



Fail Safe
Protect yourself

Product Requirements Document– Phoenix FailSafe™ SaaS with Intel® Anti-Theft 2.0

Revision Date: September 29, 2009

Revision History

Revision No	Date	Description	Revisions by
1.0	092909	<ul style="list-style-type: none">• Original document with inputs from Intel and Dale Q and Jacques L	Cary

Confidential and Proprietary Information

The contents of this document are confidential and proprietary to Phoenix Technologies Ltd. Access to this information is restricted. This document is provided for Distributor's internal use only. This document should not be disclosed to any third party, including customers.

Copyright

Copyright © 2009 Phoenix Technologies Ltd. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of Phoenix Technologies Ltd.

Table of Contents

1	SCOPE OF THE DOCUMENT	1
2	PRODUCT OVERVIEW AND FEATURES.....	1
3	ADDING INTEL® ANTI-THEFT FUNCTIONALITY TO PHOENIX FAILSAFE™ .	1
3.1	INTEL AT CORE SCHEDULE.....	1
3.2	FAILSAFE WITH INTEL AT BLOCK DIAGRAM	1
4	FEATURE/CAPABILITY PRIORITIES AND PHASING	2
4.1	PHASE 1: AT 2.0 BASELINE AND USER EXPERIENCE	2
4.1.1	<i>Phase 1 Timing.....</i>	2
4.1.2	<i>Consumer Users.....</i>	2
4.1.3	<i>Client Features.....</i>	3
4.1.4	<i>Consumer Server Features.....</i>	3
4.1.5	<i>FailSafe Consumer UI Web Portal Changes</i>	3
4.1.6	<i>TCP/IP</i>	5
4.1.7	<i>FailSafe Disable Ubiquity.....</i>	6
4.1.8	<i>SMS</i>	6
5	PHASE 2: SMS, SDK AND EUI	6
5.1.1	<i>SMS.....</i>	6
5.1.2	<i>Client utility.....</i>	6
5.1.3	<i>Support for LiveTrace</i>	6
5.1.4	<i>New state “secured”</i>	7
5.1.5	<i>Enterprise Server Features</i>	7
5.1.6	<i>Super Enterprise Admin</i>	8
5.1.7	<i>Admin</i>	9
5.2	BIOS EFI SDK TOOLKIT	9
5.3	BIOS INTEGRATION VALIDATION TOOL	9
6	PHASE 3: FAILSAFE WINDOWS ONLY CLIENT (WOC) WITH AT 2.0.....	10
7	PHASE 4: ENHANCEMENTS AND STAGING FOR AT 3.0	10
7.1.1	<i>BIOS support for SMS wakeup.....</i>	10
	<i>When client is within the Geofencing and about to or has just been DTimed support for a default” fuse” to delay lock.....</i>	10
7.1.2	<i>BIOS support for PBA.....</i>	10
7.1.3	<i>Full Disk Encryption.....</i>	10
	<i>Need to understand the business case.</i>	10
7.1.4	<i>Volume Encryption.....</i>	10
	<i>Need to understand the business case.</i>	10
7.1.5	<i>Data Access Disable</i>	10
7.1.6	<i>FailSafe Dashboard</i>	10
7.1.7	<i>XML Support.....</i>	10
8	INTEL® AT 1.0 AND 2.0 TRACEABILITY MATRIX.....	11
9	OUT OF BOX EXPERIENCE (OOBE).....	11
9.1	FAILSAFE BRANDING GUIDELINES FOR INSTALLER AND WEB SERVER	11

9.2	OEM TRIAL AND PAID FLOWS	12
9.3	TRIAL AND PAID INSTALLER SCREENS.....	12
9.3.1	<i>New First Time Install Welcome</i>	12
9.3.2	<i>New Installer Status Window</i>	13
9.3.3	<i>New FailSafe Installation Window</i>	14
9.3.4	<i>New End User License Agreement Window</i>	15
9.3.5	<i>First Time Registration Window</i>	15
9.3.6	<i>Existing User Registration Window</i>	16
9.3.7	<i>New Success Window</i>	16
10	FAILSAFE UNINSTALL PROCESSES	16
10.1	FAILSAFE UNINSTALL.....	16
10.2	CONVERSION TRIAL AND PAID FLOWS.....	18
10.2.1	<i>FailSafe Consumer Server Login within the Product Upgrade</i>	18
10.2.2	<i>My Laptops</i>	18
10.2.3	<i>Shopping Cart</i>	19
10.3	LICENSING.....	20
11	TOASTER ALERTS	20
11.1	TRY ME TOASTER ALERT	21
11.2	TRIAL TOASTER ALERT	21
11.3	EXPIRED TOASTER ALERT	21
11.4	ANNUAL RENEWAL TOASTER ALERT	22
11.5	EXPIRED ANNUAL TOASTER ALERT	23
11.6	PRODUCT UPGRADE TOASTER ALERT	23
11.7	PRODUCT PROMOTION TOASTER ALERT	23
12	BREAKFIX SCENARIOS	24
12.1	PREREQUISITES FOR THE BREAKFIX SCENARIO SUPPORT	24
13	LOCALIZATION	24
14	TARGET OPERATING SYSTEM SUPPORT	24
15	TARGET BROWSER SUPPORT.....	25
16	THIRD-PARTY APPLICATIONS SUPPORT	25
16.1	ANTI-VIRUS COEXISTENCE.....	25
16.2	TWO-FACTOR AUTHENTICATION SOLUTIONS	25
17	DOCUMENTATION.....	25
18	TECHNICAL SUPPORT.....	25
19	COMPETITIVE MATRIX.....	26
20	OPEN ITEMS.....	27
21	DEFINITIONS, ACRONYMS, ABBREVIATIONS	27

1 Scope of the Document

This document describes the baseline phased product requirements of Phoenix FailSafe™ combined with Intel® Anti-Theft technology. All items and contents described in this document are subject to change based on negotiations with Phoenix engineering and OEM feedback. Typically final implementation details are addressed in a Functional Specification.

This document covers proposed new product requirements, for coverage on how features work please see the FailSafe User Guide.

2 Product Overview and Features

FailSafe™ is an SaaS (Software as a Service) offering from Phoenix Technologies Ltd®, that provides the ability to protect, track, and remotely manage lost or stolen desktops, notebooks and netbooks.

3 Adding Intel® Anti-Theft Functionality to Phoenix FailSafe™

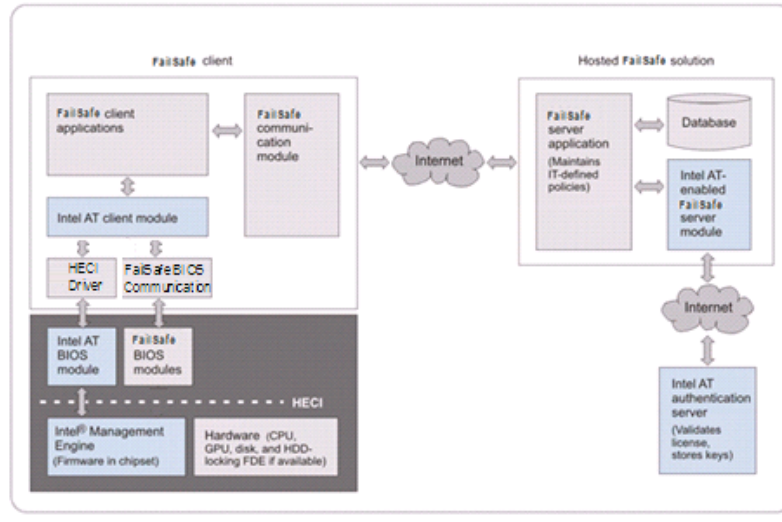
The latest Centrino® processor technology based notebooks include Intel AT. OEM vendors currently supporting Intel AT are: Lenovo, Fujitsu, Acer, Asustech and Panasonic- all as Enterprise plays. Dell at the September 24, 2009 IDF announced that they would add Intel AT support for Consumer.

