IKARUS security software

User manual

for the

IKARUS security.manager

© 2012 IKARUS Security Software GmbH

1 ABOUT IKARUS ..... - 4 -

2 INTRODUCTION ..... - 5 -

3 THE IKARUS SECURITY.MANAGER ..... - 6 -

3.1 THE IKARUS SECURITY.MANAGER SERVER ..... - 7 -
3.2 THE IKARUS SECURITY.MANAGER UI ..... - 8 -

4 INSTALLING THE IKARUS SECURITY.MANAGER ..... - 9 -

4.1 INSTALLING THE IKARUS SECURITY.MANAGER SERVER ..... - 10 -
4.1.1 SYSTEM REQUIREMENTS ..... - 11 -
4.1.2 WELCOME ..... - 12 -
4.1.3 LICENSE AGREEMENT ..... - 13 -
4.1.4 LDAP SETTINGS ..... - 14 -
4.1.5 DEPLOYMENT SETTINGS ..... - 15 -
4.1.6 USER SETTINGS ..... - 16 -
4.1.7 NETWORK SETTINGS ..... - 17 -
4.1.8 DATABASE SETTINGS ..... - 18 -
4.1.9 SELECTING THE INSTALLATION FOLDER ..... - 20 -
4.1.10 CONFIRM INSTALLATION ..... - 21 -
4.1.11 INSTALLATION COMPLETE ..... - 22 -
4.2 INSTALLING THE IKARUS SECURITY.MANAGER UI ..... - 23 -
4.2.1 SYSTEM REQUIREMENTS ..... - 24 -
4.2.2 WELCOME ..... - 25 -
4.2.3 LICENSE AGREEMENT ..... - 26 -
4.2.4 SELECTING THE INSTALLATION FOLDER ..... - 27 -
4.2.5 CONFIRM INSTALLATION ..... - 28 -
4.2.6 INSTALLATION COMPLETE ..... - 29 -
4.3 UPGRADING A LEGACY IKARUS SECURITY MANAGER X VERSION TO THE NEW IKARUS SECURITY.MANAGER ..... - 30 -

5 THE IKARUS SECURITY.MANAGER UI ..... - 31 -

5.1 LOGIN ..... - 31 -
5.1.1 SET PASSWORD ..... - 33 -
5.1.2 MANAGING MULTIPLE IKARUS SECURITY.MANAGER (MANAGEMENT MODE) ..... - 35 -
5.1.3 CHANGE MANAGEMENT ..... - 36 -
5.1.4 SET LICENSE ..... - 37 -
5.1.5 LICENSE VIOLATION ..... - 37 -
5.2 THE USER INTERFACE ..... - 39 -
5.2.1 DIRECTORY ..... - 40 -
5.2.2 PENDING TASKS ..... - 46 -
5.2.3 VIRUS LIST ..... - 50 -
5.2.4 LOG FILE ..... - 52 -
5.2.5 CHANGE LOG ..... - 53 -
5.2.6 OVERVIEW PAGE ..... - 54 -
5.2.7 PROPERTIES PAGE ..... - 56 -
5.2.8 GENERAL PAGE ON GROUPS ..... - 58 -

© 2012 IKARUS Security Software GmbH

5.2.9 General Page on Clients ..... - 60 -
5.2.10 Notification Bar ..... - 62 -
5.2.11 Charts Page ..... - 62 -
5.2.12 Global overview page ..... - 64 -
5.2.13 IKARUS anti.virus Configurations ..... - 66 -
5.2.14 IKARUS security.manager Settings ..... - 76 -
5.2.15 Dialog "Clean host-entries from database" ..... - 87 -
5.2.16 About Dialog ..... - 88 -
5.2.17 Management mode ..... - 89 -
5.2.18 The Menu Bar ..... - 98 -
5.2.19 The Toolbar ..... - 102 -

6 THE SHARED DIRECTORY ..... - 103 -

7 LICENSING INFORMATION ..... - 104 -

7.1 Registration ..... - 104 -
7.1.1 Layout ..... - 104 -
7.2 Activation Key ..... - 104 -
7.2.1 Layout ..... - 105 -

8 SOFTWARE DISTRIBUTION ..... - 106 -

8.1 Installing the IKARUS anti.virus ..... - 107 -
8.2 Uninstalling the IKARUS anti.virus ..... - 109 -

9 CONFIG FILE ..... - 110 -

9.1 The <config> Section ..... - 111 -
9.2 The <ldap> Section ..... - 112 -

10 TABLE OF FIGURES ..... - 113 -

11 GLOSSARY ..... - 115 -

© 2012 IKARUS Security Software GmbH

1 About IKARUS

As one of the first antivirus software providers, IKARUS is both a pioneer and a vibrant, fast-growing company. For more than 25 years, IKARUS software has been a name you can trust to provide outstanding antivirus protection and content security.

The development team recruited UNIX and Microsoft specialists as well as former employees from universities and research institutes. Through its numerous cooperation arrangements and special agreements with IT security experts, IKARUS is able to provide up-to-the-minute information and responses in all areas relating to security software.

Our products range from simple yet highly effective antivirus protection (**IKARUS anti.virus**) to sophisticated software for networks and gateways (**IKARUS security.manager**, **IKARUS security.proxy**) all the way to **IKARUS web.security** and **IKARUS my.mailwall**, a high-end managed security product that protects your network from viruses before they strike.

© 2012 IKARUS Security Software GmbH

2 Introduction

Thank you for choosing the **IKARUS security.manager**, the simple and inspired solution that always provides the computers on your network with the latest virus and spam database updates and **IKARUS anti.virus** versions. Basically, **IKARUS security.manager** distributes the databases and updates from a central point to the computers on your network to save bandwidth, download volume, and, above all, administration time and costs.

© 2012 IKARUS Security Software GmbH

3 The IKARUS security.manager

The **IKARUS security.manager** allows for installing, updating, uninstalling, and configuring the **IKARUS anti.virus** on your network.

The **IKARUS security.manager** consists of two separate *applications*: the **IKARUS security.manager Server** and the **IKARUS security.manager UI**. Both can be installed and run on different computers separately from each other. This separation allows you to control and maintain your network protection from anywhere and anytime you want.

© 2012 IKARUS Security Software GmbH

3.1 The IKARUS security.manager Server

The **IKARUS security.manager Server** is the core of the **IKARUS security.manager**. It is the part that actually does all the distributional and statistical work and also handles the communication between the **IKARUS security.manager** and the **IKARUS anti.virus** installed on the computers on your network.

The **IKARUS security.manager Server** runs on a Windows server operating system as a *service*. All of the settings and information the **IKARUS security.manager Server** holds are saved in a *MSSQL* database, which can but does not need to reside on the computer where the **IKARUS security.manager Server** is installed. The communication between the **IKARUS security.manager** and the **IKARUS anti.virus** on your network is established via *TCP* using *9887* as the default port number. That port can be modified in the *Config File* of the **IKARUS security.manager Server**.

Since the **IKARUS security.manager Server** needs to perform executional tasks remotely on computers on your network, it needs appropriate rights. Therefore, we highly recommend installing the **IKARUS security.manager Server** *service* using a user account with administrative rights for your *domain*. This will ensure that the **IKARUS security.manager Server** is allowed to install and administer the **IKARUS anti.virus** on computers within the *domain* on your network. For further information about this topic and the *administration* of computers outside your *domain*, please read the *Software Distribution* chapter.

© 2012 IKARUS Security Software GmbH

3.2 The IKARUS security.manager UI

The **IKARUS security.manager UI** provides the graphical interface to control the **IKARUS security.manager Server**. You can install the **IKARUS security.manager UI** on any computer you wish to control the **IKARUS security.manager Server** from. For more information about the layout and different windows of the **IKARUS security.manager UI**, refer to section 5.2.

Note: You must run the UI as an administrator; otherwise the update of the UI to a later version might fail.

© 2012 IKARUS Security Software GmbH

4 Installing the IKARUS security.manager

In this chapter, you will be guided through the installation process of the **IKARUS security.manager**. The setup is split into two separate installation processes: the **IKARUS security.manager Server** setup and the **IKARUS security.manager UI** setup. Both setup processes will automatically check your target system for installed prerequisites needed for the *application* to run and will optionally install missing software requirements automatically before the actual installation of the IKARUS product is started. Note that a restart of the target computer may be required during the installation of missing prerequisites. In this case, the setup process will automatically continue after a successful restart of the computer.

Note: To install the Server and the UI you need administrative rights. If the User Access Control feature is enabled, launch setup using the **Run as Administrator** command.

© 2012 IKARUS Security Software GmbH

4.1 Installing the IKARUS security.manager Server

To launch the installation of the **IKARUS security.manager Server**, double-click the **Setup-ISM(server)_xxxx** file (where xxxx represents the version number).

© 2012 IKARUS Security Software GmbH

4.1.1 System Requirements

Hardware requirements:

- x86-based PC with 2 GHz or better
- 1 GB RAM
- Screen resolution: 1024 × 768 or higher
- Approx. 500 MB of disk space (depending on the log volume and the download-cache size)
- Internet connection

Software Requirements:

- Windows 2003 Server, Windows Server 2008 (32-bit/64-bit)
- Windows XP, Windows Vista, Windows 7 (32-bit/64-bit)
- *MSSQL* Server (Express) 2005, 2008 (does not need to be installed on the target machine)
- *Active directory* (Microsoft *Windows Domain* structure)

© 2012 IKARUS Security Software GmbH

4.1.2 Welcome

Click Next to read the license agreement.

Figure 4-1 Server Installation – Welcome

4.1.3 License Agreement

The licensing conditions must be accepted to install the **IKARUS security.manager Server**.

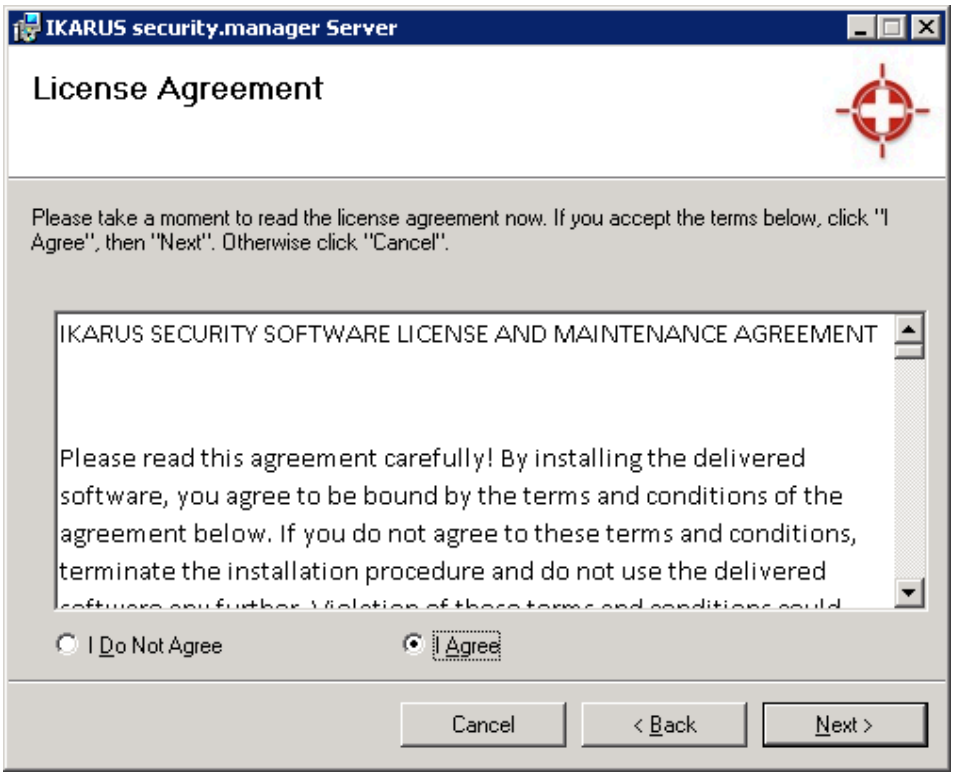


Figure 4-2 Server Installation – License Agreement

© 2012 IKARUS Security Software GmbH

4.1.4 *LDAP* Settings

If the **IKARUS security.manager Server** setup is unable to automatically read out and provide the necessary information about your *LDAP* configuration, you may define the server name and credentials the **IKARUS security.manager Server** should use for communicating with the *LDAP* server.

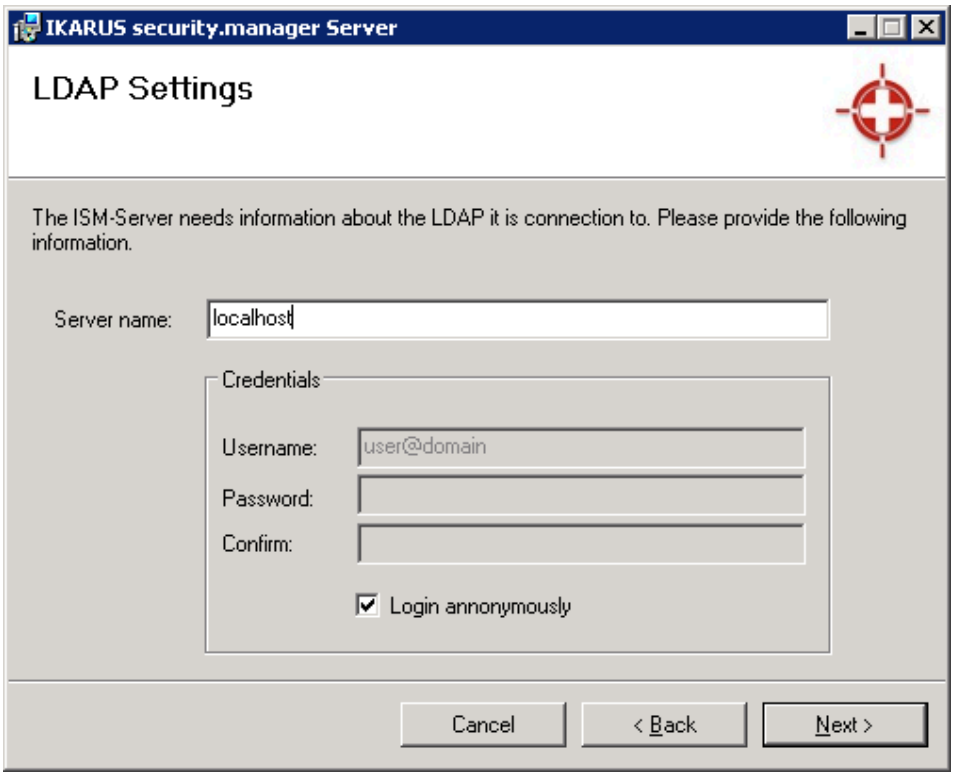


Figure 4-3 Server Installation – LDAP Settings

4.1.5 Deployment Settings

To distribute the **IKARUS anti.virus** on your network, the **IKARUS security.manager Server** needs a place to store the binaries used for installing the **IKARUS virus.utilties**. For that purpose, you will need to set up (if you have not done so already) a *network share* where all *clients* you want to install the **IKARUS anti.virus** on have at least read access to. For further information about the **IKARUS anti.virus** deployment, refer to the *Software Distribution* and *Shared Directory* sections.

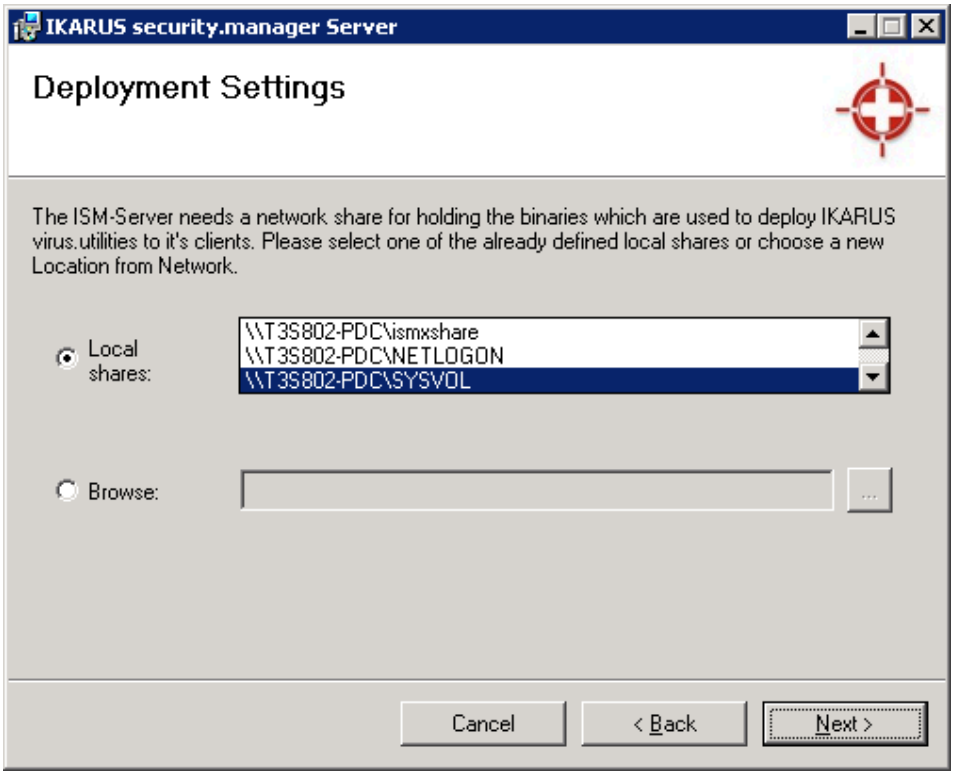


Figure 4-4 Server Installation – Deployment Settings

© 2012 IKARUS Security Software GmbH

4.1.6 User Settings

The **IKARUS security.manager Server** is installed as a *service*. *Services* can be installed with the local system accounts or a user account within your *domain*. Since the **IKARUS security.manager Server** needs appropriate rights to perform a binary execution remotely, it is highly recommended to install the **IKARUS security.manager Server** *service* with a user account which is allowed to administer the *domain*.

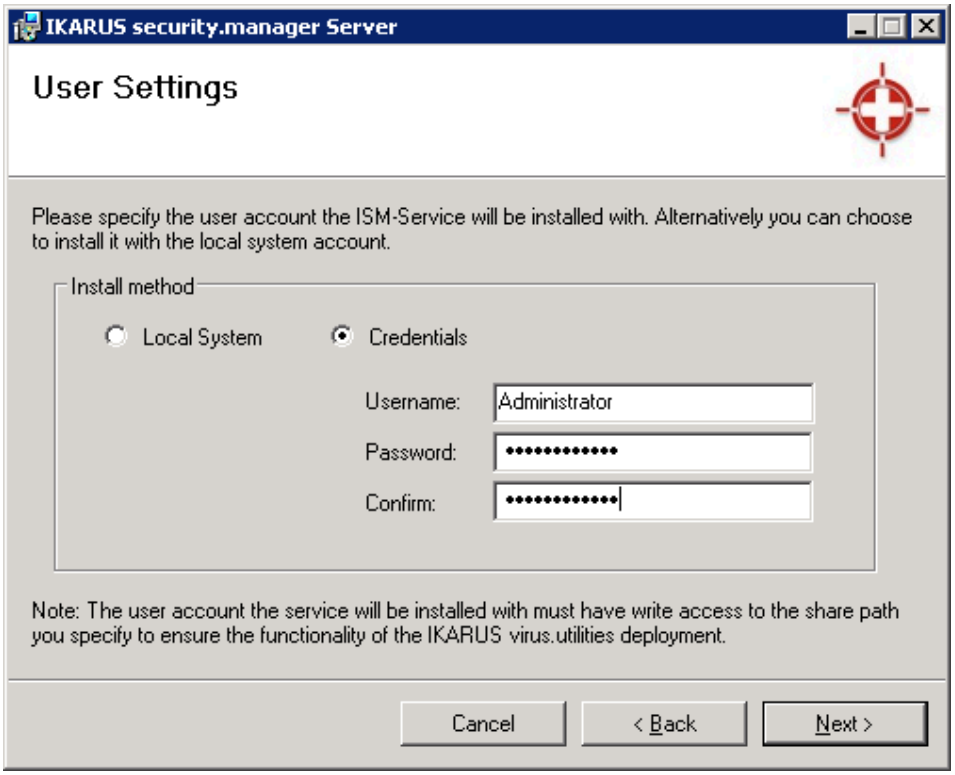


Figure 4-5 Server Installation – User Settings

Note: If you are using a **Windows Small Business Server (SBS)**, please make sure that you use the following format for the domain user credentials: **domain\user**. Windows SBS does not except credentials provided in the format user@domain.

© 2012 IKARUS Security Software GmbH

4.1.7 Network Settings

If you have set up a *proxy server* for your Internet connection, you need to specify the correct settings for your *proxy server* to allow the **IKARUS security.manager Server** to access the Internet. The accuracy of the information you provide here is mandatory for an expedient use of the **IKARUS security.manager**. **No Internet access means** that **no updates** can be retrieved from the IKARUS update servers; thus, **your network will be open to possible threats**.

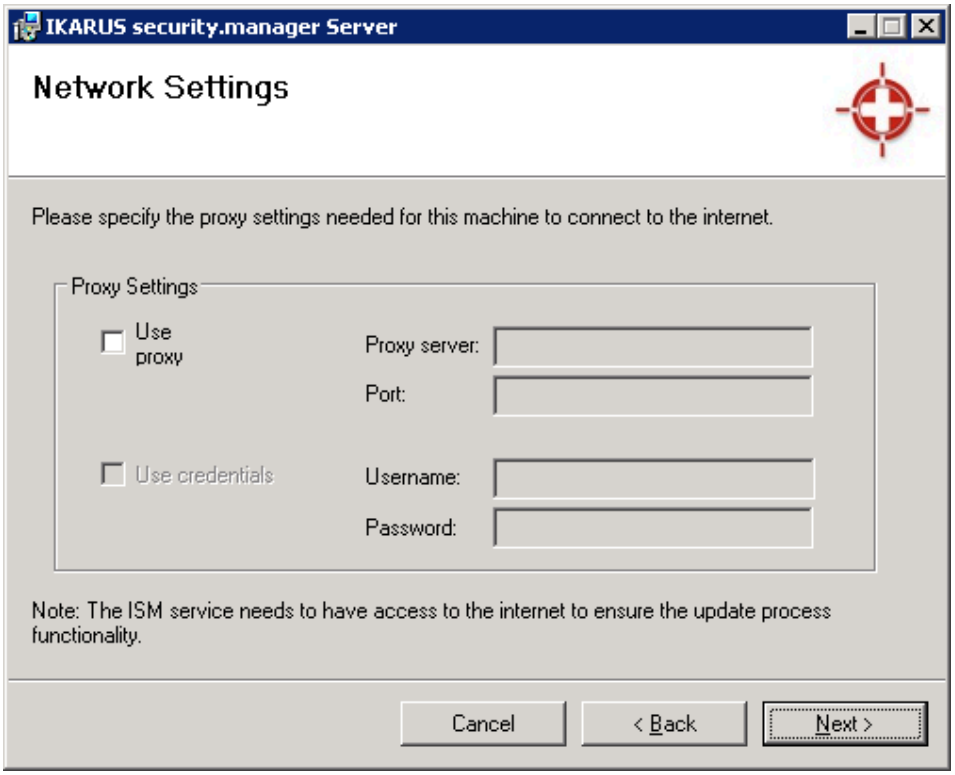


Figure 4-6 Server Installation – Network Settings

© 2012 IKARUS Security Software GmbH

4.1.8 Database Settings

The **IKARUS security.manager Server** needs a *MSSQL* database where it can store the settings, configurations and *client* information. The database can reside on the computer where the **IKARUS security.manager Server** will be installed to, but does not have to.

You can choose to install a new "Microsoft SQL Express 2005" or "Microsoft SQL Express 2008", which are both free of charge, instance, or to use an existing one on the local machine or on a remote host (see Figure 4-7). If you choose to install a new instance the software must be downloaded from the internet, therefore you will need a working internet connection. Should something go wrong with the download process you may want to check the *proxy server* information you provided at the "*Network Settings*" dialog to ensure a working connection to the Internet.

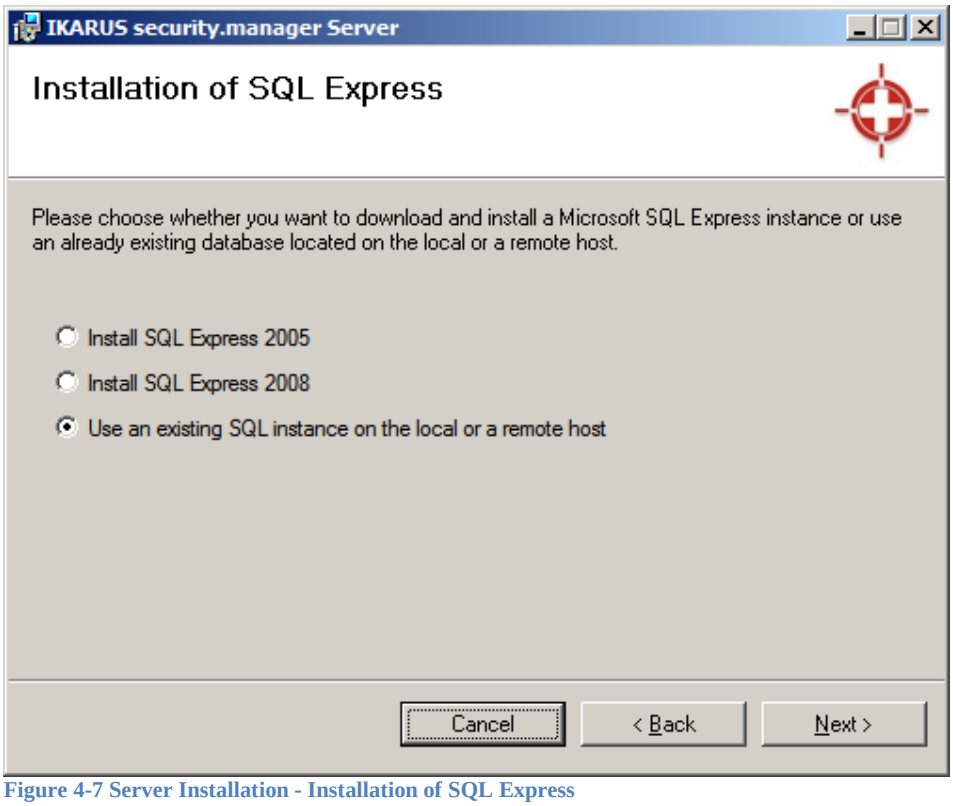


Figure 4-7 Server Installation - Installation of SQL Express

If you want to specify a *MSSQL* database on another computer simply click on "*User defined connection*" (see Figure 4-8) and replace the "*SERVER=.*" string with "*SERVER=SERVER_NAME*", where "*SERVER_NAME*" is to be replaced with the server name of the target computer where the *MSSQL* database resides.

In case you already have at least one *MSSQL* instance installed the setup will list you the installed instances from which you can choose one you want to use.

