

Administrative Console 2.1

Operating Manual

Technical Support:

1 800 678 0394

1 703 734 1998

support@safefrontier.com

Administrative Console 2.1

Operating Manual

Technical Support:

1 800 678 0394

1 703 734 1998

support@safefrontier.com

1777

Note:

Before using the True Security™ Mobile products, be sure to read the information contained in this Manual.

First Edition (Jun 2009)

The following paragraph does not apply to the countries where such provisions are inconsistent with the local law:

SAFE FRONTIER CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE LIMITED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

Some states do not allow disclaimers or express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new additions of the publication. Safe Frontier Inc. (SafeFrontier), may make improvements or changes in the products or the programs described in this publication at any time.

Request for technical information about SafeFrontier products should be made to your SafeFrontier Authorized Dealer or your SafeFrontier Marketing Representative.

Table of Contents

Welcome!

Mobile Admin interface

| | |
|---------------------------------|---|
| Main Menu..... | 1 |
| Notification Area..... | 1 |
| Computer List | 1 |
| Report and Policy List..... | 3 |
| Main Window..... | 4 |
| Interact with Mobile Admin..... | 4 |

Quick Start (How to?)

| | |
|-------------------------------------|---|
| How to use free products..... | 5 |
| How to use your free trials..... | 5 |
| How to use commercial products..... | 5 |

Installation

| | |
|--------------------------------|---|
| Download products..... | 6 |
| Get your installation key..... | 7 |
| Local installation..... | 7 |
| Centralized deployment..... | 7 |
| Update or uninstall..... | 8 |
| Update products..... | 8 |

| | |
|-------------------------------------|---|
| Local uninstall..... | 8 |
| Uninstall via Active Directory..... | 9 |

Manage licenses

| | |
|---------------------------------|----|
| All licenses..... | 9 |
| Active licenses..... | 10 |
| Empty (available) licenses..... | 10 |
| Expiring licenses..... | 10 |
| Free licenses..... | 11 |
| Trial licenses..... | 11 |
| Commercial licenses..... | 17 |
| Get new free licenses..... | 12 |
| Obtain a trial license..... | 12 |
| Order new licenses..... | 12 |
| Activate new licenses..... | 13 |
| Assign or update licenses..... | 13 |
| Remove licenses..... | 14 |

Control computers

| | |
|---------------------------|----|
| All computers..... | 15 |
| Active computers..... | 15 |
| Non-active computers..... | 15 |

Table of Contents

| | |
|-------------------------------------|----|
| New activated computers..... | 15 |
| Stolen computers..... | 16 |
| Customize your computers..... | 17 |
| Groups of computers..... | 18 |
| Computer summary..... | 18 |
| Assign policy to computer..... | 20 |
| Policy templates..... | 21 |
| Pending policies..... | 22 |
| General Mobile Security policy..... | 22 |
| Communications..... | 23 |
| Self-protection..... | 23 |
| Disable products..... | 28 |
| Licensing..... | 24 |
| Products update..... | 24 |
| Products install/uninstall..... | 29 |
| Troubleshoot..... | 25 |
| Location Tracking policy..... | 25 |
| Communications..... | 25 |
| Location tracking policy..... | 26 |
| Image capturing..... | 26 |
| Incident Response policy..... | 26 |

| | |
|----------------------------------|----|
| Communications..... | 27 |
| "Stolen" policy..... | 27 |
| "No connection" policy..... | 30 |
| Inventory Management policy..... | 31 |
| Communications..... | 31 |
| System audit policy..... | 31 |
| Event logging policy..... | 32 |
| Report computer stolen..... | 33 |
| View policy log..... | 33 |
| Computer policies log..... | 34 |
| Remove computer..... | 34 |

Process reports

| | |
|--------------------------|----|
| All reports..... | 35 |
| New reports..... | 35 |
| Load new reports..... | 35 |
| View report lists..... | 36 |
| View reports..... | 37 |
| Tree-view reports..... | 37 |
| Table-view reports..... | 38 |
| General information..... | 38 |

Table of Contents

| | |
|----------------------------|----|
| Products and Licenses..... | 38 |
| System Information..... | 38 |
| Local Users..... | 38 |
| Local Groups..... | 39 |
| Location tracking..... | 39 |
| Session Monitoring..... | 39 |
| IP Tracking..... | 39 |
| Wi-Fi Tracking..... | 39 |
| GPS Tracking..... | 40 |
| GSM Tracking..... | 40 |
| Incident response..... | 41 |
| All response results..... | 41 |
| Computer shutdown..... | 42 |
| Warning messaging..... | 42 |
| Data delete..... | 42 |
| Data download..... | 42 |
| Inventory management..... | 42 |
| Hardware tracking..... | 43 |
| Software tracking..... | 43 |
| Services..... | 43 |
| Printers..... | 44 |
| Event Viewer..... | 44 |

| | |
|------------------------------------|----|
| Compliance monitoring..... | 45 |
| Account policies..... | 45 |
| Local policies..... | 45 |
| Software restriction policies..... | 46 |
| Public key policies..... | 46 |
| Firewall policies..... | 46 |
| Security Center..... | 47 |
| Find reports..... | 48 |
| Export reports..... | 48 |
| Remove reports..... | 48 |
| Clear configuration changes..... | 48 |

Change settings

| | |
|--------------------------|----|
| Contact information..... | 49 |
| Interface settings..... | 50 |
| Security settings..... | 50 |
| Change password..... | 51 |
| Account maintenance..... | 51 |

Help Desk Service

| | |
|------------------------------|----|
| Create new support case..... | 52 |
|------------------------------|----|

Table of Contents

| | |
|---|----|
| Open your existing cases..... | 52 |
| Your existing case..... | 52 |
| Send new support message..... | 52 |
| APPENDIX 1. How to use free products..... | 53 |
| APPENDIX 2. How to use free trial..... | 54 |
| APPENDIX 3. How to use commercial products..... | 55 |
| APPENDIX 4. Standards and Guidelines..... | 56 |
| APPENDIX 5. Requirements and Limitations..... | 57 |
| Figure 1. Mobile Admin Interface..... | 2 |
| Figure 2. Computer List Toolbar..... | 3 |
| Figure 3. Computer List Controls..... | 3 |
| Figure 4. Group Operations..... | 4 |
| Figure 5. Reports and Policy List Toolbar..... | 4 |
| Figure 6. Interact with Mobile Admin..... | 5 |
| Figure 7. Assign Licenses..... | 14 |
| Figure 8. Rename Computer..... | 17 |
| Figure 9. Rename Group..... | 18 |
| Figure 10. Manage Groups and Computers..... | 19 |
| Figure 11. Open Computer Policy..... | 20 |
| Figure 12. Manage Computer Policy..... | 21 |
| Figure 13. Program Execution..... | 27 |

| | |
|--|----|
| Figure 14. Data Download..... | 28 |
| Figure 15. Data Delete..... | 29 |
| Figure 16. Report Computer Stolen..... | 32 |
| Figure 17. Computer and Policy List..... | 34 |
| Figure 18. Reports..... | 36 |
| Figure 19. Find Reports..... | 47 |
| Figure 20. Change Password..... | 49 |
| Figure 21. Create New Support Case..... | 50 |

Mobile Admin Interface

Mobile Admin Interface

The Mobile Admin console consists of five functional zones:

1. Main Menu
2. Notification Area
3. Computer List
4. Report and Policy List
5. Main Window

See **Figure 1**.

Main Menu

In the Main Menu you will find all commands available in your console. Commands are grouped in usable menu items and submenus.

At the bottom right corner of the main menu you will find three tabs:

Tasks:

This tab contains frequently used commands.

Summary:

This tab contains a summary of your account and resources.

Tips:

This tab contains help tips for current content displayed in the Main Window.

On the left of the Main Menu you will find Back and Forward buttons to navigate your visited pages. These buttons are also used to navigate your visited Help Tips. You can use the History List near these buttons to navigate to a particular page that you have visited previously.

Notification Area

This area located at the right of the Mobile Admin logo contains important notifications about your computers, licenses, new reports, and new support messages.

Clicking on the notification, you will be directed to the appropriate page.

Computer List

The Computer List located under the Mobile Admin logo displays a list of all computers. Computers can be grouped into functional, organizational, or other groups. All operations with computers and groups can be made using the Computer List toolbar or from the context (right-click) menu (see **Figure 2**).

Mobile Admin Interface

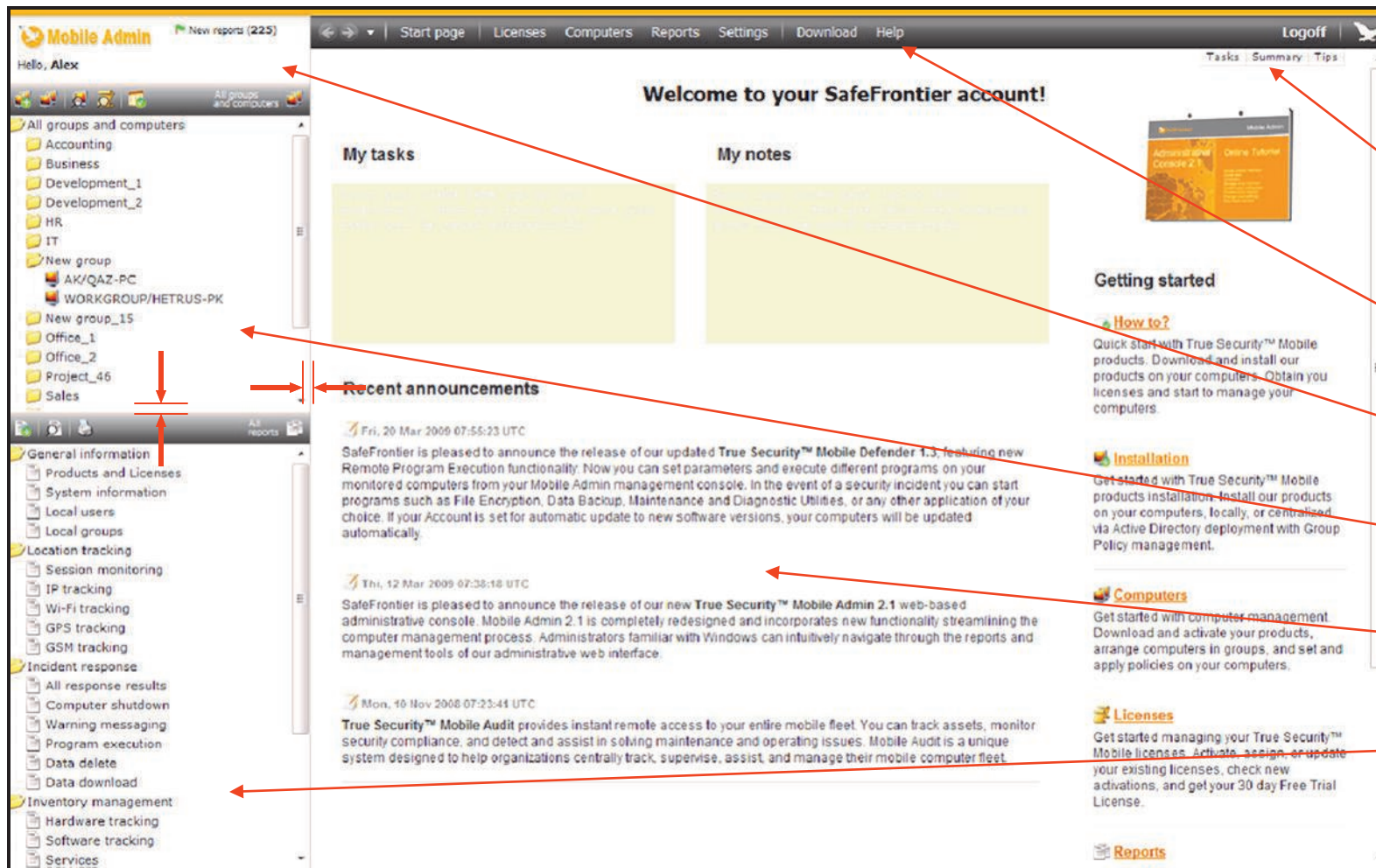


Figure 1.

Mobile Admin Interface

Tasks, Summary, Tips

Main Menu

Notification Area

Computer List

Main Window

Report and Policy List

Mobile Admin Interface

To select different views of the Computer List use the drop-down menu at the right of the Computer List Toolbar (see **Figure 2**). You can select different groups and types of computers to display in the Computer List.

Note: If the current page shown in the Main Window displays group operations, the check boxes for each computer and group in the Computer List will be shown (see **Figure 4**). To open the Computer List in the Main Window select the Manage Groups and Computers button (see **Figure 3**).