3.1 Intel AT Core Schedule

	2009-2009	2010
Business	vPro only	Core with vPro
Consumer		Core i3 Core i5 Core i7

3.2 FailSafe with Intel AT Block Diagram

Similar to FailSafe Intel AT has a client, server relationship. There is an Intel AT Authentication server that does license validation that sits behind the FailSafe server and there is a firmware portion to the client Intel® Manageability Engine (Intel® ME) integrated into the chipset. The host embedded controller interface (HECI) allows the host OS or BIOS to communicate directly with the ME.



Since Intel AT is designed into the laptop's chipset, the FailSafe anti-theft capabilities are more protected from tampering. Intel AT is a set of hardware based security building blocks to protect a computer when it is lost or stolen.

4 Feature/Capability Priorities and Phasing

4.1 Phase 1: AT 2.0 Baseline and User Experience

4.1.1 Phase 1 Timing

The target GM timeframe for phase 1 is end January 2010.

To support this phase 1 timeframe requirements are narrowed as Dell Consumer as the target customer for AT 2.0 phase 1.

4.1.2 Consumer Users

4.1.2.1 Require minimum complexity on passwords (Core PRD)

Password must be at least 6 characters long and contain at least one of each of the following:

- Uppercase letter
- Lowercase letter
- Special character or number

The characters " (double quote) and ' (single quote) are not allowed in passwords. Password may not contain your username.

4.1.2.2 Reduce Vulnerabilities (Ph 2)

Provide the ability for FailSafe with BIOS or Intel AT to generate a new unlock code. This closes vulnerability and also enables the OEM to ship the FailSafe disabled system to the end-user for enablement via call back to the OEM with confirmation of payment.

4.1.3 Client Features

4.1.3.1 Client state audit trail

FailSafe captures the last maximum number of events and forensics from the Intel ME if AT enabled

4.1.3.2 Kill Timer “KTimer”

Feature to set a default time of 5 minutes before the computer bricks to allow for emergency retrieval of files, erasure of files.

4.1.4 Consumer Server Features

4.1.4.1 New Alerts Tab (maybe Ph 1)

Below the “Agent Uninstall Alert” add optional support for automatic notifications for “at risk” devices via automatic email and UI notification that a devices. Default should be Enable for each.

Proposed new Alerts are:

- {device name} about to execute disable command
- {device name} 7 or less days until DTimer expiration

4.1.5 FailSafe Consumer UI Web Portal Changes

4.1.5.1 New Introduction Tab

In the data section (left column) of the video the following text needs to get replaced, “FBI reports that ... never recovered” with new text, “A laptop is stolen World-wide every 53 seconds” to make it less US centric. This new text is the same font size and type as preceding text. No change to voice over required.



In the disable section of the video has two text areas- one in the left column and the other in the right center section point #3 "Password Protected at BIOS Level" that need to get supplemented. For both text areas the new text should read, "Password Protected at BIOS Level and/or Intel® Anti-Theft firmware level." This new text is the same font size and type as preceding text. Intel Corporation needs to approve these UI proposals. No change to voice over required.



4.1.5.2 New Disable Tab

The logic should be that if the FailSafe system check identifies an Intel AT enabled computer AND the OEM package supports Intel AT then the Intel logo and "Intel® Anti-Theft Technology Enabled" will appear to the right of the "Display unlocking screen" disable. This

new text is the same font size and type as preceding text, but in blue font. To sum up if AT is enabled no BIOS will be used for disable.

Intel Corporation needs to approve these UI proposals.



4.1.6 TCP/IP

4.1.6.1 Enrollment

Support for basic AT enrollment if the OEM platform and package supports Intel AT.

4.1.6.2 De-enrollment or Un-enrollment

Authorized vendors can un-enroll a computer from theft management service for repair purposes. See Breakfix section below.

4.1.6.3 Rendezvous

Support for AT-based timer which triggers a policy based response when computer fails to check in after 24 hours. Rendezvous works whether PC is online or offline

4.1.6.4 Enhanced DTimer support (Time to Disable for FailSafe)

The FailSafe client can be put into a state that optionally disables the DTimer concept. Default setting is DTimer is on for typically 30 days.

4.1.6.5 Non-support of Montevina AT 1.0

FailSafe will provide EFI SDK based 3rd party or Phoenix Bios and will use Phoenix Benton2 based reference BIOS (Calpella based) for OEM/ODMs. Intel AT 1.0 will not be supported.

4.1.7 FailSafe Disable Ubiquity

One disable tab for BIOS AT, WOC (future) depending upon which is more secure and part of the OEM's package.

4.1.8 SMS (Ph 2)

4.1.8.1 Assert stolen

When the computer has 3G modem a deactivation code can be sent through SMS message. FailSafe supports remote administration and set up of the mobile device.

4.1.8.2 De-assert stolen

When the computer has 3G modem a reactivation code can be sent through SMS message.

5 Phase 2: SMS, SDK and EUI

5.1.1 SMS

5.1.1.1 Notifications

When the computer is flagged in the central server rapid notification can be sent by SMS to the server if computer is connected to a 3G modem. This is a two way communication- FailSafe can send a instant remote notification via SMS to a paired mobile device.

5.1.2 Client utility

A server push based utility that determines whether the device is FailSafe installed

5.1.3 Support for LiveTrace

Live trace is a feature that allows us to pull full debugging trace streams from a client device to the servers via our secure channel

5.1.4 New state “secured”

This is the state of a device that is returned to the user and locked in a room or shipped overseas.

5.1.5 Enterprise Server Features

5.1.5.1 New Reports Tab

Add to this section the ability to support for automatic notifications for “at risk” devices via UI notification and automatic email to the appropriate administrator that a device is:

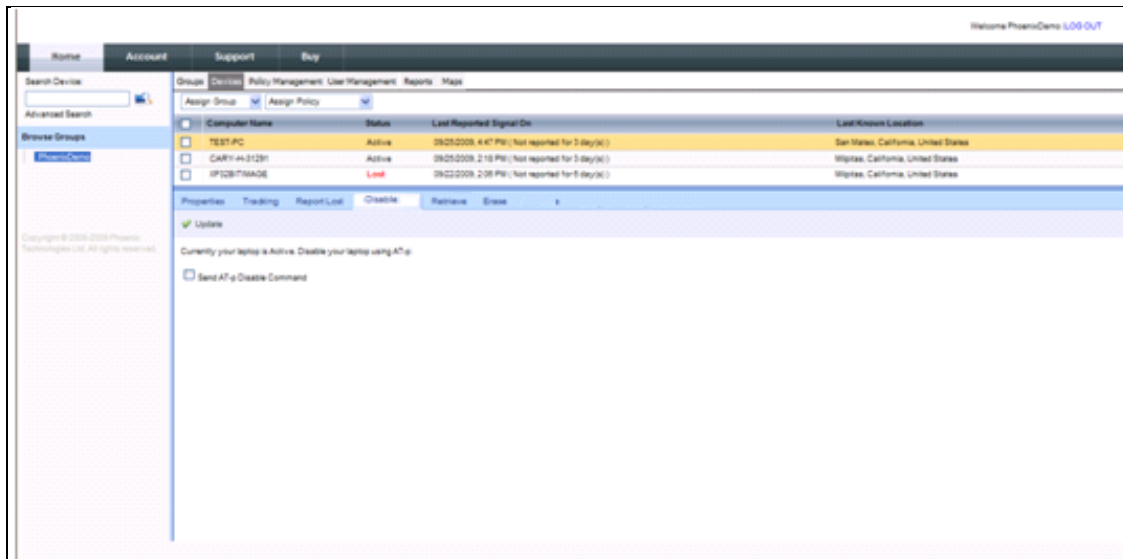
- {device name} about to execute disable command
- {device name} 7 or less days until DTimer expiration
- {device name} outside a geo fence list
- Login time in PBA module before boot for {device name} exceeds threshold
- {device name} PBA Login Timer
- {device name} PBA Login Failure
- {device name} AT module may have been tampered with

