

Outpost Network Security

- Central deployment and management
- Network and Web Surfing Safety
- Anti-malware with remote scans
- Removable USB device control
- Local updates server
- File servers and 64-bit systems support



Installation Notes for Outpost Network Security (ONS) version 3.2

Contents

| | |
|--|----|
| Installation Notes for Outpost Network Security (ONS) version 3.2..... | 1 |
| Architecture | 2 |
| System Requirements | 2 |
| Server part: | 2 |
| Client part: | 2 |
| Steps to a Successful Installation..... | 3 |
| Clients preparation | 3 |
| Server preparation | 4 |
| Installation Instructions | 7 |
| Deploying Outpost Network Security Client on Client Computers..... | 10 |
| Troubleshooting | 13 |
| Client-side issues | 13 |
| Server-side issues..... | 14 |
| Most typical malfunction cases | 15 |
| Upgrade instruction with rules import | 16 |

Architecture

The Outpost Network Security (ONS) version 3.2 working environment implies the presence of the following components:

- **Server-part:**

a computer with Management Console and Update server installed. Management console is the main managing tool that lets Administrator control client installations over the network and manage product settings. Update server provides a centralized (single download, multi-install) client update;

- **Client-part:**

one or more clients—computers to be protected with client software installed.

System Requirements

It is not necessary to install Outpost Network Security server part on a domain controller or server; it can be installed on any dedicated workstation.

Server part:

Supported platforms (x32 and x64):

- Windows 2000 (SP4 with Security Rollup)
- Windows XP SP2 +
- Windows 2003 SP2
- Windows Vista SP2
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

Min. hardware requirements: 1 GHz CPU(x86-/x64-/multi-core), 512Mb RAM, 1Gb free disk space.

Client part:

Supported platforms (x32 and x64):

- Windows 2000 (SP4 with Security Rollup)
- Windows XP SP2+
- Windows 2003 SP2
- Windows Vista SP2
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

Min. hardware requirements: 1GHz CPU(x86-/x64-/multi-core), 512Mb RAM, 450Mb free disk space.

Supported email protocols & services: POP3, SMTP, IMAP.

Note: 64-bit edition is available in separate installation package!

Steps to a Successful Installation

Clients preparation

Before deploying Outpost Network Security client, please, verify that prior versions are uninstalled. If another version of the product was previously installed on the target machine uninstall it using standard Windows features and reboot the PC, then continue with preparation steps.

1. For **Windows XP**:

- **Disable Windows Firewall** on the client PC.
- Make sure that **account with administrator privileges** is created and the **password** is set. This is required for acquiring necessary privileges for remote installation. In some cases it is necessary to specify windows domain name in administrative account name too, for example: **Domain_name\Admin_name**.
- Make sure that system shared folder **ADMIN\$** is accessible. Please, open **Control Panel > Administrative Tools > Computer Management** console and navigate to **Shared Folders > Shares** to observe all shared folders on the PC.
- In **Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options** change the **Network access: Sharing and security model for local accounts local policy** from Guest only - local users authenticate as guest to Classic - **local users authenticate as themselves**;

2. For **Windows Vista** and **Windows 7**

- **Disable Windows Firewall** on the client PC.
- Make sure that **account with administrator privileges** is created and the **password** is set. This is required for acquiring necessary privileges for remote installation. In some cases it is necessary to specify windows domain name in administrative account name too, for example: **Domain_name\Admin_name**.
- Make sure that system shared folder **ADMIN\$** is accessible. Please, open **Control Panel > Administrative Tools > Computer Management** console and navigate to **Shared Folders > Shares** to observe all shared folders on the PC.
- Run **regedit.exe** and find the key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

If there is no **LocalAccountTokenFilterPolicy** record, right-click System element and select **New-> DWORD (32-bit) Value**. Specify **LocalAccountTokenFilterPolicy** name and set **Value 1**.

