**. For more information, please refer to Updating Windows on Client Workstations.

3. Click **Next**.
4. Select the check boxes corresponding to the computers or computer groups you want the task to run on. To run the task on all managed computers, select the check box corresponding to the server's name.
5. Click **Next**.
6. By default, the task is executed on a selected client the next time that client synchronizes with Ad-Aware Management Server (within a maximum of 5 minutes after the task assignment).
7. Click **Save Task** to create and run the task. The new task will appear in the *Current Network Tasks* pane.

Updating Windows on Client Workstations

Keeping Windows up to date is an important step in securing the computer network of your organization. Many attacks can be mitigated if Windows is up to date. Using the **Install Windows updates** task, you can immediately update Windows on all client computers. This is especially useful in the following situations:

- A critical Windows update has just been released and it should be installed immediately.
- If your organization's policies require testing important Windows updates (such as service packs) before they are installed on the network computers. After testing the update, you can run this task to install it on all client computers.

To create and assign Install Windows updates tasks, follow these steps:

1. In the Create New Network Task pane, double-click the **Install Windows updates** task (or select it and click **Next**).
2. Select one of the available options to update Windows or to find out information about Windows updates available on client workstations.
    - **List the available updates**. Select this option to find out information about the Windows updates available for the target computers.
    - **Install updates**. Select this option to install the most important Windows updates available on the target computers. To also install other optional software and hardware updates, select the corresponding check boxes.
    - **Install a specific update**. Select this option to install a specific Windows update available on the target computers. You must provide the ID of the update to be installed. To find out the update ID, you must run this script with the **List the available updates** option selected.
3. If your company uses a proxy server to connect to the Internet, select **Use Proxy Server** and specify the connection settings.
    - **Address** - type in the IP of the proxy server.
    - **Port** - type in the port used to connect to the proxy server.
    - **User name** - type in a user name recognized by the proxy.
    - **Password** - type in the valid password of the previously specified user.
4. Some Windows updates require restarting the computer. You can select **Restart computer if required** to automatically restart the computer after the update is installed.
5. Click **Next**.
6. Select the check boxes corresponding to the computers or computer groups you want the task to run on. To run the task on all managed computers, select the check box corresponding to the server's name.
7. Click **Next**.
8. By default, the task is executed on a selected client the next time that client synchronizes with Ad-Aware Management Server (within a maximum of 5 minutes after the task assignment). Depending on the situation, you may want to change the default schedule.
    - To run the task at a later time, select the **Starting** check box and set the time as needed.
    - To run the task on a regular basis, choose a convenient option from the **Schedule** menu and set the frequency using the second menu. You can specify when to start and when to end the schedule by selecting the **Starting** and **Ending** check boxes.
9. Click **Save Task** to create and run the task. The new task will appear in the Current Network Tasks pane.

Enabling/Disabling Autorun or USB Storage Devices on Client Workstations

Computer worms are increasingly using USB storage devices and the autorun feature of the Microsoft Windows operating systems to spread through the network. Autorun enables automatic detection and reading of new media. Such media includes USB flash drives, network shares, CDs, DVDs and other.

To help you make the network more secure, Ad-Aware Management Server includes the following two tasks:

- **Enable/Disable Autorun for All Drives** - to remotely control autorun for all drives on managed computers.
- **Enable/Disable USB Mass Storage** - to remotely allow or block the use of USB storage devices on managed computers.

You can run these tasks on all managed computers to completely disable autorun and USB storage devices in the network. Afterwards, you can run the tasks as needed to temporarily enable them on specific managed computers.

To create and assign such tasks, follow these steps:

1. In the Create New Network Task pane, double-click the desired task (or select it and click **Next**).
2. Select whether to enable or disable autorun/USB storage devices on the target computers.

Note

The changes will take effect after the system is restarted. You can use a Computer restart task to force the target computers to restart.

3. Click **Next**.
4. Select the check boxes corresponding to the computers or computer groups you want the task to run on. To run the task on all managed computers, select the check box corresponding to the server's name.
5. Click Next.
6. By default, the task is executed on a selected client the next time that client synchronizes with Ad-Aware Management Server (within a maximum of 5 minutes after the task assignment).
7. Click Save Task to create and run the task. The new task will appear in the Current Network Tasks pane.

Network Audit

Network Audit helps you get information about your network by collecting snapshots of the software and hardware configuration. The software snapshots provide historical change management reports to track all installed or uninstalled software within the network within a specific time period. You can choose from a list of predefined reports or create your own custom reports.

Important

Network audits are available for Windows operating systems only. The WMI Service must be started on all computers you want to audit.

The network audit reports available can provide you with various types of information about the network computers.

- Installed Software

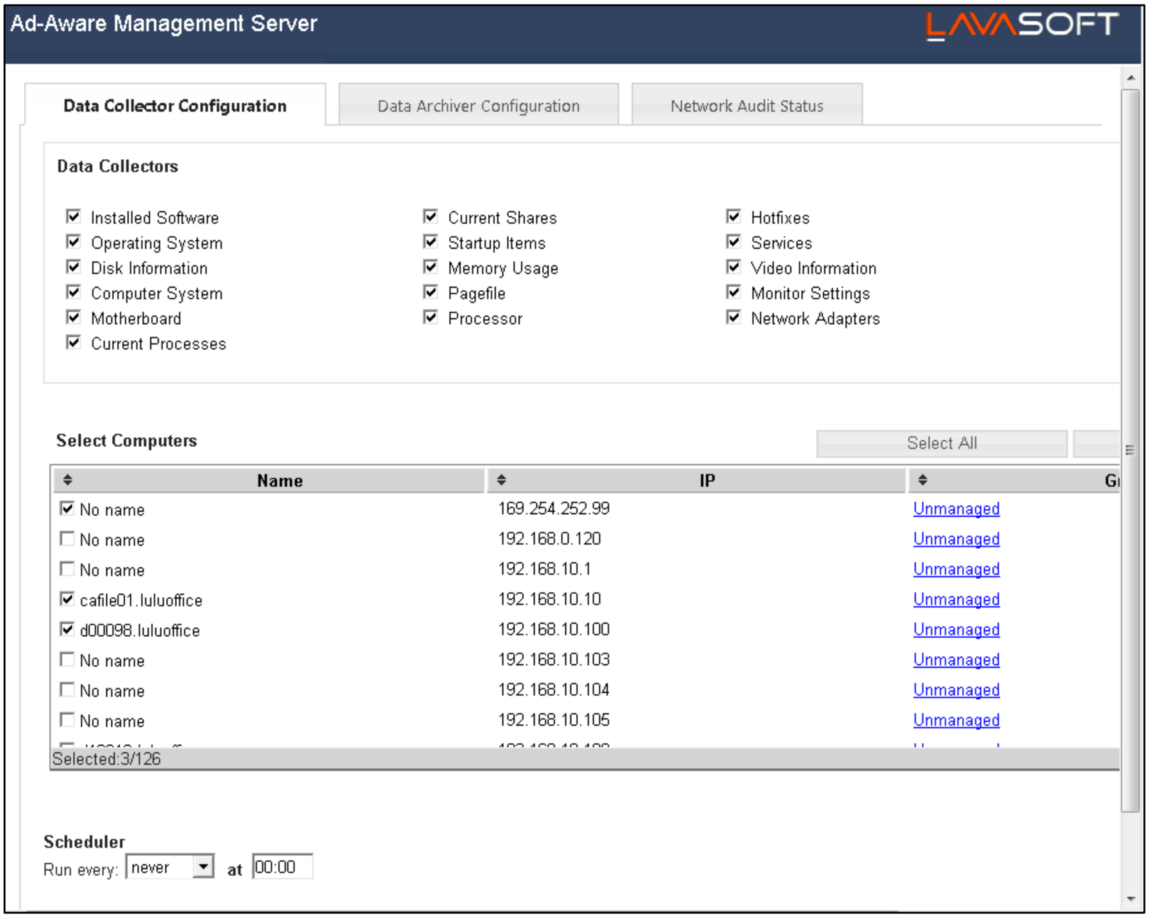
- Operating System
- Disk Information
- Computer System
- Motherboard
- Current Processes
- Current Shares
- Startup Items
- Memory
- Pagefile
- Processor
- Hotfixes
- Services
- Video Information
- Monitor Settings
- Network Adapters

Configuring Network Audit

Before you can create network audit reports, you must configure collection of necessary audit data.

You can configure network audit in the Network Audit Configuration pane. To display this pane, do one of the following:

- In the tree menu, go to **Network Tools** > **Auditing** > **Network Audit Configuration**.
- In the Network Tools pane, click the link provided.


Ad-Aware Management Server
LAVASOFT
Data Collector Configuration
Data Archiver Configuration
Network Audit Status
Select All

Data Collectors

☑ Installed Software
☑ Operating System
☑ Disk Information
☑ Computer System
☑ Motherboard
☑ Current Processes
☑ Current Shares
☑ Startup Items
☑ Memory Usage
☑ Pagefile
☑ Processor
☑ Hotfixes
☑ Services
☑ Video Information
☑ Monitor Settings
☑ Network Adapters

Select Computers

Name	IP	Gr
☑ No name	169.254.252.99	Unmanaged
□ No name	192.168.0.120	Unmanaged
□ No name	192.168.10.1	Unmanaged
☑ cafile01.luluoffice	192.168.10.10	Unmanaged
☑ d00098.luluoffice	192.168.10.100	Unmanaged
□ No name	192.168.10.103	Unmanaged
□ No name	192.168.10.104	Unmanaged
□ No name	192.168.10.105	Unmanaged

Selected:3/126

Scheduler

Run every: never at 00:00

Network Audit Configuration

The pane has three tabs:

Data Collector Configuration

This is where you can configure network audit data collection.

Data Archiver Configuration

This is where you can configure the archiving preferences for network audit data.

Network Audit Status

This is where you can check data collection and data archiving schedule and status.

Configuring Data Collection

To configure network audit data collection:

1. Open the Network Audit Configuration pane and click the **Data Collector Configuration** tab.
2. **Select data types to be collected**.

   Select the check boxes corresponding to the data types you are interested in. You will be able to create network audit reports for the selected data types only.

3. **Select computers to audit**.

Choose from the list the computers on which you want Data Collector to run. Audit data will be available for the selected computers only.

The computer list contains all computers from Computers Directory, except those in the Excluded Computers group. You can sort computers by name, IP address or the group they belong to, by clicking the corresponding column header.

For fast selection, you can use the **Select All** and **Clear** buttons. You can also click a group's name to select all computers in that group.

4. **Configure data collection schedule**.

   Specify data collection frequency using the menu, then set the time of day when audit data should be collected. Choose a time of day when most computers are online.

   > **Note**
   >
   > When specifying frequency, consider the situations when you might or will create network audit reports. If you need current information at all times, set a daily data collection routine. If you will create network audits every now and then, you can set a less frequent schedule.

5. Click **Save Collector Configuration**. You will be able to create network audit reports only after the network audit data has been collected.

Configuring Data Archiving Preferences

By default, network audit data older than 6 months will be deleted every day.

To configure data archiving:

1. Open the Network Audit Configuration pane and click the **Data Archiver Configuration** tab.

Configure data deletion or archiving schedule.

2. Specify the frequency and the time of day when to delete or archive old network audit data.

Specify what data to archive.

3. Specify the number of days, months or years after which network audit data should be archived.

Select archiving method.

4. Select whether to delete old network audit data from the database or to move it to archive files.

   If you choose to archive data, click **Browse** and choose where to save the archive files. If you want to save the archives on a network share, you must also specify a user account and a password that will be used to access archived data.

   > **Important**
   >
   > Data archived to this location will always be available from the Ad-Aware Management Server console as long as you do not move the archive files. To move any archived data to another location, move files manually and then set the new archiving location.

5. Click **Save Archiver Configuration**.

Checking Network Audit Status

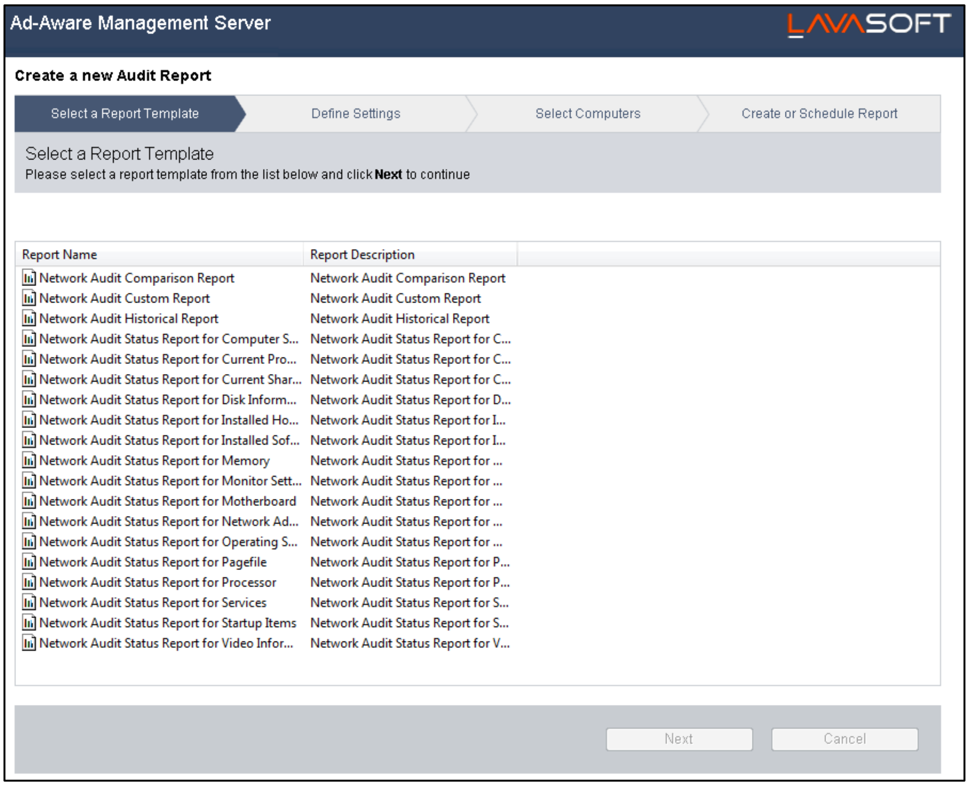
To check data collection or data archiving status, open the Network Audit Configuration pane and click the **Network Audit Status** tab.

For each operation, you can see the current status and the last and next run.

Creating New Network Audit Reports

You can create and view network audit reports in the Create New Network Audit Report pane. To display this pane, do one of the following:

- In the tree menu, go to **Network Tools** > **Auditing** > **Create New Network Audit Report**.
- In the Network Tools pane, click the link provided.



Create a new Audit Report

Select a Report Template

Please select a report template from the list below and click **Next** to continue

Report Name	Report Description
Network Audit Comparison Report	Network Audit Comparison Report
Network Audit Custom Report	Network Audit Custom Report
Network Audit Historical Report	Network Audit Historical Report
Network Audit Status Report for Computer S...	Network Audit Status Report for C...
Network Audit Status Report for Current Pro...	Network Audit Status Report for C...
Network Audit Status Report for Current Shar...	Network Audit Status Report for C...
Network Audit Status Report for Disk Inform...	Network Audit Status Report for D...
Network Audit Status Report for Installed Ho...	Network Audit Status Report for I...
Network Audit Status Report for Installed Sof...	Network Audit Status Report for I...
Network Audit Status Report for Memory	Network Audit Status Report for ...
Network Audit Status Report for Monitor Sett...	Network Audit Status Report for ...
Network Audit Status Report for Motherboard	Network Audit Status Report for ...
Network Audit Status Report for Network Ad...	Network Audit Status Report for ...
Network Audit Status Report for Operating S...	Network Audit Status Report for ...
Network Audit Status Report for Pagefile	Network Audit Status Report for P...
Network Audit Status Report for Processor	Network Audit Status Report for P...
Network Audit Status Report for Services	Network Audit Status Report for S...
Network Audit Status Report for Startup Items	Network Audit Status Report for S...
Network Audit Status Report for Video Infor...	Network Audit Status Report for V...

Create New Network Audit Report Pane

You can see the report templates that you can use to create network audit reports. You can create 4 types of network audit reports:

- **Snapshot (Status) Reports** - to view the current software and hardware configurations.
- **Comparison Reports** - to compare installed software for two different points in time.
- **Historical Reports** - to view installed software details within a specified time period.
- **Custom Reports** - to define a custom query based on the specific information you are looking for.

To create a report, follow the wizard steps:

1. **Select a report template**.

Double-click the report template you want to use (or select it and click Next).

2. **Define report settings**.

   a. Choose the reporting date.
   b. **Custom reports only**! Configure your query. Click the plus (+) button to add a filter and use the menus to configure it. You can choose which columns to be displayed in the report.
   c. Specify the parameter by which to sort report results and the sorting order. You can choose to sort results by computer IP or by report-specific criteria. If you are looking for a particular information in the report (for example, a particular computer model), use it to sort the results.
   d. If you plan to create a scheduled report, you should change the default report name. The name should help you easily identify the report.
   e. Click **Next**.

3. **Select computers to audit**.

Choose from the list the computers you want to audit.

The computer list contains all computers from Computers Directory, except those in the Excluded Computers group. You can sort computers by name, IP address or the group they belong to, by clicking the corresponding column header.

For fast selection, you can use the **Select All** and **Clear** buttons. You can also click a group's name to select all computers in that group.

Click **Next**.

4. **Create** or **schedule the report**.

   a. By default, the report is created immediately after you confirm the report settings.

If you want to create a scheduled report, proceed as follows:

- To create the report one time only, at a later moment, select **One time** from the menu and specify when to create the report.
- To create regular reports, select **Every day(s) / week(s)** and set the frequency using the second menu. You can also set a start and end time.

Scheduled reports can be sent by e-mail when they are created. You must select **Send report by e-mail** and configure the e-mail settings. For more information, please refer to Configuring E-mail Notifications.

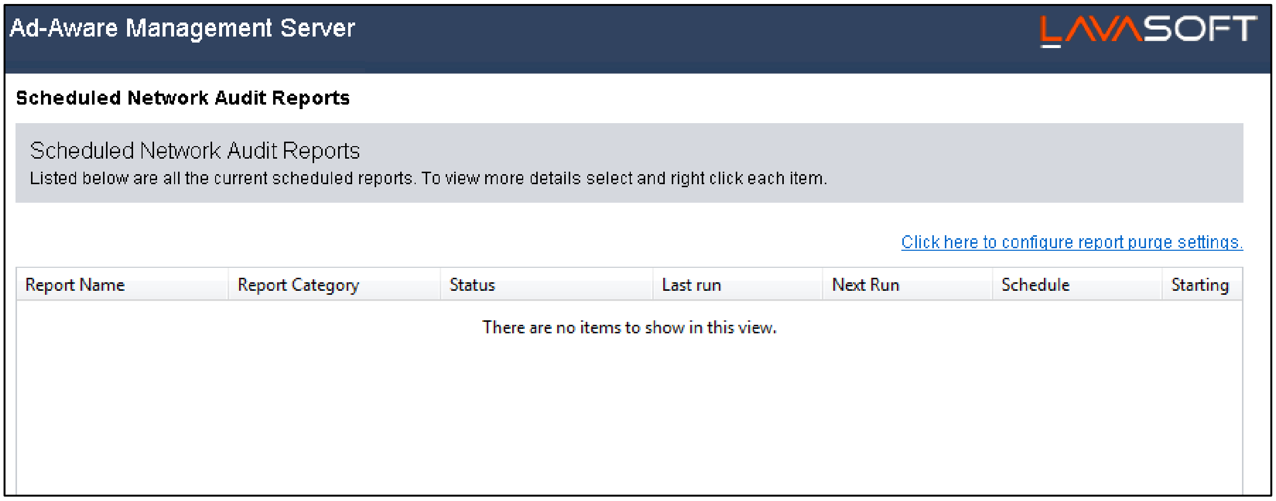
   b. Click **Finish** to create the report.

- If you have chosen to create a scheduled report, the Scheduled Network Audit Reports pane will be displayed.
- Otherwise, the report will be displayed in a few moments. The time required for reports to be created may vary depending on the number of selected computers. Please wait for the requested report to be created.

Scheduled Network Audit Reports

You can view and modify scheduled network audit reports in the Scheduled Network Audit Reports pane. To display this pane, do one of the following:

- In the tree menu, go to **Network Tools > Auditing > Scheduled Network Audit Reports**.
- In the Network Tools pane, click the link provided.



Scheduled Network Audit Reports

Scheduled Network Audit Reports

Listed below are all the current scheduled reports. To view more details select and right click each item.

Click here to configure report purge settings.

Report Name	Report Category	Status	Last run	Next Run	Schedule	Starting

There are no items to show in this view.

Scheduled Network Audit Reports Pane

You can see all scheduled reports and useful information about them:

- The report name and category
- The status
- When the report was last run
- When the report is scheduled to run next
- The report schedule
- The start and end time

Viewing Last Report

To view the last results, right-click the report and select **View last**. The report will be displayed in a browser window.

Saving Reports

To save a report to an HTML file, right-click it choose **Save** and save the file under the desired name.

To save a report to a PDF file right-click it choose **Export** and save the file under the desired name.

Renaming Reports

To rename a report, right-click it and select **Rename**.

Editing Report Settings

To change the settings of a report, right-click the report and select **Edit settings**. A new pane is displayed. You can change the report settings, target and schedule as needed.

Deleting Reports

By default, all reports older than 90 days are deleted. To change the report purge settings, click the link at the top of the table, type the desired time interval and click **OK**.

To delete a report, right-click it and select **Delete**.

Reporting Center

Reporting Center allows you to create centralized reports on the security status of the network computers managed by Ad-Aware Management Server. The reports can be used for multiple purposes, such as:

- Monitoring and ensuring compliance with the organization's security policies.
- Checking and assessing the network security status.
- Identifying network security issues, threats and vulnerabilities.
- Monitoring security incidents and malware activity.
- Providing upper management with easy-to-interpret data on network security.

Reports are created based on built-in report templates, using data from the Ad-Aware Management Server's database. Numerous report templates are available for each Ad-Aware product included into the centralized management platform (over 20 templates for Ad-Aware Business Client). The report templates are presented in detail in appendix Available Report Templates.

Reports can consolidate data from the entire network of managed computers or from specific groups only. In this way, from a single report, you can find out:

- Statistical data regarding all or groups of managed computers.
- Detailed information for each managed computer or Ad-Aware client product.

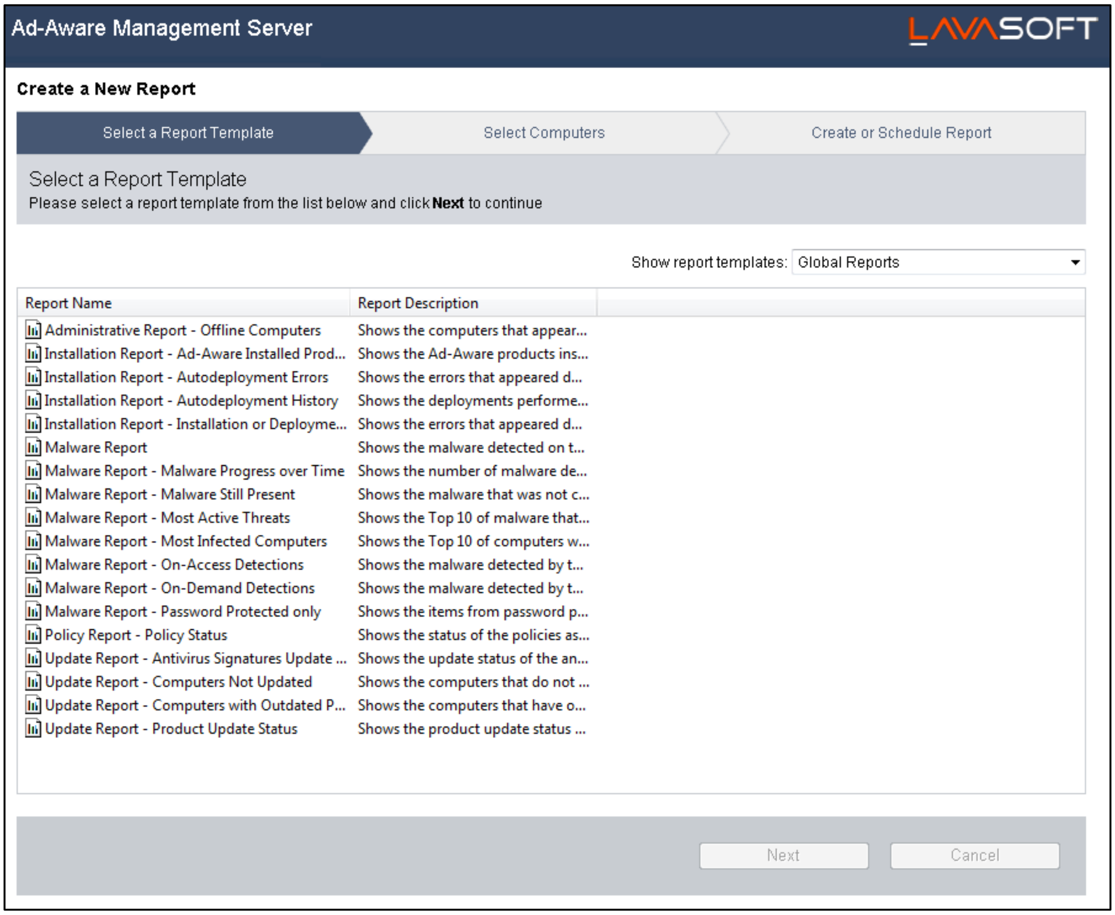
The information is presented as easy-to-read pie charts, tables and graphics, allowing you to quickly check the network security status and identify security issues.

The reports created are not automatically saved on the disk. However, you can print them or save them as HTML or PDF files.

Creating Reports

You can create and manage reports in the Create New Report pane. To display this pane, do one of the following:

- In the tree menu, go to **Reporting Center > Create New Report**.
- In the Reporting Center pane, click the link provided.



Select a Report Template

Please select a report template from the list below and click **Next** to continue

Show report templates: Global Reports

Report Name	Report Description
Administrative Report - Offline Computers	Shows the computers that appear...
Installation Report - Ad-Aware Installed Prod...	Shows the Ad-Aware products ins...
Installation Report - Autodeployment Errors	Shows the errors that appeared d...
Installation Report - Autodeployment History	Shows the deployments performe...
Installation Report - Installation or Deployme...	Shows the errors that appeared d...
Malware Report	Shows the malware detected on t...
Malware Report - Malware Progress over Time	Shows the number of malware de...
Malware Report - Malware Still Present	Shows the malware that was not c...
Malware Report - Most Active Threats	Shows the Top 10 of malware that...
Malware Report - Most Infected Computers	Shows the Top 10 of computers w...
Malware Report - On-Access Detections	Shows the malware detected by t...
Malware Report - On-Demand Detections	Shows the malware detected by t...
Malware Report - Password Protected only	Shows the items from password p...
Policy Report - Policy Status	Shows the status of the policies as...
Update Report - Antivirus Signatures Update ...	Shows the update status of the an...
Update Report - Computers Not Updated	Shows the computers that do not ...
Update Report - Computers with Outdated P...	Shows the computers that have o...
Update Report - Product Update Status	Shows the product update status ...

Create New Report Pane

You can see the report templates that you can use to create reports. The templates are grouped based on the client product they apply to. You can change the template category using the menu (at the top of the table). The report templates are presented in detail in appendix Available Report Templates.

To create a report, follow the wizard steps:

1. **Select a report template**.

    a. Select the desired report category from the menu. To create a report for all Ad-Aware products, use a global report template.

    b. Double-click the report template you want to use (or select it and click **Next**).

2. **Select the target computers**.

    - To obtain information about all managed computers, select the check box corresponding to the Ad-Aware Management Server instance.
    - To obtain information about specific groups of managed computers, select the check boxes corresponding to those groups.
    - To obtain information about the managed computers in an IP range, select **Generate report on IP** range and specify the IP range.

Click **Next**.

3. **Create or schedule the report**.

a. By default, the report is created immediately after you confirm the report settings.

If you want to create a scheduled report, proceed as follows:

- To create the report one time only, at a later moment, select **One time** from the menu and specify when to create the report.
- To create regular reports, select **Every hour(s) / day(s) / week(s)** and set the frequency using the second menu. You can also set a start and end time.

Scheduled reports can be sent by e-mail when they are created. You must select **Send report by e-mail** and configure the e-mail settings. For more information, please refer to Configuring E-mail Notifications.

b. For some types of reports, you must specify the time period to be covered in the report (the reporting period). Set a start and an end time for reports generated one time only, or choose an option from the menu for periodic reports.

c. Click **Finish** to create the report.

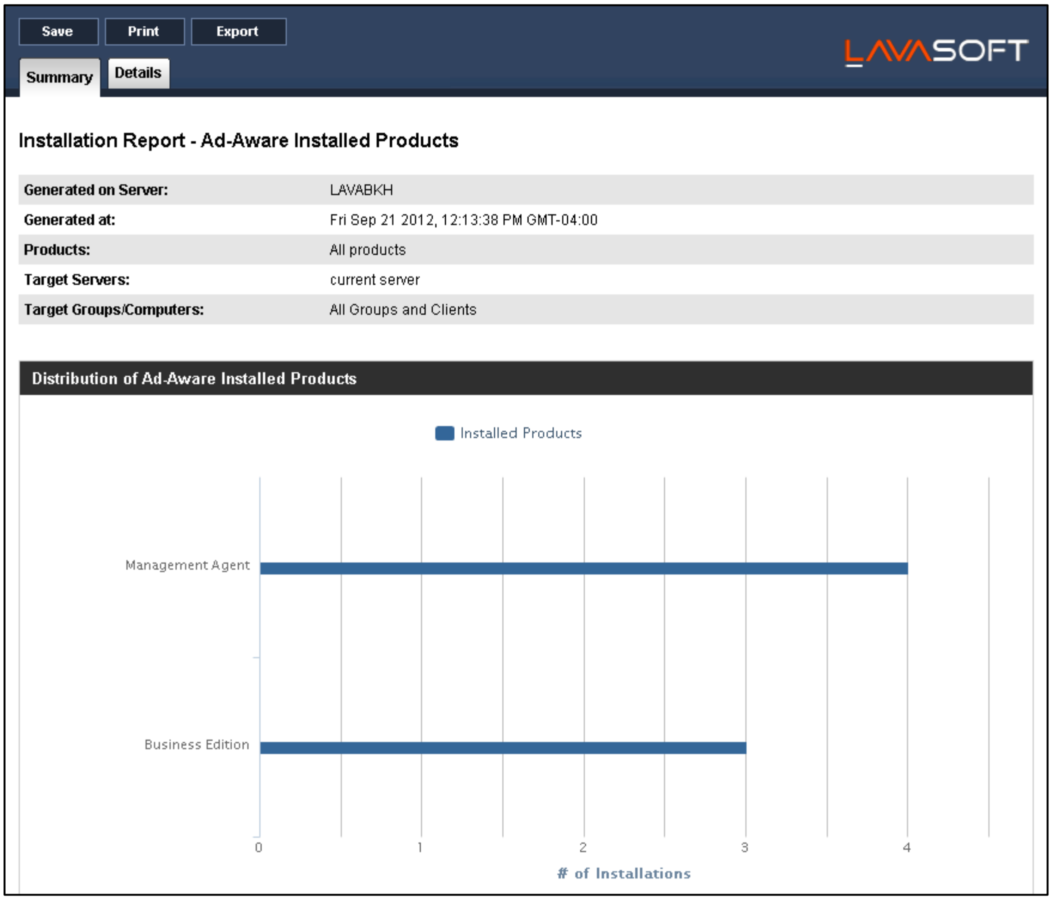
- If you have chosen to create a scheduled report, the Scheduled Reports pane will be displayed.
- Otherwise, the report will be displayed in a few moments. The time required for reports to be created may vary depending on the number of managed computers or of Ad-Aware client products. Please wait for the requested report to be created.

Viewing and Saving Reports

The reports you choose to be created immediately are displayed in the Create New Report pane.

Note

Scheduled reports can be viewed and managed in the Scheduled Reports pane.



Installation Report - Ad-Aware Installed Products

Generated on Server:	LAVABKH
Generated at:	Fri Sep 21 2012, 12:13:38 PM GMT-04:00
Products:	All products
Target Servers:	current server
Target Groups/Computers:	All Groups and Clients

Report Sample

All reports consist of a Summary page and a Details page.

- The Summary page provides you with statistical data (pie charts and graphics) for all target computers or groups.
- The Details page provides you with detailed information about each managed computer and Ad-Aware product installed.

Use the tabs in the upper-left corner of the pane to view the desired page.

At the top of the each report page, you can see general information about the report, such as its name, reporting period (if applicable), selected target computers etc.

Saving Reports

The reports created are not automatically saved on the disk.

To save a report to an HTML file click the **Save** button in the upper-left corner of the pane and save the file under the desired name.

To save a report to a PDF file click the **Export** button in the upper-left corner of the pane and save the file under the desired name.

Printing Reports

To print a report, click the **Print** button in the upper-left corner of the pane.

Sorting Report Details

The report details are displayed in a table that consists of several columns providing various information. The table can span several pages (only 50 entries are displayed per page).

If the report covers a large number of computers, it may be convenient to sort the report details in order to easily find what you are looking for.

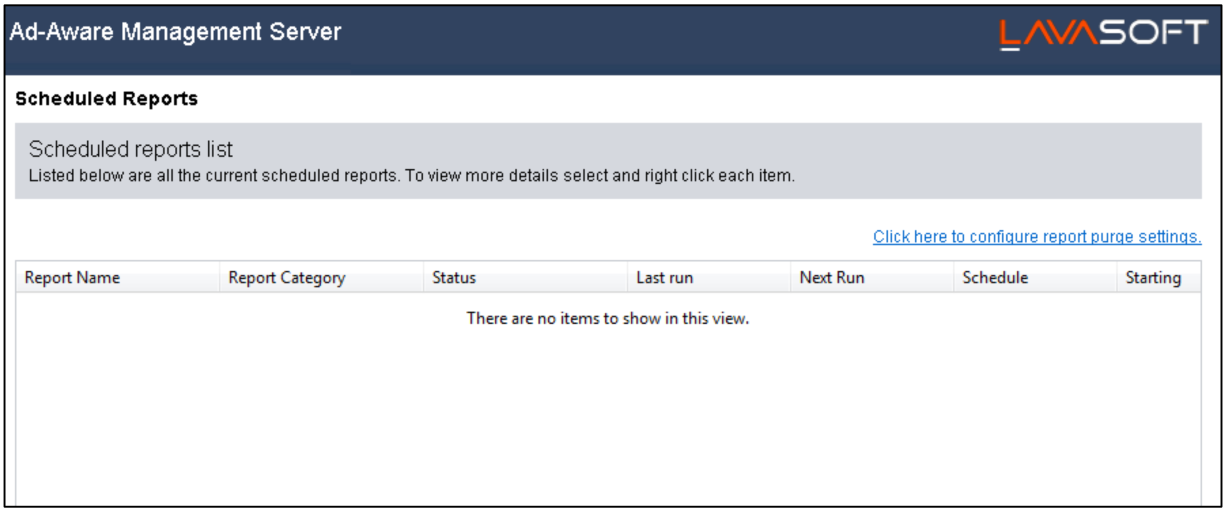
To sort report details by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

To browse through the details pages, use the buttons at the bottom of the table.

Scheduled Reports

You can view and modify scheduled reports in the Scheduled Reports pane. To display this pane, do one of the following:

- In the tree menu, go to **Reporting Center > Scheduled Reports**.
- In the Reporting Center pane, click the link provided.



Scheduled Reports

Scheduled reports list

Listed below are all the current scheduled reports. To view more details select and right click each item.

Click here to configure report purge settings.

Report Name	Report Category	Status	Last run	Next Run	Schedule	Starting

There are no items to show in this view.

Scheduled Reports Pane

You can see all scheduled reports and useful information about them:

- The report name and category
- The status
- When the report was last run

- When the report is scheduled to run next
- The report schedule
- The start and end time

Viewing Last Report

To view the last results, right-click the report and select **View last**. The report will be displayed in a browser window.

Saving Reports

To save a report to an HTML file right-click on the report and click **Save** and save the file under the desired name.

To save a report to a PDF file right-click on the report and click **Export** and save the file under the desired name.

Renaming Reports

To rename a report, right-click it and select **Rename**.

Editing Report Settings

To change the settings of a report right-click on the report and select **Edit settings**. You can change the report target and schedule as needed.

Deleting Reports

By default, all reports older than 90 days are deleted. To change the report purge settings, click the link at the top of the table, type the desired time interval and click **OK**.

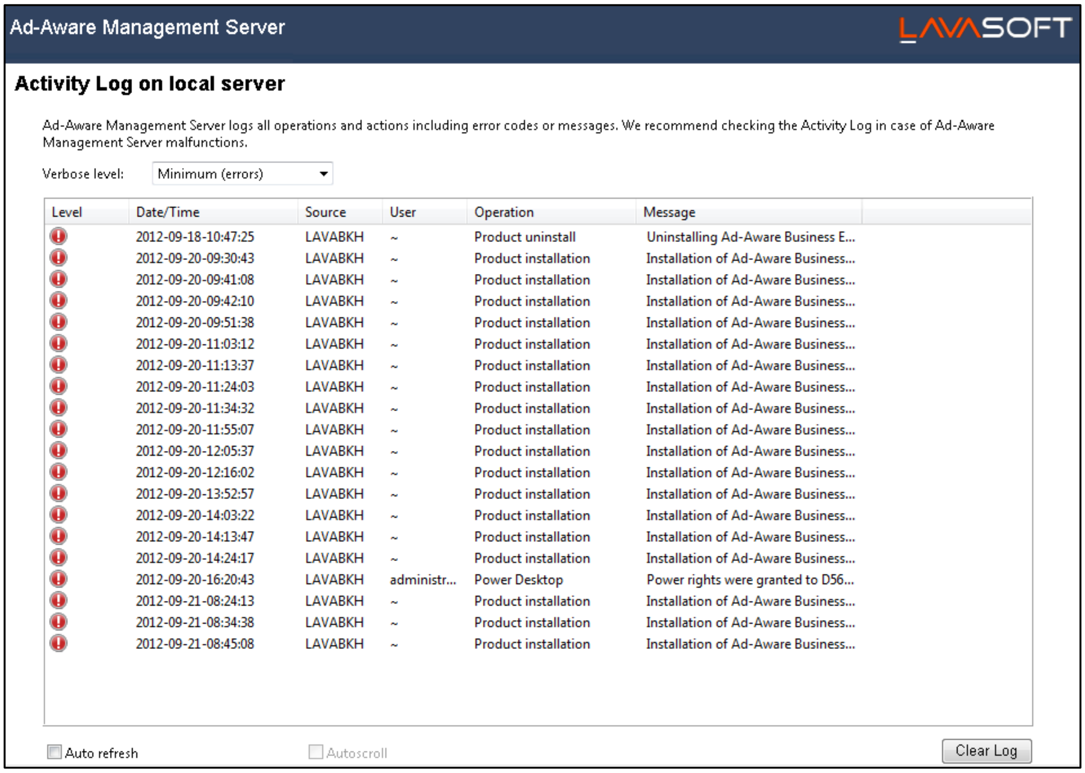
To delete a report, right-click it and select **Delete**.