Computer Name	User Name	Activation Date	First Signal Date	Last Signal Date	IP Address (LAN/WAN)	Signals in 30 days
TEST-PC	VALUE	09/17/2009 2:57 PM	09/23/2009 12:39 PM	09/25/2009 4:47 PM	192.168.1.211 / 71.135.104.222	723
CARRY-4H-31291	mark_wly	09/22/2009 10:11 AM	09/22/2009 10:13 AM	09/25/2009 2:18 PM	134.122.5.181 / 210.146.212.222	2750
JPS2BITIMAGE	localadmin	09/22/2009 1:44 PM	09/22/2009 1:48 PM	09/22/2009 2:08 PM	134.122.7.171 / 210.146.212.222	20

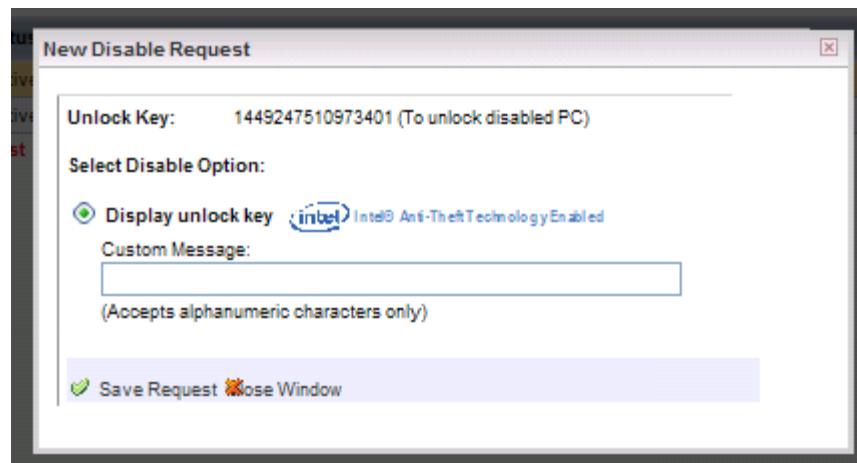
5.1.5.2 Enterprise UI Disable Tab

Remove **AT-p Disable** tab and collapse all disable functionality under one **Disable** tab.

Also remove **Encrypt** and **Encrypted Volume** tabs and contents until these features are supported.



The logic should be that if the FailSafe system check identifies an Intel AT enabled computer AND the OEM package supports Intel AT then the Intel logo and “Intel® Anti-Theft Technology Enabled” will appear to the right of the “Display unlocking screen” disable and to the right of the “Sound alarm and display alert” disable. This new text is the same font size and type as preceding text, but in blue font. Intel Corporation needs to approve these UI proposals.



5.1.6 Super Enterprise Admin

5.1.6.1 Creates Enterprise Users

Support for the creation of Enterprise Administrator users and assigned group access

Support for an administrative audit trail that captures the last 1000 events and forensics from Failsafe and the Intel ME if AT enabled

5.1.6.2 Enterprise Administrator

Support for the creation of administrator users and assigned group access

5.1.7 Admin

5.1.7.1 Tiered management

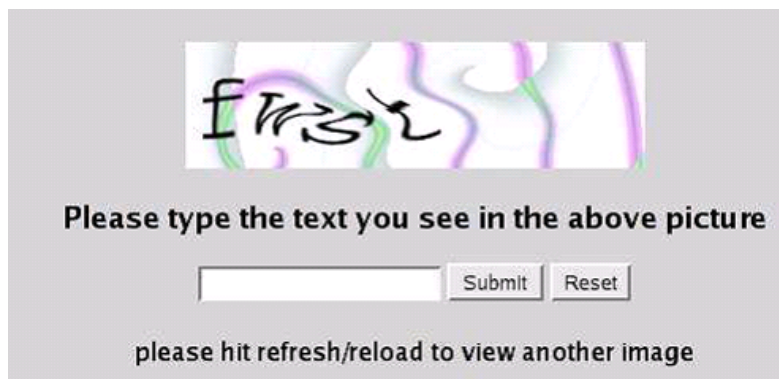
Support for tiered hierarchical policy control of devices within their groups control

5.1.7.2 “Panic Button” Feature

Pre-established, templated policies to perform automatically before kill pill delivered. Examples would be a corporate password or VPN profile file retrieve or erase before disable is executed.

5.1.7.3 Web facing login’s requirement DoS attack “image” be used

To prevent DoS and DDoS attacks to FailSafe requirement is to support a Login like the example below.



5.2 BIOS EFI SDK Toolkit

Phoenix provides a BIOS Software Development Kit (SDK) to enable integration of the FailSafe BIOS binary files into third-party EFI BIOS. Here are the main concepts of FailSafe EFI SDK:

- Seamless integration of FailSafe BIOS functionality in the BIOS of third-party BIOS vendors
- Self-sufficient Porting Guide on how to integrate the FailSafe BIOS binaries into 3rd-party codebase;
- Sample reference implementation
- Automated EFI shell tool to validation implementation
- Support for SMS needs to be added in phase 1

5.3 BIOS Integration Validation Tool

Phoenix provides FailSafe Validation tool to verify the BIOS integration and validate the Windows runtime communication to the BIOS. Validation tool includes Phoenix CryptOSD installation package and set of test cases to be executed on the target platforms.

6 Phase 3: FailSafe Windows Only Client (WOC) with AT 2.0

These requirements will be covered in a separate PRD

7 Phase 4: Enhancements and Staging for AT 3.0

These requirements will be covered in a separate PRD. Preliminary list of requirements are in 7.1.x below.

7.1.1 BIOS support for SMS wakeup

When client is within the Geofencing and about to or has just been DTimed support for a default” fuse” to delay lock

7.1.2 BIOS support for PBA

7.1.3 Full Disk Encryption

Need to understand the business case.

7.1.4 Volume Encryption

Need to understand the business case.

7.1.5 Data Access Disable

Intel added feature for PGP-based encryption key material to be escrowed in the chipset. Key material can be deleted or hidden to protect data.

7.1.6 FailSafe Dashboard

Web UI component intended to provide information about FailSafe status at a glance. It provides for easy drill down to get more complete information. It also represents the integration point for the data provided by all FailSafe, Intel AT, and any future 3rd party integrated components.