© 2012 IKARUS Security Software GmbH

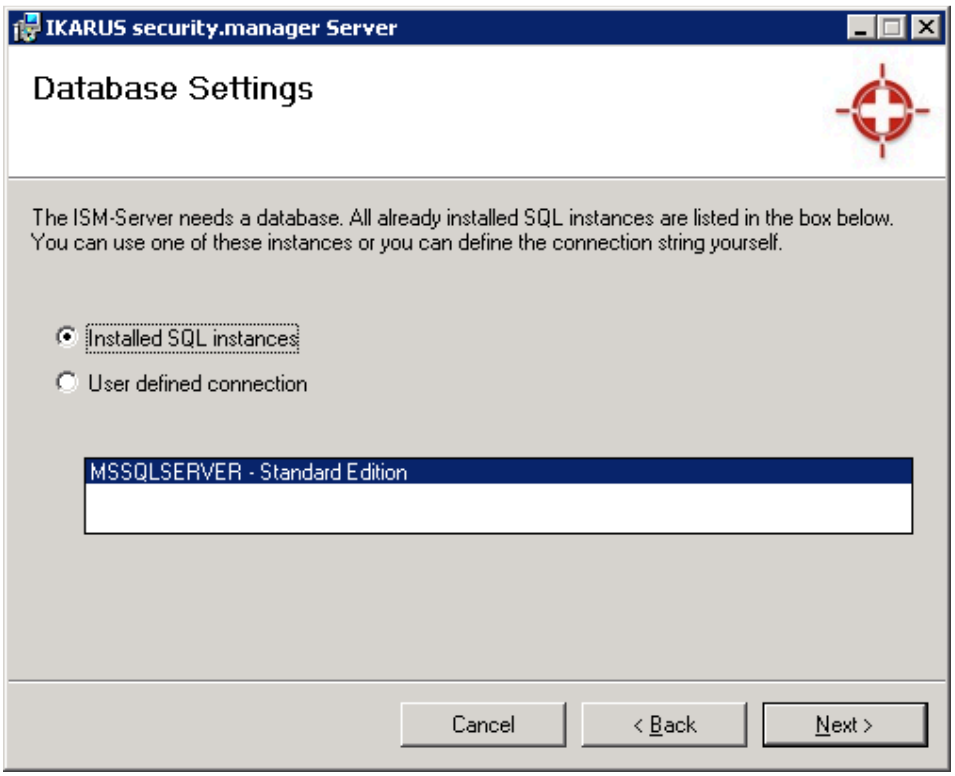


Figure 4-8 Server Installation – Database Settings

© 2012 IKARUS Security Software GmbH

4.1.9 Selecting the Installation Folder

In this dialog, you can choose the destination folder to install the **IKARUS security.manager Server** files to.

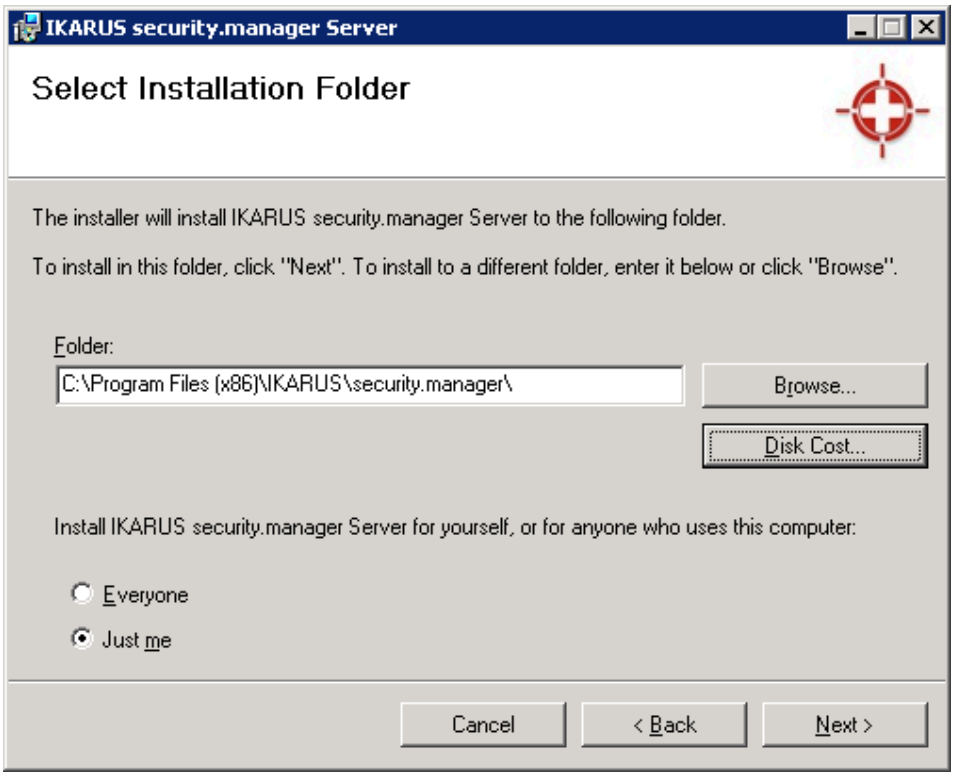


Figure 4-9 Server Installation – Select Installation Folder

© 2012 IKARUS Security Software GmbH

4.1.10 Confirm Installation

This is the final step before the **IKARUS security.manager Server** files are actually installed. Click Next to start the copy process.

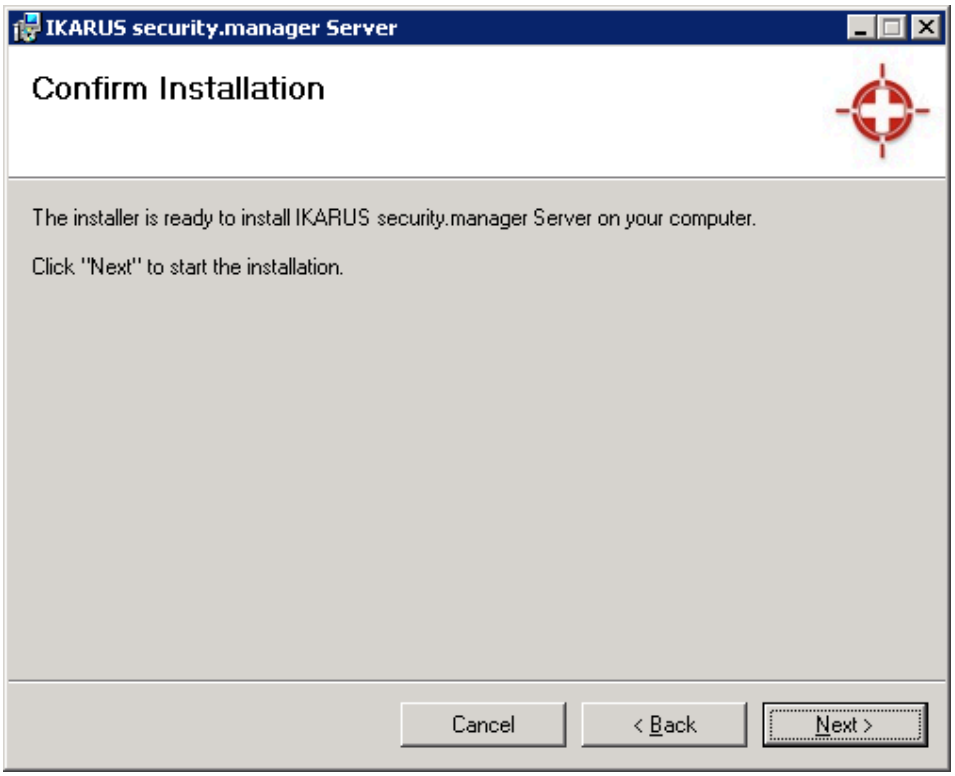


Figure 4-10 Server Installation – Confirm Installation

© 2012 IKARUS Security Software GmbH

4.1.11 Installation Complete

Congratulations! You successfully installed the **IKARUS security.manager Server**. If a different text is displayed in this dialog, contact the IKARUS support hotline.

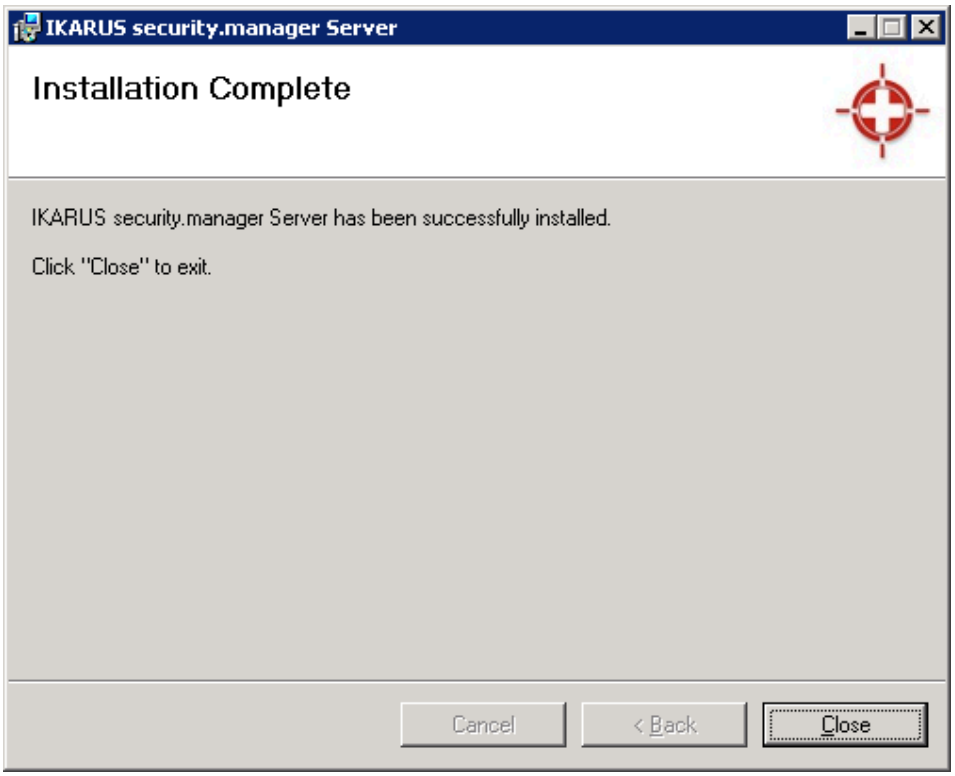


Figure 4-11 Server Installation – Installation Complete

© 2012 IKARUS Security Software GmbH

4.2 Installing the IKARUS security.manager UI

To launch the installation of the **IKARUS security.manager UI**, double-click the **Setup-ISM(UI)_xxxx** file (where xxxx represents the version number).

© 2012 IKARUS Security Software GmbH

4.2.1 System Requirements

Hardware requirements:

- x86-based PC with 2 GHz or better
- 1 GB RAM
- Screen resolution: 1024 × 768 or higher
- Approx. 20 MB of disk space.
- *LAN* connection

Software requirements:

- Windows 2003 Server , Windows Server 2008 (32-bit/64-bit)
- Windows XP, Windows Vista, Windows 7 (32-bit/64-bit)
- .NET Framework 4.0

© 2012 IKARUS Security Software GmbH

4.2.2 Welcome

Click Next to read the license agreement.

Figure 4-12 UI Installation – Welcome

© 2012 IKARUS Security Software GmbH

4.2.3 License Agreement

The licensing conditions must be accepted to install the **IKARUS security.manager UI**.

Figure 4-13 UI Installation – License Agreement

© 2012 IKARUS Security Software GmbH

4.2.4 Selecting the Installation Folder

In this dialog, you can choose the destination folder to install the **IKARUS security.manager UI** files to.

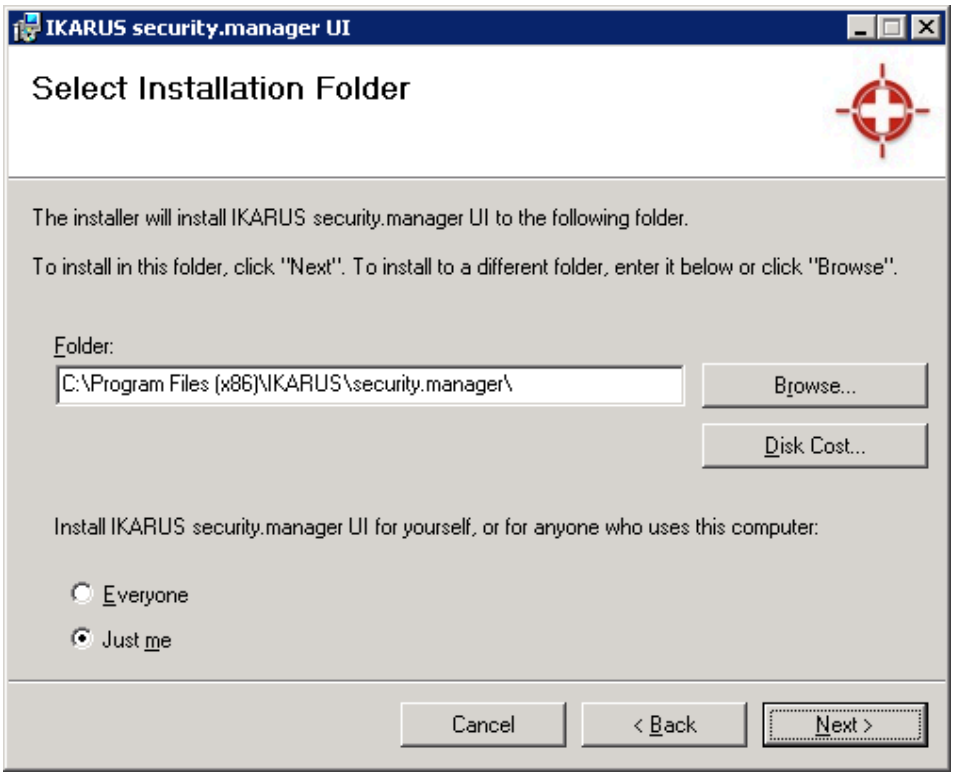


Figure 4-14 UI Installation – Select Installation Folder

4.2.5 Confirm Installation

This is the final step before the **IKARUS security.manager UI** files are actually installed. Click Next to start the copy process.

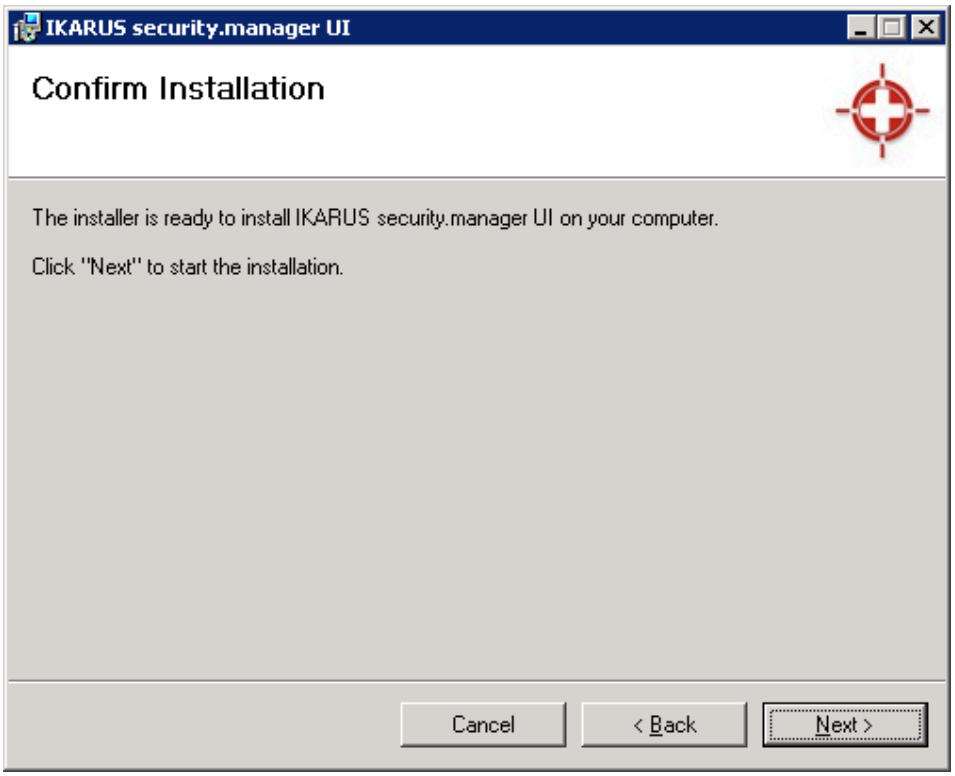


Figure 4-15 UI Installation – Confirm Installation

© 2012 IKARUS Security Software GmbH

4.2.6 Installation Complete

Congratulations! You successfully installed the **IKARUS security.manager UI**. If a different text is displayed in this dialog, contact the IKARUS support hotline.

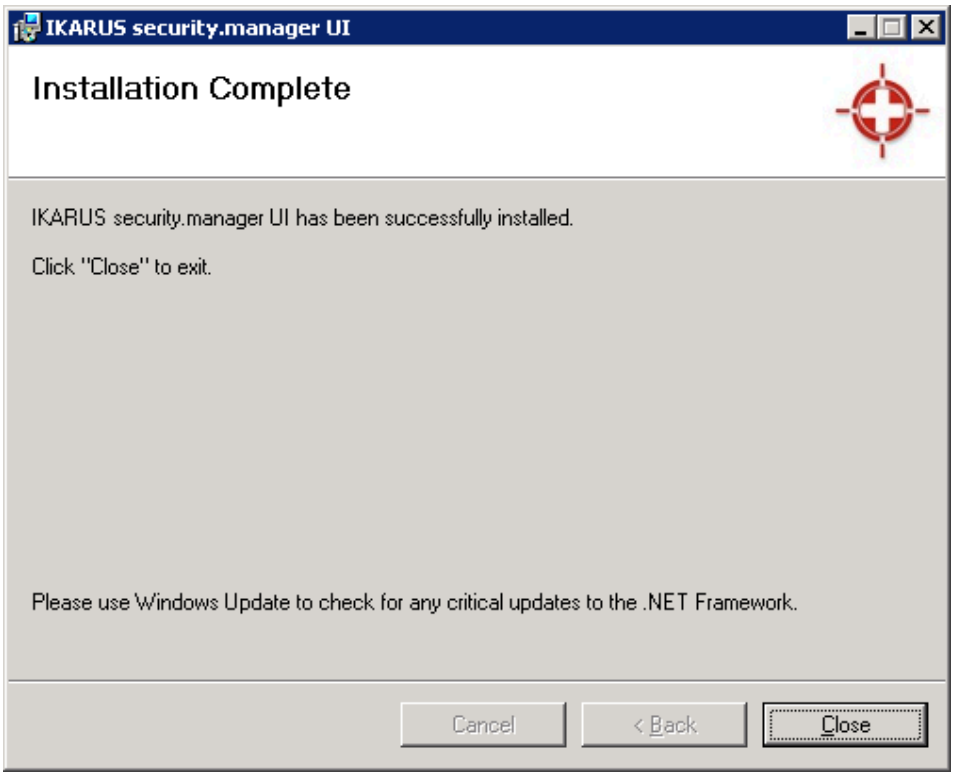


Figure 4-16 UI Installation – Installation Complete

© 2012 IKARUS Security Software GmbH

4.3 Upgrading a Legacy IKARUS Security Manager X Version to the New IKARUS security.manager

A legacy version of IKARUS Security Manager X will automatically upgrade to the new IKARUS security.manager. (This requires to enable silent updates – see section 5.2.14.4.)

After the upgrade is complete, the installation path is unchanged but the directory structure contained in will have been rearranged, and binary filenames will have changed. Therefore, you might need to create new firewall rules as appropriate.

When the upgrade has been completed successfully, the database will assume the new structure and layout.
During the upgrade, a backup of your old database named **ISMX_DATABASE_BACKUP.bak** will be created in the log folder of your installation.

© 2012 IKARUS Security Software GmbH

5 The IKARUS security.manager UI

5.1 Login

When the **IKARUS security.manager UI** starts, the first thing that appears is the ***login*** dialog box (Figure 5-1), which offers two different modes:

- Single mode ("Login to management mode" not activated)
- Management mode ("Login to management mode" activated)

Figure 5-1 UI – Login

Single mode

In this mode, it is possible to manage a specific **IKARUS security.manager**. Therefore, some menu options that are supported in management mode are not active (see chapter 5.2.18.5**Error! Reference source not found.**). The login process must be carried out again in order to connect to another **IKARUS security.manager**.

During the login, you will be requested to enter your login information and specify the server to which you would like to establish a connection (this means the server computer on which the **IKARUS security.manager server** is installed). The *TCP* standard port through which connections are established is 9887 for communication between the **IKARUS security.manager server** and the **IKARUS security.manager UI** and 9888 for communication between the **IKARUS security.manager server** and **IKARUS anti.virus** clients. You can change these ports using the *Options dialogue* of the **IKARUS security.manager UI**.

Single mode is useful for customers who only want to use one **IKARUS security.manager-Server** instance.

© 2012 IKARUS Security Software GmbH

Management mode

The basic difference from single mode is that it is possible to change between different IKARUS security.manager servers without another login process with the help of the login window. More information on changing between IKARUS security.manager servers can be found in section 5.2.1. Furthermore, the login process also changes for management mode. The login information for the individual IKARUS security.manager servers must be given at a later point in time (see section 5.1.2).

Figure 5-2: UI - Login (Management mode)

Figure 5-3: UI - Login (Single mode)

© 2012 IKARUS Security Software GmbH

5.1.1 Set Password

Single mode

When you login for the first time, you do not have to enter a password because you have not defined one yet. Simply leave the ***Password*** field free and click on the ***OK*** button. You will be prompted to enter a new password for the specified user.

Figure 5-4: UI –Password definition (single mode)

Management mode

Any password can be selected and **it is not dependent** on an **IKARUS security.manager server**. This password is used to encrypt the settings file for management mode, which contains the desired **IKARUS security.manager** data.

© 2012 IKARUS Security Software GmbH

Figure 5-5: UI –Password definition (management mode)

© 2012 IKARUS Security Software GmbH

5.1.2 Managing multiple IKARUS security.manager (management mode)

This step is **only necessary in management mode** and can be ignored by customers using single mode.

After a password has been created for the settings file, the data of the desired **IKARUS security.manager-Server** has to be added (see section **Error! Reference source not found.**). Additional information on how the password can be set for new installations can also be found in that section.

© 2012 IKARUS Security Software GmbH

5.1.3 Change Management

Single mode

If the option ***Ask for Request for Change-ID (RfC)*** is activated in the settings of the **IKARUS security.manager server** (see section 5.2.14), then you will be requested to give an RfC-ID in the login window (see figure 5-3). If the option A***sk for a comment in the login screen*** (see section 5.2.5) is activated, then you will be prompted to enter a comment each time you try to login. This is useful, for example, if you are tracking changes to the settings or if you would like to explain the actions planned for the subsequent session.

Figure 5-6 UI – Change Management

Management mode

Change management is not available for management mode.

© 2012 IKARUS Security Software GmbH

5.1.4 Set License

If you not have chosen a valid license file during the setup of the **IKARUS security.manager Server**, you will now be prompted again to either choose a license file or complete the registration using an *Activation Key*.

5.1.5 License Violation

If you are not a current **IKARUS security.manager X** user, you may skip this section; if you are, there are a number of reasons why there are more *administered* clients on your network than actually allowed. This is a license violation, which is handled in the new version of the **IKARUS security.manager**. You will be prompted to remove the excessive number of clients from *administration* to meet the requirements of the license you are using.

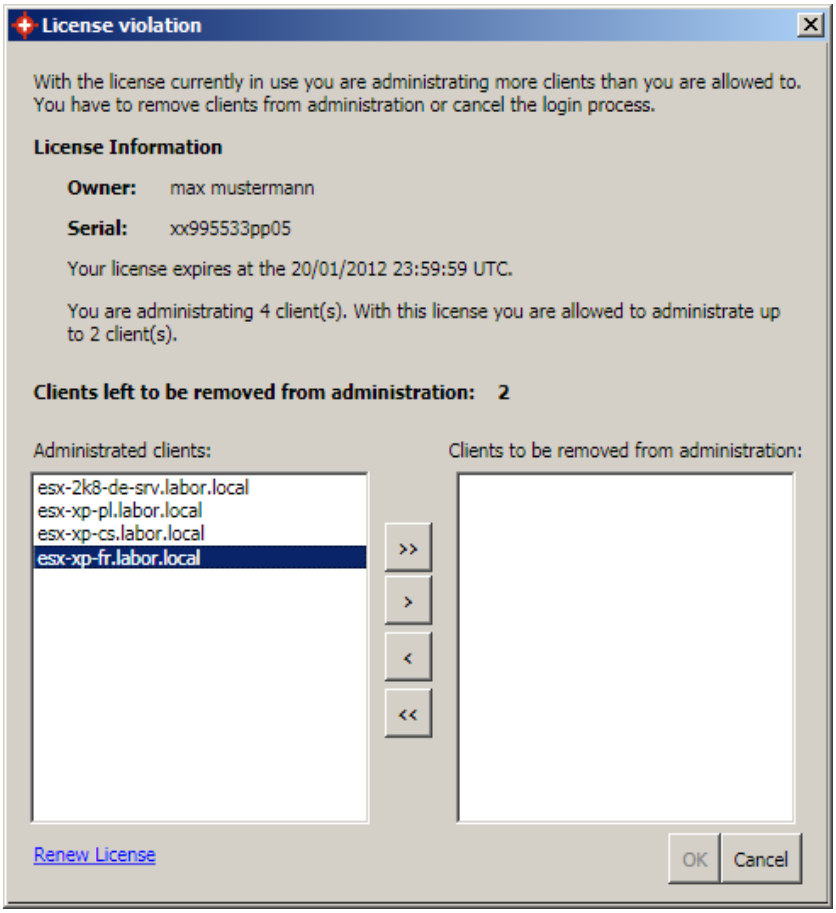


Figure 5-7 UI – License Violation

License Information: Displays the expiration date and how much of your license capacity is used and free.

Clients left to be removed from administration: Shows how many clients you need to remove from administration.

© 2012 IKARUS Security Software GmbH

The move buttons:

Move all clients to the right-hand list.

 Move selected clients to the right-hand list.

Move selected clients to the left-hand list.

Move all clients to the left–hand list.

Administrated clients: List of all clients that are administrated.

Clients to be removed from administration: List of all clients that will be removed from administration.

Renew License: Opens the registration window, see section 7.1.

The **OK** button applies all changes. This button is only enabled when you choose an appropriate number of clients. You may **cancel** this process but you will not be allowed to login to the **IKARUS security.manager UI** until you solve this issue. The **clients** will still be administered and protected by the **IKARUS security.manager** Server if you cancel this process.

If you need to purchase new licenses or have any questions concerning your license, please feel free to contact our sales team at *sales@ikarus.at*.

© 2012 IKARUS Security Software GmbH

5.2 The User Interface

The layout of the **IKARUS security.manager UI** can be customized. Each window can be docked or undocked and moved anywhere on the screen. The window layout will be stored upon closing the **IKARUS security.manager UI**.