Examining the Server Activity Log

Ad-Aware Management Server logs all its operations and actions, including error codes and messages. The information provided in the activity log can be very useful in troubleshooting specific problems (such as failed deployments or agents not synchronizing properly).

You can examine the records of the activity log in the Server Activity pane. To display this pane, do one of the following:

- In the tree menu, go to **Activity Log > Server Activity Log**.
- In the Activity Log pane, click the link provided.



Activity Log on local server

Ad-Aware Management Server logs all operations and actions including error codes or messages. We recommend checking the Activity Log in case of Ad-Aware Management Server malfunctions.

Verbose level: Minimum (errors)

Level	Date/Time	Source	User	Operation	Message
❗	2012-09-18-10:47:25	LAVABKH	~	Product uninstall	Uninstalling Ad-Aware Business E...
❗	2012-09-20-09:30:43	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-09:41:08	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-09:42:10	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-09:51:38	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-11:03:12	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-11:13:37	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-11:24:03	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-11:34:32	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-11:55:07	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-12:05:37	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-12:16:02	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-13:52:57	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-14:03:22	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-14:13:47	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-14:24:17	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-20-16:20:43	LAVABKH	administr...	Power Desktop	Power rights were granted to D56...
❗	2012-09-21-08:24:13	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-21-08:34:38	LAVABKH	~	Product installation	Installation of Ad-Aware Business...
❗	2012-09-21-08:45:08	LAVABKH	~	Product installation	Installation of Ad-Aware Business...

Server Activity Pane

Note

We recommend checking Server Activity in case Ad-Aware Management Server does not function properly.

You can see in the table the recorded events that match the selected verbosity level.

The table columns provide you with useful information about the listed events:

- **Level** - the event type, which is related to the verbosity level. Depending on the verbosity level, all or only specific types of events are displayed in the Server Activity pane. There are three levels:

  ❗ Indicates an error that occurred during the operation of Ad-Aware Management Server

  ⚠ Indicates a warning

  ⓘ Indicates a successful operation

- **Date\Time** - the moment when the event occurred
- **Source** - the machine the event took place on
- **User** - the user account under which the event occurred
- **Operation** - the operation that caused the event
- **Message** - the debug message, if any. The debug message offers additional information about the event

If you want the management console to automatically check for new events every second, select **Auto refresh**. You will also be able to select **Auto scroll** to automatically scroll down and keep visible the last added event.

Setting Verbosity Level

The verbosity level allows you to choose what type of events recorded in the activity log should be displayed in the Server Activity pane.

Select the desired verbosity level from the menu. The following options are available:

Verbosity Level	Description
Minimum (errors)	Only errors are displayed.
Intermediate (operations)	Both errors and warnings are displayed.
Full (all relevant actions)	All recorded events are displayed.

Sorting Events

To easily identify problems and monitor the Ad-Aware Management Server activity, you can sort events by:

- verbosity level (importance);
- date/time;
- source;
- user;
- message.

To sort events by any of these criteria, just click the corresponding column heading in the table.

Deleting Records

To delete the records in the activity log, click **Clear log**.

Note

The activity log has a maximum size limit of 10MB. Once the size limit has been reached, the oldest events will be overwritten as new events occur.

Backup/Restore Server Configuration Tool

Backup/Restore Server Configuration Tool helps you save the Ad-Aware Management Server configuration to a backup file or restore a previously saved configuration of Ad-Aware Management Server. This tool is very useful in the following situations:

- Moving Ad-Aware Management Server to another machine.

- If the Ad-Aware Management Server configuration is corrupted.
- Reinstalling the operating system.
- Reinstalling Ad-Aware Management Server.

Important

The configuration backup file of a specific Ad-Aware Management Server instance must only be used to restore the configuration of that specific instance. You must not use it on other Ad-Aware Management Server instances, because such instances manage different network computers.

Additionally, the configuration backup file is strictly related to the Ad-Aware Management Server version. If you back up the configuration and then upgrade Ad-Aware Management Server to a newer version, you can no longer use that configuration backup file.

The following data is backed up:

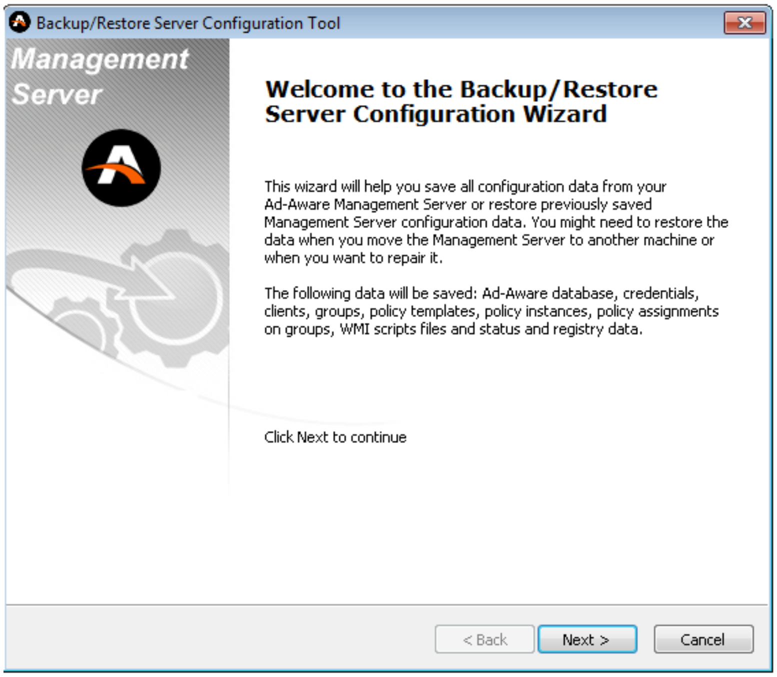
- Ad-Aware Management Server database
- authentication credentials
- client computers and groups
- policy templates
- current policies
- policy assignments on groups
- WMI script files (used by tasks)
- status and registry data

Backing Up Ad-Aware Management Server Configuration

To back up the configuration of Ad-Aware Management Server:

1. Open the management console and connect to Ad-Aware Management Server.
2. On the **Tools** menu, click **Backup/Restore Server Configuration Tool**. A wizard will appear.
3. Complete the wizard. You must select **Backup** in the second step of the wizard.

Step 1/4 - Welcome Window


Backup/Restore Server Configuration Tool

Welcome to the Backup/Restore Server Configuration Wizard

This wizard will help you save all configuration data from your Ad-Aware Management Server or restore previously saved Management Server configuration data. You might need to restore the data when you move the Management Server to another machine or when you want to repair it.

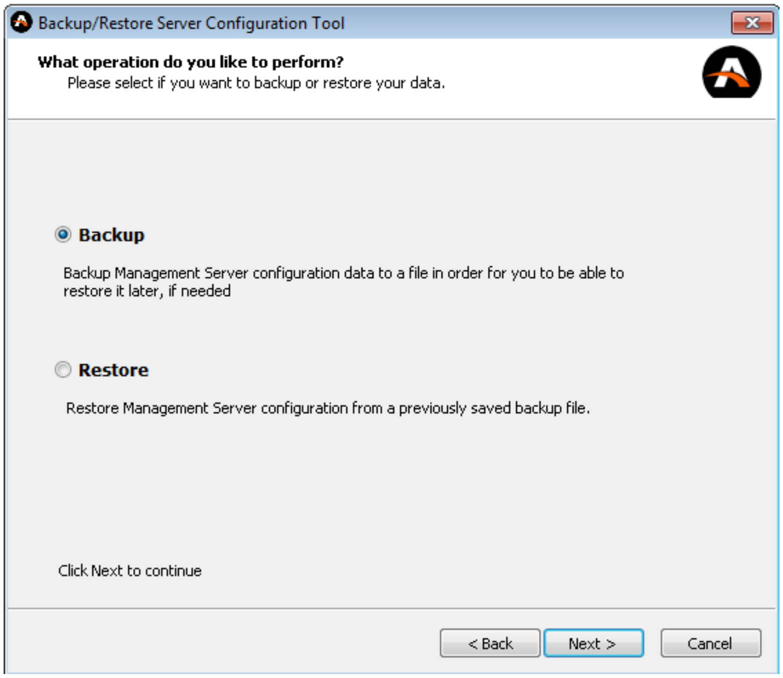
The following data will be saved: Ad-Aware database, credentials, clients, groups, policy templates, policy instances, policy assignments on groups, WMI scripts files and status and registry data.

Click Next to continue

Welcome Window

Click Next.

Step 2/4 - Select Backup


Backup/Restore Server Configuration Tool

What operation do you like to perform?
Please select if you want to backup or restore your data.

● **Backup**

Backup Management Server configuration data to a file in order for you to be able to restore it later, if needed

○ **Restore**

Restore Management Server configuration from a previously saved backup file.

Click Next to continue

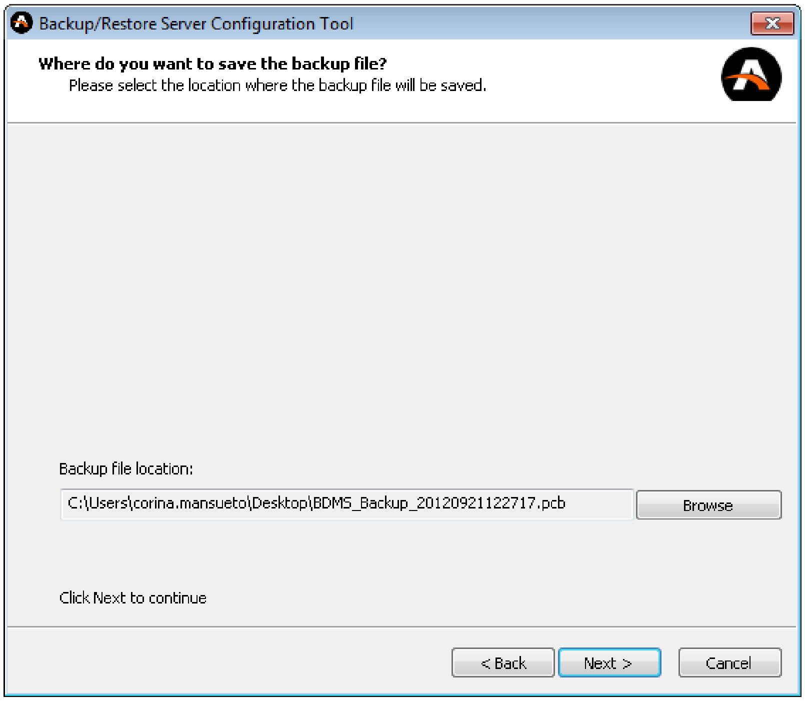
Select Backup

The following options are available:

- **Backup** - to save the Ad-Aware Management Server configuration to a backup file.
- **Restore** - to restore a previously saved configuration of Ad-Aware Management Server from a backup file.

Select the first option and click **Next**.

Step 3/4 - Specify Backup Location



Where do you want to save the backup file?

Please select the location where the backup file will be saved.

Backup file location:

C:\Users\corina.mansueto\Desktop\BDMS_Backup_20120921122717.pcb

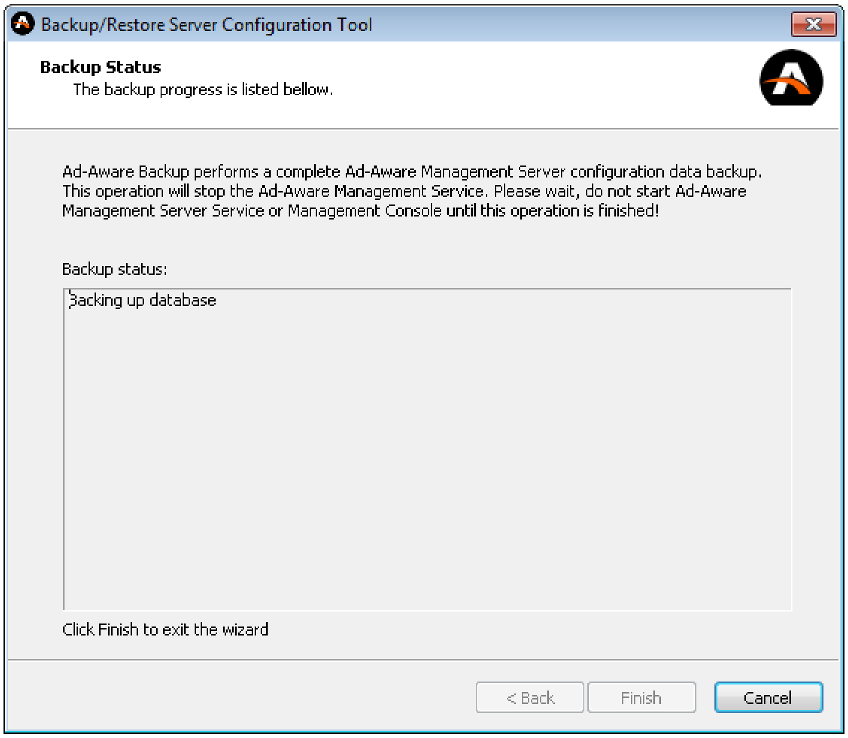
Click Next to continue

Specify Backup Location

You must specify where the Ad-Aware Management Server configuration data should be saved. Click **Browse** and choose where and under what name to save the configuration backup file. Configuration backup files have the . pcb extension.

Click **Next** to start the backup operation.

Step 4/4 – Finish


Backup/Restore Server Configuration Tool
Backup Status
The backup progress is listed bellow.

Ad-Aware Backup performs a complete Ad-Aware Management Server configuration data backup. This operation will stop the Ad-Aware Management Service. Please wait, do not start Ad-Aware Management Server Service or Management Console until this operation is finished!

Backup status:

Backing up database

Click Finish to exit the wizard

Finish

You can see the progress of the backup process. Wait until the configuration data is successfully saved. This operation may take a few minutes.

After the operation is completed, click **Finish**.

Restoring Ad-Aware Management Server Configuration

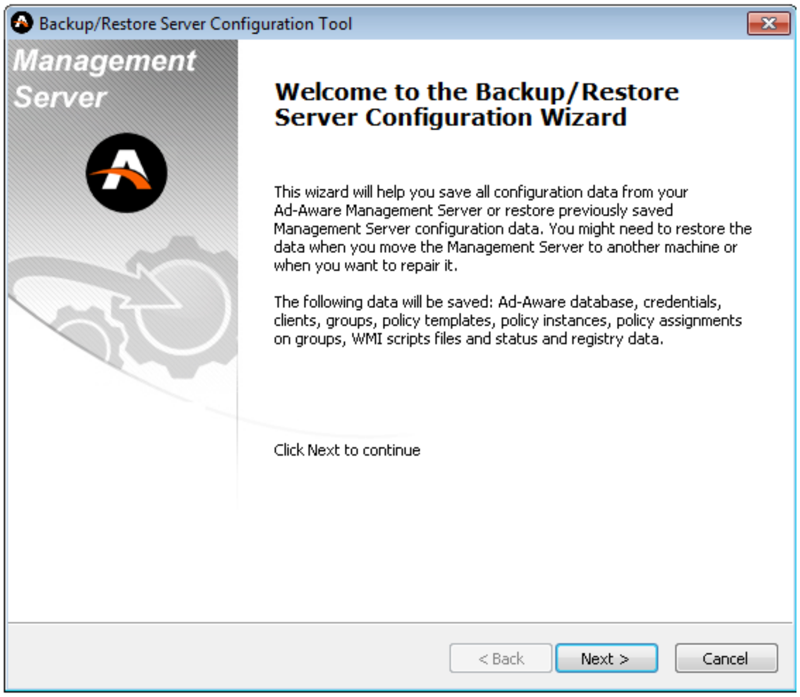
To restore a previously saved configuration of Ad-Aware Management Server:

1. Open the management console and connect to Ad-Aware Management Server.
2. On the **Tools** menu, click **Backup/Restore Server Configuration Tool**. A wizard will appear.
3. Complete the wizard. You must select **Restore** in the second step of the wizard.

Important

Restore saved configurations only if necessary. When you restore a previous configuration of Ad-Aware Management Server, all current settings are overwritten. This means that you lose all the configuration changes made after the imported configuration was saved. Lost configuration changes may include the new client groups and policies created.

Step 1/4 - Welcome Window



Welcome to the Backup/Restore Server Configuration Wizard

This wizard will help you save all configuration data from your Ad-Aware Management Server or restore previously saved Management Server configuration data. You might need to restore the data when you move the Management Server to another machine or when you want to repair it.

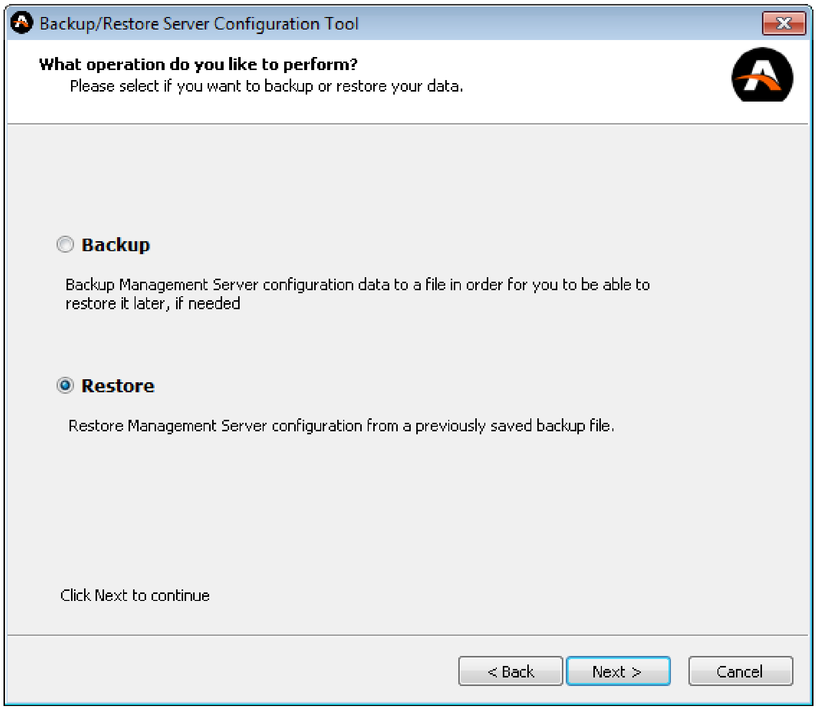
The following data will be saved: Ad-Aware database, credentials, clients, groups, policy templates, policy instances, policy assignments on groups, WMI scripts files and status and registry data.

Click Next to continue

Welcome Window

Click **Next**.

Step 2/4 - Select Restore



What operation do you like to perform?

Please select if you want to backup or restore your data.

○ Backup

Backup Management Server configuration data to a file in order for you to be able to restore it later, if needed

● Restore

Restore Management Server configuration from a previously saved backup file.

Click Next to continue

Select Restore

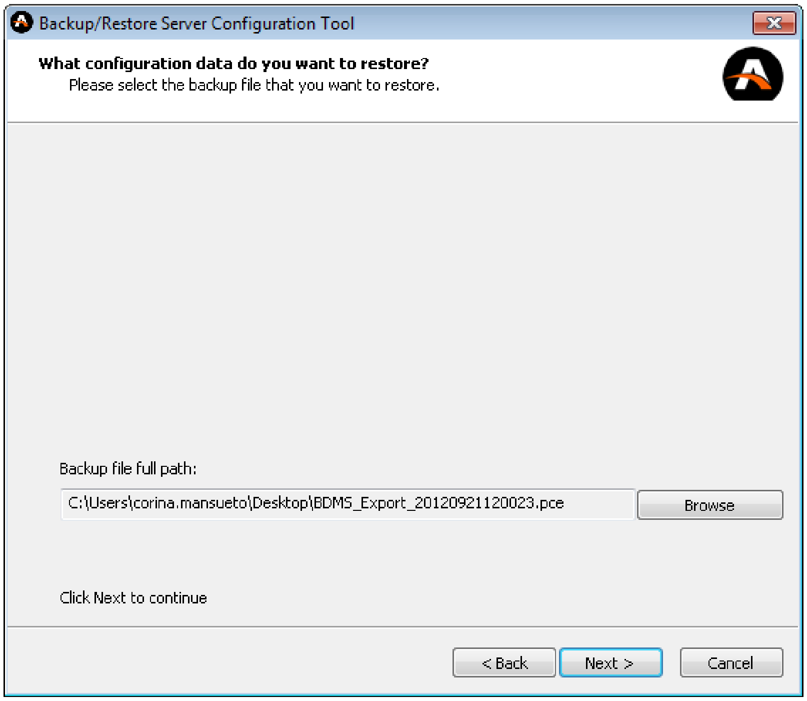
The following options are available:

- **Backup** - to save the Ad-Aware Management Server configuration to a backup file.

- **Restore** - to restore a previously saved configuration of Ad-Aware Management Server from a backup file.

Select the second option and click **Next**.

Step 3/4 - Select Backup File



Backup/Restore Server Configuration Tool

What configuration data do you want to restore?
Please select the backup file that you want to restore.

Backup file full path:

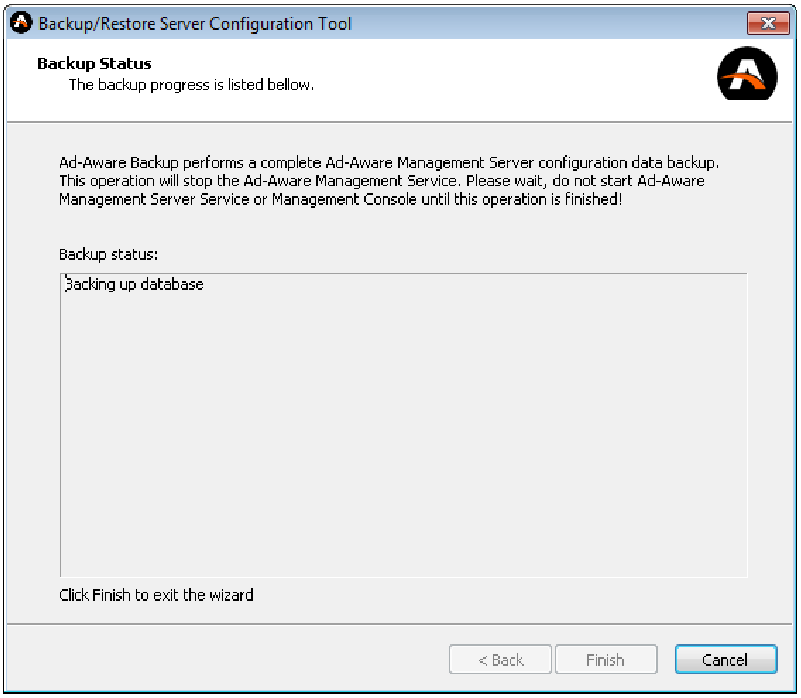
C:\Users\corina.mansueto\Desktop\BDMS_Export_20120921120023.pce

Select Backup File

You must specify the location of the backup file containing the Ad-Aware Management Server configuration that you want to restore. Click **Browse**, locate and open the configuration backup file. Configuration backup files have the . pcb extension.

Click **Next** to start the restore operation.

Step 4/4 – Finish


Backup/Restore Server Configuration Tool

Backup Status

The backup progress is listed bellow.

Ad-Aware Backup performs a complete Ad-Aware Management Server configuration data backup. This operation will stop the Ad-Aware Management Service. Please wait, do not start Ad-Aware Management Server Service or Management Console until this operation is finished!

Backup status:

Backing up database

Click Finish to exit the wizard

Finish

You can see the data restore progress. Wait until the configuration data is successfully restored. This operation may take a few minutes.

After the operation is completed, click **Finish**.

Master-Slave Configurations

Ad-Aware Management Server provides great scalability through its master-slave architecture. You can set up a master instance of Ad-Aware Management Server to manage a number of slave instances of Ad-Aware Management Server. The master-slave architecture can be used both to extend the Ad-Aware Management Server capabilities in very large computer networks and to centrally manage Ad-Aware Management Server instances in different physical locations.

In this chapter you can find information about the master-slave architecture of Ad-Aware Management Server and the differences between the single (stand-alone), slave and master instances of Ad-Aware Management Server.

Master-Slave Configuration Overview

In a master-slave architecture, a specific instance of Ad-Aware Management Server (the master server) manages other instances of Ad-Aware Management Server (the slave servers). The stand-alone and slave instances are almost identical in functionality and user interface.

A slave server acts as a single (stand-alone) instance of Ad-Aware Management Server, managing network computers. Furthermore, the slave server receives policies and tasks assigned by and reports to its master server. An extra-column added to the policies and tasks tables indicates the owner of a policy or task.

The master server does not have its own managed computers, but it indirectly manages those of its slave servers by assigning policies and tasks to them. Another main purpose of the master server is to provide you with information on the network security status, by centralizing data from all managed servers. In this way, you can get centralized results from all the clients of the slave servers in a single report.

Feature Availability in Master Servers

The functionality and user interface of the master server is similar to an extent to that of stand-alone and slave servers. Some features however are not available on master servers.

Unavailable features:

- The Management Dashboard
- Network Audit
- Scheduled Reports
- Unavailable Tools: Registration, Network Builder, Automatic Deployment, Retry Deployment, View Deployment Status, E-mail Settings

Registering a Stand-Alone Server to a Master Server

If you want a single (stand-alone) instance of Ad-Aware Management Server to be managed by a master, follow these steps:

1. Connect to the Ad-Aware Management Server instance using the management console.
2. Right-click the instance name in the tree menu and select **Register to Master server**. A new window will appear.
3. Enter the IP address or name of the master server and the server communication port. The default port is 7073.
4. Click **OK**.

Unregistering from Master Server

If you want a slave server not to be managed by its master anymore, right-click its name in the tree menu and select **Unregister from Master server**.

License Management

License management is done by the slave servers. You cannot and do not need to enter a license key on the master server.

All you have to do is to register each slave server with a license key that allows it to manage a specific number of Ad-Aware client products. You can register a slave server as described in Registering Ad-Aware Management Server.

Tree Menu on Master Servers

You can choose between two modes to view the tree menu of a master instance of Ad-Aware Management Server:

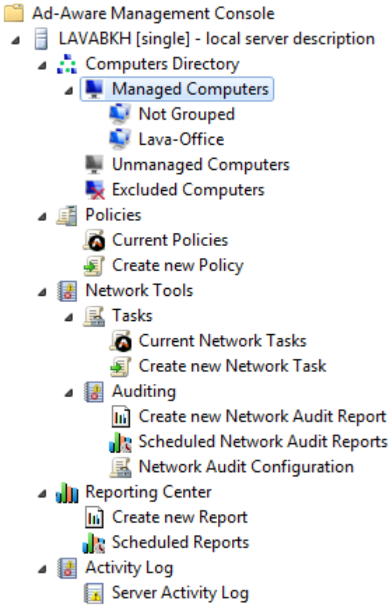
- Network View
- Virtual View

The tree menu will change depending on the chosen viewing mode.

To switch from one view to the other, right-click the Ad-Aware Management Server instance in the tree menu and select the appropriate option.

Network View

In Network View, you can see in the tree menu the servers managed by Ad-Aware Management Server grouped under **Managed servers**. Each slave server contains its Computers Directory, with the corresponding Managed Computers, Unmanaged Computers and Excluded Computers groups.



Tree Menu in Network View

Master Policies and Network Tool > Master Tasks allow managing policies and tasks for each slave server. An extra-column added to the policies and tasks tables indicates the owner of a policy or task.

Virtual View

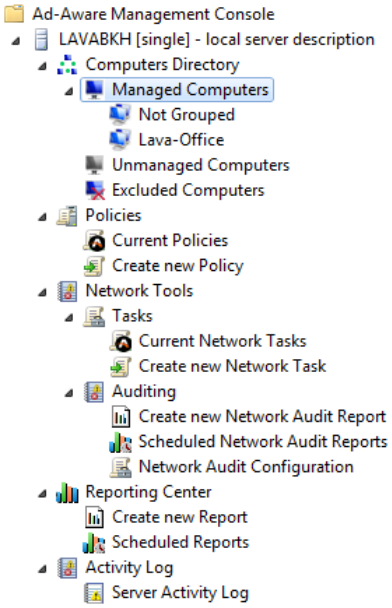
In Virtual View, there is a global Computers Directory that contains all the network computers from all Computers Directory of each slave server.

This virtual Computers Directory has the following groups:

- **Virtual Managed Computers** - displays the managed computers of all slave servers.
- **Virtual Unmanaged Computers** - does not display any computer.

  Note
  In Virtual View, you cannot see the detected network computers that are not managed by the slave instances of Ad-Aware Management Server.

- **Virtual Excluded Computers** - displays the computers excluded from the management of all slave servers.



Tree Menu in Virtual View

Master/Virtual Policies

The master server allows you to create and assign policies to its slave servers in order to indirectly manage their respective clients.

In *Network View*, you can create and assign policies to clients based on the slave servers that manage them. The current policies are also grouped based on the slave servers they are assigned to.

In *Virtual View*, you can create and assign virtual policies to any client from the virtual Computers Directory, irrespective of the slave server that manages it. All of the current virtual policies assigned are displayed in the Virtual Current Policies pane.

A policy assigned by a master server cannot be altered in any way (modified, deleted, renamed) by an administrator logged to the slave server. Moreover, such a policy has precedence over a local policy assigned by the slave server.

Master/Virtual Tasks

The master server allows you to create and assign tasks to its slave servers in order to find out more information about their respective clients or perform administrative tasks.

A task assigned by a master server cannot be altered in any way (modified, deleted, renamed) by an administrator logged to the slave server.

Master Reporting Center

Master Reporting Center is similar to Reporting Center. It allows you to create centralized reports on the security status of the network computers managed by all or only specific slave servers. In this way, you can get in a single report the security status of all the company's computers, even if they are part of networks in different physical locations.

You can create reports in the *Create New Report* pane. When creating a report, you will be able to select to create the report for the master server or only for specific slave servers.

Note
Scheduled reports are not available for master servers.

Master Activity Log

Master Activity Log is similar to *Activity Log*. It contains information regarding the activity of the master Ad-Aware Management Server.

Note
Master Activity Log does not provide information regarding the activity of the slave servers.

You can examine the activity of Ad-Aware Management Server (errors, warnings and successful actions that occurred during its operation) in the *Server Activity* pane.

Policy Templates

Ad-Aware Management Server Templates

The Ad-Aware Management Server policy templates allow you to create policies that you can assign to clients or client groups in order to manage Ad-Aware Management Server.

Note

In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Management Server:

Ad-Aware Management Agent Settings

Allows creating policies through which you can configure the settings of Ad-Aware Management Agent.

Ad-Aware Management Agent Connection

Allows creating policies through which you can change the settings used by Ad-Aware Management Agent to connect to Ad-Aware Management Server.

Ad-Aware Management Agent Settings

This policy template allows you to create policies concerning the settings of Ad-Aware Management Agent. You can specify how often Ad-Aware Management Agent should connect to Ad-Aware Management Server depending on the network type.

- **Local Area Network (LAN).** The following options are available:

Option	Description
Small	Sets the minimum connection interval to 5 minutes. Recommended for small networks.
Medium	Sets the minimum connection interval to 10 minutes. Recommended for medium networks.
Large	Sets the minimum connection interval to 2 hours. Recommended for large networks.
Custom	Allows customizing the minimum connection interval. Select the desired connection interval from the menu.

- **Virtual Private Network (VPN).** The following options are available:

Option	Description
Default	Sets the minimum connection interval to one hour.
Custom	Allows customizing the minimum connection interval. Select the desired connection interval from the menu.

Ad-Aware Management Agent Connection

This policy template allows you to create policies that change the settings used by Ad-Aware Management Agent to connect to Ad-Aware Management Server. You would typically use such a policy before moving Ad-Aware Management Server to another machine (with a different IP address) or changing the communication port.

Fill in the following fields:

- **New server name or IP address** - type in the new IP address or name of the computer Ad-Aware Management Server is installed on.
- **New server port** - type in the new port used by Ad-Aware Management Agent to connect to Ad-Aware Management Server.

If Ad-Aware Management Agent does not manage to connect to Ad-Aware Management Server using the new settings, it will use the previous settings to connect to the former Ad-Aware Management Server. Ad-Aware Management Agent will automatically connect to the new Ad-Aware Management Server once this is available.

Ad-Aware Business Client Templates

The Ad-Aware Business Client policy templates allow you to create policies that you can assign to clients or client groups in order to manage Ad-Aware Business Client. By using these policies you can ensure consistent configuration of Ad-Aware Business Client throughout the network and compliance with your organization's regulations regarding the workstation security.

Note

In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Business Client:

Update Request

Allows creating policies through which you can configure and trigger an immediate update of Ad-Aware Business Client.

Update Settings

Allows creating update policies for Ad-Aware Business Client

Scan Policy

Allows creating on-demand antimalware scan policies for Ad-Aware Business Client

Antivirus Settings

Allows creating antivirus policies for Ad-Aware Business Client

Firewall Settings

Allows creating firewall policies for Ad-Aware Business Client

Privacy Control

Allows creating policies for the Privacy Control module of Ad-Aware Business Client

Anti-spam Settings

Allows creating anti-spam policies for Ad-Aware Business Client

User Control

Allows creating policies for the User Control module of Ad-Aware Business Client

Exceptions

Allows creating scan exception policies for Ad-Aware Business Client

Advanced Settings

Allows creating policies concerning the advanced settings of Ad-Aware Business Client

Device Detection

Allows creating policies for automatic detection and scanning of removable storage media by Ad-Aware Business Client

Select Main Active Modules

Allows creating policies that control which Ad-Aware Business Client modules are installed

Update Request

This policy template allows you to create policies through which you can configure and trigger an immediate update of Ad-Aware Business Client. You can set Ad-Aware to update over the Internet or from a mirror inside the local network, directly or through a proxy server.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

The settings are organized into 4 sections:

- Used Settings
- Update Locations
- Proxy Settings
- Advanced Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Used Settings

You can choose to use the settings configured on the client or to configure the update settings as needed.

Update Locations

In this section you can configure the update location settings. You will need to configure these settings in the following situations:

- Your company connects to the Internet through a proxy server.
- Ad-Aware update files are available on a local mirror created using http://definitionsbd.lavasoft.com.

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and an **Alternate update location**. By default, these locations are the same: `http://definitionsbd.lavasoft.com`.

To download updates from a local update server, change the primary update location using one of these syntaxes:

- `http://update_server_ip:port`
- `http://update_server_name:port`

The default port is `7074`.

Note
We recommend you to set as primary update location the local mirror and to leave the alternate update location unchanged, as a fail-safe plan in case the local mirror becomes unavailable.

If the company uses a proxy server to connect to the Internet, select **Use proxy** and specify the proxy settings.

Proxy Settings

In this section you can specify the proxy settings. If you have selected **Use proxy** next to either of the update locations, you must fill in these fields:

- **Server** - type in the IP of the proxy server.
- **Port** - type in the port Ad-Aware uses to connect to the proxy server.
- **Username** - type in a user name recognized by the proxy.
- **Password** - type in the valid password of the previously specified user.

Advanced Settings

In this section you can configure advanced update settings. The following options are available:

- **Wait for reboot, instead of prompting** - If an update requires a reboot, the product will keep working with the old files until the system is rebooting. The user will not be prompted for rebooting; therefore the Ad-Aware update process will not interfere with the user's work.
- **Update components**. You can specify which updates to be downloaded and installed by choosing the appropriate option:
  - product and signature updates
  - product updates only
  - signature updates only

Signature updates enable Ad-Aware to detect and block the latest malware and spam identified by the Ad-Aware Labs. This is why it is very important to keep Ad-Aware up to date with the latest signatures.

Signature updates do not update the scan engines, but this will not cause any problems in the scanning process.

Update Settings

This policy template allows you to create update policies for Ad-Aware Business Client. You can set Ad-Aware to update over the Internet or from a mirror inside the local network, directly or through a proxy server.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

The settings are organized into 4 sections:

- Update Locations
- Proxy Settings
- Scheduler Settings
- Advanced Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Update Locations

In this section you can configure the update location settings. You will need to configure these settings in the following situations:

- Your company connects to the Internet through a proxy server.
- Ad-Aware update files are available on a local mirror created using http://definitionsbd.lavasoft.com.

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and an **Alternate update location**. By default, these locations are the same: `http://definitionsbd.lavasoft.com`.

To download updates from a local update server, change the primary update location using one of these syntaxes:

- `http://update_server_ip:port`
- `http://update_server_name:port`

The default port is `7074`.

Note

We recommend you to set as primary update location the local mirror and to leave the alternate update location unchanged, as a fail-safe plan in case the local mirror becomes unavailable.

If the company uses a proxy server to connect to the Internet, select **Use proxy** and specify the proxy settings.

Proxy Settings

In this section you can specify the proxy settings. If you have selected **Use proxy** next to either of the update locations, you must fill in these fields:

- **Server** - type in the IP of the proxy server.
- **Port** - type in the port Ad-Aware uses to connect to the proxy server.
- **Username** - type in a user name recognized by the proxy.
- **Password** - type in the valid password of the previously specified user.

Scheduler Settings

In this section you can configure the automatic update schedule of Ad-Aware Business Client.

With automatic update enabled, Ad-Aware Business Client automatically checks for, downloads and installs updates every hour (default setting). You can change the update interval as needed.

Note
Power users can disable automatic update or change how often the program checks for new updates.

You can choose to enable automatic update as an alternative to updating through scheduled update policies. Or, you can use both methods.

Advanced Settings

In this section you can configure advanced update settings. The following options are available:

- Wait for reboot, instead of prompting - If an update requires a reboot, the product will keep working with the old files until the system is rebooting. The user will not be prompted for rebooting; therefore the Ad-Aware update process will not interfere with the user's work.
- Update components. You can specify which updates to be downloaded and installed by choosing the appropriate option:
  - product and signature updates
  - product updates only
  - signature updates only

Signature updates enable Ad-Aware to detect and block the latest malware and spam identified by the Ad-Aware Labs. This is why it is very important to keep Ad-Aware up to date with the latest signatures.

Signature updates do not update the scan engines, but this will not cause any problems in the scanning process.

Scan Policy

This policy template allows you to create on-demand antimalware scan policies for Ad-Aware Business Client. By using scan policies you can set Ad-Aware to scan for malware the assigned clients, one time only or on a regular basis. You can choose a default configuration of the scan level or you can specify the scanning options, the scan target and the actions to be taken on the detected files.

The scanning is performed silently in the background. The user is informed that a scanning process is running only through an icon that appears in the system tray.

The settings are organized into 4 sections:

- Scan Level
- Scan Options
- Scan Actions
- Other Options

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Scan Level

In this section you can set the scan level. The scan level specifies the scanning options, the locations to be scanned and the actions to be taken on the detected files.