7.1.7 XML Support

FailSafe server will provide XML hooks to legacy and 3rd party management tools

8 Intel® AT 1.0 and 2.0 Traceability Matrix

Phasing below represents first FailSafe support, it is assumed that all functionality and associated UI changes are carried forward to later phases for both CUI and EUI

	AT 1.0	AT 2.0	FailSafe Phase 1	FailSafe Phase 2	FailSafe Phase 3
Intel Platform	Montevina	Calpella	PRD Section	PRD Section	PRD Section
Rendezvous Timer ¹	X	X	4.1.6.3		
PC Tamper Monitoring ¹	X	X		5.1.5.1	
PBA Login Timer ¹		X		5.1.5.1	
PBA Login Failures ¹	X	X		5.1.5.1	
Remote Notification ¹		X	4.1.4.1		
Instant Remote Notification ^{1,2}	X	X (3G only)		5.1.1.1	
PC Disable ¹	X	X	4.1.5.2		
Data Access disable	X	X			7.1.5
Reactivation Password ¹ (BIOS)		X	4.1.5.2		
Reactivation in PBA Module ¹	X	X			7.1.1
Remote Reactivation ¹		X	4.1.5.2		
Instant Reactivation Code ^{1,2}		X (3G only)		5.1.1.3	
Customizable Reactivation Screen ¹		X	4.1.5.2		
Service Un-enrollment ¹		X	4.1.6.2/12.1		
Delivery Confirmation ¹		X	4.1.4.1		
Event and Audit Logs		X	4.1.3.1		

¹ Requires support by ISV like Phoenix

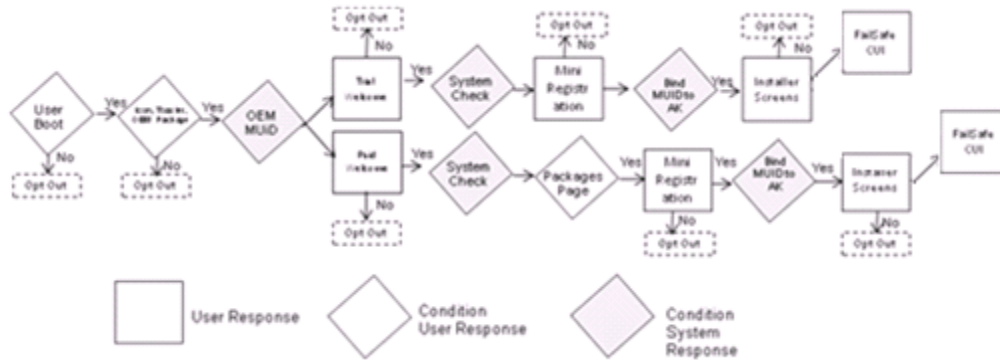
² Requires the 3G PC Module with Intel AT capabilities, like the Ericsson* 3G card

9 Out of Box Experience (OOBE)

9.1 FailSafe Branding Guidelines for Installer and Web Server

OEM specific logo treatment, colors, messaging and terminology will be used only on the introductory Installer window and the web-based login banner. The rest of the windows/webpage's will use the FailSafe generic template and "computer" terminology consistent with the package used.

9.2 OEM Trial and Paid Flows

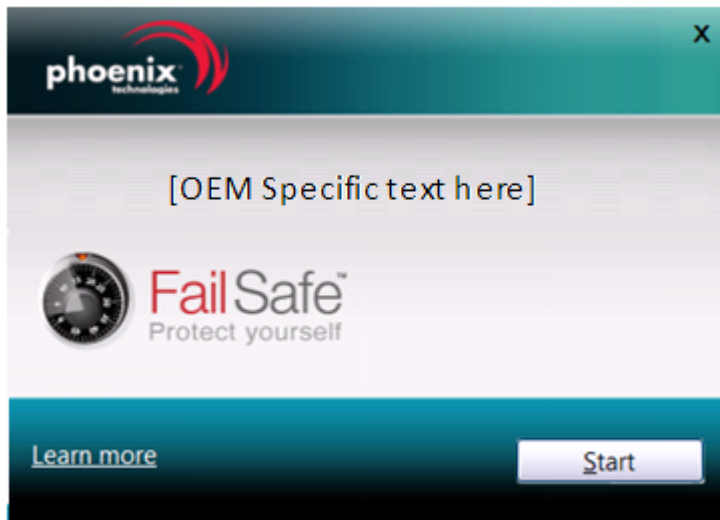


See below the FailSafe registration and activation process:

- The user has following options to get the FailSafe Installation package:
 - Computer comes with the pre-installed FailSafe Installer in case of Paid subscription;
 - The user downloads the FailSafe Installation package from the FailSafe Server in case of Trial;
- When user initiates the installation FailSafe Server will get the MUID, Authorization Flag (AF) from the BIOS, and Activation Key embedded in the FailSafe Installation package to assign unique license key for the computer.
- The user has to enter is a valid “E-mail Address” and “Create Password”
- The user completes the FailSafe Installation and will get the License Key in the email.
- The user is ready to access the FailSafe Server

9.3 Trial and Paid Installer Screens

9.3.1 New First Time Install Welcome



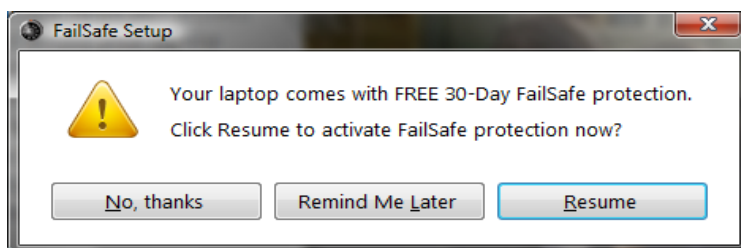
Learn More: Users will be directed to the appropriate FailSafe information at FailSafe server (www.failsafe.com)

Start: Initiate the installation process.

9.3.1.1 Cancel Warning Window

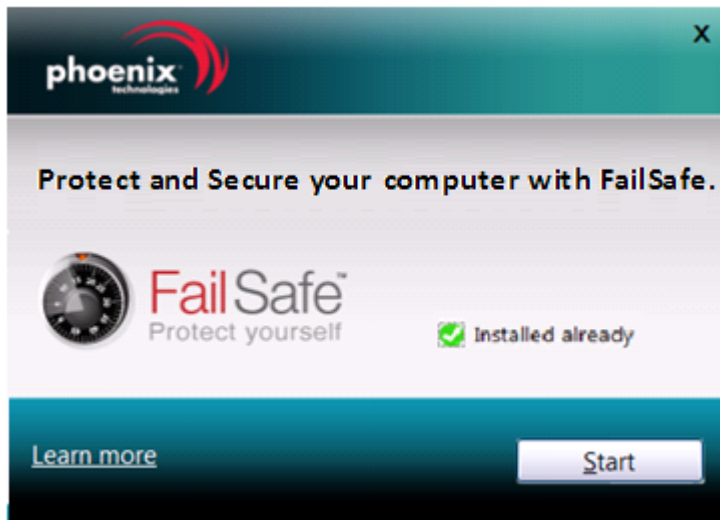
No change to existing functionality. In case of user interrupts the installation process the following screen will be displayed where users are presented with three options:

- No, thanks (will deactivate the Launcher)
- Remind Me Later
- Resume



9.3.2 New Installer Status Window

This screen will be displayed if FailSafe is already installed.



Click **Start** to continue.

9.3.3 New FailSafe Installation Window



FailSafe conducts a system check to determine:

- if Intel AT is available if the OEM has an AT package
- first time or new installation
- supported BIOS available
- supported OS is available
- Internet connectivity

Based on the results of the system check the user will see the appropriate installer window and/or warning window per the above flow.