Report and Policy List

The Report and Policy List is located below the Computer List and contains reports and policies grouped by functional problem-oriented folders.

To select between reports and policies use the drop-down menu at the right of the Report and Policy List Toolbar (see **Figure 5**).

If you click on a report in this list, and no computer is selected in the Computer List, a list of all reports of the selected type from all computers will be shown. If a computer is selected, the appropriate report from the selected computer will be shown (see **Figure 6**).



Figure 2.

Computer List Toolbar

Computer List Toolbar

Drop-Down Menu

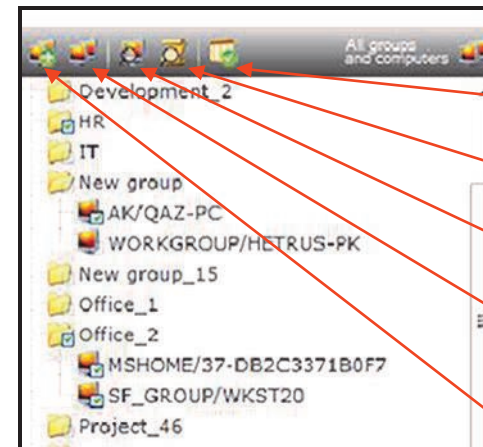


Figure 3.

Computer List Controls

Refresh Computer List

Find License

Find Computer

Manage Groups and Computers

Create New Group

Mobile Admin Interface

Main Window

This window contains all processing output.

Interact with Mobile Admin

If you select (click) a computer in the Computer List, and no item is selected in the Report and Policy List, the Computer Summary page will be loaded.

If you select a computer in the Computer List, and there is an item selected in the Report and Policy List (or if you select a report or policy in the Report and Policy List, and a computer is selected in the Computer List), the appropriate report or policy for this computer will be loaded.

If you select a report in the Report and Policy List, and no item is selected in the Computer List, a list of reports of this type from all your computers will be loaded.

If you select a policy in the Report and Policy List, and no item is selected in the Computer List, the default policy will be shown.

See **Figure 6**.

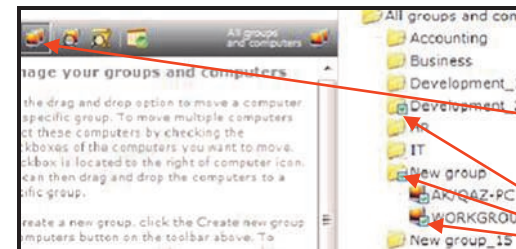


Figure 4.

Group Operations

Manage Groups and Computers

Checkboxes

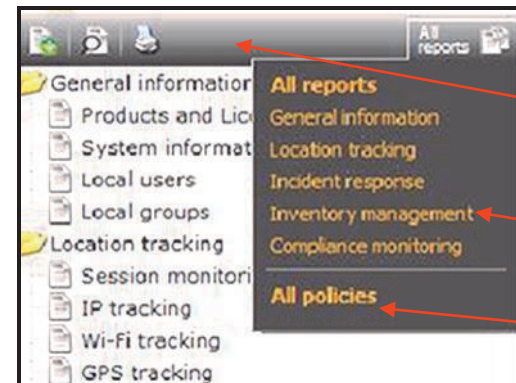


Figure 5.

Reports and Policy List Toolbar

Report and Policy List Toolbar

Drop-Down Menu

Select to switch to Policy Window

Quick Start (How to?)

Quick Start (How to?)

On this page you can find the answers to basic questions on how to use SafeFrontier True Security™ Mobile products and solutions.

How to:

- Install and start to use a free Mobile Tracking
- Install and start to use your free trial
- Install and start to use commercial products

How to use free products

If you do not have a SafeFrontier Customer Account, you will first need to register. Once you have registered you can use a free trial of True Security™ Mobile products as described below:

1. Download the product you need
2. Install the product on your computer
3. Obtain your free license
4. Assign the license to your computer
5. Process reports from your computer

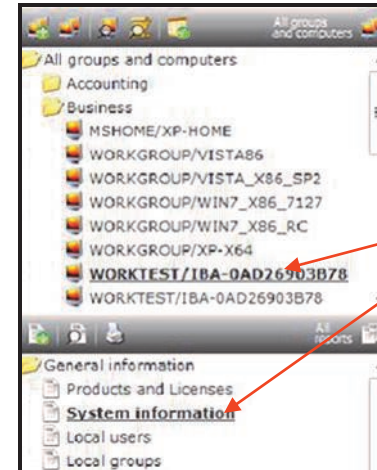


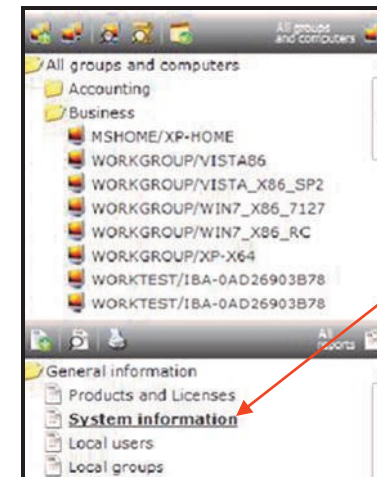
Figure 6.

Interact with Mobile Admin

Computer and Report is selected

The report from selected computer will be shown in the Main Window

To unselect click on the empty field.



The report is selected but no computer is selected

All reports of selected type will be shown from all computers

Installation

See **Appendix 1**.

How to use free trials

If you do not have a SafeFrontier Customer Account, you will first need to register. Once you have registered you can use your free trial of True Security™ Mobile products as described below:

1. Download the product you need
2. Install product the on your computer
3. Obtain your free trial license
4. Assign the license to your computer
5. Process reports from your computer

See **Appendix 2**.

How to use commercial products

If do not have a SafeFrontier Customer Account, you will first need to register. Once you have registered you can use your commercial True Security™ Mobile products as described below:

1. Download the product you need
2. Install the product on your computer
3. Order a new commercial license
4. Activate the newly ordered license
5. Assign the license to your computer
6. Process reports from your computer

See **Appendix 3**.

Installation

To install True Security™ Mobile products, use the following steps:

1. Download products
2. Obtain your installation key
3. Install products locally
4. Install products via Active Directory

Download products

Go to the "Download" Main Menu and select the product you wish to download.

Installation

Get your installation key

To install True Security™ Mobile products on your computers you will need an Installation Key.

If you download the installation package from your Mobile Admin console, the Installation Key (**key.txt** file) will be included in the package and will be applied automatically during the installation process. You will not be prompted to enter the Installation Key.

If you are not using the Mobile Admin console to download your installation package, you will need to place your Installation Key (**key.txt** file) in the same directory as the distributive package of the product you are installing.

When installation is completed the key will be removed from the target computer automatically for security reasons.

If you use Active Directory to centrally deploy your software the key must be placed to the same shared path as the distributive path.

Local installation

To install True Security™ Mobile products on a separate computer you need to

logon as a local administrator.

Run the install program setup.exe and follow the instructions. Please refer to Quick Start for more information.

When the installation is finished you will need to reboot your computer (the install program will do it automatically).

Remember!

Your new computer will be shown in the Computer List and available for administration only after it connects to the internet (the computer needs to send its activation notification during first internet connection). A new computer will be shown in the Computer List in green and will appear at the end of the list.

Centralized deployment

If you are using Active Directory, we provide a flexible mechanism to centrally deploy our products to all your computers automatically.

Download and extract the installation files to a separate folder. This folder should be available to your computers from the network (shared network folder).

Set the Group Policy to install the MSI-package for all computers on which you wish to install True Security™ Mobile products.

Installation

After the next reboot True Security™ Mobile products will be installed on these computers automatically with no user intervention.

Remember!

Your new computers will be shown in the Computer List and available for administration only after they connect to the internet (the computers need to send their activation notification during first internet connection).

Update or Uninstall

To update or uninstall True Security™ Mobile products use the following steps:

- Update products automatically
- Uninstall products locally
- Uninstall products via Active Directory

Update products

To ensure that you have current versions of True Security™ Mobile products running on your computers, set the Product update policy on all your computers to Automatic update.

Go to the General Mobile Security policy page and check the appropriate option in the "Products update" section. Then assign the policy to all your computers (this option is enabled by default on all new computers).

Local uninstall

To uninstall True Security™ Mobile products locally, logon to the computer as a local administrator and run the uninstall program from the computer Control Panel.

You can also uninstall True Security™ Mobile products directly from your Safe Frontier account. To do this, go to the General Mobile Security policy page (see **Figure 5 and 6**) and set the appropriate options in the "Remote products uninstall" section (see General Security policy, Products Install/Uninstall).

Remember!

If the General Mobile Security policy of your computer is set to Disable uninstall Mobile Security products and solutions, you will not be able to uninstall True Security™ Mobile products, until this option is switched off (see Control Computers, Self Protection)

Manage Licenses

Uninstall via Active Directory

To uninstall True Security™ Mobile products in the Active Directory environment set the uninstall Group Policy for all computers you wish to uninstall.

You can also uninstall True Security™ Mobile products directly from your SafeFrontier account . To do this, go to the General Mobile Security policy page and set the appropriate options in the "Remote products uninstall" section.

Remember!

If the General Mobile Security policy of your computer is set to **Disable uninstall Mobile Security products and solutions**, you will not be able to uninstall True Security™ Mobile products, until this option is switched off.

Manage licenses

This set of functions allows flexible and scalable license management and can be found in the Main Menu under the Licenses tab:

- Order new commercial licenses
- Activate newly ordered licenses
- Get your free trial licenses
- Get new free licenses

- Assign or update licenses to your computers
- Remove licenses from your computers

All licenses

This list shows all licenses in your account:

- Active licenses (licenses assigned, received, and applied on the computers)
- Empty licenses (licenses available in your account to be assigned to computers)
- Expiring licenses (licenses that will be expired within the next two weeks)

Each license can be one of the following types:

- Free license (license to use freeware)
- Trial license (an evaluation license for a 30 day free trial period)
- Commercial license (a paid license for use of the product during the specified license term)

You can sort your licenses using the header shortcuts above the license list.

To find specific licenses you can use the Find License form available from the Main Menu or from the Computer List Toolbar (see **Figure 3**).

Manage Licenses

Active licenses

This list contains only active licenses.

An active license has the following characteristics:

- The license has been sent, received, and confirmed by the target computer
- There are at least two weeks left until the end of the license term

All other licenses are not recognized as active. Each active license has a target computer. The computer name is shown in the Computer column of the license list.

Each active license includes an activation and expiration date. If the license was re-assigned from one computer to another, this license will include a re-assignment date.

Empty (available) licenses

This list contains all licenses available in your account that are available to be assigned to computers. The license is considered empty (available) in two cases:

- If the license has never been assigned (new license)
- If the license was removed from one computer and not re-assigned to another computer (Used or returned license)

All other licenses are not recognized as empty (available).

If the license is new, it has a full license term. If the license is returned, it has the license duration remaining from the computer from which it was removed.

Important!

Returned (used) licenses are not time tolled when removed from computers and **will continue to expire** even when not assigned.

Important!

Only NEW COMMERCIAL licenses are time tolled until assigned to computers and **will not expire**.

You can assign licenses of both of these types to all your computers.

Expiring licenses

This list contains all licenses that will expire in the next two weeks. If you have at least one expiring license, the appropriate notification will be shown in the Notification Area near Mobile Admin logo.

Once the license has expired it will be removed from your license list, and the computer will be marked as "a computer with expired license".

Manage Licenses

To avoid product deactivation you will need to assign a new license to any computer with an expired license. You can do this on the Assign or update licenses page by selecting an available license in your account. If you do not have an available product license you will need to order a new license and then update the license on the expired computer. You can also set the General mobile security policy for your computers to automatically search in your account and update expiring licenses.

Visit the SafeFrontier Online Store to learn more about license types, terms, and volume discounts.

Free licenses

This list contains all your freeware licenses. Free licenses are available for the following freeware products:

- True Security™ Mobile Tracking

SafeFrontier freeware products are commercial grade software products. You can obtain any number of freeware licenses you need and assign them to your computers. The Freeware license is issued for a term of one year. After the one year term expires you can obtain another free license and then update the appropriate computer. And so on.

SafeFrontier reserves the right to change the terms and conditions of its licenses at any time without prior notice.

Trial licenses

This list contains all your trial licenses. The Trial license has no functional limitations. These are the SafeFrontier products for which a trial (evaluation) license is available:

- True Security™ Mobile Defender
- True Security™ Mobile Audit

You can download a free trial license and then assign the license to your computer. The limitation for SafeFrontier trials is one license per product. If you need more trial licenses, please contact SafeFrontier support.