Server preparation

- The PC for the ONS server should have a static IP address assigned in order to install the server part.
- Verify that prior versions are uninstalled. If another version of the product was previously installed on the target machine, uninstall it using standard Windows features and reboot the PC.
- If a client is installed on the same PC where the ONS server is present, you need to **disable Windows Firewall**.
- If there are several network adapters on a server-side please enable routing.

Find the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

If there is no **IPEnableRouter** record right-click System element and select **New-> DWORD (32-bit) Value**. Specify name and set **Value 1**.

1. For Windows XP

- Make sure that system shared folder **ADMIN\$** is accessible using the instructions above.
- Make sure that **account with administrator privileges** is created and the **password** is set. This is required for acquiring necessary privileges for remote installation. In some cases it is necessary to specify windows domain name in administrative account name too, for example: **Domain_name\Admin_name**
- Make sure that **File and Printer Sharing** is enabled on the computer. Please, open **Control Panel > Network Connections** and select the connection properties. **File and Printer Sharing** component should be present.
- In **Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options** change the **Network access: Sharing and security model for local accounts local policy** from Guest only - local users authenticate as guest to Classic - **local users authenticate as themselves**;

2. For Windows Vista and Windows 7

- Make sure that system shared folder **ADMIN\$** is accessible using the instructions above.
- Make sure that **File and Printer Sharing** is enabled on the computer. Please, open **Control Panel > Network Connections** and select the connection properties. **File and Printer Sharing** component should be present.
- Run **regedit.exe** and find the key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

If there is no **LocalAccountTokenFilterPolicy** record, right-click System element and select **New-> DWORD (32-bit) Value**. Specify **LocalAccountTokenFilterPolicy** name and set **Value 1**.

- Make sure that **account with administrator privileges** is created and the **password** is set. This is required for acquiring necessary privileges for remote installation. In some cases it is necessary to specify windows domain name in administrative account name too, for example: **Domain_name\Admin_name**.

By default clients connect to Update server using port 80 TCP. If there are other applications that use port 80 TCP (for example IIS), another custom port should be specified for Update server. You can acquire the list of the used ports by running **netstat** command in the command prompt. Please, use the following instruction to reassign the update server port:

1. Close Management console.
2. Stop Agnitum Administration Server service in **Control Panel > Administration > Services** applet.
3. Stop Agnitum Update Server service in the same applet.
4. Open the file **C:\Program Files\Agnitum\Outpost Network Security\update_config.ini** and find the setting **ServerHTTPPort=** - by default port 80 is assigned
5. To specify a custom Update server port change **ServerHTTPPort=** to another port and save the changes.
6. Restart Agnitum Update server service.
7. Restart Agnitum Administration Server service
8. Install clients. In case clients are already installed it is necessary to modify the machine.ini file on the client PC in the following manner:
Run ONS client graphical user interface, right-click the icon and select to suspend protection (until restart). Exit Outpost and stop its service. Open **C:\Program Files\Agnitum\Outpost Security Suite Pro\machine.ini** file and navigate to **[Update]** section. Modify **server** record by adding port number, for example **server=http://192.168.7.249:8080** and save the changes.
9. Run ONS client GUI, resume protection and switch the client to Background mode if

necessary.

It is also possible to specify Update server IP address. By default IP 0.0.0.0 is used thus the server listens all network interfaces on the same port. Binding the update server to a specific IP address will grant the possibility to use the same port for different services. The following steps should be performed after server-part installation:

1. Close Management console.
2. Stop Agnitum Administration Server service.
3. Stop Agnitum Update Server service.
4. Change the Value ServerBindIP= in C:\Program Files\Agnitum\Outpost Network Security\update_config.ini to another IP address and save the changes.
5. Restart Agnitum Update server service.
6. Restart Agnitum Administration Server service

Note: It is important to bind not only the Update server to a specific IP, but perform the binding to the different IP for the service which uses the same port. Please, refer to the documentation provided with the service.