9.3.4 New End User License Agreement Window

Please review and accept the FailSafe terms of use before the registration:

PHOENIX TECHNOLOGIES LTD.

PHOENIX FAILSAFE™ SERVICE AGREEMENT

IMPORTANT: BEFORE YOU CLICK ON THE "ACCEPT" BUTTON, PLEASE READ THIS SERVICE AGREEMENT CAREFULLY AS IT CONTAINS THE LEGAL TERMS AND CONDITIONS THAT YOU AGREE TO WHEN USING THE SERVICE. BY CLICKING ON THE "ACCEPT" BUTTON, YOU (1) ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS SERVICE AGREEMENT AND (2) YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT, PERSONALLY OR ON BEHALF OF THE COMPANY YOU HAVE NAMED AS THE CUSTOMER, AND TO BIND THAT COMPANY TO THESE TERMS. THE TERM "YOU" REFERS TO THE INDIVIDUAL OR A LEGAL ENTITY, AS APPLICABLE, THAT REGISTERS FOR OR USES THE PHOENIX FAILSAFE SERVICE. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS SERVICE AGREEMENT, OR IF YOU DO NOT HAVE SUCH AUTHORITY, CLICK THE "DECLINE" BUTTON AND DO NOT USE THE PHOENIX FAILSAFE SERVICE.

YOUR ACCESS TO AND USE OF THE PHOENIX FAILSAFE SERVICE IS CONDITIONED UPON YOUR COMPLIANCE WITH THE TERMS OF THIS SERVICE AGREEMENT. A TRIAL OFFERING OF THE PHOENIX FAILSAFE SERVICE MAY BE PROVIDED TO YOU FOR YOUR USE ONLY IN ACCORDANCE WITH THIS SERVICE AGREEMENT.

ANY INFORMATION THAT PHOENIX OBTAINS ABOUT YOU OR OTHER INDIVIDUALS THROUGH YOUR USE OF THE PHOENIX FAILSAFE SERVICE SHALL BE GOVERNED BY THE FAILSAFE PRIVACY POLICY LOCATED AT <http://www.failSAFE.com/>, AS MAY BE AMENDED FROM TIME TO TIME. BY USING THE PHOENIX FAILSAFE SERVICE, YOU CONSENT TO THE COLLECTION AND PROCESSING (INCLUDING THE DISCLOSURE AND

☒ **I accept the terms of the service agreement** [FailSafe Privacy Policy](#)

< Back Next > Cancel

Need to revert back to the non-Freeze hybrid EULA that is FailSafe only.

The Service Agreement displays. Review and accept the terms of the license agreement, and then click **Next** to continue.

9.3.5 First Time Registration Window

Complete the registration to create a new account. Existing FailSafe users [click here](#)

First Name* Last Name*

Address* City/Locality*

State/Province* Zip/Post Code* Country/Region*

Phone Number

E-mail ID and password are required for the FailSafe Web Console.

E-mail* Confirm E-mail*

Password* Confirm Password*

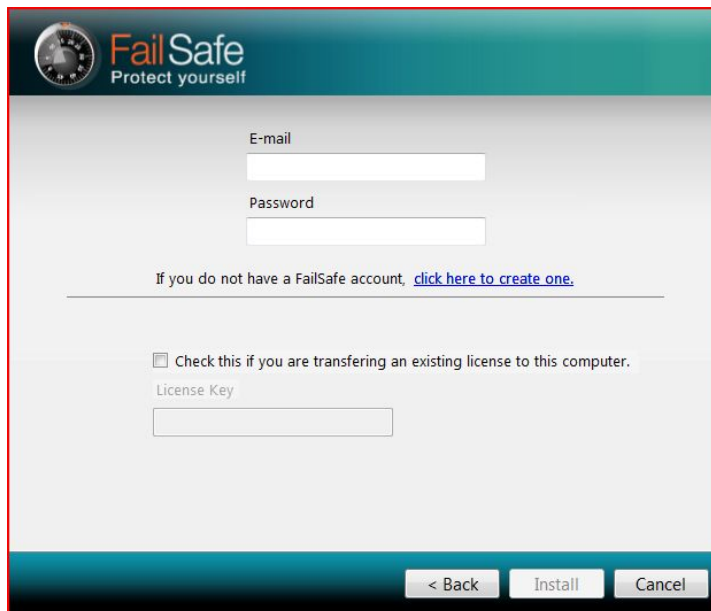
* Required fields. Password must have minimum 6 characters, 1 uppercase and 1 numeric.

[FailSafe Privacy Policy](#) < Back Next > Cancel

No change to existing window- presented for flow continuity.

Enter information in the registration form, and then click **Next** to continue. For Existing Users select "[click here.](#)" The following window displays.

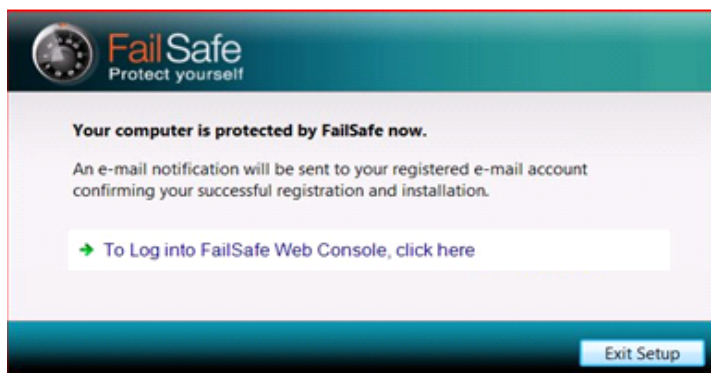
9.3.6 Existing User Registration Window



The screenshot shows the 'Existing User Registration Window' for FailSafe. The window has a teal header with the FailSafe logo and the tagline 'Protect yourself'. Below the header, there are two input fields: 'E-mail' and 'Password'. A link 'click here to create one.' is provided for users who do not have an account. There is a checkbox labeled 'Check this if you are transferring an existing license to this computer.' and a 'License Key' input field below it. At the bottom, there are three buttons: '< Back', 'Install', and 'Cancel'.

No change to existing window- presented for flow continuity.

9.3.7 New Success Window



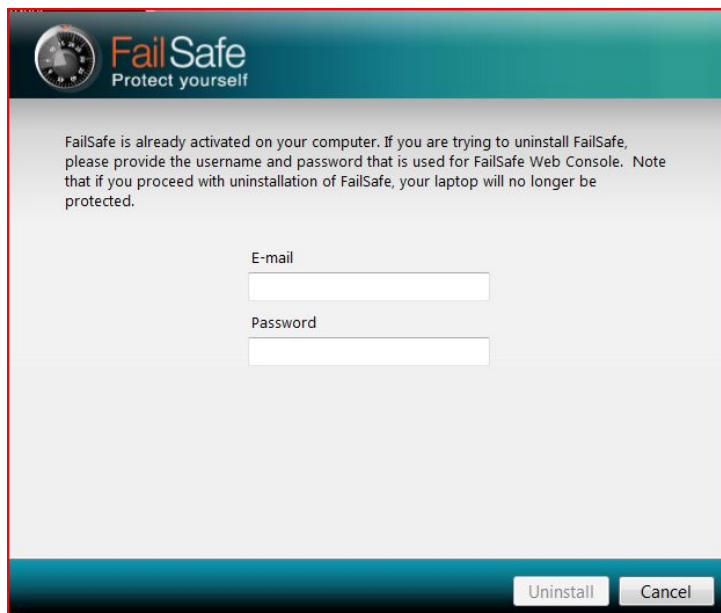
The screenshot shows the 'New Success Window' for FailSafe. The window has a teal header with the FailSafe logo and the tagline 'Protect yourself'. Below the header, the text reads: 'Your computer is protected by FailSafe now.' and 'An e-mail notification will be sent to your registered e-mail account confirming your successful registration and installation.' There is a link 'To Log into FailSafe Web Console, click here' with a green arrow icon. At the bottom right, there is a button labeled 'Exit Setup'.