Each trial license has a 30 day license term. When your trial license is about to expire or if it has expired you will need to order a new commercial license for the product and then update the license on your computer.

Visit the SafeFrontier Online Store to learn more about license types, terms, and volume discounts.

Manage Licenses

Commercial licenses

This list contains all your commercial licenses.

Commercial licenses are available for the following SafeFrontier products:

- True Security™ Mobile Defender
- True Security™ Mobile Audit

If your commercial license is about to expire, or if it has expired you can order new license for the appropriate product and then update the license on your computer.

Visit the SafeFrontier Online Store to learn more about license types, terms, and volume discounts.

Get new free licenses

Free licenses are available for the following SafeFrontier freeware products:

- True Security™ Mobile Tracking



To obtain a new free license go to: **Maine Menu - Licenses - Get new free license.** Follow the instructions on the page.

Obtain a trial license

You can obtain one 30 day free trial (evaluation) license for each SafeFrontier product. If you need more trial licenses, please contact SafeFrontier support.

The Trial license has no functional limitations. The following are the SafeFrontier products with available trial licenses:

- True Security™ Mobile Defender
- True Security™ Mobile Audit



To obtain a Free Trial license go to: **Maine Menu - Licenses - Get your trial license.** Follow the instructions on the page.

Once you activate your free trial license you can assign the license to your computer.

Order new licenses

If you have new commercial SafeFrontier product installed, or if your trial or commercial license is about to expire, you can order new licenses.



To obtain a new commercial license go to: **Maine Menu - Licenses - Order new commercial license.** Follow the instructions on the

Manage Licenses

page.

Activate new licenses

To activate your licenses you need to provide the license key(s) that you received after placing your order.



To activate go to: **Main Menu - Licenses - Activate new ordered licenses.**

There are two options for entering license keys:

If you have received license keys in the License key file and wish to activate all these licenses at the same time, you can click Browse to find the License key file where you have saved it, click on the file and the file will be attached, then click Submit.

You can also enter manually (or copy/paste) any number of license keys into the text box provided and click the Submit button. If you enter license keys manually, please be sure that each key is entered on a separate line.

After you click the Submit button, the SafeFrontier License Server will process your keys. It may take some time, depending on the number of keys you have provided.

If a key is not found in the orders database, or a key has already been used, the appropriate message will be shown in the processing results. You can review the results and make the corrections. If any of your valid license keys are not recognized, please contact our support team.

Once you activate the new licenses, they will appear in the Empty (available) licenses list in your account (Main Menu - Licenses - List of licenses - Empty (available) licenses). You can now assign these licenses to your computers.

Assign or update licenses

To activate True Security™ Mobile products on your computers, you will need to assign new (or update expired) licenses.



To assign licenses go to: **Main Menu - Licenses - Assign or update licenses.**

There are two types of licenses available:

- New licenses (that were never assigned)
- Returned (used) licenses (that were removed from your other computers)

To assign licenses, select the product from the selection (drop-down) window (see **Figure 7**). From the Computer List in the left pane, select (check mark) the computer(s) or group(s) that you wish to assign licenses to and click on the avail-

Manage Licenses

able licenses.

To assign a single license to one computer select the computer in the Computer List first, and then click on the license you want to assign.

You can assign licenses to multiple computers (use check boxes in the Computer List to select computers you want to assign licenses to).

You can also re-assign a returned (used) license to a new computer.

All licenses are grouped by license terms. If you have several licenses with the same license term you can assign all licenses with a single click (see **Figure 7**).

Notes:

The check boxes in the Computer List are shown only when the group operations are available.

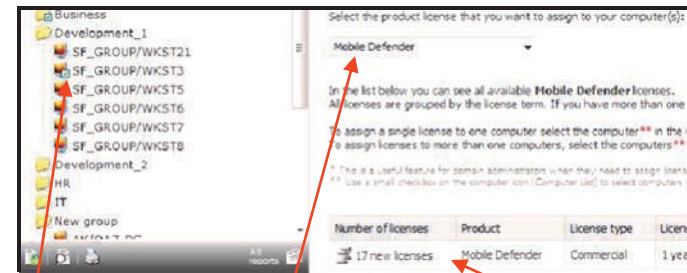
Remove licenses

If you have uninstalled one or more True Security™ Mobile products from your computer, all licenses for these products will returned to your account as Empty (available).

If you have uninstalled all True Security™ Mobile products, you will need to

Figure 7.

Assign Licenses



Checkboxes Selection Window Available Licenses

- 1. Select the product license in the Selection Window**
- 2. Select the computer(s) or a group by checking the boxes**
- 3. Click on the Available Licenses**

delete that computer from your account. To delete a computer, select the computer name in the Computer List and use the context menu (right click) to delete the computer (see **Figure 8**). You can also delete the computer from the Computer Summary page.

Control Computers

If you uninstall True Security™ Mobile products but there is at least one product still installed on the computer, then the licenses of uninstalled products will become available for reassignment automatically once that computer connects to the internet. If you uninstall all True Security™ Mobile products then the computer needs to be deleted from the account for licenses to become available for reassignment.

Remember!

In order for the licenses to return to your account the computer must connect to the internet after the uninstall.

Remember!

If you uninstall all True Security™ Mobile products from the target computer, you will need to delete the computer from your account in order for the licenses to become available for reassignment.

Control computers

This set of functions allows flexible and scalable computer management. Using these functions, you can do the following:

- Assign custom names to your computers
- Create new groups of computers
- Report a computer stolen or retrieved

- Assign policies to your computers
- View computer policy logs
- Create policy templates
- Remove computers from your account

All computers

This list contains all computers in your account. It includes:

- New computers (computers on which True Security™ Mobile product(s) is installed and pending license assignment)
- Active computers (computers with active True Security™ Mobile licenses)
- Non-active computers (computers with no or expired True Security™ Mobile licenses)
- Stolen computers (computers reported stolen and not yet retrieved)

To manage a computer click on the computer name (the Computer Summary page will appear). The Computer Summary page provides information about each computer in your account. You can sort your computers using the header shortcuts above the list.

To find computers you can also use the Find Computer form available from the Main Menu or from the Computer List toolbar (see **Figure 3**).

Control Computers

Active computers

This list contains active computers only. A computer will be included in this list if:

- The computer activation confirmation was received from the computer
- It has at least one active True Security™ Mobile license

If the computer has at least one True Security™ Mobile product with no license or an expired license, it will be include in the "Non-active computers" list.

Non-active computers

This list contains computers that have True Security™ Mobile products installed but their licenses have expired.

A computer will be included in this list if:

- It has at least one True Security™ Mobile product with no active license
- It has at least one True Security™ Mobile product with an expired license

To view which license has expired or which product is installed on the computer but has no license, click on the computer name and go to the Computer Summary page. This information will appear in the Licenses table on the Computer Summary page.

New activated computers

This list contains newly activated computers only. Once the software is installed on a computer and an internet connection is available, you will see a notification and the new computer will appear (in green) in your account at the end of the Computer List directory. A computer will be included in New activated computer list in three cases:

- If computer has True Security™ Mobile product(s) installed for the first time pending license assignment
- If computer has re-installed product(s) pending license assignment and was previously deleted from the account
- If the general computer information (such as computer or domain name, operating system, motherboard, etc.) was changed

In this list you will also find quick summary information about new computers. You can move these computers to appropriate groups (see **Figure 10**) and assign licenses as needed (see **Figure 7**).

Stolen computers

This list contains all computers reported stolen. You can report a computer sto-

Control Computers

len or retrieved from the Computer Summary page (see **Figure 15**). You can do this only if the computer has True Security™ Mobile Defender installed and the appropriate license assigned.

All stolen computers have a small red icon in the image and are highlighted red in the Computer List so you can quickly recognize these computers.

Customize your computers

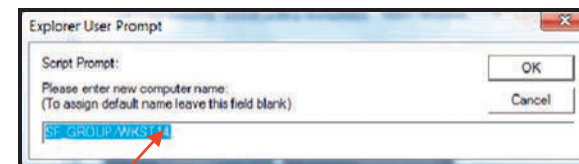
You can create custom names for all your computers in the account. To do this, go to the Computer Summary page and click the link with computer name. You can also rename your computer using the context (right-click) menu in the Computer List and choose Rename computer (see **Figure 8**) Enter the new computer name in the prompt window.

You can enter additional information about each computer in the custom data or pre-defined custom fields of the Computer Summary page. Create as many fields as you need, up to 4000 characters total. You can also search your computer data base using the custom fields parameters.

See **Figure 8**.

Figure 8.

Rename Computer



Control Computers

Groups of computers

You can organize your computers for group policy management and group report processing.

First, you need to create groups. To create a group, click the "Create new group" button on the control bar of your Computer List (see **Figure 3**). The prompt window appears. Enter a group name in the prompt window (see **Figure 9**).

Once your groups are created, you can move (drag-and-drop) your computers to the appropriate groups. You can do it right in the Computer List window (it can be stretched wider by dragging the right and lower edges) or you can use the Main Window.

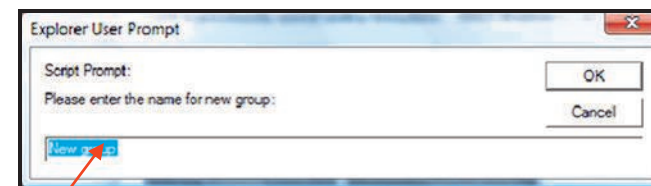
To move multiple computers, click the "Manage groups and computers" button on the Computer List Toolbar (see **Figure 3**). The Computer List will be moved to the Main Window, and the checkboxes will be shown to the right of the computer or group icon. To move multiple computers, check the boxes of each computer or the entire group(s) that you want to move and drag one of the selected computers into the target folder. All the selected computers will be moved to that folder (see **Figure 10**).

You can assign group policy for groups or for separate computers. You can also find and process reports by groups.

At any time you can change the group name, and add or remove groups by point-

Figure 9.

Rename Group



Enter custom group name in the prompt window

ing the cursor on the group name and using the right-click context menu. When you remove a group, all computers of this group will be moved to the root group "All computers".

Computer Summary

The Computer Summary is the main page of each computer. You can view all important information about a computer on this page.

Open the Computer Summary page by clicking on the computer name in the Computer List. You can also open this page from other lists: reports, licenses, or

Control Computers

policies by clicking on the computer name link.

Load new reports from the current computer by clicking the Load new reports button. You can also load new reports from the selected computer using the right-click context menu and choosing Load new reports (see **Figure 8**).

If your computer has a valid Mobile Defender license, you can report the computer stolen or retrieved by clicking the “Report computer stolen” or “Report computer retrieved” buttons (see **Figure 15**).

You can remove computer from your account by clicking Delete computer button. All messages from this computer will be ignored and reports will be removed from the account. All active licenses will be returned into your account. You should also remove the product software from that computer.

To view all policies sent to the computer, click the Computer policies log button. You will see all the polices that were sent to that computer. To view the actual configuration of the computer, click on the Policy summary button.

The **Summary** section provides information you can use to identify your computer, such as: computer and domain name, motherboard ID, asset tag number, MAC address, etc.

The Custom fields section allows you to specify and store unique information about the computer, such as: user name, lease and warranty parameters, lifecycle data, etc. This is a very useful feature for Inventory Management purposes. You can create as many fields as necessary up to 4000 characters total. You can

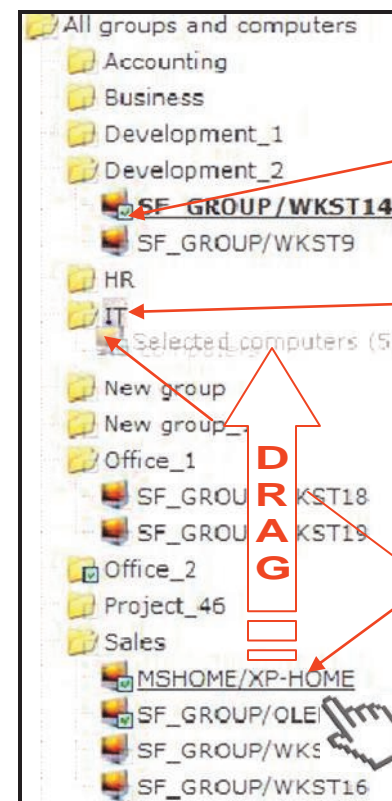


Figure 10.

Manage Groups and Computers

1. Select computers to be moved (or entire group)
2. Choose the group where computers are to be placed (target folder)
3. Point the cursor on anyone of selected computers
4. Drag computers into the target folder (it will be highlighted)
5. Confirm the operation

Control Computers

search your computers according to this data.