Choose the scan level that fits the purpose of the scan policy you want to create. There are 4 scan levels:

Scan Level	Description
Deep system scan	The entire system is scanned for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.
Full system scan	The system is scanned for all types of malware threatening its security, except for rootkits. Archives are not scanned.
Quick system scan	The `Windows`, `Program Files` and `All Users` folders are scanned for all types of malware, except for rootkits. Archives, memory, the boot sectors, the registry and cookies are not scanned.
Custom scan	Allows customizing the scanning options, the locations to be scanned and the actions to be taken on the detected files. You can configure these settings in the *Options* and *Actions* sections.

Note

If Ad-Aware is set to perform **Deep system scan** or **Full system scan**, the scanning may take a while. Therefore, you should run such scan policies on low priority or, better, when the assigned clients are idle.

Scan Options

In this section you can configure the scanning options and the locations to be scanned.

Note

These settings can be configured only if you have set the scan level to Custom scan.

The scan settings Ad-Aware offers may help you adapt the scanning process to your needs. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve the system's responsiveness during a scan.

To configure the scan settings, follow these general steps:

1. Specify the type of malware you want Ad-Aware to scan for. You can do that by selecting the appropriate options from the **Scan level settings** category.

   The following options are available:

Option	Description
Scan for viruses	Scans for known viruses. Ad-Aware detects incomplete virus bodies, too, thus removing any possible threat to the system's security.
Scan for adware	Scans for adware threats. Detected files will be treated as infected. The software that includes adware components might stop working if this option is enabled.
Scan for spyware	Scans for known spyware threats. Detected files will be treated as infected.
Scan for application	Scans for programs that can be used for spying purposes.
Scan for dialers	Scans for applications dialing high-cost numbers. Detected files will be treated as infected. The software that includes dialer components might stop working if this option is enabled.
Scan for rootkits	Scans for hidden objects (files and processes), generally known as rootkits.

Note

These options affect only the signature-based scanning. The heuristic analysis will report any suspicious file no matter the options you choose to be disabled.

2. Specify the type of objects to be scanned (all or specific file types, archives, e-mail messages and so on). You can do that by selecting specific options from the **Virus scanning options** category.

   The following options are available:

Option		Description
Heuristic Scan		Scans for unknown viruses using heuristic methods.
Scan files	**Scan all files**	All files are scanned, regardless of their type.
	Scan program files only	Only application (or program) files are scanned. For more information, please refer to Application Files.
	Scan user defined extensions	Only the files with the extensions you specify will be scanned. The extensions must be separated by ";".
Scan packed files		Scan packed programs.
Scan inside archives		Scan archive files. Password-protected archives cannot be scanned.
Scan inside e-mails archives		Scans inside mail archives. Ad-Aware may not have the legal rights or may not be able to disinfect certain e-mails from e-mail archives. In such cases, please contact us for support at Business Support.
Scan boot sectors		Scans system boot sectors.
Scan memory		Scans the memory for viruses and other malware.

Scan registry		Scans registry entries.
Scan cookies		Scans cookie files.

- Specify the locations to be scanned. You can set Ad-Aware to scan `My Computer`, `My Documents` or you can select **Paths** and type the locations to be scanned in the edit field, separated by a semi-colon `";"`.

Scan Actions

In this section you can specify the actions to be taken on the files detected by Ad-Aware as infected, suspicious or hidden.

Note

These settings can be configured only if you have set the scan level to Custom scan.

You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file.

- **Infected files**. The following options are available:

Action	Description
Take no action	No action will be taken on infected files. These files will appear in the report file.
Disinfect files	Removes the malware code from infected files. This option is available only as a first action.
Delete files	Deletes infected files immediately, without any warning.
Move files to quarantine	Moves infected files into the quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.

- **Suspicious files**. The following options are available:

Action	Description
Take no action	No action will be taken on suspicious files. These files will appear in the report file.
Delete files	Deletes suspicious files immediately, without any warning.
Move files to quarantine	Moves suspicious files into the quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.

Note

Files are detected as suspicious by the heuristic analysis. We recommend you to send these files to the Ad-Aware Lab.

- **Hidden files**. The following options are available:

Action	Description
Take no action	No action will be taken on hidden files. These files will appear in the report file.

Rename files	Changes the name of hidden files by appending aa.ren to their name. As a result, you will be able to search for and find such files on your computer, if any.

Other Options

In this section you can configure general options regarding the scanning process. The following options are available:

Option	Description
Submit suspect files to Ad-Aware Lab	Automatically submits all suspicious files to the Ad-Aware lab after the scan process has finished.
Run task with low priority	Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
Show scan progress bar in sys tray	Informs the user when a scan is running by displaying an icon in the system tray.
Shutdown computer when the task is finished	This option may be useful when you run scans during off-working hours.

Antivirus Settings

This policy template allows you to create policies for the Antivirus module of Ad-Aware Business Client. The Antivirus module protects the system against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on). This module has two components:

- On-access scanning (or real-time protection): prevents new malware threats from entering the system by scanning all accessed files, e-mail messages and the messages sent through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).
- On-demand scanning: allows detecting and removing malware already residing in the system. You can manage this component using the *Scan Policy* template.

Ad-Aware allows isolating the infected or suspicious files in a secure area, named quarantine. By isolating these files in the quarantine, the risk of getting infected disappears and, at the same time, you have the possibility to send these files for further analysis to the Ad-Aware lab.

Note

When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

The settings are organized into 5 sections:

- Real-time Protection
- Protection Level
- Settings
- Quarantine Setting

- Behavioral Scanner Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Real-time Protection

In this section you can enable or disable real-time protection.

If you want real-time protection to be enabled, select **Enable real-time protection**. Otherwise, clear this check box.

Protection Level

In this section you can configure the protection level. This is where you can easily configure real-time protection using default configurations or a custom configuration.

Choose the protection level that best suits your security needs. There are 4 protection levels:

Protection Level	Description
Aggressive	Offers high security. The resource consumption level is moderate. All files, incoming & outgoing mail messages and web traffic are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/deny access.
Moderate	Offers standard security. The resource consumption level is low. All files and incoming & outgoing mail messages are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/deny access.
Permissive	Covers basic security needs. The resource consumption level is very low. Programs and incoming mail messages are only scanned for viruses. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/deny access.
Custom	Allows customizing the real-time protection settings. You can configure these settings in the *Settings* section.

Settings

In this section you can configure the real-time protection settings individually.

Note

These settings can be configured only if you have selected the Custom protection level.

The scan settings Ad-Aware offers may help you fully adapt real-time protection to your company's regulations regarding workstation security. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve the system's responsiveness during a scan.

The following options are available:

- **Scan accessed files and P2P transfers options** - scans the accessed files and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Further on, select the type of the files you want to be scanned.

Option		Description
Scan accessed files	**Scan all files**	All the accessed files will be scanned, regardless their type.
	Scan program files only	Only application (or program) files are scanned. For more information, please refer to Application Files.
	Scan user defined extensions	Only the files with the extensions you specify will be scanned. The extensions must be separated by " ; " .
	Scan for riskware	Scans for riskware. Detected files will be treated as infected. The software that includes adware components might stop working if this option is enabled. Select **Skip dialers and applications from scan** if you want to exclude these kinds of files from scanning.
Scan boot		Scans the system's boot sector.
Scan inside archives		The accessed archives will be scanned. With this option ON, the computer will slow down.
Scan packed files		All packed files will be scanned.
First action		Select from the drop-down menu the first action to take on infected and suspicious files.
	Deny access and continue	In case an infected is detected, the access to this will be denied.
	Disinfect files	Removes the malware code from infected files.
	Delete file	Deletes infected files immediately, without any warning.
	Move file to quarantine	Moves infected code from infected files.
Second action		Select from the drop-down menu the second action to take on infected files, in case the first action fails.
	Deny access and continue	In case an infected file is detected, the access to this will be denied.
	Delete file	Deletes infected files immediately, without any warning.

	Move file to quarantine	Moves infected files into quarantine.
Do not scan archives greater than [X] Kb		Type in the maximum size of the archives to be scanned. If the size is 0 Kb, all archives will be scanned, regardless their size.

- **Scan e-mail traffic** - scans the e-mail traffic.

The following options are available:

Option	Description
Scan incoming e-mails	Scans all incoming e-mail messages.
Scam outgoing e-mails	Scans all outgoing e-mail messages.

- **Scan http traffic** - scans the http traffic.
- **Show warning when a virus is found** - opens an alert window when a virus is found in a file or in an e-mail message.

For an infected file the alert window will contain the name of the virus, the path to it, the action taken by Ad-Aware and a link to the Ad-Aware site where you can find more information about it. For an infected e-mail the alert window will contain also information about the sender and the receiver.

In case of a suspicious file, the user can launch a wizard from the alert window in order to send that file to the Ad-Aware Lab for further analysis. The user can provide an e-mail address so as to receive information regarding the report.

Quarantine Settings

In this section you can configure the quarantine settings. You can set Ad-Aware to automatically perform the following actions:

Delete old files. To automatically delete old quarantined files, check the corresponding option. You must specify the number of days after which the quarantined files should be deleted and frequency with which Ad-Aware should check for old files.

Note

By default, Ad-Aware will check for old files every day and delete files older than 30 days.

Delete duplicates. To automatically delete duplicate quarantined files, check the corresponding option. You must specify the number of days between two consecutive checks for duplicates.

Note

By default, Ad-Aware will check for duplicate quarantined files every day.

Automatically submit files. To automatically submit quarantined files, check the corresponding option. You must specify the frequency with which to submit files.

Note

By default, Ad-Aware will automatically submit quarantined files every 60 minutes.

Behavioral Scanner Settings

In this section you can configure the behavioral-based detection components. Ad-Aware Business Client includes two such components, aimed to enhance traditional signature-based and heuristic detection:

- Ad-Aware Active Virus Control is an innovative proactive detection technology which uses advanced heuristic methods to detect new potential threats in real time.

Active Virus Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful. You can configure Active Virus Control to only detect and report potentially harmful processes, or also block potentially harmful processes with or without asking the user.

- Ad-Aware Host Intrusion Detection/Prevention monitors the system for suspicious activities (for example, unauthorized attempts to alter the Ad-Aware files, DLL injections, keylogging attempts etc).

To enable and configure these components, follow these steps:

1. Enable Active Virus Control and Host Intrusion Detection/Prevention by selecting the corresponding check boxes.
2. If you want to only detect and report potentially harmful processes, select **Run in detection mode only**. You can check the detected applications in the Ad-Aware Management Server dashboard or by creating an **Ad-Aware AVC Detections** malware report.
3. Choose the protection level that best suits your security needs.

   As you set the protection level higher, Active Virus Control will require fewer signs of malware-like behavior to report a process. This will lead to a higher number of applications being reported and, at the same time, to an increased likelihood of false positives (clean applications detected as malicious).

   As for Host Intrusion Detection/Prevention, changing the protection level defines what suspicious activities to monitor. When the protection level is set to **Low**, only attempts to install malware drivers and unauthorized attempts to alter Ad-Aware files are reported. The medium protection level adds DLL injections to this list, while on the **High** protection level many other suspicious activities are reported (including Internet Explorer leaks and keylogging attempts).

4. If you have not selected the **Run in detection mode only** check box, you can add rules for trusted applications. These applications will not be monitored; therefore they will never be reported or blocked. You can also choose the action to be taken on detected applications.

   You should create rules for commonly used or known applications to prevent false positives. To configure rules for trusted applications, follow these steps:

   1. In the **Application name** field, type the name of the application.
   2. Choose the **Allow** action from the menu.
   3. Click **Add**.

The applications will appear in the table as you add them. You can add as many applications as you want. To remove an entry from the table, select it and click **Delete**.

5. By default, rules will append to those already configured on the client computer. To apply only the rules configured in this policy, clear the check box under the rules table.

Firewall Settings

This policy template allows you to create firewall policies for Ad-Aware Business Client. The Firewall protects the computer from inbound and outbound unauthorized connection attempts.

The settings are organized into 3 sections:

- General Settings
- Profile Settings
- Other Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

General Settings

In this section you can enable or disable the Ad-Aware Firewall and configure the general settings.

If you want Firewall to be enabled, select the corresponding check box. Otherwise, clear the check box.

To block all network / Internet traffic, select the corresponding check box.

If you want a generic firewall profile to be applied each time the user connects to a new network or a network is disabled, select **Use generic profile in all networks**.

Profile Settings

In this section you can configure the settings for both the current and the generic firewall profiles. The current firewall profile contains the rules that currently control applications' network / Internet access. The generic firewall profile contains the rules that are initially applied each time the network configuration changes.

In order to configure the profile settings, follow these general steps:

1. Specify whether the settings are to be applied to the current profile, the generic profile or to both.
2. Specify whether or not to check applications for changes.

Note

Usually, applications are changed by updates. But there is a risk that they might be changed by malware applications, with the purpose of infecting the local computer and other computers in the network.

Select **Check process integrity** if you want each application attempting to connect to the Internet to be checked whether it has been changed since the addition of the rule controlling its Internet access. If the application has been changed, an alert will prompt the user to allow or to block the access of the application to the Internet.

Signed applications are supposed to be trusted and have a higher degree of security. You can select Ignore signed process to automatically allow changed signed applications to connect to the Internet.

3. If you do not want to delete the firewall rules already configured on the client workstation, select the Append rules check box. If an existing rule is in contradiction with a rule configured in the policy, the second has priority.
4. Ad-Aware Business Client can inform users connected to a Wi-Fi network when a new computer joins the network. To display such notifications on the user's screen, select the Enable Wi-Fi notifications check box.
5. Configure the firewall rules that should be applied. You can select to apply the following groups of predefined rules:

Predefined rules	Description
Essential rules	Allow network / Internet connection for: • Domain Name System (DNS); • Dynamic Host Configuration Protocol (DHCP); • winlogon; • userinit; • Lightweight Directory Access Protocol (LDAP); • Windows updates; • The Kerberos computer network authentication protocol.
Remote Desktop Connection incoming rules	Allow network computers to connect to the computer using Remote Desktop Connection.
Remote Desktop Connection outgoing rules	Allow the computer to connect to other network computers using Remote Desktop Connection.
Samba incoming rules	Allow network computers to connect to the computer’s Samba shares.
Samba outgoing rules	Allow the computer to connect to the Samba shares of other network computers.
VPN incoming rules	Allow incoming VPN connections.
VPN outgoing rules	Allow outgoing VPN connections.
Internet Connection Sharing rules	If Internet Connection Sharing is enabled, these rules will allow the computer to share its Internet connection with other network computers.
Optional rules	Allow network / Internet connection for: • Universal Plug and Play (UPnP) protocol; • Network Time Protocol (NTP); • Remote Authentication Dial-In User Service • (RADIUS); • Active Sync.
Web browser rules	Allow the default web browser to connect to the Internet.
E-mail rules	Allow the default e-mail client to connect to the network or the Internet.

If you want to, you can configure the firewall rules in detail and add new rules. For more information, please refer to these topics:

- Managing Rules
- Configuring New Rules

Managing Rules

To see the configured rules, to create additional rules or to manage the rules you have created, click **Manage Rules**. A new pane will be displayed.

The configured firewall rules are grouped into two separate sections: Rules for incoming packets and **Rules for outgoing packets**. For each rule listed in the table, you can see:

- The group the rule belongs to. This can be a default group or the **Administrator rules** group, which contains the custom firewall rules that you have created
- The generic path to the application the rule applies to
- The protocol the rule applies to
- The rule action (allow or deny packets)
- The packet source (IP address, subnet mask, port) the rule applies to
- The packet destination (IP address, subnet mask, port) the rule applies to
- The network events the rule applies to

To edit an administrator rule, select it and click **Modify**. To change the priority of an administrator rule by one level, use the **Move up** and **Move down** buttons.

To delete an administrator rule, select it and click **Delete**. You can select **Delete complementary rule** to automatically delete the complementary rule for the other type of packets.

Note
You can neither delete/modify the default firewall rules, nor change their priority.

Configuring New Rules

To configure a new firewall rule, follow these steps:

1. Click **Manage Rules** and then click **Add**.
2. In the **Process path** field, type the path to the application the new firewall rule applies to.
3. From the **Protocol** menu, select the protocol the rule applies to. You can choose to apply the rule to one or all of the following protocols: ICMP, TCP, UDP.
4. From the **Direction** menu, select the traffic direction the rule applies to: incoming, outgoing or both.

Note
If you select **Both**, two complementary rules will be created: one for incoming packets and the other for outgoing packets.

4. From the **Action** menu, select the rule action (allow or deny packets).

5. Specify the packet source the rule applies to.

    Type the source IP address and subnet mask in the corresponding fields.

    If you want the rule to apply to all ports, select **Any Port** from the menu. Otherwise, select **Specific Port** or **Port Range** and type in the desired port(s).

7. Specify the packet destination the rule applies to.

    Type the destination IP address and subnet mask in the corresponding fields.

    If you want the rule to apply to all ports, select **Any Port** from the menu. Otherwise, select **Specific Port** or **Port Range** and type in the desired port(s).

8. If you have selected TCP or UDP as protocol, choose the network events the rule applies to.
9. Click **Add** to add the rule.

Other Settings

In this section you can configure the automatic response to the firewall alerts. The firewall asks for permission each time an application that does not match any rule in the current profile tries to connect to the Internet. Based on the user's response or on the automatic response configured, a rule is created for the respective application and it is added to the profile.

Choose from the menu an automatic response to the firewall alerts. The following options are available:

Automatic response	Description
Forced Yes	The application is automatically allowed to connect to the Internet.
Forced No	The application is not allowed to connect to the Internet. No alert window is displayed on the user's screen.
Ask user	An alert window with detailed information is displayed on the user's screen, prompting the user for action.
Database of known files and forced No	The application is automatically allowed to connect to the Internet only if it is in the Ad-Aware whitelist. Otherwise, its connection attempt is blocked.
Database of known files and ask user	The application is automatically allowed to connect to the Internet only if it is in the Ad-Aware whitelist. Otherwise, the user is prompted for action.

Privacy Control

This policy template allows you to create policies for the Privacy Control module of Ad-Aware Business Client. This module has two independent functionalities:

- Web Anti-phishing: ensures safe web navigation by alerting the user about potential phishing web pages.
- Privacy Control: prevents data theft, monitors applications that try to load at system startup, and protects against two types of potential Internet threats, cookies and scripts.

The settings are organized into 7 sections:

- Protection
- Protection Level
- Settings
- Identity Control
- Cookie Control
- Script Control
- Alerts

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Protection

In this section you can enable or disable Privacy Control.

If you want Privacy Control to be enabled, select the corresponding check box. Otherwise, clear this check box.

Privacy Control has the following components:

- Identity Control - prevents data theft by filtering all outgoing HTTP and SMTP traffic according to the rules you create in the Identity Control section.
- Registry Control - asks for permission whenever a new program, which does not match any of the current rules, tries to modify a registry entry in order to be executed at Windows start-up. Rules are automatically created for the local client product based on the user's response or on the automatic response configured in the Alerts section.
- Cookie Control - asks for permission whenever a new web page, which does not match any of the current rules, tries to set a cookie. Rules are automatically created for the local client product based on the user's response or on the automatic response configured in the Alerts section. You can also configure global rules manually in the Cookie Control section.
- Script Control - asks for permission whenever a new web page, that does not match any of the current rules, tries to run a script or other active content. Rules are automatically created for the local client product based on the user's response or on the automatic response configured in the Alerts section. You can also configure global rules manually in the Script Control section.

Protection Level

In this section you can configure the protection level. The protection level specifies which components of Privacy Control should be enabled.

Choose the protection level that suits the purpose of the policy you want to create.

The following options are available:

Protection Level	Description
Aggressive	All the components of the Privacy Control are enabled. You must configure appropriate Identity Control rules to prevent the unauthorized sending of confidential information.
Moderate	**Registry control** and **Identity Control** are enabled. You must configure appropriate Identity Control rules to prevent the unauthorized sending of confidential information.
Permissive	Only **Registry control** is enabled.

Note

You can also enable or disable each component of Privacy Control separately, without configuring the protection level.

Settings

In this section you can enable or disable Registry Control and Web Anti-phishing.

Registry Control. Registry Control prompts the user for permission whenever a program tries to modify a registry entry in order to be executed at Windows start-up. If you want Registry Control to be enabled, select **Registry Control.** Otherwise, clear this check box.

Show Anti-phishing Protection. Web Anti-phishing alerts the user about potentially phished web pages. If you want Web Anti-phishing to be enabled, select **Show Anti-phishing Protection**. Otherwise, clear this check box.

If you choose to enable the Anti-phishing protection, you can also choose whether or not to show the Anti-phishing toolbar. This toolbar enables the user to manage the Anti-phishing protection (even when the program operates in restricted user mode).

Identity Control

In this section you can configure Identity Control. Identity Control filters all outgoing HTTP and SMTP traffic according to the rules you created. The e-mail messages and web pages containing a string indicated in one of these rules are blocked.

If you want Identity Control to be enabled, select **Enable Identity Control**. Otherwise, clear this check box.

You can see a table where the configured rules are displayed. If you want only these rules to be applied and to overwrite the rules of the local client product, clear the **Append rules** check box.

To configure a rule, follow these steps:

1. In the **Rule name** field, type the name of the rule.
2. From the **Rule type** menu, choose the rule type (address, name, credit card, PIN, SSN etc).
3. In the **Rule data** field, type the string you want to prevent being sent.

Note

We recommend you to enter at least three characters in order to avoid the mistaken blocking of messages and web pages.

4. Select **Scan HTTP** to scan the outgoing web traffic and block the outgoing data that matches the rule data.
5. Select **Scan SMTP** to scan the outgoing mail traffic and block the outgoing e-mail messages that contain the rule data.
6. To block web pages and e-mail messages only if the rule data matches whole words, select **Match whole words.**
7. To block web pages and e-mail messages only if the rule data and the detected string case match, select **Match case**.
8. In the **Rule description** field, type a description of the specified rule.
9. Click **Add**. The new rule will be added to the table.

To remove an entry from the table, select it and click **Delete**.

At the bottom of this section you can see another table where exceptions to the specified rules are displayed. If you want only these exceptions to be applied and to overwrite those of the local client product, clear the **Append exceptions** check box.

To add an exception, follow these steps:

1. From the **Exception type** menu, choose the type of exception you want to create.
2. In the **Allowed web/e-mail address** field, type the web address or the mail address that you want to add as exception.
3. Click **Add** to add the new exception in the table.

To remove an exception from the table, select it and click **Remove**.

Cookie Control

In this section you can configure Cookie Control. Cookie Control helps you control which web pages are allowed to set cookies or to request them and which are not.

If you want Cookie Control to be enabled, select **Enable Cookie Control**. Otherwise clear this check box.

To configure a rule, follow these steps:

1. Specify the domain to which the rule applies. Do one of the following:

- To apply the rule to all domains, select **Any**.
- To apply the rule to a specific domain, select **Enter domain** and type the domain name in the edit field.

2. Select the action of the rule. The following options are available:

Action	Description
Permit	The cookies on that domain will execute.
Deny	The cookies on that domain will not execute.

3. Select the traffic direction. The following options are available:

Type	Description
Outgoing	The rule applies only for the cookies that are sent out back to the connected site.
Incoming	The rule applies only for the cookies that are received from the connected site.
Both	The rule applies to both directions.

4. Click **Add**. The new rule will be added in the table.

Note

It may be more convenient to set a global rule to block cookies for any domain and then set rules to allow cookies for the web sites that you fully trust. To block cookies for any domain, follow these steps:

1. Select **Any** for domain.
2. Set the action to **Deny**.
3. Set the direction either to **Outgoing** (to accept receiving cookies, but prevent them from being sent out back) or to **Both** (to block cookies in both directions).

You can add as many rules as needed. For the web sites for which no rule has been configured, the user can be prompted for action or a default action is taken. For more information, please refer to section Alerts.

To remove an entry from the table, select it and click **Delete**.

Cookie Control rules may already be configured on the client workstation (for example, through a previously applied policy or through Cookie Control alerts). If you want only the rules in this policy to be applied, clear the **Append rules** check box. Consequently, all of the existing rules will be deleted.

If you choose to append the newly-configured rules to the existing ones, the following situations may occur:

- The rules configured in this policy do not interfere with any of the rules already configured on the client workstation. In this case, the newly-configured rules will simply be added to the existing rules.
- A rule configured in this policy and an existing rule refers to the same web site, but they are not in contradiction. In this case, the two rules will be merged.
- A newly-configured rule is in contradiction with one of the existing rules. In this case, the rule configured in this policy has priority.

Script Control

In this section you can configure Script Control. Script Control helps you control which web pages are allowed to run active content (scripts, ActiveX controls, Java applets) and which are not.

Note

Some web pages may not be properly displayed if you block active content.

If you want Script Control to be enabled, select **Enable Script Control**. Otherwise, clear this check box.

To configure a rule, follow these steps:

1. In the **Domain** field, type the domain to which the rule applies.

2. Select the action of the rule. The following options are available:

Action	Description
Permit	The scripts on that domain will execute.
Deny	The scripts on that domain will not execute.

3. Click **Add**. The new rule will be added to the table.

You can add as many rules as needed. For the web sites for which no rule has been configured, the user can be prompted for action or a default action is taken. For more information, please refer to section Alerts.

To remove an entry from the table, select it and click **Delete**.

Script Control rules may already be configured on the client workstation (for example, through a previously applied policy or through Script Control alerts). If you want only the rules in this policy to be applied, clear the **Append rules** check box. Consequently, all of the existing rules will be deleted.

If you choose to append the newly-configured rules to the existing ones, the following situations may occur:

- The rules configured in this policy do not interfere with any of the rules already configured on the client workstation. In this case, the newly-configured rules will simply be added to the existing rules.
- A rule configured in this policy and an existing rule refers to the same web site, but they are not in contradiction. In this case, the two rules will be merged.
- A newly-configured rule is in contradiction with one of the existing rules. In this case, the rule configured in this policy has priority.

Alerts

In this section you can configure the automatic response to the registry, cookie and script alerts.

Choose from the corresponding menus an automatic response for each type of alert.

Note

You cannot choose an automatic response if the respective component is disabled.

- **Registry Alerts**. You can choose one of the following automatic responses:

Automatic response	Description
Ask user (alert is shown)	An alert window with detailed information is displayed on the user's screen, prompting the user for action.
Forced No	The application is not allowed to modify registry entries in order to be executed at Windows start-up. No alert window is displayed on the user's screen.
Forced Yes	The application is automatically allowed to modify registry entries in order to be executed at Windows start-up, without notifying the user.

- **Cookie Alerts**. You can choose one of the following automatic responses:

Automatic response	Description

Ask user (alert is shown)	An alert window with detailed information is displayed on the user's screen, prompting the user for action.
Forced No	The web page is not allowed either to place its cookies on the user's system or to receive them. No alert window is displayed on the user's screen.
Forced Yes	The web page is automatically allowed to place its cookies on the user's system or to receive them, without notifying the user.

- **Script Alerts**. You can choose one of the following automatic responses:

Automatic response	Description
Ask user (alert is shown)	An alert window with detailed information is displayed on the user's screen, prompting the user for action.
Forced No	The web page is not allowed to execute active content. No alert window is displayed on the user's screen.
Forced Yes	The web page is automatically allowed to execute active content, without user notification.

Anti-spam Settings

This policy template allows you to create policies for the Anti-spam module of Ad-Aware Business Client. Ad-Aware Anti-spam employs remarkable technological innovations and industry standard anti-spam filters to weed out spam before it reaches the user's Inbox.

The settings are organized into 3 sections:

- Protection
- Protection Level
- Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Protection

In this section you can enable or disable Anti-spam protection.

If you want the Anti-spam protection to be enabled, select Enable Anti-spam. Otherwise, clear this check box.

Protection Level

In this section you can configure the protection level. The protection level defines the anti-spam aggressiveness which Ad-Aware should use to process e-mails.

Choose the protection level that better fits your security needs. There are 5 protection levels:

Protection level	Description
Aggressive	Offers protection for accounts that receive very high volumes of spam regularly. The filter will let very little spam through, but it may produce false positives (legitimate mail incorrectly tagged as spam).
Moderate to Aggressive	Offers protection for accounts that receive high volumes of spam regularly. The filter will let very little spam through, but it may produce false positives (legitimate mail incorrectly tagged as spam).
Moderate	Offers protection for regular accounts. The filter will block most spam, while avoiding false positives.
Permissive to Moderate	Offers protection for accounts that receive some legitimate commercial mail. The filter will let most e-mail pass through, but it may produce false negatives (spam classified as legitimate mail).
Permissive	Offers protection for accounts that receive a lot of legitimate commercial mail. The filter will let most e-mail pass through, but it may produce false negatives (spam classified as legitimate mail).

Settings

In this section you can configure the anti-spam filters and settings. The Ad-Aware Anti-spam engine incorporates seven different filters that ensure protection against the various types of spam: Friends list, Spammers list, Charset filter, Image filter, URL filter, NeuNet (Heuristic) filter and Bayesian filter.

The anti-spam settings are grouped into three categories:

- Anti-spam Settings
- Basic Anti-spam Filters
- Advanced Anti-spam Filters

Anti-spam Settings

These settings allow you to specify whether or not to tag the e-mail messages detected by the Anti-spam module. If you select:

- **Mark spam messages in subject** - all e-mail messages considered to be spam will be tagged with SPAM in the subject line.
- **Mark phishing messages in subject** - all e-mail messages considered to be phishing messages will be tagged with SPAM in the subject line.

Basic Anti-spam Filters

These settings allow you to configure basic anti-spam filters and related options. You can select:

- **Friends/Spammers lists** - to filter e-mail messages according to the Friends/Spammers lists. Any e-mail coming from an address contained in the Friends list is automatically delivered to the Inbox, without further processing. Any e-mail received from an address contained in the Spammers list is automatically marked as SPAM, without further processing.

> **Note**
>
> You should recommend the users to add the e-mail addresses of their contacts to the Friends list.

You can select:

- **Automatically add recipients to Friends list** - to automatically add recipients of sent mail to Friends list.
- **Automatically add to Friends list** - to automatically add the sender of a selected e-mail to Friends list when the user clicks the **Not Spam** button from the Anti-spam toolbar. In this way, you can prevent the confirmation window from being displayed.
- **Automatically add to Spammers list** - to automatically add the sender of a selected e-mail to Spammers list when the user clicks the **Is Spam** button from the Anti-spam toolbar. In this way, you can prevent the confirmation window from being displayed.

> **Note**
>
> The Anti-spam toolbar is integrated into the most common mail clients and allows configuring the Friends/Spammers lists and training the Learning Engine. The Not Spam and the **Is Spam** buttons are used to train the Learning Engine.

- **Block mails written in Asian characters** - to consider SPAM e-mail messages written in Asian charsets.
- **Block mails written in Cyrillic characters** - to consider SPAM e-mail messages written in Cyrillic charsets.

> **Note**
>
> If certain users receive legitimate e-mails written in Asian or Cyrillic charsets, create special policies that disable the detection of such e-mails.

Advanced Anti-spam Filters

These settings allow you to configure advanced anti-spam filters and related options.

You can select:

- **Enable the Learning Engine (bayesian)** - to check e-mail messages using the Learning Engine (bayesian). The Learning Engine classifies messages according to statistical information regarding the rate at which specific words appear in messages classified as SPAM compared to those declared NON-SPAM (by the user or by the heuristic filter).

This means, for example, if a certain four-letter word is seen to appear more often in SPAM, it is natural to assume there is an increased probability that the next incoming message that includes it actually IS SPAM. All relevant words within a message are taken into account. By synthesizing the statistical information, the overall probability for the whole message to be SPAM is computed.

This module presents another interesting characteristic: it is trainable. It adapts quickly to the type of messages received by a certain user, and stores information about all. To function effectively, the filter must be trained, meaning, to be presented with samples of SPAM and legitimate messages, much like a hound is primed to trace a certain scent. Sometimes the filter must be corrected too - prompted to adjust when it makes a wrong decision.

You can configure the following options:

- **Limit the dictionary size to 200000 words** - sets the size of the Bayesian dictionary - smaller is faster, bigger is more accurate. The recommended size is: 200.000 words.
- **Train the Learning Engine (bayesian) on outgoing e-mails** - trains the Learning Engine (bayesian) on outgoing e-mails. Outgoing e-mails are considered to be legitimate messages.

- **Enable URL filter** - to filter e-mail messages using the URL filter. The URL filter checks every URL link in a message against its database. If a match is made, the message is tagged as SPAM.
- **Enable NeuNet (Heuristic) filter** - to check e-mail messages using the NeuNet (Heuristic) filter. The NeuNet (Heuristic) filter performs a set of tests on all the message components (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of SPAM. Based on the results of the analysis, it adds a SPAM score to the message.
  - You can select **Block explicit content** to activate the detection of messages marked as SEXUALLY EXPLICIT in the subject line.

Note

Starting May 19, 2004, spam that contains sexually oriented material must include the warning SEXUALLY-EXPLICIT: in the subject line or face fines for violations of federal law.

- **Enable Image filter** - to filter e-mail messages using the Image filter. The Image filter deals with image spam. It compares the image from a message with those from the Ad-Aware database. In case of a match, the message is tagged as SPAM.

User Control

This policy template allows you to create policies for the User Control module of Ad-Aware Business Client. User Control can be used to block the users' access to:

- Applications such as games, chat, file sharing programs or others.
- The Internet, for certain periods of time or completely.
- Inappropriate web pages.
- Web pages and e-mail messages if they contain certain keywords.

The settings are organized into 6 sections:

- User Control
- General Settings

- Web Control
- Applications Control
- Keywords Control
- Webtime Control

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

User Control

In this section you can enable or disable User Control.

If you want User Control to be enabled, select **Enable User Control.** Otherwise, clear this check box.

User Control has the following components:

- **Web Control** - filters web navigation according to the rules you set in the Web Control section. It also blocks access to the inappropriate content web pages included in the list provided and updated by Ad-Aware.
- **Applications Control** - blocks access to applications you specified in the Applications Control section.
- **Keyword Control** - filters web and mail access according to the rules you set in the Keywords Control section.
- **Webtime Control** - allows web access according to the timetable set by you in the Webtime Control section.
- **Heuristic web filter** - filters web access according to pre-established content-based rules.

You must enable the components you want to use and configure them accordingly.

General Settings

In this section you can block web access and configure the heuristic web filter. The heuristic web filter analyzes web pages and blocks those that match the patterns of potentially inappropriate content.

Select **Block web access** if you want to block access to all websites (not just the ones specified in the Web Control section).

To configure the heuristic web filter, follow these steps:

1. Select **Heuristic web filter tolerance**.
2. Set a specific tolerance level in order to filter web access according to a predefined content-based rule set.

There are 3 tolerance levels:

Tolerance level	Description
High	Offers unrestricted access to all web pages regardless of their content.
Medium	Offers restrictive web access. Web pages with sexual, pornographic or adult content are blocked.
Low	Offers highly restrictive web access. Web pages with inappropriate content (porn, sexuality, drugs, gambling, hacking etc)

	are blocked.

3. If you only want to alert the user when accessing a potentially inappropriate web page, select the check box corresponding **Allow the user to add blocked web pages to whitelist**. The user will be able to view and add the web page to the whitelist.

To automatically block web pages detected by the heuristic web filter, clear this check box.

If you do not want to use the heuristic web filter, either clear the **Heuristic web filter tolerance** check box or set the tolerance level to **High**.

Web Control

In this section you can configure Web Control. Web Control helps you to block access to web pages with inappropriate content. Ad-Aware provides and updates a list of candidates for blocking, made up of both web pages and parts thereof, as part of the regular update process. When assigning a policy with Web Control enabled, these web pages (mostly pornographic) are automatically blocked.

The web pages blocked by Web Control are not displayed in the browser. Instead, a default web page is displayed informing the user that the requested web page has been blocked by Web Control.

If you want Web Control to be enabled, select **Enable Web Control**. Otherwise, clear this check box.

In order to use Web Control, you must select one of the following options:

- **Block these pages** - to block access to specific web pages.
- **Allow these pages** - to allow access only to specific web pages.

Two tables are displayed: one for the blocked/allowed web pages and the other for the allowed exceptions. If you want only these web pages to be filtered and the pages indicated in the local client product to be overwritten, clear the **Append pages and exceptions** check box.

Specify the web pages to be blocked/allowed and the allowed exceptions to these pages, if any.

Note
Exceptions may be needed when defining web pages using wildcards.

To specify a web page to be blocked/allowed or an exception, follow these steps:

1. Type the name of the web page in the edit field.

Important
You can use wildcards instead of entire names of web pages. For example, if you type:

- *.xxx.com - the action of the rule will apply on all web sites finished with .xxx.com;
- *porn* - the action of the rule will apply on all web sites containing porn in the web site address;
- www.*.com - the action of the rule will apply on all web sites having the domain suffix com;
- www.xxx.* - the action of the rule will apply on all web sites starting with www.xxx. no matter the domain suffix.

2. Click **Add**. The new web page will be added in the table.

To remove an entry from the table, select it and click **Delete**.

Applications Control

In this section you can configure Applications Control. Applications Control helps you block any application from running. Games, media and messaging software, as well as other categories of software and malware can be blocked in this way.

If you want Applications Control to be enabled, select **Enable Applications** Control. Otherwise, clear this check box.

You can see a table where the applications to be blocked are displayed. If you want only these applications to be blocked and the applications indicated in the local client product to be overwritten, clear the **Append applications** check box.

To add an application to the blockading list, follow these steps:

1. Type the full name of the application.
2. Click **Add**. The application name will appear in the table.

To remove an entry from the table, select it and click **Delete**.

Keywords Control

In this section you can configure Keyword Filtering. Keyword Filtering helps you block access to e-mail messages or web pages that contain specific strings. In this way you can prevent users from accessing inappropriate content.

The web pages and e-mails matching a filtering rule are not displayed. Instead, a default web page or e-mail is displayed informing the user that the respective web page or e-mail has been blocked by Keyword Filtering.

If you want Keyword Filtering to be enabled, select **Enable Keyword Filtering**. Otherwise, clear this check box.

You can see a table where the configured rules are displayed. If you want only these rules to be applied and the rules indicated in the local client product to be overwritten, clear the **Append keywords** check box.

To configure a rule, follow these steps:

1. Type the keyword (word or phrase) you want to be blocked in the edit field.
2. Choose from the menu the protocol Ad-Aware should scan for the specified keyword. The following options are available:

Option	Description
POP3	E-mail messages that contain the keyword are blocked.
HTTP	Web pages that contain the keyword are blocked.
Both	Both e-mail messages and web pages that contain the keyword are blocked.

3. To block web pages and e-mail messages only if the keyword matches whole words, select **Match whole words.**
4. Click **Add**. The new rule will be added to the table.

To remove an entry from the table, select it and click **Delete**.

Webtime Control

In this section you can configure Webtime Control. Webtime Control helps you allow or block web access for users or applications during specified time intervals.

Note
Ad-Aware will update itself as configured no matter the settings of Webtime Control.

If you want Webtime Control to be enabled, select **Enable Webtime Control**. Otherwise, clear this check box.

You can see the timetable according to which web access is allowed. Click individual cells to select the time intervals when all internet connections will be blocked.

Important
The boxes colored in grey represent the time intervals when all internet connections are blocked.