10 FailSafe Uninstall Processes

10.1 FailSafe Uninstall

This section describes end-user initiated uninstall process. There is no Add/Remove option provided to user to uninstall the FailSafe. The user will be able to download the Uninstaller from the FailSafe Server and run it on the local machine. The Uninstall screen requires FailSafe account information in order to uninstall the product.

Challenge Window

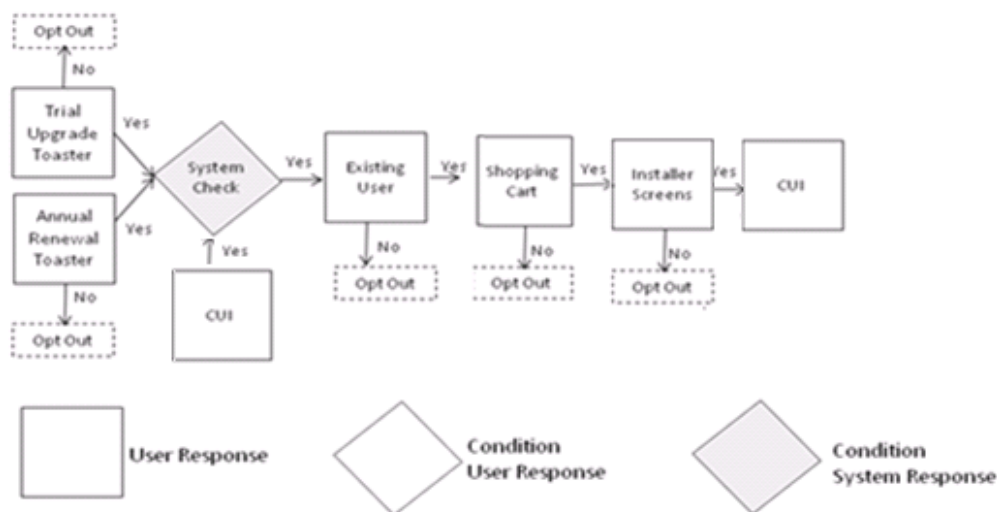


The user must input the user name and password created during the installation for a successful uninstall.

The **Cancel** button will open a Cancel Warning Window. If the Installer shortcut is populated because of HDD recovery (OEM factory image restore), then the shortcut will be removed.

Note: Authorization Flag (AF) flag is not removed after FS un-installation. This is protecting from license misuse. The use case is where the user installs, uninstalls and tries to reinstall before the term expires -- in this case we should validate AF during reinstall.

10.2 Conversion Trial and Paid Flows

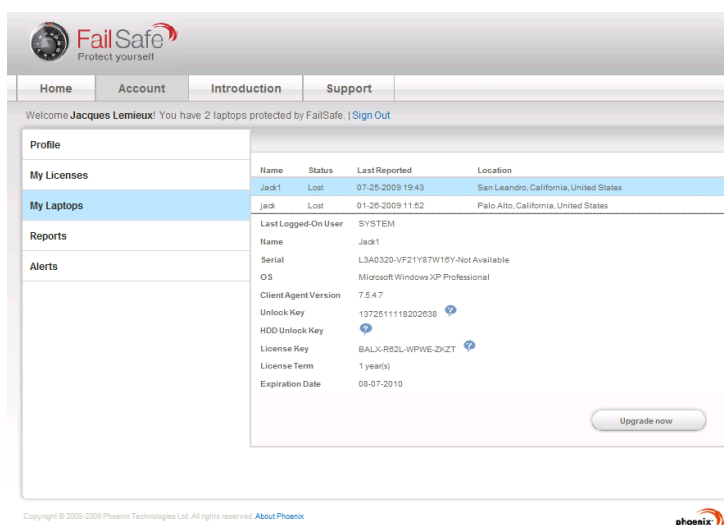


10.2.1 FailSafe Consumer Server Login within the Product Upgrade

The user can “buy” or upgrade their package by buying within the product. The first step is to login within the product via the UI.

As discussed earlier in this document, OEM specific logo treatment, colors, messaging and terminology will be used on the web-based login banner. The rest of the windows/webpage’s will use the FailSafe generic template and “computer” terminology consistent with the package used.

10.2.2 My Laptops



No change to existing functionality.

User selects on the **Buy** tab for trial-to-paid conversion and a FailSafe license upgrade. Selecting the Buy tab directs to the Shopping Cart.

10.2.3 Shopping Cart

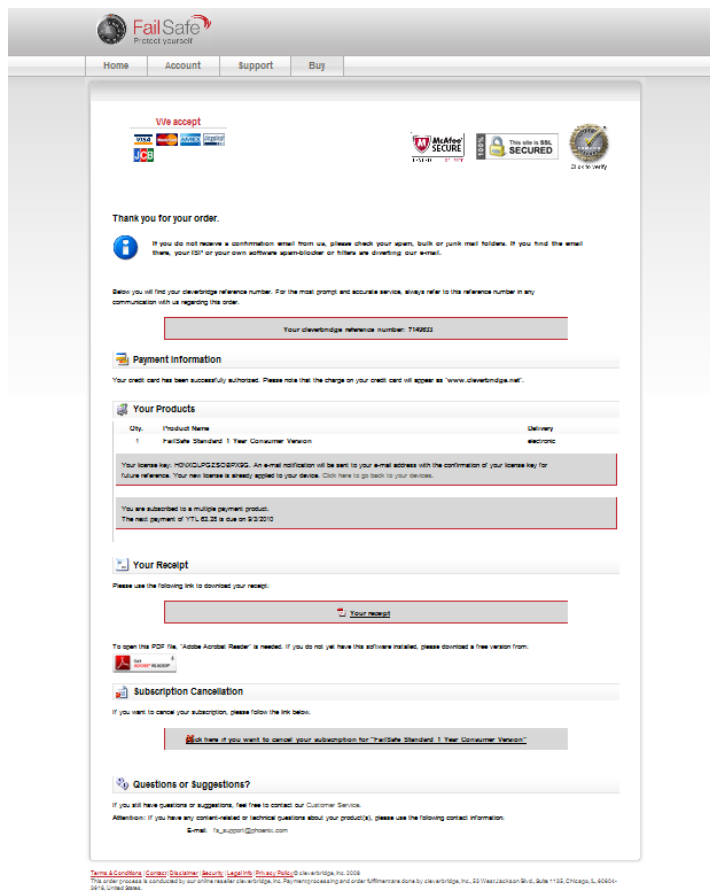
The screenshot shows the Phoenix FailSafe Shopping Cart interface. At the top, there is a navigation bar with links for Home, Account, Support, and Buy. Below the navigation bar, there are logos for 'We accept' (Visa, MasterCard, American Express, Discover) and 'McAfee SECURE' (This site is 100% SECURED). A language dropdown menu is set to 'English'. The main section is titled 'Your Shopping Cart' and contains a table with the following data:

Product Name	Delivery	Unit Price	Qty.	Price
FailSafe Enhanced by * FailSafe Enhanced by * FailSafe Enhanced by * FailSafe Enhanced by * FailSafe Enhanced by	electronic	\$58.85	1	\$58.85
Total:				\$58.85

Below the cart table, there is an 'Address' section with the heading 'Please enter your address information below:'. It contains fields for Company, First Name, Last Name, Address, City, State (dropdown), Zip/Postal Code, and Country (dropdown). Below the address section, there is a 'Payment Options' section with the heading 'Please choose your payment option here:'. It contains fields for Select currency (dropdown) and Select payment option (dropdown). A 'Next' button is located at the bottom right of the form. At the bottom of the page, there is a small footer with links for Terms & Conditions, Contact Us, Privacy Policy, and a copyright notice for Phoenix Technologies Ltd. 2008.