Installation Instructions

To start installing Outpost Network Security, run the setup file. The installation procedure is straightforward and similar to most Windows installers. Just follow the steps of the setup wizard and it will install all the required components on your computer.

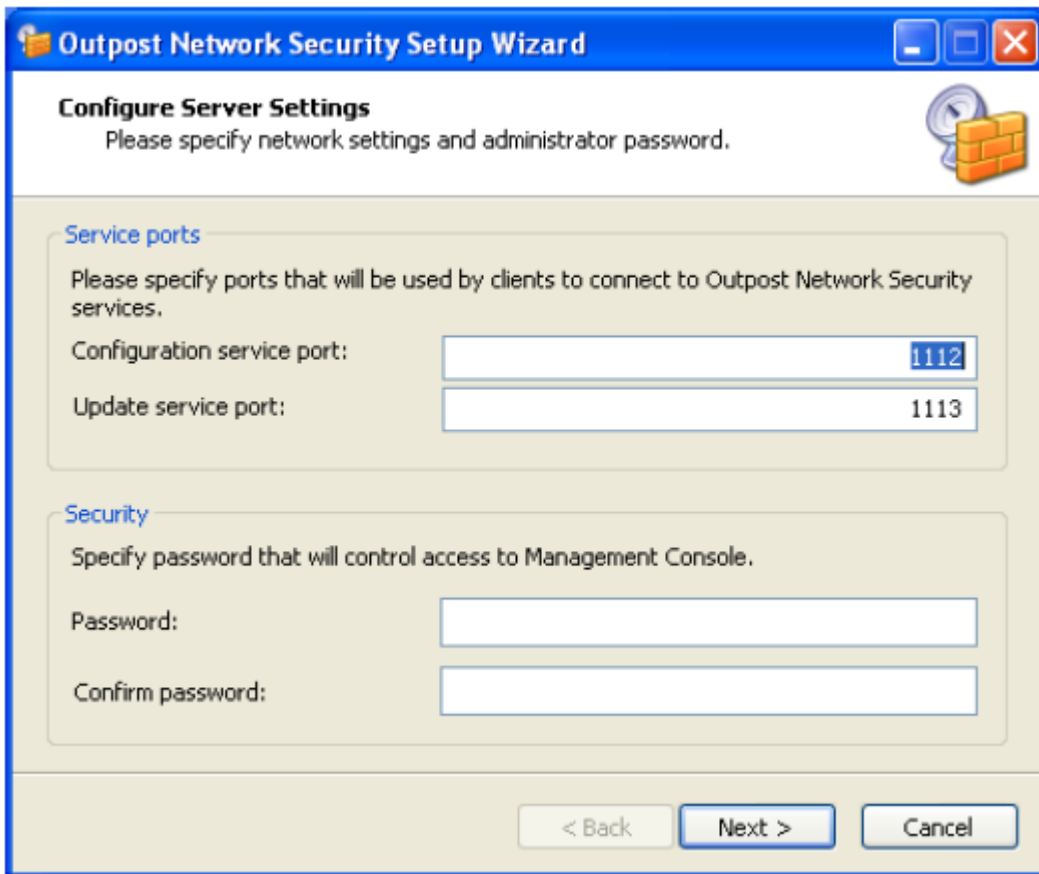


Screenshot: ONS Setup Wizard. Step 1 – Specify components to be installed

Important: Both Management Console and services should be installed on a computer with a static IP address.