The **Active licenses** table includes all valid licenses issued to your computer and license parameters.

The **Current policies** table provides quick access to all current policies assigned to your computer.

The **Pending policies** table shows all policies sent but not yet received by the computer.

The **Reports** table includes all reports received from your computer. You can open any report in a new window by clicking the appropriate icon near the report name link. You can view the actual configuration and the configuration changes over time.

Assign policy to computer

All computers with True Security™ Mobile products installed have a default policy for each product. You can view these policies from the drop-down menu "All policies" on the control bar.



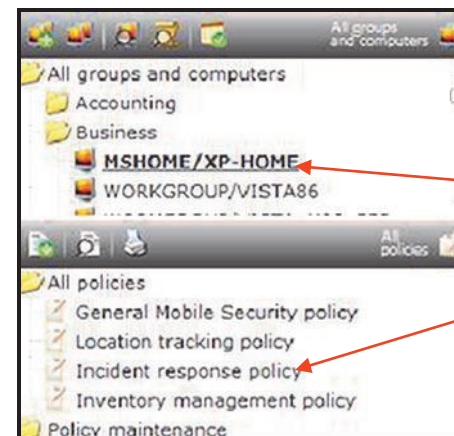
Reports and Policy List - Report and Policy List Toolbar - All Reports - All Policies

To view current computer policies, select the computer in the Computer List and then choose a policy from the Report and Policy List (see **Figure 11**). You can edit the policy and assign it to any computer(s) or group(s) of computers. You can also save the policy as a template or modify an existing template.

To assign a policy to multiple computers or groups of computers, check the checkboxes of these computers or groups in the Computer List. Then select the appropriate option at the bottom of the page and click the Send button (see **Fig-**

Figure 11.

Open Computer Policy



1. Select a Computer

2. Choose a policy

Control Computers

ure 12).

Notes:

The check boxes in the Computer List are shown only when the group operations are available.

Policy templates

Policy template is a previously saved policy that can be applied when assigning policy to computers or groups. You can select a previously saved policy from the drop-down policy template list (see **Figure 12**).

You can create a new template or modify an existing template by editing the template first, and then saving it accordingly. You can assign a new name to a policy or choose the existing policy you wish to modify from the drop-down menu. (see **Figure 12, step 2**)

To manage policies, go to the Manage policy templates page where you can view, delete, or rename policy templates.



Reports and Policy List - Report and Policy List Toolbar - All Reports - All Policies - Policy Maintenance - Manage Policy Templates

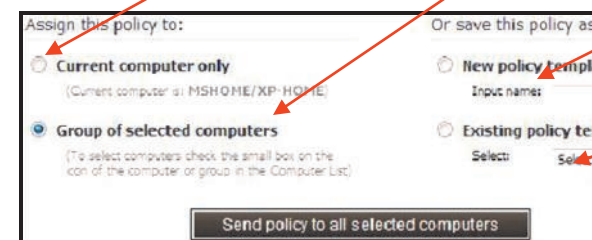
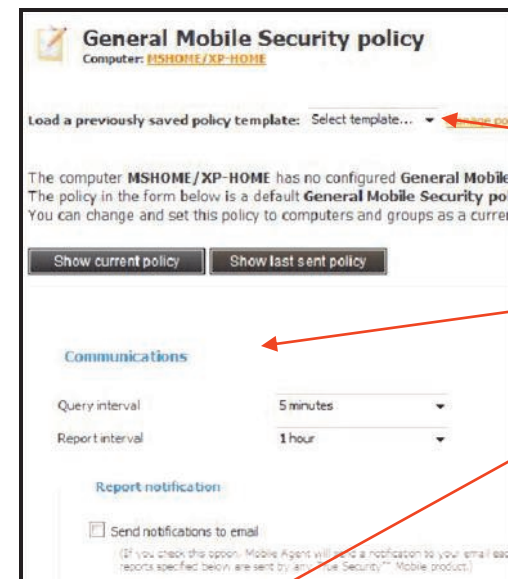


Figure 12.

Manage Computer Policy

1. Choose a previously saved policy template

Or edit the policy

2. Assign policy to a currently selected computer

Or a group (use checkboxes to select)

Or save it as a template

Or modify an existing template

Control Computers

Pending policies

Pending policies are policies that were sent but not yet received by the target computer. If the policy is pending it may be because the target computer is not connected to the internet. As soon as it connects, it will receive the policy and notify the Admin Console that the policy was applied successfully. You can see what policies are pending on all computers or on a single computer in the View pending policies page. To view all pending policies from all computers go to:



Reports and Policy List - Report and Policy List Toolbar - All Reports - All Policies - Policy Maintenance - View pending policies

For an individual computer, click on the computer name in the Computer List window and select View pending policies in the Report and policy list. You can also see what policies are pending on the Computer Summary page in the Pending policies section or use computer policy log to see what policies are pending (Computer policy log button located on the Computer Summary page). Pending policies by type can also be viewed on each individual policy page of a computer.

Important!

Even when the target computer is connected to the internet, it may take a while for the computer to receive a policy, depending on the settings you use (Quarry interval setting in the General Mobile Security policy). It will also depend on the network load and other parameters. It may take up to an hour for a target com-

puter to receive a new policy but usually it takes just a few minutes after the internet connection is available. A computer may receive a policy but may not be able to confirm it if for example, it has been disconnected from the internet or switched off. The computer will attempt to confirm the policy again once the internet is available. You must also make sure that the product license on the target computer is valid.

General Mobile Security policy

This policy regulates the main functionality and security aspects of all True Security™ Mobile products installed on the target computer.

The General Mobile Security policy consists of the following sections:

- Communications
- Self-protection
- Disable products and components
- Licensing
- Products update
- Products install/uninstall
- Troubleshoot

You can assign this policy to the current computer only, or to all computers selected in the Computer List.

Control Computers

Communications

This section contains the main communications parameters for all True Security™ Mobile products installed on the computer.

Query interval

This parameter regulates how often the software on the target computer will check incoming commands and settings. We recommend a 15 minute interval.

Report interval

This parameter regulates how often True Security™ Mobile products will send reports. You can specify this parameter for each product separately in the appropriate policy. The General Mobile Security policy report interval will govern only the reports under the section General Information. The Intervals for other reports are set in the appropriate policies.

Report notification

This feature allows you to receive notifications when all or selected reports are sent from the target computer. If the "Send notifications to email" option is enabled, notifications will be sent to the specified email address every time a report is sent from the target computer.

Update current configuration

When this option is enabled the reports sent from the target computer will show the Actual Configuration of the systems and settings of the monitored computer at the time reports were compiled. Once the reports are received, all old reports

and configuration changes will be REMOVED from the account. In the report window you can select all reports, or select specific reports.

Self-protection

This section allows you to restrict computer users from removal of True Security™ Mobile products.

Enable uninstall products

This feature allows you to protect monitored computers from unauthorized de-installation of True Security™ Mobile products. If this parameter is **disabled**, uninstall of True Security™ Mobile products can not be performed by local administrator on a target computer. Only the domain administrator will be able to uninstall products remotely. If this option is enabled, both local and domain administrators will be able to uninstall True Security™ Mobile products. Uninstalling products remotely from your Mobile Admin console is allowed regardless of this setting.

Remember!

You will not be able to uninstall True Security™ Mobile products if computer is reported "stolen".

Control Computers

Disable products

This section allows you to disable some or all True Security™ Mobile products installed on your computer.

To disable a product check the appropriate checkbox.

This feature is used to disable Mobile Security products and components. It is useful when a computer is lost or stolen, and you want to minimize internet activity to only obtain information important for computer recovery.

Licensing

This section regulates updates of the expiring True Security™ Mobile licenses on your monitored computers.

If you have New or Used licenses available in your account, and if the current license of the specified product is about to expire, the computer will receive a new license automatically without product deactivation. If this option is disabled, the product will be deactivated when the license expires.

Remember!

When the True Security™ Mobile license for the specified product is about to

expire you will receive a notification in your Mobile Admin console and can manually assign a new license to your computer.

Notes:

We recommend that you enable this option for all True Security™ Mobile products installed on your computer.

Products update

This section regulates automatic updating of True Security™ Mobile products.

Update products automatically

If this option is enabled, all True Security™ Mobile products installed on your computer will be automatically updated to the latest software version available.

Update interval

This parameter regulates how often the target computer will check for new available software versions.

Notes:

We recommend that you enable this option and set the update interval to 1 day, so your True Security™ Mobile products will always be up to date.

Control Computers

Products install/uninstall

This section allows you to install and uninstall True Security™ Mobile products remotely from your Mobile Admin console.

This may be useful if your computer is out your custody and you cannot access it . You will be able to do this remotely via the Internet.

If your computer has a specified product installed, the appropriate "Uninstall" option will be available. If one of the products is not installed, the "Install" option will be available.

Remember!

If you have uninstalled all True Security™ Mobile products from your computer, you will need to reinstall at least one of them locally or via Active Directory to be able to use this feature.

Troubleshoot

Troubleshoot is designed to assist in resolving any operating issues you may experience using True Security™ Mobile products. When activated, it troubleshoots the software and sends recorded data to the email address specified in the policy. You can forward this data to our support team,

support@safefrontier.com, so we can provide quick and efficient assistance in resolving the issue.

Location Tracking policy

This policy regulates the location tracking functionality of True Security™ Mobile products installed on your computer. The following sections are available in this policy:

- Communications
- Location tracking
- Image capturing

You can assign this policy to the current computer only, or to all computers selected in the Computer List.

Communications

This section contains reporting frequency parameters.

Report interval

This parameter regulates how often computer sends new reports. We recommend an interval from 30 minutes to 1 day.

Control Computers

Notes:

If Mobile Defender is installed on your computer, and your computer is stolen, the report interval can be as little as 5 minutes.

Location tracking policy

This section allows you to activate alternative tracking systems if they are installed on the target computer.

Enable GPS location tracking

If a GPS device is installed or temporarily attached to the monitored computer, you can enable this option to receive the GPS data of your computer location.

Enable GSM location tracking

If a GSM device (modem, cell-phone) is installed or temporarily attached to your computer, you can enable this option to receive the GSM data of your computer location.

Important!

Not all GPS and GSM devices are supported. For more information, contact SafeFrontier support.

Image capturing

If your computer is equipped with a built in or removable video camera, the True Security™ Image Capturing utility will allow you to covertly take pictures of the person using your computer.

An image will be taken every time computer is switched on or wakes up from the sleep mode, or a new location tracking report is generated.

Images will be delivered in the password protected archive to the user-specified email address.

You can set this feature in the Location Tracking policy.

Incident Response policy

This policy regulates the incident response functionality of True Security™ Mobile products installed on the monitored computer. This policy consists of the following sections:

- Communications
- "Stolen" policy
- "No connection" policy

You can assign this policy to the current computer only or to all computers se-

Control Computers

lected in the Computer List.

Communications

This section contains parameters for reporting when incident response actions are performed on the target computer.

Report interval

This parameter regulates how often the monitored computer sends a new report on incident response actions performed. We recommend an interval from 5 to 30 minutes.

Notes:

If Mobile Defender is installed on your computer, and your computer is reported stolen, a five minutes report interval will be set automatically.

"Stolen" policy

This section allows you to set incident response actions if your computer is lost or stolen.

Remember!

Figure 13.

Program Execution



Example.

This setting will allow you to perform the following on the stolen computer:

1. Kill all active programs except Internet Explorer
2. Start Internet Explorer and display a preset webpage
3. The actions will be repeated every one minute until policy is changed or computer reported "retrieved"

All these actions will be executed on your computer only after it is reported stolen. Once it is reported retrieved, Mobile Defender will stop performing incident response actions on the target computer.

Control Computers

Computer shutdown

If this option is checked, Mobile Defender will shut down a stolen computer immediately when the computer is turned on.

Warning messaging

If this option is checked, Mobile Defender will show a specified warning message on your computer every time the computer is turned on.

Program execution

Program Execution allows you to launch programs remotely. Programs such as: Disk or File Encryption, Data Backup, Computer Maintenance or Diagnostic Utilities, or any other application of your choice.