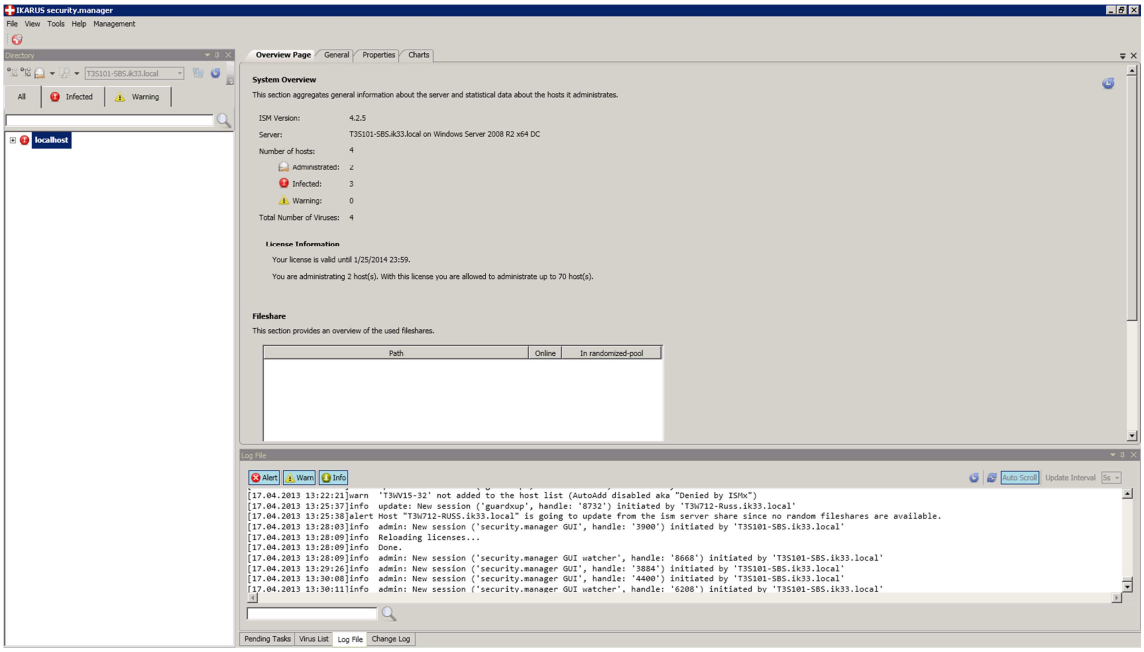


Figure 5-8 UI – User Interface

© 2012 IKARUS Security Software GmbH

5.2.1 Directory

The **Directory** (Figure 5-9) is the center of almost all *client* related operations. It holds the *clients* of your *Active Directory* and the *clients* you manually add (e.g. *clients* that exist outside your *domain* or in a different *domain*). All *clients* in the *Active Directory* are automatically listed with their ***FQDN***. It is **highly recommended to always specify the *FQDN*** of **manually added *clients*** – *clients* with the **same name might exist in different *domains*** and there is **no way to distinguish between them**.

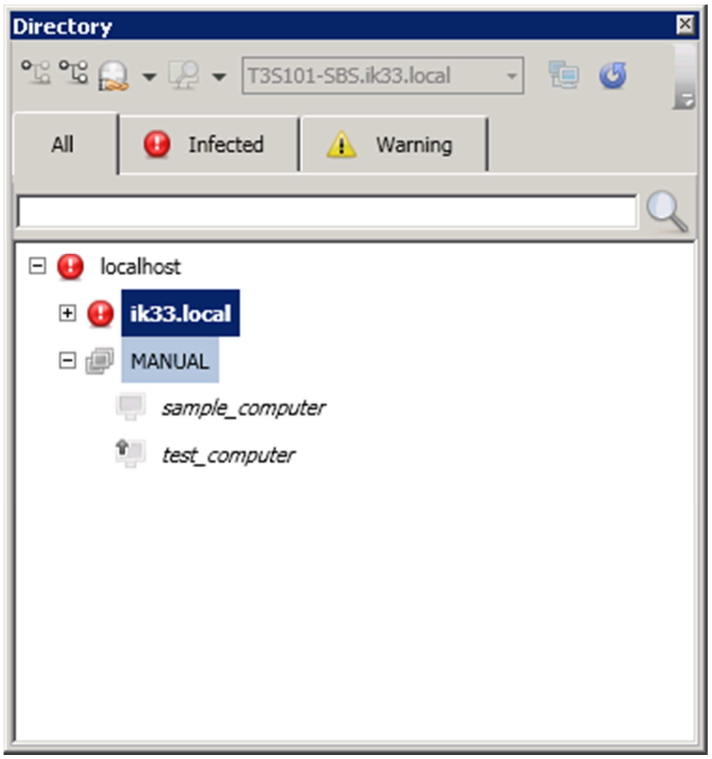


Figure 5-9 UI – Directory (single mode)

The directory window contains three sections. In the upper section the toolbar (see Figure 5-10) and in the middle section the Group/Client tree (see Figure 5-14). In the lowest section is the Filter section (See Figure 5-16), where the tree can be searched for clients or groups. The tree has also filters for clients with warning messages or infected clients.

© 2012 IKARUS Security Software GmbH

5.2.1.1 *Formatting*

Node names are formatted depending on their respective status:

Normal:	This client is **online**.
Italic:	This client is **offline**.
Bold:	This node is **selected**.

5.2.1.2 *Layout*

The ***Directory*** is separated into the following three sections:

5.2.1.2.1 The Toolbar

Figure 5-10 UI - Directory Toolbar

The symbols described from left to right mean the following:

a. Collapse all group nodes.
b. Expand all group nodes.
c. Opens the context menu for actions on the currently selected client (See Context Menu in this section).
d. Scan options, see next figure.
e. Chooses current connected IKARUS security.manager instance (check “change current IKARUS security.manager instance” in this section)
f. Connect again to the current selected IKARUS security.manager instance. (see “reconnect” in this section)
g. Refresh the directory.

The scan options: Figure 5-11 contains possible Scan Options.

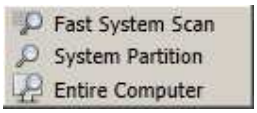


Figure 5-11 The scan options

- **Fast System Scan:** Scans the windows directory and active processes (Only on currently selected client).
- **System Partition:** Scans the system partition (Only on currently selected client).
- **Entire Computer:** Scans the entire system (Only on currently selected client).

The Context menu: Figure 5-12 shows all entries of the context menu that is available by clicking right mouse-button.

© 2012 IKARUS Security Software GmbH

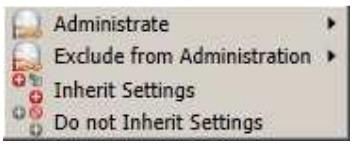


Figure 5-12 The context menu for actions on a client

Administrate/Exclude from Administration: This context menu entry is also split up in further entries (see Figure 5-13)

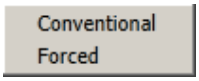


Figure 5-13 The choice for administration or exclusion from administration

- Administrate/Exclude from administration: Allows/prevents updates and system protection.
- Administrate/Exclude from administration forced: Ignores administration from another IKARUS security.manager.

Inherit Settings/Do not Inherit Settings: Settings are taken/not taken from the parent node.

Change current IKARUS security.manager instance: The main feature of the version 4.2.x is the management of more than one IKARUS security.manager-Servers. This is now possible by choosing the IKARUS security.manager-Server within the selection-box (see Figure 5-10 point (g)). The selection-box is shown only in management-mode. Single-mode uses automatically the IKARUS security.manager-Server which is entered in login-window.

Reconnect: This action is only possible when no connection to the current selected IKARUS security.manager-Server is established. If the connection may not work, please verify your connection settings. For editing use options in management-mode-menu (see 5.2.16.1).

© 2012 IKARUS Security Software GmbH

5.2.1.2.2 The Group/Client Tree

In the Group/Client tree the main node is always the first node in the tree (named “All”). This and all other nodes that have the same symbol in front of it are group nodes.

Nodes that have a computer monitor in front of them are client nodes (e.g.: node with the name “manual computer”).

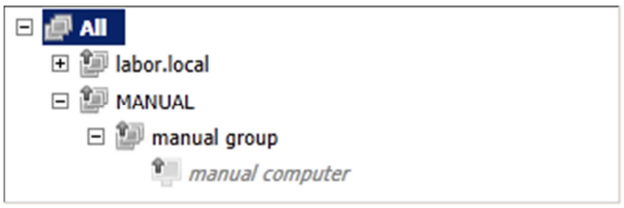


Figure 5-14 The Group/Client Tree

When an item is right-clicked with the mouse the context menu is opened. In the following figure all possible context menu entries are shown, but not all are always available. The first four in the context menu (Add Group, Add Computer, Delete and Rename) are only available for manually added groups/clients. The other entries are all shown when a group is selected. For hosts are only possible actions available. Please keep in mind that the data-estimation might take some time. This leads to the fact that the data might not be immediately shown correctly after applying some changes.

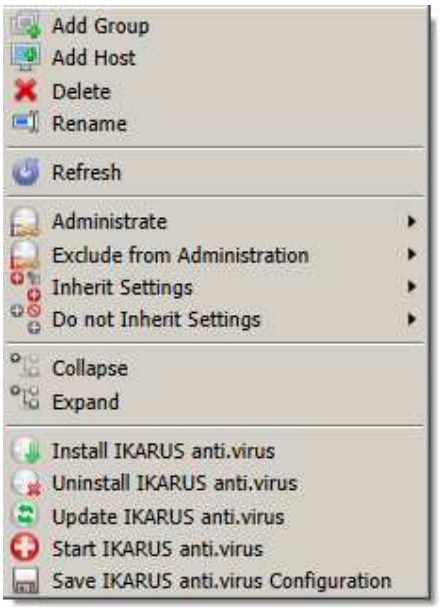


Figure 5-15 The Context-Menu for a Group/Client

© 2012 IKARUS Security Software GmbH

5.2.1.2.3 The Filter Section

Figure 5-16 UI – Directory Filter

In the filter section of the directory a filter can be defined in a text box. This applies a case-insensitive filter by name. Only nodes that meet the filter criteria will be displayed. With the magnifying glass the next element matching the filter is selected.

The predefined tab filters are (see figure above):

- All (active): Overview of all clients in your directory and all manually added clients.
- Infected (inactive): Overview of all clients that are infected.
- Warning (inactive): An overview of all outdated clients, i.e. clients with a virus database, spam database (should spam detection be enabled) and anti.virus update being older than 2 weeks. Also includes clients that are administrated and online but do not execute IKARUS anti.virus or cannot be reached by the IKARUS security.manager.

© 2012 IKARUS Security Software GmbH

5.2.1.3 *Icons*

The icons of the nodes in the *Directory* provide a quick overview of the node statuses.

This node is a **group**.

This client is **offline**.

This client is **online** and has **no IKARUS anti.virus installed**.

This client is **online**, has the **IKARUS anti.virus installed**, and is **administered**.

This client is **online**, has the **IKARUS anti.virus installed**, and is **not administered**.

(Overlaid) This node **inherits settings from its parent**.

(Overlaid) This node or one of its children **is infected**.

(Overlaid) This node or one of its children **is outdated or administered but unreachable**.

5.2.1.4 *Manual group*

The Manual group (displayed as **MANUAL** in the *directory*) is the bottommost group node in the root (**All**) node of the ***directory***. If you want to add computers from other *domains*, or from no *domain* at all, this is the place to do so. You can add, rename, remove, and move nodes (*clients* and groups).

5.2.1.5 *Multi-selection*

You can **select** multiple nodes by **holding the Ctrl key on your keyboard while clicking**. Consider that a multi-selection of a **temporary group node** does not exist anymore when multi-selection is canceled (e.g. by simply selecting a single item). **Actions and views available for group nodes** are also **available for a temporary group**.

5.2.1.6 *Administering Groups*

If you administer a group, all children (clients and subgroups) will inherit from that group and binary updates will be automatically allowed for each client. All clients within the group where the IKARUS anti.virus are installed will be administered by your IKARUS security.manager.

© 2012 IKARUS Security Software GmbH

5.2.2 Pending Tasks

Actions such as installing the **IKARUS anti.virus** or *(un)administering* clients are configured as tasks on the **IKARUS security.manager Server**. Tasks are session-specific and processed tasks get lost when the **IKARUS security.manager UI** login session is closed. Not finished tasks are still available. The **Pending Tasks** window (Figure 5-17) displays all available tasks (either *client* specific and for the whole ***Directory*** tree) with their current states, results and resolve times. Consider the resolve time the date when the task state will be re-evaluated. Depending on the task state, an action will be performed to resolve the task.

Keep in mind that next scheduled time may be outdated because automatic refresh is deactivated or the update interval is set higher. Therefore this timestamp is as new as the last refresh occurred!

5.2.2.1 *Layout*

Toolbar on the top of the window
The elements of the toolbar are described from left to right (see Figure 5-17):

a. **Pending**: Shows or hides pending tasks.
b. **Active**: Shows or hides active tasks.
c. **Waiting**: Shows or hides waiting tasks.
d. **Processed**: Shows or hides processed tasks.
e. **Client specific**: Displays tasks from the currently selected node in the Directory if enabled, otherwise all tasks are displayed.
f. **Refresh**: Retrieves an updated task list.
g. **Automatic Refresh**: Retrieves an updated task list automatically based on the user-defined update Interval.
h. **Update Interval**: Sets the update interval of the task list.

The Pending Tasks list
In the Pending Tasks List all tasks that are available on the IKARUS security.manager Server are shown, with their current status, since the last update from the server. If a task was restarted, it is shown as sub task in the task list. Those tasks show the status of the tasks, see section 5.2.2.2. Double-clicking a task will open the detail view, see Section 5.2.2.3.

The **Next Scheduled Resolve Time** shows the date and time when all tasks will be started again and the server will try to resolve them.

The Context Menu for Pending Tasks
The context menu is opened by a right-click on a task in the pending task list. There are several actions available in the context menu:

- **Force**: Forces the completion of the task.
- **Stop**: Stops the completion of the task.
- **Restart All:** Restarts all subtasks.
- **Restart Incomplete:** Restarts only the incomplete subtasks.
- **Details**: Opens the detail task view, see Section 5.2.2.3.

© 2012 IKARUS Security Software GmbH

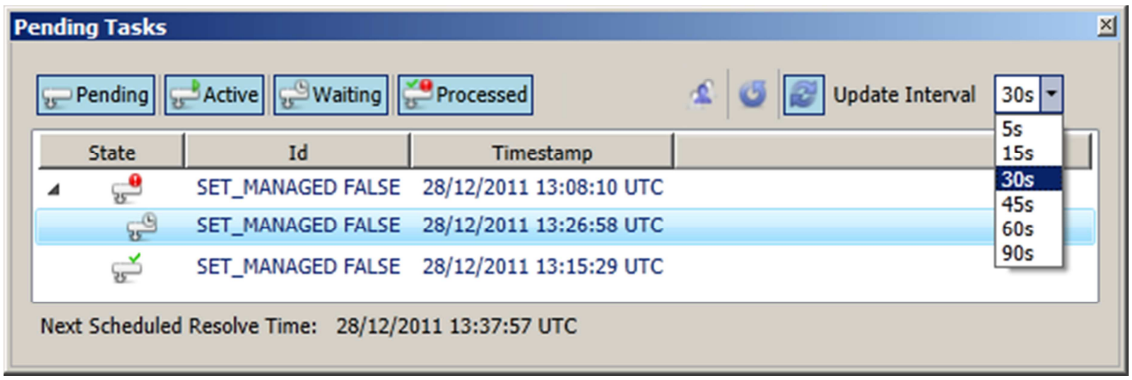


Figure 5-17 UI – Pending Tasks

© 2012 IKARUS Security Software GmbH

5.2.2.2 *Task States*

Icon	State	Reason	Action on Resolving
	Active	The action is currently in progress.	Evaluates the task state only.
	Pending	The action has not been processed yet.	The task will be processed soon.
	Waiting	The action has been launched at least once but the target client(s) were not reachable.	Will retry to reach target clients.
	Processed	The action was successfully processed.	Evaluates the task state only.
	Not processed	The action was not processed because the user canceled the task.	Evaluates the task state only.
	Processed with an error	The action was processed but there was an error during the action.	Evaluates the task state only.

5.2.2.3 *Task Details*

Toolbar

- **Number of Hosts**: Shows the amount of hosts which are targeted in this task.
- **Refresh**: Retrieves an updated host- and task-list.
- **Automatic Refresh**: Retrieves an updated host list automatically based on the user-defined update interval
- **Update Interval**: Sets the update interval of the host list.

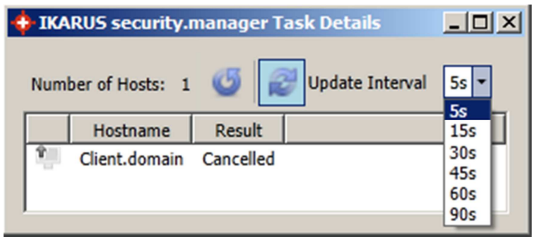
Host List

In the first column the **Host State** is described, which shows the status of the target host, see Section 5.2.1.3. The **Hostname** of the target host is shown in the second column and the **Result** of the action is shown in the last column.

Context Menu

On right click on a host list entry the context menu opens, where the following two actions are available:

- **Force**: Forces the completion of the task on this host.
- **Cancel**: Cancels the completion of the task on this host.



© 2012 IKARUS Security Software GmbH

Figure 5-18 UI – Task Details

© 2012 IKARUS Security Software GmbH

5.2.3 Virus List

The **Virus List** window (Figure 5-19) is useful for investigating the infections on your network. You can view all infections found or just those on the node currently selected in the *Directory*.

5.2.3.1 *Layout*

Information area
On the left side of the information area, in the upper third of the virus list window, you can overall information about the virus list. The information can be minimized through the toggle button “Client specific”. This button shows infections of all clients if enabled, otherwise only those of the currently selected node in the Directory, see Section 5.2.1.

On the left side of the area the **number of viruses** shown in the list is outlined.

Virus list
The virus list consists of several informational columns:

- **Is Active?:** This column is no longer shown in the virus list (It was only temporarily shown in the 4.0. IKARUS security.manager version). Inactive virus’s means that those viruses have been found on hosts that are not administrated by the IKARUS security.manager.
- **Host Status:** Shows the status of the client, see Section 5.2.1.3.
- **Hostname:** Shows the name of the client.
- **Date:** The date the infection was found.
- **Filename:** The filename of the infection.
- **Path:** The directory the infection was found in.
- **Virus Description:** The name of the infection. Clicking will open the virus dictionary for this particular infection.

With a right mouse click the context menu for a virus list entry opens. In the context menu the following actions can be chosen:

- **Virus Dictionary:** Opens the virus dictionary entry for the infection.
- **Details:** Opens the detail view for this infection, see Section 5.2.3.2.
- **Send to IKARUS Virus Lab:** Sends the infection to IKARUS for analysis.

Action area
In the action area (it can be found at the bottom of the window) several functionalities are provided that are also available in the IKARUS anti.virus.

- **Select All:** (De)Selects all entries.
- **Refresh button:** Refresh the virus list.
- **Purge System:** Deletes the selected infections of the list.
- **Temporary Unblock:** Releases the file from quarantine.
- **Save & Delete:** Creates a backup of the infected file and deletes the original.

© 2012 IKARUS Security Software GmbH

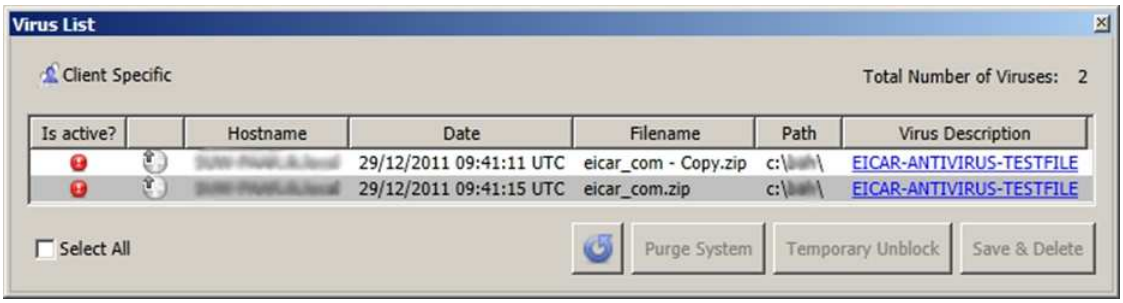


Figure 5-19 UI – Virus List

5.2.3.2 *Virus Information*

The Virus Information window (Figure 5-20) displays useful information about a particular infection. You can copy the information to the clipboard by clicking the *Copy to Clipboard* button.

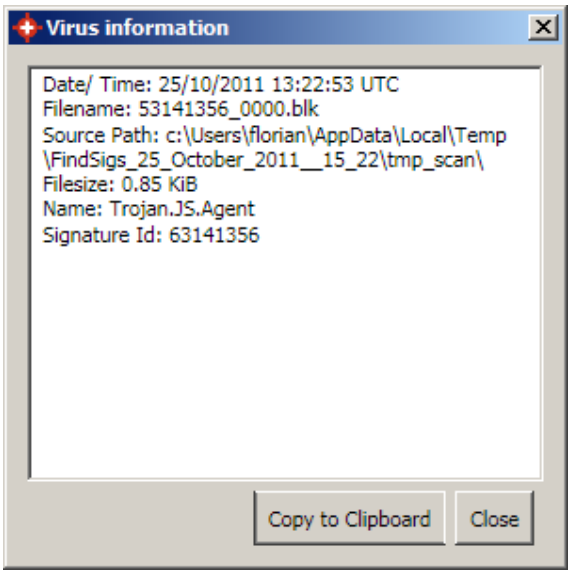


Figure 5-20 UI – Virus Information

© 2012 IKARUS Security Software GmbH

5.2.4 Log File

The **Log File** window (Figure 5-21) provides **useful information** on the **background actions** performed by the **IKARUS security.manager Server**. If you encounter unusual behavior or any kind of problem, the **Log File** window (Figure 5-21) is **an easy way to access the IKARUS security.manager Server log from anywhere** using the **IKARUS security.manager UI**. In addition, you can narrow the information to be displayed: **Alerts, Warnings or just information**. This simplifies **investigating the root cause of a problem**. Alternatively, you may use the search field to step through the **Log File**.

5.2.4.1 *Layout*

In the upper area of the Log File window it is possible to decide what information is displayed and how often the information is updated from the server.

The buttons descripted from left to right:

- **Alert**: Shows or hides alerts.
- **Warn**: Shows or hides warnings.
- **Info**: Shows or hides information.
- **Refresh**: Retrieves an updated log file from the ISM server.
- **Automatic Refresh:** Retrieves an updated log file from the ISM server automatically based on the user-defined update interval.
- **Auto Scroll:** Scrolls to the bottom of the log file on automatic refreshes.
- **Update Interval:** Set the interval at which the log file should be updated.

Beneath this area the log file is shown. In the log file you can press the right mouse button to open the context menu. In the context menu you can either press “Select All” (to select all the text of the log file) or “copy to clipboard”.

In the lower area it is possible to search for special text in the log file. Just enter the text, you want to search for, in the text box and press the loop to search the log file. The search will start from the position of the text cursor in the log file.

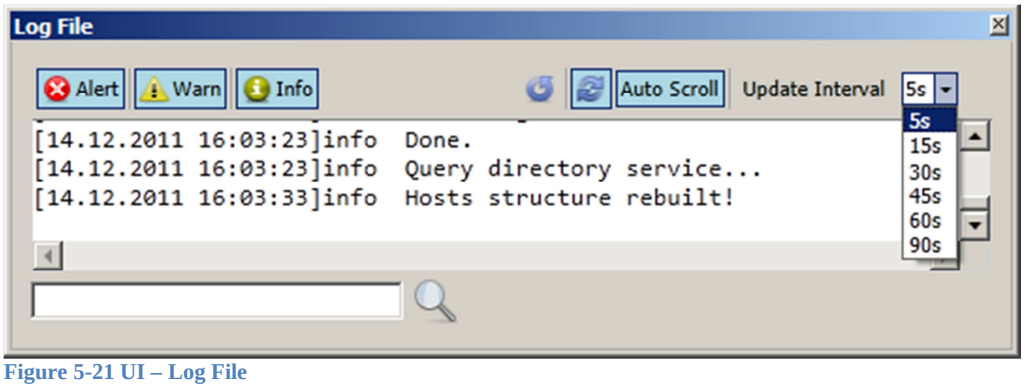


Figure 5-21 UI – Log File

© 2012 IKARUS Security Software GmbH

5.2.5 Change Log

The **Change Log** window (Figure 5-22) provides an overview of the changes a user made to settings and when they have occurred.

5.2.5.1 *Layout*

The change log can be refreshed with the refresh button in the upper right corner and in the list all changes in the IKARUS security.manager can be seen. The columns of the list are:

- **Id:** Identification number of the modification.
- **Category:** Shows where the modification happened.
- **Field Id:** Shows which particular setting was modified.
- **Old Value:** Shows the value before the modification.
- **New Value:** Shows the value after the modification.
- **Timestamp:** Shows when the value modification happened.
- **Comment:** Shows the comment entered at the login process.

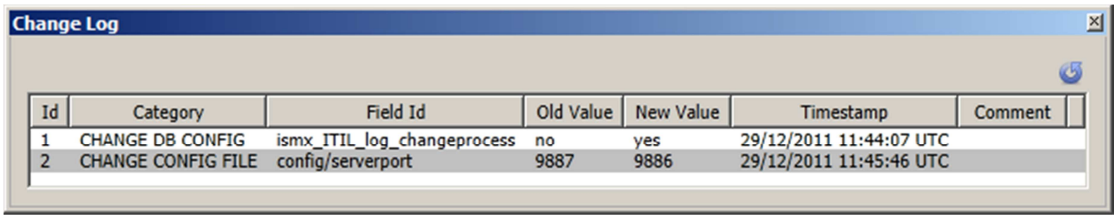


Figure 5-22 UI – Change Log

© 2012 IKARUS Security Software GmbH

5.2.6 Overview Page

The **Overview Page** window (Figure 5-23) aggregates **general information** on the **IKARUS security.manager Server** and **statistical information** on the ***clients*** **in the** ***Directory*** as well as the added *fileshares* and their online/offline-states.

5.2.6.1 *Layout*

The overview page can be refreshed with the refresh button placed in the upper right corner and consists of the following sections:

- **Server information:** Displays information about the ISM Server version and the host it is running on
- **Quick client overview:** Provides a quick overview of all clients in the directory
- **License Information:** Displays the expiration date and how much of your license capacity is used and free.
- **Fileshare Information:** Displays information of online/offline fileshares.
- **Update Overview:** Provides a quick overview of the version numbers the ISM Server has ready to deploy to its clients.