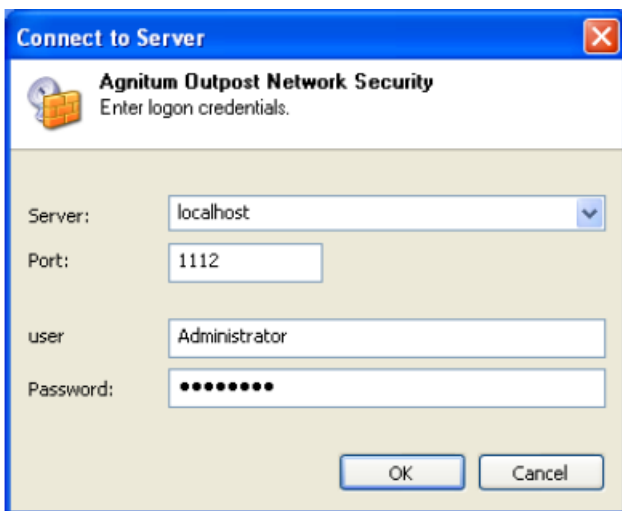
During installation, the Outpost Network Security Client installation package will be copied to the **C:\Program Files\Agnitum\Outpost Network Security\clients** folder, which is automatically shared, so the installer is available to all clients on the network.

After copying files, the setup wizard will prompt you for the port numbers to be used by the client computers to connect to the server and a password to be used to control access to the Management Console.



Screenshot: ONS Setup Wizard. Step 2 – Configure Server Settings (Service ports and Security)

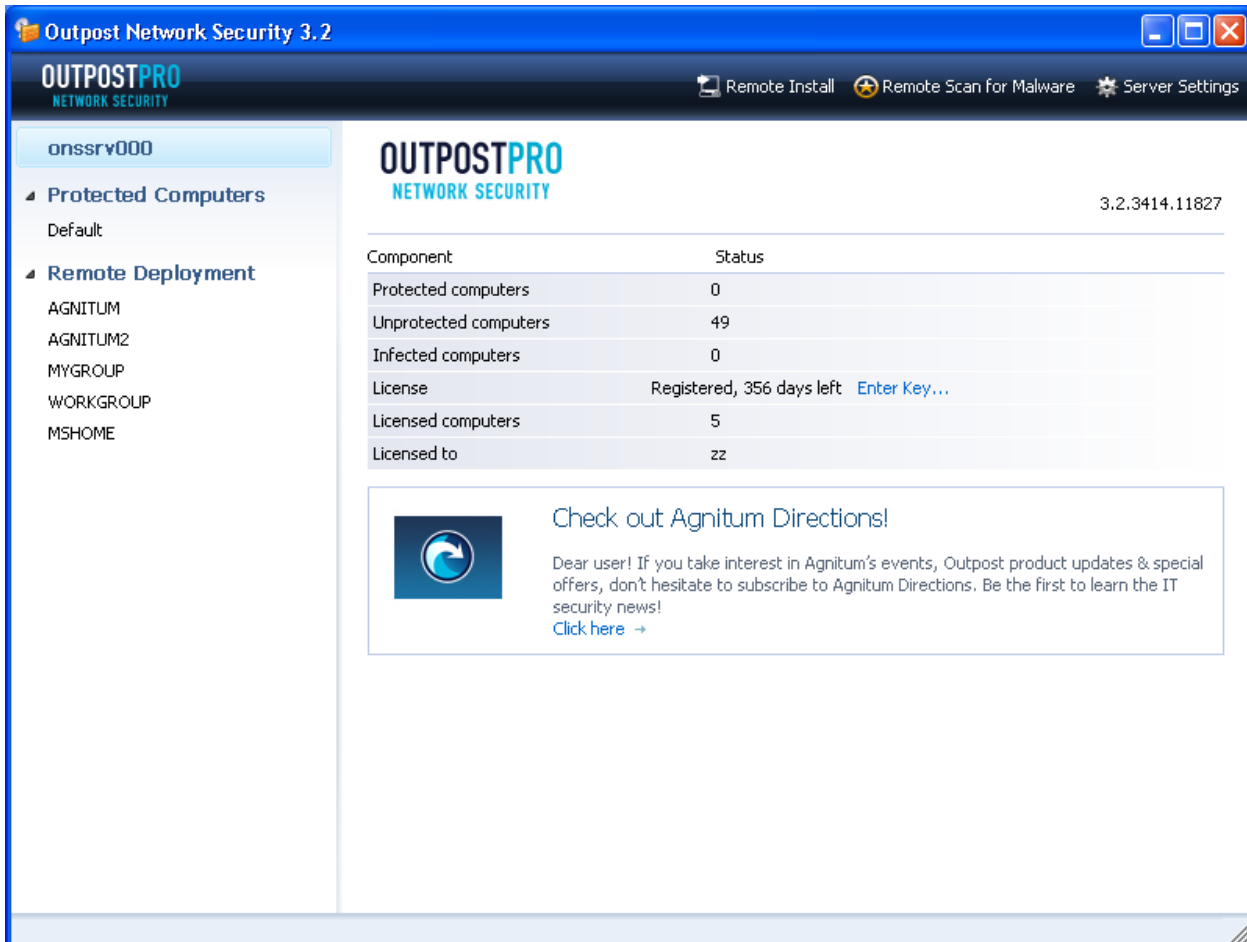
On completing the setup wizard, you will be prompted for server part connection parameters and will be able to specify access credentials to start Management Console. Type in IP address, DNS name or NetBIOS name of the computer with Outpost Network Security services installed or select it from the drop-down list. If server part is installed on a local computer, select **localhost** (by default). Also, specify the port to be used by configuration service and credentials (password, specified during server part installation).