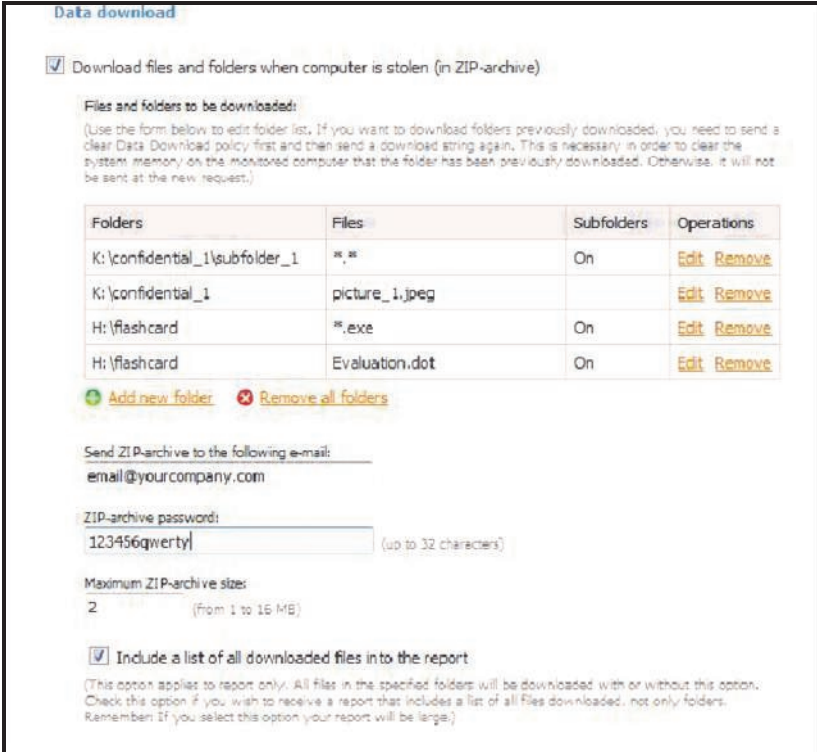
Programs can be executed with user or system privileges. If you launch a program with system privileges, the program will have access to program files and computer register but will not have access to user files and desktop. With user privileges the program will have access to user files and desktop but will not have access to program files and computer register. Programs can be launched with different execution parameters. You can edit, add, and remove programs and parameters (see **Figure 13**).

Data download

This feature allows you to download any files from your lost or stolen computer to a specified email address. It also includes downloading files stored on the removable media attached to the computer. Files are emailed in ZIP-archive. You can specify the email address, ZIP-archive password and maximum ZIP-archive

Figure 14.

Data Download



Data download

Download files and folders when computer is stolen (in ZIP-archive)

Files and folders to be downloaded:
(Use the form below to edit folder list. If you want to download folders previously downloaded, you need to send a clear Data Download policy first and then send a download string again. This is necessary in order to clear the system memory on the monitored computer that the folder has been previously downloaded. Otherwise, it will not be sent at the new request.)

| Folders | Files | Subfolders | Operations |
|-------------------------------|----------------|------------|---|
| K:\confidential_1\subfolder_1 | *.* | On | Edit Remove |
| K:\confidential_1 | picture_1.jpeg | | Edit Remove |
| H:\flashcard | *.exe | On | Edit Remove |
| H:\flashcard | Evaluation.dot | On | Edit Remove |

[Add new folder](#) [Remove all folders](#)

Send ZIP-archive to the following e-mail:
 email@yourcompany.com

ZIP-archive password:
 123456qwerty (up to 32 characters)

Maximum ZIP-archive size:
 2 (from 1 to 16 MB)

Include a list of all downloaded files into the report
(This option applies to report only. All files in the specified folders will be downloaded with or without this option. Check this option if you wish to receive a report that includes a list of all files downloaded, not only folders. Remember if you select this option your report will be large.)

Example.

Control Computers

size. If the selected files are larger in size than the maximum ZIP-archive size specified, more than one archive will be emailed in separate messages.

To download multiple files from different locations you need to list the folders and file masks to be downloaded.

You will receive a report once the "Data download" action is executed. This report includes a list of sent folders. If you would like the report to include a list of all emailed files (not only folders), check the "Include a file list" in the report option.

See **Figure 14**.

Data delete

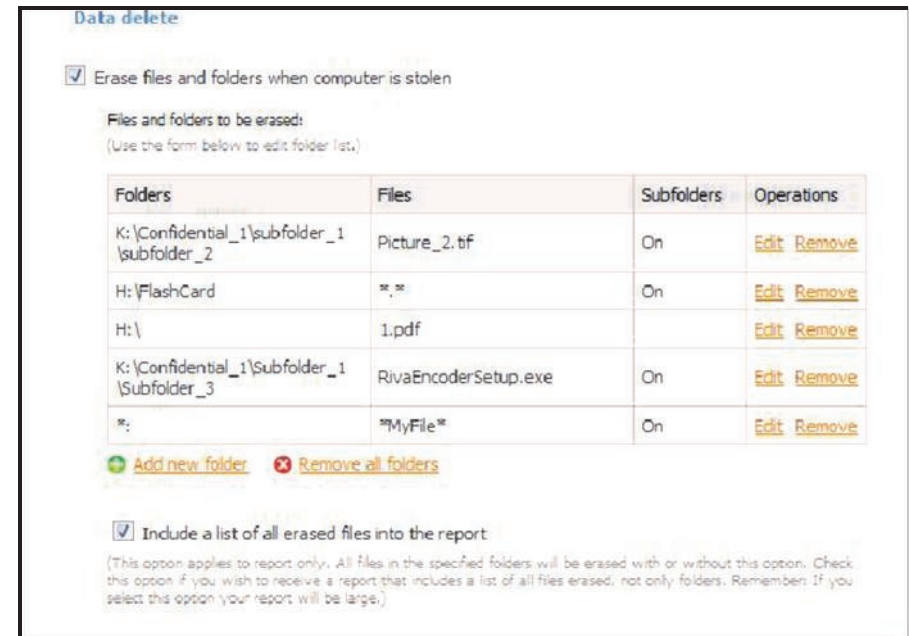
This feature allows you to erase any files and folders on your lost or stolen computer to the US Department of Defense specification for data sanitization.

To erase multiple files from different locations including attached removable media, you need to provide a list of the folders and file masks to be erased (see **Figure 15**). You can use standard syntax to indicate folders and files. For example, if you don't know the particular location of the file but you know the drive, one word of the file name, and file extension, you can input "c:\ for folders and for files *MyFile*.dot, and enable the flag Include subfolders. If you don't know the drive, you can enter "*" for folders - all local drives, etc. (see **Figure 15**).

You will receive a report once the "Data delete" action is executed. This report includes a list of deleted folders. If you would like the report to include a list of

Figure 15.

Data Delete



Data delete

Erase files and folders when computer is stolen

Files and folders to be erased:
(Use the form below to edit folder list.)

| Folders | Files | Subfolders | Operations |
|---|----------------------|------------|---|
| K:\Confidential_1\subfolder_1 \subfolder_2 | Picture_2.tif | On | Edit Remove |
| H:\FlashCard | *.* | On | Edit Remove |
| H:\ | 1.pdf | | Edit Remove |
| K:\Confidential_1\Subfolder_1 \Subfolder_3 | RivaEncoderSetup.exe | On | Edit Remove |
| * | *MyFile* | On | Edit Remove |

[Add new folder](#) [Remove all folders](#)

Include a list of all erased files into the report
(This option applies to report only. All files in the specified folders will be erased with or without this option. Check this option if you wish to receive a report that includes a list of all files erased, not only folders. Remember: If you select this option your report will be large.)

Example.

Control Computers

all erased files (not only folders), check the “Include a file list” in the report option.

Remember!

If you have the "Data delete" feature enabled and report a computer “stolen”, all the specified files will be erased completely WITHOUT THE POSSIBILITY OF RECOVERY.

Reports copy

When this option is checked and you report the computer “stolen”, all selected reports will be copied to the specified email. Reports will be ZIP-archived, and you can assign an access password. You can select one or more reports from the report list.

"No connection" policy

This section allows you to set incident response actions if your computer has no access to the internet.

"No connection" timeout

This parameter regulates how long your computer can be without access to the internet before it initiates incident response actions. When the set time lapses, the specified actions will be executed.

Computer shutdown

If this option is checked, Mobile Defender will shutdown the computer immediately after the "No connection" timeout has expired. It will also prevent the computer from starting until the network is available.

Program execution

Program Execution allows you to launch programs as a "no connect" incident response. Programs such as: Disk or File Encryption, or any other application of your choice.

Programs can be executed with user or system privileges. If you launch a program with system privileges, the program will have access to program files and computer register but will not have access to user files and desktop. With user privileges the program will have access to user files and desktop but will not have access to program files and computer register. Programs can be launched with different execution parameters. You can edit, add, and remove programs and parameters (see **Figure 13**).

Data delete

This feature allows you to erase (see **Appendix 4**) any files and folders on your computer if the period it has no access to the internet exceeds the specified "No connection" timeout period.

To erase multiple files from different locations you need to provide a list of folders and file masks to be erased (see **Figure 15**), also see “Stolen” policy, Data delete for more information.

Control Computers

You will receive a report once the "Data delete" action is executed. This report includes the erased folders list. If you would like the report to include a list of all erased files (not only folders), check the "Include a file list" in the report option.

Remember!

If you have the "Data delete" feature enabled and report a computer "stolen", all the specified files will be erased completely **WITHOUT THE POSSIBILITY OF RECOVERY**.

Allow local user to disable "No connection" actions

When this option is enabled the local user will be allowed to disable "No connection" incident response actions by entering a password in the dialog window that will be displayed for one minute before the incident response actions are executed. You can set the password in your account in the "No connection" policy. This is very useful when you need to protect your computer even when an internet connection is unavailable.

If the computer is lost or stolen and an internet connection is unavailable, the incident response actions will be performed regardless. Only the legitimate user will be able to locally abort the "No connection" incident response by entering a correct password.

Inventory Management policy

This policy regulates the inventory management functionality of True Security™ Mobile products. The following sections are available in this policy:

- Communications
- System audit policy
- Event logging policy

You can assign this policy to the current computer only, or to all computers selected in the Computer List.

Communications

This section contains parameters of reporting frequency.

Report interval

This parameter regulates how often Inventory Management reports are sent from monitored computers. We recommend an interval from 1 to 7 days.

System audit policy

Control Computers

This section contains parameters that regulate the system audit policy of the monitored computer.

Enable system audit

If this option is enabled, the operating system audit on the monitored computer will be activated and specified audit events will be tracked.

Audit categories

You can specify what kind of events you want to track.

Notes:

We recommend that you enable the failure audit only for the following events: "Logon events", "Policy change", "Account management" and "Account logon events" in order to reduce the internet traffic and processor load of the monitored computer as these reports may be very large.

Event logging policy

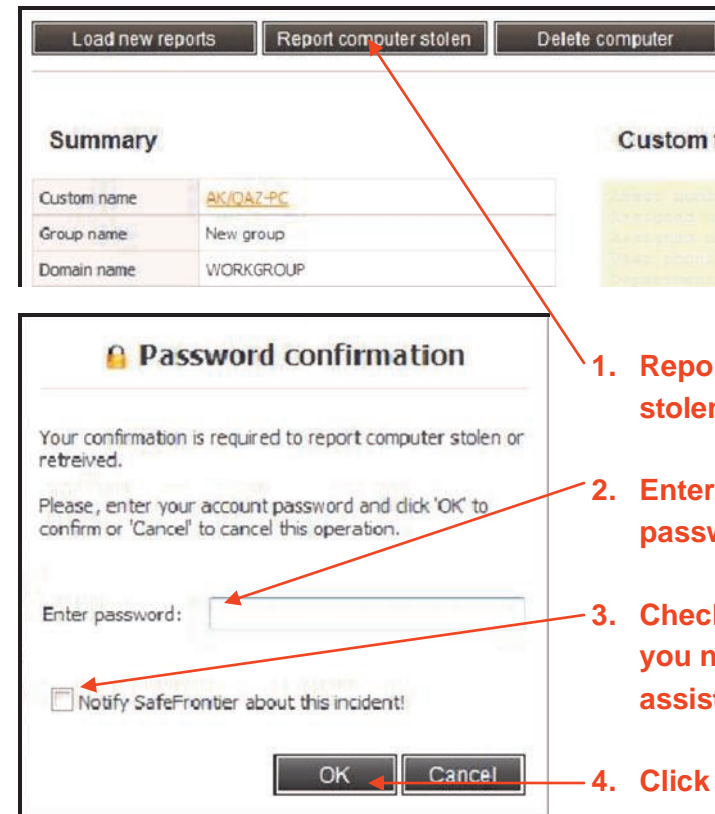
This section contains parameters that regulate the event logging policy.

Enable event logging

If this option is enabled, True Security™ Mobile products will track events on the monitored computer, and will deliver the specified event logs.

Figure 16.

Report Computer Stolen



The screenshot shows a web interface with three buttons at the top: "Load new reports", "Report computer stolen", and "Delete computer". Below these is a "Summary" section with a table:

| | |
|-------------|-----------|
| Custom name | AK/QAZ-PC |
| Group name | New group |
| Domain name | WORKGROUP |

Below the table is a "Password confirmation" dialog box. The dialog box contains the following text and elements:

Password confirmation

Your confirmation is required to report computer stolen or retrieved.