© 2012 IKARUS Security Software GmbH

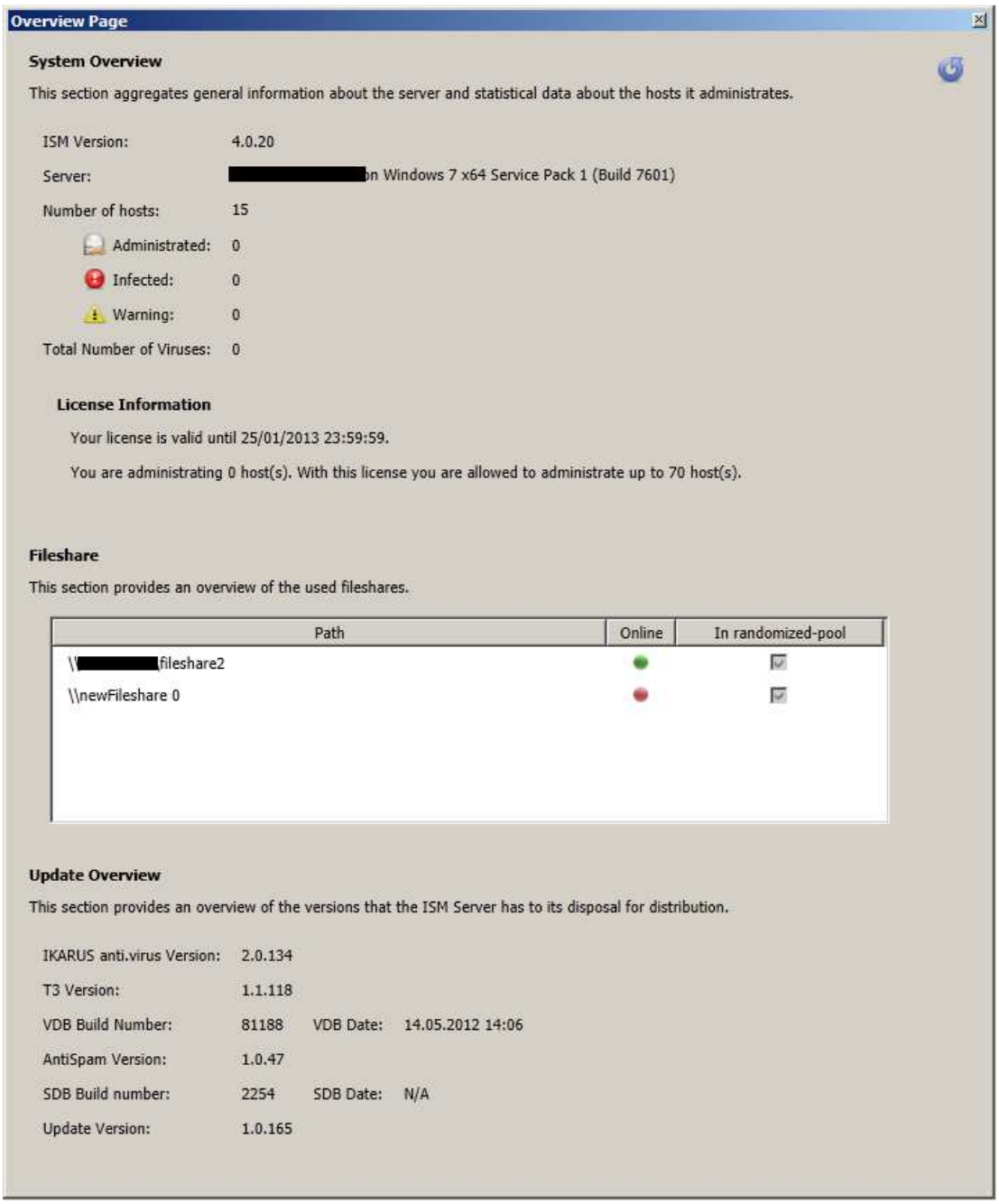


Figure 5-23 UI – Overview Page

© 2012 IKARUS Security Software GmbH

5.2.7 Properties Page

The **Properties Page** window (Figure 5-24) provides a quick overview of the **IKARUS anti.virus Configuration a *client* or group uses** and **when and how updates are issued** for this *client* or group. You can set these settings ***client*-wide** or **group-wide** and let a group's ***clients*** **inherit settings from the parent level**. If you choose to **inherit settings for a group**, you will be asked if you also want **the *clients* in that group to inherit the settings**; on the contrary, if you choose to **remove the inheritance settings of a group**, you will be asked if you want **to remove the inheritance settings from the *clients* in that group as well**.

5.2.7.1 *Update Section*

In the **Update Section,** you can specify **when and how updates are performed**. It is possible to define per group or host one concrete *fileshare* that is always asked for an update. The default way for getting updates is a **randomly chosen *fileshare* from the randomized-pool**. *Fileshares* that are shown **italic are at the moment offline**. For further information about this topic, see section 5.2.14.5.
If you **disallow binary updates, only virus and spam databases will be updated;** the **IKARUS anti.virus will not**. If you for any reason want to **hide** the **IKARUS anti.virus system tray status notifications** (e.g. on a computer used for **presentations** where pop-up windows would otherwise **distract the audience**), enable the **Disable system tray Status Notifications** checkbox.

5.2.7.2 *Rights Management*

The **Rights Management** section is useful for ***clients* that are outside the *domain* of the IKARUS security.manager Server**. Since the **IKARUS security.manager Server** needs **appropriate rights to establish a connection and execute binaries remotely,** you can specify **credentials having the appropriate rights on this *client* to perform these operations**.

5.2.7.3 *Layout*

At the top of the window is the name and status icon of the currently selected host or group shown. All other items on the window are descripted below:

- **Inherit Settings:** Inherits/disinherits settings from the parent node. Inheritance is saved automatically e.g. you do not need to click the „Save" button.
- **IKARUS anti.virus Configuration:** Sets the configuration this client is using.
- **Update Time:** Choose the time span in which updates are performed.
- **Fileshare:** Choose a concrete fileshare or take one from randomized pool if an update is necessary.
- **Allow Binary Updates:** Allows updates to the IKARUS anti.virus binaries. Databases will still be updated if binary updates are disallowed.
- **Disable system tray Status Notifications:** Prevents the IKARUS anti.virus tray status notifications to pop up.
- **Get Updates from External Servers:** Allows IKARUS anti.virus to download updates from the Internet should the ISM be unable to provide updates.

© 2012 IKARUS Security Software GmbH

- **Username/Password:** Sets the credentials to be used for interaction with this client. If the client is not in the same domain as the ISM server, setting these credentials correctly is mandatory to ensure correct administrative behavior on this client.
- **Browse Directory Group:** Defines which Directory Groups are allowed to make some changes in IKARUS anti.virus.
- **Delete restriction:** Removes a previously set Directory Group restriction.
- **Save Button:** Saves these settings.
- **Cancel Button:** Discards any changes made.

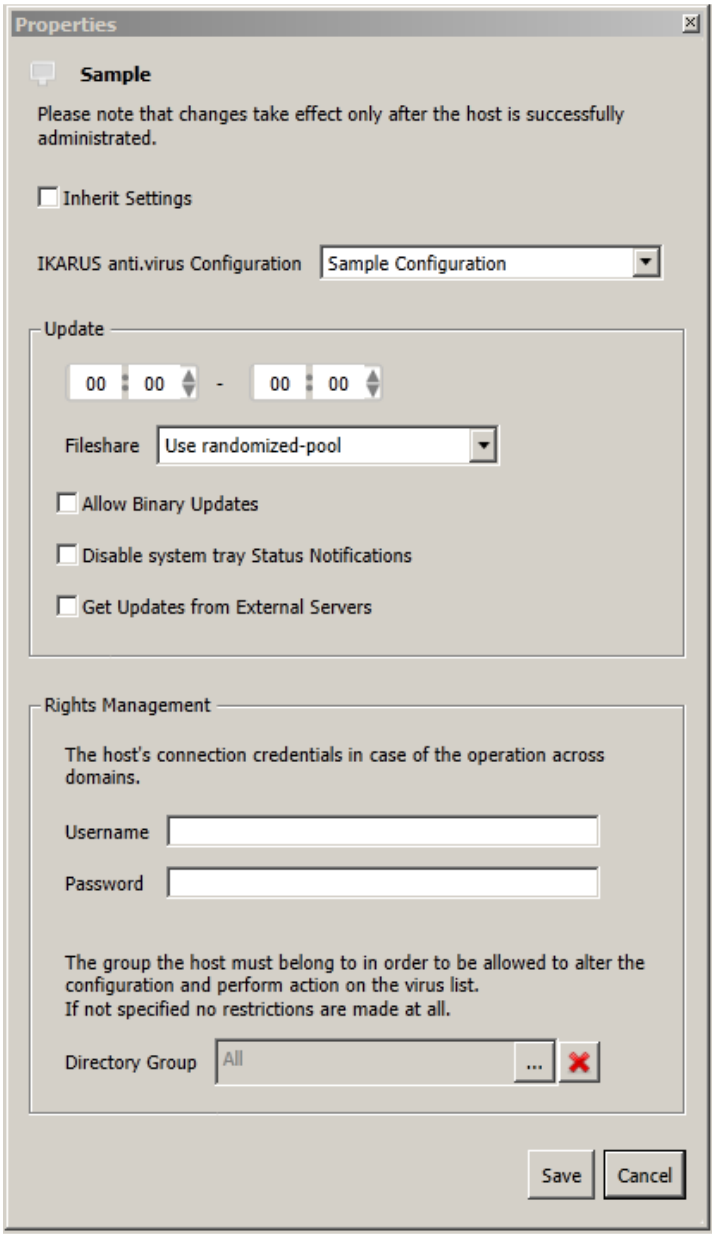


Figure 5-24 UI – Properties Page

© 2012 IKARUS Security Software GmbH

5.2.8 General Page on Groups

The **General Page** window (Figure 5-25) on **groups** displays **statistical information about *clients* within the currently selected group node.** It provides you with an **easy way to investigate the status of multiple *clients* in one place**. If you need to investigate the status of multiple *clients* **that are not in the same group**, you may use the ***Multi-selection*** **feature of the *Directory***.

5.2.8.1 *Layout*

The General page for groups' shows summed up information about all hosts that are part of this group. At the top of the page general information is shown, such as:

- **Name of the group:** Shows the name and status icons of the current node.
- **Total Number of Viruses:** Shows the total number of infections on the current node.
- **Number of Clients Online:** Shows the total number of online clients on the current node.
- **Number of Clients Guarded:** Shows the total number of guarded clients on the current node.
- **Administrated:** Shows the total number of administrated clients on the current node.

In the clients list beyond the general information, all hosts of the group can be seen in more detail, with the following information:

- **Status Icon:** Shows the status icons of this client.
- **Name:** Shows the name of this client.
- **Infections:** Shows the number of infections on this client.
- **Online:** Shows the online status of this client.
- **Service Installed:** Shows the service installation status of this client.
- **Administrated:** Shows the administration status of this client.
- **Last Update:** Shows the date in UTC of the last update process on this client.
- **Last Time Online:** Shows the date (in UTC format) of the last time this client was online.

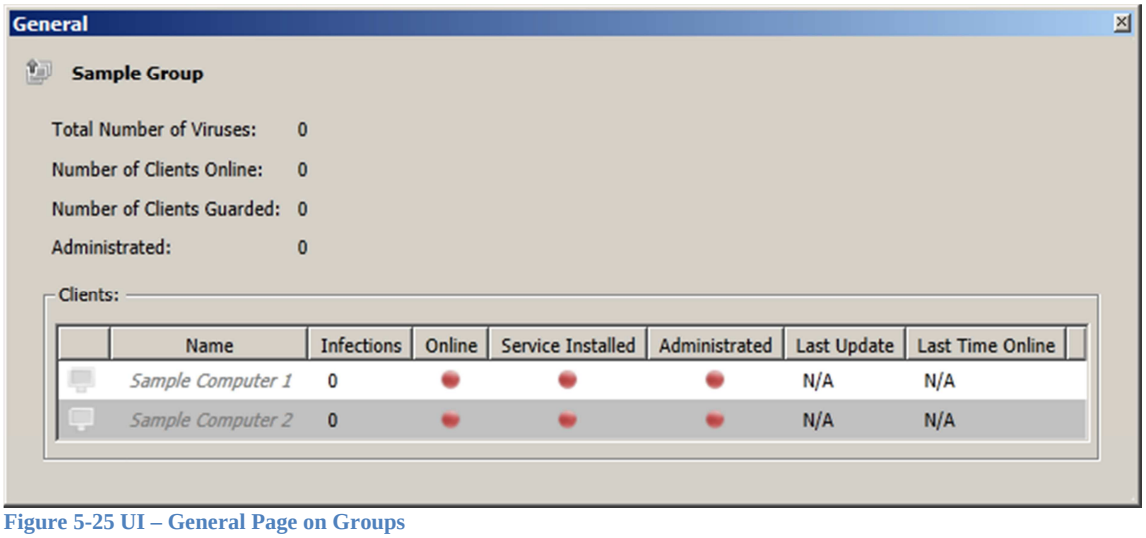


Figure 5-25 UI – General Page on Groups

© 2012 IKARUS Security Software GmbH

5.2.8.2 *Icons*

- Red icon means “No“
- Green icon means “Yes“

© 2012 IKARUS Security Software GmbH

5.2.9 General Page on Clients

The **General Page** Window (Figure 5-26) of a *Client* displays **detailed information on the currently selected** *client*.

5.2.9.1 *Layout*

The general page for clients is separated into informational sections. Those sections are:

- **General:** Displays online, service installation and administration statuses of this client.
- **Update:** Displays the time of the last update to this client and the date the next update process will occur.
- **Versions:** Displays the IKARUS anti.virus, database, scan engine and update versions of this client.
- **Protection:** Displays the serial number, scan status, number of infections and protection mechanisms that are enabled or disabled.

© 2012 IKARUS Security Software GmbH

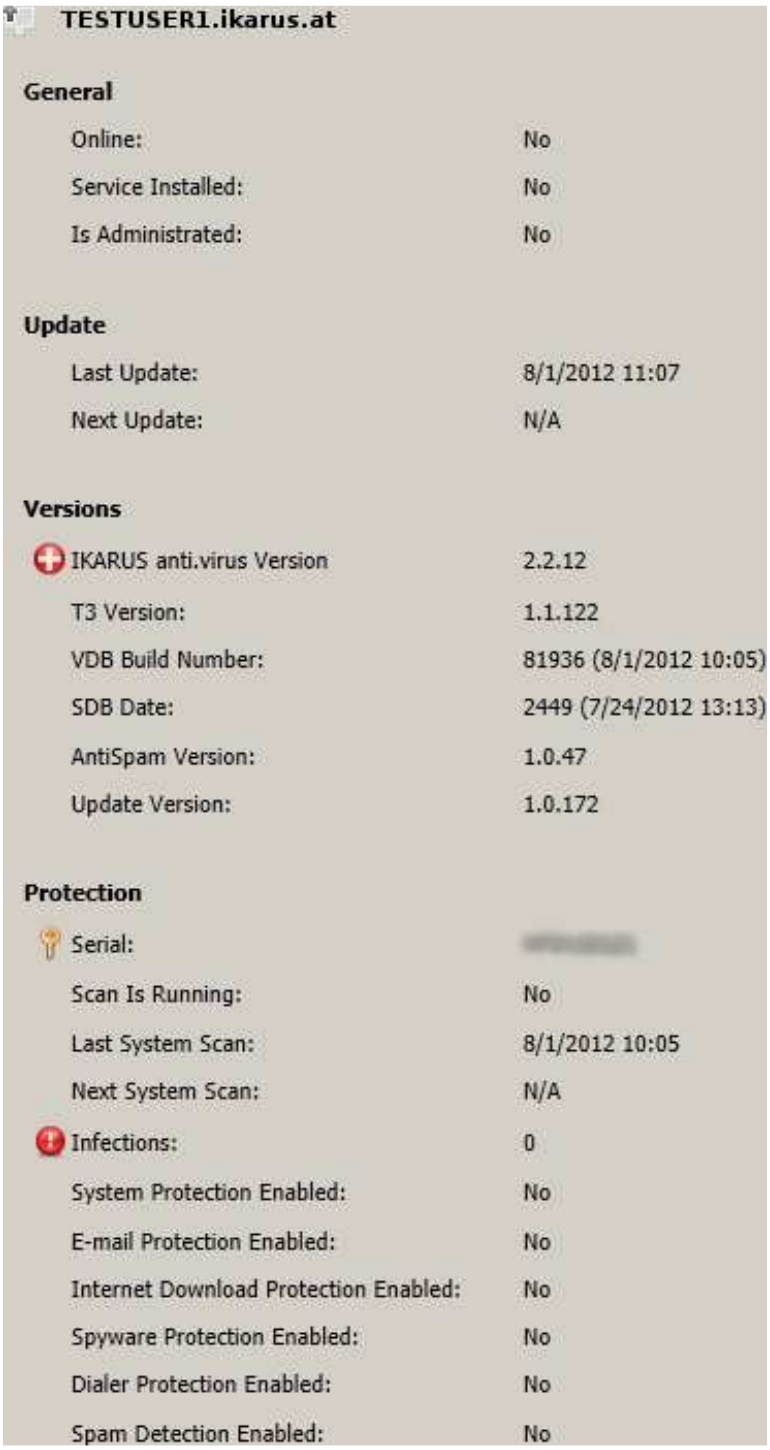


Figure 5-26 UI – General Page on Clients

© 2012 IKARUS Security Software GmbH

5.2.10 Notification Bar

The **Notification Bar** control (Figure 5-27) is hidden by default. It will only be displayed if there have been changes to the virus list of a *client*. If the **IKARUS security.manager UI** is not the active (foreground) application, the **IKARUS security.manager UI** entry in the Windows taskbar will start flashing to inform you that there are virus list changes.

5.2.10.1 *Layout*

Figure 5-27 UI – Notification Bar

5.2.11 Charts Page

The **Charts Page** shows the 5 standard charts that are currently available in the **IKARUS security.manager** and those 5 charts can be edited in the **IKARUS security.manager options** (see section 5.2.14.7).

The 5 standard charts are:

- Administration of Hosts,
- Availability of Hosts,
- Infection of Hosts,
- Virus Top 5 and
- Virus per Operating System.

In the page not only the charts are displayed, but also the time of creation. The charts can easily be refreshed by pressing the refresh button in the upper right corner.

The button to the left of the refresh button is used to create a PDF report of the charts. This report only holds all charts that were currently displayed in the **Chart Page**. The PDF report can also be adapted in the **IKARUS security.manager options.**

Note: You need to have a PDF viewer installed to view the PDF report.
Note: For further information on how the charts can be edited and adapted go to the IKARUS security.manager options (see 5.2.14).
Note: For displaying charts **at least Internet Explorer Version 7** must be installed. To ensure full functionality it is recommended to use **Internet Explorer Version 9**. Consider to enable JavaScript because this is used for estimating charts.

© 2012 IKARUS Security Software GmbH

5.2.11.1 *Layout*

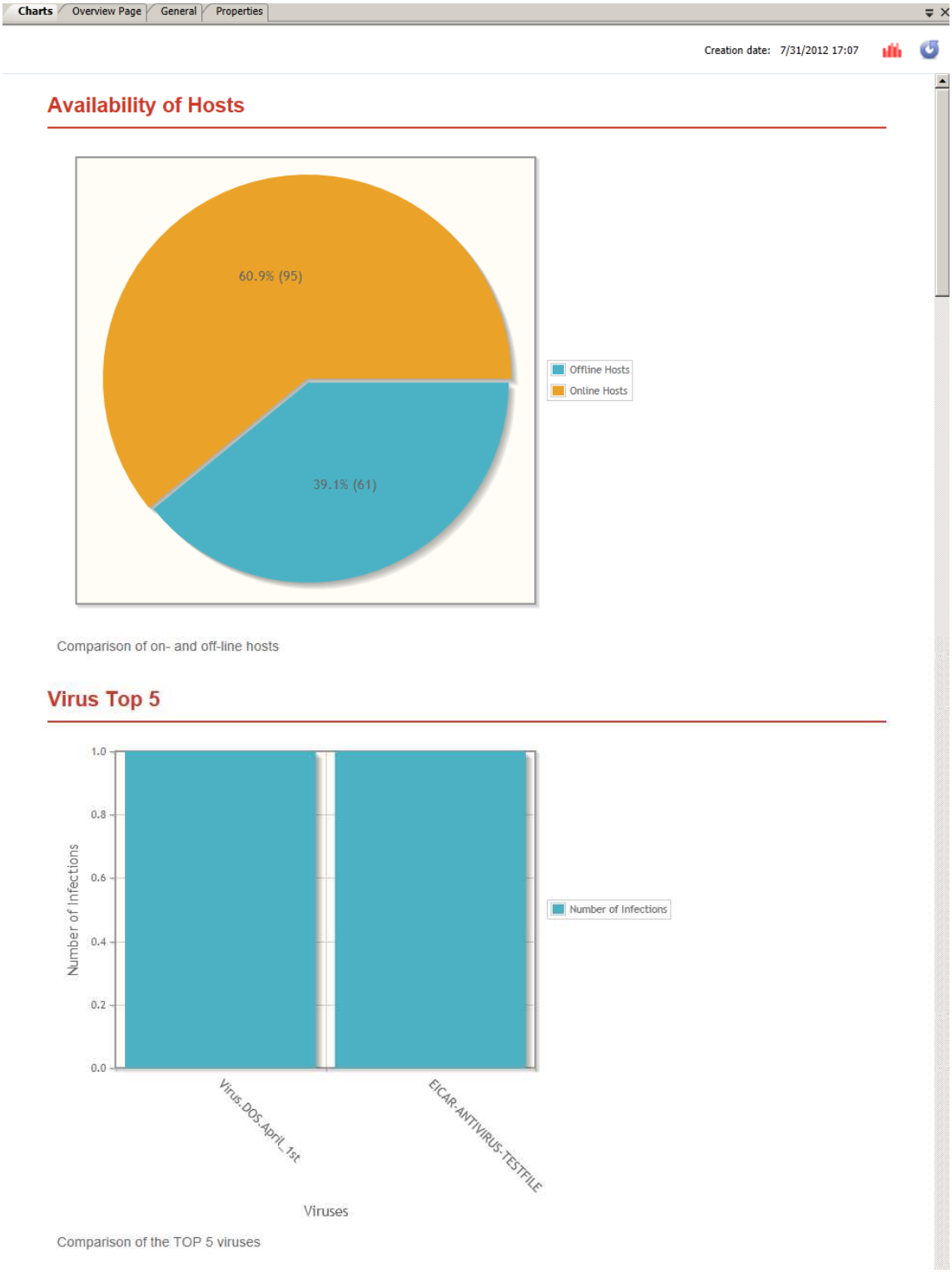


Figure 5-28 UI – Charts Page

© 2012 IKARUS Security Software GmbH

5.2.12 Global overview page

This screen is used as an overview of all registered **IKARUS security.manager servers** (see figure Figure 5-29), which is only available in management mode. The most important information is shown like the number of computers, how many computers are being administrated or are infected or not up-to-date. Furthermore, the current license, version and time stamp in connection with the last update are shown.

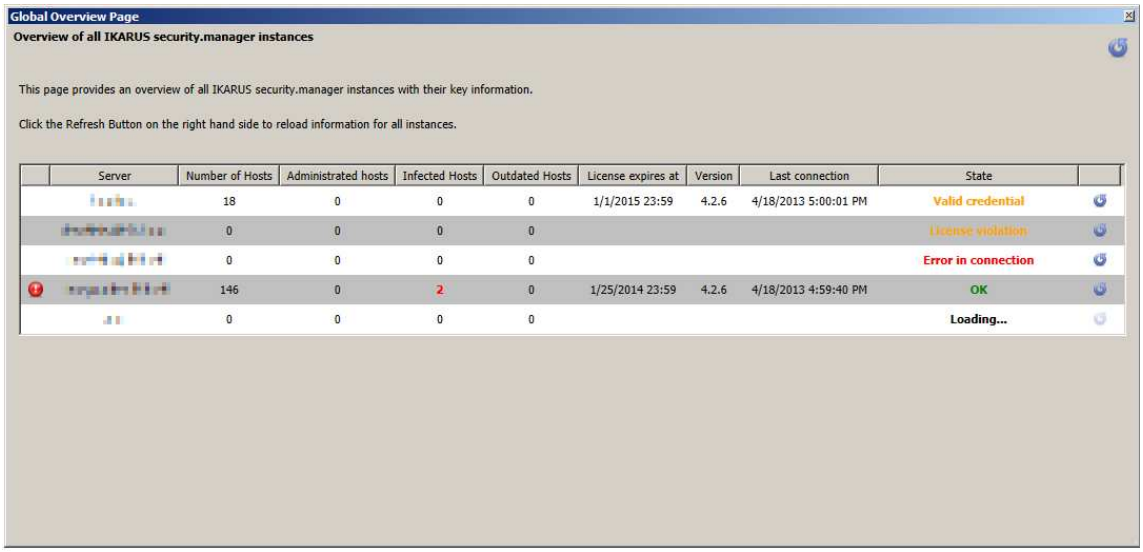


Figure 5-29 UI – Global overview page

The data of **IKARUS security.manager servers** is **not** updated automatically. The most recently retrieved connection data is saved and is available for the next login. Each **IKARUS security.manager server** can be updated individually by clicking in the respective line. The symbol on the top right can be used to update all entries in the global overview page.

After each update, the current status is provided, which gives information on possible problems:

- **Loading…**
  The data is being retrieved.
- **OK**
  The information was loaded successfully.
- **Error in connection**
  The connection could not be established.
- **Valid credentials**
  The access data is valid
- **License violation**
  There was a problem with the license, which should be clarified.
- **The last connection was established more than two days ago**
- **No connection has never been established**

If a version is being used that is older than 4.2.x, then that **IKARUS security.manager server cannot be used with management mode**. Nevertheless, they are shown in the global overview page.

© 2012 IKARUS Security Software GmbH

Furthermore, it is possible to use the right mouse button to call up the shortcut menu with the following entries (see).

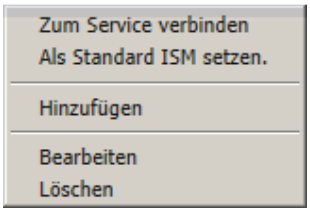


Figure 5-30 UI – Global overview page - shortcut menu

- Connect to service
  Changes to the currently selected **IKARUS security.manager server** and closes the connection to the previously selected **IKARUS security.manager server**.
- Set to default ISM.
  The currently selected **IKARUS security.manager server** is set to be the default server after a restart.
- Add
  Adds a new **IKARUS security.manager server** to the list. See chapter **Error! Reference source not found.** for more information.
- Edit
  The login properties of the currently selected **IKARUS security.manager server** are edited. The edit dialogue is not available if the selected **IKARUS security.manager** already has a connection to it or a connection is currently being established. See chapter **Error! Reference source not found.** for more information.
- Delete
  The currently selected **IKARUS security.manager server** is deleted permanently from the management list. Therefore it is no longer possible to establish a connection. The currently connected or default **IKARUS security.manager server** cannot be deleted from the list.

© 2012 IKARUS Security Software GmbH

5.2.13 IKARUS anti.virus Configurations

The **IKARUS anti.virus Configurations** window (Figure 5-31) lists all available **IKARUS anti.virus configurations** and the *clients* that use them. You can edit a configuration by clicking the "Edit selected Configuration" button or by double-clicking the configuration you want to alter. For further information about the **IKARUS anti.virus configuration** and the various settings, refer to the **IKARUS anti.virus manual**.

5.2.13.1 *Layout*

In the toolbar of the Configurations dialog it is possible to do the following actions:

- Add Configuration
- Edit selected Configuration
- Delete selected Configuration
- Import Configuration
- Export selected Configuration

In the first list of the dialog (see Figure 5-31) all available configurations of the IKARUS security.manager are shown and by opening the second list, it is also possible to view all hosts that use the selected configuration.