Exclusions

This policy template allows you to create scan exclusion policies for Ad-Aware Business Client. You can exclude specific paths or application types (extensions) from both real-time and on-demand scanning. You can also configure exceptions for HTTP traffic, which will affect real-time antimalware scanning and Identity Control and User Control rules.

Note
If you have an EICAR test file that you use periodically to test Ad-Aware, you should exclude it from on-access scanning.

The settings are organized into 4 sections:

- Exclusions
- Paths
- Extensions
- Manage HTTP Exceptions

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Exclusions

In this section you can enable or disable the use of scan exclusions.

If you want to apply scan exceptions, select **Enable scan exceptions**. Otherwise, clear this check box.

Paths

In this section you can configure specific paths to be excluded from scanning. Paths can be excluded from both real-time and on-demand scanning.

Note

The exceptions specified here will NOT apply for contextual scanning. Contextual scanning is initiated by right-clicking a file or folder and selecting **Ad-Aware Business Client.**

You can see a table containing the paths to be excluded from scanning and the type of scanning they are excluded from. If you want only these paths to be excluded from scanning, clear the **Append paths** check box. To also exclude the paths configured through previously assigned policies, keep this check box selected.

To configure paths to be excluded from scanning, follow these steps:

1. In the **New path** field, type the path to be excluded from scanning.

Note

You can use system variables to specify the path. Some of the most common are listed in the following table.

System Variable	Description
`%PROGRAMFILES%`	The Program Files folder. The typical path is `C:\Program Files`.
`%SYSTEM%`	The Windows System folder. A typical path is `C:\Windows\System32`.
`%WINDOWS%`	The Windows directory or SYSROOT. A typical path is `C:\Windows`.

2. From the menu, choose to exclude the path from the on-demand or on-access scanning, or from both.
3. Click **Add**. The new path will appear in the table.

To remove an entry from the table, select it and click **Delete**.

Extensions

In this section you can configure specific extensions to be excluded from scanning. Extensions can be excluded from both real-time and on-demand scanning.

Application files are far more vulnerable to malware attacks than other types of files. You should not exclude these extensions from scanning. For more information, please refer to Application Files.

Note

The exceptions specified here will NOT apply for contextual scanning. Contextual scanning is initiated by right-clicking a file or folder and selecting Ad-Aware Business Client.

You can see a table containing the extensions to be excluded from scanning and the type of scanning they are excluded from. If you want only these extensions to be excluded from scanning, clear the **Append extensions** check box. To also exclude the extensions configured through previously assigned policies, keep this check box selected.

To configure extensions to be excluded from scanning, follow these steps:

1. Do one of the following:

- In the **New extension** field, type the extension to be excluded from scanning.

You can enter only one extension for each rule.

- Choose an extension from the corresponding menu. The menu contains a list of all the extensions registered on your system.

2. From the menu, choose to exclude the extension from the on-demand or on-access scanning, or from both.
3. Click **Add**. The new extension will appear in the table.

To remove an entry from the table, select it and click **Delete**.

Manage HTTP Exceptions

Ad-Aware Business Client intercepts the HTTP traffic in order to scan it for malware and to apply the relevant Identity Control and User Control policies. The HTTP traffic that does not comply with the HTTP standard is automatically blocked, without any warning.

In this section you can configure HTTP exceptions. HTTP exceptions automatically allow the HTTP traffic involving specific applications or IP or web addresses.

Important

Use caution when defining HTTP exceptions. HTTP exceptions can make the workstation more vulnerable to viruses and other malware. Add HTTP exceptions only for applications, IP and web addresses that you fully trust.

Applications

When an application is added as an HTTP exception, the HTTP traffic to or from that application is no longer intercepted by Ad-Aware. This means that:

- The respective traffic is not scanned for viruses.
- The relevant Identity Control and User Control policies are not applied to the respective traffic.

Here is an example of an application that may be added as an HTTP exception: a proprietary application, which generates HTTP traffic non-compliant with the HTTP standard, does not work after Ad-Aware Business Client is deployed.

Warning
Do not add web browsers as HTTP exceptions, unless advised by an Ad-Aware support representative! Excluding a web browser from HTTP scanning will disable virus scanning and the Identity Control and User Control policies for content sent or received via that browser.

To configure applications as HTTP exceptions, follow these steps:

1. Select **Except Applications**.
2. In the **Application paths** field, type the name of the application to be excluded and then click **Add**.

The applications will appear in the table as you add them. You can add as many applications as you want. To remove an entry from the table, select it and click **Delete**.

3. If you want only these rules to be applied and to overwrite those of the local client product, clear the **Append rules** check box.

IP Addresses and IP Subnets

When an IP address is added as an HTTP exception, the HTTP traffic to or from that IP address is no longer intercepted by Ad-Aware. Similarly, when an entire IP subnet is added as an HTTP exception, the HTTP traffic to or from IP addresses belonging to that subnet are no longer intercepted by Ad-Aware. This means that:

- The respective traffic is not scanned for viruses.
- The relevant Identity Control and User Control policies are not applied to the respective traffic.

Here are some situations when you may add IP addresses or subnets as HTTP exceptions:

- Identity Control rules have been configured to prevent private or confidential information from being sent from the workstation over HTTP. To allow such information to be exchanged internally over HTTP, you may add the IP addresses of the internal web servers as HTTP exceptions.
- To disable HTTP virus scanning for specific IP addresses, which are known to be safe (for example, the IP address of an intranet HTTP server).

To configure IP addresses and subnets as HTTP exceptions, follow these steps:

1. Select **Except IPs/IP classes**.
2. Specify the exceptions:

- To exclude a single IP address, type it in the **IP Address** field, select from the menu a 32 bit subnet mask and then click **Add**.
- To exclude an entire subnet, type the subnet address in the **IP Address** field, select the subnet mask from the menu and then click **Add**.

The IP addresses or subnets will appear in the table as you add them. You can add as many exceptions as you want. To remove an entry from the table, select it and click **Delete**.

- If you want only these rules to be applied and to overwrite those of the local client product, clear the **Append rules** check box.

Web Addresses

When a web address is added as an HTTP exception, the HTTP traffic to or from that web site is no longer intercepted by Ad-Aware. This means that:

- The respective traffic is not scanned for viruses.
- The relevant Identity Control and User Control policies are not applied to the respective traffic.

You may want to add fully trusted web addresses as HTTP exceptions in order to make web browsing faster for users. For example, you can set an exception for the traffic that passes through an internal proxy server that provides antimalware scanning.

To configure web addresses as HTTP exceptions, follow these steps:

1. Select **Except web addresses**.
2. In the **Web address** field, type the web address and then click **Add**.

The web addresses will appear in the table as you add them. You can add as many as you want. To remove an entry from the table, select it and click **Delete**.

3. If you want only these rules to be applied and to overwrite those of the local client product, clear the **Append rules** check box.

Size Exceptions

You can choose to skip scanning HTTP traffic that exceeds a specific size (for example, large file downloads). Specify the size limit in kilobytes (KB) in the corresponding field.

Note
Selecting this option can make web browsing faster for users.

Advanced Settings

This policy template allows you to create policies concerning the advanced settings of Ad-Aware Business Client. You can choose to load Ad-Aware at Windows startup, to enable/disable the Scan Activity bar and to configure other general settings.

The settings are organized into 3 sections:

- General Settings
- Virus Report Settings
- Password

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

General Settings

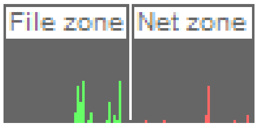
In this section you can configure the general settings of Ad-Aware Business Client.

The following options are available:

- **Show Ad-Aware News (security related notifications)** - shows from time to time security notifications regarding virus outbreaks, sent by the Ad-Aware server.
- **Show pop-ups** - shows pop-up windows regarding the product status. These pop-ups can be useful to the user.
- **Load Ad-Aware at Windows startup** - automatically launches Ad-Aware at system startup. We recommend you to keep this option selected.
- **Enable the Scan Activity bar** - displays the Scan Activity bar. The Scan Activity bar is a graphic visualization of the scanning activity on the system.

The green bars (the **File Zone**) show the number of scanned files per second, on a scale from 0 to 50.

The red bars displayed in the **Net Zone** show the number of Kbytes transferred (sent and received from the Internet) every second, on a scale from 0 to 100.



Scan Activity Bar

You may find this small window useful for two reasons:

  - The Scan Activity bar will notify the user when real-time protection or the Ad-Aware firewall is disabled by displaying a red cross over the corresponding area (**File Zone** or **Net Zone**).
  - The user can drag & drop files or folders over the Scan Activity bar in order to scan them.

- **Send information about crashes to Ad-Aware** - if the product crashes, the error log is sent to the Ad-Aware Labs and the Ad-Aware services are reinitialized.

If **Ask the user to confirm the submission of the crash information** is also selected, the user logged on to the workstation will be informed about the crash. In this case, the user must confirm the sending of the error log and the restart of the Ad-Aware services.

Virus Report Settings

In this section you can configure the virus reporting settings. The following options are available:

- **Send virus reports** - sends to the Ad-Aware Labs reports regarding viruses identified on the company's computers.

  The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.

- **Enable Ad-Aware Outbreak Detection** - sends to the Ad-Aware Labs reports regarding potential virus-outbreaks.

The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the potential virus and will be used solely to detect new viruses.

Password

In this section you can configure the administrative password of Ad-Aware Business Client. If this password is set:

- Users with an administrator account on the client workstation can remove the program only after providing the administrative password. Power users can remove the program without having to provide the administrative password.
- Users who know the password (authorized users) can temporarily switch to the power user mode and change the program settings directly from the client workstation.

Note

To switch to the power user mode, authorized users must right-click the Ad-Aware icon in the system tray, select **Switch to power user** and enter the password. Ad-Aware Business Client will operate in the power user mode until the Windows session ends (computer restart, shutdown, and log off). The user can also manually switch back to the restricted user mode.

To set or remove the administrative password, select **Administrative password** and proceed as follows:

- To set the administrative password, select Set and type the desired password. You must provide authorized users with this password.

Note

If another administrative password is already set on an assigned client workstation, it will be replaced with this new password.

- To remove the current password, select **Remove**. Consequently, users will no longer be able to switch to the power user mode by themselves.

To apply the policy without changing the current setting of the administrative password, clear the **Administrative password** check box.

Device Detection

This policy template allows you to create policies for automatic detection and scanning of storage devices by Ad-Aware Business Client. In this way, you can block malicious software from CDs/DVDs, USB storage devices or mapped network drives.

The settings are organized into 4 sections:

- General Settings
- Scan Options
- Scan Actions

- Other Options

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

General Settings

In this section you can specify the detection and notification settings.

- **Detection settings**. Choose which types of storage media you want Ad-Aware Business Client to detect and scan: CDs/DVDs, USB storage devices and mapped network drives.
- **Notification settings**. Choose the options you consider best for the users who will be assigned the policy:
- **Ask user for action**. An alert window informs the user that a storage device has been detected and prompts the user whether or not to scan the device. If you do not select this option, detected devices are scanned automatically.
- **Show a pop-up when the scanning process starts**. A small window informs the user when the scan of a detected storage device is started.
- **Show the progress and results of the scanning process**. The user can open the scan wizard by clicking the scan progress icon in the system tray in order to check the progress and results of the scan.

Do not scan devices with more than a specified size of data stored. You can choose to scan detected devices only if the amount of stored data is smaller than the specified size limit. Type the size limit (in megabytes) in the corresponding field. Zero means that no size restriction is imposed.

Note
This option applies only to CDs/DVDs and USB storage devices.

Scan Options

In this section you can configure the scan options.

The scan settings Ad-Aware offers may help you adapt the scanning process to your needs. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve the system's responsiveness during a scan.

To configure the scan settings, follow these general steps:

1. Specify the type of malware you want Ad-Aware to scan for. You can do that by selecting the appropriate options from the **Scan level settings** category.

   The following options are available:

Option	Description
Scan for viruses	Scans for known viruses. Ad-Aware detects incomplete virus bodies, too, thus removing any possible threat to the system's security.
Scan for adware	Scans for adware threats. Detected files will be treated as infected. The software that includes adware components might stop working if this option is enabled.
Scan for spyware	Scans for known spyware threats. Detected files will be treated as infected.
Scan for application	Scans for known spyware threats. Detected files will be treated as infected.

Scan for dialers	Scans for applications dialing high-cost numbers. Detected files will be treated as infected. The software that includes Scan for dialer's components might stop working if this option is enabled.

Note

These options affect only the signature-based scanning. The heuristic analysis will report any suspicious file no matter the options you choose to be disabled.

2. Specify the type of objects to be scanned (all or specific file types, archives, e-mail messages and so on). You can do that by selecting specific options from the **Virus scanning options** category.
   The following options are available:

Option		Description
Scan files	**Scan all files**	All files are scanned, regardless of their type.
	Scan program files only	Only application files are scanned. For more information, please refer to Application Files.
	Scan user defined extensions	Only the files with the extensions you specify will be scanned. The extensions must be separated by ";".
Scan packed files		Scan packed files.
Scan inside archives		Scans inside archives. Password-protected archives cannot be scanned. If such archives are detected, extract the files they contain in order to scan them.
Scan inside e-mail archives		Scans inside mail archives. Ad-Aware may not have the legal rights or may not be able to disinfect certain e-mails from e-mail archives. In such cases, please contact us for support at Business Support.

Scan Actions

In this section you can specify the actions to be taken on the files detected by Ad-Aware as infected or suspicious.

You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file.

- **Infected files**. The following options are available:

Action	Description
None (log objects)	No action will be taken on infected files. These files will appear in the report file.
Disinfect infected files	Removes the malware code from infected files. This option is available only as a first action.
Delete files	Deletes infected files immediately, without any warning.
Move files to Quarantine	Moves infected files into the quarantine.

- **Suspicious files**. The following options are available:

Action	Description
None (log objects)	No action will be taken on suspicious files. These files will appear in the report file.
Delete files	Deletes suspicious files immediately, without any warning.
Move files to Quarantine	Moves suspicious files into the quarantine.

Note

Files are detected as suspicious by the heuristic analysis. We recommend you to send these files to the Ad-Aware Lab.

Other Options

In this section you can configure general options regarding the scanning process. The following options are available:

Option	Description
Submit suspect files to Ad-Aware Lab	Automatically submits all suspicious files to the Ad-Aware lab after the scan process has finished.
Run task with low priority	Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.

Select Main Active Modules

This policy template allows you to create policies that control which main modules of Ad-Aware Business Client are active and displayed in the user interface. If you do not want to use a specific module, you can create such a policy to inactivate it. This is equivalent to installing the program without the respective module.

Clear the check box corresponding to the each module you want to be inactive. The modules set to be inactive will be removed from the user interface on the assigned client computers. Moreover, resources used by these modules will be released.

Here is the list of the main modules of Ad-Aware Business Client and their description.

Antivirus

The Antivirus module protects the system against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on).

Firewall

The Firewall protects the computer from inbound and outbound unauthorized connection attempts.

Anti-spam

The Anti-spam module checks the e-mails downloaded by the local e-mail client for spam. Detected spam e-mails are marked as [spam] in the subject. Moreover, commonly used e-mail clients are configured to automatically move these messages to a quarantine folder.

- In Microsoft Outlook, spam messages are moved to a **Spam** folder, located in the **Deleted Items** folder.
- In Outlook Express and Windows Mail, spam messages are moved directly to **Deleted Items**.

Note

Ad-Aware Business Client offers anti-spam protection only for e-mail clients configured to receive e-mail messages via the POP3 protocol. POP3 is one of the most widely used protocols for downloading e-mail messages from a mail server.

Privacy Control

Privacy Control has the following components:

- Identity Control - enables you to filter outgoing web (HTTP) and mail (SMTP) traffic to prevent users from disclosing confidential information.
- Registry Control - asks for permission whenever a new program, which does not match any of the current rules, tries to modify a registry entry in order to be executed at Windows start-up.
- Cookie Control - asks for permission whenever a new web page, which does not match any of the current rules, tries to set a cookie.
- Script Control - asks for permission whenever a new web page, that does not match any of the current rules, tries to run a script or other active content.

Anti-phishing

Anti-phishing ensures safe web navigation by alerting the user about potential phishing web pages. This module comes with an Internet Explorer toolbar to help users easily manage Anti-phishing protection.

User Control

User Control can be used to block the users' access to:

- Applications such as games, chat, file sharing programs or others.
- The Internet, for certain periods of time or completely.
- Inappropriate web pages.
- Web pages and e-mail messages if they contain certain keywords.

Backup

The Backup module enables the user to make backup copies of important data and restore them if needed.

Update

This module keeps Ad-Aware Business Client up to date to protect the system and data against the latest threats discovered by Ad-Aware Labs.

Ad-Aware Security for SharePoint Templates

The Ad-Aware Security for SharePoint policy templates allow you to create policies that you can use in order to manage Ad-Aware Security for SharePoint. By using these policies you can ensure your organization's SharePoint servers are secure.

Note

In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Security for SharePoint:

Antivirus Settings

Allow creating antivirus policies for Ad-Aware Security for SharePoint

General Settings

Allow creating policies for the general settings of Ad-Aware Security for SharePoint

Get Settings

Allow creating policies for the retrieval of Ad-Aware Security for SharePoint settings

Install product update

Allows creating policies for triggering the installation of a product update for Ad-Aware Security for SharePoint

Rollback

Allows creating policies for rollback to the previous version of Ad-Aware Security for SharePoint

Scanning Scheduled

Allows creating scheduled antivirus scan policies for Ad-Aware Security for SharePoint

Update Request

Allows creating policies for triggering a signature update for Ad-Aware Security for SharePoint

Update Settings

Allow creating policies for the configuration of both signature and product update settings for Ad-Aware Security for SharePoint

Antivirus Settings

This policy template allows you to create policies for the Antivirus module of Ad-Aware Security for SharePoint. The Antivirus module protects the SharePoint server against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on).

This module has two components:

- On-access scanning (or real-time protection): prevents users from downloading or uploading infected files and thus causing the infection to spread throughout the network.
- On-demand scanning: allows detecting and removing malware already residing in the system. You can manage this component using the Scanning Scheduled template.

Ad-Aware allows isolating the infected or suspicious files in a secure area, named quarantine. By isolating these files in the quarantine, the risk of getting infected disappears and, at the same time, you have the possibility to send these files for further analysis to the Ad-Aware lab.

Note

When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

Here you can configure the real-time protection settings that will be applied on the assigned clients. The settings are organized into 4 sections:

- General
- Antivirus Settings
- Action

- Configure scan

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

General

This is where you can set the protection level by selecting a scanning profile. You can use one of the default profiles or create a custom profile.

Choose the protection level that best suits your security needs. There are 4 protection levels:

Protection level	Description
High	Offers high security. The resource consumption level is moderate. • All downloaded and uploaded files, regardless of their extension and size, are scanned. • Files are scanned for all kinds of malware (viruses, Trojans, spyware, adware, riskware, dialers and so on). • Ad-Aware scans inside archives. • The default action taken on infected files is **Disinfect**. If disinfection fails, the files will be moved to quarantine. • The default action taken on suspect files is **Deny**.
Medium	Offers standard security. The resource consumption level is low. • Only the files that do not exceed 10 megabytes (MB) are scanned. • Files are scanned only for viruses, adware and spyware. • Ad-Aware does not scan inside archives. • The default action taken on infected files is **Disinfect**. If disinfection fails, the files will be moved to quarantine. • The default action taken on suspect files is **Deny**.
Permissive	Covers basic security needs. The resource consumption level is very low. • Only the accessed application files that do not exceed 5 megabytes (MB) are scanned. • Files are scanned only for viruses, adware and spyware. • Ad-Aware does not scan inside archives. • The default action taken on infected files is **Disinfect**. If disinfection fails, downloading or uploading such files is denied. • The default action taken on suspect files is **Deny**.
Custom	Allows customizing the real-time protection settings.

Creating Custom Profiles

To create a custom profile, follow these steps:

1. Select **Custom**.
2. Type a name for the profile in the **Custom profile name** text box.

3. Under **Options**, select **Edit profile (create the profile if it does not exist).**

You can configure the profile settings in the *Action* and *Configure Scan* sections.

Antivirus Settings

In this section you can enable or disable the Antivirus settings for the On-Access Scanner.

If you want a setting to be enabled, select the corresponding check box. Otherwise, clear the check box.

The following settings can be configured:

- Enable AV protection
- Set this profile as current profile
- Scan documents on upload
- Scan documents on download
- Allow users to download infected documents
- Attempt to clean infected documents •
- Set max scanning instances number - based on the system configuration and on the number of Ad-Aware products you have chosen to install, an optimal number of scanning instances is computed. Though not recommended, you may change this value for systems with powerful multicore CPUs to speed up scanning.

Action

You can configure the actions to be taken on infected and suspect files for any scanning profile. When an infected or suspect file is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

The antivirus actions are ordered in a list according to their priority. Click the desired action in order to move it up or down.

Actions for infected files. The following actions are available for infected files:

Action	Description
Disinfect	Remove the malware code from the infected files. Disinfection may fail in some cases, such as when the infected file is inside specific mail archives.
Deny	Deny uploading or downloading of infected files by the users.
Move to Quarantine	Move infected files from their original location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove infected files from the server, without any warning.
Ignore	Simply ignore the infected files. **Warning** Do not set **Ignore** as the first action in the list. Doing this will allow users to

	download and upload ALL infected files.

Actions for suspect files. The following actions are available for suspect files:

Action	Description
Deny	Deny uploading or downloading of infected files by the users.
Move to Quarantine	Move suspect files from their original location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove suspect files from the server, without any warning.
Ignore	Simply ignore the infected files. You should not set this action the first in the list unless you explicitly want ALL suspect files to be allowed to be uploaded and downloaded. This poses a high security risk, since some of these files are very likely to carry some form of malware.

Configure Scan

In this section you can configure the real-time protection settings individually.

Note

These settings can be configured only if you have selected a **Custom** profile.

The scan settings Ad-Aware offers may help you fully adapt real-time protection to your company's regulations regarding workstation security. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve the system's responsiveness during a scan.

The following options are available:

Scanning Files by Extension

Some file types are more likely to carry viruses than others.

To specify the file types to be scanned, select one of the following options:

Option	Description
Scan all extensions	Accessed files are scanned regardless of their type.
Scan only application files	Only application files are scanned. For more information, please refer to “Application Files”. Viruses usually infect application files. Therefore, these file types should always be scanned on access.
Scan custom extensions	Only the files with the specified extensions are scanned. You must type in the edit field the file extensions to be scanned by Ad-Aware, separating

	them by semicolons (";").
Scan all except the following extensions	The files with the specified extensions are NOT scanned. You must type in the edit field the file extensions NOT to be scanned by Ad-Aware, separating them by semicolons (";"). You should not exclude from scanning file types commonly known to carry viruses, such as `.exe`, `.doc`, `.ppt`, `.xls`, `.rtf`, `.pif`, `.bat` and others.

Configuring Advanced Settings and Exceptions

Select which types of malware Ad-Aware will scan for:

Option	Description
Applications	Scans for legitimate applications that can be used as a spying tool, to hide malicious applications or for other malicious intent
Adware	Scans for adware threats
Dialers	Scans for applications dialing premium rate phone numbers
Spyware	Scans for known spyware threats
Scan packed files	Scans inside packed files.
Scan inside archives	Scans inside archives. Enter the maximum archive depth to scan in the corresponding text box.
Maximum file size scan	Sets a size limit for the files Ad-Aware will scan. Enter the maximum size in the corresponding text box.

General Settings

This policy template allows you to create policies for general settings of Ad-Aware Security for SharePoint.

Here you can configure the Ad-Aware notification system, real time virus reporting, incident reporting and purge settings. The settings are organized into 4 sections:

- Alerts
- Virus Report
- Report Incidents
- Purge Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Alerts

In this section you can configure event notifications, mail alert templates and settings and net send alert templates.

- Events - this is a list of the events that may occur:

Event	Description
Ad-Aware Error	Groups all the errors that may appear during product operation, such as service start failure.
Update Error	Refers to the occurrence of an error during the update process.
Infected/suspect file detected	Occurs when an infected file or a file suspected of being infected has been detected.
Ad-Aware Warning	Group's critical information regarding the activity of Ad-Aware.
File not scanned	Occurs when a file could not be scanned by Ad-Aware.
Product update	Occurs when a product update is available.
Ad-Aware information	Group's information regarding the activity of Ad-Aware.
Key expired	Indicates the expiration of the registration period.
Key will expire	Indicates that there are 3 days left before the product expires.
On-demand scanning	Occurs whenever an on-demand scan is performed.
Update information	Contains information about the update process.

There are 3 types of events, depending on their importance to the security of the system:

- **Information** - such events provide information about the product activity.
- **Warning** - such events provide critical information about aspects of the product activity which requires your attention.
- **Error** - such events provide information about errors that appear during product operation.

Set the importance of the events by selecting one of the following levels from the drop-down lists corresponding to each event:

- **Low** - a record of the event is kept in the log file. No alert is sent when the event takes place.
- **Medium** - log the event and send mail alerts when the event takes place.
- **High** - log the event and send both mail and net send alerts when the event takes place.

Note

To completely disable notifications for an event, select Disabled from its corresponding drop-down list.

- **Mail Alert Templates** - if the importance of the event is medium or high, mail alerts will be sent.

Each event comes with a default alert text. To view the alert text of an event, click **Edit** next to that event. To change the text, edit the contents of the text box.

Important

You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

- **Net Send Alert Templates** - if the importance of the event is high, net send alerts will be sent.

Each event comes with a default alert text. To view the alert text of an event, click

Edit next to that event. To change the text, edit the contents of the text box.

Important

You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

- **Mail alerts** - to use the mail notification service, follow these steps:

1. Select **Enable Mail Alerts** to activate the mail notification service.

2. Configure the SMTP settings:

   - **SMTP Server** - enter the IP address of the SMTP server that your network uses to send messages.
   - **From** - enter the e-mail address that will appear in the sender field.

Important

Provide a valid e-mail address for the SMTP server, otherwise the server may decline to send an e-mail whose sender (e-mail address) is unknown to it.

3. If the SMTP server used to send messages requires authentication, select **Use SMTP Server Authentication** and enter the user name and password in the corresponding fields.

Note

NTLM authentication is not supported.

4. Indicate the recipients of the mail alerts by entering their e-mail addresses one by one in the text box located under the **Recipients** list box and clicking **Add**. To remove e-mail addresses from the list, select them and click **Delete**.

Note

The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set.

- **Net send alerts** - to use the mail notification service, follow these steps:
  1. Select **Enable Net Send Alerts** to activate the net send notification service.
  2. Indicate the recipients of the net send alerts by entering their computer names one by one in the text box located under the **Recipients** list box and clicking **Add**. To remove computer names from the list, select them and click **Delete**.

Note

The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set.

Virus Report

In this section you can configure real time virus reporting.

Real time virus reporting (RTVR) allows sending reports about the viruses found on your server to the Ad-Aware Lab in order to help us identify new viruses and find quick remedies for them. Your contribution could be essential for developing new tools to protect you and other users against virus threats.

Real time virus reporting is disabled by default. To activate it, select **Enable real time virus reports**.

The reports will contain no confidential data, such as your name, IP address or others and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.

Report Incidents

In this section you can configure the incident management module that allows creating incident reports during crashes of Ad-Aware Security for SharePoint.

By agreeing to send the incident reports to the Ad-Aware Lab, you agree to help us find quick fixes for our bugs. You could make a major contribution to the development of a stable product that satisfies your needs.

By default, the reports created automatically during product crashes are not sent to the Ad-Aware Lab. To configure Ad-Aware to send incident reports to the Ad-Aware Lab, select **I agree to submit incident reports to the Ad-Aware Lab** and enter your e-mail address in the provided text box.

The reports will only be used for debugging purposes. They will never be used as commercial data or disclosed to third parties.

Purge Settings

In this section you can configure the period of time for which Ad-Aware Security for

SharePoint will store the following data:

- Quarantine (quarantined files)
- Statistics
- Reports
- View Logs

By default, data older than 30 days is automatically deleted.

You can set a different time period for each type of data by entering the number of days / weeks / months in the text boxes corresponding to the types of data you wish to edit.

Get Settings

This policy template allows creating policies for retrieving the settings of Ad-Aware Security for SharePoint.

No additional settings are required.

Install Product Update

This policy template allows you to create policies for triggering the installation of a product update for Ad-Aware Security for SharePoint.

The product updates are different from the signature updates. Their function is to deliver bug fixes and new features to the product.

There are two types of updates for the product:

- **Product updates (patches)** - these are files that bring improvements to the current product; they are usually smaller size updates that do not require a new version of the product to be delivered.
- **Version updates** - these are installation packages of a new released version of the product.

The settings are in the *Settings* section.

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Settings

Here you can choose whether or not to allow the installation of the product update if it involves stopping / starting server traffic or rebooting the server.

To agree with the installation in one of the two cases, select the corresponding check box. Otherwise, make sure the check box is cleared.

Rollback

This policy template allows creating policies for rolling back to the previous version of Ad-Aware Security for SharePoint. The rollback feature gives you the option to revert to the previous product version once you have installed a product update.

If a rollback is available, the current product version and the version you can roll back to will be displayed. The rollback does not require other settings to be configured.

After a rollback is performed, the version currently in use and the previous version will be displayed. You can use the provided link to update back to the newer version.

Scanning Scheduled

This policy template allows you to create on-demand antimalware scan policies for Ad-Aware Security for SharePoint. By using scan policies you can set Ad-Aware to scan for malware the assigned clients, one time only or on a regular basis. You can choose a default scanning profile or you can specify the scanning options, the scan target and the actions to be taken on the detected files.

Here you can configure the antimalware scan settings that will be used to scan the assigned clients. The settings are organized into 3 sections:

- General
- Actions
- Configure Scan

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

General

In this section you can set the scan level. The scan level specifies the scanning options, the locations to be scanned and the actions to be taken on the detected files.

Choose the scan level that fits the purpose of the scan policy you want to create.

There are 3 scan levels:

Scan Level	Description
High	Allows performing a comprehensive scan of Central Administration and all the sites. The pre-defined scan settings offer the highest detection efficiency. By default, Ad-Aware is configured to take the following actions: • **Disinfect infected files**. If disinfection fails, the files will be moved to quarantine. • **Move suspect files to quarantine**.
Permissive	Allows a quick scan of all sites using a pre-defined configuration of the scan settings. Only files that do not exceed 5 megabytes (MB) are scanned. By default, Ad-Aware is configured to take the following actions: • Disinfect infected files. If disinfection fails, the files will be moved to quarantine. • Move suspect files to quarantine.
Custom	Allows customizing the scanning options, the locations to be scanned and the actions to be taken on the detected files. You can configure these settings in the *Action* and *Configure Scan* sections.

In case there are tasks scheduled with the same scanning profile, select one of the available options:

- Modify all tasks
- Delete all tasks

Creating Custom Profiles

To create a custom scanning profile, follow these steps:

1. Select **Custom**.

2. Type a name for the profile in the **Custom profile name** text box.

3. Under **Options**, select **Edit profile** (**create the profile if it does not exist**).

4. Select the location to scan - all locations or all except Central Administration.

You can configure the profile settings in the *Action* and *Configure Scan* sections.

Action

You can configure the actions to be taken on infected and suspect files for any scanning profile. When an infected or suspect file is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

The antivirus actions are ordered in a list according to their priority. Click the desired action in order to move it up or down.

Actions for infected files. The following actions are available for infected files:

Action	Description
Disinfect	Remove the malware code from the infected files. Disinfection may fail in some cases, such as when the infected file is inside specific mail archives.
Move to Quarantine	Move infected files from their original location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove infected files from the server, without any warning.
Ignore	Simply ignore the infected files. **Warning** Do not set Ignore as the first action in the list. Doing this will allow users to download and upload ALL infected files.

Actions for suspect files. The following actions are available for suspect files:

Action	Description
Move to Quarantine	Move suspect files from their original location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove suspect files from the server, without any warning.
Ignore	Simply ignore the infected files. You should not set this action the first in the list unless you explicitly want ALL suspect files to be allowed to be uploaded and downloaded. This poses a high security risk, since some of these files are very likely to carry some form of malware.

Configure Scan

In this section you can configure the on-demand antivirus scan settings individually.

Note

These settings can be configured only if you have selected a Custom profile.

The following options are available:

Scanning Files by Extension

To specify the file types to be scanned, select one of the following options:

Option	Description
Scan all extensions	Accessed files are scanned regardless of their type.
Scan only application files	Only application files are scanned. For more information, please refer to Application Files. Viruses usually infect application files. Therefore, these file types should always be scanned on access.
Scan custom extensions	Only the files with the specified extensions are scanned. You must type in the edit field the file extensions to be scanned by Ad-Aware, separating them by semicolons (";").
Scan all expect the following extension	The files with the specified extensions are NOT scanned. You must type in the edit field the file extensions NOT to be scanned by Ad-Aware, separating them by semicolons (";"). You should not exclude from scanning file types commonly known to carry viruses, such as .exe, .doc, .ppt, .xls, .rtf, .pif, .bat and others.

Configuring Advanced Settings and Exceptions

You can configure the following advanced scanning settings:

Option	Description
Applications	Scans for legitimate applications that can be used as a spying tool, to hide malicious applications or for other malicious intent
Adware	Scans for adware threats
Dialers	Scans for applications dialing premium rate phone numbers
Spyware	Scans for known spyware threats
Scan packed files	Scans inside packed files.
Scan inside archives	Scans inside archives. Enter the maximum archive depth to scan in the corresponding text box.
Maximum file size to scan	Sets a size limit for the files Ad-Aware will scan. Enter the maximum size in the corresponding text box.

Update Request

This policy template allows you to create policies for triggering a signature update for Ad-Aware Security for SharePoint.

The template does not require other settings to be configured. You can configure update settings using the *Update Settings* template.

Update Settings

This policy template allows you to create policies for configuring the update settings for Ad-Aware Security for SharePoint. You can configure automatic signature updates, product updates, update locations and notifications.

Here you can configure update settings that will be applied on the assigned clients.

The settings are organized into 4 sections:

- Options
- Product update options
- Update location
- Notifications

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Options

In this section you can configure the automatic signature updates. The automatic update feature allows updating Ad-Aware automatically, on a regular basis, without the administrator's intervention.

By default, Ad-Aware checks for updates at the specified update locations, every hour.

To change the frequency at which Ad-Aware checks for updates, type the number of hours between two consecutive checks for updates in the **Automatic update interval** text box.

To disable the automatic update, clear the check box corresponding to **Automatic update interval**.

Product Update Options

Installing product updates regularly is essential to the security of your server. Depending on the level of interference with the server, there are three types of product updates:

- Product updates that do not require stopping server traffic or to reboot the server
- Product updates that require stopping server traffic, but do not require to reboot the server
- Product updates that require to reboot the server

To configure automatic downloads and installation for each type of product update, select one of the following options:

- **Download updates and install automatically**

Select this option and Ad-Aware will automatically download and install product updates. This is the recommended choice for product updates that do not require stopping server traffic or a server reboot.

- **Download updates automatically and install... at...**

Select this option if you want Ad-Aware to install available updates at certain times. Select from the corresponding drop-down lists the date (day and time) when you want this to happen.

This way you can configure Ad-Aware to perform product updates at times when it is least likely for interferences to occur with server activity (during night time, for example).

- **Download updates and let me decide when to install them**

Select this option if you want Ad-Aware to automatically download product updates, but let you decide when to install them. This is the recommended choice for product updates that require stopping server traffic or a server reboot.

To disable automatic product updates, select the **No automatic product updates** check box.

Note
Your server will be more vulnerable unless you install updates regularly.

Update Location

Ad-Aware can update from the local network, over the Internet, directly or through a proxy server.

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and a **Secondary update location**. Both require the configuration of the following options:

- **Update location** - type the address of the update server. By default, the primary update location is: http://definitionsbd.lavasoft.com.

If multiple Ad-Aware products are installed in your network, you can setup a local server as the first update location for all the products and make http://definitionsbd.lavasoft.com the second location, to be used in case the first becomes unavailable. In this way you can reduce Internet traffic during updates.

- **Allow unsigned updates** - select this option to allow updates from a local server to be installed.
- **Use proxy** - select this option if the company uses a proxy server. The following settings must be specified:
  - **Server Name or IP** - type the IP of the proxy server.
  - **Port** - type the port Ad-Aware uses to connect to the proxy server.
  - **User** - type a user name recognized by the proxy.
  - **Password** - type the valid password of the previously specified user.

Notifications

Ad-Aware can be configured to notify you about special events that occur during its operation.

Select the update events you want to be informed about:

- **Update performed** - when an update was performed.
- **No update available** - when no update is available.
- **Update failed** - when an error occurred during an update and the update failed.
- **Product update available** - when a product update is available.

You can customize the notifications of each update event using the *Alerts* section of the **General Settings** template.

Ad-Aware Security for Mail Servers Templates

The Ad-Aware Security for Mail Servers policy templates allows you to create policies that you can use in order to manage Ad-Aware Security for Mail Servers. By using these policies you can ensure your organization's mail servers are secure.

Note

In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Security for Mail Servers:

Anti-spam filtering settings/rules

Allows creating anti-spam policies for Ad-Aware Security for Mail Servers

Antivirus Settings

Allows creating antivirus policies for Ad-Aware Security for Mail Servers

Attachment filtering rules

Allows creating attachment filtering policies for Ad-Aware Security for Mail Servers

Content filtering rules

Allows creating content filtering policies for Ad-Aware Security for Mail Servers

General Settings

Allows creating general settings policies for Ad-Aware Security for Mail Servers

Get Settings

Allows creating policies for the retrieval of Ad-Aware Security for Mail Servers settings

Install product update

Allows creating policies for triggering the installation of a product update for Ad-Aware Security for Mail Servers

Interface Settings

Allows creating policies through which you can configure SMTP interface properties for Ad-Aware Security for Mail Servers

Rollback product update

Allows creating policies for rollback to the previous version of Ad-Aware Security for Mail Servers

SMTP groups

Allows creating SMTP groups for the Ad-Aware Security for Mail Servers

Update Request

Allows creating policies for triggering a signature update for Ad-Aware Security for Mail Servers

Update Settings

Allows creating policies for the configuration of both signature and product update settings for Ad-Aware Security for Mail Servers

Anti-spam Filtering Settings/Rules

This policy template allows you to create policies for the Anti-spam module of Ad-Aware Security for Mail Servers. The Anti-spam module offers protection against spam, phishing and other attacks. It uses a combination of various filters and engines to determine whether messages are spam or not and to check them for patterns of spam.

Based on the groups the sender and the recipients belong to, you can specify various actions to be taken on the spam messages.

The settings are organized into 3 sections:

- **Anti-spam** - allows you to enable the anti-spam filtering and to configure the global anti-spam filters
- **Rules** - allows you to manage the rules (create, edit or delete a rule)
- **Rule settings** - allows you to configure the filtering options for the selected rules

Anti-spam

This is where you can enable anti-spam filtering and configure the global anti-spam filters.

If you want the anti-spam protection to be enabled, select **Enable anti-spam filtering**. Otherwise, clear this check box.

Global Filters

Several global anti-spam filters can be configured to filter all of the incoming mail traffic, in order to reduce the traffic on the server. These filters are used before a specific group filtering policy is applied.