Please, enter your account password and click 'OK' to confirm or 'Cancel' to cancel this operation.

Enter password:

Notify SafeFrontier about this incident!

At the bottom of the dialog box are "OK" and "Cancel" buttons.

Four red arrows point to specific elements in the dialog box, labeled 1 through 4:

1. Report computer stolen (points to the "Report computer stolen" button)
2. Enter the account password (points to the password input field)
3. Check the box if you need recovery assistance (points to the "Notify SafeFrontier about this incident!" checkbox)
4. Click OK (points to the "OK" button)

Control Computers

Audit sections

You can specify which event logs you want to receive. For example: Application; System; Security. If you want to receive all event logs, use * only.

Audit events

You can specify what kind of events (errors, warnings, etc.) you want to track and receive.

Notes:

We recommend that you enable only "Critical", "Error" and "Warning" events for optimum computer performance and internet traffic use.

Report computer stolen / retrieved

If you have True Security™ Mobile Defender installed on your computer, and you report computer stolen, Mobile Defender will then execute the "Stolen policy" on this computer.

Select the computer by clicking on the computer name in the Computer List and then press the "Report computer stolen / retrieved" button located in the upper left corner of the Computer Summary page (see **Figure 16**).

When your computer is recovered, report it "Retrieved" in your account, and Mobile Defender will stop executing "Stolen policy" actions.

To report a computer stolen or retrieved, go to the Computer Summary page and click the Report computer stolen or Report computer retrieved button at the top of the page. You will need to enter your account password. If you would like SafeFrontier to provide additional assistance with recovering your computer, check the Notify SafeFrontier box. Once we receive your message, we will provide further instructions on the recovery process.

Notes:

In order to provide additional assistance recovering a stolen computer, we will require a copy of the police report. Also note that these services are regional. Contact SafeFrontier support for additional information.

View policy log

All policy management activities are logged in to the Computer policies log. You can access the policy log of individual computer from the Computer Summary page.

You can also view the policy log by the type of policy. When you access the log from the individual policy page, the appropriate policy log will be available to view. The page will display current computer policies and pending policies (last sent and not yet received by the target computer).

Control Computers

Computer policies log

This list shows a log of all policies sent to your computer. Open a specified policy by clicking on the policy name link. You can sort policies by clicking on the header of the list.

The Policy Type field shows what type of policy was sent (e.g. full policy or separate command, such as: stolen, retrieved). The Sent and Received dates show when the policy was sent and received by the target computer. If the policy is not received yet, the Operations field will contain a Pending sign.

If the policy is not received by the computer, the Received Date field will contain a "Confirmation pending" string.

Remove computer

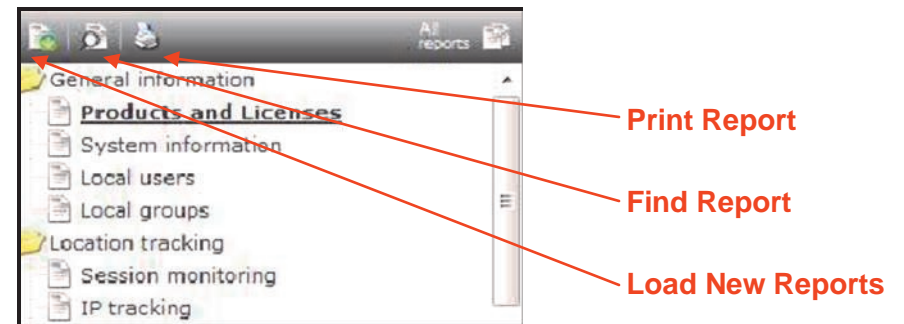
If you have uninstalled all True Security™ Mobile products from a target computer, because it is damaged or otherwise not in use, you can remove this computer from your account.

Select the computer in the Computer List and use the context (right-click) menu (see **Figure 8**), or uninstall it from the Computer Summary page.

After your computer is removed, all valid licenses from this computer will be returned to your account and all reports will be DELETED. You can re-assign the used licenses to your other computers.

Figure 17.

Computer and Policy List Controls



Process reports

Process reports

This set of operations enables you to view and manage reports. You can do the following:

- Load new reports
- Remove reports
- Clear configuration changes
- View report lists
- View reports
- Find reports

All reports

This list contains all reports including:

- All reports from all your computers
- New reports (reports received from your computers and not yet viewed)
- Groups of reports (reports grouped by product or in problem-oriented groups)

To view a specific report click on the report name (you can also view most of the reports in a new window). You can sort your reports using the header shortcuts

above the list.

To find a specific report you can use the Find Report form available from the Main Menu or from the Reports and Policy List (see **Figure 17**).

New reports

This list contains new reports only. A report is marked new if it is not yet viewed, e.g. if you have never opened this report. When you open the report, it will be unmarked automatically.

Load new reports

To fast load new reports from all your computers click the "Load new reports" button on the Report and Policy List Toolbar (see **Figure 16**) or use the **Main Menu - Reports - Load new reports** command.

To load new reports from a single computer click the appropriate button at the top of the Computer Summary page or use the context (right-click) menu of the Computer List Toolbar (see **Figure 8**).

To load new reports from a specified group of computers use the context (right-click) menu of this group.

Process reports

Once the new reports are loaded, the "New reports" page will be shown, and you will be able to view and manage your new reports. The Computer Summary page will be shown if you are loading reports from a single computer.

View report lists

You can view the report list from all your computers by selecting the appropriate command from the "Reports" option in the Main Menu.

To view reports from a specified computer, go to the Computer Summary page and scroll down to the "Reports" table. You can also, select this computer in the Computer List and then select the report in the Report and Policy List.

You can view a report in the new window by clicking the "New window" button on the report viewing page, or the appropriate link in the report lists.

All reports are grouped in problem-oriented sections:

- General Information
- Location Tracking
- Incident Response
- Inventory Management
- Compliance Monitoring

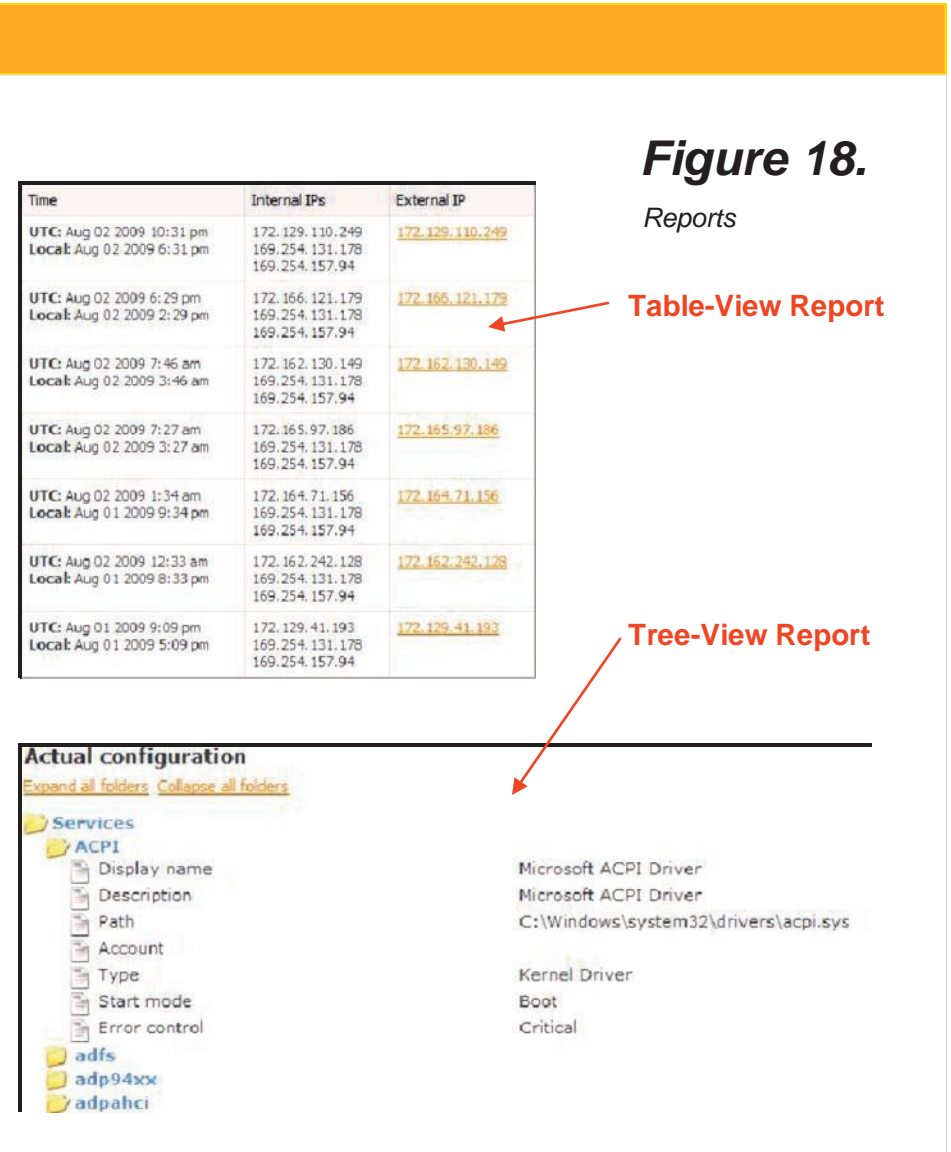


Figure 18.
Reports

Table-View Report

| Time | Internal IPs | External IP |
|---|--|---------------------------------|
| UTC: Aug 02 2009 10:31 pm Local: Aug 02 2009 6:31 pm | 172.129.110.249 169.254.131.178 169.254.157.94 | 172.129.110.249 |
| UTC: Aug 02 2009 6:29 pm Local: Aug 02 2009 2:29 pm | 172.166.121.179 169.254.131.178 169.254.157.94 | 172.166.121.179 |
| UTC: Aug 02 2009 7:46 am Local: Aug 02 2009 3:46 am | 172.162.130.149 169.254.131.178 169.254.157.94 | 172.162.130.149 |
| UTC: Aug 02 2009 7:27 am Local: Aug 02 2009 3:27 am | 172.165.97.186 169.254.131.178 169.254.157.94 | 172.165.97.186 |
| UTC: Aug 02 2009 1:34 am Local: Aug 01 2009 9:34 pm | 172.164.71.156 169.254.131.178 169.254.157.94 | 172.164.71.156 |
| UTC: Aug 02 2009 12:33 am Local: Aug 01 2009 8:33 pm | 172.162.242.128 169.254.131.178 169.254.157.94 | 172.162.242.128 |
| UTC: Aug 01 2009 9:09 pm Local: Aug 01 2009 5:09 pm | 172.129.41.193 169.254.131.178 169.254.157.94 | 172.129.41.193 |

Tree-View Report

Actual configuration
Expand all folders Collapse all folders

- Services
 - ACPI
 - Display name: Microsoft ACPI Driver
 - Description: Microsoft ACPI Driver
 - Path: C:\Windows\system32\drivers\acpi.sys
 - Account:
 - Type: Kernel Driver
 - Start mode: Boot
 - Error control: Critical
 - adfs
 - adp94xx
 - adpahci

Process reports

View reports

To view a specific report from computer, select the computer in the Computer List and then select the report in the Report and Policy List. If you select a report and do not select a specific computer, all reports of this type from all computers will be shown.

When viewing reports, you can perform the following operations by clicking the appropriate buttons at the top of the report page:

- Open report in new window
- Save report to file
- Print report
- Remove report
- Search in report

Each report has its last modified date, which is the date when the latest update was received. This date is shown at the top of the report page.

There are two different types of report views (see **Figure 18**):

- Tree-view reports
- Table-view reports

Tree-view reports

This type of report groups all data to tree-like folders and parameters (see **Figure 18**).

You can expand folders and sub-folders by clicking on the folder name link. You can also expand and collapse all folders and subfolders by clicking on the Expand or Collapse links.

Most of the reports also show changes that accrued on the monitored computer. This means that the information has changed on the monitored computer, and the new report contains the updated information. In this case the Configuration changes link will be available. If you are viewing configuration changes, each changed folder or parameter will be marked as follows:

- Changed
- Added
- Removed

All configuration changes are grouped by date so you can see what accrued within a specified folder or parameter and when.

To return to the Actual configuration use the appropriate link. The actual configuration contains synchronized data that shows you the actual (latest) state of the information on the monitored computer.

Process reports

Table-view reports

This type of report provides information as a grid (see **Figure 18**).