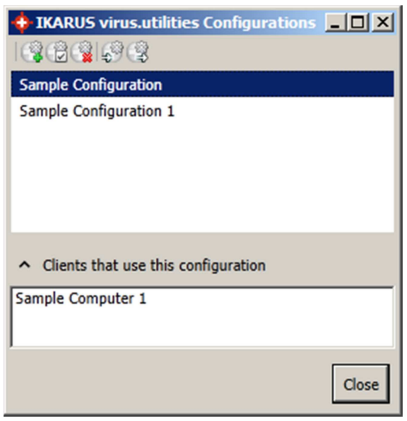


Figure 5-31 UI – IKARUS anti.virus Configurations

5.2.13.2 *General*

On the General tab of the **IKARUS anti.virus Configuration** dialog, all necessary protection settings can be enabled or disabled. The configuration can be saved by clicking the OK or the Save button and the changes can be discarded by clicking the Cancel button. Clicking the OK or Cancel buttons will also close the **IKARUS anti.virus Configuration** dialog.

It is possible to set the following settings on the General tab:

- **Enable System Protection:** Enables or disables system protection (if disabled, all other options will be disabled, too)
- **Enable Internet download protection:** Enables or disables protection for Internet downloads
- **Enable spyware protection:** Enables or disables spyware protection
- **Enable dialer protection:** Enables or disables dialer protection

© 2012 IKARUS Security Software GmbH

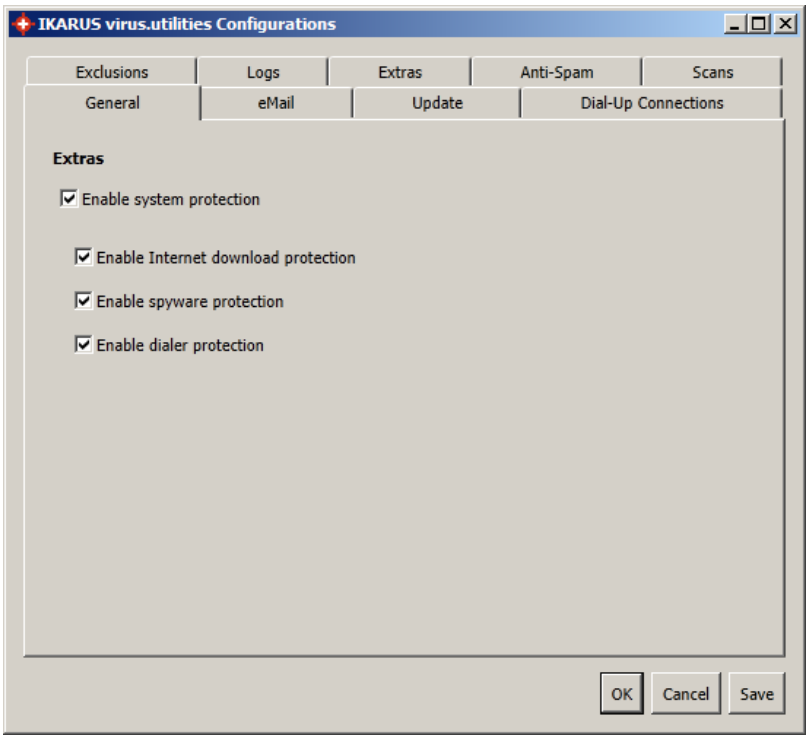


Figure 5-32 Configuration General tab

5.2.13.3 *E-mail*

On the e-mail tab of the **IKARUS anti.virus Configuration**, e-mail protection of the client can be enabled or disabled. Additionally, the administrator can configure various settings such as where the scan report is placed in the e-mail. With incoming and outgoing e-mails, the e-mail scan report can be positioned at the beginning or the end of the e-mail or be omitted.

In the email section it is possible to configure the following settings:

- **Activate email Protection:** Enables or disables e-mail protection
- **Save infected attachments:** Specifies whether attachments should be saved on the client side
- **Show scan status:** Shows the scan status
- **For incoming e-mails:** Sets the position of the scan report in incoming mail
- **For outgoing e-mails:** Sets the position of the scan report in outgoing mail

© 2012 IKARUS Security Software GmbH

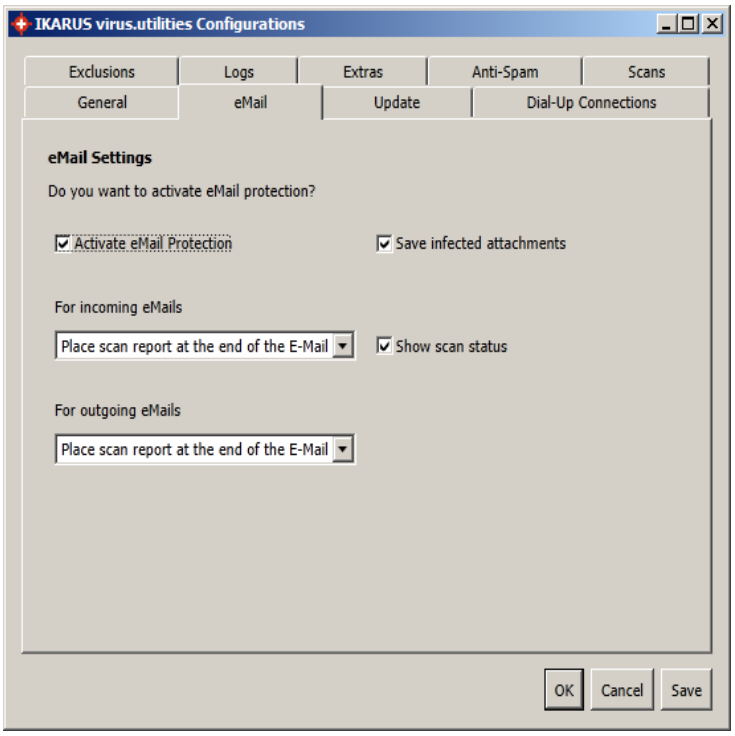


Figure 5-33 Configuration e-mail tab

5.2.13.4 *Update*

All settings necessary for updates to the IKARUS anti.virus are configured on the Update tab. In particular, when using a proxy server, you need to specify the correct settings here.

In the update tab the following settings can be set:

- Search automatically: Enables automatic search
- Install product update automatically: Automatically installs product updates
- Use proxy server: Enables/disables use of a proxy server
- Server: Proxy-server address
- Port: Proxy-server port
- Username: The username for the proxy server if needed
- Password: The password for the proxy server if needed

© 2012 IKARUS Security Software GmbH

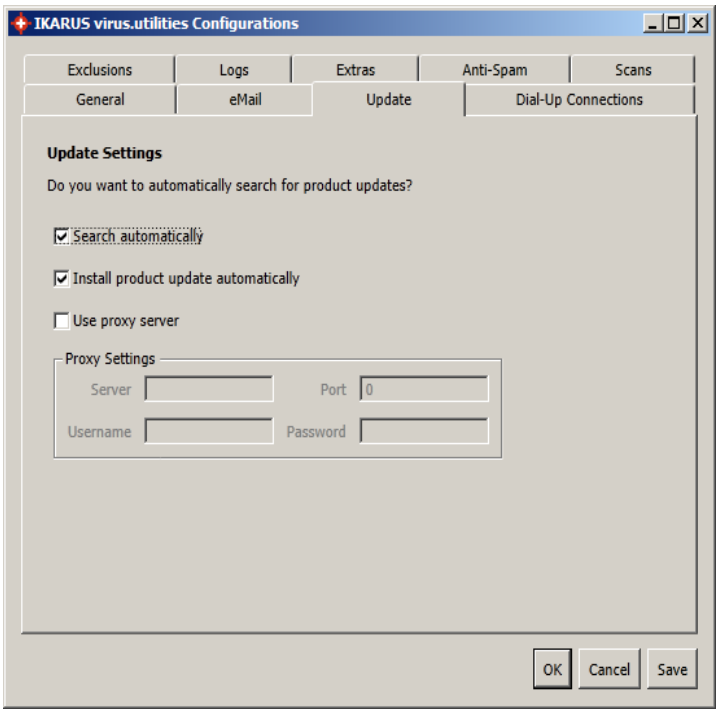


Figure 5-34 Configuration Update tab

5.2.13.5 *Dial-Up Connections*

If you still have a modem or dial-up connection in place you can set the connection settings on the Dial-Up Connections tab. The Modem connection tab allows for setting the auto-dial function for updating the IKARUS anti.virus. You can specify a period of time during which AutoUpdate will automatically connect to the Internet (if dial-up connection is selected).

In the dial-up tab the following settings can be adapted:

- Modem/Dial up connection: Enter the dial-up or modem connection name here
- Activate automatic dialing: Enables automatic dialing
- Timespan setting: Sets the time frame when the connection is automatically established

© 2012 IKARUS Security Software GmbH

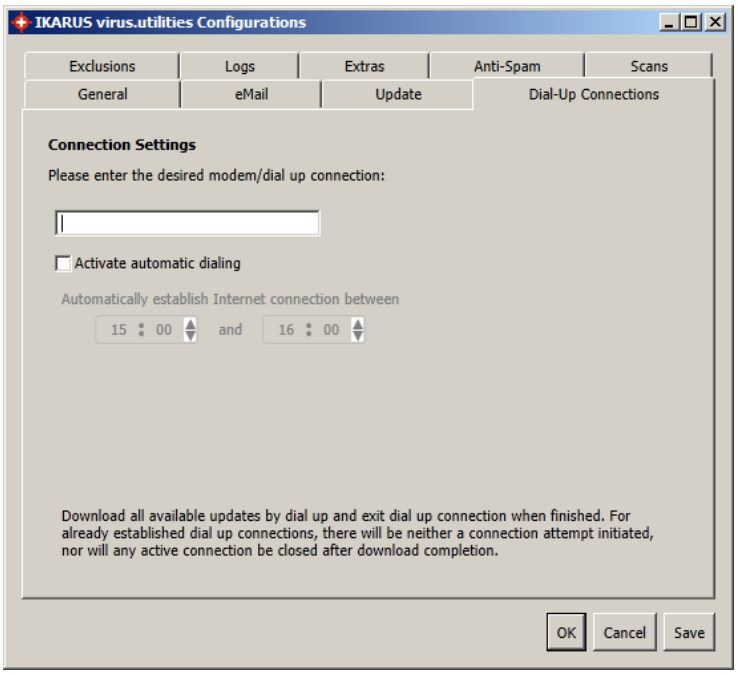


Figure 5-35 Configuration Dial-Up Connections tab

5.2.13.6 *Exclusions*

On the Exclusions tab, you can select files and process that will be excluded from the IKARUS anti.virus scan. This is useful when you want to exclude a service from the scan that is already using a considerable amount of the system resources (e.g. MP3, holiday photos, etc.), or if you do not want to scan a specific directory.

If you have set environment variables for specific folders/drives you want to exclude system-wide, use this function rather than specifying the path. If the path is different on every host, the IKARUS anti.virus will exclude the correct path. Use Ctrl + Spacebar in the textbox to display all environment variables of your current system (i.e. the system where the user interface is installed).

In the exclusion tab it is possible to configure the following settings:

- MiB number box: Enables or disables file scanning for files bigger than the specified size.
- Add button: Add paths and environment variables on the file exclusion tab.
- List of Exclusions: This is a list of already selected paths/environment variables. If you choose the process exclusions it displays the excluded processes.
- Generalize Paths: If you are not sure whether there is an environment variable for a path, click Generalize Paths. This link is not available for process exclusions.
    - Old Path: The path you entered
    - New Path: The path replaced with environment variables
    - Apply: Check if you want to apply the change

© 2012 IKARUS Security Software GmbH

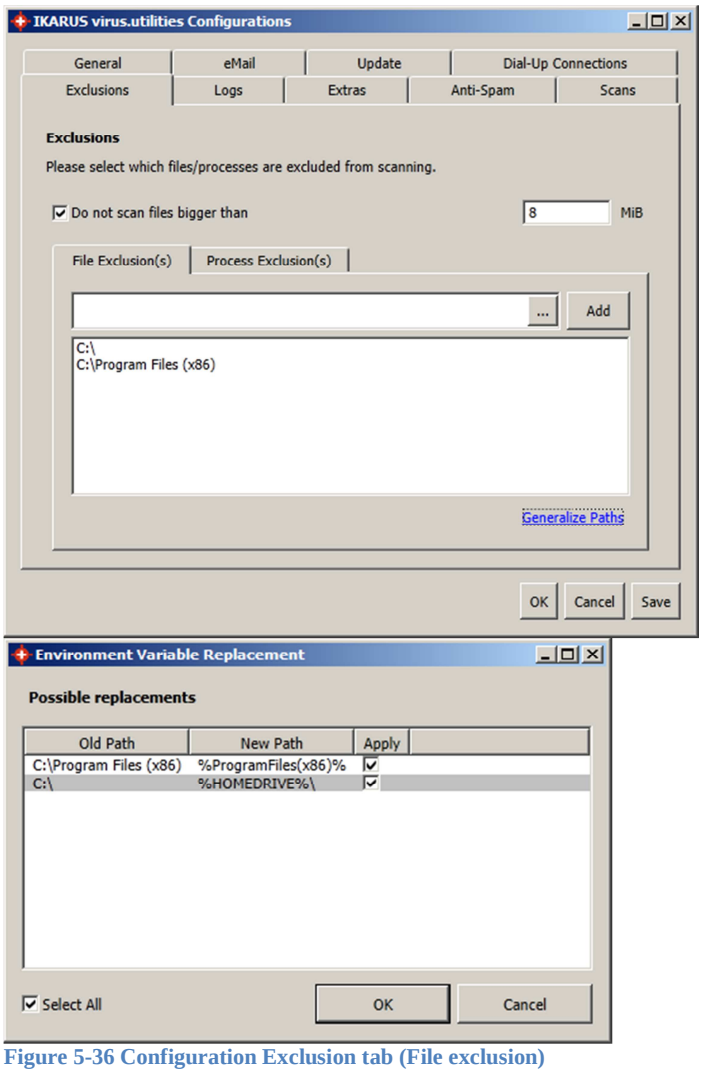


Figure 5-36 Configuration Exclusion tab (File exclusion)

5.2.13.7 *Logs*

On the Logs tab, the administrator defines actions that will be logged in the IKARUS anti.virus.

In the logs tab the following settings can be changed:

- **Log system supervision in the main log:** Logs the system supervision to the IKARUS anti.virus main log.
- **Record logs for scans:** Enable if logs should be written for the scans.
- **Record all data when scanning:** Enable if all data should be recorded.
- **Activate log file overwrite:** An existing log will be overwritten when a new scan is started.

© 2012 IKARUS Security Software GmbH

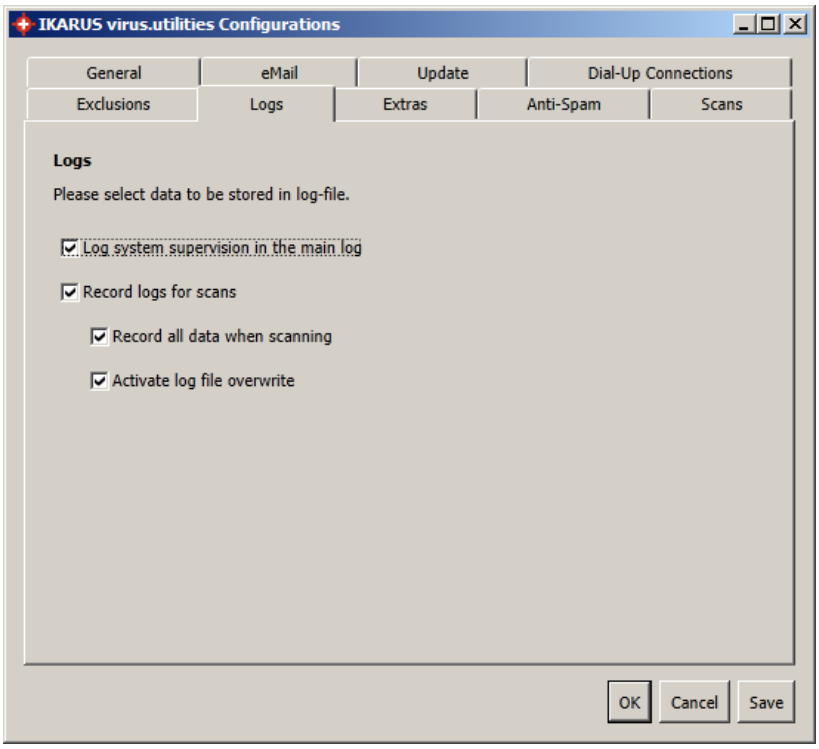


Figure 5-37 Configuration Logs tab

5.2.13.8 *Extras*

Use the Extras tab to restore the defaults of the IKARUS anti.virus and to enable system protection for the startup processes of your operation system. In the Extras tab the system protection can be enabled to start at startup and it is possible to reset all settings to the default configuration.

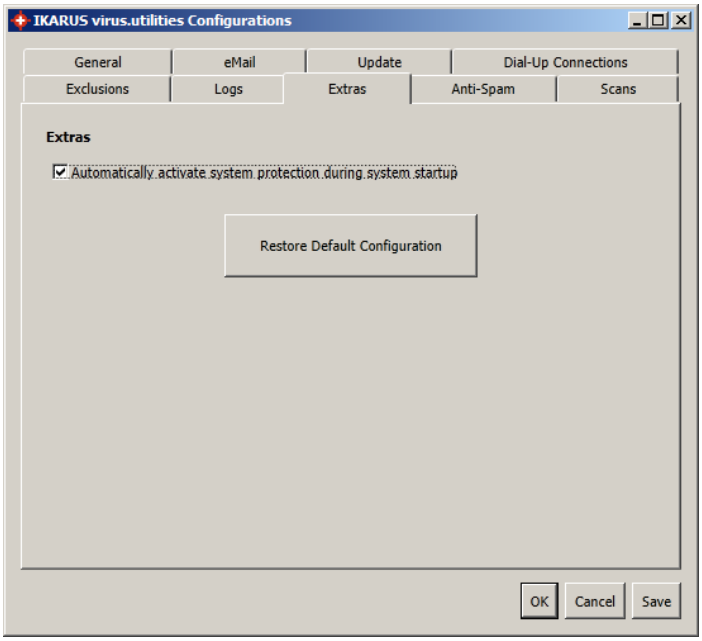


Figure 5-38 Configuration Extras tab

© 2012 IKARUS Security Software GmbH

5.2.13.9 *Anti-Spam*

The **IKARUS Anti-Spam Module** allows for filtering e-mail received in Outlook, Outlook Express, or Windows Mail. Click the Activate Anti-Spam option in the settings of **IKARUS anti.virus** to enable spam protection.

The Anti-Spam Module will be enabled after the subsequent program restart. For configuring spam evaluation, click the yellow and red controls (yellow indicates possible spam, and red indicates spam).

At the bottom, you can choose the action to perform when receiving spam mail:

- Mark e-mail with a “Possible Spam” label in the subject line, or
- Move mail to the junk mail folder of your mail client

An e-mail that is considered as a possible spam, will always be labeled in the subject line but will remain in the inbox of your mail client.

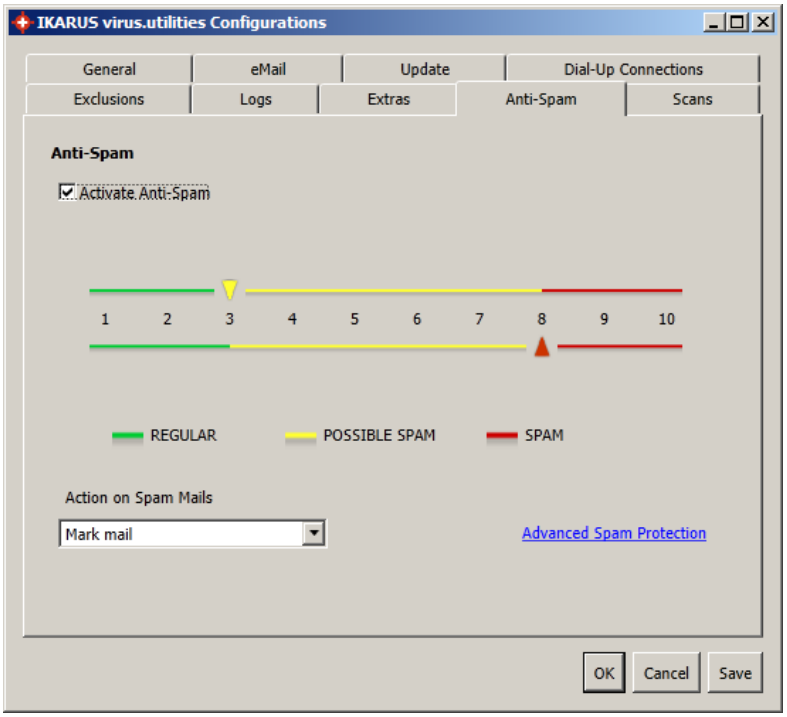


Figure 5-39 Configuration Anti-Spam tab

Advanced Spam Protection:
This option allows for configuring your own spam filter. You can define spam rules for senders, recipients, subjects, and contents.

The following settings can be made:

- **e-mail Section:** Defines what section like sender, recipient, subject or content should be used for spam-rules
- **Content:** Content to parse for
- **Type:** Type of e-mail that can be regular mail, possible spam or spam
- **Add button:** Click to enable advanced spam protection

© 2012 IKARUS Security Software GmbH

- e-mail Section column: List entry e-mail section
- Content column: List entry content
- Type column: List entry e-mail type
- Priority column: By the help of these buttons the rules can be deleted or moved to new locations:
  - Delete Advanced Spam Protection
  - Move to Top
  - Move up
  - Move down
  - Move to Bottom

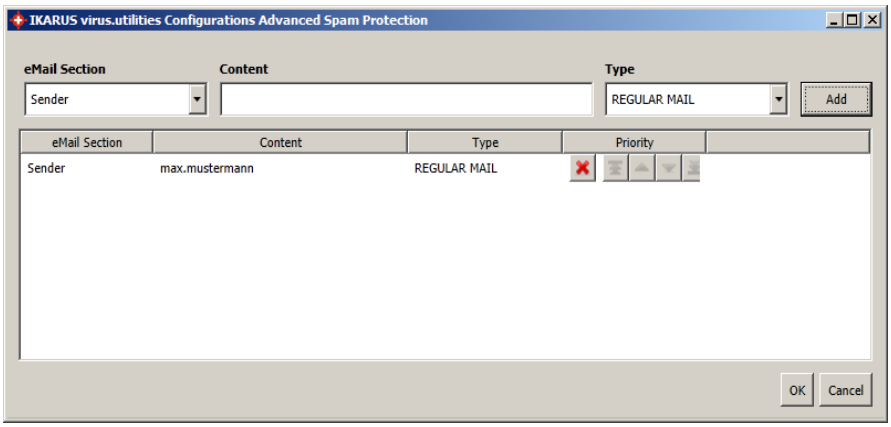


Figure 5-40 Configuration Advanced Spam Protection

5.2.13.10 *Scan*

You can configure the scan to be performed automatically or launch the scan manually in IKARUS anti.virus. You can manage and add as many scans as required.

Preset scans:

- Fast System Scan: Scans the Windows installation directory. The majority of malicious programs such as viruses and Trojan horses are located in this directory and are quickly and reliably detected.
- System Partition: This preset scans the drive where your operating system is installed. All archives, directories, folders, and files on this drive will be scanned by IKARUS anti.virus.
- Entire Host: IKARUS anti.virus will scan all drives on your computer.
- Removable media: All external drives such as USB sticks and CD ROM drives will be scanned.

© 2012 IKARUS Security Software GmbH

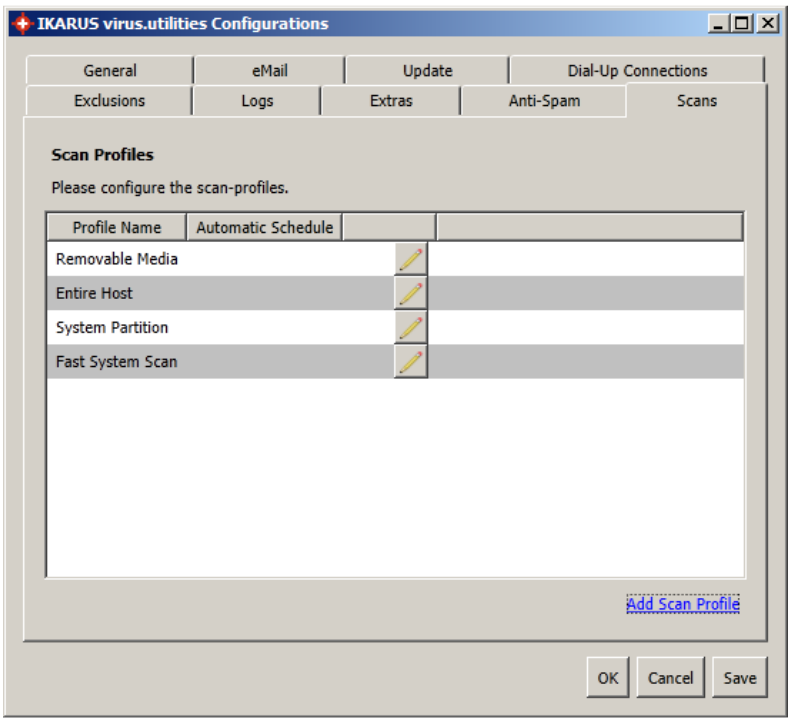


Figure 5-41 Configuration Scans tab

Click “Add Scan Profile” to configure a custom scan profile. You can enter any name for the scan. Click “Browse” to select the folders or files to scan. You can also set the program to perform an automatic scan where required.

The automatic scan can be scheduled for any time (for example, every Friday, 12pm). The scan will be performed only for those areas selected by the user.

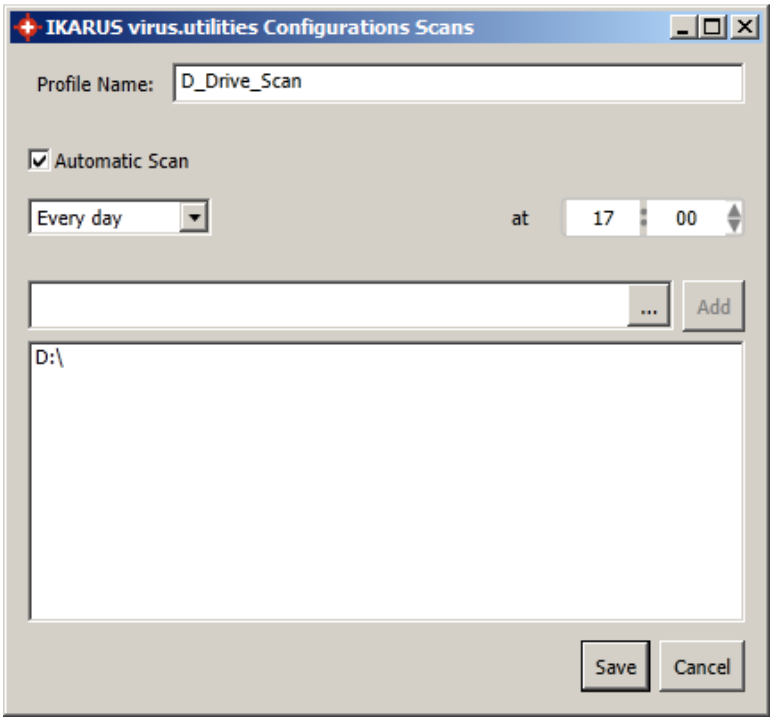


Figure 5-42 Configuration Add Scan Profile

© 2012 IKARUS Security Software GmbH

5.2.14 IKARUS security.manager Settings

The **IKARUS security.manager Settings** window (
Figure 5-43) shows settings for the **IKARUS security.manager Server**. The window is separated into five tabs: *General, E-Mail Notifications, Update, Fileshare, LDAP and Charts*. **Changes** to the settings **are committed upon clicking the *OK* or *Apply* buttons** at the bottom of the window. These two buttons will be **disabled when entries are missing or invalid**. Clicking the ***Cancel* button** will **close the window and discard all changes**, clicking the ***OK* button** will **save all changes and close the window**.