Screenshot: Connect to Server – “Enter logon credentials” alert

Note: Outpost Network Security itself does not install Outpost Network Security Client on the console. Client software can be installed on the same computer where Management Console or Outpost Network Security services are installed either manually or using the procedure described in [Deploying Outpost Network Security Client on Client Computers](#) section. However, if any security software is installed on the console, make sure that the connection to the port specified as a configuration service port is not blocked. Otherwise, clients will not be able to get the configuration settings and function properly.

Once you enter the credentials and click **OK**, the Management Console main window will be displayed.



Screenshot: ONS Management Console – Main Window

Deploying Outpost Network Security Client on Client Computers

For a small number of computers, you can install Outpost Network Security (ONS) client on each user's workstation manually (the client setup package file, named **OutpostNetworkSecurityClientInstall.exe**, is located in the **C:\Program Files\Agnitum\Outpost Network Security\clients** folder, which is shared during installation).

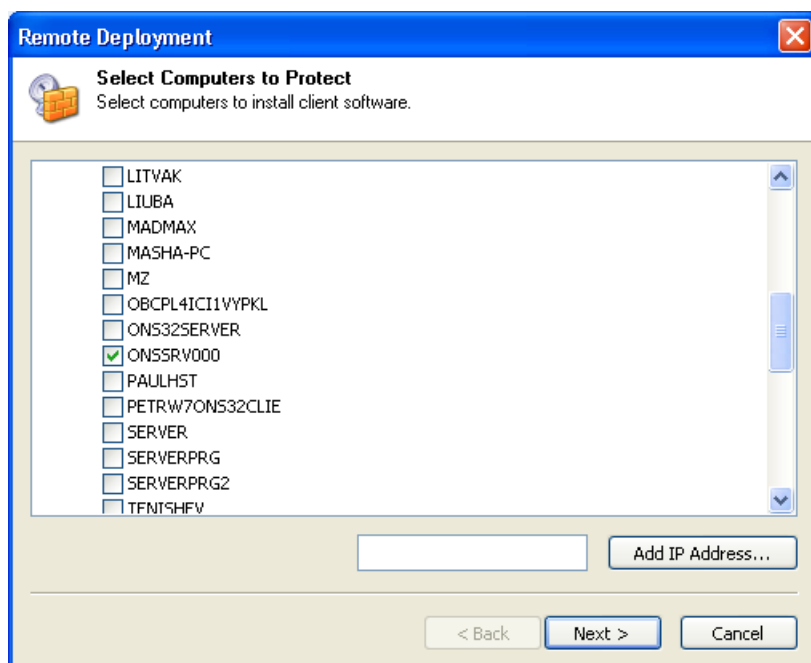
ONS allows for automatic installation of the client part on the workstations.