Each record (row) of the grid has the date when this record was created so you can track the changes of the specified parameter. Some reports may contain links to other reports or external links to other resources. These links will usually open in a new window.

If the report contains many records, a navigation pager will be shown at the top and bottom of the grid.

General information

This section includes the following reports:

- Computer summary
- Products and Licenses
- System information
- Local users
- Local groups

Products and Licenses

This report contains information about all True Security™ Mobile products and licenses installed and activated on the target computer.

System Information

This report contains general computer system information . It includes:

- Operating system installed
- Physical memory
- BIOS information
- Logical drives information

Local Users

This report contains information about all users registered on the monitored computer and other essential parameters.

Process reports

Local Groups

This report contains information about all groups of users registered on the monitored computer and other essential parameters.

Location tracking

This section includes the following reports:

- Session monitoring
- IP tracking
- Wi-Fi tracking
- GPS tracking
- GSM tracking

Session Monitoring

This report contains information about all user sessions started on the monitored computer. Each record (row) provides information indicating when the session was started and who started the session.

Important!

If the report is compiled after computer start but prior to user logon, the 'User' box in the report will be empty.

IP Tracking

This report contains information about all changes of IP addresses of the target computer.

Each record (row) provides information indicating when the address was changed and a list of all external and internal IP addresses that were registered on the computer at that time. If the external and internal IP address is indicated in the report, you can track the target computer using these addresses.

Click the link and view the WHOIS database to obtain the Internet Service Provider (ISP) contact information. You can contact the ISP and provide the information received in this report. It may greatly expedite the recovery process if the computer is lost or stolen.

Wi-Fi Tracking

This report contains information about all your computer connections to Wi-Fi

Process reports

access points.

The **Current network** folder contains the last network your computer connected to.

The **Available networks** folder includes information about all networks registered by the computer.

If the access point is registered on Google Maps, you can view the location of your computer by clicking the appropriate link at the bottom of this report.

GPS Tracking

If the monitored computer has a GPS receiver installed or connected to it, this report will provide location information from the GPS receiver.

Each record (row) provides location data you can use to track your computer. This information is essential for the recovery of a lost or stolen computer. You can see the precise location of the monitored computer on the map by clicking the View map link (the Google Maps will be shown).

GSM Tracking

If your computer has a connected or built in GSM device (cellular modem or cell-phone) , this report will contain all the information received from the GSM module connected to your computer.

Each record (row) contains information that will help track the monitored computer and provides important details about the GSM module that can significantly expedite the recovery of a lost or stolen computer.

- Time (UTC, Local)
- Roaming
- Signal (Level, Quality)
- Phone number
- Operator (Name, Code)
- Local Area Code (LAC of the tower)
- Cell ID (Tower ID)
- GSM module information

In the event of computer theft, law enforcement can quickly identify not only the location of a stolen computer but also obtain accurate information about the GSM module owner.

Important!

Not all GSM modules (telephones/modems) are supported. Contact SafeFrontier support for more information.

Process reports

Incident response

This section includes the following reports:

- All response results
- Computer shutdown
- Warning messaging
- Program execution
- Remote data delete
- Remote data download

All response results

This report provides information about the results of the executed incident response, if the computer was reported stolen or did not connect to the internet within specified time.

Each record (row) indicates a cause for the action performed and an outcome of the action. The cause of the action may be as follows:

- **Stolen** - if your computer is reported stolen
- **No-connect** - if no internet connection was available within a specified time period

The action may be as follows:

- **Computer shutdown** - the computer was shut down when the cause occurred
- **Warning messaging** - a preconfigured warning message was shown on the monitored computer
- **Data delete** - specified information was erased on the monitored computer
- **Data download** - specified files were retrieved from the monitored computer and sent to the indicated email address
- **Program execution** - a predefined program(s) was launched on the monitored computer

If the action has failed, the appropriate notification will be shown in the report.

Computer shutdown

This report contains all "Computer shutdown" reactions that occurred on the monitored computer. Each record (row) contains the status of the computer when the action occurred. The status may be as follows:

- **Stolen** - if your computer is reported stolen
- **No-connect** - if no internet connection was available within specified time period

If the action has failed, the appropriate notification will be shown in the report.

Process reports

Warning messaging

This report contains all "Warning message" reactions that occurred on the monitored computer. Each record (row) indicates the status of the monitored computer when the action occurred. The status may be as follows:

- **Stolen** - if your computer is reported stolen
- **No-connect** - if no internet connection was available within specified time period

If the action has failed, the appropriate notification will be shown in the report.

Data delete

This report contains lists of all files and folders erased as an incident response reaction that occurred on the monitored computer. You will also be able to see the date when the file was last accessed and modified.

All files and folders are grouped as an "explorer" tree.

Important!

Mobile Defender utilizes a US DoD approved information sanitization standard. THE ERASED INFORMATION CANNOT BE RECOVERED.

Data download

This report contains lists of all files downloaded (retrieved) from the target computer and sent to the specified email address.

All files and folders are grouped as an "explorer" tree.

Notes:

The downloaded files will be delivered to the email address specified in the **Incident Response - Data Download** policy.

Inventory management

This section includes the following Mobile Audit reports:

- Hardware tracking
- Software tracking
- Services
- Printers

Process reports

- Event viewer

Hardware tracking

This report provides information about the hardware devices installed on the monitored computer. Devices are grouped in classes in the same way as they are grouped by the operating system of the monitored computer. Each device folder contains specific parameters of the device. Some of the parameters are:

- **Friendly name** - the displayed device name
- **Hardware location** - the physical location of the device in the computer hardware architecture
- **Manufacturer** - the manufacturer of the device
- **Service name** - the name of the OS service (driver) that is managing this device

You can find specific devices installed on all your computers using the Find reports form.

Software tracking

This report provides information about the software installed on the monitored computer. Each program folder contains specific parameters of the program.

Some of the parameters are:

- **Version** - the version of the installed program
- **Publisher** - the publisher of the program
- **Comments** - the friendly displayed information about the software
- **Language** - the software language
- **Hidden** - if the program is hidden in the Control Panel
- **Install date** - the date of the program installation
- **Install location** - the full path where the program is installed
- **Install source** - from what location the program was installed
- **Estimated size** - the program size on the local drive

You can find specific software installed on all your computers using the Find reports form.

Services

This Mobile Audit report provides information about services installed on the monitored computer. Each service folder contains the specific parameters of the service. Some of the parameters are:

- **Display name** - the name displayed for this service in the operating system
- **Description** - the friendly displayed information about the service
- **Path to executable** - the full or related path to the service executable program

Process reports

- **Account** - what account the service uses to start
- **Type** - the service type (driver, own process, shared process, etc.)
- **Startup type** - how the service starts (system start, demand start, disabled)

You can find a specific service installed and operating on all your computers using the Find reports form.

Printers

This Mobile Audit report provides information about printers installed on the monitored computer. Each printer folder contains the specific parameters of the printer. Some of the parameters are:

- **Device ID** - the name of the printer device
- **Description** - the friendly displayed information about the printer
- **Driver name** - the driver name of the printer
- **Location** - the physical location of the printer
- **Server name** - the computer (server) name on which the printer is installed
- **Share name** - the network name of the shared printer

You can find specific printers installed on all your computers using the Find reports form.

Event Viewer

This report contains all system logs received from your computer. To view a particular log, click on the log name link. The information displayed on the log-view page will be equivalent to the Event Viewer representation of the system event logs on the monitored computer.

- Audit system events
- Audit logon events
- Audit object access
- Audit privilege use
- Audit process tracking
- Audit policy change
- Audit account management
- Audit directory service access
- Audit account logon events

You can monitor the following events:

- Critical
- Error
- Warning
- Information
- Verbose
- Audit success
- Audit failure

Process reports

- Other

Using event logs you can find specific system events, such as: errors, critical exceptions, etc.

Compliance monitoring

This section includes the following reports:

- Account policies
- Local policies
- Software restriction policies
- Public key policies
- Firewall policies
- Security Center

Account policies

This report provides information about the system account policies on the monitored computer.

The **Password Policy** folder contains all parameters of the password processing of the operating system of the monitored computer.

The **Account Lockout Policy** folder contains condition settings that regulate the disabling of the account.

You can use the Find reports form to find policies that are not compliant with your requirements.

Local policies

This report provides information about the Local Security Policy of the monitored computer.

The **Audit Policy** folder contains parameters of the audit processing of the monitored computer. You can change the audit policy of the monitored computer using the Inventory management policy.

The **User Rights Assignment** folder contains user rights assigned to users and groups of users on the monitored computer. This information allows you to monitor user access to the computer.

The **Security Options** folder contains security parameters applied on the operating system of the monitored computer.

You can use the Find reports form to find policies that are not compliant with your requirements.

Process Reports

Software restriction policies

This report provides information about the Software Restriction Policy applied on the monitored computer.

You can use the Find reports form to find policies that are not compliant with your requirements.

Public key policies

This report provides information about Public Key policies applied on the monitored computer.

You can use the Find reports form to find policies that are not compliant with your requirements.

Firewall policies

This report provides information about the firewall policy applied on the moni-

tored computer.

In the **Parameters** folder you can find the current firewall state and the current profile.

In the **Profiles** folder you can find the current firewall profile and all its parameters.

The following parameters are used to monitor firewall policy compliance:

- **Firewall state** - indicates if the firewall is turned off or on
- **Display a notification** - indicates if the warning message will be displayed when the firewall restricts the network request
- **Allow exceptions** - indicates if the firewall exception rules are allowed
- **ICMP settings** - contains all parameters for the ICMP packets
- **Remote Admin settings** - contains all parameters for the Remote Admin activity
- **Authorized application** - contains a list of all programs that the firewall does not restrict
- **Services** - contains a list of all services for which the firewall can apply exceptions
- **Global open ports** - contains a list of ports opened globally in the operating system of your computer

You can use the Find reports form to find policies that are not compliant with your requirements.

Process Reports

Security Center

This report provides information about the firewall and anti-virus software installed on the monitored computer and its current state of operation.

In the **Automatic Updates** folder you can find the current state of the auto-update service for firewall and anti-virus software installed on the monitored computer.

The **Firewalls** folder contains all firewall software installed on the monitored computer and the state of this software.

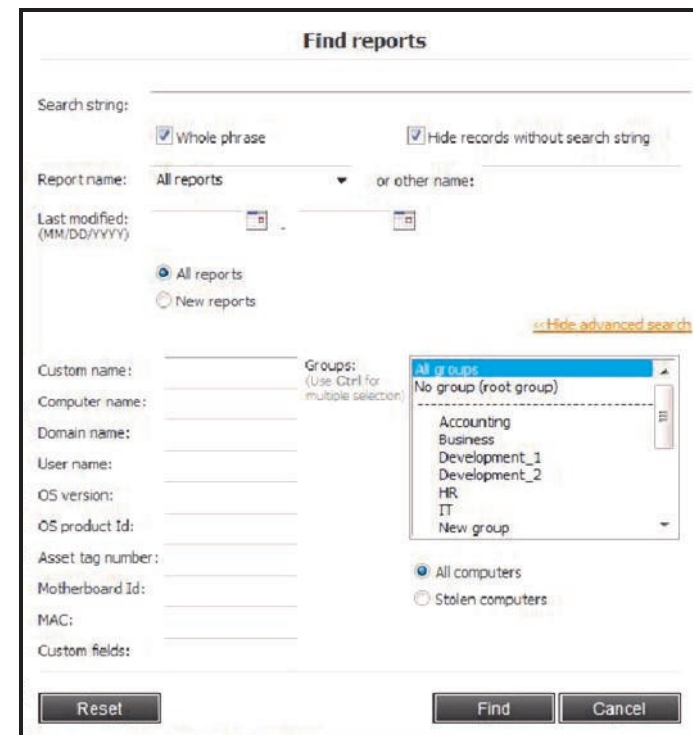
The **Antivirus** folder contains all anti-virus software installed on the monitored computer and its current state of readiness.

The **Product up to date** parameter is used to monitor your firewall and anti-virus database actuality.

You can use the Find reports form to find policies that are not compliant with your requirements.

Figure 19.

Find Reports



Example.

Process Reports

Find reports

To find a specific report, use the "Find Report" form available from the "Reports" Main Menu or from the Report and Policy List Toolbar (see **Figure 17**).

In this form you can enter a report name, receiving date, search string and other parameters (see **Figure 19**).

If you need to find reports from specific computers or groups of computers, click the Advanced search link and enter information in the additional fields.

You can search any text inside your report by clicking the "Find in report" button.

Export reports

You can export all reports from a computer by choosing an appropriate option on the Computer Summary page.