5.2.14.1 *General*

In the General tab the following settings can be set:

- **Shared Directory:** Sets the directory where ismxstartup.exe is stored for the **IKARUS anti.virus** deployment.
  - **Open Browser Button:** Opens a browser window for choosing the shared directory.
- **Enforce Client Update:** Enable or disable deployment over TCP.
- **Enforce Client Update Port:** Enable deployment over specified TCP port.
- **Administration Port:** The port the **IKARUS security.manager UI** uses for communicating with the **IKARUS security.manager Server**.
- **Automatically Add Clients:** Specifies whether new clients in the LDAP are automatically added to the Directory.

In the "Change Management" section the following settings can be enabled or disabled:

- **Enable Change Management according to the ITIL:** Enables or disables change tracking.
- **Ask for comment at Log-in screen:** If enabled, the user must enter a comment on login attempts.
- **Maintain change log for server settings:** If enabled, logs all changes made to settings.
- **Ask for Request for Change (RfC) ID:** If enabled, the user must enter an RfC ID on login attempts.

In the "Used config after drag and drop" section the following settings can be done:

- **Drag and Drop Behavior:** If enabled, user gets a notification what to do with config files after moving hosts in manual group.
- **Define Standard Behavior:** If the same behavior should be applied in every case, then choose if hosts should use own or parent config file.

© 2012 IKARUS Security Software GmbH

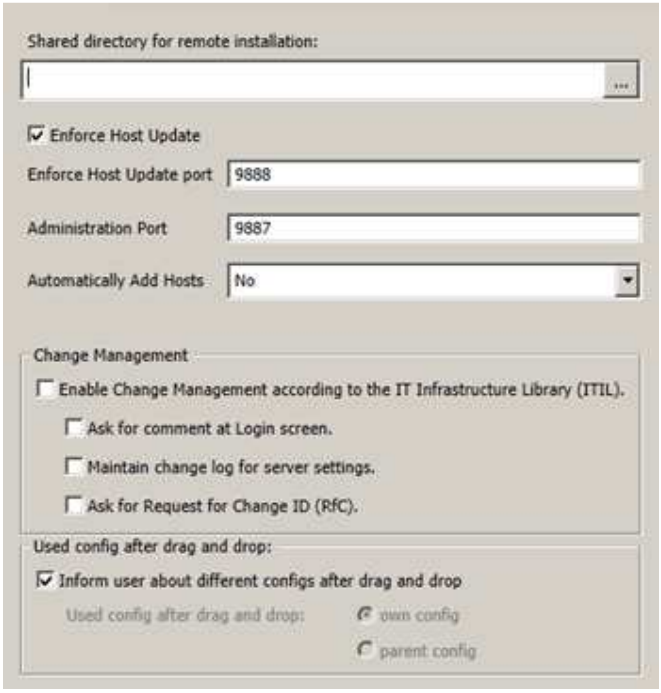


Figure 5-43 UI – IKARUS security.manager Settings – General

© 2012 IKARUS Security Software GmbH

5.2.14.2 *E-Mail Notifications*

In the e-mail tab the following settings can be set:

- **Enable e-mail Reports:** Enable or disable e-mail reports.
- **Mail Server:** Defined mail server over that the reports are sent.
- **Sender:** The address from which the reports are sent.
- **Enable Authentication:** Enables or disables user authentication with the e-mail server.
- **Username:** The username used to authenticate with the e-mail server.
- **Password:** The password used to authenticate with the e-mail server.
- **Available Reports:** Lists all available reports.
- **Add New Report:** Open the IKARUS security.manager Reports window, see Section 5.2.14.3.

Figure 5-44 UI – IKARUS security.manager Settings – E-Mail Notifications

© 2012 IKARUS Security Software GmbH

5.2.14.3 *IKARUS security.manager Reports*

In the reports dialog the following settings can be set to configure the e-Mail report:

- **Report Name:** Sets the name of the report.
- **Enable Report:** Enables or disables sending of this report.
- **Report Type:** Sets the type of the report. Following types are available:
  - **"On Virus" Report:** Send report when a virus is found.
  - **"On Auto-Add" Report:** Send report when a computer is added to the LDAP automatically.
  - **Day Report:** Send report on the set days.
  - **ISM Server Startup Report:** Send report as the server starts up.
  - **Interval Report:** Send report at the specified time.
- **Scheduled Time:** Sets the time when the report is sent.
- **Day Mask:** Sets the days on which the report is sent.
- **Enable Virus Report:** Include virus information.
- **Enable Version Report:** Include version information.
- **Enable Client Report:** Include client information.
- **Enable Server Report:** Include server information.
- **Add Button:** Add a recipient for the report.
- **Recipients:** List of all recipients of the report.

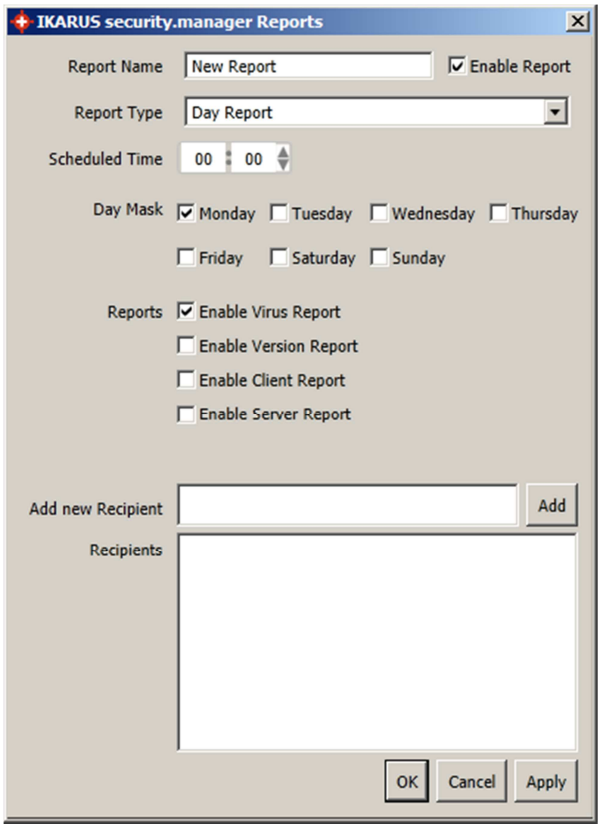


Figure 5-45 UI – IKARUS security.manager Settings – Reports

© 2012 IKARUS Security Software GmbH

Virus Report:

The virus report can either be set as a separate report type, which then will be sent, when a new virus is found in your system, or as report information additional to a different report, e.g. day report. The report has the following format:

```
-----------------------------------------------------------------------
ISM Virus Report:
testuser1.ikarus.at is infected with 1 virus(es)
testuser2.ikarus.at is infected with 38812 virus(es)

testuser1.ikarus.at:
c:\Users\TestUser1\Desktop\eicar.com (EICAR-ANTIVIRUS-TESTFILE)

testuser2.ikarus.at:
Detailed virus data for this host is currently not available on ISM!
-----------------------------------------------------------------------
```

It might happen that not all virus information is available for a host on the ism side (e.g.: Host was turned off after infection detection by user and the IKARUS anti.virus was not able to upload all information to the IKARUS security.manager Server). When this occurs the report only holds the information “Detailed virus data for this host is currently not available on ISM!”. You can either connect to the IKARUS security.manager Server and check when the data is available in the virus list (see section 5.2.3) or you can start IKARUS anti.virus in the IKARUS security.manager UI (see section 5.2.1), where the viruses were found.

© 2012 IKARUS Security Software GmbH

5.2.14.4 *Update*

In the Update tab the following settings can be set:

- Silent Update of the IKARUS security.manager Server: Enables the automatic update of the IKARUS security.manager Server.
- Proxy Server: Sets the proxy server through which the IKARUS security.manager Server is accessing the updates.
- Proxy Port: Sets the port the connection is established through.
- Username: Sets the username for authenticating with the proxy server if needed.
- Password: Sets the password for authenticating with the proxy server if needed.

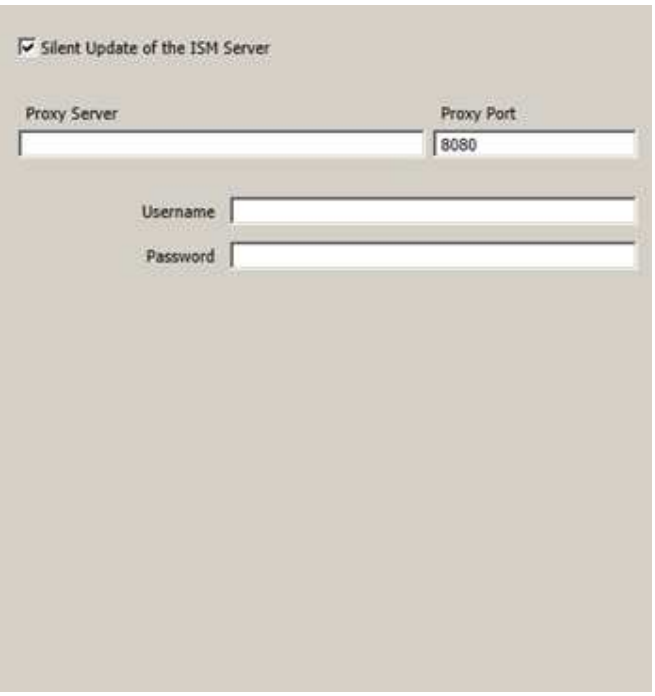


Figure 5-46 UI – IKARUS security.manager Settings – Update

© 2012 IKARUS Security Software GmbH

5.2.14.5 *Fileshare*

For avoiding resource bottlenecks, *fileshares* should be used. Administrators have to first create *fileshares* for the usage with **IKARUS security.manager**. Please notice, that the **IKARUS security.manager Server needs read and write rights** for keeping data up to date. Figure 5-47 shows the *fileshare*-tab.

In the fileshare tab the following information in the list can be seen:

- **Online/Offline:** A fileshare is set to online if all files are available and up to date.
- **Randomized Pool:** If a fileshare is in the randomized pool then it will be randomly assigned to a host that actually needs an update.
- **Fileshare List:** Contains all active or inactive fileshares

The following two actions can be performed in the fileshare tab:

- **Start Rollout:** If new fileshares are added, users may want to start immediately a rollout of the files.
- **Add fileshare:** Adds a new fileshare. Fileshares will be set to online as soon as all files are copied by the rollout process

Figure 5-47 UI – IKARUS security.manager Settings – Fileshare

The IKARUS security.manager Server checks **every minute** if a *fileshare* is available or not. The actual state is visualized by ● (*fileshare* is online) or ● (*fileshare* is offline), see Figure 5-47 second column. A *fileshare* is available if all necessary files **are existing and up to date.**

Furthermore **IKARUS security.manager Server** checks every **20 minutes** if updates are available and need to be copied to the defined *fileshares*. It is also possible to start the rollout-process of the update-files **manually with "Start Rollout"** (see Figure 5-47).
A cleanup process, which is triggered **once per day**, deletes old files for keeping the amount of data as small as possible.

© 2012 IKARUS Security Software GmbH

A *fileshare* is set to a corresponding host or group by the help of the **properties page in section update** (see section 5.2.6).

© 2012 IKARUS Security Software GmbH

5.2.14.6 *LDAP*

In the *LDAP* tab the user can configure the *LDAP* settings by changing the following settings:

- **Auto Detect Domain:** Try to auto detect the domain
- **Servername:** Name of domain controller (see section 9.2)
- **Type:** Type of *LDAP* (see section 9.2)
- **Attribute:** Sets attribute to read (see section 9.2)
- **Searchpath:** Defines domain for scanning (see section 9.2)
- **Filter:** Sets the criteria used on resolving the specified attribute (see section 9.2)
- **Auth Method:** Method for authentication on domain controller (see section 9.2)
- **Username:** Sets the username for the *LDAP* connection (see section 9.2)
- **Password:** Sets the password for the *LDAP* connection (see section 9.2)
- **Exclusions:** Overview of defined exclusions
- **Add Exclusions:** Add a new host that will be not listed in directory
- **LDAP-Settings Test:** Test if a *LDAP* can be found with the given parameters

Figure 5-48 UI – IKARUS security.manager Settings – LDAP

By the help of the dialog, which is shown in Figure 5-48, a *LDAP* can be used. Previously a *LDAP* was configured in the config-file. If a <ldap> section is within the config file, then **this section is read and set by the IKARUS security.manager Server automatically**. Afterwards the <ldap> section **will be deleted** from the config file.

Therefore **two ways** are possible for setting a *LDAP*:

- Use the *LDAP*-tab within the **IKARUS security.manager Settings**
- Add the <ldap> section to the **config file**

© 2012 IKARUS Security Software GmbH

More information about the config file and *LDAP* parameters may be found in chapter 9 as well as in section 9.2.

5.2.14.7 *Charts*

In the Charts tab it is possible to modify the appearance of the standard charts and change description text (see Figure 5-49).

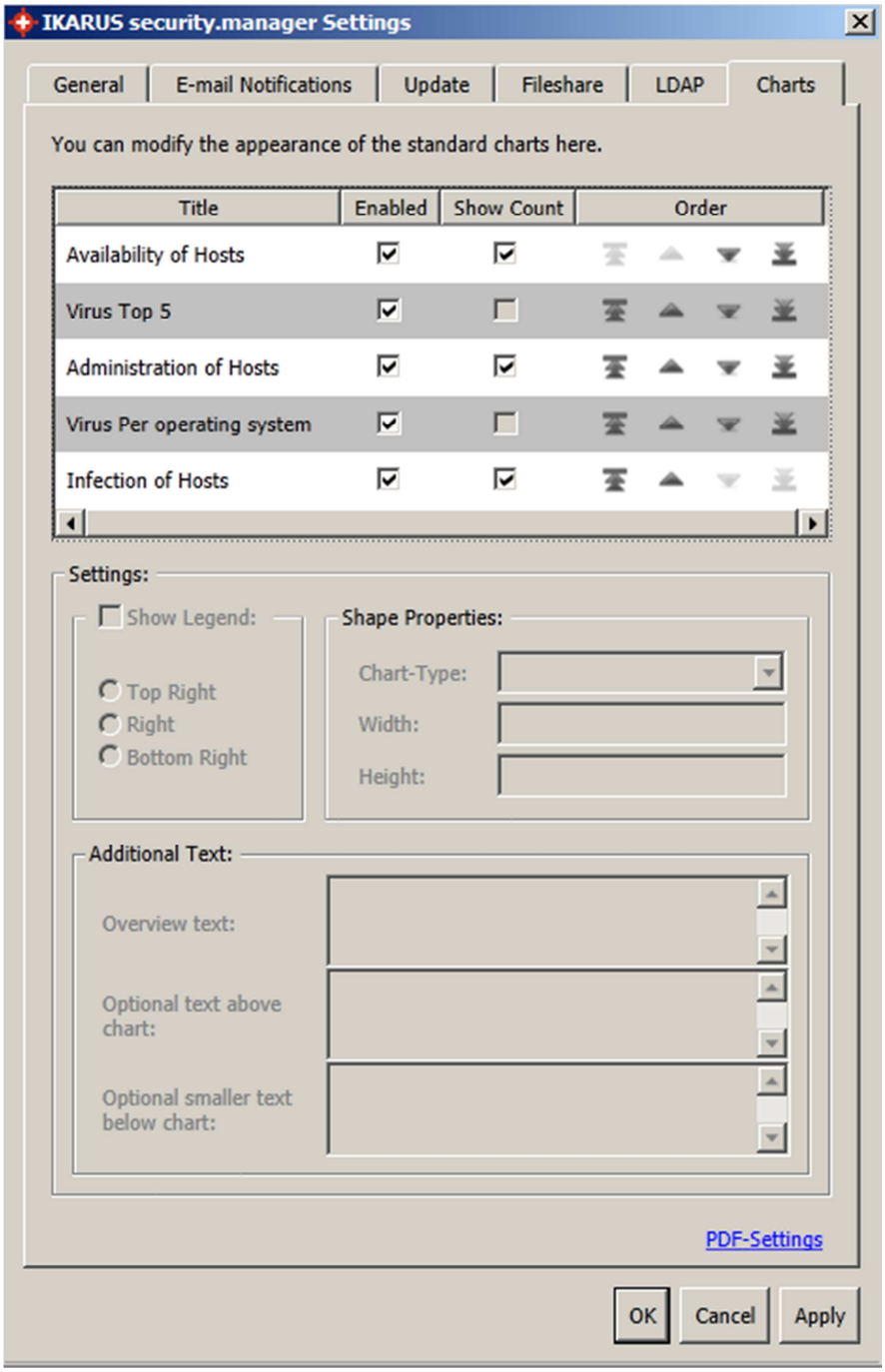


Figure 5-49 Charts options

© 2012 IKARUS Security Software GmbH

Section list of charts:
In the upper section of dialog the 5 standard charts are listed.

- With the arrow keys it is possible to **change** the **order** of the charts.
- Through the enabled checkbox it is possible to **hide charts** from the Charts Page as well as in the PDF (see section 5.2.11).
- If the **chart type** is “pie-chart”, it is possible to show the count next to the percentage in the pie chart by checking the “Show-Count” checkbox.

Section settings:
The settings are divided into 3 parts. Those settings depend on the chart that is selected in the charts list above.

In the **“Show Legend”** part it is possible to decide where the legend of the chart is situated (Top Right, Right, Bottom Right) and if a legend is even displayed.

In the **“Shape Properties”** part the chart type (pie or bar chart) can be chosen and the width and height can be set for any chart, so that it best fits your screen resolution. The minimum width and height for the charts is 500 pixels.

In the **“Additional Text”** part it is possible to add your customized descriptions. Those descriptions will be displayed in the report and on the Charts Page.

PDF Report:
The link “PDF-Settings” in the lower left corner opens a dialog, where you can change the standard header and footer of the report to your **personalized header and footer** (see Figure 5-50). It is also possible to revert it to the default header and footer. The footer and header can also be disabled, so that they are not shown in the report. Those settings only affect the appearance of **PDF report**.

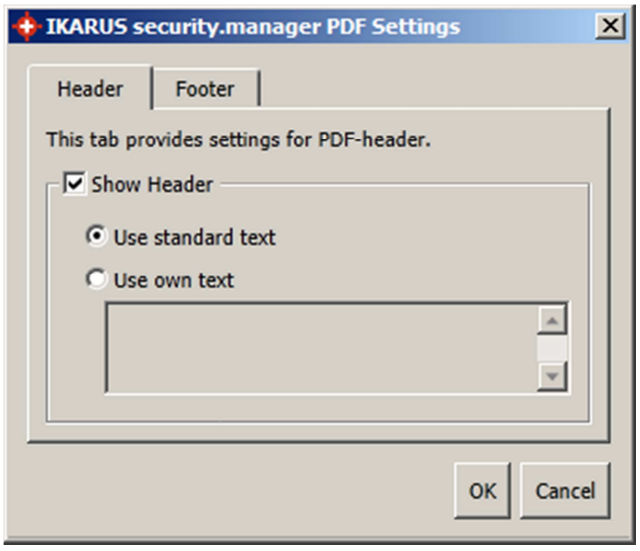


Figure 5-50 PDF Report settings

5.2.15 Dialog "Clean host-entries from database"

This dialog should only be used if hosts **were manually deleted from the Active Directory.** In this case the deleted hosts may still be available in the database, and this dialog provides a way to finally delete them from the database. Please note that the **selected hosts will be deleted irrevocably**!

On the left side of the dialog all unused hosts are displayed. These are hosts that are still in the database and managed, but do no longer appear in your *Active Directory* or in your manual group. This can occur, because the **IKARUS security.manager** does not automatically deletes hosts from the server when they are no longer available in the *Active Directory*, because the server cannot assume the user behavior.

An administrator of the **IKARUS security.manager** must manually remove those hosts, by moving a host from the left list, "Deleted hosts from Active Directory", to the right list, "Hosts that will be deleted". To move a host from one list to the other, there are 4 buttons in the middle of the two lists:

- **Select all hosts:** All hosts are set to remove host list
- **Select one host:** Selected host is set to remove host list
- **Unselect one host:** Selected host is deleted from remove host list
- **Unselect all hosts:** All hosts are deleted from remove host list

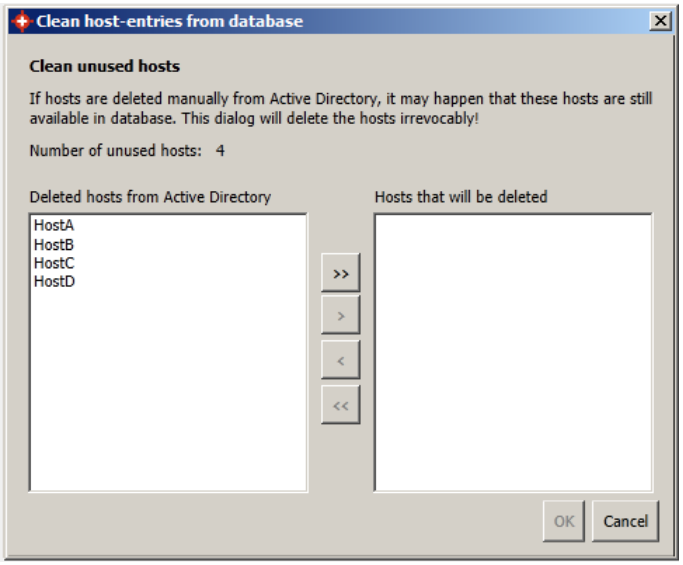


Figure 5-51 UI – Clean host-entries from database

Cleaning up the database from unused hosts, licenses that were assigned to the selected hosts may be given free. This dialog is available under **Tools → Clean host-entries from database**.

© 2012 IKARUS Security Software GmbH

5.2.16 About Dialog

5.2.16.1 *Layout*

In the About Dialog the information is separated into two sections:

- **Version Information:** Displays the **IKARUS security.manager UI**, **IKARUS security.manager Server** and Updater versions.
- **License Information:** Displays the expiration date and how much of your license capacity is used and free.

At the bottom of the dialog a user can renew his license by clicking the Renew License link (see Figure 5-52).

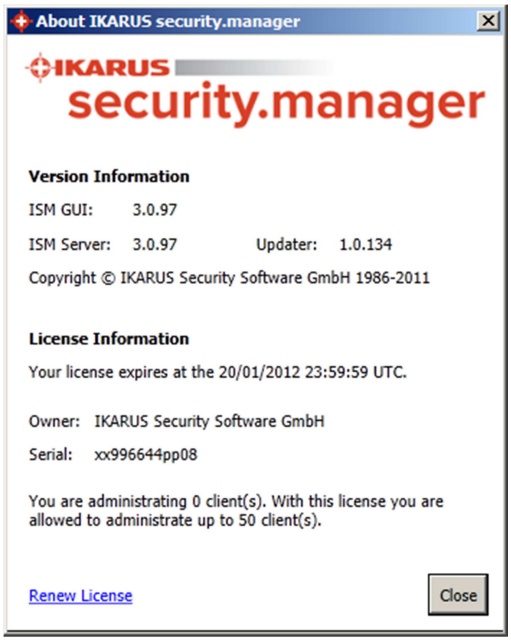


Figure 5-52 UI – About Dialog

© 2012 IKARUS Security Software GmbH

5.2.17 Management mode

Via this menu option, you are given access to all the options that concern the management mode of the IKARUS security.manager. Here you are given an overview of your IKARUS security.manager instances and can add, edit or delete them. Furthermore, you can use this menu to export the settings of your IKARUS security.manager instances to a password protected file, and change the password for the configuration file of management mode.

Please note that this menu is not available in single mode.

5.2.17.1 *The "Options" menu option*

The options dialogue can be found in the main menu under "Options".

Figure 5-53 : UI - "Management" menu, "Export configuration file" menu option

The dialogue provides an overview of your IKARUS security.manager instances. They are shown in the list with the server name, port, username and description. In addition, you can see whether an instance has valid connection data and whether it is setup as the default instance.

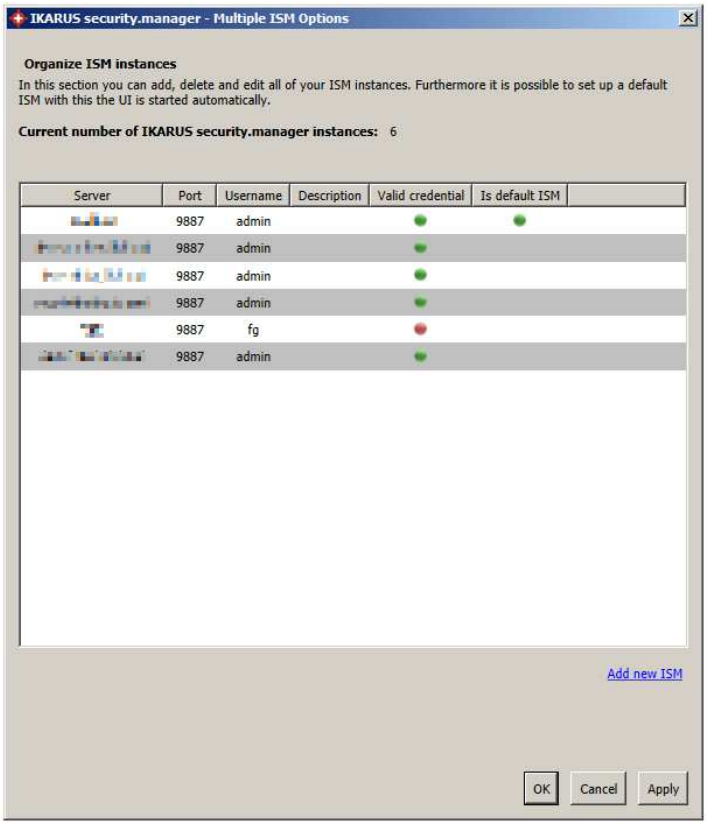


Figure 5-54 : UI – Options dialogue

© 2012 IKARUS Security Software GmbH

You can edit and delete the existing instances, and set them to be the default instance. All operations can be called from the shortcut menu.