- **Enable Allow/ Deny IP List**

Select **Enable Allow / Deny IP List** if you want to use the Allow / Deny IP List to filter the incoming mail traffic.

All incoming connections from addresses that appear on the Deny IP List are dropped.

The Allow IP List is used to except IP addresses from ranges of IP addresses defined on the Deny IP List.

Note

If you want to configure the IP addresses list, you need to access the Ad-Aware Security for Mail Servers product interface.

- **Enable Sender Black List**

Select **Enable Sender Black** List if you want to use the Sender Black List to filter incoming mail traffic.

The Sender Black List allows the administrator to specify a list of e-mail addresses which are denied access to the server. The incoming mail from these addresses will be dropped before reaching the server.

Note

If you want to configure the Sender Black List, you need to access the Ad-Aware Security for Mail Servers product interface.

- **Enable IP Match**

Spammers often try to "spoof" the sender's e-mail address to make the e-mail appear as being sent by someone in your domain. To prevent this, you can use IP Match. If an e-mail appears to be from a domain that you have specified in the IP Match rule list (such as your own company domain), Ad-Aware checks to see if the IP address of the sender matches the IP addresses provided for the specified domain.

Note

If you want to configure the IP Match rule list, you need to access the Ad-Aware Security for Mail Servers product interface.

If the domain address of the sender matches the IP address, the message bypasses anti-spam filtering. Otherwise, the connection is dropped.

- **Allow breaking of the DKIM/domain key signature when modifying the e-mails**

Ad-Aware breaks DKIM signatures if filtering rules include actions such as modifying the e-mail subject or adding footers to e-mails. To allow breaking DKIM signatures, select the corresponding check box.

Rules

This is where you can specify the anti-spam filtering options. You can modify the default rule to specify the anti-spam filtering options for all of the mail traffic, or you can configure new rules in order to create customized group filtering policies.

Default Rule. There is one rule created by default that manages the anti-spam filtering settings for all groups. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Adding New Rules. To set different filtering policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following options:

- **Create rule** - to create a new anti-spam rule and configure the anti-spam filters you need to follow these 3 steps:
  1. Go to the **Anti-spam** section and select **I want to make changes to the anti-spam filtering rules**.
  2. Select **Other** from the **Rules** section and choose a name.
  3. Configure the anti-spam filtering policies in the **Rule settings** section.
- **Edit rule** - allows you to configure the selected rule. To configure the rule, please refer to “Rule Settings”.
- **Delete rule** - deletes one / several selected rules. You will have to confirm your choice by clicking **Yes**.

Rule Settings

In this section you can configure the anti-spam filtering policies for the Ad-Aware Security for Mail Servers.

You have the option to make changes to the **Default** rule or you can customize the rules created in the Rules section.

To enable the rule, select **Enabled**. If you want the rule to be disabled, clear the check box.

Select Senders Groups

You can select:

All

The rule applies to all senders, regardless of the group they belong to.

Selected

The rule applies only to senders from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Note
To learn how to configure a group, please refer to SMTP Groups.

Select Recipients Groups

You can select:

All

The rule applies to all recipients, regardless of the group they belong to.

Selected

The rule applies only to recipients from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all groups** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note
The addresses in the Cc and Bcc fields also count as recipients.

Note
To learn how to configure a group, please refer to SMTP Group.

Configuring Groups

To configure the group follow these steps:

- Add users to the new group. Provide the e-mail address in the corresponding field and click **Add**.
- Delete users in the group. To remove one or several items from the list, select them, click **Delete**.

Update Request

This policy template allows you to create policies for triggering a signature update for Ad-Aware Security for Mail Servers.

The template does not require other settings to be configured. You can configure update settings using the *Update Settings* template.

Update Settings

This policy template allows you to create policies for configuring the update settings for Ad-Aware Security for Mail Servers. You can configure automatic signature updates, product updates, update locations and notifications.

Here you can configure update settings that will be applied on the assigned clients.

The settings are organized into 4 sections:

- Options
- Product update options
- Update location
- Notifications

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Options

In this section you can configure the automatic update interval and enable update pushing.

Update Pushing is a feature that is available only when the product is registered. This feature allows customers to benefit from "Update Announcement Messages". These alerts are sent to the Update Pushing mailing list by the Ad-Aware Lab. The mailing list is composed of mail addresses that have been submitted by the customers on the Ad-Aware website. The "Update Announcement Messages" include special elements which trigger the update process when the message is scanned by the product. Therefore, it is mandatory that the mail address submitted by the customer is a mail address protected by Ad-Aware.

To enable Update Pushing, check Enable Update Pushing. If you do not want to use this service, clear the corresponding check box.

The automatic update feature allows updating Ad-Aware automatically, on a regular basis, without the administrator's intervention.

By default, Ad-Aware checks for updates at the specified update locations, every hour.

To change the frequency at which Ad-Aware checks for updates, type the number of hours between two consecutive checks for updates in the Automatic update interval text box.

To disable the automatic update, clear the check box corresponding to Automatic update interval.

Product Update Options

Installing product updates regularly is essential to the security of your server. Depending on the level of interference with the server, there are three types of product updates:

- Product updates that do not require stopping server traffic or to reboot the server
- Product updates that require stopping server traffic, but do not require to reboot the server
- Product updates that require to reboot the server

To configure automatic downloads and installation for each type of product update, select one of the following options:

- **Download updates and install automatically**

  Select this option and Ad-Aware will automatically download and install product updates. This is the recommended choice for product updates that do not require stopping server traffic or a server reboot.

- **Download updates automatically and install... at...**

  Select this option if you want Ad-Aware to install available updates at certain times. Select from the corresponding drop-down lists the date (day and time) when you want this to happen.

  This way you can configure Ad-Aware to perform product updates at times when it is least likely for interferences to occur with server activity (during night time, for example).

- **Download updates and let me decide when to install them**

Select this option if you want Ad-Aware to automatically download product updates, but let you decide when to install them. This is the recommended choice for product updates that require stopping server traffic or a server reboot.

To disable automatic product updates, select the **No automatic product updates** check box.

Note

Your server will be more vulnerable unless you install updates regularly.

Update Location

Ad-Aware can update from the local network, over the Internet, directly or through a proxy server.

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and a **Secondary update location**. Both require the configuration of the following options:

- **Update location** - type the address of the update server. By default, the primary update location is: upgrade.adaware.com.

  If multiple Ad-Aware products are installed in your network, you can setup a local server as the first update location for all the products and make upgrade.adaware.com the second location, to be used in case the first becomes unavailable. In this way you can reduce Internet traffic during updates.

- **Allow unsigned updates** - select this option to allow updates from a local server to be installed.
- **Use proxy** - select this option if the company uses a proxy server. The following settings must be specified:
  - **Server Name or IP** - type the IP of the proxy server.
  - **Port** - type the port Ad-Aware uses to connect to the proxy server.
  - **Username** - type a user name recognized by the proxy.
  - **Password** - type the valid password of the previously specified user.

Notifications

Ad-Aware can be configured to notify you about special events that occur during its operation.

Select the update events you want to be informed about:

- **Update performed** - when an update was performed.
- **No update available** - when no update is available.
- **Update failed** - when an error occurred during an update and the update failed.
- **Product update available** - when a product update is available.

You can customize the notifications of each update event using the *Alerts* section of the **General Settings** template.

Ad-Aware Security for File Servers Templates

The Ad-Aware Security for File Servers policy templates allows you to create policies that you can use in order to manage Ad-Aware Security for File Servers. By using these policies you can ensure your organization's file servers are secure.

Note

In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Security for File Servers:

Antivirus Settings

Allows creating antivirus policies for Ad-Aware Security for File Servers

General Settings

Allows creating general settings policies for Ad-Aware Security for File Servers

Get Settings

Allows creating policies for the retrieval of Ad-Aware Security for File Servers settings

Install product update

Allows creating policies for triggering the installation of a product update for Ad-Aware Security for File Servers

Rollback

Allows creating policies for rollback to the previous version of Ad-Aware Security for File Servers

Exceptions Settings

Allows creating scan exception policies for Ad-Aware Security for File Servers

Scanning Scheduled

Allows creating scheduled antivirus scan policies for Ad-Aware Security for File Servers

Update Request

Allows creating policies for triggering a signature update for Ad-Aware Security for File Servers

Update Settings

Allows creating policies for the configuration of both signature and product update settings for Ad-Aware Security for File Servers

Antivirus Settings

This policy template allows you to create on-access antimalware scan policies for Ad-Aware Security for File Servers.

Real-time protection keeps the file server safe from new viruses, spyware and riskware. It also prevents users from accessing or copying infected files and thus causing the infection to spread throughout the network.

Ad-Aware scans files as they are accessed or copied on the disk according to the current protection level settings. The actions to be taken on the infected and suspect files detected also depend on the current protection level.

When you select to edit or to create a new policy based on this template, the following pane will be displayed:

Here you can configure the real-time protection settings that will be applied on the assigned clients. The settings are organized into 4 sections:

- Protection
- Action
- Notifications
- Configure Scan

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Protection

This is where you can set the protection level by selecting a scanning profile. You can use one of the default profiles or create a custom profile.

Choose the protection level that best suits your security needs. There are 4 protection levels:

Protection level	Description
High	Offers high security. The resource consumption level is moderate. • All accessed files, regardless of their extension and size, are scanned. The boot sectors of the available drives are scanned as well. • Accessed files are scanned for all kinds of malware (viruses, Trojans, spyware, adware, riskware, dialers and so on). • Ad-Aware scans inside archives. • The default action taken on infected files is **Disinfect**. If disinfection fails, the files will be deleted. • The default action taken on suspect files is **Delete**.
Medium	Offers standard security. The resource consumption level is low. • Only the accessed files that do not exceed 10 megabytes (MB) are scanned. The boot sectors of the available drives are scanned as well. as well • Accessed files are scanned only for viruses, Trojans and spyware. • Ad-Aware does not scan inside archives. • The default action taken on infected files is **Disinfect**. If disinfection fails, access to such files is denied. • The default action taken on suspect files is **Deny access**.
Low	Covers basic security needs. The resource consumption level is very low. • Only the accessed application files that do not exceed 5 megabytes (MB) are scanned. • Accessed files are scanned only for viruses, adware and spyware. • Ad-Aware does not scan inside archives. • The default action taken on infected files is **Disinfect**. If disinfection fails,

	access to such files is denied. - The default action taken on suspect files is **Deny access**.
Custom	Allows customizing the real-time protection settings. You can configure these settings in the *Configure scan* section.

Setting the Scanning Instances

If you want to modify the number of scanning instances configured during installation, select the corresponding check box.

Type a new value in the edit field and click **OK** to save the changes.

Action

You can configure different actions for infected and suspect files. There is a list of actions for each type of detected files (infected or suspect). When an infected or suspect file is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

Click the desired action in order to move it up or down.

Actions for infected files. The following actions are available for infected files:

Action	Description
Disinfect	Remove the malware code from the requested infected files before delivery. Disinfection may fail in some cases, such as when the infected file is inside specific mail archives.
Deny	Deny users' access to the requested files if Ad-Aware detects them to be infected.
Move to Quarantine	Move infected files from their original location to the **Quarantine** folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove infected files from the disk, without any warning.

Actions for suspect files. The following actions are available for suspect files:

Action	Description
Deny	Deny users' access to the requested files if Ad-Aware detects them to be suspect.
Move to Quarantine	Move suspect files from their original location to the **Quarantine** folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove suspect files from the disk, without any warning.

Notifications

Ad-Aware can be configured to notify you when an **Infected/suspect** file has been detected.

To configure Ad-Aware only to log the occurrence of an event, or also to alert you or other person about it through mail or net send, go to *Alerts* section and configure the corresponding event.

Configure Scan

Each protection level allows configuring the actions to be taken on infected and suspect files for real-time protection.

In this section you can configure the real-time protection settings individually.

Note

These settings can be configured only if you have selected a Custom profile from the *Protection* section.

The scan settings Ad-Aware offers may help you fully adapt real-time protection to your company's regulations regarding workstation security. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve the system's responsiveness during a scan.

The following options are available:

Setting Scan Target

By default, Ad-Aware is set to scan accessed files regardless of their location on the file server. In this way, the entire file server is protected against viruses and spyware.

If you want only files from specific locations to be scanned on-access, follow these steps:

1. Select **Custom scan**.
2. In the edit box, type the full path to the files and folders to be scanned, separating each of them by enter, comma or semicolon.

Scanning Files by Extension

Some file types are more likely to carry viruses than others. For example, the risk of getting infected when executing an .exe file is much higher than when opening a .txt or a .gif file.

To specify the file types to be scanned, select one of the following options:

Option	Description
Scan all extensions	Accessed files are scanned regardless of their type.
Scan only application files	Only application files are scanned. For more information, please refer to

	Application Files. Viruses usually infect application files. Therefore, these file types should always be scanned on access.
Scan custom extensions	Only the files with the specified extensions are scanned. You must type in the edit field the file extensions to be scanned by Ad-Aware, separating them by semicolons (";").
Scan all except the following extensions	The files with the specified extensions are NOT scanned. You must type in the edit field the file extensions NOT to be scanned by Ad-Aware, separating them by semicolons (";"). You should not exclude from scanning file types commonly known to carry viruses, such as .exe, .doc, .ppt, .xls, .rtf, .pif, .bat and others.

Scanning Files by Size

Scanning large files requires additional system resources, which slows down the system and increases access times.

You can specify the maximum size (in kilobytes) of the files to be scanned in the **Maximum file size to be scanned** field. For example, if you type 2000, all files larger than 2000 KB will be excluded from scanning.

If you want Ad-Aware to scan accessed files regardless of their size, do one of the following:

- Clear the check box corresponding to **Maximum file size to be scanned**.
- Set the size limit to 0 KB.

Configuring Advanced Settings and Exceptions

You can configure the following advanced scanning settings:

Option	Description
Scan for spyware and other riskware	Scans accessed files not only for viruses, but also for known spyware and riskware threats. The riskware category contains adware, dialers and other applications that may be used for malicious purposes. If you do not want Ad-Aware to scan for dialers and specific riskware applications, select **Skip dialers and applications from scan**. Detected files will be treated as infected. The software that includes adware components might stop working if this option is enabled.
Scan boot	Scans the boot sectors of the available drives.
Scan packed files	Scan packed files.
Scan inside archives	Scan archived files. You can specify a maximum archive depth in order to scan files archived several times. If you want to scan files no matter how many times they were archived, set the maximum archive depth to 0. Selecting this option slows down the system and may increase access times.
Do not scan network shares	Ad-Aware will not scan the network shares on the file server, allowing for a faster network access.

	You should not select this option if the network computers are not protected by an antivirus solution.

To exclude files and folders only from on-access scanning:

1. Select **Enable scan exceptions**.
2. In the edit box, type the full path to the files and folders not to be scanned, separating each of them by enter, comma or semicolon.

   You can also specify whether the global exceptions defined in the **Exceptions** section should apply to real-time scanning.

General Settings

This policy template allows you to create policies for general settings of Ad-Aware Security for File Servers.

Here you can configure the Ad-Aware notification system, real time virus reporting, incident reporting, purge settings and the Quarantine settings. The settings are organized into 6 sections:

- Alerts
- Virus Report
- Report incidents
- Purge Settings
- Tray Icon
- Quarantine Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Alerts

In this section you can configure event notifications, mail alert templates and settings and net send alert templates.

- Events - this is a list of the events that may occur:

Event	Description
Ad-Aware Error	Groups all the errors that may appear during product operation, such as service start failure.
Update Error	Refers to the occurrence of an error during the update process.
Infected/suspect file detected	Occurs when an infected file or a file suspected of being infected has been detected.
Ad-Aware Warning	Group’s critical information regarding the activity of Ad-Aware.
File not scanned	Occurs when a file could not be scanned by Ad-Aware.
Product update	Occurs when a product update is available.
Ad-Aware information	Groups information regarding the activity of Ad-Aware.
Key expired	Indicates the expiration of the registration period.

Key will expire	Indicates that there are 3 days left before the product expires.
On-demand scanning	Occurs whenever an on-demand scan is performed.
Update information	Contains information about the update process.

There are 3 types of events, depending on their importance to the security of the system:

- **Information** - such events provide information about the product activity.
- **Warning** - such events provide critical information about aspects of the product activity which require your attention.
- **Error** - such events provide information about errors that appear during product operation.

Set the importance of the events by selecting one of the following levels from the drop-down lists corresponding to each event:

- **Low** - a record of the event is kept in the log file. No alert is sent when the event takes place.
- **Medium** - log the event and send mail alerts when the event takes place.
- **High** - log the event and send both mail and net send alerts when the event takes place.

Note

To completely disable notifications for an event, select Disabled from its corresponding drop-down list.

- **Mail Alert Templates** - if the importance of the event is medium or high, mail alerts will be sent.

Each event comes with a default alert text. To view the alert text of an event, click **Edit** next to that event. To change the text, edit the contents of the text box.

Important

You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

- **Net Send Alert Templates** - if the importance of the event is high, net send alerts will be sent.

Each event comes with a default alert text. To view the alert text of an event, click **Edit** next to that event. To change the text, edit the contents of the text box.

Important

You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

- **Mail alerts** - to use the mail notification service, follow these steps:
  1. Select **Enable Mail Notification** to activate the mail notification service
  2. Configure the SMTP settings:
  - **SMTP Server** - enter the IP address of the SMTP server that your network uses to send messages.
  - **From** - enter the e-mail address that will appear in the sender field.

Important

Provide a valid e-mail address for the SMTP server, otherwise the server may decline to send an e-mail whose sender (e-mail address) is unknown to it.

3. If the SMTP server used to send messages requires authentication, select **Use SMTP Server Authentication** and enter the user name and password in the corresponding fields.

   Note

   NTLM authentication is not supported.

4. Indicate the recipients of the mail alerts by entering their e-mail addresses one by one in the text box located under the **Recipients** list box and clicking **Add**. To remove e-mail addresses from the list, select them and click **Delete**.

   Note

   The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set.

- **Net send alerts** - to use the mail notification service, follow these steps:

1. Select **Enable Net Send Alerts** to activate the net send notification service.
2. Indicate the recipients of the net send alerts by entering their computer names one by one in the text box located under the **Recipients** list box and clicking **Add**. To remove computer names from the list, select them and click **Delete**.

   Note

   The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set.

Virus Report

In this section you can configure real time virus reporting.

Real time virus reporting (RTVR) allows sending reports about the viruses found on your server to the Ad-Aware Lab in order to help us identify new viruses and find quick remedies for them. Your contribution could be essential for developing new tools to protect you and other users against virus threats.

Real time virus reporting is disabled by default. To activate it, select **Enable real time virus reports**.

The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.

Report Incidents

In this section you can configure the incident management module that allows creating incident reports during crashes of Ad-Aware Security for File Servers.

By agreeing to send the incident reports to the Ad-Aware Lab, you agree to help us find quick fixes for our bugs. You could make a major contribution to the development of a stable product that satisfies your needs.

By default, the reports created automatically during product crashes are not sent to the Ad-Aware Lab. To configure Ad-Aware to send incident reports to the Ad-Aware Lab, select **I agree to submit incident reports to the Ad-Aware Lab** and enter your e-mail address in the provided text box.

The reports will only be used for debugging purposes. They will never be used as commercial data or disclosed to third parties.

Purge Settings

In this section you can configure the period of time for which Ad-Aware Security for File Servers will store the following data:

- Quarantine (quarantined files)
- Statistics
- Reports
- View Logs

By default, data older than 30 days is automatically deleted.

You can set a different time period for each type of data by entering the number of days / weeks / months in the text boxes corresponding to the types of data you wish to edit.

Tray Icon

After the product installation is over (including computer restarting) an icon will appear in the system tray.

In this section, you can set the tray icon for Ad-Aware Security for File Servers to appear for the local users and for the users connecting through the Remote Desktop.

Quarantine Settings

This policy template allows you to manage the quarantined files from the Quarantine folder in Ad-Aware Security for File Servers:

You can change the folder the quarantine is located in. In order to operate this change, provide the new path in the edit field. The default location of the quarantine folder is: `C:\Program Files\ Ad-Aware \ Ad-Aware for Windows Servers Services\Quarantine.`

You can also set a time period for Ad-Aware to rescan the items in the Quarantine folder.

When the scan is over you can perform the following actions:

- Automatically restore files at original locations
- Repair files in quarantine without restoring

Get Settings

This policy template allows creating policies for retrieving the settings of Ad-Aware Security for File Servers.

No additional settings are required.

Install Product Update

This policy template allows you to create policies for triggering the installation of a product update for Ad-Aware Security for File Servers.

The product updates are different from the signature updates. Their function is to deliver bug fixes and new features to the product.

There are two types of updates for the product:

- **Product updates (patches)** - these are files that bring improvements to the current product; they are usually smaller size updates that do not require a new version of the product to be delivered.
- **Version updates** - these are installation packages of a new released version of the product.

The settings are in the Settings section.

Click ❯ to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Settings

Here you can choose whether or not to allow the installation of the product update if it involves stopping / starting server traffic or rebooting the server.

To agree with the installation in one of the two cases, select the corresponding check box. Otherwise, make sure the check box is cleared.

Rollback Product Update

This policy template allows creating policies for rolling back to the previous version of Ad-Aware Security for File Servers. The rollback feature gives you the option to revert to the previous product version once you have installed a product update.

If a rollback is available, the current product version and the version you can roll back to will be displayed. The rollback does not require other settings to be configured.

After a rollback is performed, the version currently in use and the previous version will be displayed. You can use the provided link to update back to the newer version.

Scan Exceptions Settings

According to the Microsoft recommendations, the Ad-Aware Security for File Servers automatically excludes from scanning a number of files, folders and processes belonging to or used by the Microsoft server products:

- Microsoft Exchange 2007 / 2003 / 2000 / 5.5
- Microsoft ISA Server 2006 / 2004 / 2000
- Microsoft SharePoint 2003

Similarly, Ad-Aware Security for File Servers does not scan specific locations and processes related to the Ad-Aware Security for Windows Servers products in order to avoid interfering with their operation and to improve their performance.

You can manually exclude from scanning other files, folders and processes. For example, you can exclude a backup process in order to avoid interference and to speed it up. You can also remove current exclusions at your choice.

Global Exceptions

To manage the files and folders excluded from both real-time and on-demand scanning, select the Enable scan exceptions check box.

The files and folders excluded from both real-time and on-demand scanning can be added manually in the box.

To exclude files and folders from scanning, do any of the following:

- In the edit box, type the full path to the files and folders not to be scanned, separating each of them by enter, comma or semicolon.
- You can also copy the locations from the text file and paste them in the edit box.

Process Exclusions

To manage the processes excluded from real-time scanning, click **Global Process Exclusions**.

To exclude a specific process from real-time scanning, follow these steps:

1. In the edit box, type the full path to the process or processes not to be scanned.

Click **Add**.

If you no longer want to exclude an application from real-time scanning, select it and click **Delete**.

Scanning Scheduled

This policy template allows you to create on-demand antimalware scan policies for Ad-Aware Security for File Servers.

On-demand scanning provides an additional protection layer for the file server. You should periodically scan the file server to make sure it is free from malware threats (viruses, spyware or rootkits). It is recommended to perform a comprehensive system scan every week.

Here you can configure the antimalware scan settings that will be used to scan the assigned clients. The settings are organized into 4 sections:

- Scan Level
- Options
- Action
- Notifications

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Scan Level

You can use one of the following scan modes:

Scan Mode	Description
Quick System Scan	Allows quickly scanning the `Program Files` and `Windows` folders using a pre-defined configuration of the scan settings. Please note that only the application files that do not exceed 10 megabytes (MB) are scanned. By default, Ad-Aware is configured to take the following actions: • **Disinfect** infected files. If disinfection fails, the files will be deleted. • **Delete** suspect files. • **Ignore** rootkits (hidden objects).
Deep System Scan	Allows performing a comprehensive scan of the entire file server. The pre-defined scan settings offer the highest detection efficiency. By default, Ad-Aware is configured to take the following actions: • **Disinfect** infected files. If disinfection fails, the files will be deleted. • **Delete** suspect files. • **Ignore** rootkits (hidden objects).
Custom Scan	Allows scanning specific locations on the file server using a custom configuration of the scan settings. To configure these settings, click *Options*.

Options

In this section you can configure the scan target and the scan settings of an on-demand scan.

In order to configure the scan settings, choose Custom Scan from the Scan Level area.

Note

The scan settings can be configured only for the custom scan mode.

Excluding Specific Malware from Scanning

You can configure Ad-Aware to scan the accessed files not only for viruses, but also for known spyware and riskware threats:

- adware
- spyware
- applications
- dialers
- rootkits

To this purpose, keep selected the check boxes corresponding to the specific malware threats you want to scan for.

Important

All malware detected (except for rootkits) is treated as infected.

Scanning Files by Extension

Some file types are more likely to carry viruses than others. For example, the risk of getting infected when executing an .exe file is much higher than when opening a .txt or a .gif file.

To specify the file types to be scanned, select one of the following options:

Option	Description
Scan all exceptions	All files are scanned regardless of their type.
Scan only application files	Only application files are scanned. For more information, please refer to Application Files. Viruses usually infect application files. Therefore, these file types should always be scanned.
Scan custom extensions	Only the files with the specified extensions are scanned. You must type in the edit field the file extensions to be scanned by Ad-Aware, separating them by semicolons (";").
Scan all except the following extension	The files with the specified extensions are NOT scanned. You must type in the edit field the file extensions NOT to be scanned by Ad-Aware, separating them by semicolons (";"). You should not exclude from scanning file types commonly known to carry viruses, such as .exe, .doc, .ppt, .xls, .rtf, .pif, .bat and others.

Scanning Files by Size

Scanning large files requires additional system resources, which slows down the system and increases access times.

You can specify the maximum size (in kilobytes) of the files to be scanned by selecting the check box **Do not scan files larger than**. For example, if you type 2000, all files larger than 2000 KB will be excluded from scanning.

If you want Ad-Aware to scan the files in the scan target regardless of their size, follow these steps:

- Select the check box corresponding to **Do not scan files larger than.**
- Set the size limit to 0 KB.

Configuring Advanced Scan Settings

To configure more advanced scanning settings to on-demand scanning, click Advanced scan settings.

You can configure the following advanced scanning settings:

Option	Description
Scan boot sectors	Scan all boot sectors of the available drives.
Scan memory	Scan all system's memory.
Scan registry	Scan Windows registry.
Scan cookies	Scan cookie file.
Open packed programs	Scan packed files.
Open archives	Scan archived files. You can specify a maximum archive depth in order to scan files archived several times. If you want to scan files no matter how many times they were archived, set the maximum archive depth to 0. Selecting this option slows down the system and may increase scanning time.

Setting Scan Target

To specify the items (drives, files, folders) to be scanned, do any of the following:

- In the edit box, type the full path to the items to be scanned, separating each of them by enter, comma or semicolon.
- You can also copy the locations from the text file and paste them in the edit box.

To exclude files and folders only from on-demand scanning:

1. Select **Except from scan**.
2. In the edit box, type the full path to the files and folders not to be scanned, separating each of them by enter, comma or semicolon. You can also copy the locations from the text file and paste them in the edit box.

Action

This is where you can configure the actions to be taken on the infected, suspect and hidden files detected by Ad-Aware.

You can configure different actions for each type of detected file: infected, suspect or rootkit. Select the actions to be taken on the detected files from the corresponding menus.

Note

You can configure two actions for infected and suspect files. The second action is enabled only in case the first action fails.

Actions for infected files, the following actions are available for infected files:

Action	Description
Disinfect	Remove the malware code from the infected files detected. Disinfection may fail in some cases, such as when the infected file is inside specific mail archives.
Move to Quarantine	Move infected files from their original location to the **Quarantine** folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove infected files from the disk, without any warning.
Ignore	Just log the infected files detected in the scan report.

Actions for suspect files. The following actions are available for suspect files:

Action	Description
Move to Quarantine	Move infected files from their original location to the **Quarantine** folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Delete	Immediately remove suspect files from the disk, without any warning.
Ignore	Just log the suspect files detected in the scan report.

Actions for rootkits (hidden objects). The following actions are available for rootkits:

Action	Description
Disinfect	Remove the malware code from the infected files detected.
Ignore	Just log the rootkits detected in the scan report.

Notifications

Ad-Aware can be configured to notify you about special events that occur during its operation. This tab allows you to configure the notification options for on-demand scanning.

Select Log start/end of on-demand scanning to record the start and the end of the scan in the Ad-Aware log.

A detailed scan report is created every time you perform an on-demand scan. The report is generated in XML format and it can be viewed using a browser. By default, the on-demand scan reports are saved in `?:\Program Files\Ad-Aware\Ad-AwareManagementServer\Reports\`.

Update Request

This policy template allows you to create policies for triggering a signature update for Ad-Aware Security for File Servers.

The template does not require other settings to be configured. You can configure update settings using the *Update Settings* template.

Update Settings

This policy template allows you to create policies for configuring the update settings for Ad-Aware Security for File Servers. You can configure automatic signature updates, product updates, update locations and notifications.

Here you can configure update settings that will be applied on the assigned clients.

The settings are organized into 4 sections:

- Options
- Product update options
- Update location
- Notifications

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Options

In this section you can configure the automatic signature updates. The automatic update feature allows updating Ad-Aware automatically, on a regular basis, without the administrator's intervention.

By default, Ad-Aware checks for updates at the specified update locations, every hour.

To change the frequency at which Ad-Aware checks for updates, type the number of hours between two consecutive checks for updates in the **Automatic update interval** text box.

To disable the automatic update, clear the check box corresponding to **Automatic update interval**.

Product Update Options

Installing product updates regularly is essential to the security of your server. Depending on the level of interference with the server, there are three types of product updates:

- product updates that do not require stopping server traffic or to reboot the server
- product updates that require stopping server traffic, but do not require to reboot the server
- product updates that require to reboot the server

To configure automatic downloads and installation for each type of product update, select one of the following options:

- **Download updates and install automatically**

  Select this option and Ad-Aware will automatically download and install product updates. This is the recommended choice for product updates that do not require stopping server traffic or a server reboot.

- **Download updates automatically and install... at**...

  Select this option if you want Ad-Aware to install available updates at certain times. Select from the corresponding drop-down lists the date (day and time) when you want this to happen.

  This way you can configure Ad-Aware to perform product updates at times when it is least likely for interferences to occur with server activity (during night time, for example).

- **Download updates and let me decide when to install them**

  Select this option if you want Ad-Aware to automatically download product updates, but let you decide when to install them. This is the recommended choice for product updates that require stopping server traffic or a server reboot.

To disable automatic product updates, select the **No automatic product updates** check box.

Note

Your server will be more vulnerable unless you install updates regularly.

Update Location

Ad-Aware can update from the local network, over the Internet, directly or through a proxy server.

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and a **Secondary update location**. Both require the configuration of the following options:

- **Update location** - type the address of the update server. By default, the primary update location is: upgrade.bitdefender.com.

If multiple Ad-Aware products are installed in your network, you can setup a local server as the first update location for all the products and make upgrade.bitdefender.com the second location, to be used in case the first becomes unavailable. In this way you can reduce Internet traffic during updates.

- **Allow unsigned updates** - select this option to allow updates from a local server to be installed.
- **Use proxy** - select this option if the company uses a proxy server. The following settings must be specified:
  - **Server Name or IP** - type the IP of the proxy server.

- **Port** - type the port Ad-Aware uses to connect to the proxy server.
- **Username** - type a user name recognized by the proxy.
- **Password** - type the valid password of the previously specified user.

Notifications

Ad-Aware can be configured to notify you about special events that occur during its operation.

Select the update events you want to be informed about:

- **Update performed** - when an update was performed.
- **No update available** - when no update is available.
- **Update failed** - when an error occurred during an update and the update failed.
- **Product update available** - when a product update is available.

You can customize the notifications of each update event using the *Alerts* section of the **General Settings** template.

Ad-Aware Security for Exchange Templates

The Ad-Aware Security for Exchange policy templates allows you to create policies that you can use in order to manage Ad-Aware Security for Exchange. By using these policies you can ensure your organization's Exchange servers are secure.

Note

In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Security for Exchange:

Anti-spam Filtering Settings/Rules

Allows creating policies to configure the anti-spam settings and rules for Ad-Aware Security for Exchange

Antivirus Rules

Allows creating antivirus rules policies for Ad-Aware Security for Exchange

Antivirus Settings

Allows creating antivirus settings policies for Ad-Aware Security for Exchange

Attachment Filtering

Allows creating policies to configure the attachment filtering settings and rules for Ad-Aware Security for Exchange

Content Filtering

Allows creating policies to configure the content filtering settings and rules for Ad-Aware Security for Exchange

General Settings

Allows creating general settings policies for Ad-Aware Security for Exchange

Get Settings

Allows creating policies for the retrieval of Ad-Aware Security for Exchange settings

Install Product Update

Allows creating policies for triggering the installation of a product update for Ad-Aware Security for Exchange

Rollback Product Update

Allows creating policies for rollback to the previous version of Ad-Aware Security for Exchange

Scanning Scheduled

Allows creating scheduled antivirus scan policies for Ad-Aware Security for Exchange

SMTP Groups

Allows creating policies to manage SMTP groups for Ad-Aware Security for Exchange

Update Request

Allows creating policies for triggering a signature update for Ad-Aware Security for Exchange

Update Settings

Allows creating policies for the configuration of both signature and product update settings for Ad-Aware Security for Exchange

Anti-spam Filtering Settings/Rules

This policy template allows you to create policies for the Anti-spam module of Ad-Aware Security for Exchange. The Anti-spam module offers protection against spam, phishing and other attacks. It uses a combination of various filters and engines to determine whether messages are spam or not and to check them for patterns of spam.

Based on the groups the sender and the recipients belong to, you can specify various actions to be taken on the spam messages.

The settings are organized into 3 sections:

- Anti-spam - Allows you to enable the anti-spam filtering and to configure the global anti-spam filters.
- Rules - Allows you to manage the rules (create, edit or delete a rule).
- Rule settings - Allows you to configure the filtering options for the selected rules.

Anti-spam

This is where you can enable anti-spam filtering and configure the global anti-spam filters.

If you want the anti-spam protection to be enabled, select **Enable anti-spam filtering Otherwise**, clear this check box.

You have an option to integrate the Anti-spam module of Ad-Aware Management Server with the Microsoft Exchange Server's Content Filtering. By selecting this option, the Ad-Aware SPAM score computed for a specific message is converted to the Content Filtering's spam confidence level (SCL) and an appropriate mail header is added to the message. In this way, the Ad-Aware Anti-spam analysis is taken into account when applying the actions configured on the Exchange server for Content Filtering.

Global Filters

Several global anti-spam filters can be configured to filter all of the incoming mail traffic, in order to reduce the traffic on the server. These filters are used before a specific group filtering policy is applied.

- **Enable Allow/ Deny IP List**

Select **Enable Allow / Deny IP List** if you want to use the Allow / Deny IP List to filter the incoming mail traffic.

All incoming connections from addresses that appear on the Deny IP List are dropped.

The Allow IP List is used to except IP addresses from ranges of IP addresses defined on the Deny IP List.

Note

If you want to configure the IP addresses list, you need to access the Ad-Aware Security for Exchange product interface.

- **Enable Sender Black List**

Select **Enable Sender Black List** if you want to use the Sender Black List to filter incoming mail traffic.

The Sender Black List allows the administrator to specify a list of e-mail addresses which are denied access to the server. The incoming mail from these addresses will be dropped before reaching the server.

Note

If you want to configure the Sender Black List, you need to access the Ad-Aware Security for Exchange product interface.

- **Enable IP Match**

Spammers often try to "spoof" the sender's e-mail address to make the e-mail appear as being sent by someone in your domain. To prevent this, you can use IP Match.

If an e-mail appears to be from a domain that you have specified in the IP Match rule list (such as your own company domain), Ad-Aware checks to see if the IP address of the sender matches the IP addresses provided for the specified domain.

Note

If you want to configure the IP Match rule list, you need to access the Ad-Aware Security for Exchange product interface.

If the domain address of the sender matches the IP address, the message bypasses anti-spam filtering. Otherwise, the connection is dropped.

- **Allow breaking of the DKIM/domain key signature when modifying the e-mails**

Ad-Aware breaks DKIM signatures if filtering rules include actions such as modifying the e-mail subject or adding footers to e-mails. To allow breaking DKIM signatures, select the corresponding check box.

Rules

This is where you can specify the anti-spam filtering options. You can modify the default rule to specify the anti-spam filtering options for all of the mail traffic, or you can configure new rules in order to create customized group filtering policies.

Default Rule. There is one rule created by default that manages the anti-spam filtering settings for all groups. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Adding New Rules. To set different filtering policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following options:

- **Create rule** - to create a new anti-spam rule and configure the anti-spam filters you need to follow these 3 steps:
  1. Go to the Anti-spam section and select **I want to make changes to the anti-spam filtering rules**.
  2. Select **Other** from the **Rules** section and choose a name.
  3. Configure the anti-spam filtering policies in the **Rule settings** section.
- **Edit rule** - allows you to configure the selected rule. To configure the rule, please refer to Rule Settings.
- **Delete rule** - deletes one / several selected rules. You will have to confirm your choice by clicking **Yes**.

Rule Settings

In this section you can configure the anti-spam filtering policies for the Ad-Aware Security for Exchange.

You have the option to make changes to the **Default** rule or you can customize the rules created in the *Rules* section.

To enable the rule, select **Enabled** and choose if the rule should apply to the incoming or the outgoing e-mail.

Select Senders Groups

You can select:

All

The rule applies to all senders, regardless of the group they belong to.

Selected

The rule applies only to senders from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Note

To learn how to configure a group, please refer to SMTP Groups.

Select Recipients Groups

You can select:

All

The rule applies to all recipients, regardless of the group they belong to.

Selected

The rule applies only to recipients from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all groups** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note

The addresses in the Cc and Bcc fields also count as recipients.

Note

To learn how to configure a group, please refer to SMTP Groups.

Actions

In this area you can specify the actions to be taken on the messages matching this policy. If you do not want the messages to be scanned using the anti-spam filters, select **Do not scan.**

If you select **Scan**, the messages will be scanned using the anti-spam filters and the anti-spam options configured for this policy. Next, you must configure the threshold level and the actions to be taken on the spam messages.

Specify Threshold Level

Ad-Aware checks all the message components (i.e. not only the header but also the message body in either HTML or text format) against many rules using several filters. Some of the filters, like the URL Filter can indicate if the message is spam directly.

The anti-spam filters give to each scanned message a Spam score. The aggregate of these scores represents an overall spam score. The overall spam score is measured against the desired level of spam sensitivity (threshold), and a decision is made. If the spam score for a message exceeds the threshold, the message is considered spam. Otherwise, the message is not spam and it is delivered in full to its recipients.

Note

Exceptions are made if the sender is in the *IPMatch* table (as not spam) or on the White list.

Specify a threshold value between 0 and 1000 in the corresponding field. The default value is 775.

If you do not want to set a threshold value, select **Let Ad-Aware anti-spam engines determine the mail spam status** to let the Ad-Aware Anti-spam Engine to decide whether a message is spam or not.