The shopping cart provides OEM SKU choices, including any available Intel AT SKUs after the system check. Refer to OEM SOW or OEM contract for package details for the defined SKUs.

21.1.3 Confirmation Page



The Confirmation page provides an order confirmation with a reference number.

10.3 Licensing

With subscription term or trial expiration FailSafe will be uninstalled after a grace period. Refer to Toaster alert section for details.

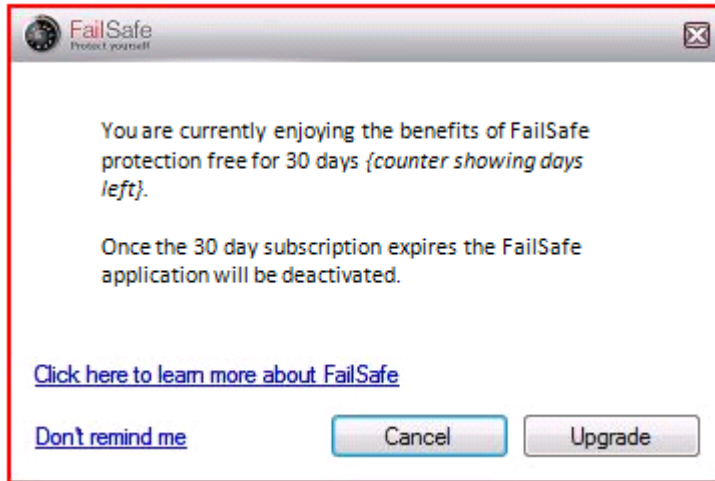
11 Toaster Alerts

There are six types of Toaster Pop-up alerts defined for FailSafe:

- “Try Me” alert
- “Trial” alert
- “Expired” Trial alert
- “Annual Renewal” alert
- “Annual Renewal Expired” alert
- “Product update” alert
- “Promotions” alert

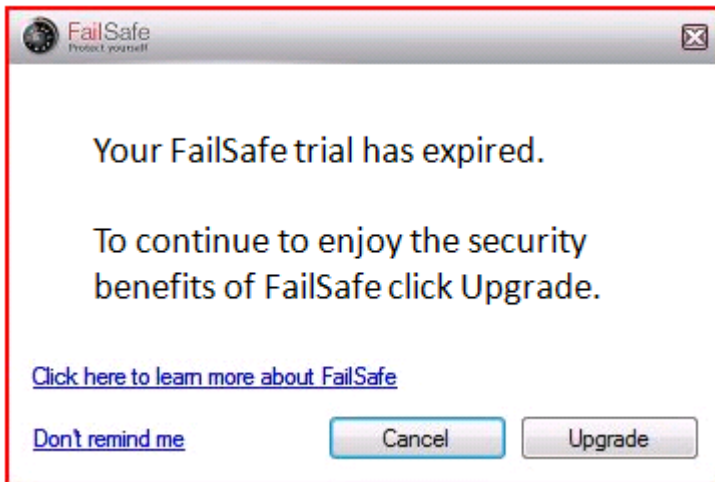
11.1 Try Me Toaster Alert

This toaster alert is designed as a replacement or in addition to a FailSafe desktop icon. General rules for all toaster alerts are that pop-ups will come up from the bottom right system tray after a 60-second time delay to allow for Internet connections to load. The popup duration is 30 seconds. The user can also close the toaster window by clicking the top right box. If the product is uninstalled, then the customer will see no toaster alerts of any kind. The user should only see the toaster after booting or once per day. The toaster application will be full-screen aware. Upgrade should be the default highlighted button.



11.2 Trial Toaster Alert

This toaster will generate alerts at 25, 27, 28, and 30 days. The Trial product will stop working after 30 days. Upgrade should be the default highlighted button.



11.3 Expired Toaster Alert

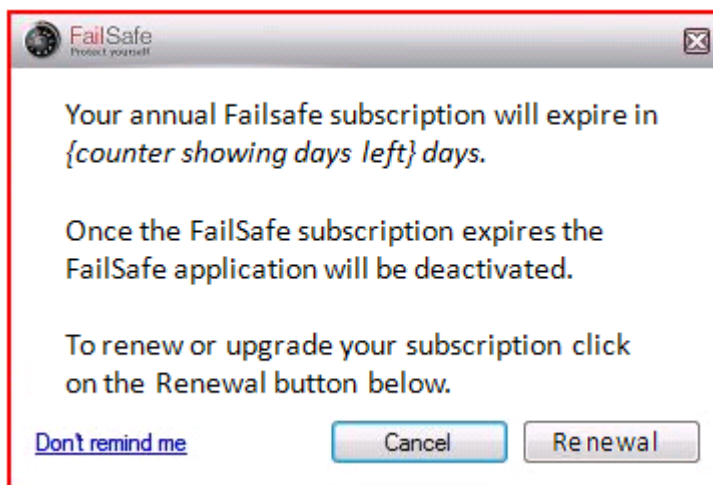
The Trial product will not work, but the trial customer will get Toaster alerts at 15 and 20 days if the product is not uninstalled. The Toaster gets its date information from the FailSafe

server. “Deactivate” is defined as a state where the server will respond, but with an empty response. The “Upgrade” link directs the user towards to the FailSafe shopping cart, where the user will see the list of full paid subscription packages. There should be no need for the trial user to log in. After 21 days from the start of a trial subscription, the Expired Trial alerts will stop being generated. The grace period is defined as the 5 days after the trial license Expires. Upgrade should be the default highlighted button.



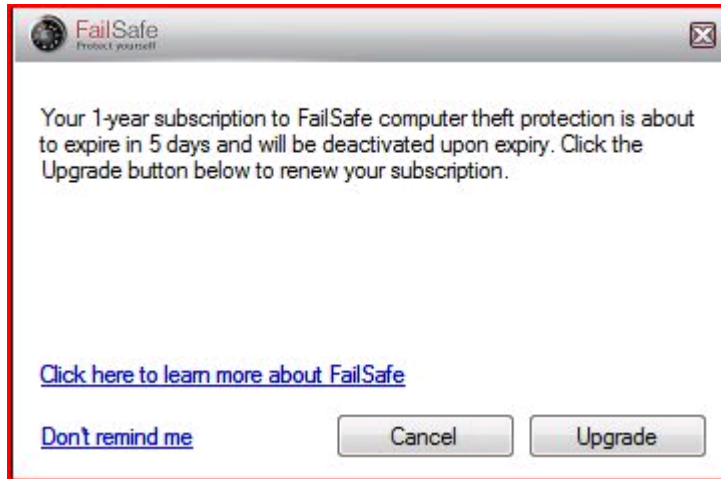
11.4 Annual Renewal Toaster Alert

“Your annual FailSafe subscription will expire in {counter showing days left} days. Once the FailSafe subscription expires, the FailSafe application will be deactivated.” The toaster will be generated at subscription expiry less 26, 16, 5, 2 and 1 day(s). The product will stop working after 375 days (365 + 10 days grace), but the customer can still browse the FailSafe Server. After expiry of the subscription, the alerts will stop being generated. The “Renewal” link directs towards the OEM or to the FailSafe shopping cart. Renewal should be the default highlighted button.