All workstations on your network are enumerated and listed under the **Remote Deployment** node in the left panel of the Management Console's main window. Also, they are grouped into domains and workgroups represented as sub nodes of this node according to your network infrastructure.

Use the **Refresh Network Environment** command available on the node's shortcut menu to refresh the information.

Note: ONS Management console detects computers which are available in Windows Network Places. If a network PC is not seen in Windows Explorer, ONS Management console will not display it either.

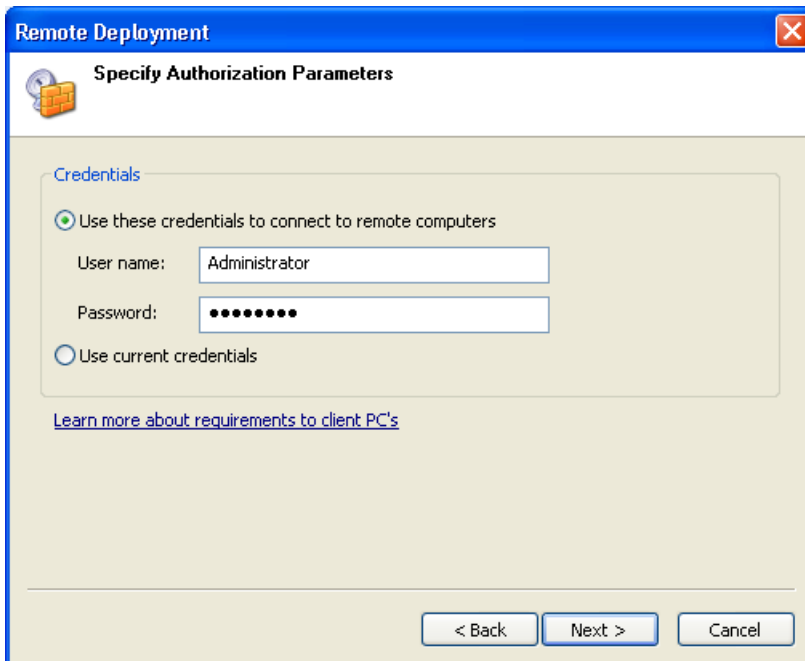
To automatically install the client part on all workstations, click **Remote Install** on the Management Console's toolbar or select **Install Outpost Network Security** on the node's or particular computer's shortcut menu and follow the **Remote Deployment Wizard**. The first step allows to select computers on your network to install client software. You can also specify the IP address manually in the provided text box below if you don't see the computer in the tree. After clicking **Add IP Address**, the IP will appear under the **Manually added IP's** node.



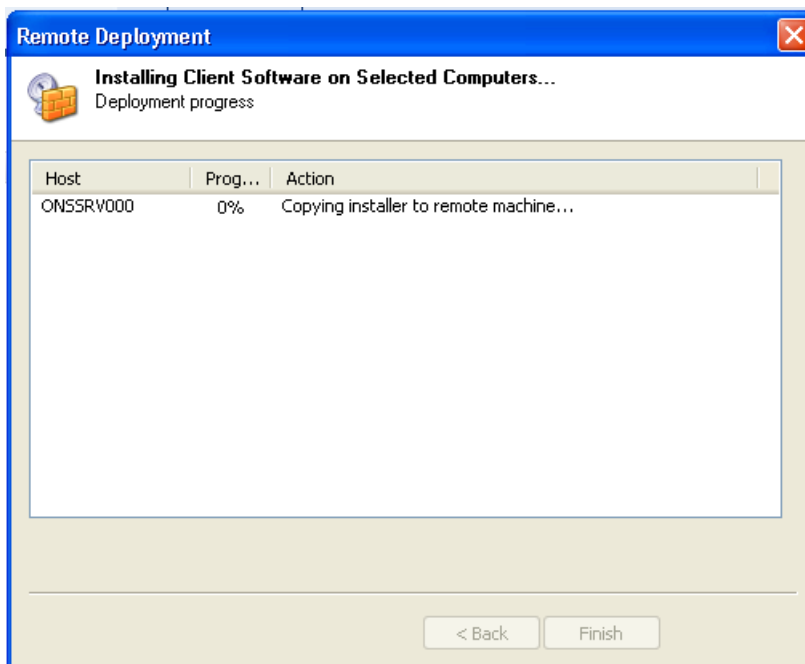
Screenshot: Remote Deployment. Step 1 – Select Computers to Protect