Set Actions

Choose from the menu one of the following actions to be taken on the spam messages:

Action	Description
Deliver e-mail	The spam message is delivered in full to its recipients.
Quarantine	The spam message is moved to the quarantine folder.
Redirect e-mail to address	The spam message is redirected to a specified e-mail address. You must specify the e-mail address where the spam messages are to be delivered in the field next to the menu. If you want to provide more than one address, separate them by a semi-colon ";". If the field is empty or the e-mail address is invalid the messages will not be redirected.
Reject e-mail	The spam message is rejected with a 550 SMTP error code.
Delete e-mail	The spam message is deleted.

By default, when a message matches the conditions of a rule, it is no longer checked against any other rules. If you want Ad-Aware to continue processing rules, clear the check box **If the rule conditions are matched, stop processing more rules.**

In order to help you process spam messages, several additional actions are available:

Action	Description
Modify the subject of the mails detected as	The subject of the messages detected as spam is modified. You can modify the subject pattern. We recommend you to use one

spam	of these patterns: • `[SPAM]${subject}[SPAM]` - to add `[SPAM]` before and after the subject. This is the default subject pattern. • `[SPAM]` - to replace the subject with `[SPAM]`. • `[$score% SPAM]$subject` - to add `[x SPAM]` before the subject, where x represents the spam score.
Add a header to the e-mails detected as spam	An e-mail header is added to the messages detected as spam. You can modify the header name and the spam and non-spam values. By default, the spam and non-spam values are `${status} (${score})`. This means that for a spam message the header will be Name: `Yes(x)`, while for a legitimate message the header will be Name: `No(x)`, where x represents the spam score received by the message.
Save email to folder	The spam message is saved to a specified folder. To specify the folder, select the check box and type the full path to the folder location.
Archive to account (enter e-mail archive address)	The spam message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Anti-spam Filters

This is where you can specify which anti-spam filters to be enabled.

The following options are available:

- **Multi Filter** - is enabled by default.

  This filter has several components:

  - **Asian** - enables / disables the filter that blocks mail written in Asian characters.
  - **Cyrillic** - enables / disables the filter that blocks mail written in Cyrillic characters.
  - **Block sexually explicit content** - enables / disables the filter that blocks messages tagged Sexually-Explicit in the subject.
- **Enable URL Filter** - enables / disables the URL Filter.
- **Enable RBL Filter** - enables / disables the global RBL Filter.
- **Enable Neunet (TM) Filter** - enables / disables the Neunet Filter.
- **Allow queries to Ad-Aware servers** - enable / disable queries to the Ad-Aware cloud.

Note

To enable / disable a filter select / clear the corresponding check box.

Configure White List / Black List

Most people communicate regularly with a group of people or even receive messages from companies or organizations in the same domain. By using the White List / Black List filter, the administrator can set a list of trusted and untrusted addresses from which to respectively "always accept" or "always reject" e-mail messages.

White List

The White List contains e-mail addresses expected to send legitimate messages. Any mail coming from an address contained in the **White List** will be considered legitimate and will bypass further anti-spam filters.

> **Note**
>
> We recommend that you add the trusted addresses to the White List. Ad-Aware does not block messages coming from the addresses on the list; therefore, adding them helps ensure that legitimate messages get through.

Black List

The Black List contains e-mail addresses expected to send spam messages. Any mail coming from an address contained in the **Black List** will be considered spam and the appropriate action will be taken.

Antivirus Rules

This policy template allows you to create policies for the Antivirus module of Ad-Aware Security for Exchange. The Antivirus module offers protection against viruses, spyware and riskware. It detects infected or suspect messages and attempts to disinfect them or isolates the infection, according to the specified actions.

Based on the groups the sender and the recipients belong to, you can specify various actions to be taken on the infected or suspect messages.

The settings are organized into 3 sections:

- Antivirus - Allows you to enable the antivirus filtering.
- Rules - Allows you to manage the rules (create, edit or delete a rule).
- Rule settings - Allows you to configure the filtering options for the selected rules.

Antivirus

This is where you can enable real-time protection and configure advanced antivirus settings.

If you want the real-time antivirus protection to be enabled, select **Enable** antivirus filtering. Otherwise, clear the check box.

Scanning Instances

Based on the system configuration and on the number of Ad-Aware products you have chosen to install, Ad-Aware computes an optimal number of scanning instances. Though not recommended, you may change this value for systems with powerful multicore CPUs to speed up scanning from the corresponding check box.

Rules

This is where you can specify the antivirus filtering rules. You can modify the default rules to specify the antivirus filtering options for the infected or suspect messages, or you can configure new rules in order to create customized group filtering policies.

Default Rules. There are two default rules you can select in order to manage the global real-time antivirus scanning settings:

- **Default SMTP** - this default rule applies to SMTP scanning.
- **Default VSAPI** - this default rule applies to VSAPI scanning.

You cannot copy, delete or disable the default rule. This rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Adding New Rules. To set different filtering policies for the SMTP scanning, add new rules. This way you can create customized SMTP filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following options:

- **Create rule** - to create a new rule for the SMTP scanning and configure the antivirus filters you need to follow these 3 steps:
  1. Go to the **Antivirus** section and select **I want to make changes to the antivirus filtering rules**.
  2. Select **Other** from the **Rules** section and choose a name.
  3. Configure the antivirus filtering policies in the **Rule settings** section.
- **Edit rule** - allows you to configure the selected rule. To configure the rule, please refer to Rule Settings.
- **Delete rule** - deletes one / several selected rules. You will have to confirm your choice by clicking **Yes**.

Rule Settings

In this section you can configure the antivirus filtering policies for Ad-Aware Security for Exchange.

You have the option to make changes to the **Default** rule or you can customize the rules created in the *Rules* section.

To enable the rule, select **Enabled** and choose if the rule should apply to the incoming or the outgoing e-mail.

Select Senders Groups

You can select:

All

The rule applies to all senders, regardless of the group they belong to.

Selected

The rule applies only to senders from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Note

To learn how to configure a group, please refer to SMTP Groups.

Select Recipients Groups

You can select:

All

The rule applies to all recipients, regardless of the group they belong to.

Selected

The rule applies only to recipients from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all groups** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note

The addresses in the **Cc** and **Bcc** fields also count as recipients.

Note

To learn how to configure a group, please refer to SMTP Groups.

Scan Options

If you do not want the messages to be scanned for malware, select **Do not scan**.

If you select **Scan**, the messages will be scanned for malware using the settings configured for this policy. You can specify:

- **Antivirus extensions to be scanned** - select one of the following options in order to scan messages depending on their extension.

Option	Description
Scan all extensions	All mail attachments are scanned, regardless of their extension.

Scan only application extensions	Only the attachments containing applications are scanned. For more information, please refer to Application Files.
Scan all except specific extensions	Only the attachments having the specified extensions are scanned. Provide the specific extensions in the edit field. These extensions must be separated by ";".
Scan all except specific extensions	All attachments except those having the specified extensions are scanned. Provide all extensions that you do not want to scan in the edit field. These extensions must be separated by ";".

- **Maximum e-mail body / Antivirus size to be scanned** - select this option if you want to specify a size limit for the mail body or for the attachments to be scanned. Provide the size limit in the edit field.

Actions

Choose from the menu one of the following actions to be taken on infected and suspect objects:

Different actions can be configured for the infected and suspect objects detected by Ad-Aware. There is a list of actions that can be applied to each category of detected objects (infected or suspect). When such an object is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

The antivirus actions are ordered in a list according to their priority. Click the desired action in order to move it up or down.

Actions for infected objects, the following actions are available for infected objects:

Action	Description
Disinfect	Removes the malware code from the infected message.
Replace object	The infected object (mail body / attachment) is replaced with an explanatory text.
Delete object	The infected object (mail body / attachment) is deleted.
Reject e-mail	The infected message is rejected. In this case, the message does not reach the recipient mail server and the sending mail server is informed that the message was not delivered. The sending mail server may then try to send the message again (most likely) or it will notify the sender that the message could not be delivered.
Move to Quarantine	The infected object (mail body / attachment) is moved to the quarantine folder.
Ignore	The infected message is delivered in full to its recipients.

Actions for suspect objects, the following actions are available for suspect objects:

Action	Description
Replace object	The suspect object (mail body / attachment) is replaced with an explanatory

	text.
Delete object	The suspect object (mail body / attachment) is deleted.
Reject e-mail	The suspect message is rejected.
Move to Quarantine	The suspect object (mail body / attachment) is moved to the quarantine folder.
Ignore	The suspect message is delivered in full to its recipients.

By default, when a message matches the conditions of a rule, it is no longer checked against any other rules. If you want Ad-Aware to continue processing rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

Objects that are replaced and moved to quarantine are replaced with an explanatory text.

To edit the text to be delivered instead of such objects, follow these steps:

- Select **Infected file replaced** and type in the edit box the text to be delivered instead of the infected or suspect objects deleted.
- Select **Infected file quarantined** and type in the edit box the text to be delivered instead of the infected or suspect objects moved to quarantine.

Notifications

In the **Notifications** area you can specify whether to issue notifications or not when infected messages are detected or files cannot be scanned.

Select the events for which to issue notifications:

- **Infected file detected** - when an infected file was detected.
- **File not scanned** - when a file could not be scanned.

Note

The corresponding event in the Alerts section must be enabled and properly configured.

Select **Alert e-mail sender** and **Alert e-mail recipients** to send e-mail alerts to the sender and, respectively, the recipients of infected messages. The e-mail notification service must be enabled in the Alerts section.

Antivirus Settings

This policy template allows you to create policies for the real-time protection and configure advanced antivirus settings.

If you want the real-time antivirus protection to be enabled, select **Enable antivirus real-time scanning**. Otherwise, clear the check box.

Several advanced settings concerning the scanning process can be configured.

- **Number of scanning threads** - type in the corresponding field the maximum number of scanning threads to be used. The recommended number can be computed in this way: 2*number of CPU+1.
- **Maximum archive depth to scan** - type in the corresponding field the maximum archive depth to scan. The default archive depth scanned is 16.

Archives can contain other archives. It is possible to find files with multiple archive levels. If there are too many such levels, the scanning process can take longer, affecting the performance of the server. It is advisable to set a maximum level up to which the archives are to be scanned.

- Based on the system configuration and on the number of Ad-Aware products you have chosen to install, Ad-Aware computes an optimal number of scanning instances. Though not recommended, you may change this value for systems with powerful multicore CPUs to speed up scanning.

Mailbox (VSAPI) Scanning

Select the **Enable Mailbox (VSAPI) scanning** check box to enable VSAPI based antivirus scanning. The antivirus scanning at VSAPI level can be done through three additional scanning methods, intended to optimize the overall scanning process: background, proactive and transport scanning.

- **Enable proactive scanning** - select this option if you want proactive scanning to be enabled.

Proactive scanning means that when a message is submitted to the information store, either via a client or a transport agent, it is placed in the global scanning queue with a low priority. If and when threads are available in the thread pool and no high priority item remains to be scanned, each item with the low priority is submitted for scanning. Therefore, enabling this scan method optimizes the overall scanning process.

If an item is on the low priority list and a client attempts to access the message, the item will be marked as high priority. Also, it will be removed from the low priority list and another low priority item will take its place.

Note

We recommend you to keep this setting enabled as it prevents the overloading of the scanning engine.

- **Enable background scanning** - to enable background scanning.

The purpose of background scanning is to scan all messages stored in the Exchange databases (mailboxes and public folders). When an object having been checked through background scanning is requested, it will not be scanned again unless a virus signature update has been performed in the meantime.

Although background scanning is performed at low priority, the process takes up system resources because databases are re-scanned after each update and updates are performed often.

The following options are available:

Option	Description
Scan only un-scanned e-mails	E-mails that already have a scan stamp will not be scanned again.
Scan all e-mails (even if they have a scan stamp)	All e-mails scanned.
Don’t update scan stamp	E-mails are scanned but their scan stamp is not updated.
Scan only e-mails with attachments	Only e-mails with attachments will be scanned.
Scan e-mails arrived between	Scan only e-mails that arrived in a time interval specified by you.

Note

By default background scanning is disabled. You should enable it only as a second layer of protection when you want to check all your databases and make sure they are clean.

- **Scan RTF** - select this option if you want the body messages in Rich Text Format (RTF) to be scanned.
- **Enable transport scanning** - select this option if you want transport scanning to be enabled.

Note
Transport scanning is available only on MS Exchange Server 2003!

Transport scanning means that messages are scanned at the transport level. This prevents infected messages from entering the Exchange mailboxes.

The messages entering the Exchange store are intercepted by the VSAPI interface and scanned by Ad-Aware. After being scanned, the messages are submitted again to the transport engine which will deliver them to their destination. Any message scanned at the gateway will be rescanned on the back-end server.

Note
We recommend enabling transport scanning only when Ad-Aware Management Server is installed on a gateway.

- **Scan Plain Text** - select this option if you want the body messages in plain text format to be scanned.
- **Scan Timeout** - type in the corresponding field the maximum time allocated to scan an object. If the scanning process is not completed before the timeout interval, an error is returned and access to the object is denied.
- **Do not scan outgoing mail if they are scanned at Exchange Transport level** - to skip the VSAPI-based antivirus scanning of outgoing e-mails.

Note
You should not select this option if no antivirus scanning is available on the Exchange server installed with the Edge Transport or Hub Transport role.

SMTP Scanning

Select the **Enable SMTP scanning** check box to enable SMTP based antivirus scanning.

If SMTP scanning is enabled, Ad-Aware can add a footer to all scanned mails. Select the **Add footer to scanned e-mails** check box to activate this option and type the desired text in the text box below.

- **Enable / disable footer** - select the **Enable footer** check box to add a footer to all scanned e-mails that lets recipients know the messages were checked for viruses by Ad-Aware. Enter the text you wish to be displayed in the footer in the text box below.

Attachment Filtering Rules

This policy template allows you to create policies for the Attachment Filtering module of Ad-Aware Security for Exchange. The Attachment Filtering module provides filtering features for mail attachments. It can detect attachments with certain name patterns, of a certain type or exceeding a certain size limit.

By using Attachment Filtering, you can achieve the following goals:

- Limit the size of the attachments entering or leaving the mail server.
- Block potentially dangerous attachments, such as .vbs or .exe files, or the e-mails containing them (for example, quarantine e-mail or delete attachment)
- Block attachments having offensive names or the e-mails containing them (for example, reject e-mail or delete attachment)

Attachment Filtering is by default enabled, but all messages are allowed to pass without being scanned. To use Attachment Filtering, go to the *Rule settings* tab and configure the default rule. The default rule manages the attachment filtering settings for all mail traffic reaching or leaving the server. By adding new rules, you can create different filtering policies based on the groups the sender and the recipients belong to.

The settings are organized into 3 sections:

- Attachment Filtering - Allows you to enable the Attachment Filtering.
- Rules - Allows you to manage the rules (create, edit or delete a rule).
- Rule settings - Allows you to configure the filtering options for the selected rules.

Attachment Filtering

This is where you can enable the attachment filtering.

If you want the attachment filtering protection to be enabled, select **Enable attachment filtering**. Otherwise, clear this check box.

Rules

This is where you can specify the attachment filtering options. You can modify the default rule to specify the attachment filtering options for all of the mail traffic, or you can configure new rules in order to create customized group filtering policies.

Default Rule. There is one rule created by default that manages the attachment filtering settings for all groups. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Adding New Rules. To set different filtering policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following options:

- **Create rule** - to create a new rule and configure the Attachment Filtering you need to follow these 3 steps:
  1. Go to the **Attachment Filtering section** and select **I want to make changes to the attachment filtering rules**.
  2. Select **Other** from the Rules section and choose a name.
  3. Configure the attachment filtering policies in the **Rule settings** section.
  - **Edit rule** - allows you to configure the selected rule. To configure the rule, please refer to Rule Settings.
  - **Delete rule** - deletes one / several selected rules. You will have to confirm your choice by clicking **Yes**.

Rule Settings

In this section you can configure the attachment filtering policies for the Ad-Aware Security for Exchange.

You have the option to make changes to the **Default** rule or you can customize the rules created in the *Rules* section.

To enable the rule, select **Enabled** and choose if the rule should apply to the incoming or the outgoing e-mail.

Select Senders Groups

You can select:

All

The rule applies to all senders, regardless of the group they belong to.

Selected

The rule applies only to senders from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose Selected, you have to select from the list the groups you want the rule to apply to.

Note

To learn how to configure a group, please refer to SMTP Groups.

Select Recipients Groups

You can select:

All

The rule applies to all recipients, regardless of the group they belong to.

Selected

The rule applies only to recipients from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose Selected, you have to select from the list the groups you want the rule to apply to.

You can select Match all groups to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note

The addresses in the Cc and Bcc fields also count as recipients.

Note

To learn how to configure a group, please refer to SMTP Groups.

Rule Conditions

In this area you can specify the actions to be taken on the messages matching this policy. If you do not want the messages to be scanned using attachment filtering options, select **Do not scan**.

If you select **Scan**, the messages will be scanned using the attachment filtering options configured for this policy. Next, you must specify the rule conditions.

Note

Messages that do not match any rule condition will not be detected. Consequently, no action will be taken on them and no notification will be issued.

Mail attachments can be scanned using the following criteria: name, file extension and file size. When defining rule conditions, any combination of scanning criteria is allowed.

Filtering Attachments by Name

To filter attachments by name, create a list of filenames and select how the rule will filter them.

- **Match only attachments listed below** - all attachments with the specified filenames will be detected.
- **Skip (don't match) attachments listed below** - all attachments with filenames different than those specified in the list will be detected.

Note

The term name refers here to the filename and the filename extension. For example, if the filename is name_of_file and the filename extension is ext, then the name you have to specify as exception is name_of_file.ext.

To specify exceptions, provide the name in the edit field and click **Add**.

Note

Wildcards can be used to specify exceptions:

- * replaces zero, one or more characters.

  For example, you can enter file*.exe to specify a large category of filenames, which includes filenames like file01.exe, file_new.exe, file.exe and others.

- ? stands for any single character.

  For example, you can enter group?_log??.doc to specify a large category of filenames, which includes filenames like group1_log01.doc, groupA_log19.doc, group4_log1a.doc and others.

All the names excepted from scanning are listed in the box. To remove entries, select them and click **Delete**.

Filtering Attachments by Type

To filter attachments by extension, create a list of file extensions and select how the rule will filter them.

- **Match only files with the extensions listed below** - all attachments with the specified extensions will be detected.
- **Skip (don't match) files with the extensions listed below** - all attachments with extensions different than those specified in the list will be detected.

Specify the permitted extensions in the edit field. The extensions must be separated by a semi-colon ";".

Note

In case of a double extension, only the last extension will be checked.

Filtering Attachments by Size

To detect attachments exceeding a certain size limit, specify the minimum size in the corresponding field. By default, this is set to 0 KB, meaning that no attachment will be detected regardless of its size.

Actions

In this area you can specify the actions to be taken on the messages containing detected attachments. If you do not want the messages to be scanned using the attachment filters, select **Do not scan**.

You must choose one of the following actions:

Action	Description
Reject e-mail	The detected message is rejected with a 550 SMTP error code.
Delete attachment	The detected attachment is deleted.
Replace attachment with text	The detected attachment is replaced with a specified text.

	Provide the text in the edit box that appears.
Redirect e-mail to address	The message containing the detected attachment is redirected to a specified e-mail address. You must specify the e-mail address where the messages are to be delivered in the field next to this option. If you want to provide more than one address, separate them by a semi-colon ";". If the field is empty or the e-mail address is invalid the messages will not be redirected.
Quarantine e-mail	The message containing the detected attachment is moved to the quarantine folder.
Delete e-mail	The message containing the detected attachment is deleted.
Deliver e-mail	The message containing the detected attachment is delivered in full to its recipients.

By default, when a message matches the conditions of a rule, it is no longer checked against any other rules. If you want Ad-Aware to continue processing rules, clear the check box **If the rule conditions are matched, stop processing more rules.**

You can also set additional actions to be taken on the detected messages. The following actions are available:

Action	Description
Modify the subject of the e-mail messages that matched this rule	The subject of the message containing the detected attachments is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[AF]${subject}` - to add `[AF]` before the subject. This is the default subject pattern. • `[AF]${subject}[AF]` - to add `[AF]` before and after the subject. • `[AF]` - to replace the subject with `[AF]`.
Add a header to the e-mails detected as spam	An e-mail header is added to the message containing the detected attachment. Provide the header name and value in the corresponding fields.
Save e-mail to folder	The detected message is saved to a specified folder. Provide the folder name and location in the corresponding fields.
Archive to account	The detected message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Notifications

In the **Notifications** area you can specify whether to issue notifications or not when attachments match the rule. Select **Rule** matched to issue notifications when attachments match the rule.

Note

The corresponding event in the *Alerts* section must be enabled and properly configured.

Content Filtering Rules

This policy template allows you to create policies for the Content Filtering module of Ad-Aware Security for Exchange.

Content Filtering helps you filter e-mail messages based on certain character strings found in the e-mail headers (subject, from, to, cc) or in the e-mail body. By using Content Filtering, you can achieve the following goals:

- Prevent unwanted mail content from entering the users' Inbox.
- Block outgoing mail containing confidential data.
- Archive messages that meet specific conditions (for example, those coming on your company's support e-mail address) to a different e-mail account or on the disk.

Content Filtering is by default enabled, but all messages are allowed to pass without being scanned. To use Content Filtering, go to the Rule settings tab and configure the default rule. The default rule manages the content filtering settings for all mail traffic reaching or leaving the server. By adding new rules, you can create different filtering policies based on the groups the sender and the recipients belong to.

The settings are organized into 3 sections:

- Content Filtering - Allows you to enable the Content Filtering.
- Rules - Allows you to manage the rules (create, edit or delete a rule).
- Rule settings - Allows you to configure the filtering options for the selected rules.

Content Filtering

This is where you can enable the content filtering.

If you want the content filtering protection to be enabled, select **Enable content filtering**. Otherwise, clear this check box.

Rules

This is where you can specify the content filtering options. You can modify the default rule to specify the content filtering options for all of the mail traffic, or you can configure new rules in order to create customized group filtering policies.

Default Rule: There is one rule created by default that manages the content filtering settings for all groups. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Adding New Rules: To set different filtering policies, add new rules. This way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following options:

- **Create rule** - to create a new rule and configure the Content Filtering you need to follow these 3 steps:
  1. Go to the **Content Filtering** section and select **I want to make changes to the content filtering rules**.
  2. Select **Other** from the **Rules** section and choose a name.
  3. Configure the content filtering policies in the Rule settings section.
- **Edit rule** - allows you to configure the selected rule. To configure the rule, please refer to Rule Settings.
- **Delete rule** - deletes one / several selected rules. You will have to confirm your choice by clicking **Yes**.

Rule Settings

In this section you can configure the content filtering policies for the Ad-Aware Security for Exchange.

You have the option to make changes to the **Default** rule or you can customize the rules created in the *Rules* section.

To enable the rule, select **Enabled** and choose if the rule should apply to the incoming or the outgoing e-mail.

Select Senders Groups

You can select:

All

The rule applies to all senders, regardless of the group they belong to.

Selected

The rule applies only to senders from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Note
To learn how to configure a group, please refer to SMTP Groups.

Select Recipients Groups

You can select:

All

The rule applies to all recipients, regardless of the group they belong to.

Selected

The rule applies only to recipients from the selected groups.

You can choose which headers are checked when filtering traffic:

- **E-mail headers** - check the message headers.
- **Connection headers** - check the SMTP connection headers.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all groups** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note

The addresses in the **Cc** and **Bcc** fields also count as recipients.

Note

To learn how to configure a group, please refer to SMTP Groups.

Rule Conditions

In this area you can specify the actions to be taken on the messages matching this policy. If you do not want the messages to be scanned using content filtering options, select **Do not scan**.

If you select **Scan**, the messages will be scanned using the content filtering options configured for this policy. Next, you must specify the rule conditions.

Note

Messages that do not match any rule condition will not be detected. Consequently, no action will be taken on them and no notification will be issued.

Messages can be scanned using the following criteria: subject, sender / recipient address, body. When defining rule conditions, any combination of scanning criteria is allowed.

Filtering Mail by Subject

Select **Subject** and specify the rule strings in order to filter mail by subject. All the messages the subject of which matched one of the defined strings will be detected.

To specify the strings, click **Configure subject**. A new window will appear, where you can configure the defined strings (please see Configuring Strings).

Filtering Mail by Sender Address

Select **Sender** and specify the rule strings in order to filter mail by the sender address. All the messages the sender address of which matches one of the defined strings will be detected.

To specify the strings, click **Configure sender**. A new window will appear, where you can configure the defined strings (please see Configuring Strings).

Filtering Mail by Recipients Address

Select **Recipients** and specify the rule strings in order to filter mail by the recipient address. All messages with at least one recipient address matching one of the defined strings will be detected.

To specify the strings, click **Configure recipients**. A new window will appear, where you can configure the defined strings (please see Configuring Strings).

Filtering Mail by Body Content

Select **Body** and specify the rule strings in order to filter mail by content. All messages containing one of the defined strings in the e-mail body will be detected.

To specify the strings, click **Configure body**. A new window will appear, where you can configure the defined strings (please see Configuring Strings).

Configuring Strings

You can see each selected rule condition listed in the box.

Provide the string in the corresponding field and click **Add**.

You can choose to enter a text, a wildcards expression or a regular expression.

Note

You can use the following wildcards:

- * replaces zero, one or more characters.
  For example, you can enter *xxx* to detect the messages that contain the xxx string in the headers (subject, sender address or recipient address).
- ? stands for any single character.
  For example, if you filter messages by the sender address, you can add ?doe@company.com to detect the messages that are sent from addresses beginning with any single character and followed by the doe@company.com string.

Two additional options are available:

Option	Description
Match case	The rule applies only if the detected item and the specified parameter case match.
Match whole word only	The rule applies only if an entire string matching the specified parameter is detected.

You can see all the defined strings in the list. To remove entries, select them and click **Remove**.

Click **OK** to save the changes.

Actions

In the **Actions** area you can specify the actions to be taken on the detected messages.

You must choose one of the following actions:

Action	Description
Reject e-mail	The detected message is rejected with a 550 SMTP error code.
Delete e-mail	The detected message is deleted.
Redirect e-mail to address	The detected message is redirected to a specified e-mail address. You must specify the e-mail address where the messages are to be delivered in the field next to this option. If you want to provide more than one address, separate them by a semi-colon ";". If the field is empty or the e-mail address is invalid the messages will not be redirected.
Quarantine e-mail	The detected message is moved to the quarantine folder.
Deliver e-mail	The detected message is delivered in full to its recipients.

By default, when a message matches the conditions of a rule, it is no longer checked against any other rules. If you want Ad-Aware to continue processing rules, clear the check box If the rule conditions are matched, stop processing more rules.

You can also set additional actions to be taken on the detected messages. The following actions are available:

Action	Description
Modify the subject of the e-mail messages that matched this rule	The subject of the detected message is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[CF]${subject}` - to add `[CF]` before the subject. This is the default subject pattern. • `[CF]${subject}[CF]` - to add `[CF]` before and after the subject. • `[CF]` - to replace the subject with `[CF]`.
Add a header to the e-mail messages that matched this rule	An e-mail header is added to the detected message. Provide the header name and value in the corresponding fields.
Save e-mail to folder	The detected message is saved to a specified folder. To specify the folder, click **Browse**, locate it and then click **OK**.
Archive to account	The detected message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Notifications

In the Notifications area you can specify whether to issue notifications or not when messages match the rule.

Select Rule matched to issue notifications when messages match the rule.

Note

The corresponding event in the Alerts section must be enabled and properly configured.

General Settings

This policy template allows you to create policies for general settings of Ad-Aware Security for Exchange.

Here you can configure the Ad-Aware notification system, real time virus reporting, incident reporting, purge settings and the Quarantine settings. The settings are organized into 5 sections:

- Alerts
- Virus Report
- Report incidents
- Purge Settings
- Quarantine Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings, click ⌄.

Alerts

In this section you can configure event notifications, mail alert templates and settings and net send alert templates.

- Events - this is a list of the events that may occur:

Event	Description
Ad-Aware Error	Groups all the errors that may appear during product operation, such as service start failure.
Update Error	Refers to the occurrence of an error during the update process.
Infected/suspect file detected	Occurs when an infected file or a file suspected of being infected has been detected.
Ad-Aware Warning	Groups critical information regarding the activity of Ad-Aware.
File not scanned	Occurs when a file could not be scanned by Ad-Aware.
Key expired	Indicates the expiration of the registration period.
Product update	Occurs when a product update is available.
Ad-Aware Information	Group’s information regarding the activity of Ad-Aware.
Key will expire	Indicates that there are 3 days left before the product expires.
Rule match	Occurs whenever a message matches a Content Filtering or Attachment Filtering rule.

Update Information	Contains information about the update process.

There are 3 types of events, depending on their importance to the security of the system:

- **Information** - such events provide information about the product activity.
- **Warning** - such events provide critical information about aspects of the product activity which requires your attention.
- **Error** - such events provide information about errors that appear during product operation.

Set the importance of the events by selecting one of the following levels from the drop-down lists corresponding to each event:

- **Low** - a record of the event is kept in the log file. No alert is sent when the event takes place.
- **Medium** - log the event and send mail alerts when the event takes place.
- **High** - log the event and send both mail and net send alerts when the event takes place.

Note

To completely disable notifications for an event, select Disabled from its corresponding drop-down list.

- **Mail Alert Templates** - if the importance of the event is medium or high, mail alerts will be sent.

  Each event comes with a default alert text. To view the alert text of an event, click **Edit** next to that event. To change the text, edit the contents of the text box.

  Important

  You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

- **Net Send Alert Templates** - if the importance of the event is high, net send alerts will be sent.

  Each event comes with a default alert text. To view the alert text of an event, click **Edit** next to that event. To change the text, edit the contents of the text box.

  Important

  You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

- **Mail alerts** - to use the mail notification service, follow these steps:

  1. Select **Enable mail alerts** to activate the mail notification service
  2. Configure the SMTP settings:
     - **SMTP Server** - enter the IP address of the SMTP server that your network uses to send messages.
     - **From** - enter the e-mail address that will appear in the sender field.

  Important

Provide a valid e-mail address for the SMTP server, otherwise the server may decline to send an e-mail whose sender (e-mail address) is unknown to it.

3. If the SMTP server used to send messages requires authentication, select Use **SMTP Server Authentication** and enter the user name and password in the corresponding fields.

   Note

   NTLM authentication is not supported.

4. Indicate the recipients of the mail alerts by entering their e-mail addresses one y one in the text box located under the **Recipients** list box and clicking **Add**.

   To remove e-mail addresses from the list, select them and click **Delete**.

   Note

   The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set.

- **Net send alerts** - to use the mail notification service, follow these steps:
  1. Select **Enable Net Send Alerts** to activate the net send notification service.
  2. Indicate the recipients of the net send alerts by entering their computer names one by one in the text box located under the **Recipients** list box and clicking **Add**. To remove computer names from the list, select them and click **Delete**.

     Note

     The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set.

Virus Report

In this section you can configure real time virus reporting.

Real time virus reporting (RTVR) allows sending reports about the viruses found on your server to the Ad-Aware Lab in order to help us identify new viruses and find quick remedies for them. Your contribution could be essential for developing new tools to protect you and other users against virus threats.

Real time virus reporting is disabled by default. To activate it, select **Enable real time virus reports**.

The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.

Report Incidents

In this section you can configure the incident management module that allows creating incident reports during crashes of Ad-Aware Security for Exchange.

By agreeing to send the incident reports to the Ad-Aware Lab, you agree to help us find quick fixes for our bugs. You could make a major contribution to the development of a stable product that satisfies your needs.

By default, the reports created automatically during product crashes are not sent to the Ad-Aware Lab. To configure Ad-Aware to send incident reports to the Ad-Aware Lab, select **I agree to submit dumps to the Ad-Aware Lab** and enter your e-mail address in the provided text box.

The reports will only be used for debugging purposes. They will never be used as commercial data or disclosed to third parties.

Purge Settings

In this section you can configure the period of time for which Ad-Aware Security for Exchange will store the following data:

- Quarantine (quarantined files)
- Statistics
- Reports
- View Logs

By default, data older than 30 days is automatically deleted.

You can set a different time period for each type of data by entering the number of days / weeks / months in the text boxes corresponding to the types of data you wish to edit.

Quarantine Settings

This policy template allows you to manage the quarantined files from the Quarantine folder in Ad-Aware Security for Exchange:
You can change the folder the quarantine is located in. In order to operate this change, provide the new path in the edit field.

Note

The default quarantine folders for each component are the following:

- `C:\Program Files\Ad-Aware\ Ad-Aware for Windows Servers Services\Quarantine\AV` for the Antivirus module.
- `C:\Program Files\ Ad-Aware\ Ad-Aware for Windows Servers Services\Quarantine\AF` for the Attachment Filtering module.
- `C:\Program Files\ Ad-Aware\ Ad-Aware for Windows Servers Services\Quarantine\AS` for the Anti-spam module.
- • `C:\Program Files\ Ad-Aware\ Ad-Aware for Windows Servers Services\Quarantine\CF` for the Content Filtering module.

Get Settings

This policy template allows creating policies for retrieving the SMTP Proxy settings of Ad-Aware Security for Exchange.

No additional settings are required.

Install Product Update

This policy template allows you to create policies for triggering the installation of a product update for Ad-Aware Security for Exchange.

The product updates are different from the signature updates. Their function is to deliver bug fixes and new features to the product.

There are two types of updates for the product:

- **Product updates (patches)** - these are files that bring improvements to the current product; they are usually smaller size updates that do not require a new version of the product to be delivered.
- **Version updates** - these are installation packages of a new released version of the product.

The settings are in the *Settings* section.

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Settings

Here you can choose whether or not to allow the installation of the product update if it involves stopping / starting server traffic or rebooting the server.

To agree with the installation in one of the two cases, select the corresponding check box. Otherwise, make sure the check box is cleared.

Rollback Product Update

This policy template allows creating policies for rolling back to the previous version of Ad-Aware Security for Exchange. The rollback feature gives you the option to revert to the previous product version once you have installed a product update.

If a rollback is available, the current product version and the version you can roll back to will be displayed. The rollback does not require other settings to be configured.

After a rollback is performed, the version currently in use and the previous version will be displayed. You can use the provided link to update back to the newer version.

Scanning Scheduled

This policy template allows you to create policies to scan all mailboxes and public folders on the Ad-Aware Security for Exchange.

Different actions can be configured for the infected and suspect objects detected by Ad-Aware. There is a list of actions that can be applied to each category of detected objects (infected or suspect). When such an object is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

Configuring Actions

In the **Actions** area you can specify the actions to be taken on infected and suspect objects.

The antivirus actions are ordered in a list according to their priority. Click the desired action in order to move it up or down.

Actions for infected objects. The following actions are available for infected objects:

Action	Description
Disinfect	The infected message is disinfected.
Move to Quarantine	The infected object (mail body / attachment / public file) is moved to the quarantine folder.
Replace object	The infected object (mail body / attachment) is replaced with an explanatory text.
Reject/Delete e-mail	The detected message is rejected with a 550 SMTP error code.
Ignore	The infected message is delivered in full to its recipients.

Actions for suspect objects. The following actions are available for suspect objects:

Action	Description
Move to Quarantine	The suspect object (mail body / attachment / public file) is moved to the quarantine folder.
Replace object	The suspect object (mail body / attachment) is replaced with an explanatory text.
Reject/Delete e-mail	The suspect message is rejected with a 550 SMTP error code.
Ignore	The suspect message is delivered in full to its recipients.

Ad-Aware replaces the infected or suspect objects that are deleted or moved to quarantine with an explanatory text.

To edit the text to be delivered instead of such objects, do any or both of the following:

- Select **Infected/ suspected file replaced** and type in the edit box the text to be delivered instead of the infected or suspect objects deleted.
- Select **Infected/ suspected file quarantined** and type in the edit box the text to be delivered instead of the infected or suspect objects moved to quarantine.

Set Advanced Settings

- If you want to limit the scanning time, select **Stop scan if it takes longer than** and specify the number of minutes or hours.
- If you do not want to scan messages that exceed a certain size limit, select **Maximum mail size to be scanned** and provide the size limit in the corresponding field.
- Beside messages, you can select other objects to be scanned: **Contacts**, **Quick Tasks** and **Appointments**.

Notifications

- Select **Log start/end of on-demand scanning** to record the start and the end of the process in the log file.

  Note

  The corresponding event from the *Alerts* section must be enabled and properly configured.

- Select **Generate Scan Report** to generate a report for the on-demand scan. By default, the report file is saved in: `C:\Program Files\Ad-Aware\Ad-AwareManagement Server\Reports`. To change this location, enter the new path in the corresponding box.

The report can be generated in HTML, text or CSV format. You can choose the format of the report file from the menu.

SMTP Groups

Ad-Aware allows creating user groups, in order to apply different scanning and filtering policies for different user categories. For example, you can create appropriate policies for the IT department, for the sales team or for the managers of your company.

To create new user groups or manage existing groups, go to the **Options** area.

You can see all the existing groups listed in the table along with their description.

Options

This is where you can create a new group or you can choose to configure a group which you have created previously.

Provide the group name and, optionally, the group description in the corresponding fields.

Configuring Groups

To configure the group follow these steps:

- Add users to the new group. Provide the e-mail address in the corresponding field and click **Add**.
- Delete users in the group. To remove one or several items from the list, select them, click **Delete**.

Update Request

This policy template allows you to create policies for triggering a signature update for Ad-Aware Security for Exchange.

The template does not require other settings to be configured. You can configure update settings using the Update Settings template.

Update Settings

This policy template allows you to create policies for configuring the update settings for Ad-Aware Security for Exchange. You can configure automatic signature updates, product updates, update locations and notifications.

Here you can configure update settings that will be applied on the assigned clients. The settings are organized into 4 sections:

- Options
- Product update options
- Update location
- Notifications

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Options

In this section you can configure the automatic update interval and enable update pushing.

Update Pushing is a feature that is available only when the product is registered. This feature allows customers to benefit from "Update Announcement Messages". These alerts are sent to the Update Pushing mailing list by the Ad-Aware Lab. The mailing list is composed of mail addresses that have been submitted by the customers on the Ad-Aware website. The "Update Announcement Messages" include special elements which trigger the update process when the message is scanned by the product. Therefore, it is mandatory that the mail address submitted by the customer is a mail address protected by Ad-Aware.

To enable Update Pushing, check **Enable Update Pushing**. If you do not want to use this service, clear the corresponding check box.

The automatic update feature allows updating Ad-Aware automatically, on a regular basis, without the administrator's intervention.

By default, Ad-Aware checks for updates at the specified update locations, every hour.

To change the frequency at which Ad-Aware checks for updates, type the number of hours between two consecutive checks for updates in the **Automatic update interval** text box.

To disable the automatic update, clear the check box corresponding to **Automatic update interval**.