You can export a specified report by choosing Export to file option on the report page. Table reports are exported in CSV (TXT) format and tree-view reports can be exported in XML format.

Note:

All reports that are sent to email are ZIP archived and can be password protected.

Remove reports

You can remove all your reports for storage maintenance or security reasons.

To remove all reports use the appropriate command of the "Reports" submenu of the Main Menu. You can also remove a specified report using the controls of the report viewing page.

Clear configuration changes

You can track changes occurring in the different systems and settings of the monitored computer. Each time the change takes place, it will be shown in the appropriate report.

You can clear all configuration changes of all computers in your account. Select Clear all configuration changes in the "Reports" submenu of the Main Menu. The Configuration changes removal command will be applied to changes only, and not to the original configurations. All current configurations will be available.

To remove all your reports, including main configurations, use the "Remove all

Change Settings

reports” command in the “Reports” submenu of the Main Menu.

You can remove a specific configuration change notice directly on the report viewing page.

Change settings

You can change the following settings in your account:

- Contact information
- Interface settings
- Security settings
- Change your account password
- Your account maintenance

Contact information

On this page you can change your contact information. If your account is registered as a company account, you will be able to update your company information as well.



Main Menu - Settings - Contact Information

Notes:

In order for SafeFrontier to provide full featured support and maintenance, it is important that you keep your contact and your company information current. Please maintain and update all email addresses and phone numbers to be able to

Figure 20.

Change Password



Change Password Dialog Box

Change Settings

receive important notifications.

Interface settings

You may set optional parameters for your account interface.

GO Main Menu - Settings - Interface Settings

Rows per page in lists - how many records will be shown in computers, licenses, reports, or policies lists.

Rows per page in reports - how many records will be shown in the table-view reports.

Show tips and notes - if this parameter is disabled, the Tips will not be shown.

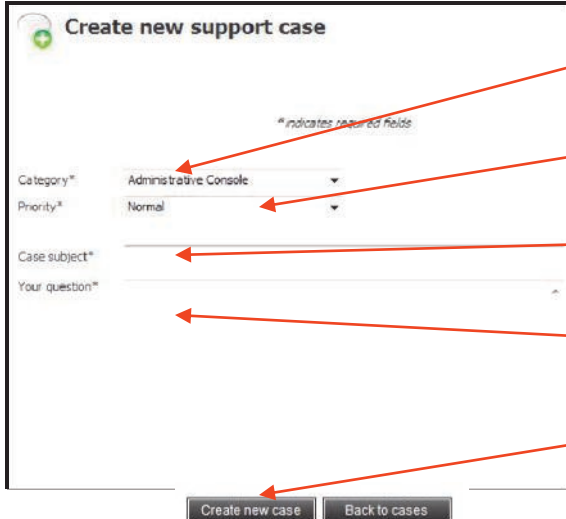
Security settings

You can set your privacy and confidentiality preferences using the following options.

Store reports in the SafeFrontier database - you can store reports in the SafeFrontier database . Your reports are encrypted and access controlled. SafeFrontier has no access to your information. You can also set this option if you want your reports to be erased from our database after you log out of your account. In

Figure 21.

Create New Support Case



The screenshot shows a mobile application interface for creating a new support case. The form includes the following fields and buttons:

- Category***: A dropdown menu currently showing "Administrative Console".
- Priority***: A dropdown menu currently showing "Normal".
- Case subject***: A text input field.
- Your question***: A text input field.
- Create new case**: A button at the bottom left.
- Back to cases**: A button at the bottom right.

Five red arrows point to these elements, numbered 1 through 5:

1. Enter Category
2. Enter Priority
3. Enter Subject
4. Enter Question
5. Click "Create New Case"

Help Desk

this case YOU WILL NOT BE ABLE TO VIEW OLD REPORTS..

Session timeout - if the inactivity in the account is longer than the set inactivity log out timeout, you will be logged out automatically.

Check activations automatically - if this option is disabled, the activations of new computers and licenses will be checked at logon only. To check new activations during your work, enable this option and enter the required check interval.

 **Main Menu - Settings - Security Settings**

Change password

To change your account password you must provide your old (current) password. If your old password is recognized the new password will be accepted. If you have forgotten your password, you can reset your password at any time (see **Figure 20**).

 **Main Menu - Settings - Security Settings - Change Password button**

Account maintenance

You can manage your disk storage and reports history:

 **Main Menu - Settings - Maintenance**

Remove all your reports

Remove all reports from the account

Clear all configuration changes

Clear all the changes in reports of all computers (only actual computer configuration will be available).

Maximum report number

Choose a maximum number of reports to be stored in your account. You can set an automatic report export for the last report to be emailed to the specified email address after you reach the maximum number of reports in your account.

If you need more disk space you can send an online request to our Help Desk Service.

Help Desk Service

SafeFrontier Help Desk Service allows you to communicate with our support

Help Desk

team online.



Main Menu - Help - Help Desk Service

If you have a new question that is not related to a previous messaging you can create new support case. You can choose the category and priority of the new question. If you already have an open support case and want to ask a new question relevant to that topic, than continue previous messaging.

Create new support case

If you have a new question that is not related to previous messaging you can create a new support case. You can choose the category and priority for the new question, so we'll be more informed about your problem.

See **Figure 21**.

Open your existing cases

This page allows you to view your existing support cases. Each case has a Case #, subject, category and priority. You can arrange and find your cases by these parameters.

If you have other questions based on an existing case subject, please open the appropriate case and continue messaging. If you have a new question unrelated to a previous message, you can create new support case.

Your existing case

On this page you can view your previous messages for a specific case and information about the case.

If your next question is based on the same case subject, you can send a new message in this case and continue messaging. If your next question is unrelated to the subject of this case, you can create a new support case with different parameters.

Send new support message

If you have a new question related to an existing support case you can continue messaging in this case. You can change the subject of a new message, if it does not apply to your question.

Appendix 1

How to use Free Products

1. Download your free Mobile Tracking

From the Main Menu, select "Download" and the "Free products" sub-menu. Click on the Mobile Tracking link. Download the ZIP archive and extract the installation files to a separate folder.

2. Install Mobile Tracking on your computer

A. To install True Security™ Mobile products on a separate computer you need to logon to this computer as a local administrator.

B. Run the install program setup.exe and follow the instructions.

C. When the installation is finished you will need to reboot your computer (the install program will do it automatically).

Remember!

The new computer will be shown in the Computer List and available for administration only after it connects to the internet (the computer needs to send its activation notification during first internet connection).

3. Obtain your free license

From the Main Menu select "Licenses" then Get your new free license and

follow the instructions on the page.

4. Assign a license to your computer

To assign a free Mobile Tracking license to your computer, go to the Main Menu, "Licenses", Assign or update licenses and follow the instructions on the page. You can also refer to Tips for help (see Figure 1).

5. Processing reports from your computer

Once Mobile Tracking is activated you can receive and process reports from your computer. The following reports are available when Mobile Tracking is installed on your computer:

- Computer Summary
- System Information
- Local Users
- Local Groups
- Products and Licenses
- Session Monitoring
- IP tracking
- Wi-Fi tracking
- GPS tracking
- GSM tracking
- Image Capturing

For help on a specific report, view Tips (see Figure 1) for the selected report.

Appendix 2

How to use Free Trial

1. Download your free trial of SafeFrontier products.

From the Main Menu, select "Download" and the "Trial versions" sub-menu. Click on the appropriate product link. Download the ZIP archive and extract the installation files to a separate folder.

2. Install a free trial on your computer

A. To install True Security™ Mobile products on a separate computer you need to logon to this computer as a local administrator.

B. Run the install program setup.exe and follow the instructions.

C. When the installation is finished you will need to reboot your computer (the install program will do it automatically).

Remember!

The new computer will be shown in the Computer List and available for administration only after it connects to the internet (the computer needs to send its activation notification during first internet connection).

3. Obtain your free trial license

To obtain your license do the following:

From the Main Menu select "Licenses" then Get your trial license and follow the instructions on the page.

4. Assign a license to your computer

To assign a trial license to your computer, go to the Main Menu, "Licenses", Assign or update licenses and follow the instructions on the page. You can also refer to Tips for help (see Figure 1).

5. Process reports from your computer

Once your trial is activated you can receive and process reports from your computer. All full-featured reports for the appropriate product will be available with the free trial installed on your computer.

For help on a specific report, view Tips (see Figure 1) for the selected report.

Appendix 3

How to use Commercial Products

1. Download commercial SafeFrontier products

From the Main Menu, select "Download" and the "Commercial products" sub-menu. Click on the appropriate product link.

Download and extract the installation files to a separate folder.

2. Install product on your computer

A. To install True Security™ Mobile products on a separate computer you need to logon to this computer as a local administrator.

B. Run install program setup.exe and follow the instructions.

C. When the installation is finished you will need to reboot your computer (the install program will do it automatically).

Remember!

The new computer will be shown in the Computer List and available for administration only after it connects to the internet (the computer needs to send its activation notification during first internet connection).

3. Order a new commercial license

You can order new commercial licenses through the SafeFrontier Online Store. Go to the Main Menu, "Licenses", Order new commercial licenses.

To activate your licenses, go to the Main Menu, "Licenses", Activate new ordered licenses and follow the instructions on the page.

4. Assign a license to your computer

To activate the product, you need to assign a commercial license to the computer where the product is installed. To assign a license to your computer, go to the Main Menu, "Licenses", Assign or update licenses and follow the instructions on the page. You can also refer to Tips for help (see Figure 1).

5. Process reports from your computer

Once your product is activated you can receive and process reports from your computer. Reports will be available depending on the product installed on your computer.

For help on a specific report, view Tips (see Figure 1) for the selected report.

Appendix 4

Standards and Guidelines

Common Standards and Guidelines

NIST Special Publication 800-12 An Introduction to Computer Security: The NIST Handbook

NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems

NIST Special Publication 800-40 Creating a Patch and Vulnerability Management Program

NIST Special Publication 800-44 Guidelines on Securing Public Web Servers

NIST Special Publication 800-95 Guide to Secure Web Services

NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems

FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems

Cryptography

NIST Special Publication 800-21 Guideline for Implementing Cryptography In the Federal Government

NIST Special Publication 800-45 Guidelines on Electronic Mail Security

NIST Special Publication 800-52 Guidelines for the Selection and Use of Trans-

port Layer Security (TLS) Implementation

NIST Special Publication 800-57 Recommendation for Key Management

NIST Special Publication 800-107 Recommendation for Applications Using Approved Hash Algorithms

NIST Special Publication 800-108 Recommendation for Key Derivation Using Pseudorandom Functions

FIPS Publication 140-2 Security Requirements for Cryptographic Modules

FIPS Publication 180-3 Secure Hash Standard (SHS)

FIPS Publication 197 Advanced Encryption Standard (AES)

FIPS Publication 198-1 The Keyed-Hash Message Authentication Code (HMAC)

Media Sanitizing

NIST Special Publication 800-88 Guidelines for Media Sanitization

DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM)

Forensics and Incident

NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response

Appendix 4

NIST Special Publication 800-72 Guidelines on PDA Forensics

NIST Special Publication 800-101 Guidelines on Cell Phone Forensics

NIST Special Publication 800-92 Guide to Computer Security Log Management

FISMA Requirements

The product was developed and confirms to the following specifications FIPS PUB 200 i NIST SP 800-53 in the chapters relevant to the product functional application and security requirements: i, iii, v, vii, viii, ix, x, xvi, xvii.

The following publications were utilized in the product development: NIST version SP 800: 12, 14, 21, 40, 44, 45, 52, 53, 57, 72, 86, 88, 92, 95, 101, 107, 108.

Cryptography

Fully complies with FIPS 140-2 Level 2, (in the process of certification). The following algorithms and protocols approved by NIST and required by FIPS 140-2 are utilized in the product:

AES (256 bits) - data encryption (FIPS PUB 197)

SHA2 (256 bits) - data integrity (FIPS PUB 180-3)

HMAC (256 bits) - message authentication (FIPS PUB 198-1)

TLS 1.0 - transport level security (NIST SP 800-52)

Appendix 5

Requirements

Operating system:

- Windows XP SP2 (SP3 recommended)
- Windows Vista (SP1 recommended)
- Windows 7

..NET Framework 2.0 SP1

Web browser:

- Internet Explorer 7+
- Mozilla Firefox 3+
- Opera 9+
- Safari 3+
- Google Chrome
- Other W3C compatible browsers

Not all GSM phone models are supported. Contact SafeFrontier support for more information.

It is required that the following ports to be open: HTTP (80), Secured POP3 (995), Secured SMTP (465). These are the standard ports used for browsers (80), and protected email (995, 465). The product can be configured to use different none standard ports.