After clicking **Next**, you will be prompted for the credentials to connect to all the selected computers. The specified account should possess administrative rights on all the computers.

Click **Next** to start remote installation.



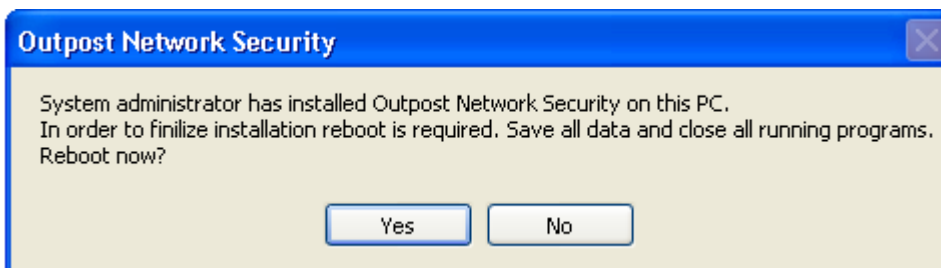
Screenshot: Remote Deployment. Step 2 – Specifying Authorization Parameters



Screenshot: Remote Deployment. Step 3 – Installing Client Software on Selected Computers –

Deployment Progress

Clients are informed of reboot necessity and a corresponding warning is displayed on a client-side. Make sure that client PC is restarted.



Screenshot: Outpost Network Security client installation – reboot warning

As soon as client installation is complete, **Finish** button in the Remote Deployment window becomes available.

After client installation, all the computers where it was installed successfully will be listed under the **Default** group of the **Protected Computers** node. After selecting this group in the left panel, you will see the list of computers belonging to it.

Troubleshooting

If you come across any issues please contact [Agnitum support service](#). To provide technical information please refer to the following instruction:

Client-side issues

In order to troubleshoot client issues please do the following:

- 1) Open management console in Start > All programs > Agnitum > Outpost Network Security > Outpost Network Security.
- 2) Right-click on the group with the client computers with the problem (by default it is a Default group) and select Settings.
- 3) Open Logs, turn on 'Log debugging information' and set the logging level to 2 and save the changes.
- 4) Restart the client. If the client runs in Background mode start the client on a problem PC from the Start menu.
- 5) Reproduce the problem.
- 6) Immediately after the problem is reproduced, right-click Outpost system tray icon, and select 'Save and archive logs'. After you will click it, 'Feedback' sub-directory will open.
- 7) Send us *feedback.zip* file, and also attach your configuration files:
 - 1) *configuration.conf*
 - 2) *ons_conf.ini*
 - 3) *machine.ini*

that can be found in Outpost installation folder

(by default *C:\Program Files\Agnitum\Outpost Security Suite Pro*).

If you can't see extensions of these files, please, open "Start - Control Panel - Folder options - View" and untick "Hide extensions for known filetypes". All extensions will now be visible to you.

Server-side issues

- 1) Open management console in Start > All programs > Agnitum > Outpost Network Security > Outpost Network Security.
- 2) Open Server Settings - Advanced menu.
- 3) Turn on log debugging information and set log level 2. Press OK.
- 4) Reboot the PC.
- 5) Reproduce the problem.
- 6) Right after this copy and archive the folder

C:\Program Files\Agnitum\Outpost Network Security\log and send it to us for the investigation.