Product Update Options

Installing product updates regularly is essential to the security of your server. Depending on the level of interference with the server, there are three types of product updates:

- product updates that do not require stopping server traffic or to reboot the server
- product updates that require stopping server traffic, but do not require to reboot the server
- product updates that require to reboot the server

To configure automatic downloads and installation for each type of product update, select one of the following options:

- **Download updates and install automatically**

Select this option and Ad-Aware will automatically download and install product updates. This is the recommended choice for product updates that do not require stopping server traffic or a server reboot.

- **Download updates automatically and install... at...**

Select this option if you want Ad-Aware to install available updates at certain times. Select from the corresponding drop-down lists the date (day and time) when you want this to happen.

This way you can configure Ad-Aware to perform product updates at times when it is least likely for interferences to occur with server activity (during night time, for example).

- **Download updates and let me decide when to install them**

Select this option if you want Ad-Aware to automatically download product updates, but let you decide when to install them. This is the recommended choice for product updates that require stopping server traffic or a server reboot.

To disable automatic product updates, select the **No automatic product updates** check box.

Note
Your server will be more vulnerable unless you install updates regularly.

Update Location

Ad-Aware can update from the local network, over the Internet, directly or through a proxy server.

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and a **Secondary update location**. Both require the configuration of the following options:

- **Update location** - type the address of the update server. By default, the primary update location is: `http://definitionsbd.lavasoft.com`.

If multiple Ad-Aware products are installed in your network, you can setup a local server as the first update location for all the products and make http://definitionsbd.lavasoft.com the second location, to be used in case the first becomes unavailable. In this way you can reduce Internet traffic during updates.

- **Allow unsigned updates** - select this option to allow updates from a local server to be installed.
- **Use proxy** - select this option if the company uses a proxy server. The following settings must be specified:
  - **Server Name or IP** - type the IP of the proxy server.
  - **Port** - type the port Ad-Aware uses to connect to the proxy server.
  - **Username** - type a user name recognized by the proxy.
  - **Password** - type the valid password of the previously specified user.

Notifications

Ad-Aware can be configured to notify you about special events that occur during its operation.

Select the update events you want to be informed about:

- **Update performed** - when an update was performed.
- **No update available** - when no update is available.
- **Update failed** - when an error occurred during an update and the update failed.
- **Product update available** - when a product update is available.

You can customize the notifications of each update event using the *Alerts* section of the **General Settings** template.

Ad-Aware Security for Mail Servers (Unices) Templates

The Ad-Aware Security for Mail Servers (Unices) policy templates allows you to create policies that you can use in order to manage Ad-Aware Security for Mail Servers (Unices). By using these policies you can ensure your organization's mail servers are secure.

Note
In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Security for Mail Servers (Unices):

File logging policy

Allows creating file logging policies for Ad-Aware Security for Mail Servers (Unices)

Mail alerts policy

Allows creating mail alerts policies for Ad-Aware Security for Mail Servers (Unices)

Mail settings policy

Allows creating mail settings policies for Ad-Aware Security for Mail Servers (Unices)

SMTP protocol policy

Allows creating SMTP protocol policies for Ad-Aware Security for Mail Servers (Unices)

Update settings policy

Allows creating update settings policies for the Ad-Aware Security for Mail Servers (Unices)

File Logging Policy

This policy template allows you to create file logging and log rotate policies for Ad-Aware Security for Mail Servers (Unices).

The settings are organized into 2 sections:

- File Logging - allows you to configure file logging policies for Ad-Aware Security for Mail Servers (Unices).
- Log Rotate - allows you to rotate the logs according to several criteria.

File Logging

This is where you can enable file logging.

For each rule you can select the component (daemon) it applies to, the message type and the location of the log file. For more information on each type of daemon, please refer to Core Modules.

The message types for the modules above can take the following values: info, error, license, debug, virus, spam, cf and scanning.

Let's say you enable the **Error messages** for a component (daemon) rule. This means that all error-related information, coming from all Ad-Aware daemons, will be found in this location: /var/log/error. log. Of course, you can easily modify the location by editing the **Log File** text box.

If you want to create a new policy, select the component (daemon) it applies to and the message type from the corresponding drop-down lists, type the location of the file into the **Log File** text box and click **Finish**.

Log Rotate

This policy template is useful when you have to manage systems that generate large numbers of log files. **Log rotate** allows the automatic rotation of the log files according to the following criteria:

- Rotate interval: the log files may be rotated by hour, day, week or month.
- Rotate log size: the log files may be rotated when they reach a certain size.
- Rotate entries: the log files may be rotated taking into consideration the number of entries.
- Rotate count: how many times the log files are rotated before starting to delete the old files.

Mail Alerts Policy

This policy template allows you to create policies for mail alerts of Ad-Aware Security for Mail Servers (Unices).

Mail alerts are simple e-mail messages sent by Ad-Aware to the system administrator to inform him or her about special events or to the partners of an e-mail communication to inform them about malware found.

If you want to add a new rule, select the component it applies to and the rule type from the corresponding drop-down lists, type the e-mail address(es) the alerts should be sent to and click **Finish**. For more information on each type of daemon, please refer to Core Modules.

Mail Settings Policy

This policy template enables you to create mail filtering policies for Ad-Aware Security for Mail Servers (Unices).

By default you are dealing with one `Default` group only, containing the entire list of users, both senders and receivers. The `Default` group specifies the implied settings, if they are not otherwise specified in a certain group.

At the same time you can customize a certain group to meet your needs, by changing its settings. In this way, the new settings will have higher precedence over the default ones.

To edit the settings for an existing group, enter the group name in the corresponding text box in order to select it.

Antivirus

The Antivirus module offers protection against viruses, spyware and riskware. It detects infected or suspect messages and attempts to disinfect them or isolates the infection, according to the specified actions.

If you want the antivirus protection to be enabled or add a header to the scanned e-mails, select the corresponding check boxes.

Antivirus Actions

The antivirus actions are ordered in a list according to their priority. Click the desired action in order to move it up.

The selected actions which appear at the top of the list in red will apply according to their order.

Select the actions to be taken on **viruses**, **suspected objects** and **riskware**:

Disinfect

> Remove the malware from the infected attachment (or any other mail component that can be used to send malware). If successful, the mail is passed to the next plugin (if any) or forwarded. Otherwise, the next action is executed.

Delete

> Remove the attachment or other mail components that contain the malware. If successful, the mail is passed to the next plugin (if any) or forwarded. Otherwise, the next action is executed.

When the mail is completely deleted, a replacement letting the recipient know what happened will be generated.

Move to quarantine

Move the mail to quarantine. If the action fails, an error message line is written to the log.

After this action is taken, the mail will either be dropped (the default action) or rejected.

Copy to Quarantine

Copy the mail to quarantine. If the action fails, an error message line is written to the log.

Drop (the default action)

Send the message to the mail transport agent (MTA) to drop the mail. This is the default action. Thus, the final action will always be Drop, unless you decide otherwise.

This action prohibits the mail from passing. The MTA will return no response to the sender.

Reject

Send the message to the mail transport agent (MTA) to reject the mail.

This action prohibits the mail from passing. However, the MTA will send back a rejection message.

Ignore

Send the message to the mail transport agent (MTA) to forward the mail.

Anti-spam

The Anti-spam module offers protection against spam, phishing and other attacks. It uses a combination of various filters and engines to determine whether messages are spam or not and to check them for patterns of spam.

Anti-spam Settings

If you want the anti-spam protection to be enabled, select the corresponding check box.

These settings allow you to configure basic anti-spam filters and related options. If you select:

- **Add headers** - new headers will be added to all mails (by default `X-Ad-Aware-Spam`). The SpamStamp Header, by default `X-AdAware-SpamStamp`, is a special feedback header, used by Ad-Aware Anti-spam specialists as feedback, when false negatives and positives are submitted to spam_submission@bitdefender.com.
- **Modify subject** - the `subject` of the e-mail messages will be modified conforming to the Subject template field.
- **Aggressivity** - use the corresponding drop-down list to select the desired level.

  The scale goes from `1` (minimum trust in anti-spam score returned by the Ad-Aware filters) up to `9` (maximum trust). Choosing `1` might increase the amount of unsolicited e-mails, while choosing `9` might increase the amount of false positives.

Anti-spam Engines

Each of the anti-spam engines can be enabled or disabled individually.

Select the check boxes corresponding to the engines you want to enable:

The Multipurpose filter

The Multipurpose filter is a generic name for GTUBE (an anti-spam test) and two specialized filters: the Charset filter and the Sexually explicit filter.

GTUBE, the Generic Test for Unsolicited Bulk E-mail, is an anti-spam test similar to EICAR antivirus test. The test consists in entering a special 68-byte string in the message body of an e-mail in order to be detected as spam. Its role is to check the product functionality to see if the filters are correctly installed and detect the incoming spam.

The Charset filter can be instructed to detect messages written in other languages (for instance Asian languages, or Cyrillic) and mark them as spam. This comes in handy when the user is certain that they will not receive mail in these languages.

The American law demands that all sexually explicit advertisement e-mails be marked as such, with “sexually explicit” in their subject. The Sexually explicit filter can detect and mark these messages as spam directly.

Note

The GTUBE is the first filter to come to action, while the specialized filters follow after the black list / white list filter.

The Black list / White list filter

The black list / white list filter can be very useful when the user wants to block incoming messages from a certain sender (blacklist), or when the user wants to make sure that all messages from a friend or a newsletter arrive in the Inbox, regardless of their contents. The black list / white list filter is often called “Friends / Spammers list”. It can define allow or deny lists either for individual e-mail addresses, or for entire domain names (for instance all mail from any employee of bigcorporation.com).

Add friends to the white list

We recommend that you add your friends’ names and e-mail addresses to the white list. Ad-Aware will not block messages from those on the list; therefore, adding them ensures that legitimate messages get through.

The two lists are plain text files, containing one entry per line. You can find these text files (as_wlist and as_blist) in this location: /opt/ Ad-Aware/etc. The entries may be usual e-mail addresses or domain names, respecting the following format.

The RBL filter

RBL stands for “Real time Black List” or “Real time Blackhole List”. The Ad-Aware implementation uses the DNSBL protocol and RBL servers to filter spam based on mail server's reputation as spam sender.

The mail server address is extracted from the e-mail header and checked for validity. If the address belongs to a private class (10.0.0.0/8 or 192.168.0.0/16) or it is not relevant, it will be ignored.

A DNS check will be performed on the domain d.c.b.a.rbl.example.com, where d.c.b.a is the reversed IP address of the server and rbl.example.com is the RBL server. If the DNS replies that domain is valid, it means that the IP is listed in the RBL server and a certain server score is provided. This score can take values from 0 to 100, according to the server confidence (trust level), which you are free to configure.

The query is performed for every RBL server in the list and the score returned by each one is added to the intermediate score. When reaching 100, no more queries are performed.

Finally, a spam score is computed from the RBL servers score and added to the global e-mail's spam score.

The Image filter

Some messages have image attachments, and we have the Image filter to detect them and compare them to a database of known spam images, which is also maintained and updated by our lab.

The new image filter combines old techniques from CBIR (Content Based Image Retrieval) with a new special image distance specifically designed for spam pictures called SID (Spam Image Distance). It also learns histograms (graphs that displays the number of pixels at each color value within an image or region) met in spam images and then quickly identifies them at the user. The Image filter is trained by Ad-Aware Anti-spam Labs and updated several times a day in order to provide high-accuracy and spam detection rate.

The URL filter

Almost all spam links to a site: whether they want us to buy cheap Rolexes or enter our login and password on a fake Citibank site, they have a link. The URL filter detects these links and looks them up in a database created and maintained (via update) by our lab. If a message links to a “forbidden” site, the odds are high that it's spam.

The Bayesian filter

We know that not all of our users will agree with us when classifying a message as spam or legit. For instance, a doctor talking about Viagra with his patients will certainly need to customize his filters. That's why we've added the Bayesian filter.

Every user can train it by example, and make it learn what messages are spam and what messages are legit (from specific examples in the user's mailbox). After enough learning, the Bayesian filter is adapted to the specifics of legitimate and spam messages the user usually receives, and it becomes a powerful factor in the decision process.

The Pre-trained Bayesian filter

While the Bayesian filter is user-trained, this filter is pre-trained by the Ad-Aware Anti-spam Lab and updated periodically.

You can help improve the pre-trained filter by submitting spam messages to our Anti-spam Lab. The submission process works as follows:

1. A spam e-mail is delivered to a user
2. The user forwards the e-mail as an attachment to a predefined POP3 e-mail account that Ad-Aware periodically checks
3. Ad-Aware retrieves the e-mail and feeds it to the Bayes dictionary

Important
E-mails retrieved by Ad-Aware are erased from the Inbox.

The Heuristic filter

When we create detection rules, our anti-spam analysts consider the spam messages that are available to us. Even though there are millions of them, it's impossible to consider each one thoroughly. That's why we've created a powerful filter using a Neural Network (a concept borrowed from the field of Artificial Intelligence).

The most important feature of the Neural Network (NeuNet) is that we have trained it in the Anti-spam Labs, allowing it to look at a lot of spam messages. Much like a child in school, it has learned to distinguish between spam and legit e-mails, and its formidable advantage is that it can recognize new spam by perceiving similarities (oftentimes very subtle) between the new messages it sees and the messages it has learned.

The Signatures filter

A rule-based method of identifying new spam by using the spam signatures it contains in its data base.

Anti-spam Actions

The anti-spam actions are ordered in a list according to their priority. Click the desired action in order to move it up.

The selected action which appears at the top of the list in red will apply.

Select the actions to be taken by the anti-spam filter:

Ignore

Send the message to the mail transport agent (MTA) to forward the mail.

Move to quarantine

Move the mail to quarantine. If the action fails, an error message line is written to the log.
After this action is taken, the mail will either be dropped (the default action) or rejected.

Drop (the default action)

Send the message to the mail transport agent (MTA) to drop the mail. This is the default action. Thus, the final action will always be **Drop**, unless you decide otherwise.

This action prohibits the mail from passing. The MTA will return no response to the sender.

Copy to Quarantine

Copy the mail to quarantine. If the action fails, an error message line is written to the log.

Reject

Send the message to the mail transport agent (MTA) to reject the mail.

This action prohibits the mail from passing. However, the MTA will send back a rejection message.

Content Filter

Content Filtering helps you filter e-mail messages based on certain character strings found in the e-mail headers (subject, from, to, cc) or in the e-mail body. By using

Content Filtering, you can achieve the following goals:

- Prevent unwanted mail content from entering the users' Inbox.
- Block outgoing mail containing confidential data.
- Archive messages that meet specific conditions (for example, those coming on your company's support e-mail address) to a different e-mail account or on the disk.

To enable the content filter or add a header to filtered e-mails, select the corresponding check boxes.

SMTP Protocol Policy

This policy template allows you to create SMTP protocol policies for Ad-Aware Security for Mail Servers (Unices).

For SMTP Proxy integration, you have to specify the following information in order to allow Ad-Aware to scan all e-mail traffic:

- The **Real mail server** address and **Real mail port** where Ad-Aware routes mail traffic to. By default the address is 127.0.0.1 and the port is 10025.
- The **SMTP port** Ad-Aware will listen on. By default, the port is 25.
- The connection timeout specifies how long Ad-Aware will wait for incoming data through an already established connection before closing it.

Type the connection timeout value in seconds. For instance, if you type 60 and no data is transmitted across the already established connection for 60 seconds, Ad-Aware will abort the connection. When the value is 0, no timeout connection is enforced.

- The **Maximum threads** represent the maximum number of incoming concurrent connections Ad-Aware will be able to handle. If the value entered is negative, all the incoming connection will be refused. When the value is 0, no threads limit is enforced.
- The **Maximum mail size to be scanned** represents the size limit accepted by Ad-Aware.

You can type a number into the corresponding text box, to set a size limit for files scanning. If a message size surpasses this limit, the e-mail message will be rejected.

When the value is 0, no size limit is enforced. All the files, regardless of their size, will be scanned.

Networks

This section contains the networks Ad-Aware relays e-mail messages from. You must add the address in IPv4 dotted format to the list to instruct Ad-Aware to accept e-mails coming from these addresses, no matter of their destination.

Domains

The relay domains Ad-Aware will use to accept e-mails for are configured in this section. For example, if your e-mail server handles e-mails for the company1.com and company2.com domains, you must enter both domains in this section. If you have subdomains, you must specify them explicitly as subdomain1.company3.com, subdomain2.company3.com, etc.

Update Settings Policy

This policy template allows you to create policies for configuring the update settings for Ad-Aware Security for Mail Servers (Unices). You can configure automatic product updates, update locations and proxy settings.

Here you can configure update settings that will be applied on the assigned clients.

The settings are organized into 3 sections:

- Live! Update
- Insecure Update
- Proxy Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Live! Update

The Live! Update window provides information regarding the general update settings and update status.

The default update server is http://definitionsbd.lavasoft.com and the default update interval is 1 hour. To use a different server or set a different time interval between updates, enter the new information in the corresponding text box.

PushUpdate is an ordered update launched by Ad-Aware servers in imminent situations, when a prompt update can save the server from allowing the infected e-mails to pass.

If a proxy server is used to connect to the Internet, select the **Use Proxy** check box.

Insecure Update

If you want to use a different update server, select this option to allow updates from a local server to be installed.

Proxy Settings

This is where you can enter the proxy server settings.

Enter the server address and port in the corresponding text box. If authentication is required, you also have to enter the user name, password and domain in the corresponding text boxes.

Core Modules

Ad-Aware Security for Mail Servers (Unices) is a highly complex modular structure. It is made up of several central components and additional modules, each of them having assigned a specific task. The modules are loaded during Ad-Aware startup and enabled or not, according to the user's preferences. On a UNIX-like system, these components run as daemons, on one or multiple threads, and communicate with the others.

Listed by their file names, the core modules are represented in the following table.

Module	Description
aamond	The Ad-Aware Core Monitor is the supervisor of several Ad-Aware modules. When one of them crashes, the Core Monitor isolates the object causing the crash in a special quarantine directory, notifies the administrator and restarts the involved module. Thus, even if one process dies, the whole filtering activity is not disturbed, ensuring continuous server protection.
aascand	This is the Ad-Aware Scan Daemon. Its purpose is to integrate the scanning engines, receive scanning requests from several daemons, such as the mail daemon or the file daemon. It scans the objects, takes the necessary actions and sends back the object and the scanning results.
aaemclientd	The Ad-Aware Enterprise Manager Client acts as a link between Ad-Aware Management Server and Ad-Aware Security for Mail Servers (Unices). It allows the security product to interpret the policies sent by Ad-Aware Management Server.
aamagentd	The Ad-Aware Enterprise Manager Agent enables communication between Ad-Aware Management Server and the Ad-Aware products it manages.
aamilterd	Ad-Aware Agent For Sendmail is the filtering solution for Sendmail with the Milter interface. Milter allows third-party applications to access and filter mail messages as they are being processed.
aamaild	The Ad-Aware Mail Daemon has the role of receiving scanning requests from the MTA integration agents. It calls the Scan Daemon to perform the scan, expecting the scanning results from it. Then it applies its actions and sends back the results to the MTA integration agent.
aafiled	The Ad-Aware File Daemon has the role of receiving scanning requests from the Samba Virtual Filesystem module. It calls the Scan Daemon to perform the scan, expecting the scanning results from it. Then it applies his actions and sends back the results to Samba.
aalogd	The Ad-Aware Logger is a complex component, handling all logging and notification actions

	of Ad-Aware. There are several types of logging, all of them realized by plugins. • File logging: the data is sent to a normal log file, respecting a typical format. • Mail notification: alerts are sent by e-mail to the server administrator or to the sender and the recipients of an e-mail, on special events (such as infected e-mail found). • Real Time Virus and Spam Report: anonymous statistics are sent to Ad-Aware Labs to keep a map of malware activity and to detect outbreaks.
aalived	The Ad-Aware Live Update is the module responsible with updating the scanning engines and some other Ad-Aware components. The module runs continuously and periodically checks the update server. It can also be triggered manually or by the Update Pushing mechanism.
aasnmpd	aasnmpd accepts SNMP GET and SET messages related to Ad-Aware registry keys. Thus, an authorized user is able to read and modify some of the Ad-Aware configuration settings remotely.

Ad-Aware Security for Samba Templates

The Ad-Aware Security for Samba policy templates allow you to create policies that you can use in order to manage Ad-Aware Security for Samba. By using these policies you can ensure your organization's file servers are secure.

Note

In this chapter you can find out what settings and parameters each template allows you to configure and manage. To find out how to create and manage policies, please refer to Policies.

These are the available policy templates for Ad-Aware Security for Samba:

File logging policy

Allows creating file logging policies for Ad-Aware Security for Samba

Mail alerts policy

Allows creating mail alerts policies for Ad-Aware Security for Samba

Samba protocol policy

Allows creating Samba protocol policies for Ad-Aware Security for Samba

Update settings policy

Allows creating update settings policies for the Ad-Aware Security for Samba

File Logging Policy

This policy template allows you to create file logging and log rotate policies for Ad-Aware Security for Samba.

The settings are organized into 2 sections:

- File Logging - allows you to configure file logging policies for the v Security for Samba.

- Log Rotate - allows you to rotate the logs according to several criteria.

File Logging

This is where you can enable file logging.

For each rule you can select the component (daemon) it applies to, the message type and the location of the log file. For more information on each type of daemon, please refer to Core Modules.

The message types for the modules above can take the following values: info, error, license, debug, virus, spam, cf and scanning.

Let's say you enable the **Error messages** for a component (daemon) rule. This means that all error-related information, coming from all Ad-Aware daemons, will be found in this location: /var/log/error.log. Of course, you can easily modify the location by editing the **Log File** text box.

If you want to create a new policy, select the component (daemon) it applies to and the message type from the corresponding drop-down lists, type the location of the file into the **Log File** text box and click **Finish**.

Log Rotate

This policy template is useful when you have to manage systems that generate large numbers of log files. **Log rotate** allows the automatic rotation of the log files according to the following criteria:

- Rotate interval: the log files may be rotated by hour, day, week or month.
- Rotate log size: the log files may be rotated when they reach a certain size.
- Rotate entries: the log files may be rotated taking into consideration the number of entries.
- Rotate count: how many times the log files are rotated before starting to delete the old files.

Mail Alerts Policy

This policy template allows you to create policies for mail alerts of Ad-Aware Security for Samba.

Mail alerts are simple e-mail messages sent by Ad-Aware to the system administrator to inform him or her about special events or to the partners of an e-mail communication to inform them about malware found.

If you want to add a new rule, select the component it applies to and the rule type from the corresponding drop-down lists, type the e-mail address(es) the alerts should be sent to and click **Finish**. For more information on each type of daemon, please refer to Core Modules.

Samba Protocol Policy

This policy template allows you to create Samba protocol policies for Ad-Aware Security for Samba.

Ad-Aware Security for Samba offers protection against viruses, spyware and riskware. It detects infected or suspect messages and attempts to disinfect them or isolates the infection, according to the specified actions.

Antivirus Actions

The actions are ordered in a list according to their priority. Click the desired action in order to move it up.

The selected actions which appear at the top of the list in red will apply according to their order.

Select the actions to be taken on **viruses**, **suspected objects** and **riskware**:

Disinfect

Remove the malware code from the requested infected files before delivery.

Disinfection may fail in some cases, such as when the infected file is inside specific mail archives.

Delete

Immediately remove infected files from the disk, without any warning.

Deny

Deny users' access to the requested files if Ad-Aware detects them to be suspect.

Move to Quarantine

Move suspect files from their original location to the **Samba Quarantine** folder.

Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.

Copy to Quarantine

Copy the infected file to the **Samba Quarantine** folder.

Ignore

Simply ignore the infected files.

Warning

Do not set Ignore as the first action in the list. Doing this will allow users to download and upload ALL infected files.

Extensions

This is where you can set what kind of files are to be scanned, according to their file extensions. You have three options to choose from, using the corresponding radio button.

All

All files will be scanned, regardless of their file extensions.

Custom

Only the files ended with the file extensions you have typed into the text box will be scanned. The file extensions must be separated by semicolon (;).

Executable

Only the executable files will be scanned.

Maximum File Size

The **Maximum File Size** represents the maximum size (in bytes) of the files that will be considered by the Samba integration agent.

You can type a number into the corresponding text box, to set a size limit for files scanning.

Virus risk

If a file's size surpasses the limit you have set, the respective file will not be scanned for viruses or other threats.

When the value is 0, no size limit is enforced. All the files, regardless of their size, will be scanned.

Update Settings Policy

This policy template allows you to create policies for configuring the update settings for Ad-Aware Security for Samba. You can configure automatic product updates, update locations and proxy settings.

Here you can configure update settings that will be applied on the assigned clients.

The settings are organized into 3 sections:

- Live! Update
- Insecure Update
- Proxy Settings

Click › to expand a section and see all configurable settings. To collapse a section and hide all settings click ⌄.

Live! Update

The Live! Update window provides information regarding the general update settings and update status.

The default update server is http://definitionsbd.lavasoft.com and the default update interval is 1 hour. To use a different server or set a different time interval between updates, enter the new information in the corresponding text box.

PushUpdate is an ordered update launched by Ad-Aware servers in imminent situations, when a prompt update can save the server from allowing the infected e-mails to pass.

If a proxy server is used to connect to the Internet, select the **Use Proxy** check box.

Insecure Update

If you want to use a different update server, select this option to allow updates from a local server to be installed.

Proxy Settings

This is where you can enter the proxy server settings.

Enter the server address and port in the corresponding text box. If authentication is required, you also have to enter the user name, password and domain in the corresponding text boxes.

Core Modules

Ad-Aware Security for Samba is a highly complex modular structure. It is made up of several central components and additional modules, each of them having assigned a specific task. The modules are loaded during Ad-Aware startup and enabled or not, according to the user's preferences. On a UNIX-like system, these components run as daemons, on one or multiple threads, and communicate with the others. Listed by their file names, the core modules are represented in the following table.

Module	Description
aamond	The Ad-Aware Core Monitor is the supervisor of several Ad-Aware modules. When one of them crashes, the Core Monitor isolates the object causing the crash in a special quarantine directory, notifies the administrator and restarts the involved module. Thus, even if one process dies, the whole filtering activity is not disturbed, ensuring continuous server protection.
aascand	This is the Ad-Aware Scan Daemon. Its purpose is to integrate the scanning engines, receive scanning requests from several daemons, such as the mail daemon or the file daemon. It scans the objects, takes the necessary actions and sends back the object and the scanning results.
aaemclientd	The Ad-Aware Enterprise Manager Client acts as a link between Ad-Aware Management Server and Ad-Aware Security for Samba. It allows the security product to interpret the policies sent by Ad-Aware Management Server.
aamagentd	The Ad-Aware Enterprise Manager Agent enables communication between Ad-Aware Management Server and the Ad-Aware products it manages.
aafiled	The Ad-Aware File Daemon has the role of receiving scanning requests from the Samba Virtual Filesystem module. It calls the Scan Daemon to perform the scan, expecting the scanning results from it. Then it applies his actions and sends back the results to Samba.
aalogd	The Ad-Aware Logger is a complex component, handling all logging and notification actions of Ad-Aware. There are several types of logging, all of them realized by plugins. • File logging: the data is sent to a normal log file, respecting a typical format. • Mail notification: alerts are sent by e-mail to the server administrator or to the sender

	and the recipients of an e-mail, on special events (such as infected e-mail found). • Real Time Virus and Spam Report: anonymous statistics are sent to Ad-Aware Labs to keep a map of malware activity and to detect outbreaks.
aalived	The Ad-Aware Live Update is the module responsible with updating the scanning engines and some other Ad-Aware components. The module runs continuously and periodically checks the update server. It can also be triggered manually or by the Update Pushing mechanism.
aasnmpd	aasnmpd accepts SNMP GET and SET messages related to Ad-Aware registry keys. Thus, an authorized user is able to read and modify some of the Ad-Aware configuration settings remotely.

Ad-Aware Update Server

What Is Ad-Aware Update Server?

Ad-Aware Update Server allows you to set up an Ad-Aware update location within the local network. Having a local update location, you can configure update policies and assign them to clients so that the Ad-Aware products update from this local mirror instead of updating from the Internet.

By using a local Ad-Aware update location, you can reduce Internet traffic (only one computer connects to the Internet to download updates) and achieve faster updates. Moreover, you do not have to worry about updating the Ad-Aware products installed on computers that are not connected to the Internet.

Ad-Aware Update Server is completely automated. In order to update the client products from the local network, you only have to install Ad-Aware Update Server and assign policies for the client products to update from the local update server.

Once installed, Ad-Aware Update Server automatically downloads the updates for the Ad-Aware Business Client products available in the installation package (both the 32-bit and 64-bit version). Moreover, when other client products request updates (for example, a Ad-Aware server security solution or an Ad-Aware Business Client product in a different language), Ad-Aware Update Server automatically downloads updates for those clients.

The local update address that must be configured on the Ad-Aware client products must follow one of these syntaxes:

- `http://update_server_ip:port`
- `http://update_server_name:port`

The default port is `7074`. Configure and assign update policies using such an update location to set the Ad-Aware client products to update from the local mirror.

Configuration and Management

Refer to the following topics to find out how to configure and manage an Ad-Aware update location in the local network using Ad-Aware Update Server.

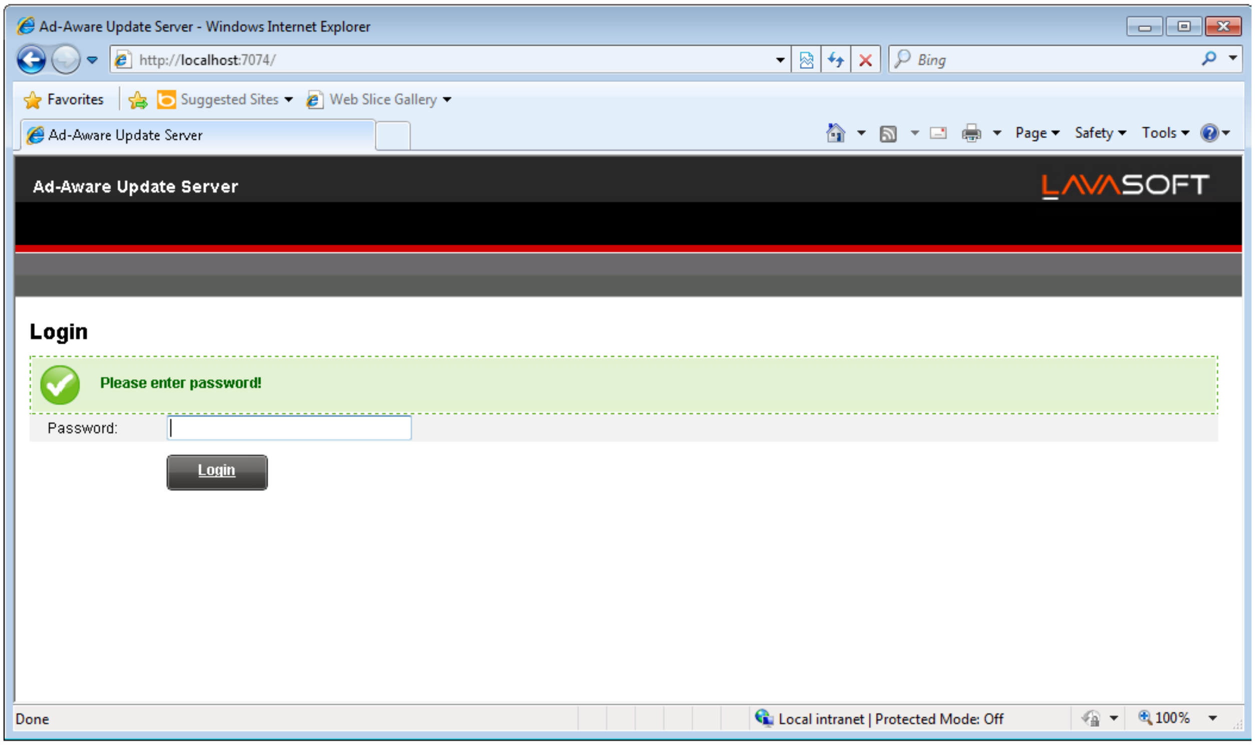
- Accessing Management Panel
- What You Have to Do After Installation
- Managing Client Products and Downloaded Updates
- Configuring Settings
- Changing Login Password

Accessing Management Panel

Ad-Aware Update Server has a web-based interface, which facilitates easy configuration and monitoring from any computer connected to the network.

To access the Ad-Aware Update Server management panel, do any of the following:

- Open a web browser and type the server address using one of these syntaxes:
  - `http://update_server_ip:port`
  - `http://update_server_name:port`
- On the computer on which the Ad-Aware Update Server is installed, go to the Windows Start menu and follow the path: **Start – Programs** - **Ad-Aware Management Server** - **Ad-Aware Update Server**.



Login

Please enter password!

Password:

Login

Login Page

Type the login password in the corresponding field and click **Login**. The default password is `admin`.

What You Have to Do After Installation

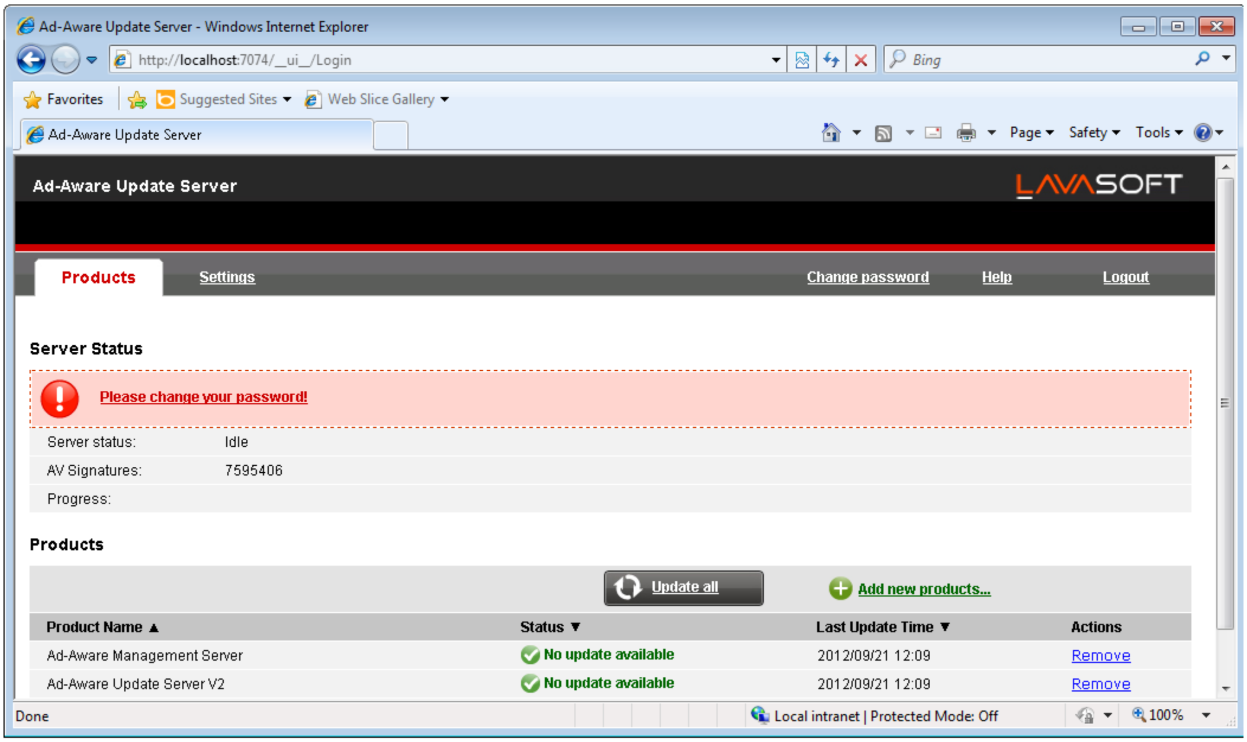
This is what you have to do after installation:

1. Change the default `admin` password to prevent unauthorized access. For more information, please refer to Changing Login Password.
2. If the computer on which Ad-Aware Update Server is installed connects to the Internet through a proxy server, you must configure the proxy settings.
   a) Access the Ad-Aware Update Server management panel.
   b) Click **Settings** in the upper menu.
   c) Select the **Use proxy settings** check box.
   d) Specify the proxy settings to be used. For more information, please refer to Configuring Settings.
3. Configure the client products installed in the network to download updates from the local update server. The local update address that must be configured on the Ad-Aware client products must follow one of these syntaxes:
   - `http://update_server_ip:port`
   - `http://update_server_name:port`

The default port is `7074`. Configure and assign update policies using such an update location to set the Ad-Aware client products to update from the local mirror.

Managing Client Products and Downloaded Updates

To manage the client products for which updates are downloaded and to see update information, access the management panel, the **Products** page (displayed by default after logging in).



Server Status

Please change your password!

Server status:	Idle
AV Signatures:	7595406
Progress:	

Products

Product Name ▲	Status ▼	Last Update Time ▼	Actions
Ad-Aware Management Server	✓ No update available	2012/09/21 12:09	Remove
Ad-Aware Update Server V2	✓ No update available	2012/09/21 12:09	Remove

Products Page

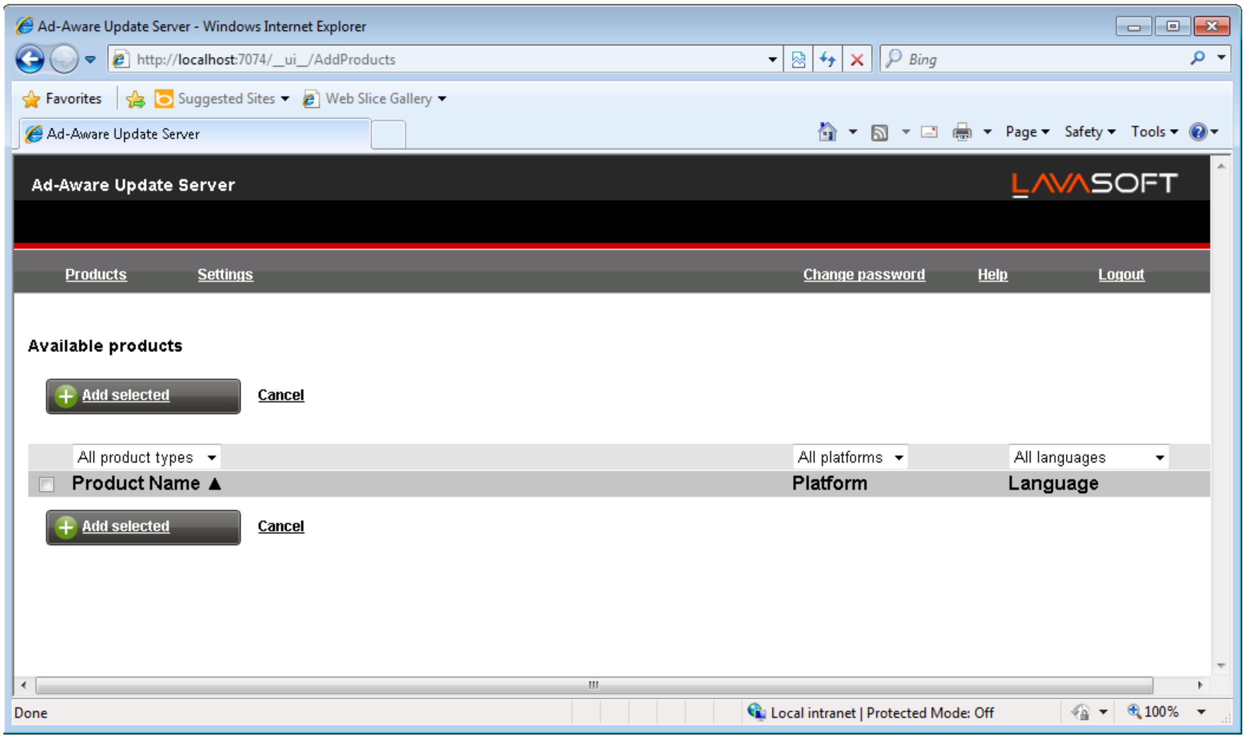
You can see Ad-Aware Update Server statistics and the list of client products for which updates are downloaded. The status and time of each client product's latest update are displayed.