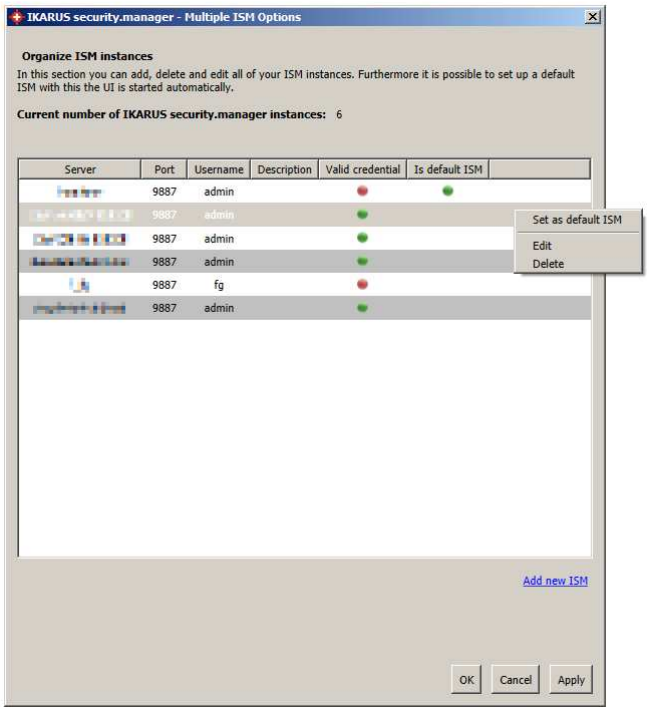


Figure 5-55 : UI – Shortcut menu in the options dialogue

"Set as default ISM" means that when the program restarts, the connection will be established automatically to that IKARUS security.manager instance. There must always be a default instance. You cannot delete it.

If you click "Delete", the selected instance will be deleted from the list. Please note that you cannot delete the IKARUS security.manager instance to which you are currently connected nor the default instance. It is also possible to delete instances by selecting an instance and then pressing the delete key of your keyboard.

5.2.17.1.1 Editing the IKARUS security.manager server

If you click "Edit" in the shortcut menu of an IKARUS security.manager instance, you will reach the edit dialogue. There, you have the possibility to change the server name, port, username, password and description.

As an alternative, you can double-click an IKARUS security.manager instance in the list, which will also open the edit dialogue.

© 2012 IKARUS Security Software GmbH

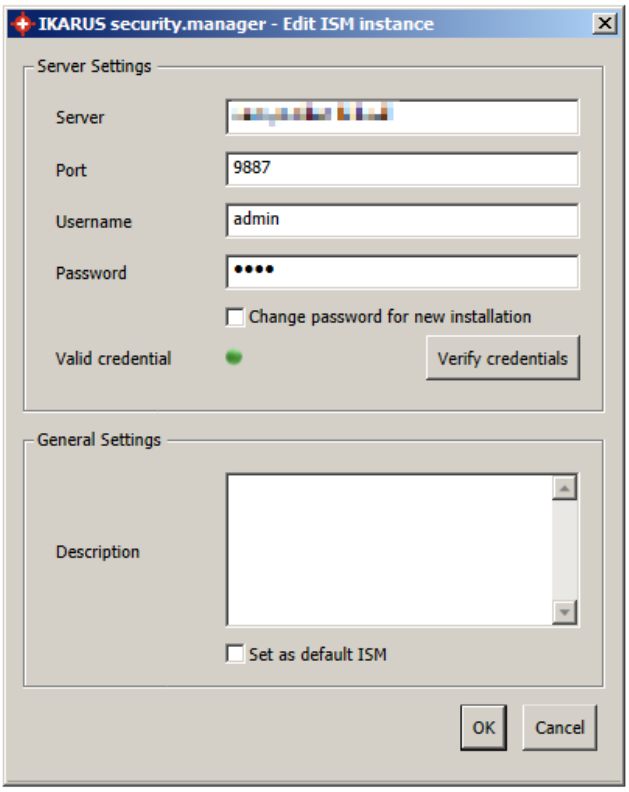


Figure 5-56 : UI - Edit dialogue

The program will make you aware of any invalid input. It is only possible to confirm the data if all entries have been acknowledged as valid. The port number must, for example, lie in a specific range of numbers to be able to successfully create this instance.

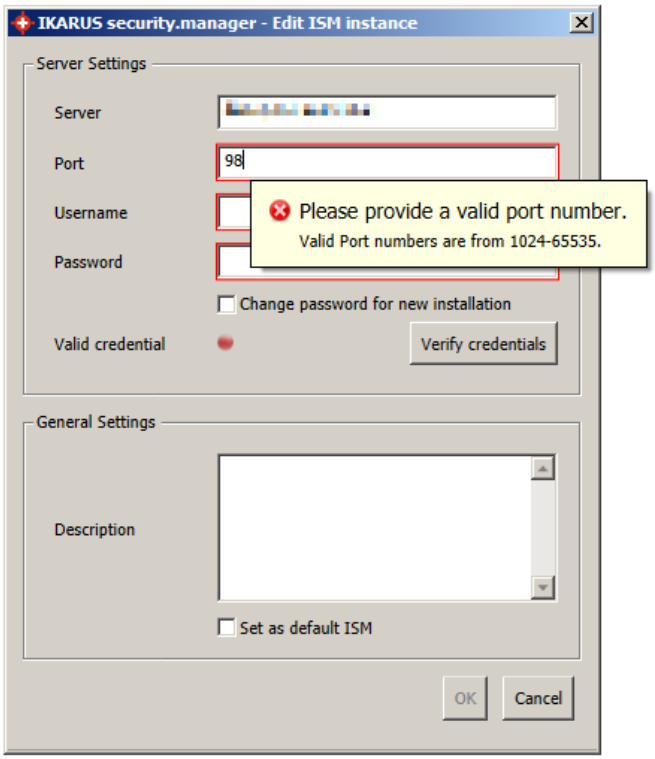


Figure 5-57 : UI - Edit dialogue, entering invalid data

© 2012 IKARUS Security Software GmbH

Activate the "Change password for a new installation" option. Then you can change the password of the IKARUS security.manager instance. However, that is only possible after a new installation.

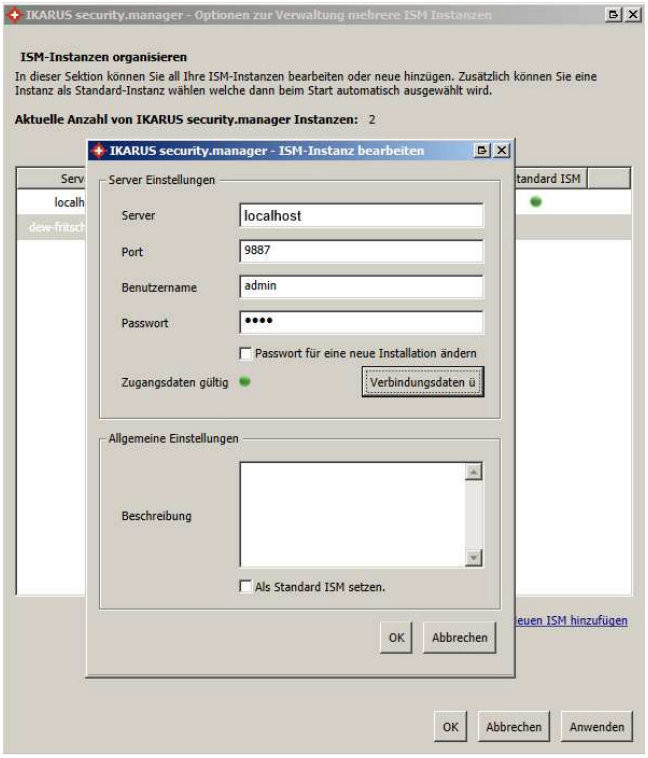


Figure 5-58 : UI - Edit dialogue, changing the password for a new installation

You must enter the same value in both password fields. Click "Set password" to check whether the password change is possible. If it is, then the password of the IKARUS security.manager instance will be reset.

Click the "Check connection data" button to have the program check the correctness of the entered data. You will be informed of the result of the verification by a message window as well as the status indicator to the left of the button. It is green if the connection was established successfully, or red if the test connection failed.

© 2012 IKARUS Security Software GmbH

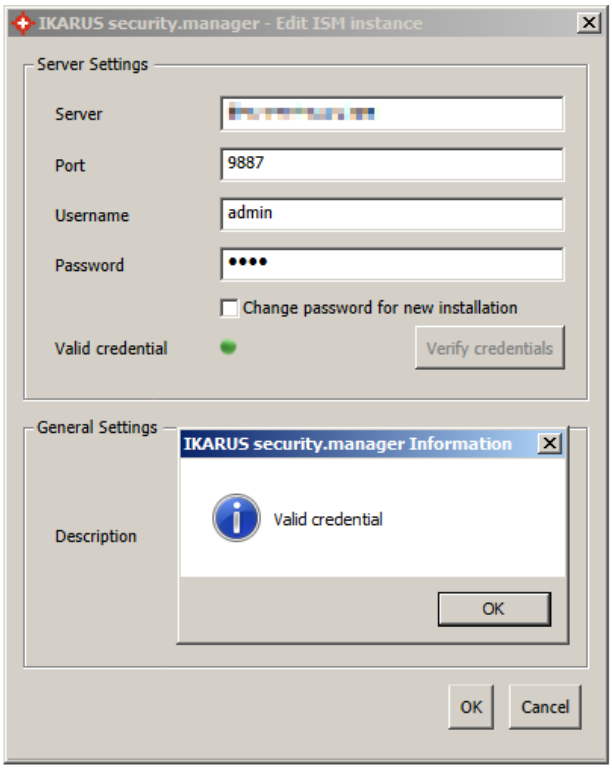


Figure 5-59 : UI - Edit dialogue, checking the access data

With the checkbox on the bottom edge of the dialogue, you define whether the instance is your default instance. You will be automatically connected to the default instance every time the program restarts. Please note that there must always be such a default instance. You may be requested by the program to set this option.

When you have completed all the necessary fields and the entered data is valid, then you can close the edit dialogue by clicking "OK".

5.2.17.1.2 Add IKARUS security.manager server

In addition, it is possible to add new instances in the options dialogue. You can do this by using the "Add instance" link under the list. One click on it opens the edit dialogue described in the previous pages. Naturally, no fields are filled in. You must first of all specify all the required information.

Please note that changes to **IKARUS security.manager** instances will only be accepted permanently after clicking "Accept" or alternatively "OK".

5.2.17.2 *The "Export configuration file" menu option*

By using the "Export configuration file" dialogue, it is possible to write the settings of the individual **IKARUS security.manager** instances to a new configuration file in an encrypted form. This file can then be forwarded at will. You can call the dialogue using the *Management → Export configuration file* menu.

© 2012 IKARUS Security Software GmbH

Figure 5-60: UI - "Management" menu, "Export configuration file" menu option

Please note that the "Management" menu is not available in single mode.

The dialogue shows a list with all **IKARUS security.manager** instances as well as their key information. You can use the checkboxes on the left edge of the list to choose whether all instances or only specific ones are to be exported.

Auswahl aller Instanzen

Auswahl einzelner Instanzen

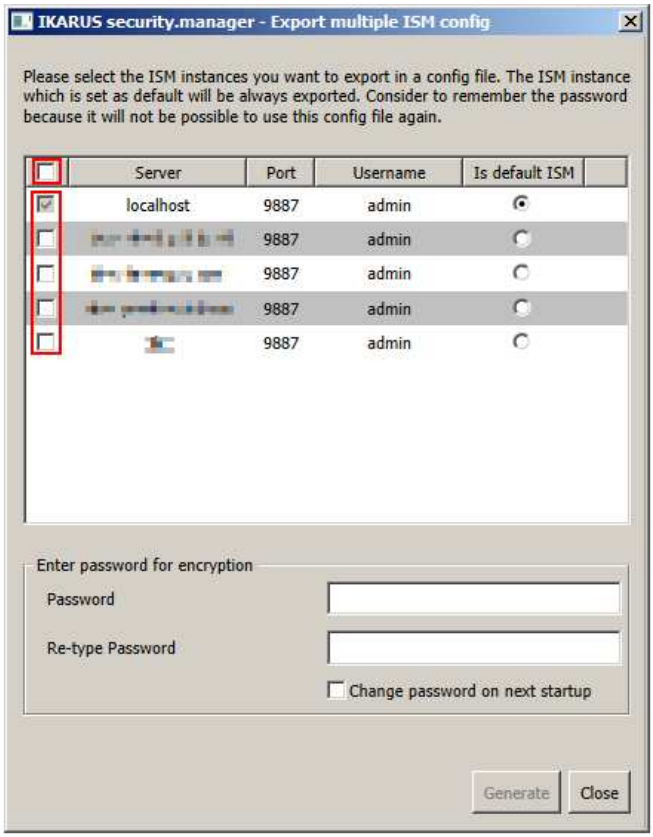


Figure 5-61: UI - "Export configuration file" dialogue - selecting the ISM instances to be exported

For security reasons, it is necessary to give a password before exporting the file. It is used to encrypt the file. You must enter it using the two text boxes under the list, and the entries must be identical.

Attention: The password must be at least 4 characters long, and you must enter that same value in both text boxes. You can only export the data when these conditions have been met.

© 2012 IKARUS Security Software GmbH

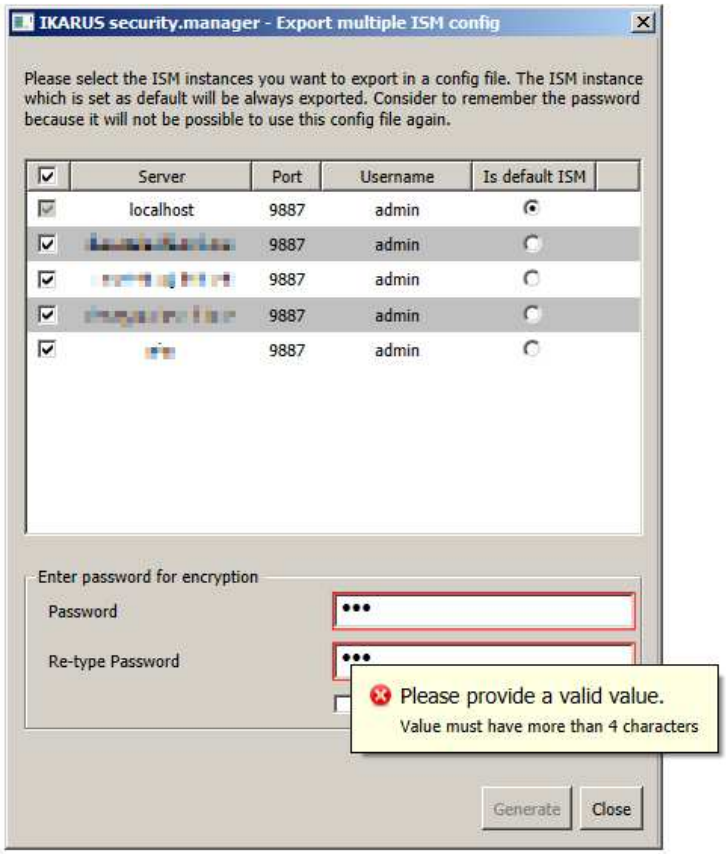


Figure 5-62: UI "Export configuration file" dialogue - error message in the event of an invalid password.

If you mark "Change password on next start-up", then the user who wants to use your exported file will be requested to reset the password for the encryption of the file when the program is started for the first time with your configuration file. Otherwise, the value that you set will be used for this.

© 2012 IKARUS Security Software GmbH

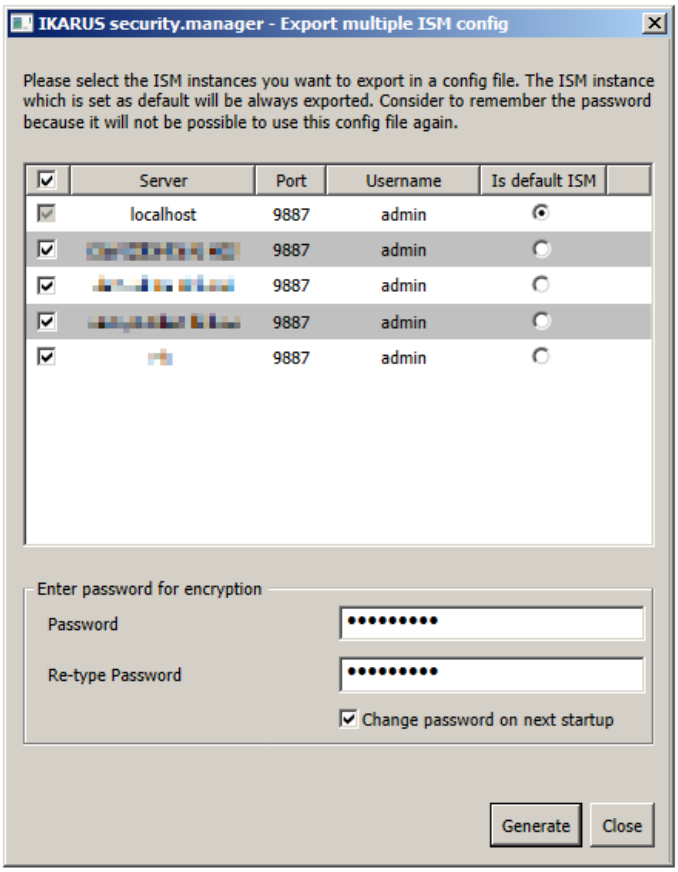


Figure 5-63: UI "Export configuration file" dialogue - valid password

Now, you can start the export of the selected IKARUS security.manager instances by clicking "Generate". In the following dialogue, you will be requested to specify the storage path as well as a file name.

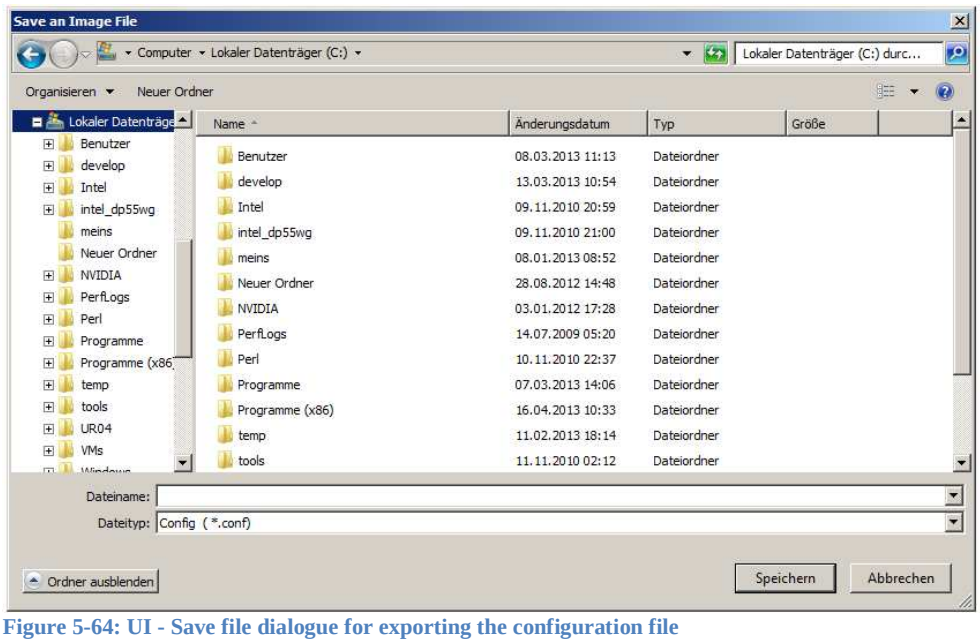


Figure 5-64: UI - Save file dialogue for exporting the configuration file

© 2012 IKARUS Security Software GmbH

One click on "Save" saves the information in an encrypted form in the new file.

5.2.17.3 *The "Change the password for management mode" menu option*

This dialogue can be used to change the password for logging in to management mode. It is available under the Management menu option.

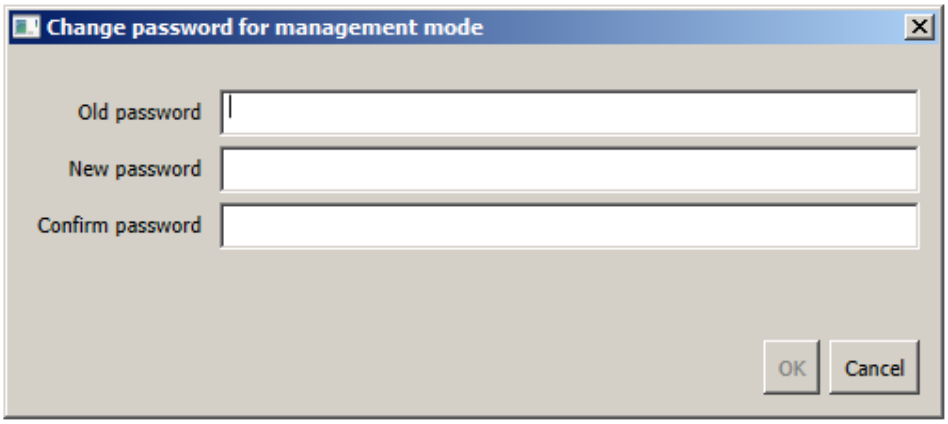


Figure 5-65: UI - Changing the password for management mode

It is important to note that password changes in management mode have no effect on the passwords of the registered IKARUS security.manager servers. These changes only affect the settings file that contains the list of registered IKARUS security.manager servers.

© 2012 IKARUS Security Software GmbH

5.2.18 The Menu Bar

The **menu bar** (Figure 5-66) is located at the top of the **IKARUS security.manager UI** main window.

The menu bar includes the following sub-menus:

- *File Menu* (Figure 5-66)
- *View Menu* (Figure 5-67)
- *Tools Menu* (Figure 5-68)
- *Help Menu* (Figure 5-69).

5.2.18.1 *File Menu*

The File Menu includes the following entries:

- **Update ISM (F6):** Invokes an update process of the ISM server.
- **Exit (Alt+F4):** Quits the current session and the ISM UI.
- **Logout (Ctrl+Alt+F4):** Quits the current session and opens the Login window.

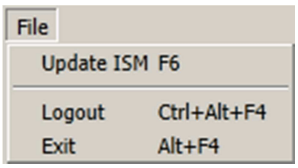


Figure 5-66 UI – Menu Bar – File Menu

5.2.18.2 *View Menu*

The View Menu includes the following entries:

- **Overview Page:** Shows or hides the Overview Page, see section 5.2.6.
- **Directory:** Shows or hides the Directory, see section 5.2.1.
- **General:** Shows or hides the General Page, see section 5.2.8/5.2.9.
- **Properties:** Shows or hides the Properties Page, see section 5.2.7.
- **Pending Tasks:** Shows or hides the Pending Tasks window, see section 5.2.2.
- **Virus List:** Shows or hides the Virus List, see section 5.2.3.
- **Log File:** Shows or hides the Log File, see section 5.2.4.
- **Change Log:** Shows or hides the Change Log, see section 5.2.5.
- **Restore Default Layout:** Restores the default window layout.
- **Toolbars/Main toolbar:** Shows or hides the Main toolbar, see section 5.2.19.
- **IKARUS anti.virus Configurations:** Opens the **IKARUS anti.virus** Configurations Window, see section 0.

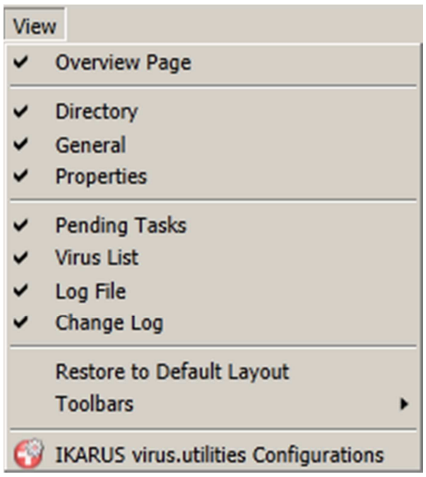


Figure 5-67 UI – Menu Bar – View Menu

© 2012 IKARUS Security Software GmbH

5.2.18.3 *Tools Menu*

The Tools Menu includes the following entries:

- **Options (F12):** Opens the **IKARUS security.manager** Options window, see Section 5.2.14.
- **Clean host-entries from database:** It is possible to clean up the database from unused hosts by using the dialog "**Clean host-entries from database**". For further information on this dialog see section 5.2.15.
- **Change Password:** Opens the Change Password window where you can set a new password for the **IKARUS security.manager**.
- **Change Language:** Opens the Change Language window where you can select a different **IKARUS security.manager UI** language. Changing the UI language does not require a program restart.
- **IKARUS Virus Dictionary:** Opens the default web browser and changes to the IKARUS Virus Dictionary.
- **Save Support Info:** Generates a "*ZIP*" file that is generated on the **IKARUS security.manager Server** that can be saved on your local system. This file holds all necessary information which the support department of **IKARUS Security Software** needs to retrieve information about your system.

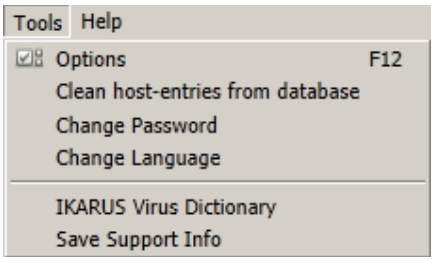


Figure 5-68 UI – Menu Bar – Tools Menu

5.2.18.4 *Help Menu*

The Help Menu includes the following entries:

- **User Manual (F1):** Opens this **IKARUS security.manager** User Manual.
- **Contact Information:** Opens the Contact Information window.
- **General Business Terms:** Opens the General Business Terms of the **IKARUS security.manager**.
- **About IKARUS security.manager:** Opens the About dialog that displays the **IKARUS security.manager** version and information about the license in use.

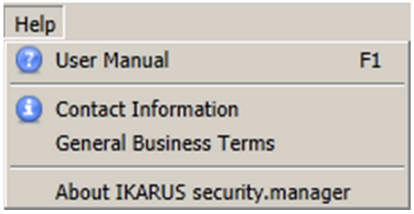


Figure 5-69 UI – Menu Bar – Help Menu

5.2.18.5 *Management Menu*

The management menu includes the following entries and is only available when management-mode is activated:

- **Options:** Opens the options-window for editing settings of the used **IKARUS security.manager-Servers** (see section 5.2.17.1).
- **Export config:** Using this menu it is possible to export already entered **IKARUS security.manager-Server** (see section 5.2.17.2).
- **Change password for management mode:** Use this dialog if changing the management-mode password is necessary (see chapter 5.2.17.3). **Note**, that changes of the management-password have no impact of the password of all entered **IKARUS security.manager-Server**.

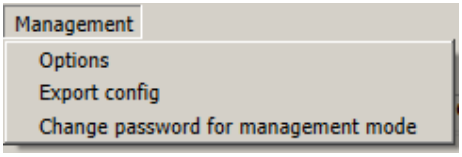


Figure 5-70: UI – Menu Bar – Management Menu

© 2012 IKARUS Security Software GmbH

5.2.19 The Toolbar

The **Toolbar** (Figure 5-71) can be found at the top of the **IKARUS security.manager UI** main window right below the *Menu Bar*. The **IKARUS anti.virus** Configurations opens the **IKARUS anti.virus** Configurations window, see section 0 for more information.