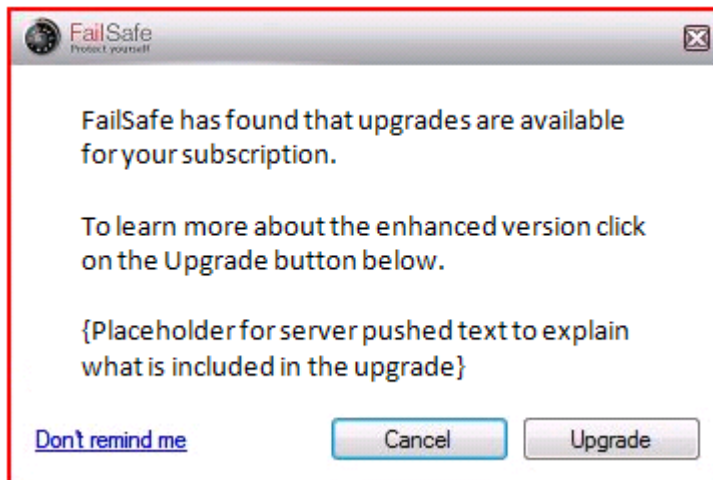
11.5 Expired Annual Toaster Alert

Expired” annual alerts begin after subscription expiration at 1st and 10th day, then 1 time every month thereafter for 12 months if the product is not uninstalled. The “Renewal” link directs towards the FailSafe shopping cart where the user will see the list of full paid subscription packages. The “Don’t remind me” button will be shown after 1 month-12 months. Upgrade should be the default highlighted button.



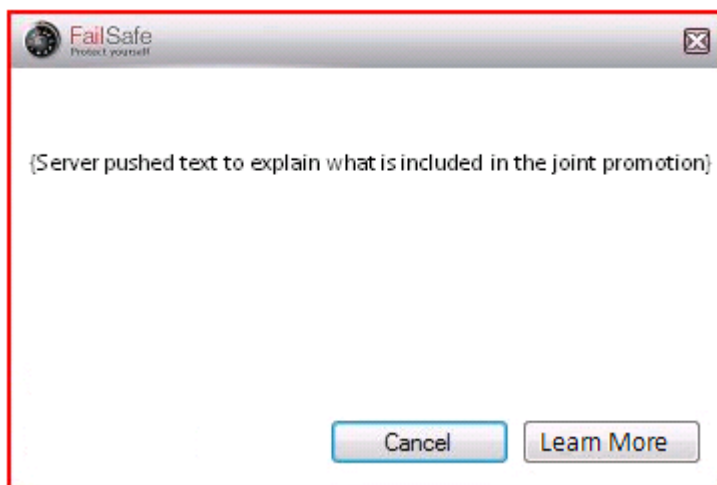
11.6 Product Upgrade Toaster Alert

The Product Upgrade toaster alert can be triggered by Phoenix for major product upgrades. The toaster provides a link that directs the user towards the OEM FailSafe Packages on the shopping cart, where the user will see the list of full paid subscription packages. Upgrade should be the default highlighted button.



11.7 Product Promotion Toaster Alert

The Product Upgrade toaster alert can be triggered by Phoenix for joint OEM/Phoenix commercial programs. Learn More should be the default highlighted button.



12 Breakfix Scenarios

12.1 Prerequisites for the breakfix scenario support

With AT this is handled at the OEM level and only when the device is not in stolen state. FailSafe Breakfix support remains the unchanged.

13 Localization

FailSafe Server, Installer, Documentation will be supported in the following languages:

- Japanese (not a Dell requirement)
- English
- French
- Italian
- German
- Spanish
- Danish
- Dutch
- Finnish
- Swedish
- Norwegian
- Korean (not a Dell requirement)
- Simplified Chinese
- Traditional Chinese
- Brazilian Portuguese

14 Target Operating System Support

- Windows XP Home SP3+
- Windows XP Prof SP3+

- Windows Vista Ultimate SP2+ (32-bit) and (64-bit)
- Windows Vista Home Premium SP2+ (32-bit) and (64-bit)
- Windows7 Ultimate (32-bit) and (64-bit)
- Windows7 Starter (32-bit) and (64-bit)
- Windows 7 Premium (32-bit) and (64-bit)

15 Target Browser Support

- Internet Explorer 7
- Internet Explorer 8

16 Third-Party Applications Support

16.1 Anti-virus coexistence

FailSafe Client modules are whitelisted in Trend Micro and McAfee. In the case of “high” security settings, the user might be prompted to allow FailSafe modules to run. AV patterns are updated automatically to cover a whitelist update for FailSafe entitlement and don’t require additional actions from user.

16.2 Two-factor authentication solutions

Two-factor authentication, such as fingerprint authentication, will not impact FailSafe.

17 Documentation

FailSafe provides Online Help, Getting Started Guide, User Guide and FAQs on the FailSafe Server

18 Technical Support

Technical support is contingent on OEM contractual terms and conditions and is outside the scope of this doc. Typically it is covered in the contract or SOW.

19 Competitive Matrix

Information about AT 2.0 needs to get added as we learn more about our readiness and the specifics of Absolutes readiness.

Feature Set		Phoenix FailSafe Consumer	Absolute Computrace Complete
BIOS Client Features	Remote BIOS based Disable/Lock		
	BIOS Level HDD protection		
	Client Persistence		
Intel AT 1.0	Disable using AT		
Intel AT 2.0	Disable using AT		
	Reactivation (SMS, PDA)		
	Detect (Audit, Logs)		
	Custom Message		
Features	IP Trace		
	GPS		
	Webcam		
	Remote Delete		
	Remote Retrieve		
	Wifi		
Web Console	Flexible Remote Policy Enforcement		
Try and Buy			
Localization Coverage		English, French, Spanish, Italian, German, Swedish, Norwegian, Dutch, Danish, Finnish, Braz. Port., Traditional Chinese, Simplified Chinese	English, French, Italian, German, Spanish and Portuguese

20 Open Items

- Need to collect Ericsson WWAN card share
- Need to start 3rd party engagement on SMS
- Absolute AT 2.0 competitive information needs to get added
- Need to identify target platforms for reference to OEMs/ODMs

21 Definitions, Acronyms, Abbreviations

AES	Advanced Encryption Standard
AF	Authorization Flag
AK	Activation Key (embedded in FailSafe PreInstaller)
AR	Application Router
AT	Intel® Anti-Theft
BIOS	Basic Input Output System
CryptOSD	Phoenix Driver that provides communication between OS and BIOS. WHQL certified.
CTO	Configure To Order
DC	Data Center
FE	Front End Server
FSS	FailSafe Server
Heartbeat	Calling special API in BIOS
MUID	Machine Unique Identifier
NTFS	http://en.wikipedia.org/wiki/NTFS
POST	Power On Self Test
SaaS	Software as a Service
SDM	Secure Data Manger (SDM) is Data storage in the BIOS
Signal	Sending XML data to FSS
SKU	Stock Keeping Unit
SMM	System Management Mode
SMRAM	System Management RAM
SN	Unique Serial Number
Speke	Simple Password Exponential Key Exchange (SPEKE) is a cryptographic method for password-authenticated key agreement