- 7) Also attach your server configuration files:

- 1) *administrative.stg*
- 2) *configuration.conf*
- 3) *machine.ini*
- 4) *ons_con.ini*
- 5) *ons_con.stg*
- 6) *shuttle.ini*
- 7) *update_config.ini*

Note, that in most cases both server-side and client-side logs will be needed.

Most typical malfunction cases

| Case | Troubleshooting steps |
|---|---|
| The clients cannot access the server | <p>Ensure that the ports are accessible by using telnet. In Windows Vista and Windows 7 this tool should be first activated by opening</p> <p>Control Panel > Programs And Features, turning Windows features on / off and by checking Telnet Client and clicking OK.</p> <p>Type telnet <ONS server IP> 1113 in order to find out if the server is accessible. If the console shows “connecting...” without any visible progress, the port is blocked. Please, disable Windows Firewall in this case.</p> |
| The clients are not updated | <p>The server downloads the whole database from Agnitum servers and it takes significant amount of time. Please, ensure that the server is updated and wait approximately 40 minutes prior to updating the clients.</p> |
| It is not possible to remotely install the client | <p>Ensure that the client PC is prepared according to instruction and is operated with administrator account. User Account Control (UAC) should be disabled.</p> |

Upgrade instruction with rules import

It is highly recommended to install new version from scratch and create new configuration. Though if you have set up custom groups with custom settings and custom application rules on clients, please follow the steps below.

1. Back-up your configuration on a PC where Management console and update server are installed:

Copy the following files from C:\Program Files\Agnitum\Outpost Network Security\

- 1) *administrative.stg*
- 2) *ons_con.stg*
- 3) *machine.ini*
- 4) *ons_con.ini*
- 5) *shuttle.ini*
- 6) *update_config.ini*

2. Back-up your client configuration (on each PC with client software installed in case of unique application rules created):

Copy the following file from C:\Program Files\Agnitum\Outpost Security Suite Pro\

configuration.conf

3. Remove client software (on each PC with client software installed) using Add or Remove programs feature and restart client PC.
4. Remove previous version of Management console and update server on a PC where Management console and update server are installed.
5. Install the latest version of Management console and update server.
6. Download the latest version from our site. Run the installation.
7. Run Management Console. All protected PCs will now be unprotected. You will have to manually upgrade clients.
8. Import previous Management console and update server configuration on a server-side:
 - Close Management Console.
 - Open Administrative tools – Services.
 - Stop Agnitum Administration Server service.
 - Stop Agnitum Update Server service.
 - Copy backed up server configuration files to C:\Program Files\Agnitum\Outpost Network Security
 - Overwrite existing files.
 - Start Agnitum Update server service.
 - Start Agnitum Administration Server service.
 - Open Management Console and check if your custom Groups and rules are there.

- Console will detect clients but will show them offline as there is no client software installed.
- Delete these clients (your Group settings will be preserved).
- Refresh Network Environment.

9. Install client software on client PCs:

After network environment is refreshed client will appear in Unprotected computers list. Install clients from Management console.

Note, that in the current version clients are informed on reboot necessity and a warning is displayed on a client-side. Make sure that client PC is restarted.

As soon as client installation is complete Finish button in the Remote Deployment window becomes available.

Clients are now installed with default settings and can be moved in the existing Groups with custom settings.

10. Import custom client applications rules on each client individually

If there are special custom application rules on a client-side you wish to be imported on a client PC please do the following:

- 1) Start the client from **Start – All programs – Agnitum – Outpost Security Suite Pro - Outpost Security Suite Pro.**
- 2) Suspend protection (for 5 minutes).
- 3) Exit the client and shutdown the service.
- 4) Copy backed up configuration file configuration.conf to C:\Program Files\Agnitum\Outpost Security Suite Pro
- 5) Overwrite existing file.
- 6) Start the client from **Start – All programs – Agnitum – Outpost Security Suite Pro - Outpost Security Suite Pro.**
- 7) Resume protection.
- 8) Exit the client and switch to background mode if desired.