5.2.19.1 *Layout*

Figure 5-71 UI – Toolbar

© 2012 IKARUS Security Software GmbH

6 The Shared Directory

The **Shared Directory** is the *network share* where the *ismxstartup.exe* file will reside. As this executable is required for installing the **IKARUS anti.virus** on a *client*, that particular *client* needs read access to that share and file. Further, the **IKARUS security.manager Server** needs write access to that *network share* to place the file on the share in the first place. You can specify the **Shared Directory** in the *General IKARUS security.manager Settings* dialog (see
Figure 5-43).

© 2012 IKARUS Security Software GmbH

7 Licensing Information

To **secure your network and operate the IKARUS security.manager**, you will need a **valid license**. A license grants a **defined amount of user licenses** and should be selected appropriately for the **size of your company**. The **IKARUS security.manager** license is shared with all *clients* you need to administer. It is not possible to administer and run more **IKARUS anti.virus** instances on your network than the license allows. Licenses for non-administered *clients* (if you previously have bought one or more licenses for them) may exist; if not, you will not be able to administer any more *clients* after reaching the *client* limit of your **IKARUS security.manager** license. In this case, those particular clients will not be secured by the **IKARUS anti.virus** and will thus be unsecure. **Remember that clients without a valid license are a possible threat to your entire network**.

7.1 Registration

If there is no valid **IKARUS security.manager** license, the following dialog (Figure 7-1) will show up asking you to provide a valid license using an IKARUS license file or an *IKARUS Activation Key*.

In the Registration dialog it is possible to choose one out of the following two options to register your IKARUS security.manager:

- **License File:** Opens a file browser where you can choose the IKARUS license file you want to use.
- **Activation Key:** Opens the activation window, see section 7.2.

7.1.1 Layout

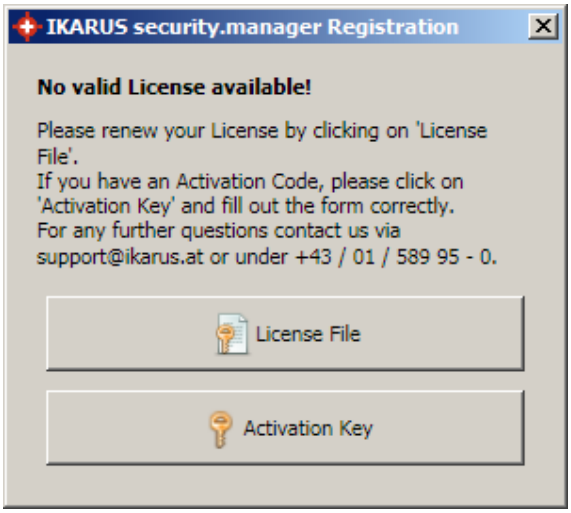


Figure 7-1 UI – IKARUS security.manager Registration

7.2 Activation Key

If you have an *IKARUS Activation Key* rather than IKARUS license file, you may obtain a valid license from the *License Activation* window (Figure 7-2). Provide the requested information and submit your data. Upon successful submission of your data, you will get an e-mail with your license file attached to the specified address. All fields that have an asterisk are obligatory.

© 2012 IKARUS Security Software GmbH

7.2.1 Layout

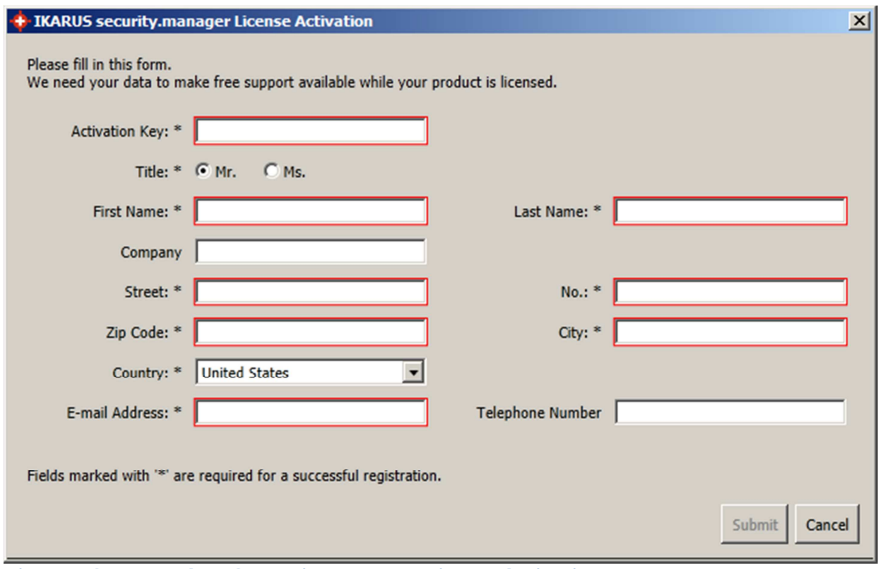


Figure 7-2 UI – IKARUS security.manager License Activation

© 2012 IKARUS Security Software GmbH

8 Software Distribution

The installation and uninstallation processes for the **IKARUS anti.virus** are subdivided into different steps. To complete these steps successfully, the following criteria **must be met**:

- The **IKARUS security.manager Server** needs a *shared directory* (see Figure 5-43) set to place the binaries needed for a remote installation.
- The **IKARUS security.manager Server** needs appropriate rights to remotely execute binaries on the target *client*. If the **IKARUS security.manager Server** has been installed with a *domain* administrator account and the target *client* is on the same *domain* as the **IKARUS security.manager Server**, no further adjustments need to be made for that *client*; otherwise, you need to specify credentials having appropriate rights to launch executable files on the target *client*. You can configure this on a client's *Rights Management* tab on the **IKARUS security.manager UI**.
- The target *client* needs at least read access to the user-defined *shared directory* to retrieve the *ismxstartup* binary.
- The *TCP* communication ports need to be forwarded when using a firewall.
- The target *client* must meet the hardware and software requirements specified to operate the **IKARUS anti.virus**. Refer to the requirements indicated in the **IKARUS anti.virus manual**.
- The *Enforce Client Update* option in the ***IKARUS security.manager*** *Settings* windows (Figure 5-43) must be enabled.

© 2012 IKARUS Security Software GmbH

8.1 Installing the IKARUS anti.virus

To install and deploy the **IKARUS anti.virus,** right-click a *client* or group in the *Directory* to open the context menu and click on the *Install anti.virus* entry (Figure 5-15). The installation of the **IKARUS anti.virus** includes the below steps (Figure 8-1). It can take a moment, so please wait patiently:

- Step 1: The **IKARUS security.manager Server** places the needed executable files in the *Shared Directory*.
- Step 2: The **IKARUS security.manager Server** tries to install the *ismxstartup service* remotely from the *Shared Directory*. The target *client* needs read access to the *Shared Directory* and to files in it.
- Step 3: The *ismxstartup service* retrieves the *guardxup* binary from the **IKARUS security.manager Server**, places it into the Windows temp directory of the target *client*, and launches it.
- Step 4: The *guardxup* binary performs all further steps left for installing the **IKARUS anti.virus** on the target *client*. This includes retrieving the **IKARUS anti.virus** binaries from the **IKARUS security.manager Server** and installing them on the target.

© 2012 IKARUS Security Software GmbH

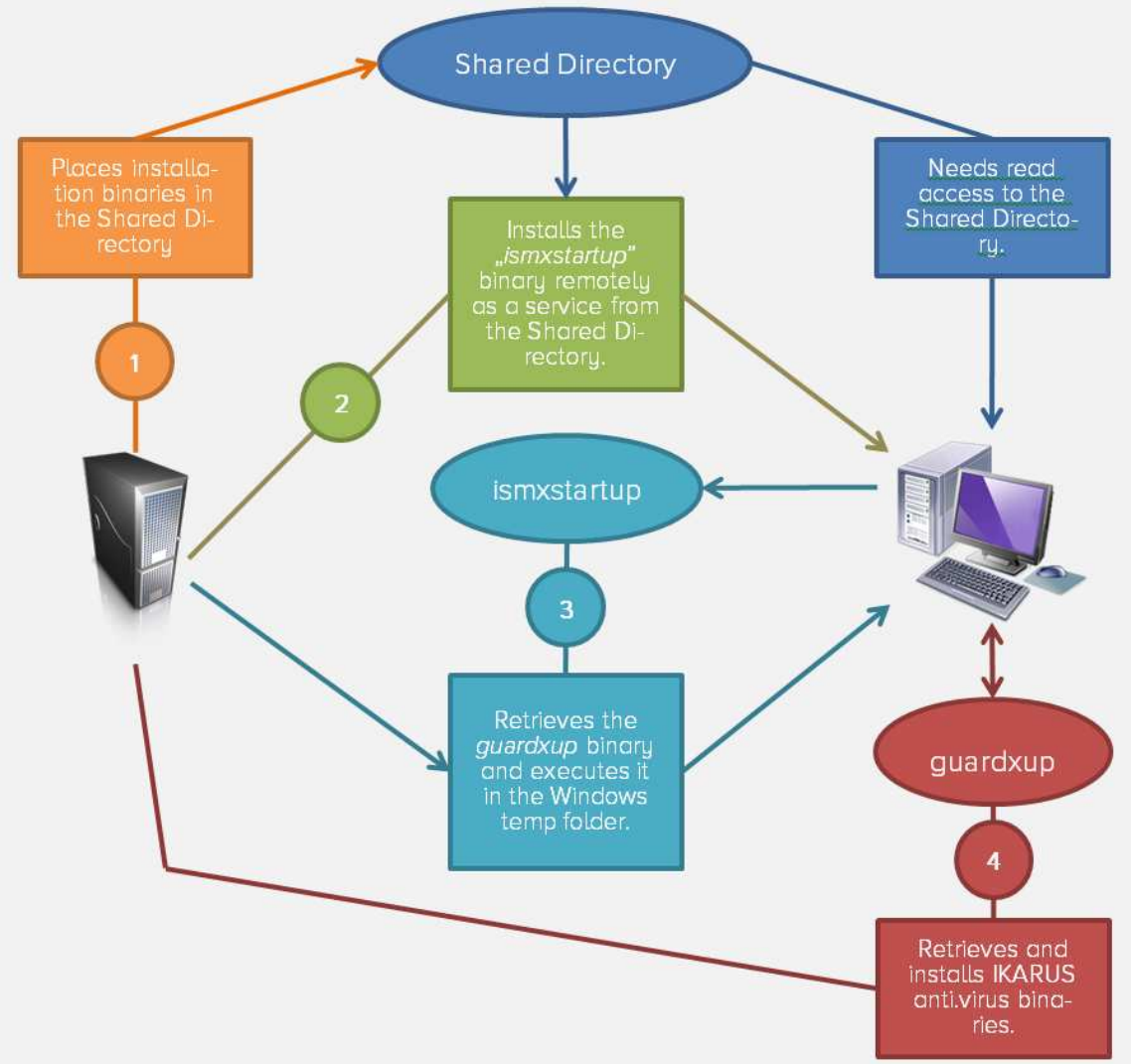


Figure 8-1 Software Distribution – Installation process

© 2012 IKARUS Security Software GmbH

8.2 Uninstalling the IKARUS anti.virus

To uninstall the **IKARUS anti.virus,** right-click the *client* or group of the *Directory*. In the opening context menu, click the *Uninstall anti.virus* item (Figure 5-15).

Note: Uninstallation can be done for *administered clients* only.

© 2012 IKARUS Security Software GmbH

9 Config File

The **Config File** (named *ism.conf*) exists in the *conf* directory of the installation destination which will be chosen when installing the **IKARUS security.manager Server** (see section 4.1.9). The *MSSQL*-database connection information as well as the *LDAP* connection settings and the *TCP* ports used for the communication between the **IKARUS anti.virus** and the **IKARUS security.manager** are configured by this file.

Sample Config file:

```
<config>
  dbconnstring      DRIVER={SQL Server};SERVER=localhost
  serverport        9887
  clientupdateport  9888
  timespanAD        12
</config>

<ldap>
  type              native
  servername        esx-2k8-de-srv.labor.local
  searchpath        dc=labor,dc=local
  authmethod        simple
  username          LDAP Connector
  password          none
  attribute         dNSHostName
  filter            (objectCategory=computer)
</ldap>
```

Note: It is possible to edit *LDAP* parameters by the help of the **IKARUS security.manager** settings within the **IKARUS security.manager UI**. For further information please check section 5.2.14.6.

© 2012 IKARUS Security Software GmbH

9.1 The <*config*> Section

In the <*config*> section, you can provide information about the *MSSQL* database used by the **IKARUS security.manager Server** for storing data and information and about the *TCP* ports used for communication. Furthermore it is possible to set the scheduled time or timespan, when the *Active Directory* should be refreshed in the **IKARUS security.manager Server**.

Setting	Description
`dbconnstring`	The information used for establishing a connection to the target *MSSQL* database. Includes the server name where the database resides and authentication methods needed for accessing the database. For more information about the syntax and available properties of the connection string, refer to your *MSSQL* documentation.
`serverport`	The *TCP* port used for the communication between the **IKARUS security.manager Server** and the **IKARUS security.manager UI**. If you use a ***firewall***, make sure to **forward** this port.
`clientupdateport`	The *TCP* port used for the communication between the update binaries and the **IKARUS anti.virus**. If you use a ***firewall***, make sure to **forward** this port.
`timespanAD`	Allows values between **1 and 24**, which means that from the time, when the value was provided (or the server was restarted), every X hours the *Active Directory* is reloaded. The default setting for reloading the *AD* is internally set to **"every 12 hours"**. This setting always overrules, if set in the config file, the **dailytimeAD** setting.
`dailytimeAD`	Allows values between **0 and 23**, which means that every day at the given time the *AD* is reloaded. It is not possible to use this setting together with the **timespanAD** setting. The **timespanAD** setting, if set, always overrules the **dailytimeAD** setting.

© 2012 IKARUS Security Software GmbH

9.2 The <*ldap*> Section

The <*ldap*> section includes information about the *LDAP* *server* the **IKARUS security.manager Server** connects to resolve the *clients* existing in your *active directory*. If no <*ldap*> section is found in the *config file*, the **IKARUS security.manager Server** will try to obtain the information from the *domain controller*.

Setting	Description
`type`	The type of the *LDAP* configuration.
`servername`	The name of the *domain controller*.
`searchpath`	Specifies the domains to scan. *Domain* levels are split with the *dc* (*Domain* component) keyword. Example for a *.company.local* domain: `searchpath dc=company dc=local`
`authmethod`	Describes the method used for authenticating with the *domain controller*. If you do not want to authenticate with a specific user, specify *anonymous* here.
`username`	Sets the username used for authenticating with the *domain controller*. Only required if the authentication method is not set to *anonymous*.
`password`	Sets the password used for authenticating with the *domain controller*. Only required if the authentication method is not set to *anonymous*.
`attribute`	Sets the attribute to read.
`filter`	Sets the criteria used on resolving the specified *attribute*.

© 2012 IKARUS Security Software GmbH

10 Table of Figures

Figure 4-1 Server Installation – Welcome ..... - 12 -
Figure 4-2 Server Installation – License Agreement ..... - 13 -
Figure 4-3 Server Installation – LDAP Settings ..... - 14 -
Figure 4-4 Server Installation – Deployment Settings ..... - 15 -
Figure 4-5 Server Installation – User Settings ..... - 16 -
Figure 4-6 Server Installation – Network Settings ..... - 17 -
Figure 4-7 Server Installation - Installation of SQL Express ..... - 18 -
Figure 4-8 Server Installation – Database Settings ..... - 19 -
Figure 4-9 Server Installation – Select Installation Folder ..... - 20 -
Figure 4-10 Server Installation – Confirm Installation ..... - 21 -
Figure 4-11 Server Installation – Installation Complete ..... - 22 -
Figure 4-12 UI Installation – Welcome ..... - 25 -
Figure 4-13 UI Installation – License Agreement ..... - 26 -
Figure 4-14 UI Installation – Select Installation Folder ..... - 27 -
Figure 4-15 UI Installation – Confirm Installation ..... - 28 -
Figure 4-16 UI Installation – Installation Complete ..... - 29 -
Figure 5-1 UI – Login ..... - 31 -
Figure 5-3: UI - Login (Single mode) ..... - 32 -
Figure 5-4: UI –Password definition (single mode) ..... - 33 -
Figure 5-6 UI – Change Management ..... - 36 -
Figure 5-8 UI – User Interface ..... - 39 -
Figure 5-9 UI – Directory (single mode) ..... - 40 -
Figure 5-10 UI - Directory Toolbar ..... - 41 -
Figure 5-11 The scan options ..... - 41 -
Figure 5-12 The context menu for actions on a client ..... - 42 -
Figure 5-13 The choice for administration or exclusion from administration ..... - 42 -
Figure 5-14 The Group/Client Tree ..... - 43 -
Figure 5-15 The Context-Menu for a Group/Client ..... - 43 -
Figure 5-16 UI – Directory Filter ..... - 44 -
Figure 5-17 UI – Pending Tasks ..... - 47 -
Figure 5-18 UI – Task Details ..... - 49 -
Figure 5-19 UI – Virus List ..... - 51 -
Figure 5-20 UI – Virus Information ..... - 51 -
Figure 5-21 UI – Log File ..... - 52 -
Figure 5-22 UI – Change Log ..... - 53 -
Figure 5-23 UI – Overview Page ..... - 55 -
Figure 5-24 UI – Properties Page ..... - 57 -
Figure 5-25 UI – General Page on Groups ..... - 58 -
Figure 5-26 UI – General Page on Clients ..... - 61 -
Figure 5-27 UI – Notification Bar ..... - 62 -
Figure 5-28 UI – Charts Page ..... - 63 -
Figure 5-29 UI – Global overview page ..... - 64 -
Figure 5-30 UI – Global overview page - shortcut menu ..... - 65 -
Figure 5-31 UI – IKARUS anti.virus Configurations ..... - 66 -
Figure 5-32 Configuration General tab ..... - 67 -
Figure 5-33 Configuration e-mail tab ..... - 68 -
Figure 5-34 Configuration Update tab ..... - 69 -
Figure 5-35 Configuration Dial-Up Connections tab ..... - 70 -
Figure 5-36 Configuration Exclusion tab (File exclusion) ..... - 71 -

© 2012 IKARUS Security Software GmbH

Figure 5-37 Configuration Logs tab ..... - 72 -
Figure 5-38 Configuration Extras tab ..... - 72 -
Figure 5-39 Configuration Anti-Spam tab ..... - 73 -
Figure 5-40 Configuration Advanced Spam Protection ..... - 74 -
Figure 5-41 Configuration Scans tab ..... - 75 -
Figure 5-42 Configuration Add Scan Profile ..... - 75 -
Figure 5-43 UI – IKARUS security.manager Settings – General ..... - 77 -
Figure 5-44 UI – IKARUS security.manager Settings – E-Mail Notifications ..... - 78 -
Figure 5-45 UI – IKARUS security.manager Settings – Reports ..... - 79 -
Figure 5-46 UI – IKARUS security.manager Settings – Update ..... - 81 -
Figure 5-47 UI – IKARUS security.manager Settings – Fileshare ..... - 82 -
Figure 5-48 UI – IKARUS security.manager Settings – LDAP ..... - 84 -
Figure 5-49 Charts options ..... - 85 -
Figure 5-50 PDF Report settings ..... - 86 -
Figure 5-51 UI – Clean host-entries from database ..... - 87 -
Figure 5-52 UI – About Dialog ..... - 88 -
Figure 5-53 : UI - "Management" menu, "Export configuration file" menu option ..... - 89 -
Figure 5-54 : UI – Options dialogue ..... - 89 -
Figure 5-55 : UI – Shortcut menu in the options dialogue ..... - 90 -
Figure 5-56 : UI - Edit dialogue ..... - 91 -
Figure 5-57 : UI - Edit dialogue, entering invalid data ..... - 91 -
Figure 5-58 : UI - Edit dialogue, changing the password for a new installation ..... - 92 -
Figure 5-59 : UI - Edit dialogue, checking the access data ..... - 93 -
Figure 5-60: UI - "Management" menu, "Export configuration file" menu option ..... - 94 -
Figure 5-61: UI - "Export configuration file" dialogue - selecting the ISM instances to be exported ..... - 94 -
Figure 5-62: UI "Export configuration file" dialogue - error message in the event of an invalid password. ..... - 95 -
Figure 5-63: UI "Export configuration file" dialogue - valid password ..... - 96 -
Figure 5-64: UI - Save file dialogue for exporting the configuration file ..... - 96 -
Figure 5-65: UI - Changing the password for management mode ..... - 97 -
Figure 5-66 UI – Menu Bar – File Menu ..... - 98 -
Figure 5-67 UI – Menu Bar – View Menu ..... - 99 -
Figure 5-68 UI – Menu Bar – Tools Menu ..... - 100 -
Figure 5-69 UI – Menu Bar – Help Menu ..... - 101 -
Figure 5-70: UI – Menu Bar – Management Menu ..... - 101 -
Figure 5-71 UI – Toolbar ..... - 102 -
Figure 7-1 UI – IKARUS security.manager Registration ..... - 104 -
Figure 7-2 UI – IKARUS security.manager License Activation ..... - 105 -
Figure 8-1 Software Distribution – Installation process ..... - 108 -

© 2012 IKARUS Security Software GmbH

11 Glossary

Abbreviation	Term	Description
	IKARUS anti.virus	The IKARUS virus.utilities will be renamed to IKARUS anti.virus in 2012; This is why the new name of the product is already used in this document.
	Windows service	A Windows service is an executable designed for running in the background without user interaction. Windows services can be set up to automatically start at boot time. Windows services can be installed either using a user account available on your Windows network or a local service account.
MSSQL	Microsoft Structured Query Language	Microsoft SQL Server is a relational database server developed by Microsoft. Its primary function is to store and retrieve data as requested by other software applications running on the same computer or a different computer on a network (including the Internet).
TCP	Transmission Control Protocol	The Transmission Control Protocol is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite and complements the *Internet Protocol*. Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable ordered delivery of a byte stream from a program on one computer to another program on a different computer.
IP	Internet Protocol	The Internet Protocol is the principal communication protocol used for relaying datagrams (packets) across an internetwork using the IP Suite. It allows for routing packets across network boundaries and is the primary foundation of the Internet.
LDAP	Lightweight Directory Access Protocol	LDAP is an application protocol for accessing and maintaining distributed directory information services over an *Internet Protocol* network.
	Proxy Server	In computer networks, a proxy server is a server (i.e. a computer system or an *application*) acting as an intermediary for requests from *clients* seeking resources from other *servers*.

© 2012 IKARUS Security Software GmbH

	Network share	In computing, a shared resource or network share is a device or piece of information on a computer that can be remotely accessed from another computer, typically on a *local area network* or an enterprise *intranet*. The access is transparent: There is no difference between accessing a local or remote resource.
LAN	Local Area Network	A local area network is a computer network that interconnects computers in a specific area such as a home, a school, a computer laboratory, or an office building.
	Intranet	An intranet is a computer network that uses *Internet Protocol* technology for securely sharing any parts of an organization's information or network operating system within that organization.
AD	Active Directory	The Active Directory is a *directory service* developed by Microsoft for Windows domain networks. It is part of the most Windows Server operating systems. Server computers running Active Directory are referred to as *domain controllers*.
	Windows domain	A Windows domain is a collection of security principals sharing a central directory database. This central database (known as *Active Directory* starting with Windows 2000[1], *Active Directory* Domain Services in Windows Server 2008 and Server 2008 R2, also referred to as NT Directory Services on Windows NT operating systems, or NTDS) holds the user accounts and security information for resources in that domain. Each person who uses computers in a domain gets a unique account or user name. This account can then be assigned access to resources within the domain.
	Directory Service	A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows for looking up values associated with a name; this is similar to a dictionary.
DC	Domain Controller	On Windows Server systems, a domain controller is a *server* handling security authentication requests (logins, permissions checks, etc.) in the *Windows Server domain*. A domain is a concept introduced with Windows NT that

© 2012 IKARUS Security Software GmbH

		grants a user access to a number of computer resources if he or she can provide a combination of a username and password.
	Server	In the context of client-server architectures, a server is a computer program serving the requests of other computer programs named *clients*. The means that the server performs computational tasks on behalf of *clients*. The *clients* either run on the same computer or connect through a network.
	Client	A client is an application or system that accesses a service made available by a *server*. The *server* typically (but not always) exists on a different computer system. In that case, the client accesses the service over the network.
FQDN	Fully Qualified Domain Name	A fully qualified domain name, sometimes also referred as an “absolute domain name”, is a domain name that specifies its exact location in the tree hierarchy of the *Domain Name System* (DNS). The FQDN includes all domain levels including the *top-level domain* and the *root zone*. A fully qualified domain name is distinguished by its unambiguity; it can only be interpreted one way.
	Domain Name	A domain name is an identification string that defines a scope of administrative autonomy, authority, or control on the Internet. Domain names are formed according to the rules and procedures of the *Domain Name System (DNS)*.
DNS	Domain Name System	The Domain Name System is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various pieces of information with *domain names* assigned to each of the participating entities. Most importantly, it translates *domain names* meaningful to humans to the numerical identifiers associated with networking equipment for the purpose of locating and addressing those devices worldwide.
TLD	Top-Level Domain	A top-level domain is a domain at the highest level in the hierarchical *Domain Name System (DNS)*. Top-level domain names are installed in the *root zone* of the name space. For all subordinate domains, the top-level domain is the

© 2012 IKARUS Security Software GmbH

		last part of the *domain name*, that is, the last label of a *fully qualified domain name*.
	Root Zone	A root zone is the top-level DNS zone in a hierarchical namespace using the *Domain Name System (DNS)*. The term typically refers to the root zone of the largest global network, the Internet.
	DNS Zone	A DNS zone is a part of a *domain name* space using the *Domain Name System (DNS)*, for which administrative responsibility has been delegated.
	IKARUS Activation Key	
	Administer	In the context of the IKARUS security.manager, administration means that a *client* with the IKARUS anti.virus installed is managed by the IKARUS security.manager: The client gets updates, configurations, licenses and settings from the IKARUS security.manager. If a *client* is not administered, only status information will be displayed. The limit of *clients* you are allowed to administer is specified in the license you are using.
	Application (Software)	Application software, also known as an application or an “app”, is *computer software* designed to help the user to perform specific tasks.
	Computer Software	Computer software, or just software, is a computer programs with its related data providing instructions for telling a computer what to do and how to do it. In other words, software is a conceptual entity, which is a set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system.
	Firewall	A firewall is a device or set of devices designed to permit or deny network communication based upon a set of rules. Firewalls are typically used for protecting networks from unauthorized access while permitting legitimate communications.
	ZIP	ZIP is a file format used for data compression and archiving. A zip file contains one or more files that have been compressed, to reduce file size, or stored as is.

© 2012 IKARUS Security Software GmbH

© 2012 IKARUS Security Software GmbH

© 2012 IKARUS Security Software GmbH. All rights reserved

The information contained in this document represents the current view of IKARUS Security Software GmbH on the issues discussed as of the date of publication. Because IKARUS Security Software GmbH must respond to changing market conditions, it should not be interpreted to be a commitment on the part of IKARUS Security Software GmbH, and IKARUS cannot guarantee the accuracy of any information presented after the date of publication.

This paper is for informational purposes only. IKARUS Security Software GmbH MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Other product and company names mentioned herein may be the trademarks of their respective owners.

IKARUS Security Software GmbH Blechturmgasse 11 in 1050 Vienna Austria