Downloading Latest Updates

To download the updates available for all the products in the list, click **Update all.**

Adding New Products

To select additional products to be updated by Ad-Aware Update Server, click **Add new products**. A new page is displayed.



Available Products

You can see the list of additional Ad-Aware client products that can be updated using Ad-Aware Update Server. To browse easily through the list, you can filter products by type, platform and language.

Select the check box corresponding to the desired products and click **Add selected**.

Removing Products

To remove a product from the list of updated products, click the corresponding **Remove** link in the **Actions** column. When you remove a client product from the list:

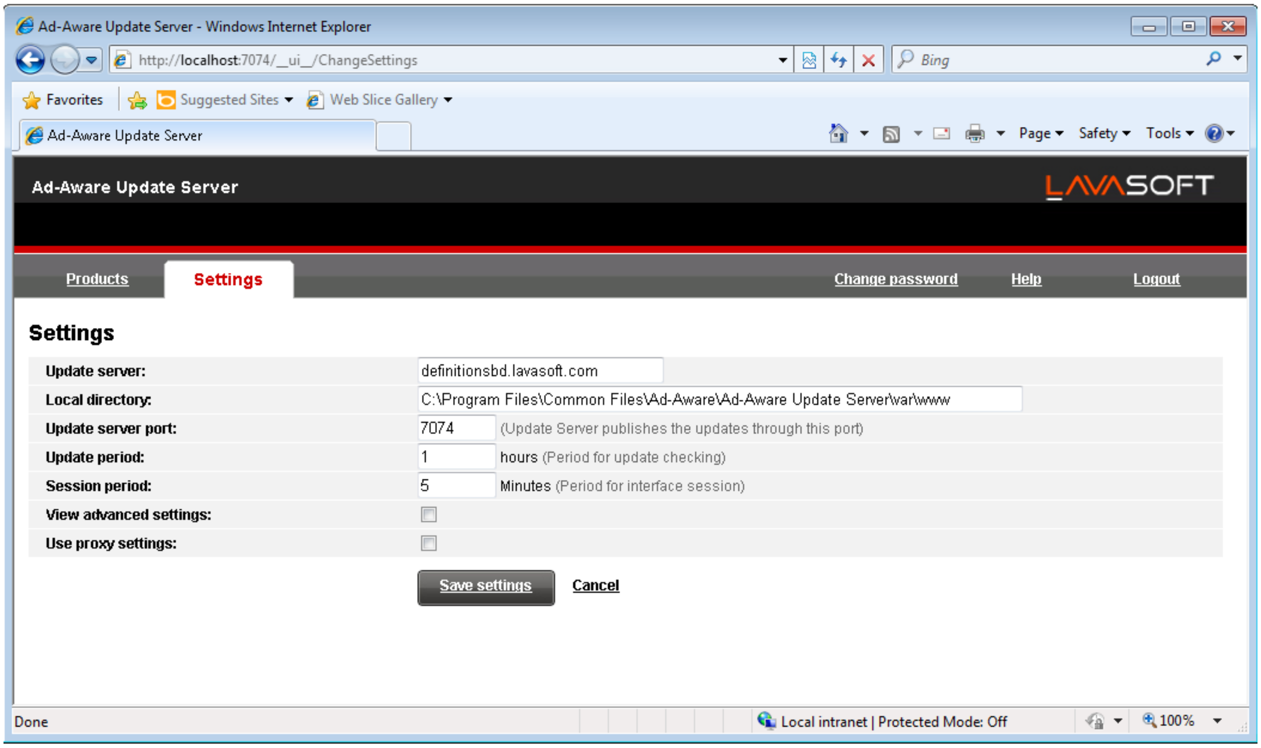
1. Ad-Aware Update Server will no longer download updates for that client product.

   However, if the client product later connects to Ad-Aware Update Server to check for updates, it will be automatically added to the list.

2. The updates downloaded for that client product are removed if they are not used by another product in the list. For example, malware signatures are common to all language versions of a specific product and platform (32-bit or 64-bit).

Configuring Settings

To configure the Ad-Aware Update Server settings, access the management panel and click Settings in the upper menu. A new page is displayed.



Settings

Update server:	definitionsbd.lavasoft.com
Local directory:	C:\Program Files\Common Files\Ad-Aware\Ad-Aware Update Server\var\www
Update server port:	7074 (Update Server publishes the updates through this port)
Update period:	1 hours (Period for update checking)
Session period:	5 Minutes (Period for interface session)
View advanced settings:	□
Use proxy settings:	□

Save settings Cancel

Settings Page

The following settings can be configured:

- **Update server**. By default, Ad-Aware Update Server will download updates on the local computer from http://definitionsbd.lavasoft.com:80 . This is a generic address that is automatically resolved to the closest server that stores Ad-Aware malware signatures in your region.

To check for and download updates from a local update server (cascading configuration), replace the Internet update address with the address of the local update server. Use one of these syntaxes:

- `http://update_server_ip:port`
- `http://update_server_name:port`

The default port is 7074.

- **Local directory**. If you want to change the folder the updates are downloaded to, type the path to the new folder in this field.
- **Update server port**. In this field you can change the Ad-Aware Update Server port configured during installation. The default port is 7074. The Ad-Aware Update Server port must not be used by other applications installed on the system.

  Note

  If you change the port at a time when Ad-Aware Update Server is already in use, the update location of all Ad-Aware products configured to download updates from the local update server must be changed accordingly.

- **Update period**. By default, Ad-Aware Update Server downloads updates from the Internet update location every hour. If you want to change the update period, type a new value in this field.
- **Session period**. By default, you are automatically logged out of the management panel after 5 minutes of inactivity. If you want to change the maximum allowed period of inactivity, type a new value in this field. You can set this period between 1 and 30 minutes.
- **View advanced settings**. Select this check box to view and configure advanced settings.
  - **Gateway roles**. Ad-Aware Update Server can act as gateway for data sent by the Ad-Aware client products installed in the network to the Ad-Aware servers. This data may include anonymous reports regarding virus and spam activity, product crash reports and data used for online registration. Enabling the gateway roles is useful for traffic control and in networks with no Internet access.

    Note

    You can disable the product modules that send statistical or crash data to Ad-Aware Labs anytime you want. You can use policies to remotely control these options on the computers managed by Ad-Aware Management Server.

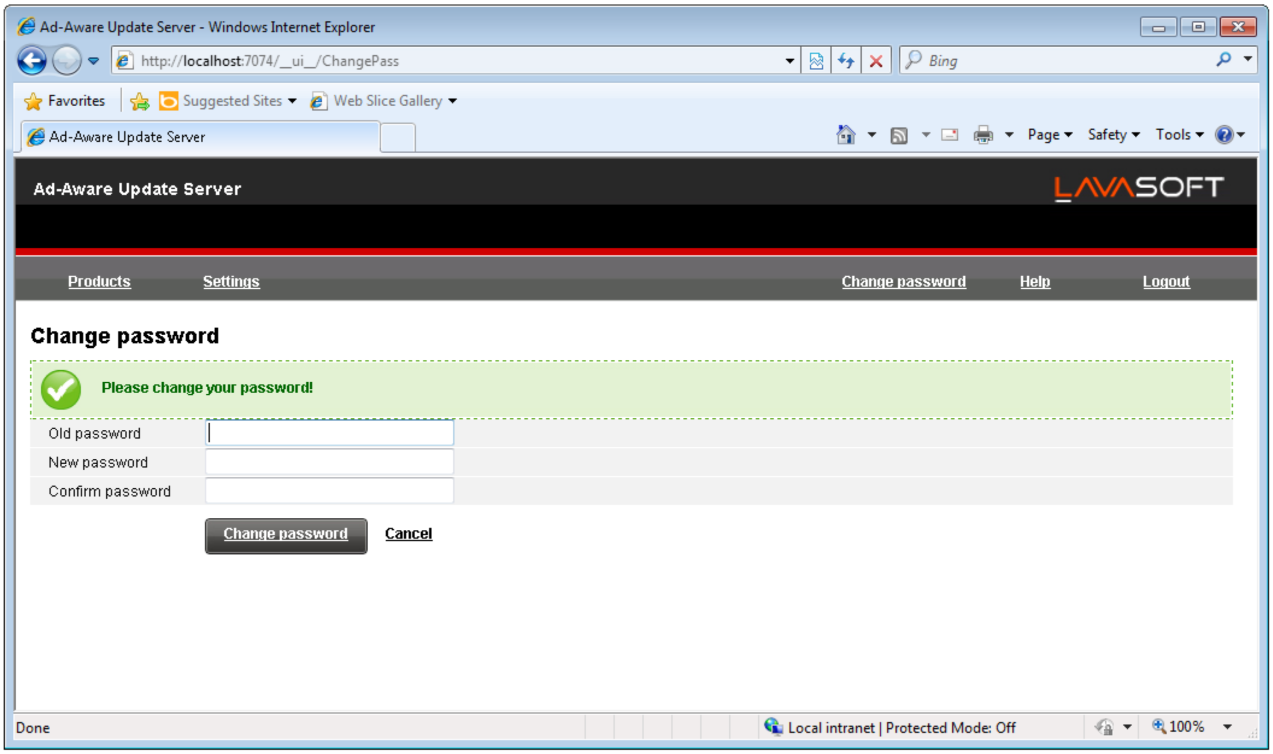
  - **Download not-selected locations**. Ad-Aware Update Server automatically downloads updates for any Ad-Aware client product that requests them (even if you have not selected that product in the *Products* page). If you want only updates for the authorized products to be downloaded, clear this check box.
  - **Allow update for unused products**. Ad-Aware Update Server checks for and downloads updates regularly for all Ad-Aware products that request updates. If you want to stop downloading updates that have not been requested for some time, clear this check box and specify the inactivity period.
- **Use proxy settings**. Select this check box if your company connects to the Internet through a proxy. You must fill in the following fields:
  - **Proxy Address** - type in the IP address of the proxy server
  - **Proxy Port** - type in the port used to connect to the proxy server
  - **Proxy Username** - type in a user name recognized by the proxy
  - **Proxy Password** - type in the valid password of the previously specified user

If you select **Use proxy cache**, Ad-Aware Update Server will first check the proxy server's cache for recently downloaded updates and will use such updates, if available. This option is not recommended, but it may be useful if you pay your Internet connection for traffic.

Click **Save** settings to save the changes.

Changing Login Password

To change the login password, access the management panel and click **Change Password** in the upper menu. A new page is displayed.



Change password

Please change your password!

Old password	
New password	
Confirm password	

Change Password Page

You must fill in the following fields:

- **Old password** - type in the old password.
- **New password** - type in the new password.
- **Confirm password** - type in the new password again.

Click **Change password** to change the password.

Cascading Configuration

You can set up Ad-Aware local update servers to download Ad-Aware updates from another local update server instead of the Internet. This particular configuration is known as cascading configuration.

Cascading configuration is generally used in geographically distributed computer networks, when one of the following conditions applies:

- Only the central network has direct Internet access (the other networks may connect through the central network or they may not have Internet access at all).
- The connection to the central network is faster (or more convenient in some other way) than the direct Internet connection.

To set up a cascading configuration:

1. Install and set up the local update server that will download Ad-Aware updates from the Internet. No special configuration is required for this update server to allow distribution of Ad-Aware updates to other local update servers (updates are automatically available to both Ad-Aware clients and other local update servers, provided they are properly configured).
2. Configure the update servers in the isolated networks to download updates from the main update server. This is what you have to do:
   a. Access the management panel and click **Settings** in the upper menu.
   b. In the **Update Server** field, replace the Internet update address with the address of the local update server that downloads updates from the Internet. Use one of these syntaxes:
      - `http://main_update_server_ip:port`
      - `http://main_update_server_name:port`

      The default port is `7074`.
   c. Make sure the update servers can communicate. The easiest way to test this is to go to the *Products* page, add a new product to the list and start an update. If the update cannot be performed, check your network and firewall configurations.
3. There are no changes in how you configure the Ad-Aware client products to update from their local update server.

Getting Help

Support

Ad-Aware strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issues or if you have any question about your Ad-Aware product; go to our online Support Center. It provides several resources that you can use to quickly find a solution or an answer. Or, if you prefer, you can contact the Ad-Aware Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

Note

You can find out information about the support services we provide and our support policy at the Support Center.

Ad-Aware Support

You can get assistance with your issue by emailing Business Support.

You can use several resources to quickly find a solution or an answer:

- Ad-Aware Business Support
- Ad-Aware Business Manuals

You can also use your favorite search engine to find out more information about computer security, the Ad-Aware products and the company.

Ad-Aware Business Support

The Ad-Aware Business Support provides Ad-Aware users with an easy way to get help. You can email any problem or question related to your Ad-Aware product.

The Ad-Aware Business Support is available at businesssupport@lavasoft.com.

Ad-Aware Business Manuals

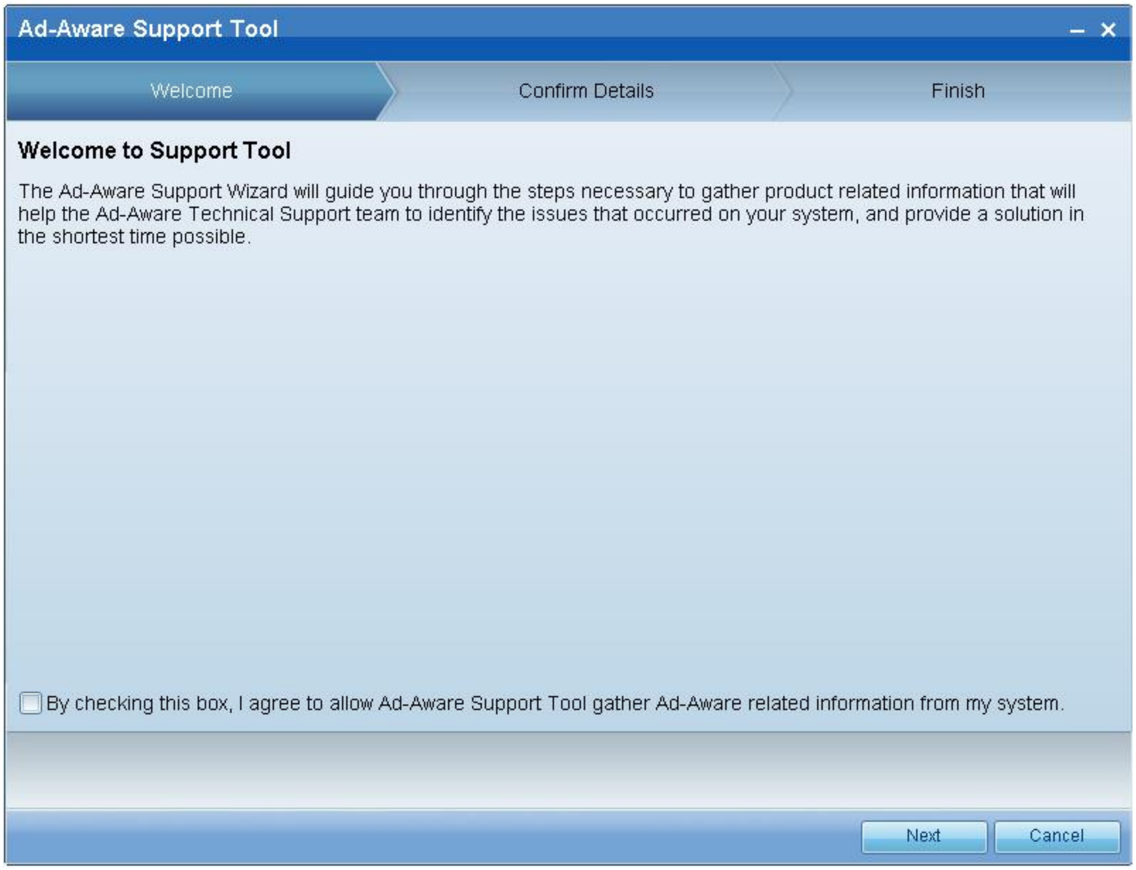
Product documentation is the most complete source of information about your product. You can check and download the latest version of documentation for Ad-Aware Business products at http://www.lavasoft.com/mylavasoft/support/supportcenter/product_manuals.

Ad-Aware Support Tool

The Ad-Aware Support Tool creates a zip archive of files required by our support technicians to troubleshoot Ad-Aware Management Server.

To use the Support Tool, follow these steps:

1. Open the Ad-Aware Support Tool by following the path: **Start Menu** - **All Programs** - **Ad-Aware Management Server** - **Ad-Aware Support Tool**.



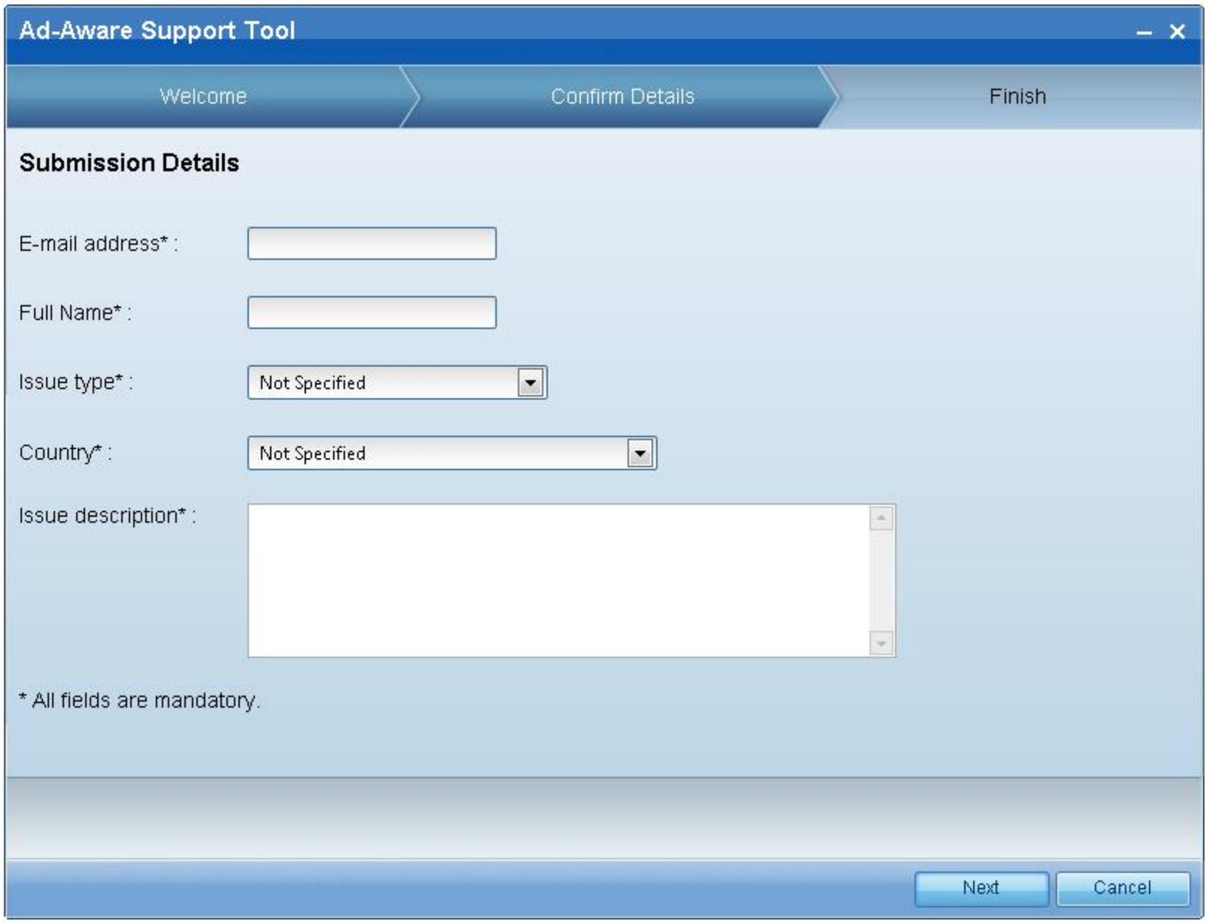
Welcome to Support Tool

The Ad-Aware Support Wizard will guide you through the steps necessary to gather product related information that will help the Ad-Aware Technical Support team to identify the issues that occurred on your system, and provide a solution in the shortest time possible.

□ By checking this box, I agree to allow Ad-Aware Support Tool gather Ad-Aware related information from my system.

Ad-Aware Support Tool

2. Select the agreement check box and click **Next**.



Submission Details

E-mail address* :

Full Name* :

Issue type* : Not Specified

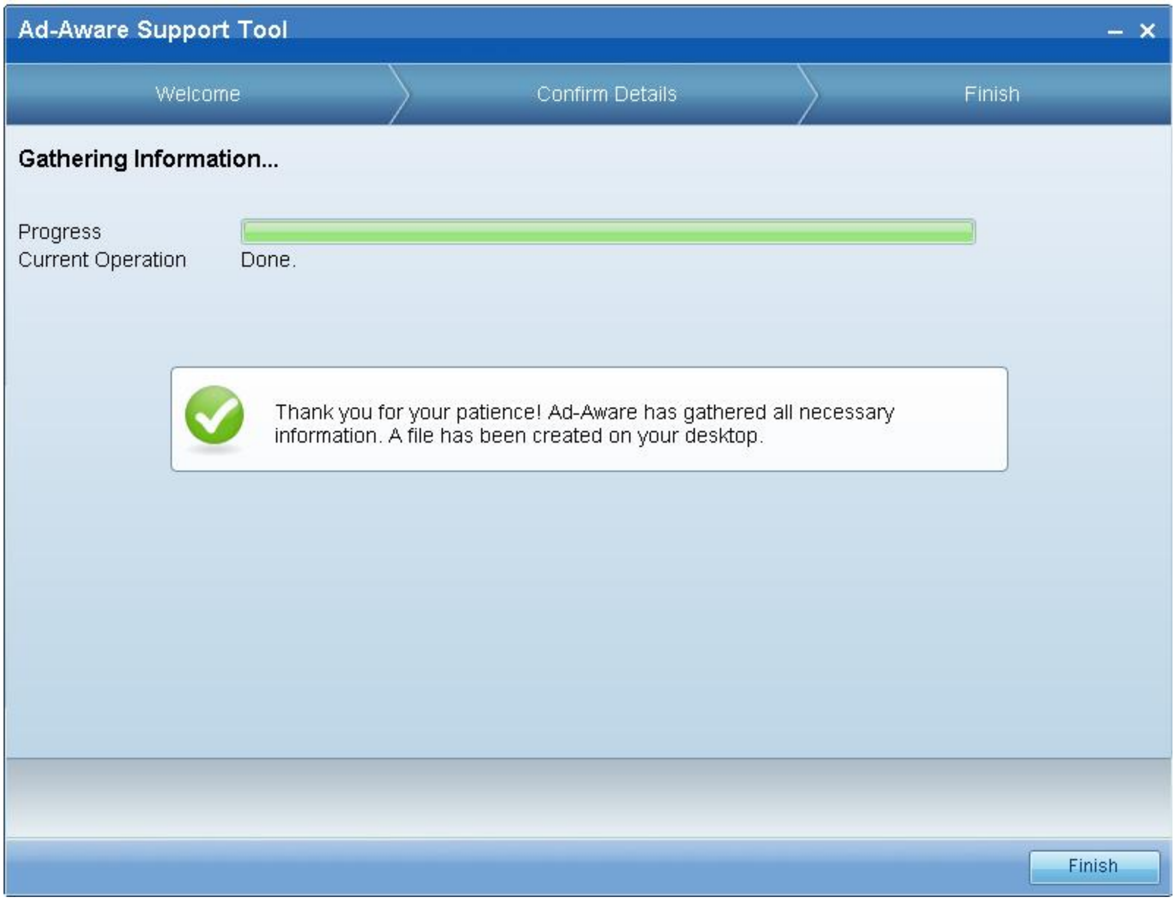
Country* : Not Specified

Issue description* :

* All fields are mandatory.

Submission Details

3. Complete the submission form with the necessary data:
    a. Enter your e-mail address.
    b. Enter your name.
    c. Choose from the corresponding menu the type of issue you have encountered.
    d. Choose your country from the corresponding menu.
    e. Enter a description of the issue you encountered.
4. Click **Next**. The Support Tool gathers product information, information related to other applications installed on the machine and the software and hardware configuration.
5. Wait for the process to complete.



Gathering Information...

Progress

Current Operation Done.

Thank you for your patience! Ad-Aware has gathered all necessary information. A file has been created on your desktop.

Finish

A zip archive has been created on your desktop. Click **Finish** to close the window.

You can send the zip archive together with your request for support in order to reduce the time needed to resolve the query.

Contact Information

Efficient communication is the key to a successful business. During the past 11 years Ad-Aware has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

Appendices

Available Network Tasks

This appendix provides a detailed description of the network management tasks provided by Ad-Aware Management Server (known as WMI scripts in earlier versions). Networks tasks are organized into the following categories:

- Desktop Management
- Processes
- Files and Folders
- Disk and File Systems
- Computer Hardware
- Operating Systems
- Accounts and Domains
- Computer Software
- Networking
- Services
- WMI Service

Desktop Management

Computer restart

Restarts client workstations

Computer shutdown

Shuts down client workstations

Enumerate startup programs

Provides information about all the programs that run on client workstations at startup

List startup info

Provides information on the startup of client workstations

List startup menu

Lists the program shortcuts from the Start menu of client workstations, the entries are grouped by user

Remote Desktop Connection

Changes the Windows settings on client workstations in order to allow or block incoming remote connections through Remote Desktop Connection

Run program

Runs a specific application on client workstations, the application can be located on the target workstation or on the local machine (where the Ad-Aware Management Console is installed).

Send message

Sends a message to the user logged on client workstations

For Windows 2000 workstations, the task uses the `net send` command and requires the **Messenger** service to be started (default setting). For other Windows workstations, the task uses the msg command and requires the **Terminal Services** service to be started (default setting)

Processes

Current processes

Provides information on the processes currently running on client workstations

Kill process

Ends a specific process running on client workstations, the **Current Processes** script can be used to obtain the list of running processes

Files and Folders

Current shares

Provides information about the existing shares on client workstations

Disk and File Systems

Enable/Disable autorun for all drives

Enables or disables the Windows Autorun feature for all drives on client workstations, Autorun enables automatic detection and reading of new media

Enable/Disable USB mass storage

Enables or disables USB storage devices on client workstations, such devices include USB memory sticks (flash pens) and mp3 players

Free disk space

Provides the list of the logical disks on client workstations and the available disk space on each of them

List logical disk info

Provides information about the logical disks (floppy drive, hard-disk drives, CD-ROM drive etc) on client workstations

This includes:

- name (label)
- description
- free disk space
- size

Computer Hardware

Enumerate memory

Provides the size of the physical (RAM) memory installed in client workstations

Enumerate pagefile

Provides information about the virtual memory (the page file) available on client workstations

This includes:

- the location and size of the page file
- the initial and the maximum size

List CPU info

Provides various information about the processor of client workstations

This includes:

- processor name and ID
- description
- manufacturer
- clock speed

List MB settings

Provides information about the motherboard of client workstations

This includes:

- name
- manufacturer
- serial number

List monitor settings

Provides information about the monitor of client workstations

This includes:

- monitor type
- manufacturer
- physical dimensions

List video info

Provides various information regarding the video display of client workstations

This includes:

- video adapter name and type
- graphics memory
- resolution
- driver name and version
- minimum and maximum refresh rates

Operating Systems

Get last SP installed

Provides the version of the Windows Service Pack installed on client workstations

Get system info

Provides useful information about client workstations

This includes:

- operating system information
- system name, model and manufacturer
- total RAM memory
- processor
- BIOS version

Install Windows updates

Helps you identify the Windows updates available for client workstations and install all or specific Windows updates on client workstations

List hotfix

Provides information about the Microsoft and Windows hotfixes installed on client workstations

Operating system

Provides useful information about the operating system running on client workstations

This includes:

- operating system and version
- registered user
- serial number
- installation time

Windows automatic updating

Configures Windows Automatic Updates on client workstations, Windows Automatic Updates helps users keep their operating system up-to-date

Accounts and Domains

List current users

Lists the users currently logged on to client workstations

List domain and workgroup info

Provides information on the domain or workgroup client workstations are part of

List local users

Provides information about the local Windows user accounts configured on client workstations

List logon session info

Provides information regarding the logon session on client workstations

Log off user

Logs off the current user logged on to client workstations

Computer Software

List installed software

Provides the list of all software and Microsoft and Windows updates installed on client workstations

An uninstall command line is provided for each application or update.

You can remove an application using this command line with a **Remove Software** script

Remove software

Removes a specific application installed on client workstations, the script can be used to remove any application that appears in the **Add or Remove Programs** applet in the Control Panel

Networking

List network adapter values

Provides detailed information about the network adapters installed in client workstations

This includes:

- adapter type
- manufacturer
- MAC and network address

Services

List services

Provides various information regarding the services running on the client workstation

This includes:

- service name and display name
- state (stopped / running)
- start mode (automatic / manual / disabled)
- description

WMI Service

List WMI settings

Provides information about the WMI settings of client workstations

Available Report Templates

This appendix provides a detailed description of the built-in report templates. The templates are grouped based on the client product they apply to. These are the available categories:

- Global Reports (for all client products)
- Ad-Aware Management Server Reports
- Ad-Aware Business Client Reports
- Ad-Aware Antivirus for Mac Reports (only if the product is installed in the network and integrated with Ad-Aware Management Server)
- If you have installed the Ad-Aware Security for Windows Servers add-on:
  - Ad-Aware Security for File Servers Reports
  - Ad-Aware Security for Mail Servers Reports
  - Ad-Aware Security for Exchange Reports
  - Ad-Aware Security for SharePoint Reports
- If you have installed the add-on for the Ad-Aware solutions for Unix-based servers:
  - Ad-Aware Security for Samba Reports
  - Ad-Aware Security for Mail Servers (Unices) Reports

Note

For more information about the add-ons, please refer to Integration of the Ad-Aware Solutions for Server Systems.

Common Reports for Windows Products

The report templates presented here are common to Ad-Aware Business Client and to all Ad-Aware Security for Windows Servers solutions. You can create product-specific reports or global reports that consolidate data from all these client products.

Installation Report - Ad-Aware Installed Products

Shows the Ad-Aware products installed on the selected computers

Installation Report - Installation or Deployment Errors

Shows the errors that appeared during installation or deployment processes

Policy Report - Policy Status

Shows the status of the policies assigned to the selected computers

Update Report - Antivirus Signatures Update Status

Shows the update status of the antivirus signatures

Update Report - Computers Not Updated

Shows the computers that do not have the latest antivirus signatures

Update Report - Computers with Outdated Products

Shows the computers that have older versions of Ad-Aware products

Update Report - Product Update Status

Shows the update status for the Ad-Aware products installed

Global Reports

The global malware reports consolidate information from Ad-Aware Business Client and Ad-Aware Security for File Servers. The global auto-deployment installation reports consolidated information from Ad-Aware Management Agent and Ad-Aware Business Client. For complete information, also check Common Reports for Windows Products.

Administrative Report - Offline Computers

Shows the computers that appear to be offline or inactive

A computer is considered offline or inactive if it has not synchronized for more than 1 day (by default). Such computers may be disconnected from the network (mobile employees, telecommuters) or a firewall may block their synchronization with the server.

Installation Report - Autodeployment Errors

Shows the errors that appeared during the autodeployment process

Installation Report - Autodeployment History

Shows the deployments performed by autodeployment process over a period of time

Malware Report - Malware Progress over Time

Shows the number of malware detected over a period of time

Malware Report - Malware Still Present

Shows the malware that was not cleaned

Malware Report - Most Active Threats

Shows Top 10 malware by number of infected objects

Malware Report - Most Infected Computers

Shows Top 10 computers by number of malware detections

Malware Report - On-Access Detections

Shows the malware detected by the on-access scan

Malware Report - On-Demand Detections

Shows the malware detected by the on-demand scans

Malware Report - Password Protected Only

Shows password-protected archives detected during scans, such archives cannot be scanned for malware

Ad-Aware Management Server Reports

Administrative Report - Offline Computers

Shows the computers that appear to be offline or inactive

A computer is considered offline or inactive if it has not synchronized for more than 1 day (by default). Such computers may be disconnected from the network (mobile employees, telecommuters) or a firewall may block their synchronization with the server

Installation Report - Ad-Aware Installed Products

Shows the Ad-Aware products installed on the selected computers

Installation Report - Installation or Deployment Errors

Shows the errors that appeared during installation or deployment processes

Policy Report - Policy Status

Shows the status of the policies assigned to the selected computers

Update Report - Computers with Outdated Products

Shows the computers that have older versions of Ad-Aware products

Update Report - Product Update Status

Shows the update status for the Ad-Aware products installed

Ad-Aware Business Client Reports

For complete information, also check Common Reports for Windows Products.

Anti-spam Report - Anti-spam Progress

Shows the percentage of spam e-mails detected over a period of time

Anti-spam Report - Top Spam Senders

Shows Top 10 e-mail addresses from which the most spam e-mails were received

Detected Phishing

Shows information about the detected phishing attempts

Firewall Report - Computers with Firewall Disabled

Shows the computers that have the Ad-Aware Firewall module disabled

Installation Report - Autodeployment Errors

Shows the errors that appeared during the autodeployment process

Installation Report - Autodeployment History

Shows the deployments performed by autodeployment process over a period of time

Malware Report

Shows the malware detected on the selected computers

Malware Report – Ad-Aware AVC Detections

Shows the applications suspected by Ad-Aware Active Virus Control to perform malware activity

Malware Report - Malware Progress over Time

Shows the number of malware detected over a period of time

Malware Report - Malware Still Present

Shows the malware that was not cleaned

Malware Report - Most Active Threats

Shows Top 10 malware by number of infected objects

Malware Report - Most Infected Computers

Shows Top 10 computers by number of malware detections

Malware Report - On-Access Detections

Shows the malware detected by the on-access scan

Malware Report - On-Demand Detections

Shows the malware detected by the on-demand scans

Malware Report - Password Protected Only

Shows password-protected archives detected during scans. Such archives cannot be scanned for malware

User Control Report - Blocked Applications

Shows the applications and web pages by the User Control module

Ad-Aware Antivirus for Mac Reports

Malware Report

Shows the malware detected on the selected computers

Malware Report - Malware Progress over Time

Shows the number of malware detected over a period of time

Malware Report - Malware Still Present

Shows the malware that was not cleaned

Malware Report - Most Active Threats

Shows Top 10 malware by number of infected objects

Malware Report - Most Infected Computers

Shows Top 10 computers by number of malware detections

Malware Report - On-Access Detections

Shows the malware detected by the on-access scan

Malware Report - On-Demand Detections

Shows the malware detected by the on-demand scans

Ad-Aware Security for File Servers Reports

For complete information, also check Common Reports for Windows Products.

Malware Report - Malware Progress over Time

Shows the number of malware detected over a period of time

Malware Report - Malware Still Present

Shows the malware that was not cleaned

Malware Report - Most Active Threats

Shows Top 10 malware by number of infected objects

Malware Report - Most Infected Computers

Shows Top 10 computers by number of malware detections

Malware Report - On-Access Detections

Shows the malware detected by the on-access scan

Malware Report - On-Demand Detections

Shows the malware detected by the on-demand scans

Malware Report - Password Protected Only

Shows password-protected archives detected during scans. Such archives cannot be scanned for malware

Ad-Aware Security for Mail Servers Reports

For complete information, also check Common Reports for Windows Products.

Mail Servers Attachment Filtering Report

Shows the attachment filtering data in real time

Mail Servers Content Filtering Report

Shows the content filtering data in real time

Mail Servers Malware Report

Shows the email malware data in real time

Mail Servers Spam Report

Shows the spam data in real time

Ad-Aware Security for Exchange Reports

For complete information, also check Common Reports for Windows Products.

Exchange Attachment Filtering Report

Shows the attachment filtering data in real time

Exchange Content Filtering Report

Shows the content filtering data in real time

Exchange Malware Report

Shows the email malware data in real time

Exchange Spam Report

Shows the spam data in real time

Ad-Aware Security for SharePoint Reports

For complete information, also check Common Reports for Windows Products.

SharePoint Malware Report

Shows the malware data in real time

Ad-Aware Security for Samba Reports

Installation Report - Ad-Aware Installed Products

Shows the Ad-Aware products installed on the selected computers

Installation Report - Installation or Deployment Errors

Shows the errors that appeared during installation or deployment processes

Samba Malware Report

Shows threats in real time

Samba Traffic Report

Shows traffic data in real time

Update Report - Antivirus Signatures Update Status

Shows the update status of the antivirus signatures

Update Report - Computers Not Updated

Shows the computers that do not have the latest antivirus signatures

Ad-Aware Security for Mail Servers (Unices) Reports

Installation Report - Ad-Aware Installed Products

Shows the Ad-Aware products installed on the selected computers

Installation Report - Installation or Deployment Errors

Shows the errors that appeared during installation or deployment processes

Mail Servers Malware Report (Unices)

Shows the threats in real time

Mail Servers Spam Report (Unices)

Shows the spam data in real time

Mail Servers Traffic Report (Unices)

Shows the traffic data in real time

Update Report - Antivirus Signatures Update Status

Shows the update status of the antivirus signatures

Update Report - Computers Not Updated

Shows the computers that do not have the latest antivirus signatures

Default Communication Ports

Ad-Aware Management Server and its components communicate on specific ports, which you can configure during installation. These ports must not be used by any other application installed in the network. Access to them must also be allowed by the local firewalls.

These are the default communication ports:

- 7072 - The communication port between Ad-Aware Management Server and Ad-Aware Management Agent. This port must be allowed on all network computers.
- 7071 - The communication port between Ad-Aware Management Server and Ad-Aware Management Console. This port must be allowed on all Ad-Aware Management Server computers and on all computers on which you install Ad-Aware Management Console.
- 7073 - The communication port between a master and a slave instance of Ad-Aware Management Server. This port must be allowed on all Ad-Aware Management Server computers. The default port on which Ad-Aware Update Server accepts connections from clients is 7074. The Ad-Aware Update Server port must not be used by other applications installed on the system.

Application Files

The antimalware scanning engines included in the Ad-Aware security solutions can be configured to limit scanning to application (or program) files only. Application files are far more vulnerable to malware attacks than other types of files.

This category is limited to files with the following extensions:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz;

wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp