Customer Center User Guide

AbsoluteSoftware

www.absolute.com

May 3, 2011

Customer Center User Guide 5.4.5 - Documentation Release 1

This document, as well as the software described in it, is confidential and contains proprietary information protected by non-disclosure agreements. No part of this document may be reproduced in any form or disclosed to any party not bound by a non-disclosure agreement without the express written consent of Absolute® Software Corporation.

Absolute Software Corporation reserves the right to revise this document and to periodically make changes in the content hereof without obligation of such revisions or changes unless required to do so by prior agreement.

Information contained herein is believed to be correct, but is provided solely for guidance in product application and not as a warranty of any kind. Absolute Software Corporation assumes no responsibility for use of this information, nor for any infringements of patents or other rights of third parties resulting from the use of this information.

Absolute Software Corporation, Suite 1600, Four Bentall Centre, 1055 Dunsmuir Street PO Box 49211 Vancouver, British Columbia, Canada V7X 1K8.

Table of Contents

Chapter 1 Introduction

Since 1993, Absolute Software has helped organizations overcome the security risks and asset management challenges associated with the ownership and maintenance of large numbers of devices: remote, mobile, or desktop. The company's unique, patented technology platform and the user-friendly Customer Center let system administrators to manage their Information Technology (IT) assets.

The technology platform is a client/server architecture that delivers Absolute Software's computer security, data security, and asset management products as standalone products or as a part of a complete package. The communication between the secure, patented Agent software and the Monitoring Center ensures organizations have secure access to up-to-date information about their entire IT inventory. Authorized users can utilize the built-in Customer Center tools to track assets, report lost or stolen devices, and initiate Data Delete operations.

Customer Center is designed to help system administrators track and monitor device assets. This document describes how to access Customer Center using a Web browser to:

- Monitor assets and generate reports.
- Report a theft (only available to Computrace®Plus, Computrace®Complete, or Computrace®One™customers).
- Initiate Data Delete (only available to pre-authorized Computrace®Plus, Computrace®Complete, Computrace®Data Protection, or Computrace®One™ customers).
- Configure and administer user accounts.
- Define user and asset information.

NOTE To purchase Computrace®Plus, AbsoluteTrack, Computrace® for Netbooks, Computrace®Complete, or Computrace®Data Protection contact Absolute Software's sales department at sales@absolute.com.
Computrace®One™ is available in the EMEA region only. To purchase Computrace®One™ contact the Absolute Software EMEA sales department via e-mail at sales@EMEA.absolute.com.

Service Levels

Customer Center contains different levels of service: Computrace®Plus, AbsoluteTrack, Computrace® for Netbooks, Computrace® Data Protection, and Computrace®Complete. Depending on the level of service you have purchased, some Customer Center functionality and reports are not available.

For example, AbsoluteTrack and Computrace®Complete reports are unavailable to customers who have only subscribed to Computrace®Plus.

NOTE For purchase enquiries, contact Absolute Software's sales department by e-mail at sales@absolute.com. For complete contact information, see "Technical Support" on page 15.

Computrace Plus

Computrace®Plus provides Theft Recovery, Data Protection, and basic Secure Asset Tracking™ reports. Computrace®Plus enables IT professionals to track their organization's device assets, recover lost or stolen machines, and remotely wipe sensitive data if a device is lost, stolen or nearing the end of its lifecycle.

Computrace®Plus reports are available to all customers. For more information about Computrace®Plus reports, see "Service Levels and Reports" on page 97.

Computrace for Netbooks

For netbooks using the Intel® Atom™ processor, Absolute Software provides basic Secure Asset Tracking™ (no geolocation capabilities) and up to five hours of Computer Theft Recovery services for lost or stolen devices.

AbsoluteTrack

AbsoluteTrack is an advanced Secure Asset Tracking™ solution for corporate, government, and education environments. Traditional asset management systems can lose track of IT assets such as laptops when they disconnect from the LAN or drift to unknown locations. With AbsoluteTrack, the Agent installed within the laptop reports changes in asset information on a daily basis regardless of location, letting IT departments to manage their entire device population, including remote and mobile assets centrally.

For more information about Absolute Track reports, see "Reports Reference" on page 97.

Computrace Data Protection

Computrace® Data Protection lets customers track stationary, remote, and mobile device assets and remotely wipe sensitive data if the device is lost, stolen or nearing the end of its lifecycle.

See "Service Levels and Reports" on page 97 for more information about AbsoluteTrack Reports.

Computrace Complete

Computrace®Complete is a comprehensive solution combining Computer Theft Recovery, Data Protection, and advanced Secure Asset Tracking. Computrace®Complete lets IT administrators centrally manage their assets by monitoring device movement, call history, asset leasing information, and software license compliance, and includes a Service Guarantee.

Computrace One

Computrace®One™ is a comprehensive solution for EMEA customers combining Computer Theft Recovery, Data Protection, and Secure Asset Tracking. Computrace®One™ lets IT administrators centrally manage their assets by monitoring device movement, call history, asset leasing information, and software license compliance.

Computrace®One does not offer a Service Guarantee.

NOTE For Computrace®One™ sales enquiries contact the Absolute Software sales department via e-mail at sales@EMEA.absolute.com. For complete contact information, see "Technical Support" on page 15.

For more information about reports available to AbsoluteTrack, Computrace®Complete, Computrace® Data Protection, and Computrace®One™ customers, see "Service Levels and Reports" on page 97.

Audience and Usage

Who Should Use this Guide

The Customer Center User Guide is designed to instruct system administrators in using the Customer Center to manage IT assets, report device loss or theft, and manage Data Delete operations. This guide includes detailed information on various tools and functionalities available to authorized users.

Using this Guide

"Accessing Customer Center" on page 17 — lists the minimum hardware and software requirements, describes the methods to access Customer Center, and discusses the Security Administrator role for use with data and device security operations.

"Generating Reports" on page 90 — describes the procedures required to generate basic and customized reports based on the data collected from monitored assets.

"Reports Reference" on page 97 — describes the various reports available in Customer Center.

"Administration" on page 35 — describes the Customer Center Administration tab and procedures required to set event alerts and define user and asset information.

"Using Intel Anti-Theft Technology" on page 144 — describes the advanced Intel Anti-theft Technology feature and the procedures required to install and configure it.

"Theft Reporting" on page 172 — describes the procedures required to report the loss or theft of monitored assets as well as view and manage theft reports.

"Using Data Delete" on page 178 — describes the Data Delete functionality and the procedures required to launch and manage Data Delete operations.

"Managing Geofences" on page 195 — describes the Geofencing functionality and the procedures to be followed to manage Geofencing boundaries.

"Using Device Freeze" on page 202 — describes the Device Freeze functionality, including initiating freeze requests and creating custom freeze messages for regular and Lenovo Lost and Found accounts.

"Managing Encryption" on page 219 — describes the Volume Encryption functionality including setting encryption defaults at the account and device group level and managing encrypted volumes on devices containing encryption.

"User Access Rights" on page 242 — outlines the different access rights and the functions of the major Customer Center user groups.

"Theft and Service Guarantee Submission Checklist" on page 244 — lists the process to be followed to submit a Theft Report to Absolute Software.

"Installing and Activating the Intel Anti-Theft Technology Feature" on page 245 — describes best practices you should follow when installing and activating Intel AT on devices.

"Intel Anti-theft Technology Error Codes" on page 248 — describes common errors that can occur during different Intel AT processes.

Conventions Used in this Guide

- Directory, file names, field names, and screen objects are shown in bold. Examples:
  - In Windows XP, the file **notepad.exe** is located in the **windows\system32** directory.
  - **UserID** — enter your user identification number in this field
  - Click **Apply**.
- Computer input and output, such as sample listings, messages that are shown on-screen, and typed commands or statements, are shown in Courier typeface. Example:
  `Type lanmake ctinst.txt`

Global Navigation

Navigation Bar

All pages in Customer Center contain a global navigation bar on the left. This bar contains links that let you navigate from one section to another with a few clicks.

To get a full view of any page, you can click the grey button on the immediate right of the navigation bar. It has an arrow pointing to the left by default. When you click this button, the global navigation bar is hidden. To restore the page to its original state, click the grey button again.

The navigation bar contains the following links:

- **Reports** — This link gives you access to the different reports in Customer Center. See "Reports Reference" on page 97.
- **Administration** — This link lets you set event alerts and define user and asset information. The Administration area also lets you manage self-serve Agent Removal requests using the Create and Edit Agent Removal Requests pages. See "Administration" on page 35 for more information.
- **Data and Device Security** — This link lets you perform security activities such as Data Delete, Device Freeze, and Intel® Anti-theft Technology (AT). See "Using Data Delete" on page 178, "Using Device Freeze" on page 202, and "Using Intel Anti-Theft Technology" on page 144 for more information.
- **Theft Report** — This link lets you create, view, and modify Theft Files. See "Theft Reporting" on page 172 for more information.
- **Custom Pages** — This link gives you access to any special functionality available for your account.

  NOTE The **Custom Pages** link and area is only available for accounts with specially modified functionality (built under contract).

- **Documentation** — This link opens the Documentation page, listing all the important Customer Center documentation. The Documentation page lists documents sorted alphabetically depending upon the locale set for the logged in user. Click the appropriate link on the Documentation page to view the preferred document.
- **Support** — This link opens the Support page that provides some helpful links and a form to submit a support case. See "Technical Support" on page 15 for more information.
- **Training Services** — This link opens the Training Services pages that gives you access to the personal training services provided by Absolute Software.

Other Links

All pages in Customer Center contain the following links at the top of the page:

- **My Profile** — This link opens the Manage User Profile page. See "Editing Your User Profile" on page 28 for more information.
- **Documentation** — This link opens the Documentation page that lists all the important Customer Center documentation. Click the appropriate link on the Documentation page to view the preferred document.
- **Support** — This link opens the Support page that provides some helpful links and a form to submit a support case. See "Technical Support" on page 15 for more information.
- **Logout** — This link logs you out of Customer Center and returns you to the Customer Center Login page.

All pages in Customer Center also contain the **Absolute Software Corporation** link at the bottom right. This link opens the Absolute Software Web site.

Technical Support

If you have difficulty using Customer Center or installing the Agent contact Absolute Software Technical Support. We welcome your questions, comments, and feature requests.

IMPORTANT Security Administrators can now use the self-serve Agent removal feature available in the Administration area to remove the Agent from one or more managed devices. For more information about the self-serve Agent removal feature see "Managing Agent Removal Requests" on page 85.

To contact support:

1. Click the **Support** link on the global navigation bar or at the top of any page in Customer Center. The Support page opens.
2. In the **Submit a Support Case** area, provide the following details, and then click **Submit**:

- **Problem Title** constitutes the heading of the message sent to Technical Support.
- **Problem Description** provides detailed information about the issue for which you are contacting Technical Support.

  IMPORTANT Problem Description is a mandatory field. A warning message shows if you try to submit a support case without a description.

- **Error Message** allows you to add information about any system notifications, errors, or warnings you may have encountered along with the problem.
- **Problem Severity** helps Technical Support to determine the urgency and impact of the problem. See the *Global Support Guide* available on the Documentation page of Customer Center for more information.
- **Problem Type** directs the issue to the appropriate Support Representatives for timely solution.
- **Operating System** provides specific information about the OS of the device where the problem occurred and hence also the Agent present on the device.
- **Attachments** allows you to add any supporting documents or images further describing the issue.

  NOTE Attachment size cannot exceed 4096 Kilobytes (4 Megabytes or MB) per attachment or 12 MB in total.

  Customer Center sends a message to Absolute Technical Support including the details about your problem. Technical Support contacts you if more details are necessary and/or when a solution to your problem is available.

NOTE You can also contact Absolute Software Technical Support from the Absolute Software Web site at http://www.absolute.com/support. Please follow the on-screen instructions to contact technical support for your region.

Chapter 2 Accessing Customer Center

This chapter introduces you to Customer Center and describes the following basic functionality:

- System Requirements
- Real-time Technology and components
- Data and Device Security Administration
- Logging In
- Retrieving Lost or Forgotten Passwords
- Using the Home Page
- Downloading the Agent
- Data and Device Security Administration

System Requirements

- **Internet access** — Customer Center is not available in offline mode, and Internet access is required.
- **Browser support** — Customer Center supports the following browsers:
    - Internet Explorer (current and previous versions)
    - Safari (current version)
    - Firefox (current Mac and Windows versions)
- **Screen resolution** — The minimum supported resolution is 1024 x 768 pixels. Customer Center pages automatically scale to fit screens with higher resolutions.

Prerequisites For Using Real-time Technology (RTT)

What is Real-time Technology?

Real-time Technology (RTT) allows users to better track their mobile broadband-enabled devices. Additionally, RTT leverages mobile broadband and SMS messaging, also known as text messaging, to dramatically increase the performance of the Computrace Asset Tracking and Recovery features.

RTT encompasses the following three features:

- **Mobile Broadband Adapter Tracking (MBAT)**: MBAT permits Computrace customers to view a list of mobile broadband adapters and their attributes including equipment, subscriber, and network information in Customer Center. MBAT is a unique feature allowing

Computrace customers to track and manage devices using mobile broadband adapters and data plans in their asset base.

- **Monitoring Center-initiated Calling (MCIC)**: MCIC allows customers to remotely initiate a Computrace Agent call using Customer Center. Monitoring Center-initiated calling, under specific circumstances, enables a drastic reduction in the time required to initiate action on the target device. For example, MCIC can be used to initiate Data Delete, Device Freeze, and Intel AT operations on the target device within minutes of submitting a request in Customer Center. MCIC also enables near real-time geolocation updates and tracking for the asset. In the absence of MCIC, each of these operations will only start at the next scheduled Agent call. Under some circumstances, MCIC also permits communications with computers that do not have an active IP connection.
- **Intel Anti-Theft (AT) SMS Lock Requests**: Customers with newer devices equipped with mobile broadband adapters have an additional feature available. RTT supports a direct Intel AT lock-down of such devices via a sequence of SMS messages. No Agent call is required in this case and consequently the lock happens even faster than via MCIC.

System Requirements

- **Operating System** —The target device must have one of the following Operating Systems installed:
  - Windows XP (32-bit editions only)
  - Windows Vista (any 32-bit or 64-bit edition)
  - Windows 7 (any 32-bit or 64-bit edition)

  NOTE Currently, RTT and MCIC technology is not available for devices with Macintosh, Linux, BlackBerry, Windows Mobile or S60 Agents. RTT and MCIC technology is also not available for target devices running Computrace Manage.

- **Processor** — The target device must have one of the following processors:
  - Intel Core i3
  - Intel Core i5
  - Intel Core i7
  - Intel Core i7 Extreme

  NOTE If the target device does not run on one of the above mentioned processors, you can still use MCIC to lock the device with Intel AT faster than the time required to lock it with an Agent call.

- **Computrace Agent** — The target device must have an active Computrace Agent Version 857 or higher installed and regularly calling in to the Absolute Monitoring Center.

  NOTE We highly recommend using Computrace Agent Version 885 or later, since such devices have a higher call success rate over cellular data connections.

- **Broadband Adapter** — The mobile broadband adapter installed on the target device must be one of the following models or a close variant:
  - **Gobi** — 1000, 2000, and variants
  - **Ericsson** — F3507g, F3607gw
  - **Novatel** — Wireless mobile broadband adapters
  - **Sierra** — Wireless UMTS, MC5720, and MC 5725

    See "Supported Mobile Broadband Adapters" on page 19 for a complete list of mobile broadband adapters supported.

- **Valid Data Subscription With SMS Support**: The target device must have a valid mobile data subscription that supports SMS messaging. We now use Clickatell's SMS gateway for RTT features. Refer to the following link for a list of Clickatell coverage areas for mobile terminated messages: http://www.clickatell.com/pricing/standard_mt_coverage.php?region=.

IMPORTANT Before using RTT, ensure that the target device has an active Agent regularly calling in to the Absolute Monitoring Center. Additionally, you should be able to establish a data connection and send and receive SMS messages using the “watcher application” provided with your mobile broadband adapter. Refer to the instructions provided with your mobile broadband adapter or the device for more information.

Supported Mobile Broadband Adapters

The following mobile broadband adapters are supported:

NOTE Some OEM-branded variants of the following mobile broadband adapters may be supported as well.

- **Gobi 1000** — an embedded mobile broadband adapter available on UMTS and EVDO networks. Including the following Gobi variants:
  - Qualcomm UNDP-1
  - Qualcomm 9202
  - Dell 5600
  - HP un2400

- **Gobi 2000** — an embedded mobile broadband adapter available on UMTS and EVDO networks. Including the following Gobi variants:
  - Qualcomm 920b
  - HP un2420
- **Ericsson F3507g** — an embedded UMTS mobile broadband adapter
- **Ericsson F3607gw** — an embedded UMTS mobile broadband adapter
- **Novatel Wireless mobile broadband adapters** on UMTS and EVDO networks
- **Sierra Wireless Mobile Broadband Adapters** — mobile broadband adapters on the UMTS and CDMA/EVDO networks
  - Sierra Wireless UMTS mobile broadband adapters
  - Sierra Wireless MC5720 — an embedded CDMA/EVDO mobile broadband adapter
  - Sierra Wireless MC5725 — an embedded CDMA/EVDO mobile broadband adapter

To successfully receive and process Real Time Technology (RTT) and Monitoring Center Initiated Calling (MCIC) features such as SMS messages and Intel® AT SMS Lock Requests, the target device must be powered on and the mobile broadband adapter on the device must be:

- Powered on
- Associated with an active SMS service
- In the network coverage area

If the device or mobile broadband adapter is off or out of the network coverage area, the Intel® AT SMS Lock Request is delivered when the device and adapter are powered on and in the network coverage area.

See "Mobile Broadband Adapter Report" on page 103 for more information about searching for devices in your account with mobile broadband adapters. See "Sending Intel AT SMS Lock Requests" on page 166, "Forced Call Log" on page 67, and "Initiating a Forced Call" on page 67 for more information about the MCIC features such as SMS messages and new Intel AT features such as SMS Lock Requests.

Supported Platforms

The Agent is supported on the following platforms:

- Windows Operating Systems:
  - Windows 2000 Service Pack 4
  - Windows XP Service Pack 2 and higher (32-bit versions)
  - Windows Vista (32-bit and 64-bit versions)

    - Windows 7 (32-bit and 64-bit versions)
    - Windows Server 2003 (32-bit versions)
    - Windows Server 2008 (32-bit and 64-bit versions)
    - Windows Server 2008 R2
- Mac OS X v10.3.9 and higher
- Linux-based Operating Systems:
    - RedHat Enterprise Linux 5, Centos 5
    - Fedora 11 and 12
    - openSUSE 11.1 and 11.2
    - Debian 5.0.3
    - Ubuntu 8.04, 9.04, and 9.10
    - Mint 9.10
- Windows Mobile 5.0 and Windows Mobile 6
- Netbooks using the Intel® Atom™ Processor

Logging In

To ensure only authorized users have access to customer data, each registered user must log in to access Customer Center. To access Customer Center:

1. From Absolute Software's home page at www.absolute.com, click **Login** to open the login page.
2. Click the **Customer Center** link to open the Customer Center Login page. The current Customer Center version number shows on the bottom right corner of the Login page.

   IMPORTANT If your organization hosts its own Customer Center, consult your system administrator for the correct URL.

3. Enter your Username (not case sensitive) and Password.

   NOTE The Password field is case sensitive. Ensure that you enter the Password in the correct case.

4. Click **Login**. If your username and password combination is correct, the Customer Center home page opens.

Selecting the Language

Customer Center supports the following languages:

- English

- French
- Italian
- German
- Spanish
- Portuguese
- Chinese (Traditional)
- Chinese (Simplified)
- Japanese
- Korean

To select a language, click the language list located at the top of the Login page. When you select a language, the page refreshes to show in the new language.

NOTE All Customer Center pages scale to accommodate the changes in text size due to language changes.

Retrieving Lost or Forgotten Passwords

If you are a registered user and attempt to log in with an incorrect password, you receive a message stating an incorrect username or password was entered.

To reset a lost or stolen password:

1. On the Login page, click the **Forgot your Password** link. The Retrieve Password page opens.
2. Enter the Username you used when registering the software in the **Username** field.
3. Enter the e-mail address associated with your username and used when registering the software in the **E-mail** field.
4. Click **Submit**. Absolute Software Technical Support generates a new password and sends it to the e-mail address associated with your Username.

Using the Home Page

After you log in, the Customer Center home page opens. The Customer Center home page is dynamic, enabling you to gather all pertinent information such as account related messages, action items, and a summary of your account activity at a single glance.

The home page contains two distinct areas showing information related to your account:

- "Recent Announcements" on page 24
- "Dashboard" on page 24

In some cases, after you log in, an Announcements dialog box opens to inform you of items that need your immediate attention. See "Announcements Dialog Box" on page 23 for more information. For Dell ProManage accounts, the home page contains a set of quick links to the some of the most commonly used functionality in Customer Center. See "Dell ProManage — Quick Links page" on page 27 for more information.

Announcements Dialog Box

In some instances, a small splash screen or dialog box shows upon successful login. The Announcements dialog box provides a list of all action items that need your immediate attention, including items specific to you, your Customer Center account, and the Absolute products used in your account. The Announcements dialog box contains the following items that may be used for performing different actions:

- **OK** — acknowledges all the messages showing in the dialog box. See "Acknowledging Messages" on page 23 for more information.
- **Do not show again** — available only for non-mandatory messages, the **Do not show again** checkbox acknowledges the messages but does not indicate that you accept the message. The message is shown again upon the next login to Customer Center. See "Dismissing Messages" on page 23 for more information.
- ■ — closes the dialog box without saving any settings. See "Closing the Announcements Dialog Box" on page 24 for more information.

Acknowledging Messages

To acknowledge the messages and close the dialog box:

➢ Click **OK** to acknowledge all the messages showing in the dialog box. When you click **OK**, the messages are marked complete and the Announcements dialog box does not open again for these messages.

If there are new messages or announcements that apply to you or your Customer Center account, the Announcements dialog box may open again when you log in to Customer Center.

Dismissing Messages

To dismiss non-mandatory messages:

IMPORTANT The **Do not show again** box is only available for non-mandatory messages.

➢ Select the **Do not show again** box, and then click ■ to remove the message from the list of announcements showing in the dialog box. The Announcements dialog box may open the next time you log in to Customer Center, but the messages for which you selected the **Do not show again** box do not show again in the Announcements dialog box.

Closing the Announcements Dialog Box

To close the dialog box irrespective of the messages shown:

➢ Click ■. The dialog box closes. When you log in to Customer Center again, the dialog box opens to show these messages again.

Recent Announcements

The **Recent Announcements** area of the home page lists any important messages from Global Support that apply to your account or user profile.

Dashboard

The **Dashboard** area of the home page shows the widgets available for your account. The dashboard widgets show important information relating to your account in an easy-to-use graphical interface. Depending upon your account and the service levels applicable to the account, one or more of the following widgets are available in the Dashboards area:

- **Agent Call Rate (Service Guarantee)** shows the Agent call statistics for devices in your account with a Service Guarantee. Click the appropriate call-in period to open the Asset Report page with the specific date ranges pre-populated in the **Most recent call** field and the value **Service Guarantee ESNs** selected in the **Device Group** field.
- **Agent Call Rate (All products)** shows the Agent call statistics for all devices in your account. Click the appropriate call-in period to open the Asset Report page with the specific date ranges pre-populated in the **Most recent call** field.
- **Agent Versions** shows the version numbers of the various Agents on your managed assets. Click the appropriate version number to open the Asset Report page with the selected version number pre-populated in the **Agent Version** field.
- **Active Products** shows the Computrace products active for devices in your account. Products are associated with Service Levels, which, in turn, dictate the functionality available for specific devices and groups. See "Service Levels" on page 11 for more information.
- **Anti-malware Summary** shows a summary of devices in your account containing detected anti-malware products and devices without any anti-malware products. The following actions are possible:

- ○ Click the appropriate **anti-malware product name** to open the Anti-malware Report page with the specific application or vendor name pre-populated in the **Application Vendor** field.
- ○ Click the area labelled **Missing Anti-malware** to open the Missing Anti-malware report.

- **License Summary** shows the available licenses within your account, compared to the number of licenses now in use. Clicking a license type opens the list of devices now using those licenses.

Using Widgets

Each widget contains a set of icons allowing you to refresh, close, or change the settings for the widget. Each widget contains the following icons:

- ⟳ — refreshes the widget by generating the latest data.
- 🔧 — opens the Widget Settings dialog box allowing you to manage display settings for the widget. See "Customizing Widgets" on page 26 for more information.
- ✖ — closes the widget. You can show the widget again by enabling it in the Add/Remove Widgets area. See "Showing or Hiding Specific Widgets" on page 25 for more information.

  NOTE You cannot close mandatory widgets.

Showing or Hiding Specific Widgets

The Add/Remove Widgets area allows you to show or hide specific non-mandatory widgets.

To show a specific widget:

1. In the Dashboard area on the home page, click the **Add/Remove Widgets** link. The Dashboard area expands to show a series of checkboxes and buttons.
2. Select the checkboxes for the specific widgets you want to add to the view.
3. Click **Apply**. The Dashboard refreshes with the new widgets showing.

To hide specific widgets:

1. In the Dashboard area on the home page, click the **Add/Remove Widgets** link. The Dashboard area expands to show a series of checkboxes and buttons.
2. Clear the checkboxes for the specific widgets you want to hide.
3. Click **Apply**. The Dashboard refreshes without the selected widgets showing.

Customizing Widgets

The Widget Settings dialog box allows you to specify various display options for the selected widget.

To change the settings for each widget:

➢ Click 🔧 on the widget. The Widget Settings dialog box for the specific widget opens. Refer to the specific descriptions in the following sections for each Settings dialog box, for more information about the options available.

To move the position of the widget:

➢ Click and drag the title bar of the widget to the preferred location. The widget moves to the new location.

Agent Call Rate (Service Guarantee) Settings

The Agent Call Rate (Service Guarantee) Settings dialog box offers the following options:

- The **Chart Options tab** containing:
  - **Chart Type** — choose the type of graph from Pie, Bar, or Column
  - **Chart Palette** — select the color scheme associated with the graph
  - **Show as 3d** — show the graph with three-dimensional effects
  - **Show percent** — show percentage values

    NOTE showing percentage values applies only to pie charts.

- The **Chart Data** tab containing:
  - **Day ranges** — specify the number of days for which the data is shown on the graph. Separate multiple day range numbers with a comma.

  NOTE By default, dormant devices are excluded from the chart data. To include dormant devices, select the **Include Dormant Devices** checkbox located at the bottom of the tab.

Agent Call Rate (All products) Settings

The Agent Call Rate (All products) Settings dialog box is similar to the Agent Call Rate (Service Guarantee) settings dialog box. See "Agent Call Rate (Service Guarantee) Settings" on page 26 for more information.

Agent Versions Settings

The Agent Versions Settings dialog box contains a single tab called Chart Options and is similar to the Chart Options tab for the Agent Call Rate (Service Guarantee) settings dialog box. See "Agent Call Rate (Service Guarantee) Settings" on page 26 for more information.

Active Products Settings

The Active Products Settings dialog box contains a single tab called Chart Options and is similar to the Chart Options tab for the Agent Call Rate (Service Guarantee) settings dialog box. See "Agent Call Rate (Service Guarantee) Settings" on page 26 for more information.

Anti-malware Summary Settings

The Anti-malware Summary Settings dialog box contains a single tab called Chart Options and is similar to the Chart Options tab for the Agent Call Rate (Service Guarantee) settings dialog box. See "Agent Call Rate (Service Guarantee) Settings" on page 26 for more information.

License Summary Settings

The License Summary Settings dialog box contains a single tab called Chart Options and is similar to the Chart Options tab for the Agent Call Rate (Service Guarantee) settings dialog box with one difference. The License Summary Settings dialog box does not contain a checkbox to show percentage values. See "Agent Call Rate (Service Guarantee) Settings" on page 26 for more information.

Dell ProManage — Quick Links page

For all Dell ProManage accounts, the Quick Links page shows upon successful log in. The Quick Links page includes the following links:

- **Create and Edit Theft Report** allows filing of a Theft Report and reporting a device as stolen. See "Making a New Report" on page 175 for more information.
- **Request Data Delete for one or more files on a device** opens the Request Data Delete page to initiate a Data Delete request. See "Requesting a Data Delete Operation" on page 179 for more information.
- **Create a Device Freeze Request** allows freezing a device. See "Requesting a Device Freeze" on page 203 for more information.
- **Read the User's Guide** opens the Customer Center User Guide.

To return to the Quick Links page:

1. On the global navigation bar, click the **Home** link to expand the menu. The Quick Links menu item shows on the global navigation bar.
2. Click the **Quick Links** menu item. The Quick Links page opens.

Downloading the Agent

The Customer Center home page includes a link called **Download Packages** located in the Helpful Links area under the Dashboard.

IMPORTANT Security Administrators can now use the self-serve Agent removal feature available in the Administration area to remove the Agent from one or more managed devices. For more information about the self-serve Agent removal feature see "Managing Agent Removal Requests" on page 85.

To download the Agent:

1. Click the **Download Packages** link. The Download Packages page opens with a list of all versions of the Agent that are created for your account.
2. Click the appropriate link to download a specific version. Please refer to "Downloading the Agent" on page 81 for more information.

Editing Your User Profile

The Profile page, also known as the Manage User Profile page, contains all the basic information on the account owner. The Manage User Profile page lets you edit the following details:

- User details
- User system settings

Editing User Details

The User Details section contains the following information:

- **Account ID**
- **E-mail**
- **Username**
- **First Name**
- **Last Name**
- **Password** (contains link to “Change Password”)

You cannot edit the **Account ID** field is not editable. However, you can edit all the other files if necessary.

To edit **E-mail**, **First Name**, and **Last Name**:

1. Edit the appropriate field with the new value.

2. Click **Save Changes**. The changes are saved and the Customer Center home page opens.

NOTE Contact Technical Support to edit the **Username**. For more information on how to contact Technical Support see "Technical Support" on page 15.

To change your login password:

1. Click the **Change Password** link. The Change Password dialog box opens.
2. Enter your existing password in the **Enter Current Password** field.
3. Enter a new password in the **Set New Password** field.

   IMPORTANT If your user account requires strong passwords and the new password does not meet these requirements, a warning message shows. The new password must be at least 8 characters long; and must contain a mix of upper and lower case alpha characters, numeric characters, or symbols.

4. Re-enter the password you entered earlier, in the **Confirm New Password** field.
5. Click **Save**. The Change Password dialog box refreshes to show a message confirming the changes you have made.
6. Click **Continue**. The Manage User Profile page opens.

Editing User System Settings

The User System Settings section contains the following editable information:

- Default User Language and Locale
- Default Timezone
- Default User Session Timeout

To edit these values:

1. Click the preferred list and select the appropriate value.
2. Click **Save Changes**. The Customer Center session re-initializes, sending you back to the login page.

NOTE If you select a new value for the Default User Language and Locale list, the date, time, and number formatting is automatically updated to match your selection.

Data and Device Security Administration

Customer Center offers several data and device security services that enable authorized Security Administrators to ensure that managed devices and the data contained on these devices are not compromised in case of device loss. The following data and device security services are available from the Data and Device Security option on the global navigation bar:

- Security Authorization
- Data Delete
- Device Freeze
- Intel® Anti-theft Technology (AT)
- Encryption
- File List
- Remote File Retrieval

Due to the destructive nature of these data and device security services, several security checks are implemented to ensure that the services are only initiated by authorized individuals and that they only run on correctly targeted devices:

1. Absolute Software must have a signed preauthorization agreement on file for your company.
2. Each data and device security operation must be authenticated using an RSA SecurID® Token or an e-mailed authorization code.
3. The device to be targeted with the security service must have an activated Agent with a unique Identifier.

Any Absolute employee, irrespective of their access rights, cannot start a data and device security operation. To invoke commands such as the Data Delete command, the customer needs their login, their password, and the unique password generated from their RSA SecurID® token or the Authorization Code received via e-mail.

Security Administrator Preauthorization Agreement

In order to use the data and device security services, Absolute Software must have a signed preauthorization agreement on file. The preauthorization agreement identifies the personnel in your company authorized to execute security operations and specifies the type of authentication method used by your company.

Downloading the Preauthorization Agreement

To download a blank copy of the preauthorization agreement:

1. Login to Customer Center.

2. Click the **Documentation** link on the global navigation bar.
3. In the **Service Request Forms** area, click the **Security Administrator Preauthorization Form** link.
4. The preauthorization agreement opens in PDF format. Complete the document, print it, sign it, and return it to Absolute Software:

   Absolute Software Corporation
   Suite 1600, Four Bentall Center
   1055 Dunsmuir Street PO Box 49211
   Vancouver, British Columbia, Canada
   V7X 1K8

   Attention: Global Support — Corporate Support Team Lead
   Fax: (604) 629-7063

Security Authentication Methods

Absolute Software uses either RSA SecurID® tokens or unique e-mailed authorization codes to authenticate security operations. If you purchased directly from Absolute Software, you select your Security Authentication Method when you complete your preauthorization agreement. If you purchased from a reseller, you can specify your authentication method when you register your account at https://registration.absolute.com.

RSA SecurID Tokens

A RSA SecurID® Token is a key-chain token that is synchronized with a RSA database server at Absolute Software and generates a new six digit random number every sixty (60) seconds. The RSA SecurID® token is unique and linked to an individual Security Administrator account.

If you are using RSA SecurID® Tokens as the authentication method, the Security Administrator enters the code from the RSA SecurID® Tokens to validate each security operation.

RSA is the security division of EMC^2®. However, all RSA SecurID® Tokens must be purchased directly from Absolute Software.

When Absolute Software receives your signed preauthorization agreement, we send the RSA SecurID® Tokens to authorized Security Administrators by mail.

Authorization Codes

A Security Authorization Code is a unique authorization code e-mailed to a Security Administrator in response to a request made in Customer Center. The e-mailed authorization code is valid for two (2) hours from the time it is issued, may only be used by the Security Administrator who requested the code, and may only be used once. If you are using authorization codes as your authentication method, you must request a new authorization code for each security operation. See "Disabling Security Administrator Authorization" on page 32 for more information.

Requesting an Authorization Code

If your company uses authorization codes to authenticate security operations, you must request an authorization code before initiating any action in the data and device security section. When you receive your authorization code by e-mail, you use it to validate your security operation.

To request an Authorization Code:

1. Log in to the Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the Security Authorization section, click the **Request Authorization Code** link. The Request Authorization Code page opens.
4. Click **Request Code**. Customer Center shows a confirmation message informing you that an authorization code is generated and will be e-mailed to you.

   NOTE The authorization code is e-mailed to the e-mail account on file for the Security Administrator who requested it.

Changing your Authentication Method

To change your authentication method, contact Absolute Technical Support at http://www.absolute.com/support. It is not possible to change your authentication method in Customer Center.

Disabling Security Administrator Authorization

If you feel that the security of your security administration operations has been compromised for any reason, you may disable your Security Administrator preauthorization agreement with Absolute Software. Disabling the preauthorization agreement makes it impossible for any new requests to be created by any Security Administrator, and cancels all existing security requests such as Data Delete, Device Freeze, and Intel® Anti-theft Technology (AT).

To disable your Security Administrator authorization:

1. Log in to the Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Administration** link on the global navigation bar. The Administration page opens.
3. In the Account section, click the **Disable Preauthorization** link. The Disable Preauthorization page opens.
4. Click **Disable**. A confirmation dialog box shows.
5. Click **OK** to confirm the request.

IMPORTANT To enable the Security Administrator authorization again, you must contact the Absolute Software Recovery department. Click the **Support** link and follow the on-screen instructions to contact Absolute Software.

Transferring RSA SecurID Tokens

If a Security Administrator changes roles or leaves your company, you can transfer an existing RSA SecurID® token to another employee.

To transfer a token:

1. Click the **Documentation** link on the global navigation bar. The Documentation page opens.
2. In the **Service Request Forms** section, click the **Security Administrator RSA SecurID Token Transfer Form** link. The token transfer agreement opens in a new window as a PDF file.
3. Print the agreement.
4. Fill in the form and return it by courier or fax to Absolute Software, using the mailing address or fax number provided on the agreement.

Returning Expired RSA SecurID Tokens

Each RSA SecurID® token expires after a fixed time period. RSA Security has a secure disposal process in place for expired tokens. Expired tokens should be packaged for shipping, marked **Attention: Expired Token Disposal** and mailed to one of the following addresses:

North and South America

RSA Security Inc.
174 Middlesex Turnpike
Bedford, MA, USA 01730
T: +1 781 515-5000
F: +1 781 515-5170

EMEA

RSA Security Ireland
Bay 127
Shannon Free Zone
Shannon, County Clare, Ireland
T: +353 61 72 5100

To return an expired RSA token and request a replacement:

1. Send your expired RSA token(s) to RSA Security.
2. Contact Absolute Software and request a new token.

Absolute Software associates a new RSA SecurID® token with your Security Administrator account and mails you the replacement token(s). You do not need to complete a new preauthorization form.

Additional information on RSA's token disposal program can be found on the Internet at: http://www.rsa.com/support/pdfs/Token_Disposal_statement.pdf

Summary

After you install the Agent and register your account, you are able to access Customer Center and view the data associated with your monitored devices.

Chapter 3 Administration

The **Administration** section of the Absolute Customer Center contains six comprehensive sub-sections for setting event alerts and defining user and asset information. The sections are:

- Alerts
- Data
- Groups
- Software Policy
- Users
- Account
- Manage AT equipped Computers
- System Notifications

Alerts

The Alerts area allows users to configure alerts for events. An alert is a pager or e-mail message that notifies users when specific, user-definable conditions are met. An alert event is a record of an alert that was triggered in Customer Center. Alerts can be configured to use a single criterion or to use multiple criteria. An alert configured to use multiple criteria is only triggered after all criteria are met. Additionally, alerts can be created to target or exclude single assets or groups of assets.

When an alert is triggered, the user receives an e-mail or pager message. E-mail messages contain a summary of the conditions that triggered the alert and a link to the Customer Center home page.

Pre-defined Alerts

Customer Center contains the following pre-defined alerts:

- Change in Serial Number
- Agent Is Newly Installed
- Hard Drive Nearly Full
- Last called 20 days ago
- Lease Ending
- Missing Software on Required List
- Modem Added
- New Program File Detected
- Out of Date antivirus

- Software on Banned List
- Warranty Ending

Accessing the Alerts area

To access the Alerts area:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Alerts** link on the global navigation bar or the Administration page. The Alerts page opens. To perform various alert administration tasks, click the appropriate links.

Viewing Triggered Alert Events

The Alert Events page shows a table containing a record for each alert that was triggered. The Alert Events table includes the following headings:

- **Alert** — the Alert ID number (automatically generated by the system)
- **Alert Name** — the name of the alert
- **Identifier** — the Identifier of the device that triggered the alert
- **Username** — the user name of the device that triggered the alert
- **Device Name** — the name of the device that triggered the alert
- **Last Event** — the time the event was triggered
- **Suspicion Level** — the severity of the suspicious event that triggered the alert
- **Reset Date** — the date on which the alert was reset

  NOTE Reset alerts are included in database scans.

- **Last Event** — the date when the last known event occurred
- **Status** — the current status of the device

NOTE It is important to note that alerts can be applied to a single device or to a device group, whereas *alert events* always refer to a single device.

To view alert events:

1. Click the **Alert Events** link on the global navigation bar or the Alerts page. The Alert Events page opens.
2. By default, the Alert Events table shows all existing alert events.
3. If you want to filter the results, select the appropriate criteria in the **Field** list, and then enter the appropriate search criteria in the field. You can also select an alert from a list of detected alerts. Click **Choose** to open the Choose page and search for the appropriate alert. For more

information on the **Choose** feature, see “Using the Choose Feature” on page 92.

4. Click **Show Results**. The report is regenerated using the defined criteria.

Viewing Alerts

The View and Manage Alerts page shows a table containing a record for all existing alerts including the attributes and status for each alert. The Alerts table includes the following headings:

- **Alert** — the Alert ID number (automatically generated by the system)
- **Alert Name** — the name of the alert
- **Conditions** — the conditions set for the alert
- **Scope Include** — the specified criteria for devices that trigger alerts
- **Scope Exclude** — the specified criteria for devices excluded from alerts
- **Status** — the current status of the device
- **Type** — the alert type

NOTE Alerts can be applied to a single device or to a device group, whereas *alert events* always refer to a single device.

To view existing alerts:

1. Click the **View and Manage Alerts** link on the global navigation bar or the Alerts page. The View and Manage Alerts page opens.
2. By default, the Alerts table shows all existing alerts. To filter the results in the Alerts table:
    - Select the appropriate alert ID in the **Alert ID** list.
    - Enter a part of or the entire alert name in the **Alert Name** field.
3. Click **Show Results**. The report is regenerated using the defined criteria.

Creating New Alerts

You can use the Create and Edit Alerts page to create and edit alerts. To create a new alert:

1. Use one of the following methods to open the Create and Edit Alerts page:
    - Click the **Create and Edit Alerts** link on the global navigation bar or the Alerts page. The Create and Edit Alerts page opens.
    - Click **Create Alert** on the Alert Events page. The Create and Edit Alerts page opens.

- Click **Create Alert** on the View and Manage Alerts page. The Create and Edit Alerts page opens.

  The Create and Edit Alert page contains an Alert Description area and five sections for configuring alerts: Conditions, Scope, Alert Type, Alert Option, and Action.

2. **Alert Description** — Use this section to name and describe the alert.

   a) Enter or edit the value in the **Alert Name** field. The alert name is available in the **Alert** column of the Alert Events page.

   b) Enter or edit the value in the **Alert Description** field. Use this field for a detailed description of this alert.

3. **Suspicion Level** — Use this section to specify a severity level for suspicious events. Possible values range from **Not Suspicious** to a suspicion level of **5**.

   NOTE Events triggered by Alerts defined as representing suspicious activity are used to determine the overall suspicion level of a device within a particular time period. Use the Suspicious Devices report to view and manage a list of devices that have a high level of suspicion.

4. **Conditions** — Use this section to define or modify the conditions that trigger the alert.

   NOTE A single alert can have several separate conditions that must all be met to trigger user notification.

   IMPORTANT Conditions prefixed with an asterisk (*) are not trigger by the Agent calls, and can only be combined with other conditions with an asterisk.

   - Select the appropriate value in the **Field** list, and then select the appropriate value in the **Rule** list. This list includes all appropriate rules for the field selected in the **Field** list.
   - Depending upon your selections in the **Field** and **Rule** lists, the **Criteria** field shows. Enter the appropriate criteria or use **Choose** to select a value from the list of all existing criteria. For more information about using the Choose feature see “Using the Choose Feature” on page 92. For examples of setting conditions for alerts, see “Alert Condition Examples” on page 40.

5. Click **Add Condition**. The Create and Edit Alert page refreshes, listing the new condition in the **Condition** table. Repeat steps 4 to 5 as needed to add all appropriate conditions.

   NOTE To delete an existing condition from an alert, click **Delete** in the **Delete** column.

6. **Scope** — Use this section to specify the Identifiers or devices included in or excluded from the alert.

    - Select devices or Identifiers to be included in the report:

        - Select the Identifier or device group to which this alert applies in the **Devices in the group** list.

        - Select a value from the **Only Where** list. The values included are **Any field**, **Identifier**, **Device Name**, **Username**, and **Serial Number**.

        - Enter a search criteria in the **contains** field. You can also use **Choose** to select a value from the list of all existing criteria. For more information about using the Choose feature see “Using the Choose Feature” on page 92.

    - Select devices or Identifiers to be excluded from the report:

        - Select the Identifier or device group to which this alert does not apply in the **Devices in the group** list.

        - Select a value from the **Only Where** list. The values included are **Any field**, **Identifier**, **Device Name**, **Username**, and **Serial Number**.

        - Enter a search criteria in the **contains** field. You can also use **Choose** to select a value from the list of all existing criteria. For more information about using the Choose feature see “Using the Choose Feature” on page 92.

7. **Alert Type** — Use this area to define how the alert is reset after it is triggered.

    - If you want to create an alert that must be manually reset from the Alert Events page, select the **Manual reset** option.

    - If you want to create an alert that automatically resets after a specific number of days, select the **Automatic reset after** option, and then enter a value in the **day(s)** field.

8. **Alert Option** — Use this area to specify whether a single alert e-mail or multiple alert e-mails should be sent when the alert is triggered.

    - If you want to have a single e-mail sent when the alert is first triggered, select the **Single e-mail** option.

    - If you want to have an e-mail sent each time the alert is triggered, select the **Multiple e-mails** option.

        NOTE Using the **Multiple e-mails** option may result in a large number of e-mails.

9. **Action** — Use this area to define how Customer Center handles the alert when triggered. Customer Center always logs triggered alerts for the Suspicious Devices report. By default, Customer Center also notifies Administrators via e-mail or pager when an alert is triggered. You can set an alert so that no notifications are sent, for example when creating an alert considered low level.

    ○ Select **Log event** to send no notifications when the alert is triggered. Select **Log event and notify** to contact Administrators automatically via e-mail or pager when the alert is triggered.

    ○ For alert notifications to be e-mailed, enter one or more addresses in the **E-mail address** field. Multiple recipients can be defined by separating them with a semicolon.

    ○ For alert notifications to be sent via pager, enter the destination pager address in the **Pager** field.

    NOTE Pager alerts can only be received by alpha-numeric pagers.

10. If you want to suspend alert scanning, select the **Suspend alert scanning** option. For more information on suspending alert scanning, see "Suspending Alert Scanning" on page 41.

11. Click **Save**. The page from which you navigated to the Create and Edit Alerts page opens to show a confirmation message.

12. To delete the alert, click **Delete this alert**.

    NOTE You cannot delete any predefined alerts. If deleted, these alerts are automatically recreated in a suspended state. See "Pre-defined Alerts" on page 35 for more information.

Alert Condition Examples

The following examples describe some of the more commonly used conditions for alerts.

Geofence Location

If you select the value `Geofence Location` in the **Field** list in the **Condition** area of the **Create and Edit Alerts** page, the Rule field refreshes to show the following additional options:

- **Location** — The first drop-down list shows two options:

    ○ **Outside** — Select this option to specify an alert whenever a device travels outside a specified Geofence boundary.

    ○ **Inside** — Select this option to specify an alert whenever a device travels inside a specified Geofence boundary.

- **Geofence Name** — The second drop-down list shows a list of geofences existing for your account. Select the appropriate Geofence name in the list.
- **Duration** — The field and final drop-down list in the Rule fields allows you to specify the duration after which an alert is triggered. Enter the appropriate number in the field and select the appropriate option from `Hours`, `Days`, or `Weeks` to specify the duration.

Self Healing Call

If you select the value `Self Healing Call` in the **Field** list in the **Condition** area of the **Create and Edit Alerts** page:

1. The Rule list refreshes to show additional options.
2. To continue, select the value `has occurred` in the **Rule** list.

Operating System Product Key

If you select the value `Operating System Product Key` in the **Field** list:

1. The Rule list refreshes to show additional options.
2. Select the value `Changed` in the **Rule** list to continue.

Editing Existing Alerts

The processes to create new alerts and to edit existing alerts are identical. The only difference is the method by which you access the Create and Edit Alerts page.

To edit existing alerts:

1. On the Alert Events or View and Manage Alerts page, click the **Alert ID** link. The Create and Edit Alerts page opens.
2. Modify the appropriate details, and then click **Save**. The page from which you navigated to the Create and Edit Alerts page opens to show a confirmation message.

Suspending Alert Scanning

The **Suspend Alert Scanning** checkbox is available on the Create and Edit Alerts page. Use this checkbox to disable an alert without deleting it (from the Edit Alert page), or to create an alert without activating it (from the Create Alert page).

Suspended alerts are identified on the Alert Events page with the text `--Suspended--` listed below the alert description in the **Alert** column.

Triggered Alerts

After you have configured an alert and it is triggered, an e-mail or pager alert is sent and a record is added to the Alert Events page. E-mailed alert notifications provides a summary of the alert criteria that triggered the alert. Pager alert notifications identify the alert number.

Resetting Alerts

When an alert is triggered, e-mail or pager notification is sent out and the alert is flagged at the Monitoring Center (unseen to users) to prevent repeat notification. The triggered alert remains in the database but must be reset before it is active again.

To reset an alert:

1. Open the Alert Events or View and Manage Alerts page.
2. Select the checkbox in the first column for the specific alert you want to reset.
3. Click **Reset**. The alert's status is updated and it is included in database alert scans.

NOTE If the conditions that initially triggered the alert remain, the alert is re-triggered and notification messages resume.

Data

The Data area of Customer Center is used to define company-specific asset data. After users have entered information into Customer Center, this data can be included in the Asset and Lease Completion reports.

To open the Data area, click the **Data** link in the global navigation bar or on the Administration page.

The Data area includes the following sections:

- Creating and Editing Departments
- Exporting and Importing Data
- Viewing and Editing User-defined Fields Data
- Managing User-defined Fields
- End-user Messaging

Creating and Editing Departments

Use this section to add, remove or edit department titles from your account. The **Create and Edit Departments** table lists all departments configured for your account, as well as a count of devices included in the department. The department field is included in the filter of many Customer Center reports.

To add a new Department:

1. On the **Create and Edit Department** page, click **Create New Department**.
2. Enter a name for the department in the **Department Name** field.
3. Click **Save**. The Create and Edit Department page opens with a message confirming successful creation of the new department.

To edit a Department:

1. On the **Create and Edit Department** page, for the appropriate department, the **Edit** link in the **Edit Department** column.
2. Edit the department name in the **Department Name** field.
3. Click **Save**. The Create and Edit Department page opens with a message confirming successful update.

To delete a Department:

IMPORTANT A Department cannot be deleted if there are Identifiers associated with it. You must first disassociate all Identifiers from the department.

1. On the **Create and Edit Department** page, for the appropriate department, click the **Edit** link in the **Edit Department** column.
2. Click **Delete**. The Create and Edit Department page opens with a message confirming successful deletion.

Exporting and Importing Data

In instances where target devices receive different values for the same data point, use the **Export Data** and **Import Data** pages. The Export and Import Data process allows users to download their current data in a Comma Separated Value (CSV) or an XML file. The user can then alter the data and upload (or import) the data back into the Customer Center.

A CSV file is a plain text file used to export or import data into spreadsheets and databases. CSV files provide a mechanism to import asset data prepared using other applications or to expedite entering information for multiple Identifiers simultaneously. Most spreadsheet programs can automatically export data in CSV format. CSV files can also be created manually. But it is up to the user on which format works best.

NOTE The Export and Import Data process is a multi-step procedure and involves some offline processing of database data to prepare the files. For this reason, if all devices receive the same value, the **Edit Data** page described above is more efficient than the Export and Import Data process.

Step 1: Export existing data to a file

1. To open the **Export Data** page, click the **Data** group in the Administration section, and then click the **Export Data** link.
2. From the **Group** list, select the Device Group for which you want to modify data.
3. Define a name and format for the data export file.
4. If you want to receive an e-mail notification when the file is available, enter your e-mail address in the space provided.
5. Click **Continue**. The request for the data file is processed offline. When the request is processed, the report is available for download from the Export Data Status page. If you have provided an e-mail address, an e-mail notification is sent.

Step 2: Modify the file

The Export Data Status page is used to download an exported file for modification purposes. To download and modify an exported file:

1. Click the **Export Data Status** link in the global navigation bar or on the Administration page.
2. To retrieve the data file, click the appropriate **Ready** link. Follow on-screen instructions to save the file to your local machine.

   IMPORTANT Absolute Software recommends that you archive a copy of the original download file. Should an error occur during the import process, the download file allows you to restore the data to its original state.

3. Open the file and modify the values you want to change.
4. Save the updated file.

Step 3: Upload the Modified File

1. Click the **Import Data** link in the global navigation bar or on the Administration page.
2. Define a name for the data import file in the space provided.
3. If you want to receive e-mail notification when the data upload is complete, enter your e-mail address in the space provided.
4. Enter the full path to the modified file or click **Browse** to select it from your local machine.
5. Click **Upload**.

The upload of the data file is processed offline. If you provided an e-mail address, Customer Center sends an e-mail notification.

Step 4: Verify File Upload

1. Click the **Import Data Status** link in the global navigation bar or on the Administration page.
2. When the import is complete, the updated data is visible in all Customer Center reports, and the Import Data Status table shows the status of the files as **Ready**.
3. Click the **Ready** link to download a copy of the uploaded file.

Viewing and Editing User-defined Fields Data

The Customer Center stores asset information for many pre-defined data points. Also, the users can define up to twenty additional unique data fields.

The pre-defined fields are as follows:

NOTE Some of these fields may not be applicable in your environment.

- **Fixed Fields**
  - **Asset #**
  - **Assigned User Name**
  - **Has Service Guarantee**
  - **Department**
  - **Assigned User E-mail**
  - **Lease Start Date**
  - **Lease End Date**
  - **Lease Number**
  - **Lease Vendor**

  - **Lease Responsibility**
  - **Service Contract Start Date**
  - **Service Contract End Date**
  - **Service Contract Vendor**
  - **Warranty Start Date**
  - **Warranty End Date**
  - **Warranty Contract Vendor**
  - **Device Purchase Date**
  - **Physical/Actual Location**
  - **Cost Center/Code**
  - **User Phone/Extension**
  - **Purchase Order Ref**
  - **Dormant**

The View and Edit User-Defined Fields Data page can be used to assign data values to individual devices or to device groups. Additionally, Customer Center users can migrate stored data from one device to another or copy stored data from one device to another.

Assigning values to an Identifier

To assign values to an individual Identifier:

1. Click the **View and Edit User-defined Fields Data** link in the global navigation bar or on the Administration page.
2. Click **Choose Device**. A dialog box opens listing all the Identifiers associated with your account.
3. To select the Identifier from the list, click the appropriate link. The View and Edit User-Defined Fields Data page opens with the selected Identifier shown in the **Data For The Device** field. The report table refreshes, listing any values previously assigned to the Identifier.
4. Enter or update the information in the fields you want to define.
5. Click **Save Changes**.

Assigning values to a device group

To assign values to all devices in a device group:

1. Click **Choose Device Group**. A dialog box opens listing all device groups associated with your account.
2. To select a device group from the list, click the appropriate group. The View and Edit User-Defined Fields Data page opens with the selected device group listed in the **Data For the Group** field. The table refreshes, listing any values previously assigned to the device group as well as any conflicts. See “Multiple Values” on page 47.

3. Enter or update the information in the fields you want to define.
4. Click **Save Changes**.

When defined, you can view these data fields in the Asset report by selecting the **User-defined Fields** checkbox. The fields can also be viewed in the default Lease Completion report.

Multiple Values

Because an individual Identifier can be a member of any number of device groups, or have values assigned to it specifically, it is possible for conflicting values to be associated with the same Identifier, or for a single data point when dealing with Device Groups. In such a case, the **Data** field of the table shows a link labelled `Multiple Values.` Click the link to view a table listing the Identifiers and values that are in conflict. Ensure the shown values are correct. To correct an error, enter the correct information in the field and click **Save & Close**. If the information is correct, click **Close** to return to the View and Edit Data page.

Migrating Data

The Customer Center supports three methods of migrating stored data between two Identifiers:

- Copying Data
- Moving Data
- Switching Data

Copying Data

The Copy data feature allows you to copy field values from one Identifier to another Identifier, that results in identical values for both Identifiers.

For example, if **Device A** has the following two fields:

- **Depot**: 3752
- **Building ID**: North28

and **Device B** has the following two fields:

- **Depot**: 4788
- **Building ID**: West35

If the data from these two fields is copied from **Device A** to **Device B**, then the original values from **Device B** would be overwritten to match those of **Device A**. When completed, both machines would have identical data in these two fields.

- **Depot**: 3752
- **Building ID**: North28

For instructions on Copying Data see “To Copy Data” on page 49.

Moving Data

Moving data differs from copying data in that when complete, the data fields associated with the first device are cleared and left blank.

For example, if **Device A** has the following two fields:

- **Depot**: 3752
- **Building ID**: North28

and **Device B** has the following two fields:

- **Depot**: 4788
- **Building ID**: West35

If the data from these two fields is moved from **Device A** to **Device B** then the original values from **Device B** would be overwritten to match those of **Device A** and Device A's values are cleared. When complete, the devices would have the following values:

- **Device A:**
  - **Depot:** <null>
  - **Building ID:** <null>
- **Device B:**
  - **Depot**: 3752
  - **Building ID**: North28

For instructions on Moving Data see "To Move Data" on page 50.

Switching Data

When migrating data using the Switch Data option, the two target Identifiers exchange their data values with each other. Neither retains its original values.

For example, if **Device A** has the following two fields:

- **Depot**: 3752
- **Building ID**: North28

and **Device B** has the following two fields:

- **Depot**: 4788
- **Building ID**: West35

If the data from these two fields is switched between **Device A** and **Device B** when complete, the devices would have the values below.

- **Device A:**
  - **Depot**: 4788
  - **Building ID**: West35

- **Device B:**
  - **Depot**: 3752
  - **Building ID**: North28

For instructions on Switching Data see “To Switch Data” on page 51.

Data Migration Summary

The table below outlines how data is moved when using the different data migration methods.

	Copy Data	Move Data	Switch Data
Data changes on Device A	No	Yes	Yes
Data changes on Device B	Yes	Yes	Yes

To Copy Data

To copy stored data from one Identifier to another:

1. **Navigate to the View and Edit User-Defined Fields Data page —** From the Customer Center home page, click **Administration**. Then click the **View and Edit User-Defined Fields Data** link in the Data section. The View and Edit User-Defined Fields Data page opens.

2. **Select the data source**

   a) On the View and Edit User-Defined Fields Data page, click **Choose Device**. A dialog box opens listing all device groups associated with your account.

   a) To select a device group from the list, click the appropriate group. The View and Edit User-Defined Fields Data page opens with the selected device group listed in the **Data For the Group** field.

3. The View and Edit User-Defined Fields Data page refreshes to show the user-defined data for the selected Identifier.

4. **Select the target device**

   a) On the View and Edit User-defined Fields Data page, click **Copy Data To New Device**. The Copy Data to Another Device page opens.

   b) Review the details listed for **Device A** to verify you have selected the correct data source.

   c) Click **Select Device for Copy** to open the Choose page.

   d) To select the target Identifier from the list, click the appropriate Identifier. The Copy Data to Another device page refreshes to show the identification information of the target device listed as **Device B**.

e) Review the listed details for **Device B** to confirm the correct Identifier was selected.

5. **Select the data fields to copy**

   a) Click **Copy Data** to open the Copy page.

   b) Select the checkboxes for the fields you want to copy from the source device to the target device. If you are a power user your copy options are preselected by your administrator.

   NOTE You cannot copy some data points, such as **Serial Number**.

6. Click **Copy From A to B** to initiate the copy process. The View and Edit User-Defined Fields Data page refreshes with a message indicating the data is copied.

To Move Data

To move stored data from one Identifier to another:

1. **Navigate to the View and Edit User-Defined Fields Data page —** From the Customer Center home page, click **Administration**. Then click the **View and Edit User-Defined Fields Data** link in the Data section. The View and Edit User-Defined Fields Data page opens.

2. **Select the data source**

   c) On the View and Edit User-Defined Fields Data page, click **Choose Device**. A dialog box opens listing all device groups associated with your account.

   d) To select a device group from the list, click the appropriate group. The View and Edit User-Defined Fields Data page opens with the selected device group listed in the **Data For the Group** field.

3. The View and Edit User-Defined Fields Data page refreshes to show the user-defined data for the selected Identifier.

4. **Select the target device**

   a) On the View and Edit User-defined Fields Data page, click **Move Data To New Device**. The Move Data to Another Device page opens.

   b) Review the details listed for **Device A** to verify you have selected the correct data source.

   c) Click **Select Device for Move** to open the Choose page.

   d) To select the target Identifier from the list, click the appropriate Identifier. The Move Data to Another device page refreshes to show the identification information of the target device listed as **Device B**.

   e) Review the listed details for **Device B** to confirm the correct Identifier is selected.

5. **Select the data fields to move**

   a) Click **Move Data** to open the Move page.

   b) Select the checkboxes for the fields you want to move from the source device to the target device. If you are a power user your move options are preselected by your administrator.

   NOTE You cannot move some data points, such as **Serial Number**.

6. Click **Move From A to B** to initiate the move process. The View and Edit User-Defined Fields Data page refreshes with a message indicating the data was moved.

To Switch Data

To switch stored data from one Identifier to another:

1. **Navigate to the View and Edit User-Defined Fields Data page —** From the Customer Center home page, click **Administration**. Then click the **View and Edit User-Defined Fields Data** link in the Data section. The View and Edit User-Defined Fields Data page opens.

2. **Select the data source**

   a) On the View and Edit User-Defined Fields Data page, click **Choose Device**. A dialog box opens listing all device groups associated with your account.

   b) To select a device group from the list, click the appropriate group. The View and Edit User-Defined Fields Data page opens with the selected device group listed in the **Data For the Group** field.

3. The View and Edit User-Defined Fields Data page refreshes to show the user-defined data for the selected Identifier.

4. **Select the target device**

   a) On the View and Edit User-defined Fields Data page, click **Switch Data With Another Device**. The Switch Data With Another Device page opens.

   b) Review the details listed for **Device A** to verify you have selected the correct data source.

   c) Click **Select Device for Switch** to open the Choose page.

   d) To select the target Identifier from the list, click the appropriate Identifier. The Move Data to Another device page refreshes to show the identification information of the target device listed as **Device B**.

   e) Review the listed details for **Device B** to confirm the correct Identifier was selected.

5. **Select the data fields to switch**

   a) Click **Switch Data** to open the Switch page.

   b) Select the checkboxes for the fields you want to move from the source device to the target device. If you are a power user your move options are preselected by your administrator.

   NOTE You cannot switch some data points, such as **Serial Number**.

6. Click **Switch From A to B** to initiate the move process. The View and Edit User-Defined Fields Data page refreshes with a message indicating the data was switched.

Creating User-defined Fields

In addition to the fifteen predefined data fields, Customer Center administrators can define up to twenty additional unique data points. To define a new data point:

1. Click the **Manage User-Defined Fields** link in the global navigation bar or on the Administration page.
2. Click **Create User-Defined Field**. The Create User-Defined Field page opens.
3. Enter a name for your data point in the **Field Label** field.
4. Select the appropriate data type for the new field from the **Field Type** list. Possible values are:
   - **Text (50)** — this field type accepts plain text up to 50 characters in length
   - **Date (m/d/yyyy)** — this field type accepts date values in the form m/d/yyyy
   - **Drop-down List** — this field type accepts values specified from a drop-down list. When this field type is selected, the Create User-Defined Field window is refreshed to include the **Drop-down List Values** field. Use this field to enter the values that show in the drop-down list for the field. Separate the different values to be listed with a comma.
5. If you want to allow editing of the field by Power Users, select the **Editable by Power Users** checkbox.
6. Click **Save**. The Manage User-Defined Fields page refreshes with the new User-Defined Field listed at the bottom.

   NOTE If the Edit Data page does not list your new data point, click your browser’s refresh button to update the display.

Managing User-defined Fields

To rename, edit, delete an existing data point, or the values listed for a field:

1. Click the **Manage User-Defined Fields** link in the global navigation bar or on the Administration page.
2. To select the data point to modify, click the associated **Edit** link. The Edit User-Defined Field page opens.
3. Modify or delete the field:
    - **To Edit the Field** — Update the **Field Label** or the **Drop-down List Values** as appropriate and click **Save Changes**. You are returned to the Edit Data page.
    - **To Delete the Field** — Click **Delete**. You are returned to the View and Edit Data page.

End-user Messaging

The **End-user Messaging** page allows Customer Center Administrators to define the contents and rules for messages shown to device users during the Agent call to the Monitoring Center.

IMPORTANT End-user Messaging is only available on PCs running Windows with Internet Explorer installed and computers running the Mac OS. Currently, End-user Messaging is not available for Windows Mobile or other mobile devices.

These messages allow you to provide information to device end-users, such as a notification of an upcoming server outage. They also allow you to create data entry forms to gather additional information directly from the user.

Administrators can specify the content of the message and any data input fields to include. Messages are stored as web pages and reside on the Absolute Software Web site.

When a message is deployed to an end-user and the end-user has completed the data input, the resulting data is stored in the equivalent user-defined fields for that device (Identifier). Administrators can then use this information to gather asset data about the device or user that is not retrieved automatically by the Agent. This can be a physical location, phone number, asset label, department, or other data.

There are two types of end-user messages:

- Custom messages designed inside Customer Center
- URL messages that show any selected URL in the end-user’s browser

You can create any number of end-user messages, and deploy them to all of your devices, a device group, or a specific machine.

NOTE End-user Messages are not supported on Windows Mobile devices.

Creating Custom Messages

To create a custom end-user message:

IMPORTANT End-user Messaging is only available on PCs running Windows with Internet Explorer installed and computers running the Mac OS. Currently, End-user Messaging is not available for Windows Mobile or other mobile devices.

1. Click the **End-user Messaging** link in the global navigation bar or on the Administration page. The End-user Messaging page opens.
2. Click **Create New End-user Message**. The Create End-user Message page opens.
3. Enter a descriptive name for the new message in the **Message Name** field.

   NOTE This message name is for your reference only, and is not shown to the user.

4. In the **Message Type** section, click the **Custom Message** option.
5. Enter the title that should show on the title bar of the message shown to the end-user in the **Message Title** field.
6. Enter the **Message Text**. The field accepts URL links and the following standard HTML tags:
   - `<A>`
   - `<BR>`
   - `<B>`
   - `<FONT>`
   - `<I>`
   - `<P>`
   - `<U>`
7. If you want to include an image with your message, enter the **Image URL**, **Image Location,** and **Image Hyperlink** (all optional). You are limited to one image per message.
8. If the page is used for data entry, click **Choose Fields**. The Fields dialog box opens. The left column of the dialog box shows all **Available Fields** which can be added to the message. The right column of the dialog box lists all currently **Selected Fields**.

9. Select the fields you want to include. When finished, click **OK**. The Fields dialog box closes and the End-user Message page opens, now showing all selected fields as a list of checkboxes under the **Included Fields** heading.

10. If necessary, select the **Required** checkbox for all fields. Selecting the **Required** checkbox makes the specified field mandatory and the user needs to provide information for these fields to successfully submit a response to the End-user Message.

11. In the **Send To** section, select the appropriate option to define the end-users who receive the message:

    ○ **All Devices** — Select this option to send the message to all devices.

    ○ **Specific Device** — Select this option and use **Choose** to select a device to which the message should be sent.

    ○ **Specific Group** — Select this option and use **Choose** to select one specific group to which the message should be sent. This option allows you to send messages to a subset of your end-users. The group must be defined before you can select it. Refer to "Groups" on page 58 for more information.

    IMPORTANT When an end-user message is applied to "All Devices", any newly activated devices automatically receive the end-user message. Also, when an end-user message is applied to a specific group, any device added or removed from that group is similarly associated or disassociated with the end-user message.

12. In the **Message Display Rules** section, select the appropriate option to define the frequency that the web page should be presented to end-users. Available options are:

    ○ **On next call** — The web page is presented to end-users only once, on their device's next call to the Monitoring Center.

    ○ **On or after** — Click the **On or after** field to show the calendar dialog box. Select the appropriate date in the calendar dialog box.

    NOTE Clicking a date in the calendar updates the values in the date fields.

13. Review the message you have created, and use one of the following buttons to save it:

    ○ Click **Save & Activate** to save the message and activate it immediately.

    ○ Click **Save & Suspend** to save the message and suspend it. You can activate the message later.

14. The End-user Messaging page opens with the new message shown in the list of end-user messages.

Previewing Custom Messages

After you create an end-user message, you can preview it prior to sending it out to your end-users. Typically, you would want to Save and Suspend the message, and then preview it prior to sending it to your end-users.

NOTE You must save the message before you can preview it.

To preview a custom end-user message:

IMPORTANT End-user Messaging is only available on PCs running Windows with Internet Explorer installed and computers running the Mac OS. Currently, End-user Messaging is not available for Windows Mobile or other mobile devices.

1. On the **End-user Messaging** page, click the message name link for the message you want to preview. The Create End-user Message page opens.
2. Click **Preview in New Window** to open the message in a new window.
3. Click **Cancel** to close the preview window and return to the Create End-user Message page.
4. Click **Cancel** to close the Create End-user Message page and return to the End-user Messaging page.

Editing Custom Messages

To edit an existing end-user message:

IMPORTANT End-user Messaging is only available on PCs running Windows with Internet Explorer installed and computers running the Mac OS. Currently, End-user Messaging is not available for Windows Mobile or other mobile devices.

1. On the **End-user Messaging** page, click the **Edit** link for the message you want to edit. The Create End-user Message page opens.
2. Make the appropriate changes to the message. When you are finished:
   - Click **Save & Activate** to save the message and activate it immediately.
   - Click **Save & Suspend** to save the message and suspend it. You can activate the message later.
3. The End-user Messaging page opens with the edited message shown in the list of end-user messages.

URL Messages

A Uniform Resource Locator (URL) message shows any World Wide Web address in the end-user's browser. Customer Center does not make a record of when the end-user has acknowledged receipt of an URL message.

To create an URL message:

IMPORTANT End-user Messaging is only available on PCs running Windows with Internet Explorer installed and computers running the Mac OS. Currently, End-user Messaging is not available for Windows Mobile or other mobile devices.

1. Click the **End-user Messaging** link in the global navigation bar or on the Administration page. The End-user Messaging page opens.
2. Click **Create New End-user Message**. The Create End-user Message page opens.
3. Enter a descriptive name for the new message in the **Message Name** field. This message name is for your reference only, and is not shown to the user.
4. In the **Message Type** section, click the **URL** option.
5. Select the message delivery option:
   - **Attempt to send once** — the message is sent only on the next Agent call.
   - **Send repeatedly —** the message is sent on all Agent calls. This is useful if the end-user has signed out a device and failed to return it by the due date. When the device is returned, you can suspend or delete the message.
6. Review the message you have created, and save it:
   - Click **Save & Activate** to save the message and activate it immediately.
   - Click **Save & Suspend** to save the message and suspend it. You can activate the message later.
7. The End-user Messaging page opens with the new URL message shown in the list of end-user messages.

Resending Messages

There are times when it is useful to resend a message, even if it has already been received and acknowledged by end-users. For example, you could edit a complex existing message and resend it, rather than creating a new message from scratch.

To resend a message:

IMPORTANT End-user Messaging is only available on PCs running Windows with Internet Explorer installed and computers running the Mac OS. Currently, End-user Messaging is not available for Windows Mobile or other mobile devices.

1. In the **End-user Messaging** page, click the **Edit** link for the message you want to edit. The Create End-user Message page opens.
2. In the **Message Display Criteria (Rules)** section, select the **Re-Send** checkbox.
3. When you are finished:
   - Click **Save & Activate** to save the message and send it again immediately.
   - Click **Save & Suspend** to save the message and suspend it. You can send the message later.

Groups

The Groups area allows you to assign devices to different logical groups. Device groups can be created based on department, geographical area, or any other criteria. When created, you can use the group to send reports to a specific group of machines.

When an End-user Message is applied to a group, all Identifiers in that group receive the message.

To open the Device Groups page:

1. Click the Groups link on the global navigation bar or the Administration page.
2. Click the **Device Groups** link on the global navigation bar or on the Groups page. The Device Groups page opens.

The Device Groups page includes a filter area at the top of the page and a table including all device groups associated with your account. If necessary, use the filters to locate the device group(s) you want to view.

The table includes the following fields for each device group:

- **Device Group Name** — the name of the device group.
- **Count** — the total number of monitored Identifiers included in the group.
- **Description** — A brief description of the group.
- **Created By** — the creator of the group or the creators e-mail address.

- **Last Modified** — the date the group was created or last Creating New Device Groups

To create a new device group:

1. Click **Create New Device Group**. The Create New Device group page opens.
2. Enter a name for the new group in the **Group Name** field. Click the **Check Name Availability** link to verify that the name you created is not in use.
3. Enter a description for the group in the **Group Description** field.
4. If necessary, select the **Lock as Read-Only** checkbox under **Group Information**.

   NOTE When locked as read-only, group details are not be alterable except by members of the Administrator user group. Customer Center User Groups are described in "Users" on page 75.

5. Click **Save**. The Create and Edit Device Group page refreshes.
6. In the **Change Membership** section, click **Choose Device**. The Choose Device page opens in a new window.
7. Select the boxes beside all of the devices you want to add to the group, and then click **Choose Device(s)**. The Choose Devices page closes, and the Identifier(s) of the selected device(s) show in the **Change Membership** field.

   NOTE You can also add devices to the group manually. Click **Enter List of Devices**, and then enter device names in the field. Separate multiple entries with a comma.

8. Click **Add these Devices** to add the devices to the group.

Managing Device Groups

Use the Device Group page to manage Device Group membership. To open the Device Group Details page:

1. On the Device Groups page, click the group name link for the Device Group you want to edit. The Create and Edit Device Group page opens.

   NOTE You can also search for a particular Device Group by entering a value in the Search Criteria section, and then clicking **Show Results**.

2. Make the appropriate changes and then click **Save**.

NOTE When first created, device groups do not have any Identifiers associated with them, therefore the Members table on the Device Groups page does not contain any entries.

Device Group – Group information

You can modify the following details using the Group Information section on the Create and Edit Device Group page:

- **Change the device group's name or description** — Edit the information in the field you want to update. Click **Save**. The page refreshes with a message stating that the device group information was successfully updated.
- **Lock the device group's name and description** — Select or clear the **Lock as Read-only** checkbox.

  NOTE When locked as read-only, group details are not be alterable except by members of the Administrator user group. Customer Center User Groups are described in "Users" on page 75.

Device Group – Change Membership

You can modify the following details using the Change Membership section on the Create and Edit Device Group page:

- **Add devices to the group** — Click **Choose Device**, and then select the appropriate devices.

NOTE You can also add devices to the group manually. Click **Enter List of Devices**, and then enter device names in the field. Separate multiple entries with a comma.

Device Group Details – Members

The Group Members table of the Device Groups Details page lists all devices included in the device group. You can remove selected devices from the group. The table includes the following fields for each listed device:

- **Select All** — a checkbox to select all entries
- **Identifier** — the Identifier associated with the device
- **Department** — the Department Name associated with the device
- **Device Name** — the Device Name
- **User Name** — the User Name associated with the device
- **Make** — the make of the device
- **Model Number** — the model number of the device

- **Serial Number** — the device's serial number
- **Asset Number** — the asset number assigned to the device

Removing devices from Device Groups

To remove any or all devices from a device group follow these steps:

1. On the Create and Edit Device Group page, select the checkbox in the **Select** column for the each device you want to remove.
2. Click **Remove Selected Device(s)**. The page refreshes with a message stating the selected devices are removed from the device group.

Deleting Device Groups

To delete a device group:

1. On the Create and Edit Device Group page, click **Delete This Group**. A confirmation message shows, warning that all associations with the device group will also be deleted. This means the group is no longer be listed in report filters and any alerts applied to the device group cease to function.
2. Click **OK** to confirm the deletion and return to the Device Groups page or click **Cancel** to cancel the delete operation.

Viewing and Editing the Device Summary for a Single Identifier

To view or alter the details associated with a specific Identifier, open the Device Summary page.

To open the Device Summary page click the Identifier link on any report or page that lists it. The Device Summary page is divided into four main sections:

- Asset Summary
- Hardware Summary
- Software Summary
- Call Tracking

Asset Summary

The Asset Summary section shows the following information for a specific Identifier:

- Identifier — unique identifier of the device
- Make
- Model
- Serial #
- Device Name

- Full Windows Device Name (Windows computers only)
- Windows Domain (Windows computers only)
- Workgroup (Windows computers only)
- Department
- User Name
- Assigned User Name
- Assigned User E-Mail Address
- Detected Asset Number
- Asset #
- Device Groups — lists all groups to which the device belongs

Users may modify and update the recorded values for **Department**, **Assigned User Name**, **Assigned User E-mail Address**, and **Asset #** fields by entering the appropriate information in the fields provided. To save changes, click **Save Changes**.

NOTE Depending on the type of device, some values in the Device Summary are not populated. For example, if the Identifier is a Windows Mobile device, only the subset of the hardware and software information relevant to Windows Mobile devices are shown.

Hardware Summary

The Hardware Summary section lists information on the hardware configuration of the device:

- **Detected Make**
- **Detected Model**
- **Detected Serial**

  NOTE Values listed in the Hardware Summary section for **Detected Make**, **Detected Model** and **Detected Serial Number** are captured by the Agent and may differ from the manually entered values listed in the Asset Summary section.

- **CPU**
- **RAM**
- **Drive Info** — lists detected information regarding the installed hard drives on the device. The following information is available:
  - **Volume** — the name of the detected hard drive partition.
  - **Type** — the type of the hard drive.
  - **File System** — the storage and organization method for the data and files saved on the device.

  - **Total Space** — the aggregate of used and unused storage capacity of the hard drive.
  - **Free Space** — the unused storage capacity of the hard drive.

- **Mobile Broadband Adapters** — lists detailed information about the mobile broadband adapters, also known as cellular modems, detected on the device. The following information is available:

  NOTE Mobile Broadband Adapter reporting and Monitoring Center Initiated Calling (MCIC) is currently available only for devices running Windows. These features are not available on Macintosh devices.

  IMPORTANT Before using Real Time Technology (RTT) including Mobile Broadband Adapter asset tracking, Monitoring Center Initiated Calling, and SMS Lock Requests, you need to activate these features for your account or individual Identifiers within your account. Contact Absolute Software Technical Support to activate these features. See "Technical Support" on page 15 for more information on contacting support.

  - **Manufacturer** — the name of the manufacturer of the mobile broadband adapter.
  - **Model**— the model number, if available, of the device.
  - **Network** — the mobile service provider associated with the mobile broadband adapter.
  - **Service Status** or availability of the network
  - **Details** link allowing access to the Mobile Broadband Adapter Details dialog box. See "Mobile Broadband Adapter Details Dialog Box" on page 64 for more information.
  - **Detected Phone Number** — the phone number associated with the mobile broadband adapter, as reported by the device.
  - **Phone Number Override** — the alternative or override phone number associated with the mobile device or broadband adapter. If Computrace does not automatically detect the phone number, the device automatically sends an SMS to the Monitoring Center. The reply-to address from the SMS becomes the value for the **Phone Number Override** field. See "Edit Phone Number Override Dialog Box" on page 65 for more information.

    NOTE The value of the **Phone Number Override** field takes precedence over the value of the **Detected Phone Number** field when sending SMS messages to devices.

  - **Attempt Forced Call** — send a request for an immediate Agent call to the device via SMS. Such calls are called Monitoring Center Initiated Calls (MCIC). See "Forced Call Log" on page 67 and "Initiating a Forced Call" on page 67 for more information.

- **Smart Phone Radios** — lists detailed information about the detected radios available on the device. The following information is available:
  - **Radio Type** — the mobile network radio available on the device. Possible values are:
    - GSM
    - CDMA
    - AMPS
  - **Equipment ID** — the identification number unique to the mobile device
  - **Subscriber ID** — the unique number associated with the subscriber; stored in the network radio, the Subscriber Identity Module (SIM) card, or equivalent.
  - **Detected Phone Number** — the phone number associated with the mobile device. as reported by the device.
  - **Phone Number Override** — the alternative or override phone number associated with the mobile device. If Computrace does not detect the phone number automatically, the device automatically sends an SMS to the Monitoring Center. The reply-to address from the SMS becomes the value for the **Phone Number Override** field.

Viewing Details of the Hardware on an Individual Device

To see a more complete list of the hardware installed on the machine, click the **Hardware Summary** tab. Exhaustive details about the machine are available in the **See Hardware Details** section.

To download the Printer Driver report which lists all printer drivers installed on the device:

➢ Click the **Download Printer Report** link. This report is identical to the "Printer Report" on page 100, with the exception that results are limited to printer drivers installed on this device.

Mobile Broadband Adapter Details Dialog Box

IMPORTANT Before using Real Time Technology (RTT) including Mobile Broadband Adapter asset tracking, Monitoring Center Initiated Calling, and SMS Lock Requests, you need to activate these features for your account or individual Identifiers within your account. Contact Absolute Software Technical Support to activate these features. See "Technical Support" on page 15 for more information on contacting support.

The Mobile Broadband Adapter Details dialog lists the following information about the adapter detected on the device:

- **Time Attributes Collected** — the date and time when information about the mobile broadband adapter installed on the device was collected.
- **Manufacturer** — the name of the manufacturer of the mobile broadband adapter.
- **Model** — the model number, if available, of the mobile broadband adapter.
- **Equipment ID** — the identification number unique to the mobile broadband adapter; usually available on the bottom of the notebook or on the removable mobile broadband adapter. For EVDO adapters, the Electronic Serial Number (ESN) and/or the Mobile Equipment ID (MEID) may be reported. For UMTS networks, the International Mobile Equipment Identifier (IMEI) is reported.
- **Subscriber ID** — the unique number associated with the subscriber; stored in the adapter, the Subscriber Identity Module (SIM) card, or equivalent.
- **Network** — the mobile service provider associated with the mobile device.
- **Service Status** — the last reported status of the availability of the associated network.
- **Detected Phone Number** — the phone number associated with the mobile broadband adapter. as reported by the device.
- **Phone Number Override** — the alternative or override phone number associated with the mobile device or broadband adapter. If Computrace does not detect the phone number automatically, the device automatically sends an SMS to the Monitoring Center. The reply-to address from the SMS becomes the value for the **Phone Number Override** field. You can edit the phone number using the **Edit Phone Number Override** dialog box.

To return to the Device Summary page:

➢ On the Mobile Broadband Adapter Details dialog box, click **Close**.

Edit Phone Number Override Dialog Box

IMPORTANT Before using Real Time Technology (RTT) including Mobile Broadband Adapter asset tracking, Monitoring Center Initiated Calling, and SMS Lock Requests, you need to activate these features for your account or individual Identifiers within your account. Contact Absolute Software Technical Support to activate these features. See “Technical Support” on page 15 for more information on contacting support.

The Edit Phone Number Override dialog box allows you to enter a new phone number to use instead of the detected phone number when sending SMS text messages to the adapter. SMS text messages are used to contact devices as part of the MCIC and Intel AT SMS Lock Request features.

To set an override phone number:

1. On the **Edit Phone Number Override** dialog box, type the new phone number including country and area codes in the **Phone Number Override** field. The phone number should follow the format: +16045556789, without spaces, parentheses, periods, or hyphens.
2. Click **Set Override**. Customer Center closes the Edit Phone Number dialog box and opens the Device Summary page to show the new phone number override value in the **Mobile Broadband Adapters** area.

Software Summary

The Software Summary section lists the following information as detected by the Agent:

- Operating System
- OS Service Pack
- Symantec Antivirus installed

To review all the software applications detected on the device by the Agent, go to the report page. The report is described in "Software by Device Report" on page 104.

Call Tracking

The Call Tracking tab lists the following information regarding the operation of the Agent:

- Installation Date (date and time of first Agent call to the Monitoring Center)
- Version Number (Agent version number)
- Date and time of the last Agent call to the Monitoring Center (the **Agent Last Called On** field)
- Source IP address or telephone number of its last call to the Monitoring Center (the **Agent Last Called From** field)
- Next scheduled call time

If the device is equipped with Geolocation Tracking functionality, the Call Tracking section also shows the **Last Known Location** and the **Location Determination Date** for the device.

NOTE To view the Call History Report for the Identifier, go to the Call History Report page. To get detailed IP tracking or caller ID information, click the IP address or telephone number listed in the **Agent Last Called From** field. The Extended Call Information page opens. This page lists details regarding the location of the IP address or telephone number. See "Report Descriptions" on page 99.

Forced Call Log

IMPORTANT Before using Real Time Technology (RTT) including Mobile Broadband Adapter asset tracking, Monitoring Center Initiated Calling, and SMS Lock Requests, you need to activate these features for your account or individual Identifiers within your account. Contact Absolute Software Technical Support to activate these features. See "Technical Support" on page 15 for more information on contacting support.

The Forced Call Log tab shows detailed information about events associated with all forced calls attempted on a device. Typical events that may be included in the Forced Call Log include information about SMS messages sent to devices to initiate a call and SMS messages sent back from the device to acknowledge receipt of the forced call. The following information is available:

- **Time** — the date and time associated with a forced call-related event.
- **Type** — the category of the event related to the forced call. Possible events are: information, warning, or an error message.
- **Description** — the details of the events prompting the SMS message or forced call. When sending an SMS message, the description includes the phone number and initial status of the mobile service provider. When receiving a response, the description includes the phone number only.

Initiating a Forced Call

Monitoring Center Initiated Calling (MCIC), also known as forced calls, are SMS messages sent from the Monitoring Center to an Intel AT and RTT enabled device prompting the device to initiate an Agent call.

To force a call from a device:

IMPORTANT You can only attempt a forced call on a device that has a functioning mobile broadband adapter installed and identified by Computrace. See Prerequisites For Using Real-time Technology (RTT) for more information.

1. Open the Device Summary page for the device on which you want to attempt a forced call. See "Viewing and Editing the Device Summary for a Single Identifier" on page 61 for more information on searching for and opening a Device Summary page.
2. Do one of the following:
   - In the **Mobile Broadband Adapters** area on the **Hardware Summary** tab, click **Attempt Forced Call**. The Monitoring Center sends an SMS to the adapter, requesting an immediate call from the Agent. If the device is on and the mobile broadband adapter is within network coverage, the Agent initiates a call to the Monitoring Center. If conducive circumstances are not available, the Agent calls in when all

conditions are conducive and the adapter is able to receive the SMS message and/or initiate a call.

- In the **Smart Phone Radio** area on the **Hardware Summary** tab, click **Attempt Forced Call**. The Monitoring Center sends an SMS to the mobile device, requesting an immediate call from the Agent. If the device is on and the mobile broadband adapter is within network coverage, the Agent initiates a call to the Monitoring Center. If conducive circumstances are not available, the Agent calls in when all conditions are conducive and the mobile device is able to receive the SMS message and/or initiate a call.
-

You can view the status of the forced call request on the Forced Call Log tab. See “Forced Call Log” on page 67 for more information.

You can also force calls using MCIC as part of Data Delete, Device Freeze, and Intel AT lock requests. See “Using Data Delete” on page 178, “Using Device Freeze” on page 202, and “Using Intel Anti-Theft Technology” on page 144 for more information.

Automatic Device Group Assignment

Customer Center can be configured to assign devices to Device Groups automatically, based on the calling IP address of the device. This feature is useful if your network includes multiple subnets, each with a range of IP addresses. The following rules apply:

- If a device calls the Monitoring Center and its IP address is within the IP range specified in a Device Group, it is assigned to the Device Group associated with that subnet.
- If a device calls from an IP address that is not part of a range specified in a Device Group, the device is not assigned to a group.
- If a device is already in a Device Group, and calls in from an IP address that is not part of that Device Group or any other defined Device Group, the device stays in the original Device Group.
- If a device is already in a Device Group, and calls in from an IP address that is part of another defined Device Group, the device is reassigned to the new Device Group.

In the following example, two auto-grouping rules are defined:

- **Auto-group Lincoln High School:** IP Range 175.165.050.001 - 175.165.050.100
- **Auto-group Washington High School:** IP Range 175.165.050.101 - 175.165.050.200

If a teacher's computer calls in with the IP **175.165.050.025**, it is auto-assigned to the **Lincoln High School** group. The teacher then takes the computer home for the weekend, and it calls in from the teacher's home with the IP **123.134.075.013**. There is no auto-group rule for that IP range, so the computer stays in group Lincoln High School. It does not get unassigned from Lincoln due to the new IP address.

However, if the teacher then takes the computer to **Washington High School** for a few days, and it calls in from **175.165.050.150**, the computer gets assigned to a new group. Unlike the teacher's IP address at home, there is an auto-group range for that IP (Washington High School), so the computer is moved out of group Lincoln and into group Washington. It does get unassigned from Lincoln, provided there is another defined Device Group into which it can be assigned.

To use the auto-grouping feature of Customer Center, follow the three steps below:

1. **Create a resource CSV (comma separated value) file** — Define the IP subnets and device group associations existing in your organization in a two-column CSV file. This CSV file must use the column headings **GroupName** and **IPSubnet**. Populate the CSV file with the Device Group names you want to use, and with the IPSubnet to associate with each group. Use the asterisk (*) as a wild card to group devices calling from different subnets. Refer to the sample below.

GroupName	IPSubnet
IP Group One	192.168.*.*
IP Group Two	172.16.*.*
IP Group Three	10.*.*.*

2. **Import the CSV file into Customer Center** — When you have prepared your CSV file, you must upload it to Customer Center using the Import Groups <-> IP Mapping page. To open the page, from the Administration home page, click the **Groups** link, and then click the **Import Groups <-> IP Mapping** link. Enter a name for your import in the first field. This name is used to track the status of the CSV file import.

   NOTE CSV file imports are queued and processed offline. Most imports are completed within an hour of the file upload. You can track the progress of your import from the **Import Group <-> IP Mapping Status** page.

3. If you want to receive e-mail notification when the import is processed, enter your e-mail address in the field provided.
4. Verify the success of the CSV Import:
   a) Open the **Import Group <-> IP Mapping Status** page and review the import status in the table. When complete, the status is shown as **Ready**. If you entered an e-mail address, notification is sent.

   b) To verify the success of the import, click the **Ready** link and view the status CSV file. The status CSV file is identical to the

CSV file you uploaded, with the addition of two columns indicating the success of the import line by line.

NOTE See *Technical Note 050221 – Dynamic Group to IP Subnet Mapping* on the Customer Center Documentation page for more information.

Manual Device Group Assignment

You can manage membership in your Device Groups creating and uploading a CSV or XML file. You can download a CSV or XML file which lists all devices in any Device Group (including the All Devices group), with their Device Group associations. Management of Device Group associations is achieved by modifying and uploading the CSV or XML file back into the Customer Center. Using this process, you can associate each device with up to twenty different device groups.

To define Device Group associations manually:

1. Request Download of Current Device Group Associations as follows:

    a) On the Groups page, click the **Export Groups** link to open the Export Groups page.

    b) Select the appropriate group from the **Group** list.

    c) Name the file in the **Name** field and select a format in the **Format** list.

    d) To receive e-mail notification when the export file is available, enter your e-mail address in the text filed provided. (Optional)

    e) Click **Continue**.

2. Retrieve Current Device Group Associations CSV or XML file as follows:

    a) On the Groups page, click the **Export Groups Status** link.

    b) When your request is processed, click the appropriate **Ready** link in the **Status** column.

    c) Follow the on-screen instructions to download the CSV or XML file. When prompted, choose the option to save the file to your local device.

3. Edit the Device Group Associations CSV or XML File as follows:

    a) Open the downloaded CSV or XML file.

    IMPORTANT You can open the CSV file with almost any text editing program. However, Absolute Software recommends editing the file with a spreadsheet editor to preserve the table layout. If the layout of the file is not preserved, the import process fails.

    b) Ensure that the 1st column for each row contains the device's Identifier. The file may contain additional columns useful to identify the device, such as Username, Device Make, or Device Model. These columns are ignored for the purposes of editing device group associations.

c) The last 20 columns of the CSV file refer to group memberships. Edit the last 20 columns of the CSV file to define device group memberships. You can use the CSV file to associate each listed device with up to 20 different Device Groups.

IMPORTANT Do not alter the format of the CSV or XML file. Doing so causes the data import process to fail. Additionally, changes should only be made to the last 20 columns of the CSV file. Changes to other data points are discarded and may cause the data import process to fail.

d) Save the modified CSV file to the desired location.

IMPORTANT Absolute Software recommends that you archive a copy of the original download file. Should an error occur during the import process, you can use the CSV or XML file to restore the data to its original state.

4. Upload the modified CSV or XML file as follows:

a) To open the Import Groups page, click the **Import Groups** link on the Groups page.

b) Enter a name for your import in the first field. This name is used to track the status of the CSV file import.

NOTE CSV and XML file imports are queued and processed offline. Most imports are completed within an hour of the file upload. You can track the progress of your import from the **Import Group <-> IP Mapping Status** page.

c) If you want to receive e-mail notification when the import is processed, enter your e-mail address in the **E-mail** field.

d) In the Filename area, click **Browse** to open the Choose File to Upload dialog box. Do the following:

- Browse to the location where you saved the modified CSV file in step 3.
- Click the file you want to upload, and then click **Open** to select the desired file. The Import Groups page opens to show the path to the selected file in the **Filename** field.

e) Select one of the following to specify whether to retain or remove existing group memberships:

- **DO NOT Delete Identifier Group Membership If Group Missing From Import** retains the existing group membership settings if the existing device group associations are not mentioned in the imported file. After the import process is complete, the device is associated with all existing device groups not specified in the import file and all new device groups specified in the imported file.

- **Delete Identifier Group Membership If Group Missing From Import** removes existing group associations if the device is associated with any device groups not available in the imported file. After the import process is complete, the device is only associated with the device groups specified in the imported file.

f) Click **Upload** to start the file import process.

5. Verify the success of the CSV or XML Import.

a) Open the **Import Group Status** page and review the import status in the table. When complete, the status is shown as **Ready** and, if you entered an e-mail address, notification is sent.

b) Click the **Ready** link and review the status CSV or XML file.

NOTE The status of the CSV file is identical to the file you uploaded, with the addition of two columns indicate the success of the import line by line.

Software Policy

Software policy allows administrators to define and group software requirements. A Software Policy is a list of Banned, Required, and Approved software titles. When you define a policy, it is applied to Device Groups, after which non-compliant devices can be identified via the Software Policy Non-Compliance report. See “Software Policy Non-compliance Report” on page 107. Software policy supports three categories of software titles:

- `Banned`
- `Required`
- `Approved`

Each Device Group can only be targeted by one software policy. As a single device can belong to multiple Device Groups, it is possible for a single device to be targeted by multiple software policies. In this scenario, the Software Policy Non-Compliance report shows any occurrence of non-compliance.

Creating a Software Policy

To define a software policy:

1. Click the **Software Policy** link on the global navigation bar or the Administration page. The Software Policy page opens.

2. Click the **Create and Edit a Software Policy** link. You can also navigate to the View and Manage Software Policies page and click **Create Software Policy**. The Create and Edit a Software Policy page opens.
3. Enter a descriptive name in the **Policy Name** field.
4. If you want, enter a brief description of the policy in the **Description** field.
5. Click **Add** showing next to the **Policy Groups** field. The Choose Groups for Software Policy dialog box opens.
6. Click to select the appropriate device groups in the **Available** column and click the right arrow. The selected device groups are moved to the **Selected** column.
7. After you have selected all the relevant groups, click **OK**. The Create and Edit a Software Policy screen refreshes, listing the selected groups in the **Policy Groups** field.

   NOTE To remove a group, highlight its name in the **Policy Groups** field and click **Remove**.

8. Define the Banned, Required, and Approved software lists for the Policy as follows:
   - To add applications to the Banned list:
     - Click the **Banned Items** tab, and then click **Add**. The Choose Software Licenses or Executable Programs dialog box opens.
     - In the dialog box, enter part or all of a Publisher or Application name in the **Filter** field.
     - Select the appropriate option to show licenses and/or executables in the list.
     - Select the appropriate option to show version independent or version specific licenses/executables.
     - If you want to see only the licenses installed on your organization's devices, select the **Show Only Licenses or Executable Programs** checkbox.
     - Click **Filter**.
     - Click a specific **Publisher** name to refresh the **Application** column to show the publisher's titles.
     - Double-click an **Application** name to add it to the **Selected** column. To remove an entry from the **Selected** list, double-click it in the list.
     - After you have selected the appropriate Applications, click **OK** to return to the New Software Policy page.
   - To add applications to the Required list:

    - Click the **Required Items** tab, and then click **Add**. The Choose Software Licenses or Executable Programs dialog box opens.
    - The process of adding an application to the Required list is identical to the process of adding an application to the Banned list. See “To add applications to the Banned list:” on page 73 for more information.
  - To add applications to the Approved list:
    - Click the **Approved Items** tab and click **Add**. The Choose Software Licenses or Executable Programs dialog box opens.
    - The process of adding an application to the Approved list is identical to the process of adding an application to the Banned list. See “To add applications to the Banned list:” on page 73 for more information.

9. Save the Software Policy by doing one of the following:
   - Click **Save & Close** to save the changes and go to the View and Manage Software Policies page.
   - Click **Save** to save the changes and refresh the Create and Edit Software Policy page.

Editing a Software Policy

To edit an existing Software Policy:

1. Click the **Software Policy** link on the global navigation bar or the Administration page. The Software Policy page opens.
2. Click the **View and Manage Software Policies** link. The View and Manage Software Policies page opens.
3. Click the **Edit** link for the policy you want to edit. The Create and Edit Software Policy page opens.
4. Modify the Software Policy:
   - To edit the name and description of the policy, modify the shown values by entering the new information in the appropriate fields.
   - To add or remove software titles from the Banned, Required, and Approved software lists, use the appropriate **Add** or **Remove**.

     NOTE To remove a software title you must highlight its name listed in the list, and then click **Remove**.
5. Click **Save & Close** to save your changes and return to the View and Manage Software Policies page.

Deleting a Software Policy

To delete a software policy:

1. Click the **Software Policy** link on the global navigation bar or the Administration page. The Software Policy page opens.
2. Click the **View and Manage Software Policies** link. The View and Manage Software Policies page opens.
3. Click the **Edit** link for the policy you want to edit. The Create and Edit Software Policy page opens.
4. Click **Delete**.

IMPORTANT Exercise caution in using the Delete functionality. When you click **Delete**, it deletes the policy without prompting you for a confirmation.

Users

Multi-level Security

The User section is designed to set up access rights and restrictions for users of the Customer Center. The multi-level security features of the Customer Center allow an authorized user to grant different access rights and privileges to specific users or groups of users.

To open the Users page:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Users** link on the global navigation bar or from the **Users** section on the Administration page. The Users page opens.

The following three user groups are defined within User Manager:

- **Administrator** — This user group has full access rights to all Customer Center features and can grant access rights to other users.

  Members of the Administrator group is always able to view all Identifiers associated with their account. Any number of Administrators can be defined.

- **Power User** — This user group has access rights to all Customer Center features, but these rights can be restricted to specific Identifiers or Device Groups.

  Members of the Power User group have identical access rights to the Administrator group with the exception that they can be restricted to viewing a specific Identifier or Device Group by an Administrator. Power Users can grant access rights to other Power Users, but can only edit their own access rights.

- **Guest** — This user group has access rights to view user information and generate reports.

  Members of the Guest group have limited access to Customer Center features. They cannot alter or assign user access rights and cannot alter details on the Device Summary page. Members of the Guest group can only browse Theft Reports they have created and can only view Saved Reports they have saved.

Appendix A: "User Access Rights" describes the access rights and restrictions of each of the three user groups.

The Users page shows a button for creating new users and a table listing the three user groups and the users assigned to each.

Creating New Users

Before creating a new user account, users should be familiar with the different access rights each of the user groups' grants. The different access rights are listed in the Access Rights matrix that is included in this document as Appendix A: "User Access Rights".

To create a new user:

1. Click the **View and Manage Users** link on the global navigation bar or on the Users page. The View and Manage Users page opens.
2. Click **Create New User**. The Create and Edit User page opens.

   NOTE To create a new user, click the **Create and Edit User** link on the global navigation bar or on the Users page.

3. In the **User details** area, provide the following information:
   a) Enter the e-mail address which is used to send e-mail notifications to the user in the **E-mail** field.

   b) Enter a user name for the user in the **Username** field.

   NOTE The username must be a minimum of six characters in length.

   c) Select a role and the access rights for the user in the **Role** list.

   d) Enter the user's first and last names in the **First Name** and **Last Name** fields respectively.

   e) Enter an access password for this user to log on in the **Set Password** field.

   NOTE The password must be a minimum six characters in length.

f) Enter the access password again in the **Confirm Password** field.

g) Select all appropriate options from the following:

   - **User must change Password upon next login** — force user to change the login password upon next successful login.
   - **User must change Password every 30 days** — force the user to change the login password every 30 days.
   - **Require strong password** — allow user to only use strong passwords. Strong passwords must be at least 8 characters long; and must contain a mix of upper and lower case alpha characters, numeric characters, or symbols.

h) If you want to restrict the user's access to a single Identifier or device group, select a value from the **Device Group** list.

NOTE Only one Identifier or device group can be selected for an individual user. It may be necessary to create a new device group to limit a specific user's monitoring rights.

4. In the **User System Settings** area, provide the following information:

   a) Select the language and associated locale from the **Default User Language and Locale** list.

   b) Select a time zone from the **Default Time Zone** list.

   c) Select a value from the **Default User Session Timeout** list.

5. In the **User Status and suspension settings** area, provide appropriate information in the following sections:

   ○ **User Status** — Select the appropriate status from the following:

   - **Active** — Select this option to activate disabled or suspended users. This is the default value for new and existing users.
   - **Suspended** — Select this option to manually suspend an active user.
   - **Temporarily suspend until** — Select this option, and click the field to show a calendar dialog box. Select a date in the dialog box to specify an end date for the suspension.

   ○ **Auto-suspension on failed login** — Select the appropriate auto-suspension setting from the following:

   - **Never auto-suspend user on failed login** — Select this option to allow unlimited failed login attempts for the user.
   - **Auto-suspend user after 3 failed login attempts** — Select this option to automatically suspend a user after

3 failed login attempts. This is the default setting for all users, unless specifically selected otherwise. This option requires manual re-enabling of the user account by the administrator.

- **Temporarily auto-suspend user for 24 hours after 3 failed login attempts** — Select this option to automatically suspend a user for 24 hours from the time of the last failed login attempt, upon 3 failed login attempts.
- **E-mail all administrators if a user is suspended due to inactivity** — Select this checkbox to send an automatic e-mail notification to all administrators in your account whenever a user is suspended due to failed login attempts.

○ **Auto-suspension due to inactivity** — Select the appropriate auto-suspension setting from the following:

- **Never auto-suspend due to inactivity** — Select this option to allow users to login to Customer Center after long periods of time.
- **Auto-suspend if user has not logged in for 30 days** — Select this option to automatically suspend a user, if the user account is not used for a specified period of time.

6. After you enter all the appropriate information for the new user, click **Save**. The View and Manage User page opens to show a message stating the new user was created successfully and the details of the new user in the Users table.

Altering Existing User’s Details

To view or modify information for an existing user:

1. On the View and Manage Users page, click the **Edit** link for the appropriate user. The Manage User Details page opens.
2. Modify the appropriate information for the user on this page.
3. Click **Save Changes** to save the changes and return to the View and Manage Users page.

Changing Group Membership

To view or modify information for an existing user:

1. On the View and Manage Users page, click the **Edit** link for the appropriate user. The Manage User Details page opens.
2. Assign the user to a different User Group by selecting a new role from the **Role** list.

3. Click **Save Changes** to save the updated information and return to the View and Manage Uses page.

Deleting Users

To delete a user account:

1. On the View and Manage Users page, click the **Edit** link for the appropriate user. The Manage User Details page opens.
2. Click **Delete**. A message opens to warn you that you are about to delete the user account permanently.
3. To complete the deletion of the user account, click the **OK** to delete the user and return to the View and Manage Users page.

Account

The Account section of Customer Center includes the following sections:

- **Account Settings** — This section allows users to change their access password and to define the session time-out duration for their account.
- **Add Licenses** — This section allows users to add additional Agent licenses to their account.
- **Download Packages** — This section provides a download link for all available versions of the Agent and the Absolute Manage packages prepared for your account.
- **System Notifications** — This section lets users to send e-mail notifications of system notification messages.
- **Disable Pre-Authorizations** — This section lets Security Administrators to revoke all pre-authorizations in the event of a security breach.
- **Create and View Agent Removal Requests** — This section lets Administrators to remove the Agent from one or more devices.

Editing Account Settings

To edit Account Settings:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Account** link on the global navigation bar or the Administration page. The Account page opens.
3. Click the **Account Settings** link on the global navigation bar or the Account page. The Account Settings page opens.
4. Modify the default locale for the account by selecting a new value in the Default Language and Locale list. Changing this value changes the default language and time display formats showing across all pages in Customer Center.

5. Modify the default time zone for the account by selecting a new value in the **Default Timezone** list. Changing the default time zone updates the local times across all pages in Customer Center.
6. Click **Save Changes**.

Adding Licenses

The Add Licenses page allows you to add additional Agent licenses to your account. Licenses for a particular product are bundled together and sold as Product Keys. For example, 10 licenses of Computrace® Complete with a 3-year term could be grouped together as a single Product Key.

Product Keys are available from your reseller, or can be purchased directly from Absolute Software.

To add licenses to your account:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Account** link on the global navigation bar or the Administration page. The Account page opens.
3. Click the **Add Licenses** link on the global navigation bar or the Account page. The Add Licenses page opens.
4. Enter your Product Keygroup, and then click **Add**. Repeat this process to add all additional keys.
5. Once you have entered all Product Keys, click **Save**. You receive a confirmation message indicating that your account is being configured. New Agent files are created for your additional licenses.
6. Once you have registered all of your Product Keys, continue to the **Download Packages** page and download your Agent. The **License Summary** widget on the home page is also updated to show the additional licenses for your account. See "Dashboard" on page 24 for more information.

NOTE For more information on purchasing additional licenses, contact Absolute Software directly at http://www.absolute.com/purchase.asp.

Downloading Packages For Your Account

The Download Packages page contains the following sections:

- The **Agent** section allows you to download all Agent installation packages for your account. See "Downloading the Agent" on page 81 for more information.
- The **Absolute Manage** section allows you to download Absolute Manage installation packages and monitor the data extraction status for

your account. See "Using the Absolute Manage section" on page 82 for more information.

Downloading the Agent

The Agent section on the Download Packages page provides links to all Agent installation packages which are *stamped* for your account. The following information is listed for each installation package:

- **Agent Type** — platform-specific Agent type. The Agent is currently supported on Windows, Mac, Windows Mobile, BlackBerry and S60 platforms.
- **Agent Version** — the version (build) number of the Agent
- **Last Updated** — the date and time the Agent files were created.
- **Last Downloaded** — the date and time the Agent files were last downloaded from Customer Center.

To download the stamped Agent installation files:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Account** link on the global navigation bar or the Administration page. The Account page opens.
3. Click the **Download Packages** link on the global navigation bar or the Account page. The Download Packages page opens.
4. In the **Agent** section, click the appropriate link in the **Agent Type** column.
5. Follow the on-screen instructions to complete the download.
6. After the Agent is installed on a client device, the device is automatically associated with your account.

Refer to the *Agent Installation Guide* available on the Documentation page in Customer Center for more information on installing the Agent on different platforms.

Upgrading to the Latest Version of the Agent

Periodically, Absolute Software releases a new version of the Agent. When a new Agent is available, an announcement is posted on the Home Page. If you are running an older version of the Agent and want to upgrade, contact Absolute Technical Support at http://www.absolute.com/support. A support representative creates new Agent files for you and informs you when the files are ready for download from the Download Packages page.

IMPORTANT The Agent listing on the Download Packages page is not automatically updated when a new Agent version is released. You must contact Technical Support if you want to upgrade your Agent.

Downloading the McAfee ePolicy Agent

For some Customer Center accounts, the Agent section also contains a section called McAfee ePolicy Agent (ePO Agent), which provides a link to the stamped Absolute McAfee ePO enabled Agent. The McAfee ePO enabled Agent is available for organizations and network administrators who use McAfee ePO or who want to start using ePO to manage security on their networks. Customers can get a complimentary copy of ePO directly from McAfee, if they do not already have ePO installed. The McAfee ePO Agent enables reporting of Agent calls within the ePO console and helps answer a customer's three core security questions. Refer to the *McAfee ePO Agent User's Guide* for information on installing and using the ePO Agent.

Using the Absolute Manage section

The Absolute Manage suite is a uniquely seamless, multi-platform client management solution for managing all of your Mac OS and Windows workstations in a single unified console on the platform of your choice. All Absolute Manage components including the server, admin console and clients can be mixed and matched from either platform. Network and system administrators often find that there are multiple ways to accomplish the same task within Absolute Manage, and it is up to them to decide which one fits into the organizational workflow and works best in the proprietary computing environment.

The Absolute Manage installation packages available in the Absolute Manage section allow administrators to extract, download and use the data collected by Agents on managed devices. For accounts including Absolute Manage, the data that was previously available only via reports on Customer Center is now available using the Absolute Manage application on the local device. The Absolute Manage section allows you to perform the following functions:

- Downloading the Absolute Manage Installation Packages
- Monitoring Absolute Manage Data Extraction Status
- Uploading a Stamped Agent Including Absolute Manage

Downloading the Absolute Manage Installation Packages

To download the Absolute Manage packages for your operating system:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Account** link on the global navigation bar or the Administration page. The Account page opens.
3. Click the **Download Packages** link on the global navigation bar or the Account page. The Download Packages page opens.

4. In the Absolute Manage section, click the appropriate link from the following:
   - ○ **Download Absolute Manage for Windows Computers**
   - ○ **Download Absolute Manage for Macintosh Computers**
5. Follow the on-screen instructions to complete download.
6. Install the Absolute Manage application on your device. When prompted, provide the **Registration Code** and the **Serial Number** available on the Download Packages page.

   NOTE The Registration Code and the Serial Number showing in the Absolute Manage section are specific to your account.

   For more information refer to the *Getting Started Guide* and the *Absolute Manage User Guide* for your operating system available on the *Documentation* page of Customer Center.

Monitoring Absolute Manage Data Extraction Status

The Absolute Manage section on the Download Packages page also allows you to monitor the extraction status of your device and reports related data. The following information is available:

- **Data Extract Status** — the current status of the data extraction process. Depending upon the information received from Agents on managed devices and the date and time of the last synchronization call to the Absolute Manage server, the status can be any of the following:
  - ○ **Disabled** — Absolute Manage data extraction is not enabled for the account. Contact Absolute Software Global Support for more information or to enable extraction for your account. See "Technical Support" on page 15 for contact details.
  - ○ **First Extraction Queued** — Data extraction process for your account has not been completed, but is scheduled for completion within the next 24 hours. Once data extraction is complete, you can download your Absolute Manage data using the Absolute Insight application.
  - ○ **Delta Extraction Queued** — The reporting data extraction process for your account was completed on the date shown. Depending upon the settings for your account, a subsequent data extraction process is scheduled. A **Delta Extraction Queued** status indicates that the primary data extraction process is complete, and you can download the Absolute Manage data using the Absolute Insight application.
  - ○ **Data Extraction In Progress** — The data extraction process is currently running and is scheduled for completion within the next 24 hours. Once data extraction is complete, you can download your Absolute Manage data using the Absolute Insight application.

- **Account ID** — The unique account identification number associated with your account.
- **Password** — The system-generated passcode that you need to provide when viewing extracted data using the Absolute Manage application.

Uploading a Stamped Agent Including Absolute Manage

The Agents on devices managed using the Absolute Manage server contain a special Agent. You can create a modified Agent Installation Package to reinstall the Agent containing Absolute Manage components in the event that the Agent on one of your managed devices is removed. The Upload Absolute Manage Agent area in the Absolute Manage section allows you to upload a modified Windows Agent Installation Package for use at a later date.

The installation package can have any name, as long as it is a valid ZIP file. The file name changes to a system generated name upon successful upload. To ensure that the file is uploaded successfully, the installation package you are uploading must conform to the following manifest:

- The package must be a valid ZIP file. Any package extraction errors lead to showing a validation failure error and the failure of the upload process.
- The package must contain the following files:
  - \Absolute Manage Agent\0x0409.ini
  - \Absolute Manage Agent\AgentVersion.exe
  - \Absolute Manage Agent\Data1.cab
  - \Absolute Manage Agent\DefaultDefaults.plist
  - \Absolute Manage Agent\Info.plist
  - \Absolute Manage Agent\instmsiw.exe
  - \Absolute Manage Agent\ISScript9.msi
  - \Absolute Manage Agent\LANrev Agent.msi
  - \Absolute Manage Agent\LANrevAgentSafeInstaller.exe
  - \Absolute Manage Agent\LANrevAgentUpdater.bat
  - \Absolute Manage Agent\LANrevAgentUpdater.exe
  - \Absolute Manage Agent\LANrevAgentUpdater_Launcher.bat
  - \Absolute Manage Agent\setup.exe
  - \Absolute Manage Agent\Setup.ini
- The **DefaultDefaults.plist** file must contain a “ServerList” configuration with at least one primary inventory server and an address. See http://www.lanrev.com/forum/viewtopic.php?t=230 for more information.
- The **Info.plist** file must contain a “CFBundleGetInfoString” XML element with appropriate and valid content.

To upload a modified Agent installation package:

IMPORTANT Currently, the upload functionality is supported only for Windows Agents.

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Account** link on the global navigation bar or the Administration page. The Account page opens.
3. Click the **Download Packages** link on the global navigation bar or the Account page. The Download Packages page opens.
4. In the Absolute Manage section, click **Browse**. A File Upload dialog box opens.
5. Browse to the location on the local hard disk of your device to find the appropriate Agent Installation file.
6. In the File Upload dialog box, click the **file name**, and then click **Open** to select the file. The Download Packages page refreshes to list the file name in the Filename field in the Absolute Manage section.
7. Click **Upload**. The file is uploaded to Customer Center and the Download Packages page refreshes to show the file in the Upload Absolute Manage Agent table.

Managing Agent Removal Requests

In Customer Center accounts with a lot of devices, there may be more than a few devices that are no longer functional or are being retired due to one or more reasons. IT administrators need to remove the Agent from such devices and free up the licenses in use.

Customer Center lets you remove the Agent from one or more of your devices, whether or not these devices are part of a device group. Depending upon how your Customer Center account is set up, the Security Administrator or Administrator users can use this new self-serve Agent removal feature to create new Agent removal requests as well as manage existing requests. The following two scenarios can occur:

- If your Customer Center account contains at least one Security Administrator, *only* the Security Administrator can use the self-serve Agent removal feature.
- If your Customer Center account does not contain any Security Administrators, any Administrator level user can use the self-serve Agent removal feature.

Minimum System Requirements For Agent Removal

Currently, the self-serve Agent removal feature is available for devices that meet the following requirements:

1. The device is running one of the following operating systems:
   - Windows
   - Mac
   - Linux

   IMPORTANT If you want to remove the Agent from a device running any other operating system, such as Windows Mobile, Symbian (S60), or BlackBerry, contact Absolute Software Global Support. See "Technical Support" on page 15 for more information on how to contact Absolute Software Global Support.

2. The device does not have an active Agent removal request or one of the data and device security features enabled. You cannot remove the Agent from a device if the device:
   - Has an open Agent removal request.
   - Was reported lost or stolen and has an open Theft Report. You must cancel the Theft Report before continuing. For information about reporting a device lost or stolen see "Theft Reporting" on page 172.
   - Includes active Intel AT features. You must turn Intel AT off before continuing. For information about turning Intel AT features off see "Turning AT On or Off" on page 160.
   - Is locked using Intel AT. You must unlock the device and turn Intel AT off before continuing. For information about unlocking devices see "Unlocking Locked Devices" on page 168.
   - Is frozen using Device Freeze. You must unfreeze the device before continuing. For information on unfreezing devices see "Unfreezing a Frozen Device" on page 210.
   - Contains an encrypted volume, with or without data in the encrypted volume. You must remove encryption from all encrypted volumes on the target device before continuing. For more information on removing encryption from encrypted devices see "Removing Volume Encryption" on page 226.
   - Has an active Remote File Retrieval request. You must cancel the File Retrieval request before continuing. For more information on canceling a file retrieval request see "Canceling a File Retrieval Request" on page 235.

Creating a New Agent Removal Request

IMPORTANT Before creating a new Agent removal request, check that the device does not have an open Agent removal request or is running a data and device security feature. For more information see "Minimum System Requirements For Agent Removal" on page 85.

To remove the Agent from a qualifying device:

1. Click the **Administration** link on the global navigation bar to open the Administration page.
2. Click the **Account** link on the global navigation bar or the Administration page to open the Account page.
3. Click the **Create and View Agent Removal Requests** link on the global navigation bar or the Account page to open the Create and View Agent Removal Requests page.
4. Click **Create New Request for Agent Removal**. The Select Device(s) for Agent Removal dialog box opens.
5. In the **Device Group** list, select the appropriate Device Group to show a list of devices from which you need to remove the Agents.
6. If you want to provide specific details to show devices that meet specific criteria, enter the appropriate information in the **Field Includes** field. For example, if you want to show only the devices where the Username field starts with the word "Absolute", enter `Absolute` in the **Field Includes** field.
7. By default, the list of devices shown in the list of results are limited to only those devices from which you can remove the Agent. If you want to show all the devices matching the criteria you specified, clear the **Show eligible devices only** checkbox.
8. By default, all the devices that match your specified criteria are shown in the list. If you want to show only the devices that are dormant, select the **Show Dormant Devices only** checkbox.
9. Click **Filter**. The Select Device(s) for Agent Removal dialog box refreshes to show a list of devices matching your criteria.
10. Select the devices by doing one of the following:
    - ○ Select the individual checkboxes for the appropriate devices.
    - ○ To select all the devices shown, select the checkbox in the header. The Select All dialog box opens to ask you whether you want to select all the devices that meet the filter criteria or only the devices shown on the current page. Click **Select All** records or **This Page Only** as appropriate. The Select Device(s) for Agent Removal dialog box opens with the specified devices you have selected.
11. Click **Continue**. The Set Device(s) for Agent Removal Authorization dialog box opens.
12. One of the following happens:
    - ○ If you are a Security Administrator, you are prompted to provide authorization. Enter your Customer Center password and the Authorization Code and continue to step 13. For more information about Authorization Codes, see "Authorization Codes" on page 31.
    - ○ If you are an Administrator level user, continue to step 13.

13. Click **Set For Removal**. An Agent Removal request for the devices you have selected is created and runs on the target devices on the next Agent call.

Intel Anti-theft Technology

The Intel® Anti-theft Technology section allows you to administer devices equipped with Intel® Anti-theft Technology (AT). See “Using Intel Anti-Theft Technology” on page 144 for details.

System Notifications

The System Notifications page allows Customer Center administrators to configure a list of recipients for system notification messages. System notifications are auto-generated messages warning the user(s) of potential problems with the account.

For example, if one of your Devices covered by the Service Guarantee stops calling the Monitoring Center, the **Devices With The Service Guarantee Not Calling** system notification warns you that the device is no longer calling.

System notifications are sent to the list of recipients by e-mail. You likely want to include all Customer Center system administrators on your recipient list. You are limited to twenty (20) recipients per notification.

To update the System Notifications page:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Account** link on the global navigation bar or the Administration page. The Account page opens.
3. Click the **System Notifications** link on the global navigation bar or the Account page. The System Notifications page opens.
4. Click the appropriate tab and edit the list of e-mail addresses.
5. Click **Save**.

Devices With The Service Guarantee Not Calling

The **Devices With The Service Guarantee Not Calling** system notification warns recipients that one or more of their devices covered by the Service Guarantee has stopped calling the Monitoring Center.

To edit the Devices With The Service Guarantee Not Calling system notification:

1. Click the **System Notifications** link on the global navigation bar or the Account page. The System Notifications page opens.

2. Click the **Devices With The Service Guarantee Not Calling** tab.

    - **To add recipients** — Select the **Enable Notification for All E-mail Addresses Below** option and enter the e-mail addresses of the appropriate recipients in the **E-mail Addresses for Notification** field.

      NOTE You can add a maximum of twenty (20) e-mail addresses in this field. Separate each entry with a semicolon.

    - **To remove recipients** — Select the **Disable Notification for All E-mail Addresses Below** option and enter the e-mail addresses of the appropriate recipients in the **E-mail Addresses for Notification** field. To remove multiple recipients simultaneously, separate each entry with a semicolon. Click **Save** to save any changes.
    - **To disable the system notification** — Select the **Disable Notification for All E-mail Addresses Below** option and remove all e-mail addresses from the list of the recipients.

3. Click **Save**.

Recovery Flag Disparity

The **Recovery Flag Disparity** system notification warns recipients that the number of Devices with the recovery flag set exceeds the number of licenses with the recovery service purchased.

1. Click the **System Notifications** link on the global navigation bar or the Account page. The System Notifications page opens.
2. Click the **Recovery Flag Disparity** tab.
3. **To add recipients** — Enter the e-mail addresses of the appropriate recipients in the **E-mail Addresses for Notification** field.

NOTE You can add a maximum of twenty (20) e-mail addresses in this field. Separate each entry with a semicolon.

4. **To remove recipients** — Remove the e-mail addresses of the appropriate recipients in the **E-mail Addresses for Notification** field. Make sure that all remaining entries are separated with a semicolon, with no spaces.
5. **To disable the system notification** — Remove all e-mail addresses from the recipient list.
6. Click **Save**.

Chapter 4 Generating Reports

This chapter describes how to use Customer Center to generate reports based on the data the Agent collects from monitored devices. Reports can be customized and filtered to focus on key areas of interest.

Customer Center shows most reports on-screen. You can also download report results in CSV or XML format. Typically, downloading report results provides more information than viewing results on screen. For a few reports, results are available in CSV or XML format only.

If you create a customized report, you can save the report's criteria. You can retrieve saved report criteria on subsequent visits to Customer Center and regenerate the report to show updated results.

NOTE When a report is saved, the filter criteria is saved rather than the results because data changes over time.

Several features are common to most Customer Center reports:

- Running reports
- Navigating reports
- Using the Choose feature
- Changing report sort order
- Modifying asset information
- Printing reports
- Saving reports
- Modifying Saved Report Filters
- Downloading reports

Running Reports

To show a report in Customer Center:

1. Log in to Customer Center. The Customer Center home page opens.
2. Click the **Reports** link on the global navigation bar.
3. In the **Reports** window, click the report to run.

OR

In the global navigation bar, click the category containing the report to run, and then click the report.

NOTE See “Report Descriptions” on page 99 for an overview of each Customer Center report.

4. If necessary, click **Accept** to agree to the terms and conditions of running the report.
5. In the **Search Criteria** pane, specify how to filter report results.

NOTE When first opened, some reports return results based on default filter criteria. See “Report Filter Criteria” on page 124, for details on available filter criteria for a report. See “Using the Choose Feature” on page 92, for information about using the Choose feature.

6. Click **Show Results**. If no records match your filter criteria, Customer Center shows the message **No records found matching your search criteria**.

NOTE For details on data Customer Center shows in the output of a report, see “Displayed Report Output” on page 129. For information on downloading CSV or XML output for reports that Customer Center shows on screen, see “Downloading Reports” on page 95. For information on preparing reports with results only available for download, see the individual report in “Report Descriptions” on page 99.

If your Customer Center session times out when you are viewing a report, a time-out warning message shows. Follow the on-screen instructions to continue.

Navigating Reports

The Search Criteria can expand or collapse by using the button on the far right. The Expand/Collapse button shows the upward arrows or downward arrows, depending on whether the Search Criteria section is expanded or collapsed, respectively.

Columns in Reports are presented in a horizontal format. To see the entire row in the report record, simply drag the bottom scroll bar to the right.

Tomove to a specific page of the report, click the page number located above the right-most column. A maximum of ten pages at a time can be listed. To move to the next page, click the **Next** link at the right of the number set or to move to the previous page click the **Previous** link at the left of the number set. To move to the first page in the set, click the **First** link at the left of the **Previous** link.

The default number of records shown in each report depends upon the report. You can change the default value by selecting the appropriate number in the **Per Page** list at the bottom of the report page.

Using the Choose Feature

Many areas of the Customer Center require the user to enter specific data such as an Identifier or serial number. To avoid human error, most reports include a **Choose** button.

To use the Choose feature:

1. Click **Choose** on any page. The Choose dialog box opens to show a table listing all the available valid values for the data field in question.
2. Click the appropriate value to select it. A progress indicator opens to provide information about the selection process. When processing is complete, the selected value is entered into the appropriate field of the report filter.

Changing Sort Order

Most reports are initially sorted by Identifier. To sort a report by any other criterion (included as the column headings of the report), simply click the column heading.

Modifying Asset Information

Each device on which the Agent is installed is given a unique **Identifier** by the Monitoring Center. Clicking an **Identifier** opens the Device Summary report that can be used to update the information associated with a particular Identifier. For example, if an Identifier is transferred to a new device, you can change the device information attached to that **Identifier**. To update information attached to an **Identifier**:

1. In any report, click the **Identifier** you want to modify. The Device Summary page opens.
2. Type or use available lists to enter new information in appropriate fields.
3. Click **Save Changes**. The Device Summary page updates to confirm that your changes are saved.
4. To regenerate the report and view modifications, click the **Back** link.

NOTE To return to the report, click the browser’s **Back** button. Note that returning does not refresh the report with changes. You must regenerate the report to see your modifications.

See “Viewing and Editing the Device Summary for a Single Identifier” on page 61 for a detailed explanation of the Device Summary page.

Assigned User Name

Assigned Username is a static, editable field allowing administrators to identify to whom a device was originally assigned. The static field is useful in organizations where end-user network IDs are not easily identifiable. Also, in many organizations, staff members periodically swap their devices. In these environments, a network ID or e-mail address does not accurately identify the actual owner of a device.

NOTE The **Assigned Username** field is appended to all report downloads that include an Identifier or user name, regardless of whether the **Assigned Username** field is included in the actual Customer Center report.

Dormant Devices

Dormant is a static, editable field allowing administrators to identify devices that are not expected to contact the Monitoring Center. The field helps administrators distinguish devices that are truly missing from devices that are located in places without access to an Internet connection, such as storage facilities. For more information on how to set user-defined fields, see “Viewing and Editing User-defined Fields Data” on page 45.

IMPORTANT Setting devices as **Dormant** results in devices being excluded from the Missing Devices report and from the Agent Call Rate Widgets. For more information, see “Missing Devices Report” on page 111 and “Dashboard” on page 24.

Printing Reports

Reports can be printed in whole or in part. Each page on a report includes a **Print** icon. Clicking the **Print** icon generates a version of the current page of the report optimized for creating a hardcopy.

NOTE By default, the current page shows 10 records from the entire report. To print a larger selection of records, use the **Per Page** list to select appropriate number of records to show on the page.

To generate a version of the current page of a report for printing:

1. In any report page, click 🖨.
2. The current page is downloaded into an MS Excel spreadsheet. Print the report page using Excel.

Saving Report Filters

Most reports allow the user to modify the shown data. Customized reports may be saved using the **Save Report Filter** feature.

NOTE Saved reports define the criteria for a report, not the existing data. The actual data that meets these criteria changes with time, altering the show of the saved report.

To save a report filter:

1. In any report window, click 💾.
2. Enter a name (not more than 48 characters) for the saved report.
3. Click **OK**. When you click **OK**, the dialog box refreshes to show that the report was successfully saved.
4. Click **Close** to exit the dialog box.

The report is available under **My Filters** in the **My Content** section of Customer Center.

Modifying Saved Report Filters

To modify a saved report filter:

1. Click the **Reports** link on the global navigation bar, and then click the **My Content** link. The My Content page opens.
2. Click the **My Filters** link on the global navigation bar or the My Content page. The My Filters page opens to show a list of saved filters.
3. Click the appropriate Filter name to select it for modification. The Asset Report page opens, showing the original filters that were saved.
4. Modify the existing filters, and then click the **Save Report Filters** icon. Enter a new name for your report filter, and then click **OK**. A new saved report filter is created.

   NOTE The original saved report filter remains unchanged.

Downloading Reports

Users can download any Customer Center report in whole or in part. Requests for report downloads are queued and processed offline. When processed, report downloads are made available from the My Reports page. Report data can be downloaded in a Comma Separated Values (CSV) or an XML format.

Downloading a report typically provides more information in results than viewing the output for the same report on screen.

To download a report:

1. In any report window, define any appropriate filters.
2. Click **Show Results**.
3. When the report shows, click ⬇.
4. Enter a name for the report in the **Report Name** field.
5. Select a value (CSV or XML) from the **Report Format** list.
6. If you want to receive e-mail notification when the download is available, enter your e-mail address in the **Create Email Alert** field.
7. Click **Continue** to queue the download.

When your request is processed, you can retrieve the report file from the **My Reports** page.

1. Click the **My Content** link in the global navigation bar or on the Reports page. The My Content page opens.
2. Click the My Reports link in the global navigation bar or on the My Content page. The My Reports page opens.
3. Click the **Ready** link in the Status column.
4. Follow the on-screen instructions to download the file.

NOTE When your file request is being processed, the status column shows `Pending` and the report is not available. When processed, the status column shows the **Ready** link and, if configured to do so, Customer Center sends an e-mail notification.

Multi-level Security

The multi-level security features of the Customer Center allow an authorized user to grant different access rights and privileges on reports to specific users or groups of users. There are three different user access levels: Administrator, Power User, and Guest.

User accounts are fully described in “Users” on page 75. Additionally, Appendix A: “User Access Rights” describes the access rights and restrictions of each of the three user groups.

Chapter 5 Reports Reference

Customer Center reports help track and manage your assets, allowing you to review many information types, including the following:

- Lease deadlines
- Hardware requirements
- Software requirements
- Software License status
- Necessary upgrades

The **Reports** tab of the Absolute Customer Center contains a list of all reports available in the system. Reports are organized into several categories:

- Hardware Assets
- Software Assets
- Security
- Call History and Loss Control
- Lease and Inventory Management
- Account Management

Service Levels and Reports

The Customer Center reports available to you depend on the level of service you have purchased. Computrace® Plus reports are available to all customers. Computrace® Plus customers do not have access to advanced Secure Asset Tracking™ reports and are not eligible for a Service Guarantee.

NOTE For purchase enquiries, contact Absolute Software's sales department by e-mail at sales@absolute.com. For Computrace® One™ sales enquiries, e-mail sales@EMEA.absolute.com. See "Technical Support" on page 15 for complete contact information.

Table 1 on page 98 lists the Customer Center reports available with each product.

Table 1. Customer Center Reports by Product

Report	Computrace Plus	Absolute Track Computrace Complete Computrace Data Protection Computrace One
Hardware Assets		
Asset	✓	✓
Printer	✓	✓
Monitor	✓	✓
Hardware Configuration Change	✘	✓
Hard Disk Space	✘	✓
Device Readiness	✓	✓
Mobile Broadband Adapter	✘	✓
Smart Phone Report	✘	✓
Software Assets		
Installed Software Overview	✘	✓
Software Configuration Change	✘	✓
Software By Device	✘	✓
Software License Compliance Overview	✘	✓
Microsoft Audit Summary	✓	✓
Software Policy Non-compliance	✘	✓
Installed Programs By Device	✘	✓
Installed Programs By Account	✘	✓
Security		
Operating System Updates	✘	✓
Internet Browsing Configuration	✘	✓
Unauthorized Software	✘	✓
Anti-malware	✓	✓
Missing Anti-malware	✘	✓
Modem Addition	✘	✓
Suspicious Devices	✓	✓
Call History and Loss Control		
Call History	✓	✓
Missing Devices	✓	✓
Device Drift by Device Name	✓	✓
Device Drift by Username	✓	✓
Activation	✓	✓
Device Location	✓	✓

Table 1. Customer Center Reports by Product

Report	Computrace Plus	Absolute Track Computrace Complete Computrace Data Protection Computrace One
Device Location History	✓	✓
Lease and Inventory Management		
Lease Completion	✓	✓
User-entered Data	✓	✓
Account Management		
License Usage Summary	✓	✓
Calling Profiles	✓	✓
User Audit Report	✓	✓
User Event Report	✓	✓

Report Descriptions

The following section describes each Customer Center report.

Customer Center reports vary widely in scope. Some reports are broad and include a summary of numerous assets, and others focus and specify minute details pertaining to a single device.

Hardware Asset Reports

Asset Report

The Asset report shows all devices in your organization that have the Agent installed. The report lists devices in ascending order by Identifier. You can customize the report to show a subset of devices that meet criteria. For example to list all the devices in a particular department.

NOTE By default, the Asset report shows dormant devices. To exclude dormant devices, de-select the **Include Dormant Devices** checkbox located at the bottom of the **Search Criteria** pane.

NOTE For Windows Mobile devices, the Asset report shows a subset of information.

Printer Report

The Printer Report does not show data on-screen. Instead, the printer report enables users to download a CSV (comma separated value) file that identifies installed printer drivers.

To download a Printer Report:

1. Click the **Printer Report** link on the global navigation bar or the Reports page in the Hardware Assets section. The Printer Report page opens.
2. Printer CSV files can be created to show information in three different formats, each of which is described below. To select a format for the Printer Report, choose the appropriate option from the **Show the following printer information** list.
   - `Printer Drivers` — Create a CSV file that organizes printer driver data according the printer driver's name. The printer driver data can provide important information for help desk troubleshooting. Printer Driver CSV files include the following columns:
     - **Server Name** — the server hosting the printer
     - **Share Name** — the printer's network name
     - **Printer Driver** — the printer driver's name
     - **Printer Name** — the printer's name
     - **Port** — the port the printer operates under
     - **Attribute** — indicates whether the printer is installed locally or is a network share
   - `Printer Ports` — Create a CSV file that organizes printer driver data according to their port. Printer Port CSV files include the following columns:
     - **Port** — the port under which the printer operates
     - **Server Name** — the server hosting the printer
     - **Share Name** — the printer's network name
     - **Printer Driver** — the printer driver's name
     - **Printer Name** — the printer's name
     - **Attribute** — indicates whether the printer is installed locally or is a network share
   - `Devices by Printer` — Create a CSV file that lists all devices with installed printer drivers. When **Show the following printer information** is set to this value, the Printer download window refreshes to include the **Group** filter. Select a group from the **Group** list to limit values in the Devices by Printer report by device group. Devices by Printer CSV files include the following columns:
     - **Server Name** — the server hosting the printer

- **Share Name** — the printer's network name
- **Printer Driver** — the printer driver's name
- **Printer Name** — the printer's name
- **Attribute** — indicates whether the printer is installed locally or is a network share
- **Identifier** — the unique identifying number associated with the device
- **Device Name** — the device's network name as captured by the Agent
- **Username** — the device's username as captured by the Agent
- **Department** — the department the device belongs to

When you have configured the report's options, download the report as follows:

1. Click **Download Results**. The Request Report: Printer Report page opens.
2. Read the on-screen information and define a name for the report.
3. If you want to receive e-mail notification when the download is available, enter your e-mail address in the **E-mail Address** field.
4. Click **Continue** to queue the download.
5. When your request is processed, you can retrieve the CSV or XML file of the report from the **My Reports** page. See "Downloading Reports" on page 95 for more information.

Monitor Report

The Monitor Report does not show data on-screen. Instead, the monitor report enables users to download a CSV or XML file that identifies installed monitor drivers.

To generate the Monitor Report download:

1. Click the **Monitor Report** link in the menu bar or from the Hardware Assets page.
2. Configure any appropriate filters, and then click **Download Results**. The Request Report: Monitor Report page opens.
3. Read the on-screen information and define a name for the report.
4. If you want to receive e-mail notification when the download is available, enter your e-mail address in the space provided.
5. Click **Continue** to queue the download.
6. When your request is processed, you can retrieve the CSV or XML file of the report from the **My Reports** page. See "Downloading Reports" on page 95 for more information.

The monitor report CSV file includes the following data:

- **Identifier** — the Identifier of the device
- **Device Name** — the device’s Device Name as captured by the Agent
- **Username** — the device’s username as captured by the Agent
- **Device Serial #** — the device’s serial number as captured by the Agent
- **Asset Number** — the device’s asset number, if one was recorded
- **Department** — the department to which the device belongs
- **Make** — the device’s make
- **Model** — the device’s model number
- **Monitor Manufacturer** — the manufacturer of the device’s monitor
- **Monitor Type** — the monitor type
- **Monitor Refresh Rate** — the monitor’s refresh rate
- **Video Device** — the name of the device’s video card
- **Video Resolution** — the monitor’s screen resolution in pixels
- **Video Color Depth** — the monitor’s color depth in bits

NOTE If a monitored device uses a generic device driver for its monitor or video card, some values in the Monitor Driver report may be recorded and shown as **Standard Monitor Type**, **Plug and Play Monitor**, **Generic Monitor**, or **Standard Monitor**.

Hardware Configuration Change Report

The Hardware Configuration Change report identifies all assets that have had modifications to their critical hardware during a time period defined by the user. The report shows both previous and current hardware for each detected change.

Hard Disk Space Report

The Hard Disk Space Available report shows total, used and available hard disk space on each disk present on tracked devices. The data collected using the report allows customers to track devices that may not be able to accept software upgrades or that are running out of free hard disk space.

Device Readiness Report

The Device Readiness report identifies assets that do not meet user- specified minimum requirements for hardware or the operating system. The Device Readiness report allows users to:

- Locate devices that cannot support a particular software or operating system rollout
- Reveal assets that are ready to be retired
- Identify hardware components requiring upgrade

The default report is generated using the minimum specifications for Windows XP Professional according to Microsoft:

- CPU speed is greater than 300 MHz
- RAM is greater than 128 MB
- Hard Drive (HD) size is greater than 2 GB
- Hard Drive free space is greater than 1.5 GB

The Device Readiness report shows all devices failing to meet any or all of the defined requirements, grouped according to criteria that devices failed to meet.

Mobile Broadband Adapter Report

IMPORTANT Before using Real Time Technology (RTT) features including Mobile Broadband Adapter asset tracking, Monitoring Center Initiated Calling, and Intel AT SMS Lock Requests, you need to activate these features for your account or individual Identifiers within your account. Contact Absolute Software Technical Support to activate these features. See “Technical Support” on page 15 for more information on contacting support.

The Mobile Broadband Adapter report shows a list of mobile broadband adapters, also known as cellular modems, installed and operational on managed devices.

Information showing in the Mobile Broadband Adapter report is also available on the Device Summary page for a specific device. See “Viewing and Editing the Device Summary for a Single Identifier” on page 61 for more information.

Smart Phone Report

The Smart Phone Report shows a list of smart phone assets in an account. A smartphone is a mobile phone offering advanced capabilities, often with computer-like functionality, and offers a good computer-mobile handset convergence.

Smart Phones that support more than one network technology, such as CDMA and GSM, are shown multiple times in the report. In such cases, the Phone Number, Equipment Id, and Subscriber Id columns hold different values for each network technology detected.

Software Asset Reports

Installed Software Overview Report

The Installed Software Overview report shows detected software applications on tracked devices. Use the report for software inventory and license management as well as identifying essential or non-essential software applications.

The Installed Software Overview report shows one record for each executable discovered on a device and is independent of software licenses. A licensed application may have multiple records listed in the Installed Software Overview report. For example, Microsoft Office would shows separate records for Word, Access, Excel, and any other Office applications.

By default, the Installed Software Overview report shows all software titles detected on monitored devices, organized by publisher name. The report shows all devices that meet any or all of the defined requirements.

IMPORTANT There is no information available to identify the **Publisher** of an application on Windows Mobile devices. Therefore, if your assets include Windows Mobile devices, all software applications on those devices are grouped together as **Publisher: (None)** and shown at the top of the Installed Software Overview report.

Use the "Software License Compliance Overview Report" on page 105 to monitor and review software licensing details.

Software Configuration Change Report

The Software Configuration Change report identifies all devices that have software installed, uninstalled or upgraded in a specified time period. For upgrades, the report shows both previous and new version numbers.

NOTE The default configuration of the Software Configuration Change report may not return results. It may be necessary to increase the date range or modify other filters and regenerate the report.

Software by Device Report

The Software by Device report shows a list of all detected software installed on each tracked device.

A Note on Software Listings in Customer Center

The ability of the Agent to automatically identify installed applications is hindered by the fact that software developers do not adhere to published standards for identifying their products. Generally, application developers embed identifying information into the actual code of their products. Unfortunately, the information is not embedded the same way from one company to another, or in some cases from one product to another from the same company. To address the issue caused by differences in embedded information, Absolute Software maintains a database that distinguishes applications by how their identifying information is recorded within the application. As the database develops, the ability of the Agent to identify specific applications increases.

Requesting New Software Mappings

Absolute Software invites end-users to request specific applications they would like added to the database. To request that a specific application be mapped, and therefore included in the Software License Overview report, send an e-mail message to techsupport@absolute.com with the subject `Request Software to Map`.

Include the following information in the e-mail request:

- Application Name
- Program Version
- Publisher Name
- Publisher Home Page
- **Identifier**, **Device Name** and **User Name** or **Assigned E-mail Address** of at least one device on which the application is installed, including the date and time it was installed

IMPORTANT Absolute Software does not guarantee implementing all software mapping requests.

Software License Compliance Overview Report

The Software License Compliance Overview report shows the number of licensed and unlicensed software applications on devices.

When the Software License Compliance Overview Report is generated using the Show Version-Specific Licenses option, values in the following fields show as hyperlinks:

- **License Name**—Clicking a license name opens the Edit License page. See "Editing License Values" on page 105 for more information.
- **Installed In This Group**—Click a value to open the Devices by License report. See "Devices by License Report" on page 106 for more information.

Editing License Values

The Edit License page shows the following information for the selected license:

- **Publisher Name**
- **License Name**

- **Licenses Purchased**
- **Number of Program Installations**
- **Installations on non-Agent Devices**
- **Licenses Available**

The Edit License page also shows the Customer Center User Name of the last user to modify the license information, as well as the date and time of the change.

See "Report Data Definitions" on page 134 for more detail on information that the Edit License page shows.

To update the licensing information for a specific license:

1. In the Software License Compliance Overview report, click the name of the license you want to update in the **License Name** column. The Edit License page opens.

   IMPORTANT License names are presented as links only when the Software License Compliance Overview report is generated using the **Show Version-Specific Licenses** option.

2. If necessary, edit the number of licenses purchased by your organization in the **Licenses Purchased** field.
3. If necessary, edit the number of devices on which the software license is installed in the **Licenses installed on non-Agent equipped devices** field.
4. Do one of the following:
   - To save your changes and refresh the Edit License page with the new values, click **Save**.
   - To save your changes and return to the Software License Compliance Overview report, click **Save & Close**.

Devices by License Report

The Devices by License Report lists all devices on which a specific application is installed. This report can only be accessed through the Software License Compliance Overview report.

To view the Devices by License Report:

1. In the Software License Compliance Overview report output, click a value in the **Installed In This Group** column. The Devices by License report opens for the selected license.
2. Set filter criteria as needed.
3. Click **Show Results**.

Microsoft Audit Summary Report

The Microsoft Audit Summary Report is a downloaded CSV or XML file that lists all of Microsoft licenses shown in the Software License Overview Report. Use the Microsoft Audit Summary file to track your organization's compliance with Microsoft's licensing requirements. This file adheres to the layout and content of one of the Microsoft Audit Summary templates published by Microsoft.

To generate the report:

1. Click the **Microsoft Audit Summary Report** link on the global navigation bar or the Software Assets page. The Request Report: Microsoft Audit Summary page opens.
2. Enter a name for the report in the **Name** field.
3. Select a report format (CSV or XML) in the **Format** list.
4. If you want to receive an e-mail notification when the report is available, enter your e-mail address in the **Your E-mail address** field.
5. When your request is processed, you can retrieve the CSV or XML file of the report from the **My Reports** page. See “Downloading Reports” on page 95 for more information.

The Microsoft Audit Summary Report includes, for each license listed, the following fields:

- **Name** — the license name
- **# of Installs** — the sum of detected instances of the application, and the manually entered value for Installed on non-Agent equipped devices
- **# of Licenses** — the number of licenses purchased
- **# Available** — the number of available licenses for the application (negative numbers indicate non-compliance)

Software Policy Non-compliance Report

The Software Policy Non-compliance Report lists all devices that have software installed that violates defined software policy, whether the violation is the presence of a banned software title or the lack of a required title. You can also configure the report to show all devices that have software that, although not banned, is not on an approved list.

IMPORTANT In order to use the Software Policy Non-compliance report, you must first define and apply a software policy. See “Software Policy” on page 72.

Installed Programs by Device Report

The Installed Programs by Device report shows a list of all properly installed software installed on each tracked device.

Clicking values in the Name column of the report output opens the Program Details dialog box to show more details about a program installed on a particular device.

Program Details Dialog Box

The Program Details dialog box shows detailed information about a particular installed program.

To view the Program Details dialog box:

1. In the Installed Programs by Device report output, click the value in the **Name** column for the appropriate program.
2. Click **OK** to return to the Installed Programs by Device report output.

The Program Details dialog box lists the following information for the selected program:

- **Program Name**
- **Publisher Name**
- **Help Link**
- **Support Telephone**
- **Installation Directory**
- **Install Source**
- **Comments**
- **Contact**
- **Readme**

See “Report Data Definitions” on page 134 for more detail on information that the Program Details dialog box shows.

Installed Programs by Account Report

The Installed Programs by Account report shows a list of all properly installed software installed on one or more tracked devices associated with an account.

Clicking values in the Name column of the report output opens the Program Details dialog box to show more details about a program installed on a particular device. See “Program Details Dialog Box” on page 108.

Clicking values in the Quantity column of report output opens the Installed Programs By Device Report – Details page to show data in the same format as the Installed Programs by Device report for a specific program only.

IMPORTANT The Installed Programs by Device Report – Details page shows data according to filter criteria specified for the Installed Programs by Account report.

Security Reports

Operating System Updates Report

The Operating System Updates report shows installed operating systems, service packs and hotfix details for each tracked device.

You can filter the report to show devices that have a specific hotfix or devices that do not have a specific hotfix.

Internet Browsing Configuration Report

The Internet Browsing Configuration report shows the browser type and version, as well as the monitor show settings for all monitored devices.

Unauthorized Software Report

The Unauthorized Software report allows users to simultaneously search all their assets for installed applications.

Anti-malware Report

The Anti-malware Report identifies devices that have anti-malware software installed. You can use the report to identify devices that use an older version of anti-malware software or have outdated virus definition files.

NOTE See Anti-malware Vendors Detected for a list of anti-malware programs and vendors that the Agent detects and shows in Customer Center.

Missing Anti-malware Report

The Missing Anti-malware Report identifies all tracked devices that do not have an anti-malware product installed.

NOTE The Agent only detects the anti-malware programs and vendors listed in Anti-malware Vendors Detected. If the target device contains an anti-malware program that does not show in the list, the Agent may not detect the presence or absence of the program accurately.

Anti-malware Vendors Detected

The Agent detects and reports anti-malware applications and vendors based on a two tiered approach:

- **Tier 1 applications** are installed, tested, and proactively patched by Absolute Software, and include:
  - Symantec Norton Antivirus (SMB)
  - Symantec Antivirus (Enterprise)

    - McAfee VirusScan (SMB)
    - McAfee VirusScan for Enterprise
    - Sophos Anti-Virus

- **Tier 2 applications** are reactively reviewed by customers and patched by Absolute Software, and include:
    - AVG Antivirus (Grisoft)
    - Bitdefender Antivirus
    - Computer Associates Anti-Virus
    - F-Prot Antivirus
    - F-Secure Internet Security
    - Kaspersky Anti-Virus
    - Microsoft Windows Live OneCare
    - Panda Antivirus Pro
    - Trend Micro Internet Security

Modem Addition Report

The Modem Addition report identifies all devices that have a modem installed or reconfigured in a given date range.

Suspicious Devices Report

The Suspicious Devices report identifies all devices that have triggered one or more alert notifications defined as representing suspicious activity. You can use the Alerts area on Customer Center to specify events that trigger suspicious alert notifications. See "Alerts" on page 35 for more information about creating and managing alerts in Customer Center.

Scenarios

For example, if a group of devices is not meant to be removed from the network at your organization, you can use the Public IP Address Changed alert to log any occurrences when a device in the group is assigned a different IP address to access the Internet.

As another example, you can use the Major Change alert to notify Administrators immediately when a device is detected as that have the Device Name, Username and Operating System Product key changed simultaneously, with the Agent subsequently making a self-healing call.

Call History and Loss Control Reports

Use Call History and Loss Control reports to ensure that your devices call the Monitoring Center regularly from expected locations and report expected users. If a device calls the Monitoring Center regularly, the chance of recovery is much higher when a device is missing. To be eligible for the Service Guarantee payment after a device is missing, the device must make at least one post-theft call.

Call History Report

The Call History report shows all communications made by a specific Identifier, or group of Identifiers, to the Monitoring Center.

IMPORTANT Call data is stored online for one year, after which time data is archived. If a Call History report is configured to show data from over a year ago, the data must be retrieved from the archive server and the report takes longer to generate results.

Extended IP Call Information

Call History, Missing Devices and Device Drift History reports may contain caller identification information. The caller identification information usually shows as a link. Clicking the link opens the Extended IP Call Information page, providing details about the location or origin of an IP address or telephone number. The information is useful for locating devices that are outside a corporate network.

The Extended IP Call Information page lists the following information:

- **Identifier**
- **Server Time** (Unused)
- **Local IP Address**
- **Proxy IP Address**
- **Host Name**
- **MAC Address**
- **Local IP RDNS**
- **Proxy IP RDNS**
- **ARIN Who IS Info**

For more details on information provided in the Extended IP Call Information dialog box, see “Report Data Definitions” on page 134.

Missing Devices Report

The Missing Devices report allows you to identify devices that have not contacted the Monitoring Center for a given period of time.

Periodically review the Identifiers assigned to devices in your organization. Check for any devices that have not contacted the Monitoring Center for an unusually long period of time (e.g.—45 days). Lack of contact from a device may indicate that the Agent is missing, or that an event has occurred preventing the Agent from contacting the Monitoring Center.

IMPORTANT Dormant devices are excluded from the report.

NOTE You may need to adjust the Most Recent Call filter value so that report output contains results.

See also "Extended IP Call Information" on page 111.

Device Drift by Device Name Report

The Device Drift by Device Name report identifies devices that have had a change in their Device Name within a specified date range and provides links to more detailed information on specific devices. You can specify filter criteria pertaining to current or previous Device Names.

NOTE The default configuration of the Device Drift by Device Name report may not show any results. You may need to define a date range for the report to return any information.

Device Drift by User Name Report

The Device Drift by User Name report identifies devices that have had a change in the User Name within a specified date range. You can specify filter criteria pertaining to current or previous User Names.

NOTE The default configuration of this report may not show any results. It may be necessary to define a date range for the report to return any information.

Device Drift History Report

The Device Drift History report is a sub-report available from the **Device Drift by Device Name** and **Device Drift by Username** reports. The Device Drift History report shows all changes to the User Name, Device Name, and Assigned E-mail Address for a specific Identifier.

NOTE The Device Drift History report is **not** available from the Call History and Loss Control group of reports.

To view the Device Drift History report:

➢ In report output for the Device Drift by Device Name or Device Drift by Username reports, click the **Machine History** link.

To view more detailed caller ID information:

➢ Click a telephone number or IP address in the **Caller ID** column. See "Extended IP Call Information" on page 111 for more details.

Activation Report

The Activation report identifies, in real time, all devices that have completed a first call to the Monitoring Center within a given period of time.

NOTE The default configuration of the Activation report may not show any results. You may need to define the date range for the report output to contain any information.

Device Location Report

IMPORTANT Only Administrators and Power Users are able to view Device Location and Device Location History reports. Guest users do not have sufficient access privileges to access Geolocation Tracking data. The first time you access any geolocation page in a login session, a confirmation page prompts you to accept the Terms and Conditions of use.

The Device Location report shows the most recent geographic locations—geolocations—of devices based on the best geotechnology available on a device when reporting a location. In order of accuracy and reliability, location information is collected using one of the following technologies:

1. **Global Positioning System (GPS)** technology monitors devices using built-in sensors that capture satellite signals indicating the exact location of a device.
2. **API and other location sampling technologies** such as Microsoft Windows 7 Location Sensor use a variety of methods to identify device locations.
3. **Wi-fi triangulation** determines the location of monitored devices indirectly by cross-referencing the list of Wi-fi networks that a device detects with a database of known Wi-fi networks and their locations. Wi-fi triangulation is most effective in North America and Europe.
4. **IP Georesolution** uses a database of known locations of assigned IP addresses to determine the location of monitored devices. Accuracy varies from the city to the country level. The highest degree of accuracy is achieved in North America and Europe.

Except for IP Georesolution, location data is collected hourly and uploaded to Customer Center each time a device calls the Monitoring Center (usually once a day). For IP Georesolution, locations are collected every time the device calls the Monitoring Center.

NOTE Location data is collected for devices equipped with the Geolocation Tracking feature only. See "Geolocation System Requirements" on page 115 for a list of the hardware and software required for Customer Center to collect geolocation information from a device.

In report output, devices equipped with Geolocation Tracking show as icons on Microsoft® Bing™ Maps. The map automatically resizes for optimal display considering all devices found and includes existing Geofence boundaries for your account.

Each type of location technology is depicted using a specific icon on the map:

- 📡 — GPS location technology
- 🖥 — Computers using API or other location technologies
- 📱 — Mobile devices using API or other location technologies
- 📶 — Wi-fi triangulation technology
- 🖧 — IP georesolution technology

A small number in the top right corner of an icon indicates the number of devices in the area on the map under the icon. If all devices in the map area under the icon use the same type of location technology, the icon shows the location technology. Otherwise, the icon does not show any location technology.

Clicking an icon opens a dialog box containing a **Zoom In** link to view the icon location closely as well as the following details about devices that the icon represents:

- **Identifier** — the unique identifying number associated with the device
- **Device Name** — the network name of the device as captured by the Agent
- **Username** — the username associated with the device as captured by the Agent
- **Make** — the name of the device manufacturer as captured by the Agent
- **Model** — the model number of the device as captured by the Agent
- **Location** — a link allowing you to zoom in to the last known location of the device
- **Location Time** — the date and time of the last known location of the device. Clicking the **History** link opens the Device Location History Report for the device.
- **Location Technology** — the technology used to determine the location of the device

The report output below the map lists full details for each device included in report output.

See "Managing Geofences" on page 195 for more details about using Customer Center geotechnology.

Geolocation System Requirements

You must install a supported version of the Computrace Agent on devices that you want Customer Center to track. The Customer Center Geolocation Tracking feature supports the following platforms, hardware and software on devices:

- PC
    - Operating Systems
        - Windows XP (32-bit editions only)
        - Windows Vista (any 32- or 64-bit edition)
        - Windows 7 (any 32- or 64-bit edition)

        NOTE Windows 2000 and Windows XP 64-bit edition are **not** supported.

    - Computrace Agent series 8 (version 8*xx*)
    - GPS receiver

        IMPORTANT Customer Center supports most GPS receivers available for PCs. The following list is **not** exhaustive. Customer Center does **not** collect location data from a tether—using Bluetooth wireless, USB or serial connection for example—to a device that have a GPS receiver.

        - Qualcomm UNDP-1 (Gobi 1000) mobile broadband adapter
        - Qualcomm 9202 mobile broadband adapter
        - Ericsson F3507g & F3607gw mobile broadband adapters
        - HP un2400 & un2420 mobile broadband adapters
        - Dell 5600 mobile broadband adapter
    - Windows 7 Location Sensor API
    - Wi-fi network adapter
- Mac
    - Mac OS X 10.3.9 or later
    - Computrace Agent version 870 or later

- Wi-fi network adapter

NOTE CoreLocation is **not** supported at this time.

- Mobile devices (such as cell phones)
  - GPS receiver
  - Windows Mobile Agent version 2003 or later
  - Wi-fi network adapter

Enabling Geolocation Reporting

By default, the Device Location and the Device Location History reports are not enabled for your Customer Center account. You must submit a Geolocation Authorization Form before the reports are enabled.

To enable Geolocation reporting in Customer Center:

1. Click the **Documentation** link on the global navigation bar.
2. In the Service Request Forms area, click the **Security Administrator and Geolocation Tracking Authorization Form**.
3. Complete and return the form to the Absolute Global Support fax number listed on the form.

Global Support will notify you when the Geolocation Reporting feature is enabled for your account.

Limitations of Global Positioning Systems (GPS)

1. GPS receivers are designed to receive a signal from satellites reliably when outside with an unobstructed view of the sky. Therefore, GPS receivers are unlikely to work well when surrounded by high rise buildings or inside metal-framed or concrete buildings. GPS receivers may work inside non-metal framed buildings or near a window.
2. The accuracy of the location reported by a GPS depends on environmental issues such as how many satellites are in view, potential reflection of satellite signals from nearby objects, or atmospheric effects. In ideal conditions, the GPS available typically reports locations within 10m of actual location. When conditions are less favorable, error may increase to 100m or more. GPS coordinates are unlikely to be exact.

Limitations of Wi-fi Triangulation

Wi-fi triangulation is a correlational tracking method based on the known GPS location of Wi-fi networks detected near a device.

Typically, Wi-fi triangulation provides a location accurate to within a few city blocks.

Device Location History Report

IMPORTANT Only Administrators and Power Users are able to view Device Location and Device Location History reports. Guest users do not have sufficient access privileges to access Geolocation Tracking data. The first time you access any geolocation page in a login session, a confirmation page prompts you to accept the Terms and Conditions of use.

The Device Location History report tracks the location of a single device over time, using the best location technology available when the device reported a location. For a list of available location technologies in order of accuracy and reliability, see "Device Location Report" on page 113.

Report output represents the position of a device over time as a set of icons on a Microsoft® Bing™ Map. For the meaning of icons, see "Device Location Report" on page 113. In addition, in the Device Location History report the color of the screen in an icon indicates the timeline. More recent locations are red. The older a location, the more the screen color of the icon looks white.

Clicking an icon opens a dialog box showing details about the devices that the icon represents. For a description of details that are shown, see "Device Location Report" on page 113.

Report output below the map lists latitude and longitude coordinates, measured in decimal degrees.

See "Managing Geofences" on page 195 for more details about using Customer Center geotechnology.

Lease and Inventory Management Reports

Lease Completion Report

The Lease Completion report identifies all assets that have leases expiring in a given time period.

NOTE See "Data" on page 42 for detailed instructions on entering new lease information or updating information on existing leases.

By default, Lease Completion report output includes devices that have a lease expiring within the next 30 days. You can change the range of dates to include in report output.

Report results list up to fourteen data fields and their values for each Identifier included in the report. Users can define six of the fields. Here are the remaining eight fields:

- **Lease Start Date**
- **Lease End Date**

- **Lease Number**
- **Lease Vendor**
- **Service Contract Start Date**
- **Service Contract End Date**
- **Service Contract Vendor**
- **Lease Responsibility**

NOTE The Lease Completion report does not list fields with null values.

The remaining data fields included in the Lease Completion report are the same user-defined fields that the Asset report shows. Create user-defined fields using the Data tool in the Customer Center Administration area. See "Data" on page 42.

NOTE Not all equipment lessors provide maintenance and service support. For this reason, the lease vendor and service vendor may not be the same and the contract dates may differ.

User-entered Data

The User-entered Data report allows you to view all manually-entered data associated with your tracked devices, including all data stored in user-defined fields (UDFs) and data points that the Agent is unable to capture automatically.

NOTE See "Exporting and Importing Data" on page 43 for a complete discussion of UDFs.

To select data points to show in report output:

1. Click **Choose Columns** to open the Custom Fields dialog box.
2. Select the appropriate field in the **Available Fields** pane, and then click **>** to add the field to the **Selected Fields** pane. To add all fields, click **>>**.

   NOTE To remove a field from report output, select the field in the **Selected Fields** pane, and then click **<**. To remove all fields, click **<<**.

3. Repeat step 2 as needed to prepare the report output format.
4. Click **Close** to return to the User-entered Data report page.

Account Management Reports

Use Account Management reports to monitor and track Agent licenses belonging to your organization, and to help resolve licensing issues.

License Usage Summary Report

The License Usage Summary report provides details regarding the current licensing status of your account including the installation rate.

To download the License Usage Summary report:

1. Click the **License Usage Summary** link on the global navigation bar or the Reports page in the Account Management area. The License Usage Summary report page opens.
2. Enter a name for your report in the **Name** field.
3. Select a format (CSV or XML) for your report in the **Format** list.
4. If you want to receive an automated alert when the report is available, enter a valid e-mail address in the **Your E-mail Address** field.
5. Click **Continue** and follow the on-screen instructions to generate the report. The report download is processed offline and, when completed, is available for download from the **My Reports** page.

The License Usage Summary download includes the following data:

- **AbsoluteTrack** — total number of AbsoluteTrack licenses purchased
- **ComputraceComplete** — total number of Computrace® Complete licenses purchased
- **Total Licenses** — combined total of AbsoluteTrack and Computrace® Complete licenses purchased
- **Total Installed** — combined total of all AbsoluteTrack and Computrace® Complete licenses installed under your account
- **Over(-) or Under Install (+)** — total number of licenses purchased, minus the total number installed
- **Install Rate** — percentage of purchased licenses that are installed
- **Called In Last 30 Days** — combined total of licenses that have called the Monitoring center in the last 30 days
- **Recent Call In Rate** — the above value as a percentage
- **Service Guarantee Installed** — total number of Service Guarantee licenses installed
- **Over(-) or Under Install(+)** — total number of Service Guarantee licenses purchased, minus the total number of Service Guarantee licenses installed
- **Install Rate** — percentage of purchased Service Guarantee licenses that are installed
- **Called In Last 30 Days** — total number of Service Guarantee licenses that have called the Monitoring center in the last 30 days
- **Recent Call In Rate** — the above value as a percentage

Calling Profiles Report

The Calling Profiles report provides detailed information on the calling patterns of each device.

To download the Calling Profiles report:

1. Click the **Calling Profiles** link on the global navigation bar or the Reports page in the Account Management area. The Calling Profiles report page opens.
2. Set filter criteria for the report output as needed.
3. Enter a name for your report in the **Name** field.
4. Select a format (CSV or XML) for your report in the **Format** list.
5. If you want to receive an automated alert when the report is available, enter a valid e-mail address in the **Your E-mail Address** field.
6. Click **Continue** and follow the on-screen instructions to generate the report. The report download is processed offline and, when completed, is available for download from the **My Reports** page.

The Calling Profiles download includes the following data for each device:

- **Identifier**
- **Device Make**
- **Device Model**
- **Department**
- **Last Host Name**
- **Last Username**
- **Serial Number**
- **Asset Number**
- **Activation Date**
- **Last Caller ID**
- **Local IP**
- **Last E-mail**
- **Agent Version Number**
- **First Call**
- **Last Call**
- **Second to Last Call**
- **Third Last Call**
- **Fourth Last Call**
- **Fifth Last Call**
- **Calls 0-30 Days**

- **Calls 31-60 Days**
- **Calls 61-90 Days**
- **Calls Over 90 Days**
- **All Calls**

User Audit Report

The User Audit report enables Customer Center administrators to download a CSV (comma separated value) file that identifies all users that are added or modified. The User Audit report does not show data on-screen.

The User Audit report file includes the following fields:

- **Changed By User Name** — the Customer Center User ID of the person who made the change
- **Changed By User First/Last Name** — the name of the person who made the change
- **Type** — the nature of the change. Possible values are Insert (new user created), Edit, Delete, or Reactivate.
- **Date/Time Of Change** — the date and time when the change was made
- **Old User name** — the old username or logon ID associated with the user account
- **Old E-mail** — the old e-mail addresses associated with the user account
- **Old User Type** — the user type associated with the old user account
- **Old First/Last Name** — the first and/or last name associated with the old user account
- **Old Device Group** — the device group to which the old user account belongs
- **New User name** — the new or changed username or logon ID
- **New E-mail** — the new or changed e-mail address associated with the user account
- **New User Type** — the modified value of the user type
- **New First/Last Name** — the new or changed first and/or last name associated with the user account
- **New Device Group** — the modified value of the device group

To download a User Audit report:

1. Click the **User Audit** link on the global navigation bar or the Reports page in the Account Management area. The User Audit Report page opens.
2. Enter a name for your report in the **Name** field.
3. Select a format (CSV or XML) for your report in the **Format** list.

4. If you want to receive e-mail notification when the download is available, enter your e-mail address in the **Your E-mail Address** field.
5. Click **Continue** to queue the download.
6. After your request is processed, you can retrieve the CSV file of the report from the **My Reports** page. Click the **My Reports** tab in the navigation bar and click the **Ready** link in the status column. Follow on-screen instructions to download the CSV file.

NOTE When your file request is being processed, the status column shows `Pending` and the report is not available. When processed, the status column shows the **Ready** link and, if configured to do so, Customer Center sends an e-mail notification.

User Event Report

The User Event report enables Customer Center administrators to view a log of user events classified by Customer Center User Name and/or time of occurrence.

My Content

My Reports

All Customer Center reports can be downloaded as a CSV or XML file. Report download requests are queued and processed offline. When the processing is complete, the CSV or XML files are made available through the My Reports page.

To view the My Reports page and download a processed report:

1. Click the **Reports** link on the global navigation bar. The Reports page opens.
2. On the Reports page, click the **My Reports** link in the **My Content** area. You can also click the **My Content** link on the global navigation bar, and then click the **My Reports** link. The My Reports page opens.

   The My Reports page lists all requested report downloads and includes the following information for each report:

   - **Report Requested On** — lists the date and time when the CSV file was requested
   - **Name of Report** — lists the name assigned to the CSV request
   - **Status** — indicates the status of the request. Possible values are `Pending`, `Ready`, and `Error`.

3. To download a processed request, in the row containing the appropriate report, click the **Ready** link in the status column and follow the on-screen instructions.

NOTE When your file request is being processed, the status column shows `Pending` and the report is not available. When processed, the status column shows the **Ready** link and, if requested, Customer Center sends an e-mail notification.

My Filters

The My Filters report category is a repository for all saved report filters. Saved filters define the criteria for a report, not report output. Data meeting criteria may change with time, so report output can change as well.

To use a saved report filter:

1. Click the **Reports** link in the global navigation bar.
2. On the Reports page, click the **My Filters** link in the **My Content** area.

OR

3. Click the **My Content** link in the global navigation bar, and then click the **My Filters** link.
4. Click the appropriate filter name in the table.
5. The report is regenerated based on the saved filter criteria.

Modifying Saved Report Filters

To modify a saved report:

1. Open the My Filters page.
2. Click the appropriate filter name in the table.
3. Modify the existing filters and click **Show Results**. The report regenerates and shows on the page.
4. If necessary, save the modified filters as a new saved filter. See "Saving Report Filters" on page 94 for information on how to save a report filter.

   NOTE The original saved report remains unchanged.

Report Filter Criteria

Table 2 on page 124 indicates the data you can filter to prepare applicable Customer Center reports. For a description of data you can filter, see "Report Data Definitions" on page 134.

Table 2. Report Filter Criteria

Report	Criteria																																										
	Common																					Specific to Category																					
	Group	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Department	Date Range	Operating System	Publisher Name	Application Name	Program Name	Program Version	Warranty Contract Vendor	Change Type	IP Address	Monitor Type	Monitor Manufacturer	Monitor Refresh Frequency	Video Device Name	Video Display Resolution	Video Display Color Depth	Hard Drive Free Space	Hard Drive Size	CPU Name	CPU Speed	RAM Size	Adapter Manufacturer	Adapter Model	Adapter Equipment ID	Adapter Subscriber ID	Adapter Network	Detected Phone Number	Phone Number Override	Phone Number	Equipment ID	Subscriber ID	MAC Address
Hardware Assets																																											
Asset	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						✓																								
Monitor	✓	✓	✓	✓	✓	✓	✓					✓										✓	✓	✓	✓	✓	✓																
Hardware Configuration Change	✓	✓		✓	✓	✓	✓				✓	✓	✓							✓																							
Hard Disk Space	✓	✓		✓	✓	✓	✓				✓	✓																✓	✓														
Device Readiness	✓											✓		✓														✓	✓	✓	✓	✓											
Mobile Broadband Adapter	✓	✓										✓																					✓	✓	✓	✓	✓	✓	✓				

Table 2. Report Filter Criteria

Report	Criteria																																										
	Common																					Specific to Category																					
	Group	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Department	Date Range	Operating System	Publisher Name	Application Name	Program Name	Program Version	Warranty Contract Vendor	Change Type	IP Address																						
Software Assets																						License Version Dependence	License Name	License Status	Policy Name	Compliance	Unlicensed Software																
Installed Software Overview	✓											✓			✓	✓	✓																										
Software Configuration Change	✓											✓	✓		✓	✓				✓																							
Software By Device	✓	✓	✓							✓		✓			✓	✓	✓	✓																									
Software License Compliance Overview	✓														✓							✓	✓	✓																			
Devices by License	✓	✓	✓							✓		✓																															
Software Policy Non-compliance	✓	✓	✓									✓	✓			✓							✓		✓	✓	✓																
Installed Programs By Device	✓	✓	✓							✓		✓			✓		✓	✓																									

Table 2. Report Filter Criteria

Report	Criteria																																										
	Common																					Specific to Category																					
	Group	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Department	Date Range	Operating System	Publisher Name	Application Name	Program Name	Program Version	Warranty Contract Vendor	Change Type	IP Address																						
Installed Programs By Account	✓	✓	✓							✓		✓																															
Security																						Latest Service Pack	Hotfix Name	Browser Name	Browser Version Number	Anti-malware Software Vendor	Anti-malware Software Version	Virus Definition Date	Suspicion Level														
Operating System Updates	✓											✓		✓								✓	✓																				
Internet Browsing Configuration	✓	✓	✓							✓		✓												✓	✓																		
Unauthorized Software	✓											✓			✓	✓	✓	✓																									
Anti-malware	✓	✓	✓							✓		✓														✓	✓	✓															
Missing Anti-malware	✓											✓																															
Modem Addition	✓	✓	✓							✓		✓	✓																														
Suspicious Devices	✓	✓	✓				✓			✓		✓		✓															✓														

Table 2. Report Filter Criteria

Report	Criteria																										
	Common																					Specific to Category					
	Group	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Department	Date Range	Operating System	Publisher Name	Application Name	Program Name	Program Version	Warranty Contract Vendor	Change Type	IP Address						
Call History and Loss Control																						Number of Calls	Recent Activations	Persistence Status	Device	Location Type	Location Obtained Via
Call History	✓	✓	✓			✓				✓	✓	✓	✓								✓						
Missing Devices	✓											✓	✓														
Device Drift by Device Name	✓		✓									✓	✓														
Device Drift by Username	✓									✓		✓	✓														
Device Drift History																						✓					
Activation	✓	✓		✓	✓	✓	✓	✓			✓	✓	✓										✓	✓			
Device Location	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						✓								✓
Device Location History													✓												✓	✓	✓

Table 2. Report Filter Criteria

Report	Criteria																																										
	Common																				Specific to Category																						
	Group	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Department	Date Range	Operating System	Publisher Name	Application Name	Program Name	Program Version	Warranty Contract Vendor	Change Type	IP Address																						
Lease and Inventory Management																						Assigned E-mail Address	Cost Center/Code	Lease Number	Lease Responsibility	Lease Vendor	Location	Purchase Order Reference	Service Contract Vendor	User Phone/Extension													
Lease Completion	✓		✓			✓	✓			✓	✓	✓	✓						✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓													
User-entered Data	✓	✓	✓							✓		✓																															
Account Management																						Event Details																					
Calling Profiles	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓																															
User Event										✓			✓									✓																					

Displayed Report Output

Table 3 on page 129 lists the data showing in the display output for each Customer Center report. For a description of data that Customer Center shows in report output, see "Report Data Definitions" on page 134.

Table 3. Displayed Report Output

Report	Data																																															
	Common																						Specific to Category																									
	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Assigned E-mail Address	Department	Location	Last Call Date	Operating System	Publisher Name	Application Name	Program Name	Program Version	Date Change Detected	Change Status	User-defined																										
Hardware Assets																							Date Stolen	Hardware Description	Previous Value	New Value	Drive Letter	Hard Drive Space Threshold	Hard Drive Size	Hard Drive Free Space	Hard Drive Used Space	Hard Drive Total Size	Hard Drive Total Free Space	Hard Drive Total Used Space	CPU Name	CPU Speed	RAM Size	Adapter Last Detected Date	Adapter Manufacturer	Adapter Model	Equipment ID	Subscriber ID	Network	Last Detected Service Status	Detected Phone Number	Phone Number Override	e-mail Address	MAC Address
Asset	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓								✓	✓																									
Hardware Configuration Change	✓	✓							✓											✓	✓			✓	✓	✓																						
Hard Disk Space	✓	✓							✓		✓																✓	✓	✓	✓	✓	✓	✓	✓														
Device Readiness	✓	✓							✓						✓																	✓	✓		✓	✓	✓											
Mobile Broadband Adapter	✓	✓	✓	✓					✓																													✓	✓	✓	✓	✓	✓	✓	✓	✓		
Smart Phone	✓		✓	✓					✓					✓	✓																										✓	✓			✓		✓	✓

Table 3. Displayed Report Output

Report	Data																																		
	Common																						Specific to Category												
	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Assigned E-mail Address	Department	Location	Last Call Date	Operating System	Publisher Name	Application Name	Program Name	Program Version	Date Change Detected	Change Status	User-defined													
Software Assets																							Number of Program Installations	Previous Program Version	New Program Version	License Name	Licenses Purchased	Licenses Available	Installations on non-Agent Devices	Installations in Selected Group	Installations in Other Groups	Product ID	Software Policy ID	Policy Name	Software Status
Installed Software Overview	✓	✓			✓	✓						✓			✓	✓	✓	✓	✓				✓												
Software Configuration Change	✓								✓							✓	✓	✓		✓	✓			✓	✓										
Software By Device	✓	✓			✓	✓			✓			✓				✓	✓	✓	✓																
Software License Compliance Overview																✓										✓	✓	✓	✓	✓	✓				
Devices by License	✓	✓			✓	✓			✓						✓																	✓			
Software Policy Non-compliance	✓	✓							✓					✓		✓										✓							✓	✓	✓
Installed Programs By Device	✓	✓			✓	✓			✓			✓				✓		✓	✓																
Installed Programs By Account																✓		✓	✓				✓												

Table 3. Displayed Report Output

Report	Data																																															
	Common																						Specific to Category																									
	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Assigned E-mail Address	Department	Location	Last Call Date	Operating System	Publisher Name	Application Name	Program Name	Program Version	Date Change Detected	Change Status	User-defined																										
Security																							Latest Service Pack	Hotfix Name	Video Display Resolution	Video Display Color Depth	Browser Name	Browser Version Number	First Call Date	Anti-malware Software Vendor	Anti-malware Software Version	Virus Definition File Name	Virus Definition Date	Virus Definition Detection Date	Current Modem Model	Current Port	Previous Modem Model	Previous Port	Suspicion Level	Suspicious Event								
Operating System Updates	✓	✓							✓						✓								✓	✓																								
Internet Browsing Configuration	✓	✓							✓																✓	✓	✓	✓																				
Unauthorized Software	✓	✓							✓							✓	✓	✓	✓										✓																			
Anti-malware	✓	✓							✓			✓		✓																✓	✓	✓	✓	✓														
Missing Anti-malware	✓	✓	✓	✓	✓	✓			✓	✓		✓		✓																																		
Modem Addition	✓	✓							✓											✓															✓	✓	✓	✓										
Suspicious Devices	✓	✓	✓	✓		✓			✓																														✓	✓								

Table 3. Displayed Report Output

Report	Data																																															
	Common																						Specific to Category																									
	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Assigned E-mail Address	Department	Location	Last Call Date	Operating System	Publisher Name	Application Name	Program Name	Program Version	Date Change Detected	Change Status	User-defined																											
Call History and Loss Control																							Location Time	Last Location Before Call	Call Time	Local IP Address	Public IP Address	Full Windows Device Name	Caller ID	Activation Date	Persistence Status	System BIOS Version	System BIOS Date	Confidence Level	Location Technology													
Call History	✓	✓	✓	✓	✓	✓			✓				✓												✓	✓	✓																					
Missing Devices	✓	✓	✓	✓	✓	✓			✓	✓			✓												✓	✓	✓																					
Device Drift by Device Name	✓	✓			✓	✓																						✓																				
Device Drift by Username	✓				✓	✓			✓																			✓																				
Device Drift History	✓	✓							✓																✓				✓																			
Activation	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓		✓																✓	✓	✓	✓															
Device Location	✓	✓	✓	✓					✓				✓	✓									✓											✓	✓													
Device Location History	✓	✓	✓	✓					✓				✓	✓									✓	✓										✓	✓													

Table 3. Displayed Report Output

Report	Data																																															
	Common																						Specific to Category																									
	Identifier	Device Name	Make	Model	Serial Number	Asset Number	Agent Version	Agent Status	User Name	Assigned User Name	Assigned E-mail Address	Department	Location	Last Call Date	Operating System	Publisher Name	Application Name	Program Name	Program Version	Date Change Detected	Change Status	User-defined																										
Lease and Inventory Management																							Lease Start Date	Lease End Date	Lease Number	Lease Vendor	Service Contract Start Date	Service Contract End Date	Service Contract Vendor	Lease Responsibility	Purchase Date	Cost Center/Code	Has Service Guarantee	IP Address	Purchase Order Reference	Size	User Phone/Extension	Warranty Contract Vendor	Warranty Start Date	Warranty End Date								
Lease Completion	✓		✓	✓	✓	✓			✓			✓										✓	✓	✓	✓	✓	✓	✓	✓	✓																		
User-entered Data	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓									✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓								
Account Management																							Date and Time	Event Details																								
User Event Report									✓														✓	✓																								

Report Data Definitions

Table 4 provides a list of descriptions of data pertaining to report filtering and output. Data are listed alphabetically by name.

Table 4. Report Data Definitions

Data	Definition
Activation Date	When the Agent first contacted the Monitoring Center from a device
Adapter Equipment ID	The identifier unique to each broadband adapter. For EVDO adapters, the Electronic Serial Number (ESN) and/or the Mobile Equipment ID (MEID) may be reported. For UMTS networks, the International Mobile Equipment Identifier (IMEI) is reported.
Adapter Last Detected Date	When information about a network adapter was last collected
Adapter Manufacturer	The maker of a mobile broadband network adapter
Adapter Model	The product type of a mobile broadband network adapter
Adapter Network	The mobile service provider associated with a mobile broadband adapter
Adapter Subscriber ID	The unique identifier associated with a network service subscriber that is stored in the network adapter, indicated by the Subscriber Identify Module (SIM) card or equivalent
Agent Status	The operating condition of an Agent with the following possible values: • **Active**—Devices that call the Monitoring Center regularly • **Inactive**—Registered devices that have never made a call to the Monitoring Center • **Disabled**—Devices that have their Agent permanently disabled
Agent Version	The version number of the Agent that contacts the Monitoring Center
Anti-malware Software Vendor	The provider of an application that blocks and removes malware
Anti-malware Software Version	The unique name or number assigned to a particular release of anti-malware software
Application Name	The title of an executable. In practice, many publishers mutually exchange Application Name and Program Name values. See also Program Name.

Table 4. Report Data Definitions

Data	Definition
ARIN Who IS Info	Information related to the registrant or assignee of a Proxy IP Address
Asset Number	The identification number associated with a device in Customer Center
Assigned E-mail Address	The e-mail address of the individual responsible for the device
Assigned User Name	The user name assigned to a device by a system administrator
Browser Name	The name of a software application used to navigate the Internet
Browser Version Number	The unique name or number assigned to a particular release of a Web browser
Call Time	When a device contacted the Monitoring Center
Caller ID	A telephone company service describing the origin of an incoming call, including the phone number. See also Public IP Address.
Change Status	Indicates whether a detected difference involves New, Removed or Changed hardware or software
Change Type	The Change Status values to include in report output
Comments	The description showing under the Uninstall Registry Key for a program, available in the Add or Remove Programs Control Panel icon in earlier versions of Windows and Programs and Features in Windows Vista or higher
Compliance	The type of software violations to include in the output of a report: • Software on the Banned list • Software not on the Approved list • Missing software on the Required list
Confidence Level	The estimated accuracy of a Location
Contact	The contact information for a publisher available under the Uninstall Registry Key for a program, available in the Add or Remove Programs Control Panel icon in earlier versions of Windows and Programs and Features in Windows Vista or higher
Cost Center/Code	A unique identifier for a unit for which costs are accumulated or computed
CPU Name	The known identification of the microprocessor in a device
CPU Speed	The rate at which a microprocessor computes

Table 4. Report Data Definitions

Data	Definition
Current Modem Model	The product type of a modem installed in a device at the present time
Current Port	The interface to which a modem currently installed in a device is connected
Date and Time	When an action occurred
Date Change Detected	When a difference was detected
Date Range	Date limits determining inclusion in report output
Date Stolen	The date on which a device was noticed missing
Department	The unit in an organization responsible for a device
Detected Phone Number	The phone number associated with a mobile broadband adapter, as reported by the device. See also Phone Number Override.
Device	A computer, laptop, phone or other appliance that Customer Center tracks
Device Name	The name assigned to the device in the operating system. For Macs, the Device Name is recorded based on the device’s network resolution. In some cases, the recorded name may be inaccurate due to improper or delayed refreshing of DHCP information on the network.
Drive Letter	The alphabetical identifier for a physical or logical disk drive or partition
Equipment ID	The identification number unique to a smart phone. The equipment ID is typically found on a printed label on the battery. For CDMA smart phones, the Electronic Serial Number (ESN) and/or the Mobile Equipment ID (MEID) are reported. For GSM and UMTS smart phones, the International Mobile Equipment Identifier (IMEI) is reported.

Table 4. Report Data Definitions

Data	Definition
Event Details	A description of activity related to user administration in Customer Center. Possible values include: • User suspended permanently due to failed login attempts • User suspended temporarily due to failed login attempts • User suspended permanently due to inactivity • User suspended manually (permanently) • User suspended manually until specified date • Password changed successfully • Password validation failed • Password reset • Password validated successfully
First Call Date	When an unauthorized program was initially detected on a device
Full Windows Device Name	The fully qualified domain name (FQDN) of a device, including the device name, domain name and all higher-level domains
Group	The logical aggregation association of a device
Hard Drive Free Space	The amount of storage currently available on a hard disk
Hard Drive Space Threshold	The minimum amount of storage on a hard disk that needs to be unavailable in order for a device to show in report output
Hard Drive Total Free Space	The amount of storage currently available on all hard disks installed in a device
Hard Drive Size	The full capacity of a hard disk
Hard Drive Total Size	The full capacity of all hard disks installed in a device
Hard Drive Total Used Space	The amount of storage currently unavailable on all hard disks installed in a device
Hard Drive Used Space	The amount of storage currently unavailable on a hard disk
Hardware Description	The type of hardware that changed
Has Service Guarantee	Indicates whether a payment may be issued if attempts to execute a guaranteed service fails
Help Link	The home page for a software publisher or application
Host Name	See Device Name.
Hotfix Name	The known identifier of a software patch

Table 4. Report Data Definitions

Data	Definition
Identifier	The Electronic Serial Number (ESN) of a device. Clicking an identifier listed in report output opens the Device Summary page for the device. See "Viewing and Editing the Device Summary for a Single Identifier" on page 61 for more information.
Install Source	The full directory path to the folder containing the installation files for a program
Installation Directory	The full directory path to the primary folder where a program is installed
Installations in Other Groups	The number of application installations recorded in Groups not included in the output of a report
Installations in Selected Group	The number of application installations recorded in the Group selected for inclusion in report output
Installations on non-Agent Devices	The number of installations of an application on devices that do not have the Agent installed. Type the value in the field on the Edit License page. See "Editing License Values" on page 105.
IP Address	A unique number identifying a computer on the Internet. See also Local IP Address and Public IP Address. In Customer Center, enter IP addresses in the format *[1-255].[0-255].[0-255].[0-255]*. You can use the asterisk (*) wildcard character. For example, to search for all IP addresses in the range 127.10.*[0-255].[0-255]*, type **127.10.*.***
Last Call Date OR **Last Call Time**	When the Agent installed on a device most recently contacted the Monitoring Center. If available, clicking the Last Call Date or Last Call Time link opens the Call History page for the asset.
Last Detected Service Status	The last reported availability of the network associated with a mobile device
Last Location Before Call	Indicates whether or not position information is the last set of coordinates received prior to an Agent call
Latest Service Pack	The most recent collection of updates, fixes and/or enhancements to a software program delivered in the form of a single installable package
Lease End Date	When an agreement to let goods ends
Lease Number	A unique identifier assigned to a lease
Lease Responsibility	A party accountable for let goods
Lease Start Date	When an agreement to let goods begins
Lease Vendor	The provider of let goods

Table 4. Report Data Definitions

Data	Definition
License Name	The known identifier of an installed application
License Status	The following values are possible: • **Show all licenses**—Includes all licenses listed in the Monitoring Center license database • **Show only licenses that are purchased or installed**—Includes licenses that have purchases recorded, or when devices do not have the Agent installed, installation values entered manually • **Show only licenses installed on Agent-equipped devices**—Includes licenses for applications detected on Agent-equipped devices
License Version Dependence	Whether or not the Program Version informs inclusion in report output
Licenses Available	The difference between the number of installations of an application and the number of Licenses Purchased
Licenses Purchased	The number of owned licenses for an application. Type the value in the field on the Edit License page. See "Editing License Values" on page 105.
Local IP Address	The IP address assigned to a device on the Local Area Network (LAN) when calling the Monitoring Center. See also IP Address and Public IP Address.
Local IP RDNS	The domain name associated with a Local IP Address. See also Proxy IP RDNS.
Location	The position of a device on the surface of the earth expressed in latitude and longitude
Location Obtained Via	The Location Technology used to determine the location of a device. See also Location Technology.
Location Technology	Customer Center supports numerous technologies for determining the location of a device. For details, see "Device Location Report" on page 113.
Location Time	When the position of a device was recorded
Location Type	The following values are possible: • **Include Intermediate Locations** — the position of a device over time • **Show Last Location At Call** — the most recent recorded position of a device only

Table 4. Report Data Definitions

Data	Definition
MAC Address	- **Laptops and computing devices with mobile broadband adapters** — Media Access Control (MAC) address of the network adapter used to complete a call to the Monitoring Center - **Smart phones** — One or more Media Access Control (MAC) addresses detected on the smart phone, most commonly Wi-fi MAC addresses. Some platforms may also have an Ethernet MAC address.
Make	The manufacturer of a device or other hardware
Model	The product type of a device or other hardware
Monitor Manufacturer	The maker of a device display
Monitor Refresh Frequency	The scanning rate of a display
Monitor Type	The kind of device display
Network	The mobile service provider associated with a mobile broadband adapter.
New Program Version	The current version number of a program installation
New Value	The current Hardware Description
Number of Calls	The amount of history Customer Center shows in report output
Number of Program Installations	The number of devices that have a program installed
Operating System	Software that controls the execution of computer programs and may provide various services
Persistence Status	How the Agent is automatically restored when necessary
Phone Number	The phone number detected on a smart phone or device. Currently, the Agent only detects the phone number for BlackBerry smart phones.
Phone Number Override	The alternative phone number associated with a mobile device or broadband adapter. If a phone number for a device is not automatically detected, the device sends a Short Message Service (SMS)—text message—to the Monitoring Center. The Reply-to address in the text message becomes the value in the Phone Number Override field. When sending text messages to a device, the value in the Phone Number Override field takes precedence over the value in the Detected Phone Number field.

Table 4. Report Data Definitions

Data	Definition
Policy Name	The name of a defined Software Policy. See "Software Policy" on page 72.
Previous Modem Model	The product type of a modem installed in a device in the past. Customer Center stores information about up to two prior modem installations.
Previous Port	The interface to which a Previous Modem Model was connected
Previous Program Version	The prior version number of a program installation
Previous Value	The prior Hardware Description
Product ID	A unique identifier for an application
Program Name	The title associated with one or more related applications. In practice, many publishers mutually exchange Program Name and Application Name values. See also Application Name.
Program Version	A unique name or number assigned to an identified and documented body of software
Proxy IP Address	See Public IP Address.
Proxy IP RDNS	Results of performing a Reverse Domain Name System (RDNS) lookup on a Proxy IP Address
Public IP Address	The IP address used to communicate with the Internet. For modem calls, Customer Center reports caller ID information instead. See also IP Address, Local IP Address and Caller ID.
Publisher Name	The organization creating a software application
Purchase Date	When a device was acquired
Purchase Order Reference	A unique identifier associated with an authorization to buy goods or services
RAM Size	The amount of dynamically accessible memory in a device
Readme	The full directory path to the Readme file for a program
Recent Activations	Agent activations occurring in a specified date range according to default report filter criteria
Serial Number	The serial number of the device or other hardware
Service Contract End Date	When provision of support and maintenance expires

Table 4. Report Data Definitions

Data	Definition
Service Contract Start Date	When provision of support and maintenance begins
Service Contract Vendor	A provider of support and maintenance
Service Pack	A collection of updates, fixes and/or enhancements to a software program delivered in the form of a single installable package
Size	A physical magnitude
Software Policy ID	The unique identifier assigned to a Software Policy in Customer Center. See "Software Policy" on page 72
Software Status	The type of non-compliance of a software installation with a Software Policy. These are possible values: • Banned • Missing • Not Approved
Subscriber ID	The unique number associated with the smart phone network service subscriber. The number is retrieved from the Smart Phone hardware, the Subscriber Identity Module (SIM) card, or an equivalent.
Support Telephone	The technical support phone number for a software program
Suspicious Event	An event that triggered one or more alert notifications based on alerts defined for the account.
Suspicion Level	The importance level or grade that defines the severity of a suspicious event.
System BIOS Date	When the Basic Input/Output System (BIOS) installed in a device released
System BIOS Version	The unique name or number assigned to the Basic Input/Output System (BIOS) of a device
Unlicensed Software	Software that does not have a license defined in Customer Center
User-defined	Data associated with tracked devices that is unique to a customer
User Name	The user name of an individual associated with a device
User Phone/Extension	The complete telephone number of an individual associated with a device
Video Device Name	The known identifier of a video card in a device

Table 4. Report Data Definitions

Data	Definition
Video Display Resolution	The number of distinct horizontal and vertical pixels showing on a monitor
Video Display Color Depth	The number of bits used to represent color on a monitor
Virus Definition Date	When a file containing signatures to identify viruses or malware was released
Virus Definition Detection Date	When a virus definition file was first identified on a device
Virus Definition File Name	The name of a file containing signatures to identify viruses or malware
Warranty Contract Vendor	The warranty provider for a device
Warranty End Date	When a warranty expires
Warranty Start Date	When a warranty begins

Chapter 6 Using Intel Anti-Theft Technology

Certain laptops equipped with Intel® Anti-theft Technology (AT) technology can be managed in Customer Center. AT technology allows an Administrator to lock a device if the notebook is lost or stolen.

IMPORTANT Only Security Administrators can change AT settings in Customer Center. Administrators, Power Users and Guests can only view and filter the list of Intel® AT devices. See "Data and Device Security Administration" on page 30 for more information.

Intel® equipped devices come pre-installed with Intel® AT drivers, such as the Host Embedded Controller Interface (HECI) driver, the Active Management Technology driver (AMT), and the Management Engine Interface driver (MEI). These drivers are necessary to perform any Intel® AT Management activities. It is important to re-install all Intel® AT drivers after re-installing the operating system or re-imaging the device. Refer to your product documentation for more information on locating these drivers.

IMPORTANT If you do not re-install AT drivers on a newly installed OS or system image, Intel® AT management requests, such as sending a poison pill or changing settings, do not work as intended. Without the necessary drivers, the timer is unable to reset and leads to counting down to zero and locking the device.

Anti-theft Technology integrates the following features:

- **Agent Call Lock Request**—Using Customer Center, you can set a request to lock the device next time the device makes an Agent call. Locking a lost or stolen device using AT is independent of reporting the missing device to Absolute Software for recovery.
- **Countdown Timer**—Each time a device equipped with AT contacts the Monitoring Center, an AT countdown timer resets. If the timer reaches zero, the device automatically locks. Use the countdown timer carefully and allow for flexibility. For example, a device using a three-day countdown timer must contact the Monitoring Center at least every three days. If the user goes on vacation and does not use the device for one week, the device locks and is rendered unusable. Customer Center sends an e-mail alert to the device user and the administrator when a device is 2 days or less from locking.
- **SMS Lock Request**—On devices with mobile broadband adapters and Intel 2.0 support, where Real Time Technology (RTT) and Intel® AT 2.0 from Computrace are enabled, you can send Intel® AT lockdown requests and receive confirmation of successful lockdown using SMS messages.

When a locked device is switched on, the device shows a screen prior to booting that explains the device has been locked. Typing a reactivation Password or Server Recovery Token unlocks the device.

NOTE Locked devices do **not** boot without entering the Password or Server Recovery Token. You cannot reinstall the operating system on a locked device.

Why Use Anti-theft Technology?

Intel® Anti-theft Technology provides excellent security when guarding the data on a device is more important than the hardware.

Consider the following scenarios.

Locking on an Agent Call

Jeff, a Sales Representative, has his AT equipped laptop stolen when he was attending a conference. On realizing the theft, Jeff immediately contacts his organization's IT department. The administrator logs into Customer Center and changes the laptop's AT Theft Status from Active to Locked.

The next time the laptop contacts the Monitoring Center, an action to lock the device is initiated. Within moments, the system locks and becomes unusable. See "Locking Devices With Intel AT" on page 164 for more information.

The administrator contacts Jeff, informing him the device has been protected. The IT department helps Jeff get set up with a replacement device, restoring data from the organization's backup system.

See "Locking Devices on an Agent Call" on page 164 for more information.

Using the Countdown Timer

Beth, who lives in a rural area and works remotely every second Friday, forgets the briefcase containing her notebook commuting to the office for an emergency meeting. She does not notice that she has lost the briefcase until the following Friday.

Reporting the stolen notebook to her IT department, the administrator assures her that since the Agent has not contacted the Monitoring Center in a week, Intel® AT has been used to lock-down the device.

See "Locking Devices With a Countdown Timer" on page 168 for more information.

Customer Center Overview

When devices have Intel® AT and you have AT service, the Intel® Anti-Theft Technology area is available on the Data and Device Security page in Customer Center. The Intel® Anti-Theft Technology area lists links to two pages:

- **Set Intel® Anti-Theft Technology Defaults** allows you to set default parameter values for new Intel® AT activations. Each new AT equipped device you activate automatically inherits the default values.
- **Manage Devices Equipped with Intel® Anti-Theft Technology** lists and allows you to administer specific devices that have Intel® AT technology and AT service. For example, you can configure a subset of your devices with different AT settings, lock devices, set the timer, and generate recovery tokens.

Intel AT Device States

Intel® AT equipped devices can have the following states:

- **Inactive (Intel® AT State is Off)** devices have the Intel® AT Agent Call Lock Request and Countdown Timer features turned off. Inactive devices do not lock. See “Turning AT On or Off” on page 160 for more information on changing the Intel® AT State for a device.
- **Active (Intel® AT State is On)** devices have the Intel® AT Agent Call Lock Request and Countdown Timer features turned on. See “Turning AT On or Off” on page 160 for more information on changing the Intel® AT State for a device.
- **Locked** devices lock according to default Intel® AT settings specified using Customer Center. See “Locking Devices With Intel AT” on page 164 for more information.

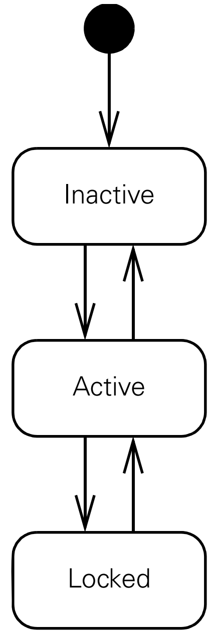

FIGURE 1. Allowed Intel® AT Device State Changes

Setting Default Parameter Values

Each new AT equipped device you activate automatically inherits the values for the following parameters:

- **Default Timer Period** — This field determines the duration of the countdown timer. The timer ranges from 2 to 48 days. Out of the box, the AT Timer Value is the maximum 48 days. For example, to create a default timer value to lock devices that do not contact the Monitoring Center within two weeks, set the timer to 14 days. To avoid the countdown timer locking devices, set the timer to the maximum value of 48 days.
- **Default Timer Action** and **Default Lock Request Action** — Default Timer Action sets the action to occur when the countdown timer reaches zero. Default Lock Request Action determines how to lock a device when invoking the lock request on an Agent call. For each parameter, the following actions may occur:
  - **Do Nothing** — The Intel® AT countdown timer runs down to zero, but the device does not lock.

    NOTE The **Do Nothing** option is available on some first generation AT devices.

  - **Immediate System Lock** — The device is locked without delay, for example when the operating system is running. The risk of corrupting data is higher if a device is locked when the operating system is running and files are open.

  - ○ **Lock on Next Reboot**—The device is locked next time the system starts. The out-of-the-box value for both parameters is Lock on Next Reboot.

- **Default AT Password**—This field sets the password used to unlock a locked device. The AT password supports **only** digits (0-9). The AT password does **not** support letters. You must type the AT password using the number row on the keyboard. Do **not** type the AT password using a numeric keypad.

  IMPORTANT A default password is required and must be set prior to activating Intel AT on any device.

- **Automatically turn on Intel AT for new devices** — This field sets automatic enrollment for all new Intel AT-equipped devices. When you select the checkbox, if additional Intel AT licenses are available, Intel AT is turned on for all newly activated devices by default. If there are no Intel AT licenses available for your account, Intel AT is not turned on automatically. In such cases, you may choose to free up licenses by disabling Intel AT on other devices, such as devices that are no longer in use or do not need Intel AT services. For more information on manually managing Intel AT on devices see "Changing Parameters for Active Devices" on page 152.

For new activations, Customer Center sets AT parameters for devices using default values the first time the device contacts the Monitoring Center after AT service is available.

IMPORTANT Always ensure that new Agent installations and activations complete successfully. Successful activations are available in the list of devices on the Manage Devices Equipped with Intel® Anti-Theft Technology page showing **Active** in the **AT State** field. See the *Agent Installation Guide* available on the *Customer Center Documentation* page for more information on installing and activating the Agent.

Changing default values applies to new activations only. For example, if your default password is 667788, and then you change the default password to 778899, only subsequent new activations inherit the new default password. Devices you activated using the previous password retain the previous password. However, you can also easily change parameter values such as the password for devices that are already active. See "Changing Parameters for Active Devices" on page 152 for more information.

Specifying Intel AT Default Settings

To set AT parameters for new activations:

1. Log in to the Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click **Set Intel® Anti-Theft Technology Defaults** in the **Intel® Anti-Theft Technology** section.

NOTE Devices that have had AT turned on at least once in the past do not receive default values specified using the Set Intel® Anti-Theft Technology Defaults page.

Setting a Default Timer Period

To set the default timer period for new activations:

1. On the **Set Intel® Anti-Theft Technology Defaults** page in Customer Center, type the number of days to count down ranging between two and 48 in the **Default Timer Period** field.
2. Click **Save**. If your account uses authentication, the Request Authentication page opens.

   NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

3. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
4. Click **OK**.

Setting a Default Timer Action

To set the default timer action for new activations:

1. In the **Default Timer Action** section, on the **Set Intel® Anti-Theft Technology Defaults** page in Customer Center, select one of the following:
   - **Do nothing** — allows the device to remain active after the timer runs down. When the timer runs down for the devices with the **Do Nothing** option set, the timer trips but the device is not

locked. The device only accepts requests to initialize the Kill Pill or change the device state to **Active**.

> **NOTE** The **Do Nothing** option is not available on first generation AT devices. If the **Do nothing** option is not available, the **Lock on Next Reboot** option is executed on the next Agent call.

- **Immediate System Lock** — locks the device immediately after the AT timer runs down.
- **Lock on Next Reboot** — locks the device on the next device restart after the AT timer runs down.

2. Click **Save**. If your account uses authentication, the Request Authentication page opens.

> **NOTE** By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See “Technical Support” on page 15 in the Customer Center User’s Guide.

3. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
4. Click **OK**.

To set the default lock request action for new activations:

1. In the **Default Lock Request Action** section on the **Set Intel® Anti-Theft Technology Defaults** page in Customer Center, select one of the following:
   - **Do Nothing**
   - **Immediate System Lock**
   - **Lock on Next Reboot**
2. Click **Save**. If your account uses authentication, the Request Authentication page opens.

> **NOTE** By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See “Technical Support” on page 15 in the Customer Center User’s Guide.

3. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
4. Click **OK**.

Specifying a Default Intel AT Message

Newer AT equipped devices can show a user-specified message every time the device is AT locked.

NOTE First generation AT devices do not support user-specified messaging.

To specify a default AT lock message:

1. In the **Default Locked Device Display String** section on the **Set Intel® Anti-Theft Technology Defaults** page in Customer Center, enter the appropriate message text in the field. The message can use a maximum of 127 characters.
2. Click **OK** at the bottom of the dialog box. If your account uses authentication, the Request Authentication page opens.

   NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

3. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
4. Click **OK**.

Setting the Default AT Password

By default, AT is turned off for all devices in accounts without a default AT password.

To set the default AT password for new activations:

1. In the **Default Passcode for New Activations** section on the **Set Intel® Anti-Theft Technology Defaults** page in Customer Center, type the numeric password to use from now on in the **Enter Passcode** field.
2. In the **Confirm Passcode** field, re-type the numeric password typed in the **Enter Passcode** field.
3. Click **Save**. If your account uses authentication, the Request Authentication page opens.

   NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

4. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.

5. Click **OK**.

Automatically Turning Intel AT On for New Devices

By default, when you add a new Intel AT-equipped device to your account, Intel AT is turned on for the device. This feature is called Auto-enrollment in Intel AT and is available for accounts which have:

- open Intel AT licenses; and
- one or more existing Security Administrators authorized to perform Data and Device Security options.

If your account does not have Intel AT licenses or Security Administrators available, the automatic enrollment of new devices in Intel AT is turned off. If you would still like to turn on automatic enrollment of new devices in Intel AT, you must turn off Intel AT on some of your existing devices. For more information on turning Intel AT off on selected devices see "Turning AT Off" on page 162.

To automatically turn Intel AT On for newly activated Intel AT devices in your account:

1. On the **Set Intel® Anti-Theft Technology Defaults** page in Customer Center, select the **Automatically turn on Intel AT for new devices** checkbox.
2. Click **Save**. If your account uses authentication, the Request Authentication page opens.

   NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

3. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
4. Click **OK**. If there are any free Intel AT licenses available for your account, when you add any new Intel AT-equipped devices to your account Intel AT is automatically turned on for these devices.

Changing Parameters for Active Devices

Using Customer Center, you can change parameter values for one or more active devices to override default parameter values. You can also make devices inactive, turning off the Intel® AT Agent Call Lock and Countdown Timer features.

Customer Center synchronizes parameter value changes the next time devices make an Agent call to the Monitoring Center.

NOTE Customer Center shows pending parameter value changes next to current device states.

Changing Settings For Selected Intel AT equipped Devices

To change Intel® Anti-theft Technology parameter values for active devices:

1. Log in to the Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Intel® Anti-Theft Technology** section, click **Manage Devices Equipped with Intel® Anti-Theft Technology**.

Changing Intel AT Timer Period

To change the AT timer period for active devices:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the active devices whose values you want to change.
2. Do one of the following:
   - If you want to select all the devices showing in the results grid, select the checkbox in the left-hand column of the top row to open the Select All dialog box. Continue with step 3.
   - If you want to select specific devices, select the checkbox next to devices requiring a change to the AT timer value. Continue to step 4.
3. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid.
   - **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid only.

   The Manage Devices Equipped with Intel® Anti-Theft Technology page opens to show the checkboxes for the devices selected.

4. Click **Change AT Settings for selected devices** to open the Change Settings for Selected Intel® AT-equipped Devices dialog box.
5. In the **Action** list for the **Timer Period** row, select **Change Timer Period**.
6. In the **Days** field, type the number of days ranging from 2 to 48 to count down.
7. Scroll down to click **OK** at the bottom of the dialog box. One of the following happens:

   NOTE When turning on AT for devices, Customer Center sets AT parameters, including the AT password, using default values.

   - If your account uses authentication, the Request Authentication page opens. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. The new Intel AT timer value is saved for your selected devices.

     NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

   - If your account does not use authentication, the new Intel AT timer value is saved for your selected devices.

Changing Intel AT Timer Action

The AT Timer Action specifies the action that occurs when the AT timer for a device runs down.

To change the AT timer action for active devices:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the active devices whose values you want to change.
2. Do one of the following:
   - If you want to select all the devices showing in the results grid, select the checkbox in the left-hand column of the top row to open the Select All dialog box. Continue with step 3.
   - If you want to select specific devices, select the checkbox next to devices requiring a change to the AT timer value. Continue to step 4.
3. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the

Manage Devices Equipped with Intel® Anti-Theft Technology results grid.

- **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid only.

The Manage Devices Equipped with Intel® Anti-Theft Technology page opens to show the checkboxes for the selected devices checked.

4. Click **Change AT Settings for selected devices** to open the Change Settings for Selected Intel® AT-equipped Devices dialog box.
5. In the **Action** list for the **Timer Action** row, select one of the following options to specify the action:
   - **Do nothing**
   - **Immediate System Lock**
   - **Lock on Next Reboot**

NOTE See “Setting a Default Timer Action” on page 149 for more details on each of these actions.

6. Click **OK** at the bottom of the dialog box. One of the following happens:

NOTE When turning on AT for devices, Customer Center sets AT parameters—including the AT password—using default values.

- If your account uses authentication, the Request Authentication page opens. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. The new Intel AT timer action value is saved for your selected devices.

  NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See “Technical Support” on page 15 in the Customer Center User’s Guide.

- If your account does not use authentication, the new Intel AT timer action value is saved for your selected devices.

Changing the AT Lock Request Action

The AT Lock Request Action setting determines the action that occurs when the Agent calls the Monitoring Center if the device state is set to Lock. The device locks immediately or next time the device reboots.

To change the action performed when a device is AT locked:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the active devices whose values you want to change.
2. Do one of the following:
   - If you want to select all the devices showing in the results grid, select the checkbox in the left-hand column of the top row to open the Select All dialog box. Continue with step 3.
   - If you want to select specific devices, select the checkbox next to devices requiring a change to the AT timer value. Continue to step 4.
3. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid.
   - **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid only.

   The Manage Devices Equipped with Intel® Anti-Theft Technology page opens to show the checkboxes for the selected devices checked.
4. Click **Change AT Settings for selected devices** to open the Change Settings for Selected Intel® AT-equipped Devices dialog box.
5. In the Action list for the **Lock Request Action** row, select one of the following:
   - **Immediate System Lock**
   - **Lock on Next Reboot**.
6. Click **OK** at the bottom of the dialog box. One of the following happens:

   NOTE When turning on AT for devices, Customer Center sets AT parameters—including the AT password—using default values.

   - If your account uses authentication, the Request Authentication page opens. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. The new Intel AT lock request action is saved for your selected devices.

     NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

   - If your account does not use authentication, the new Intel AT lock request action is saved for your selected devices.

Specifying a New Intel AT Message

AT equipped devices can show a user-specified message every time the device is AT locked.

IMPORTANT First generation AT devices do not support the Custom AT message functionality.

To specify a new or change an existing AT lock message:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the active devices whose values you want to change.
2. Do one of the following:
   - If you want to select all the devices showing in the results grid, select the checkbox in the left-hand column of the top row to open the Select All dialog box. Continue with step 3.
   - If you want to select specific devices, select the checkbox next to devices requiring a change to the AT timer value. Continue to step 4.
3. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid.
   - **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid only.

   The Manage Devices Equipped with Intel® Anti-Theft Technology page opens to show the checkboxes for the selected devices checked.
4. Click **Change AT Settings for selected devices** to open the Change Settings for Selected Intel® AT-equipped Devices dialog box.
5. In the **Action** list for the **Intel AT Message** row, select **Change AT message**. The Change Settings for Selected Intel® AT-equipped Devices dialog box refreshes to show a field under the **Action** list.
6. Enter the appropriate message text in the field.
7. Click **OK** at the bottom of the dialog box. One of the following happens:

   NOTE When turning on AT for devices, Customer Center sets AT parameters—including the AT password—using default values.

   - If your account uses authentication, the Request Authentication page opens. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization

Code, and then click **OK**. The new Intel AT message is saved for your selected devices.

NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

- If your account does not use authentication, the new Intel AT message is saved for your selected devices.

Viewing Intel AT Messages for a Device

The Intel® AT Message dialog box shows the existing AT message used for the device and the new message in queue for showing on the next Agent call.

To view the current and future AT messages:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the appropriate device.
2. In the **Identifier** column of the results grid, click the shortcut button. A shortcut menu opens.
3. Click the **View Message** link. The Intel® AT Message dialog box opens.
4. Click **Close** at the top right corner of the dialog box to return to the previous page.

Changing the AT Password

A default AT password is used to unlock AT locked devices. You can specify a default password for all devices in your account or separate default passwords for different devices in your account.

IMPORTANT If a default password is not set for your account, all Intel® Anti-Theft functionality on the AT equipped devices in your account remains turned off. For security purposes, the AT Off state remains in place until a default unlock password is set for your account.

To change the AT password for active devices:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the active devices whose values you want to change.
2. Do one of the following:
   - If you want to select all the devices showing in the results grid, select the checkbox in the left-hand column of the top row to open the Select All dialog box. Continue with step 3.

   - If you want to select specific devices, select the checkbox next to devices requiring a change to the AT timer value. Continue to step 4.

3. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid.
   - **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid only.

   The Manage Devices Equipped with Intel® Anti-Theft Technology page opens to show the checkboxes for the selected devices checked.

4. Click **Change AT Settings for selected devices** to open the Change Settings for Selected Intel® AT-equipped Devices dialog box.
5. In the **Action** list for the **Passcode** row, select **Change Passcode**. The Change Settings for Selected Intel® AT-equipped Devices dialog box refreshes to show the **Enter Passcode** and **Confirm Passcode** fields under the **Action** list.
6. In the **Enter Passcode** field, enter the new 4 to 20 digit numeric password to use from now on.
7. In the **Confirm Passcode** field, re-type the numeric password you typed in the **Enter Passcode** field.

   IMPORTANT Do **not** forget the AT password. Using the AT password is the quickest way to unlock locked devices.

8. Click **OK** at the bottom of the dialog box. One of the following happens:

   NOTE When turning on AT for devices, Customer Center sets AT parameters—including the AT password—using default values.

   - If your account uses authentication, the Request Authentication page opens. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. The new Intel AT passcode is saved for your selected devices.

     NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See “Technical Support” on page 15 in the Customer Center User’s Guide.

   - If your account does not use authentication, the new Intel AT passcode is saved for your selected devices.

Turning Off Automatic Enrollment of Intel AT-equipped Devices

By default, when you add a new Intel AT-equipped device to your account, Intel AT is turned on for the device. You can turn off automatic enrollment of new devices in Intel AT.

To turn off automatic enrollment of new devices in Intel AT:

1. On the **Set Intel® Anti-Theft Technology Defaults** page in Customer Center, clear the **Automatically turn on Intel AT for new devices** checkbox.
2. Click **Save**. If your account uses authentication, the Request Authentication page opens.

   NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

3. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
4. Click **OK**. When you add any new Intel AT-equipped devices to your account, Intel AT is no longer turned on for these devices.

Turning AT On or Off

AT equipped devices in your account can fall into two categories:

- **AT Turned On** — devices against which you can submit AT requests. Devices with AT turned on and contacting the Monitoring Center regularly are also known as "Active" devices. At any given point, the number of Active Intel AT-equipped devices must be less than or equal to the number of available Intel AT licenses for your account.
- **AT Turned Off** — devices that cannot accept AT requests and have their countdown timers switched off. Devices with AT turned off are also known as "Inactive" devices.

Depending upon whether AT on a device is turned on or off, you can submit AT lock, unlock, or state change requests against a device. You can turn AT on or off for a single or multiple devices at the same time.

Turning AT On

IMPORTANT Before you continue, ensure that you have an adequate number of Intel AT licenses available for your account. If you do not have any Intel AT licenses available for your account, you cannot turn on Intel AT for any devices for your account. If you do not have an adequate number of licenses, you must turn off Intel AT on some devices to free up some licenses before you continue with turning AT on for any new devices.

To turn AT on for selected devices:

1. Log in to the Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Intel® Anti-Theft Technology** section, click **Manage Devices Equipped with Intel® Anti-Theft Technology** to open the Manage Devices Equipped with Intel® Anti-Theft Technology page.
4. In the **AT State** list, select **Intel AT Off**.
5. Specify all the other appropriate search criteria.
6. Click **Show Results**. The Manage Devices Equipped with Intel® Anti-Theft Technology page refreshes to show a list of all the devices matching your search criteria in the results grid.
7. Select the checkbox in the left-hand column of the top row to open the Select All dialog box.
8. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid.
   - **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid only.

   The Manage Devices Equipped with Intel® Anti-Theft Technology page opens to show the checkboxes for the selected devices checked.
9. Click **Change states for selected devices** to open the Change AT State dialog box.
10. In the **Action** list for the **Intel AT Off** row, select **Turn Intel AT On**.

11. Click **Submit**. One of the following happens:

    NOTE When turning on AT for devices, Customer Center sets AT parameters—including the AT password—using default values.

    - If your account uses authentication, the Request Authentication page opens. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. Intel AT is turned on for the selected devices on the next Agent call.

      NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

    - If your account does not use authentication, Intel AT is turned on for the selected devices on the next Agent call.

Turning AT Off

If the number of Active Intel AT devices in your account exceeds the number of available Intel AT licenses, you cannot turn on Intel AT for any additional devices. You can free up some licenses by turning Intel AT off for some Active devices.

To turn AT off for selected devices:

1. Log in to the Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Intel® Anti-Theft Technology** section, click **Manage Devices Equipped with Intel® Anti-Theft Technology** to open the Manage Devices Equipped with Intel® Anti-Theft Technology page.
4. In the **AT State** list, select **Active**.
5. Specify all the other appropriate search criteria.
6. Click **Show Results**. The Manage Devices Equipped with Intel® Anti-Theft Technology page refreshes to show a list of all the devices matching your search criteria in the results grid.
7. Select the checkbox in the left-hand column of the top row to open the Select All dialog box.
8. Click the appropriate button from the following:

- **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid.
- **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped with Intel® Anti-Theft Technology results grid only.

The Manage Devices Equipped with Intel® Anti-Theft Technology page opens to show the checkboxes for the selected devices checked.

9. Click **Change states for selected devices** to open the Change AT State dialog box.
10. In the **Action** list for the **Active** row, select **Turn Intel AT Off**.

NOTE When you turn Intel AT off for one or more devices, the corresponding number of Intel AT licenses are made available for your account.

11. Click **Submit**. One of the following happens:

- If your account uses authentication, the Request Authentication page opens. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. Intel AT is turned off for the selected devices on the next Agent call.

  NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

- If your account does not use authentication, Intel AT is turned off for the device on the next Agent call.

Filtering the Device List

To simplify administering a large number of devices equipped with AT technology, you can filter listed devices based on the following criteria:

- **Group**—This field determines the Device Group to show.
- **Field**—You can filter on user-defined fields as well as the following system fields: **Identifier**, **Detected Full Computer Name**, **Detected User Name**, **Detected Make**, **Detected Model**, **Detected Serial #**, and **Asset #**
- **Last Call**—This field uses the time and date stamp of the most recent contact devices have with the Monitoring Center to filter.
- **AT State**—Filter inactive devices or devices invoking the AT Agent Call Lock Request.

- **AT Timer Value**—Filter based on the duration of the AT countdown timer.
- **AT Lock Request Action**—Filter based on the setting indicating how to lock a device when the AT Agent Call Lock Request is invoked. You can also filter based on the setting indicating the lock action on the next Agent call.
- **AT Timer Action—**Filter based on the setting indicating the action to take when the AT countdown timer reaches zero. You can also filter based on the setting indicating the timer action on the next Agent call.
- **AT Changes—**Show or hide devices that have parameter values to update, pending contact with the Monitoring Center.

NOTE By default, the device list shows active devices.

To filter the list of devices that have AT:

1. In the **Show Intel® AT equipped devices where** area on the **Manage Devices Equipped with Intel® Anti-Theft Technology** page, use the drop-down menus and fields to set criteria for filtering.
2. Click **Show Results**.

The list of devices shows current parameter values for each device.

NOTE In case of any Intel® AT errors, a warning icon shows in the **Current State** column in the results grid. Click the warning icon to view details about the error. Refer to Intel Anti-theft Technology Error Codes for detailed information about the types of errors that can occur.

Locking Devices With Intel AT

You can lock Intel® AT equipped devices in the following ways:

- Locking Devices on an Agent Call
- Locking Devices With Intel AT SMS Lock Requests
- Locking Devices With a Countdown Timer

Locking Devices on an Agent Call

You can use the Lock Device on Agent Call functionality to implement an immediate Intel® AT lock on lost or stolen devices. Once you set the lock request, the device locks on the next Agent call to the Monitoring Center depending upon the settings specified.

To lock devices on Agent call:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the appropriate device.
2. In the **Identifier** column of the results grid, click the shortcut button. A shortcut menu opens.
3. Click the **Change State** link. The Change AT State dialog box opens.
4. Select the **Lock** option.
5. Click **OK**. Depending upon the technology supported on the target device, one of the following two actions occur:
   - If the device is RTT and Intel AT enabled, a dialog box prompting you to force a call to the device using MCIC opens. If appropriate, force a call to the device. See "Initiating a Forced Call" on page 67 for more information. Once the device receives and processes the SMS message, depending upon the AT defaults set for the account, the device locks. For possible lock methods see step 6.
   - For all other devices, the Intel® AT Agent Call Lock Request is set and the Change AT State dialog box closes. For possible lock methods see step 6.
6. Depending upon the AT settings specified for the account and/or the individual target device, the device locks in one of the following ways upon the next Agent call:
   - **Immediate System Lock** — the device locks on the Agent call, immediately once the request is sent to the device.

     IMPORTANT The Immediate System Lock option should be selected with care since the risk of corrupting data is higher if a device is locked when the operating system is running and files are open.

   - **Lock on Next Reboot** — the device locks upon the next system restart after the Agent call.

Locking Devices With Intel AT SMS Lock Requests

For devices supporting RTT and Intel® AT technology, and equipped with a mobile broadband adapter, you can choose to send the Intel® AT lock request using an SMS text message. Devices locked with an Intel® AT SMS Lock Request are immediately locked upon processing the SMS message. Whether the lock takes place immediately or on the next reboot, and the message shown on the locked device depends upon the Intel® AT settings specified for the device. Ensure that the mobile broadband adapter meets the requirements listed in Prerequisites For Using Real-time Technology (RTT).

NOTE If the target device does not run on one of the processors required to support RTT and MCIC, you can still use MCIC to lock the device with Intel AT faster than the time required to lock it with an Agent call.

Currently, the Intel AT SMS Lock Request and MCIC features are only available if you are locking a single device. You cannot initiate SMS lock requests using RTT or MCIC if you are editing more than one device.

The Intel® AT SMS Lock Request feature offers the following functionality:

- Sending Intel AT SMS Lock Requests
- Monitoring the Intel AT SMS Lock Request Status

Sending Intel AT SMS Lock Requests

To lock devices with an Intel® AT SMS Lock Request:

IMPORTANT The Intel® AT SMS Lock Request locks the device upon receipt depending upon the Intel® AT settings for your device. Use the Immediate Lock setting with care since the risk of corrupting data is higher if a device is locked when the operating system is running and files are open. See "Setting Default Parameter Values" on page 147 for more information about possible options.

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the appropriate device.
2. In the **Identifier** column of the results grid, hover over the shortcut button. A shortcut menu opens.
3. Click the **Change State** link. The Change AT State dialog box opens.
4. Select the **Lock** option.
5. Click **OK**. The following scenarios are possible:
   - For devices supporting RTT and Intel® AT 2.0 technology, the Send Intel® Anti-Theft SMS Lock Request dialog box opens.
   - For devices not supporting RTT and Intel® AT 2.0, the device locks upon the next Agent call. See "Locking on an Agent Call" on page 145 for more information.
6. Click **Send SMS Lock Request** for the appropriate mobile broadband adapter. If the device and mobile broadband adapter meet the requirements for successfully receiving Intel® AT SMS Lock Requests, the Intel® AT SMS Lock Request is sent. The Intel® AT SMS Lock Request Send Status dialog box opens to show a message confirming successful transmission.

7. Click **Continue**. The Manage Devices Equipped with Intel® Anti-Theft Technology page opens.

Monitoring the Intel AT SMS Lock Request Status

The Intel® AT SMS Lock Request Status dialog box allows you to monitor the status of previously sent Intel® AT SMS Lock Requests and send up to three new Intel® AT SMS Lock Requests before the next scheduled Agent call. The Intel® AT SMS Lock Request Status dialog box lists the following information about Intel® AT SMS Lock Requests in the **Recently Sent SMS Lock Requests** section:

- **Created**—the date on which the Intel® AT SMS Lock Request was sent
- **Updated**—the date on which the information about the Intel® AT SMS Lock Request was last updated.
- **ID**—the unique system generated identification number assigned to the Intel® AT SMS Lock Request
- **Phone Number**—the phone number associated with the mobile broadband adapter to which the Intel® AT SMS Lock Request was sent
- **Status**—the current status of the Intel® AT SMS Lock Request

To view the status of previously sent Intel® AT SMS Lock Requests:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the appropriate AT locked device.
2. In the **results** grid, hover over the shortcut button in the Identifier column of the appropriate device. A shortcut menu opens. If the device is currently in the Lock Requested or Locked states, the **SMS Lock Requests** link is available in the shortcut menu.
3. Click the **SMS Lock Requests** link. The Intel® AT SMS Lock Request Status dialog box opens listing Intel® AT SMS Lock Request information in the **Recently Sent SMS Lock Requests** section.

To send a new Intel® AT SMS Lock Request using the Intel® Anti-Theft SMS Lock Request Status dialog box:

1. On the Intel® Anti-Theft SMS Lock Request Status dialog box, click **Send SMS Lock Request**. If the device is not locked and meets the requirements for successful transmission of the Intel® AT SMS Lock Request, the new Intel® AT SMS Lock Request is sent. The Intel® Anti-Theft SMS Lock Request Send Status dialog box opens to show a message confirming successful transmission.
2. Click **Close**. The Intel® Anti-Theft SMS Lock Request Status dialog box opens listing the status for all Intel® AT SMS Lock Requests sent to the device.

Locking Devices With a Countdown Timer

Using the countdown timer enables you to lock devices with Intel® AT if the device does not call in to the Monitoring Center for a specified period of time. The Lock Devices With a Countdown Timer feature allows you to monitor the security of devices in your account.

To use the countdown timer:

1. Set the appropriate Intel® AT defaults at the account level using the **Set Intel® AT Defaults** page or at a device level using the **Change AT Settings For Selected Devices** page. See "Specifying Intel AT Default Settings" on page 148 and "Changing Settings For Selected Intel AT equipped Devices" on page 153 for more information.
2. Depending upon the Timer Period and Timer Action settings specified for the device, when the timer runs down, the device locks in one of the following ways:
   - **Immediate System Lock** — the device locks immediately once the timer runs down.

     IMPORTANT The Immediate System Lock option should be selected with care since the risk of corrupting data is higher if a device is locked when the operating system is running and files are open.

   - **Lock on Next Reboot** — the device locks upon the next system restart after the Timer runs down.

Unlocking Locked Devices

You can unlock a device in one of the following ways:

- Unlocking Devices Using the AT Password

  NOTE When unlocking a locked device, type the AT password using the number row on the keyboard. Do **not** type the AT password using a numeric keypad.

- Using a Server Recovery Token

  IMPORTANT Once the device is unlocked, you need to change the device state to **Unlock Requested** in Customer Center. If you do not change the device state to **Active** for an unlocked device, the device locks again on the next Agent call to the Monitoring Center. See "Changing Device State to Unlocked" on page 170 for more information.

Unlocking Devices Using the AT Password

To unlock a locked device using the AT password:

1. Turn on the device.
2. When prompted to enter your reactivation Password or Server Recovery Token, press **1**, and then type the AT password using the number row on the keyboard (**not** using a numeric keypad), and then press ENTER. The device boots.

Using a Server Recovery Token

If the unlock password for a locked device is unknown or does not work, you can use a server recovery token to unlock the device.

To generate a server recovery token for your locked device:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the appropriate AT locked device.
2. In the **results** grid, click the shortcut button in the Identifier column of the appropriate device. A shortcut menu opens.
3. Click **Generate Server Recovery Token**. The Generate Server Recovery Token page opens.
4. Type the **Platform Recovery ID** for the locked device in the **Enter Platform Recovery ID** field.

   NOTE You can find the Platform Recovery ID for a locked device on the Intel® AT Recovery message screen.

5. Click **Generate Server Recovery Token**. If your account uses authentication, the Request Authentication page opens.

   NOTE By default, authentication is turned off for all accounts. To enable authentication for your account, contact Absolute Software Customer Support. See "Technical Support" on page 15 in the Customer Center User's Guide.

6. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
7. Click **OK**. The page refreshes to show the server recovery token. Copy the generated code to the clipboard and provide it to the user.

To unlock a locked device using the Server Recovery Token:

1. Turn on the locked device.
2. When prompted to enter your reactivation Password or Server Recovery Token, press **2** on your keyboard, then type the Server Recovery Token, and then press ENTER. The device boots.

Changing the Device State

Changing Device State to Unlocked

Once a device locked with an Intel® AT Lock Request is unlocked, a security administrator needs to change the state for the device to Active in Customer Center. If you do not change the state to Active, the device locks again on the next Agent call.

NOTE By default, Customer Center does not request authentication for generating a server recovery token or changing the AT state. To enable authentication for your account, contact Absolute Software Customer Support. See “Technical Support” on page 15 for more information.

To change the state of an unlocked device:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the appropriate device.
2. In the **Identifier** column of the results grid, click the shortcut button. A shortcut menu opens.
3. Click the **Change State** link. The Change AT State dialog box opens.
4. In the **Change AT State** section, select the **Unlocked** option.
5. Click **OK**. The device state changes to **Unlock Requested**, and changes to **Active** on the next Agent call.

Customer Center shows pending state changes next to current device states. The next time a device for which you set the status to unlocked or active contacts the Monitoring Center, the device unlocks.

Canceling a Change Device State Request

Security administrators can cancel a pending unlock request that has not been implemented on the device.

NOTE By default, Customer Center does not request authentication for generating a server recovery token or changing the AT state. To enable authentication for your account, contact Absolute Software Customer Support. See “Technical Support” on page 15 for more information.

To cancel a device unlock request:

1. On the **Manage Devices Equipped with Intel® Anti-Theft Technology** page in Customer Center, search for the appropriate device for which you want to cancel the unlock request.

2. In the **Identifier** column of the results grid, click the shortcut button. A shortcut menu opens.
3. Click the **Change State** link. The Change AT State dialog box opens.
4. In the **Change AT State** section, select the **Cancelled** option.
5. Click **OK**. The device state changes to **Active**.

Customer Center shows pending state changes next to current device states. The next time a device for which you set the status to unlocked or active contacts the Monitoring Center, the device unlocks.

Preparing Intel AT Equipped Devices for Service

If you need to send an Intel® AT equipped device for service, do one of the following:

➢ Set the **Default Timer Action** to **Do Nothing**. See “Setting a Default Timer Action” on page 149 for more information.

Or

➢ Turn AT off for the device to ensure the state is **Inactive**. See “Turning AT On or Off” on page 160 for more information.

NOTE The **Do Nothing** option is not available on first generation AT devices. If the **Do Nothing** option is not available, simply turn off AT for the device.

IMPORTANT Turning AT off or changing the Default Timer Action does not compromise the security of your devices. Your devices can still be tracked, reported as stolen, and remotely locked in the even of theft. However, we recommend that you reconfigure your Intel AT equipped devices after service.

Chapter 7 Theft Reporting

When you determine that one of your devices is lost or stolen, you can use Customer Center to report the theft to Absolute Software.

IMPORTANT Theft recovery services are included with the Computrace®Plus, Computrace®Complete, and Computrace®One services only. Theft recovery services are **not** supported on Windows Mobile devices. Deactivating a lost or stolen device using Intel® Anti-theft Technology is independent of reporting a lost or stolen device to Absolute Software for recovery. See "Using Intel Anti-Theft Technology" on page 144 for full details.

Viewing Existing Theft Reports

To view existing theft reports:

1. Click the **Theft Report** link on the global navigation bar. The Theft Report page opens.
2. Click the **Theft Report Summary** link on the global navigation bar or the Theft Report page.
3. For each reported theft associated with your account, the page lists the following information:
   - **Report ID #** — a unique ID number created by the system. Click the ID number to review the details of the specific report.
   - **Identifier**
   - **Date Of Theft**
   - **Date Reported**
   - **Location**
   - **City, State, and Country**
   - **Make, Model, and Serial**
   - **Device Status** — the device's theft report status
   - **Guarantee Status**

NOTE If no thefts are recorded, the page shows the message "`No records found.`"

Filtering the List of Theft Reports

By default, the **Theft Report Summary** page lists all reports made by your organization.

You can use the following criteria to filter devices included in the Theft Report Summary:

- Group
- Keyword
- Date
- Theft Report File Status.
  - **Active**
    - **Under Investigation: Researching** — the Recovery Team is actively analyzing the Theft Report.
    - **Under Review: First Contact Received** — the device has initiated an Agent call to the Absolute Monitoring Center for the first time after being reported stolen.
    - **Awaiting Customer: Device Connecting Internally** — the Agent calls originating from the device are from within the internal customer network, and the Recovery Team is anticipating a request to close the Theft Report without need for further processing.
    - **Awaiting Customer: Require Information** — the Recovery Team needs further information or details from the customer to process the Theft Report.
  - **Monitoring**
    - **Awaiting Device Movement** — the Recovery Team is monitoring the location of the device with geolocation tracking.
    - **Awaiting 1st Post Theft Contact** — the Agent on the stolen device has not initiated any calls with the Absolute Monitoring Center after being reported stolen.
    - **Pending New Leads** — Information received from the stolen device is minimal and insufficient to pursue recovery. The Recovery Team will continue to monitor the file for more information that can lead to a successful recovery.
    - **Awaiting Further Device Contact** — the number of Agent calls from the stolen device are not sufficient to enable definitive recovery action, and the Recovery Team is monitoring the device for further Agent calls.
    - **Police Unable to Pursue** — the device is calling in or is located in an area where the law enforcement agency is unable to pursue the investigation further.

    - **Closed**
        - **Recovered** — the device is recovered, and the Theft Report is closed.
        - **Police Recovered** — the law enforcement agency recovered the device.
        - **Customer Requested Closure** — the customer requested closing the Theft Report.
        - **Perpetual Delete Deployed by Customer** — the customer has set a perpetual Data Delete request on the stolen device, which invalidates the Service Guarantee and halts the recovery process.
        - **Software not Installed** — the Agent is not installed on the stolen device making tracking and recovery impossible.
        - **Retrieved-Not Stolen** — the device was recovered internally, or returned after being found.
        - **Canceled** — the Theft Report was canceled.
        - **Incomplete Theft Report** — the information available in the Theft Report is insufficient to allow pursuing recovery.
        - **No Post Theft Contact** — the Agent on the stolen device has not called in to the Absolute Monitoring Center, making recovery impossible.
        - **Other** — the Theft Report was closed for a reason other than the previously defined reasons.
- Guarantee Payment Status
    - **Paid** where the service guarantee was fulfilled by paying out the value of the stolen device.
    - **Declined** where the service guarantee payment was not paid out.
    - **Eligible** where the stolen device and the customer is eligible for a service guarantee fulfillment, but the value has not been paid out.
    - **N/A** where the service guarantee is not applicable.
- Report ID

To filter the list of Theft Reports:

➢ Set appropriate filter criteria, and then click **Show Results**.

Editing Existing Theft Reports

To review and edit the information in an existing theft report:

1. On the **Theft Report Summary** page, click the **Report ID #** link for the appropriate report. A read-only version of the **Create and Edit Theft Report** page for the selected report opens.
2. To update the report, click **Update**, located at the top or bottom of the page. A modifiable version of the **Create and Edit Theft Report** page for the selected report opens.
3. Edit the information you need to change, and then click **Save**. A confirmation page shows, indicating that the report was updated and a copy of the updated report is sent to you by e-mail.

   NOTE If you make an error and want to cancel any changes you have made to the reports, click **Cancel**. the **Theft Report Summary** page opens.

4. Click the **Back to Report Listing** link to return to the **Theft Report Summary** page.

Making a New Report

To report a missing or stolen Agent equipped device:

1. Click the **Theft Report** link on the global navigation bar. The Theft Report page opens.
2. Click the **Create and Edit Theft Report** link on the global navigation bar. The Create and Edit Theft Report page opens.

   NOTE You can also create a new Theft Report from the Theft Report Summary page. Click **Create Theft Report**. The Create and Edit Theft Report page opens.

3. Select a value from a list of all detected identifiers, click **Choose**. The Choose page opens. For more information on the **Choose** feature, see "Using the Choose Feature" on page 92.

   NOTE If you know the identifier for the stolen device, you can enter the value in the **Choose Device** field.

4. To select the device that was lost or stolen, click the appropriate record. You are returned to the **Create and Edit Theft Report** page. Depending upon the device selected, some of the information is pre-populated in the theft report.
5. Enter all available details. Required fields are indicated with an asterisk (*). The greater the accuracy and detail of the information you provide, the greater the likelihood that the police are able to help facilitate a recovery. Once you have completed entering information in the report, click **Send this Report**. The Report Validation page opens.

6. Review your information to make sure that the report is correct, and then click **This Report is Correct**.

   NOTE If you need to make further changes, click **Edit this report**. The Create and Edit Theft Report page opens. Make the necessary changes and click **Send this Report**.

7. The confirmation page opens, listing the file number of the theft report. From the confirmation page, you can:
   - Click the **file number** link to open the report you have just completed.
   - Click the **Reports Made** link to go to the list of theft reports for your organization.
   - Click **Make Another Report** to create a new report.

Cloning an Existing Report

You can clone an existing theft report and assign it to a different Identifier. This is useful in the unfortunate circumstances when multiple devices are stolen at the same time, from the same location. Rather than re-typing the details of the theft for each device, you can clone the report and assign the new report to a different Identifier. Customer Center automatically assigns a new Report ID to the cloned report.

To clone an existing report:

1. From the **Theft Report Summary** page, search for the appropriate Theft Report.
2. For the appropriate report, click the **Clone** link showing in the last column of the results grid. The **Create and Edit a Theft Report** page opens. All fields except the Identifier are populated with the information from the selected report.
3. Select a value from a list of all detected identifiers, click **Choose**. The Choose page opens. For more information on the **Choose** feature, see "Using the Choose Feature" on page 92.

   NOTE If you know the identifier for the stolen device, you can enter the value in the **Choose Device** field.

4. To select the device that was lost or stolen, click the appropriate record. You are returned to the **Create and Edit Theft Report** page. Depending upon the device selected, some of the information in the theft report pre-populated.
5. Enter all available details. Required fields are indicated with an asterisk (*). The greater the accuracy and detail of the information you provide, the greater the likelihood that the police are able to help facilitate a

recovery. Once you have completed entering information in the report, click **Send this Report**. The Report Validation page opens.

6. Review your information to make sure that the report is correct, and then click **This Report is Correct**.

   NOTE If you need to make further changes, click **Edit this Report**. The Create and Edit Theft Report page opens. Make the necessary changes and click **Send this Report**.

7. The confirmation page opens, listing the file number of the theft report. From the confirmation page, you can:

   - Click the **file number** link to open the report you have just completed.
   - Click the **Reports Made** link to go to the list of theft reports for your organization.
   - Click **Make Another Report** to create a new report.

Chapter 8 Using Data Delete

Data Delete allows pre-authorized Customer Center users to delete some or all of the hard drive data on a remote device. Data Delete is available for:

- Computers running Windows NT/2000/XP/Vista operating systems
- Macintosh OSX devices running System 10.3 or higher
- Windows Mobile devices running Windows Mobile 5.0 or Windows Mobile 6, including both Smartphones and Pocket PCs.
- Mobile handsets running S60 3rd edition and later releases such as FP1, FP2, and 5th edition.
- Blackberry 4.2.1 and later

IMPORTANT For all S60 mobile handsets, if you synchronize your handset following a Data Delete operation, the synchronized data on your computer is also deleted. For example, if a Data Delete command removes a user's contacts, any subsequent synchronization operation removes these contacts from the PIM provider such as Microsoft Outlook or Lotus Notes. Before executing a Data Delete operation on your handset, back up all sensitive data that can be accidentally deleted upon any subsequent Nokia PC Suite Sync operations.

The Agent installed on the client device must be an 800 series Agent.

Deletion Algorithms

The Data Delete service uses different deletion algorithms for different types of devices and operating systems. The algorithm used on Windows computers far exceeds the recommendations documented by the United States National Institute of Standards and Technology. For further details, see *NIST Special Publication 800-88: Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology*, referenced at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

The algorithm used on Windows Mobile devices meets all the guidelines except for resetting the phone to its factory default settings.

On all operating systems, data cannot be recovered once deleted, even using forensic software and data remanence analysis tools.

Deletion Logs

When a Data Delete operation completes, a log file can be viewed from within Customer Center. This log file displays all of the files that have been deleted, confirming that all sensitive data was removed, and helping companies comply with data protection regulations.

IMPORTANT If you use a Data Delete policy file that specifies **no boot without log file** (Windows devices only), no log file is available for viewing.

NOTE Data Delete is available with the Computrace®Plus, Computrace®Complete. Computrace® Data Protection, Computrace®One, and Computrace®Mobile services only.

Requesting a Data Delete Operation

NOTE The following instructions assume you have already signed and delivered the Security Administrator Pre-Authorization form to Absolute Software and selected your Authorization Method.

To initiate data delete:

1. Log in to Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Data Delete** link. The Data Delete page opens.
4. Click the **Request Data Delete** link. The Request Data Delete page opens. All fields except the **Identifier** field and **Choose** button are greyed out.
5. Use the **Choose** feature to specify the target device for the Data Delete operation. To select a device using the Choose feature:
   - Click the **Choose** button. The Choose dialog opens to display a list of all devices in your account.

- Click the **Identifier** of the desired device. The Choose dialog closes and the Request Data Delete page refreshes listing details of the selected device.

IMPORTANT If you initiate Data Delete on a machine with a Device Freeze request in the **Freeze Requested** state, the Data Delete request implements before the Device Freeze request. The Device Freeze request status changes to **Pending** until the Data Delete Request is complete.

However, you cannot request Data Delete on a device that is already frozen. You must unfreeze the device before requesting Data Delete.

IMPORTANT You cannot choose a device that already has an outstanding Remote File Retrieval request. You must either cancel the outstanding Remote File Retrieval request or wait for the request to complete. See Using Remote File Retrieval for more information.

6. In the **Reason for Data Delete Request** list, select one of the following values and then continue to step 7:
   - **Stolen** — for stolen devices. For stolen devices, a Theft Report is mandatory. If a Theft Report is not available for the specified device, a warning message appears prompting you to create a Theft Report before continuing.
     Selecting **Stolen** as the reason displays the Date of Theft as a read-only value based on information available in the Theft Report.
   - **Missing** — for devices that are lost but not stolen.
     Selecting **Missing** as the reason displays a field allowing you to enter a Date of Loss for the device. Enter a Date of Loss to continue.
   - **Other** — for devices that are nearing the end of their lease, retiring, or are being taken out of commission for any other reason.
7. In the **Data Delete Policy** section, select the desired Data Delete policy that should drive the Data Delete operation and then continue to step 8. Possible values are:

- **All Files Except OS** deletes all files on the device, with the exception of the operating system. Once the delete operation is completed, a results log is sent to the Monitoring Center.

  NOTE When you select the All Files Except OS option, Windows folder and the root folder (usually C:\) are not deleted. All other files and folders are deleted. In addition, Data Delete searches for and deletes any files in the Windows folder and the root with the following extensions: `"doc", "xls", "ppt", "pdf", "mdb", "vsd", "mpp", "txt", "pst", "ost", "msg", "csv", "xml", "htm", "html", "gif", "jpg", "jpeg", "tif", "tiff", "zip", "rtf", "bak", "dot", "bmp"`

- **All Files Including OS** deletes all files on the target device, including the operating system. The Data Delete operation is executed in two phases. In phase one, all user files are deleted, and a results log is sent to the Monitoring Center. In phase two, all system files excluding the Windows directory and the system root are deleted. No results log is created during phase two, as the operating system is destroyed, and it is not possible to upload the log file. All special settings and/or software components such as Antivirus software, encryption software, or special proxy settings are deleted in phase two, which might, occasionally result in a premature reboot or an incomplete Data Delete. For best results, it is recommended that you create a custom deletion policy that emulates **All Files Including OS** that keeps files necessary for completing the Data Delete process intact. See "Creating a Deletion Policy" on page 184 for instructions on creating a deletion policy.

  NOTE It is not possible to delete the Operating System on Windows Mobile devices. Operating System files on Windows Mobile devices are stored in non-volatile ROM that cannot be deleted. If you select **All Files Including OS** during a Data Delete operation targeting a Windows Mobile device, all files in the **\Windows** folder not stored in ROM are deleted, but the Operating System itself is not removed.

- **Custom Policy** allows you to specify a customized Data Delete policy. Specify the custom Data Delete policy using one of the following methods and then continue to step 8. one of the following methods:

  - Select the desired value in the list appearing next to the **Custom Policy** option button.
  - Create a new policy to meet your specific needs. Click the **Create a Policy** link. The Create and Edit Data Delete Policies page opens. See "Creating a Deletion Policy" on page 184 for instructions on creating a deletion policy.

8. In the **Data Delete Options** section, select the desired option in the **Number of Data Overwrites** list. The Data Overwrite feature deletes the specified data and overwrites it with random or garbage data to make the original data impossible to recover. The overwrite process is called a "data wipe". Possible data wipe values are:

   - **1 Data Overwrite** wipes the data once. The process is the fastest and offers the lowest level of security.
   - **3 Data Overwrites** wipes the data three times. The process is slower than the process for 1 data wipe and offers a higher level of security.
   - **7 Data Overwrites** is the default value for the **Number of Data Overwrites** list. The process is the slowest and offers the highest level of security.

9. If desired, select the **Perpetual Deletion** option. Perpetual Deletion allows Data Delete to re-initialize on the targeted device should the Agent on the device make a call to the Monitoring Center after the deletion cycle has completed.

   IMPORTANT Selecting a Data Delete against a device for which there is an open theft report results in the closure of that theft report, as Perpetual Deletion removes and/or prevents collection of forensic evidence required to recover the device.

   NOTE **Perpetual Deletion** is only supported on Windows computers and Windows Mobile devices. On Windows Mobile devices, Perpetual Deletion is not dependent on a call to the Monitoring Center. Once Perpetual Deletion is initialized on a Windows Mobile device, deletion restarts automatically every twelve (12) hours.

10. If desired, select the **Include File Date Attributes in the Data Delete Log** option to specify Data Delete Attributes. Selecting this option includes the Created, Modified, and Accessed dates in the Data Delete log file.

    By default, the **Created** and **Modified** dates appear in the log file for Windows Vista devices, and the **Created**, **Modified,** and **Accessed** dates appear for Windows XP devices. See "Deletion Log Files" on page 192 for more information on setting the file date attribute parameters for Windows devices.

    NOTE File Date Attribute reporting is only supported on Windows computers.

    IMPORTANT Including file date attributes increases the size of the data delete log file. If the log file is large and the target machine has a low-bandwidth Internet connection, data delete completion may be delayed while the client device repeatedly attempts to upload the log file to Customer Center.

11. In the Data Delete Validation section, if desired, select the **Ignore hard drive serial number check** box. Selecting the box allows Data Delete to override the Hard Disk Serial Number (HDSN) check and continue even when the Hard Disk serial number is unknown or changes during the lifecycle of the request.

    IMPORTANT Use the Ignore HDSN check feature with care. A Data Delete operation deletes data on the target device. Overriding the HDSN check before performing a Data Delete operation may delete data created or owned by any post-loss possessors of the device.

    NOTE If no hard drive serial number is detected for the target device, the **Ignore hard drive serial number check** box is selected by default. To continue, do not change the default value.

12. Read the Data Delete Authorization Agreement carefully and select the **I accept the agreement** box to indicate you have read the agreement and accept the terms.
13. Click the **Set Data Delete** button. The Confirm Data Delete Request page opens.
14. Review the information, and then click the **Submit** button. The Request Authentication page opens.
15. Enter your Customer Center password and the RSA SecurID® Token Code or Security Authorization Code.
16. Click the **OK** button.

    IMPORTANT Once you have clicked the **OK** button on the Request Authorization page, the Delete Request cannot be modified. However, it can be cancelled, provided the request has not been launched on the target device. See "Cancelling a Data Delete Request" on page 191.

    NOTE To save your draft without launching the data delete operation, click the **Save Draft** button. Type your Customer Center Password and RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. To cancel the data delete request, click the **Cancel** button.

    IMPORTANT Only draft requests can be deleted. Submitted requests can be cancelled from the Data Delete Details page, provided the request has not been launched on the target device. See "Cancelling a Data Delete Request" on page 191. Once a delete request is launched, it cannot be cancelled, nor can the request be edited.

17. If the device is RTT and Intel AT enabled, a dialog box prompting you to force a call to the device using MCIC opens. If desired, force a call to the device. See "Initiating a Forced Call" on page 67 for more information. Once the device receives and processes the SMS message, depending

upon the Data Delete settings specified for the account, the data delete request runs. See step 18 for more details on the data delete operation.

18. Once initiated, the Data Delete operation runs on the next Agent call, even if the user does not log in to the OS. Once the Data Delete process has begun, it cannot be stopped. If the Data Delete operation is interrupted by a system restart, Data Delete restarts only when the Windows or OS Login Screen appears.

    IMPORTANT In some cases, if the hard drive serial number option is not selected, the Data Delete operation may fail because the Agent believes that the target device is different from the desired device. If the Data Delete operation fails in such cases, Customer Center sends a notification e-mail to the Security Administrator who requested the Data Delete operation.

Deletion Policies

In addition to the pre-defined options of:

- all files except the operating system
- all files including the operating system

Data Delete can be customized to delete specific sets of files and folders specified by the Security Administrator. A Deletion Policy is a user created list of file and folder locations. When Data Delete is invoked, all files on the target device in the specified locations are deleted. Deletion Policies can only be created by Security Administrators.

Deletion Policies are only available for Windows computers. Mac users are limited to using the default policies of all files including or all files excluding the operating system.

Refer to the **Data Delete FAQs** in the in Customer Center Documentation repository for some sample policy file entries.

Creating a Deletion Policy

To create a Deletion Policy:

1. Log into Customer Center as an administrator with Security administration privileges.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

3. Click the **Data Delete** link. The Data Delete home page opens.

4. Click the **Create and Edit Data Delete Policies** link. The Create and Edit Data Delete Policies page opens.
5. Enter a name for your deletion policy in the **Policy Name** text box.

   NOTE Data Delete Policies must have unique names.

6. Enter a brief description for your deletion policy in the **Description** text box.
7. Define all files and directories to be deleted. Customer Center includes a number of predefined file and directory entries. Additionally, Security Administrators can define their own unique file and folder entries. A single Deletion Policy may include any combination of predefined and user-defined entries.
8. To add predefined entries:

   a) Click the **Pre-defined Data Deletes** tab.

   b) Select the desired files and directories in the **Available Data Delete Functions** list, and then click the **Add** button. The selected items move to the **Selected Data Deletes** list on the right.

   c) Repeat this process to add additional predefined entries to the policy.

   d) To remove any entries from the **Selected Data Deletes** table click the **Remove** button.

9. To define and add unique entries:

   a) Click the **Custom Data Deletes** tab.

   b) Enter an entry for each file or folder to be deleted into the text box provided, following the standard Windows file path convention.

   NOTE The `*` wildcard is supported. When specifying a folder, be sure to include the trailing backslash after the folder name (e.g.— `c:\temp\`). All files in the main folder and all files and subfolders are deleted. The root directory is retained, empty.

   c) Click the **Add** button to move each entry into the **Selected Data Deletes** list on the right.

   d) Repeat this process to define all desired entries.

   e) To remove any entries from the **Selected Data Deletes** table click the **Remove** button.

10. Once you have defined all desired descriptions, click the appropriate button at the bottom of the page:

    ○ **To save the policy** — click the **Save** button.

    ○ **To delete the policy** — click the **Delete** button.

- ○ **To copy the policy** — click the **Copy** button. The **View Data Delete Policies** page opens with the new copy of the policy named **Copy of %original policy name%**. This feature is useful if you want to create a Deletion Policy which is similar to the currently displayed one. First copy the original and then click the appropriate **View** link and make any desired changes. See "Editing a Deletion Policy" on page 186.

Editing a Deletion Policy

The process for modifying a Deletion Policy is identical to the creation process. The exception is that you are editing an existing policy, rather than defining a new one. Deletion Policies can only be edited by authorized Security Administrators.

NOTE A Deletion Policy cannot be modified if it is associated with an active Data Delete request.

To edit an existing Deletion Policy:

1. Log into Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

3. Click the **Data Delete** link on the global navigation bar. The Data Delete home page opens.
4. Click the **View and Manage Data Delete Policies** link. The View Data Delete Policies page opens, listing all currently defined Deletion Policies.
5. Click the **View** link of the Deletion Policy you want to modify. The Create and Edit Data Delete Policies page opens to display the current configuration of the selected Deletion Policy.
6. If you want to change the name of the policy, enter the new name for the policy in the **Policy Name** text box.

   NOTE Data Delete Policies must have unique names.

7. Make any desired changes to the Deletion Policy, and then click the **Save** button.

Deletion Policies on Windows Mobile Devices

Windows Mobile devices do not have drives identified by drive letter. When applying a Deletion Policy to Windows Mobile device, the drive letter components of all Deletion Policy entries are ignored. For example, a Deletion

Policy entry of `C:\Temp\*.txt` is executed as `\Temp\*.txt` on the Windows Mobile device.

The standard file system on Windows Mobile devices is also organized somewhat differently than the standard file system on Windows computers. As a result, if you have existing Deletion Policies which reference standard file locations on a Windows computer, they do not work as expected on a Windows Mobile device. For example, the location of the `'My Documents'` folder on a Windows Mobile devices is different than on a Windows computer. As a result, you may need to update your existing Deletion Policies or create specific Deletion Policies for Windows Mobile devices.

Tracking Data Delete Status

Customer Center provides real-time status updates on the progress of Data Delete requests. Additionally, upon successful completion of a Data Delete cycle, the Customer Center stores a Deletion Log listing all files and folders which were deleted.

Viewing Data Delete Status

The Data Delete Summary Report page lists all devices that have had Data Delete requested. For each device listed, the Data Delete Summary Report page includes the following information:

- **Identifier** — the target device's Identifier
- **Make** — the target device's make
- **Model** — the target device's model
- **Serial #** — the target device's serial number
- **Requested** — the date and time when the Data Delete was requested
- **Status** — the current status of the Data Delete request. Possible values are:
    - `Requested` — The request has been submitted and is in a transitory state while the Data Delete instructions are setup. Data Delete requests only stay in state for a short period of time.
    - `Set, Awaiting Call` — The Monitoring Center has been configured to send the Data Delete instructions to the target device on its next call.
    - `Launched` — The Data Delete instructions have been sent to the target device.
    - `Completed, Log File Uploaded` — Data Delete has completed on the target device and the Agent has sent a log file containing details of the Data Delete operation to the Monitoring Center.

  - `Completed, Attempting to Upload Log File (If Applicable)` — Data Delete has completed on the target device and the Agent is unable to send the log file to the Monitoring Center. If specified for your account or the device, the Agent continues to initiate calls to the Monitoring Center until the log file is uploaded to the Monitoring Center.
  - `Cancelled` — The Data Delete request has been cancelled.
  - `Failed` — The Data Delete request failed to execute on the target device. Contact Customer Support. See "Technical Support" on page 15.
  - `Draft` — The Data Delete request has only been saved as a draft and has not been initiated.
  - `Cleared` — The target device has been recovered prior to the execution of Data Delete. Absolute's recovery team has cancelled the request
- **Reason** — the reason of the Data Delete request. Possible values are:
  - `Retiring` — The device is being retired
  - `End of Lease` — The device is at the end of its lease
  - `Lost/stolen` — The device is either lost or stolen
  - `Other` — All other reasons for the Data Delete request

To view the status of a Data Delete request:

1. Log into Customer Center as a Security Administrator.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Data Delete** link. The Data Delete page opens.
4. Click the **Data Delete Summary Report** link. The Data Delete Summary Report page opens.
5. Set the desired filtering and display options for the results using the following criteria:
   - **Filter results by device group** — Select the desired device group from the **Group** list.
   - **Filter results by specific Identifier, Assigned Username, Make, Model, or Serial Number** — Select the value type from the **Field** list, and then enter the value to search for in the **is or contains** text box or use the **Choose** feature. For more information on the **Choose** feature, see "Using the Choose Feature" on page 92.
   - **Filter by status** — Select one or more boxes in the **Data Delete Status** list.

- **Filter by reason** — Select one or more boxes in the **Data Delete Reason** list.

6. Click the **Show Results** button to regenerate the report using specified criteria.

Data Delete Details Page

The Data Delete Details page displays the setup information for each Data Delete request. The Data Delete Details page also provides a link to the Deletion Log file once the delete operation has completed. See "Deletion Log Files" on page 192.

To open the Data Delete Details page:

➢ Click the appropriate **View** link on the Data Delete Summary Report page. The Data Delete Details page opens, listing the following information:

- **Reason** — reason specified at creation detailing why the Data Delete operation was initiated.
- **Identifier** — the target device’s Identifier
- **Make** — the target device’s make
- **Model** — the target device’s model
- **Serial #** — the target device’s serial number
- **Asset #** — the asset number of the target device
- **Last Call** — the date and time of the target device’s last call to the Monitoring Center
- **Perpetual Deletion** — displays a Yes or No value, depending on whether perpetual deletion was applied
- **Data Overwrites** — displays the number of data wipes selected. Possible values are 1, 3, or 7.
- **Data Delete Type** — displays the delete options configured for the request. There are three possible values:
  - `All Files Including OS`
  - `All Files Excluding OS`
  - `Specific Files/Directories` — This indicates a Deletion Policy has been selected. In this circumstance, the name of the policy is listed along with a list of all files and folders specified in the policy
- **Include Field Date Attributes in the Data Delete log** — indicates whether the file date attributes are included in the data delete log
- **Agreement Accepted** — indicates whether the **I Accept the agreement** box was selected when the request was prepared

- **Requestor Name** — displays the name of the Security Administrator who submitted the request
- **Requestor Phone Number** — the phone number of the Security Administrator who submitted the request
- **Requestor E-mail** — E-mail address of the Security Administrator who submitted the request
- **Requestor User Login** — the Customer Center User ID of the Security Administrator who submitted the request
- **Data Delete Status Table** — displays information on the status of the delete request and includes the date and time when each status was achieved.

Removing Details of a Data Delete Operation

In certain circumstances, you may no longer need to save the details of a particular Data Delete Request in Customer Center. Some examples are when a Data Delete Request was cancelled, completed, or the device recovered successfully. You can remove the details of such a Data Delete operation from Customer Center.

IMPORTANT Exercise caution in removing the details of a Data Delete operation, once you have removed the details of a Data Delete operation, the details cannot be restored.

To remove details of a Data Delete operation:

1. On the Data Delete Summary Report page, click the **View** link of the Data Delete operation for which you want to remove details. The Data Delete Details page opens.

   NOTE If you have not done so already, it is strongly recommended that you download the log file first before removing these Data Delete details.

2. Click the **Remove Details** button. A confirmation message is displayed.
3. Click the **OK** button to remove the details of the Data Delete operation.

Forcing a Data Delete Operation to Complete

You cannot launch a second Data Delete operation on a specific device if there is an existing process underway. If a Data Delete operation fails to complete, you can force it to complete. This sets the status of the Data Delete operation in the database to `Complete`, and allows you to start a new Data Delete operation. It does not affect any processes currently running on any client machines, and it does not abort any Data Delete operations currently in progress. Once you have forced a Data Delete operation to complete, you are not able to undo the status change.

To force a Data Delete operation to complete:

1. On the Data Delete Summary Report page, click the **View** link of the Data Delete operation you want to force to completion. The Data Delete Details page opens.
2. Click the **Complete Request** button. A confirmation message is displayed.
3. Click the **OK** button to complete the Data Delete operation.

Clearing Perpetual Data Delete

If a Data Delete request was submitted with the Perpetual Deletion option, you can stop the Perpetual Data Delete on a target device.

IMPORTANT Perpetual Data Delete can be stopped only after the initial deletion cycle has completed.

To clear Perpetual Data Delete:

1. On the Data Delete Summary Report page, click the **View** link of the Data Delete operation that was requested with the Perpetual Deletion option.
2. Click the **Clear Perpetual Data Delete Flag** button. A confirmation message is displayed.
3. Click the **OK** button to clear Perpetual Data Delete for the Data Delete request.

Cancelling a Data Delete Request

Provided Data Delete has not been launched on the target device, a Data Delete request can be either deleted or cancelled, depending on its status. If the request’s status is `Draft`, it can be deleted. If the status is `Requested` or `Set Awaiting Call`, the request cannot be deleted but may be cancelled.

To delete a draft request:

1. On the Data Delete Summary Report page, click the **View** link for the draft Data Delete operation.
2. Review the details of the draft to ensure this is the one you want to delete.
3. Scroll to the bottom of the page and click the **Delete** button. A confirmation message is displayed.
4. Click the **OK** button to confirm the delete operation.

To cancel a request:

1. On the Data Delete Summary page, click the **view** link for the desired Data Delete operation.
2. Review the details of the request to ensure this is the one you want to cancel.
3. Click the **Cancel Request** button to cancel the Data Delete request. A confirmation message is displayed.
4. Click the **OK** button to confirm the cancellation.

Deletion Log Files

Once a Data Delete request has been completed, a Deletion Log file is uploaded to the Customer Center and made available via the Data Delete Details page. A Deletion Log file is a plain text file which provides details on what was deleted from the targeted device. Deletion Log Files include the following information about the data delete operation:

- **Completion Date** — the date and time when the delete request completed on the target device
- **Data Delete Type** — indicates the deletion type. Possible values are:
  - `All Files Except OS`
  - `All Files Including OS`
  - `Specific Files/Directories` (Windows computers only)
- **Identifier** — the Identifier of the target device
- **Model** — the target device's model
- **Make** — the target device's make
- **Serial Number** — the target device's serial number
- **Asset Tag** — the target device's asset tag (this is an optional user defined tracking number)
- **Device Name** — the target device's network name
- **Started** — the date and time when Data Delete began executing on the target device
- **Deleted File List** — the full path of all deleted files
- **Finished** — the date and time when the Data Delete process was completed
- **Data Overwrites** — the number of data wipes performed.

- **File List** — a list of all files deleted in the operation. The file date attributes (**Created**, **Modified,** and **Accessed**) for each file are also listed, if this setting has been selected, in tab-delimited format.

  IMPORTANT In a post-theft scenario, the **Accessed** date for a file may be later than the date of theft. The Accessed date is not necessarily indicative of a file which has been compromised post-theft. Undetected malware, antivirus and spyware scans, automated backup and other similar applications may all trigger an **Accessed** date change, indicating when the file was last accessed. As a result, this value should be considered useful for determining whether a file has definitively not been accessed, but not the converse.

- e-mail Accounts — (Android phones only) a list of all the e-mail accounts deleted from the mobile device during the Data Delete operation.

Viewing the Deletion Log File

Once the Data Delete request has completed, the **View Deletion Log** button becomes available, allowing you to download and view the results of the Data Delete operation.

To download and view the log file:

1. On the Data Delete Summary Report page, click the **View** link for the desired Data Delete operation. The Data Delete Details page opens.
2. Click the **View Deletion Log** button. The **File Download** dialog is displayed.
3. Click **Open** to open the log file, **Save** to save the file to your local device, or **Cancel** to cancel the operation.

The log file is in a text format and can be viewed using any text file editor.

Enabling Accessed Date Logging in Windows Vista

When you create a data delete request, you can choose to list the **Created**, **Modified,** and **Accessed** file date attributes for each file deleted. If this setting is enabled, the log file displays the date attributes next to the name of each deleted file. By default, the log file displays the **Created** and **Modified** dates for devices running Windows Vista or higher, and the **Created**. **Modified,** and **Accessed** dates for Windows XP devices. The list of files and their attributes is in a tab-delimited format, suitable for export into Microsoft Excel or other applications.

In the registry of all devices running Windows Vista or higher, **Accessed Date** logging is turned off by default. When the setting is turned off, the **Accessed Date** value is not written to the Data Delete log file.

This setting is controlled by the following registry key:

- Key: **NtfsDisableLastAccessUpdate**
- Path: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem**

To enable Accessed Date logging on a Windows Vista device:

1. Open the Windows registry.
2. Navigate to the **NtfsDisableLastAccessUpdate** registry key.
3. Set the value of the key to **0** (zero).

NOTE Enabling **Last Accessed Date** logging in devices running Windows Vista or higher may slow down the performance of your device.

The **NtfsDisableLastAccessUpdate** registry key does not exist on Windows XP devices. By default, Windows XP always logs the **Accessed Date**. However, it is possible to add this key to the registry of a Windows XP device, and set the key value to **1** to disable **Accessed Date** logging. If **Accessed Date** logging is turned off on a Windows XP device, the log file still displays the **Accessed** column in the log file, but the date shown is the last date on which the file was accessed before the **NtfsDisableLastAccessUpdate** registry key was set. See "Requesting a Data Delete Operation" on page 179 for more information.

Chapter 9 Managing Geofences

The Geofences feature in Customer Center allows administrators to specify boundaries based on Geolocation Tracking data and allow device tracking. Absolute Software's Geolocation Tracking and Geofences features allow your organization to more precisely and immediately determine the physical location of a specific computing device as of the most recent Agent call to the Monitoring Center. It is also assumed that the device is properly equipped with a positioning device approved for use with these features.

An administrator can specify boundaries using the Geofences editor and track the movement of devices through these locations. Whenever a device crosses the boundary set using Geofences, alerts are triggered in Customer Center and, depending upon the settings specified for the account, result in e-mail notifications to administrators and/or other events on Customer Center. Geofencing is available to all accounts authorized for the Geolocation Tracking feature. Further, Geofencing is supported for all Agents (devices) in that account for which Geolocation Tracking data is available.

Geofencing Security

Due to the sensitive nature of the Geolocation Tracking and Geofencing features, several security checks are implemented to ensure the service is only initiated by authorized individuals and that it only runs on correctly targeted devices:

1. Absolute Software must have a signed pre-authorization agreement on file for your company.
2. The device to be assigned to a Geofence area must have an activated Agent with a unique Identifier and valid Geolocation Tracking data.

Before Geolocation Tracking or Geofences are available to you, you must submit an Authorization form authorizing the use of Geolocation Tracking for devices in your account.

Geolocation Tracking Authorization Agreement

In order to use the Geolocation Tracking and Geofences features, Absolute Software must have a signed authorization agreement for your company on file. The authorization agreement identifies the signing officers in your company authorized to allow device tracking.

Downloading the Pre-Authorization Agreement

To download a blank copy of the pre-authorization agreement:

1. Login to Customer Center.
2. Click the **Documentation** link on the global navigation bar.

3. In the **Service Request Forms** area, click the **Geolocation Tracking Authorization Form** link.
4. The authorization agreement opens in PDF format. Complete the document, print it, sign it, and return it to Absolute Software:

   Attention: Global Support - Corporate Support Team Lead
   Absolute Software Corporation
   Suite 1600, Four Bentall Center
   1055 Dunsmuir Street PO Box 49211
   Vancouver, British Columbia, Canada
   V7X 1K8

   Fax: (604) 629-7063

Using Geofence Technology

Geofences are primarily used as building blocks of security policies based on the location of devices. Geofences in combination with Geolocation Tracking can be used to pinpoint the location of a device and consequently ensure that the security of these devices is not breached. For example, a Geofence specifying the entire state of New York as a secure zone and an accompanying alert in Customer Center are created for Account A. When one of the devices in Account A travel outside New York state, all administrators for that account are alerted via an automated notification e-mail. Depending upon the location and the secure status of the device, the Administrator can then choose to implement other security measures such as running a Data Delete or locking the device using Intel AT.

To effectively use Geofences, create a Geofence, and then create an alert that links to the Geofence.

When you create an alert associated with a Geofence, you need to specify the rules for triggering the alert based on the following options:

- **Location**
  - **Outside** — Select this option to specify an alert whenever a device travels outside a specified Geofence boundary.
  - **Inside** — Select this option to specify an alert whenever a device travels inside a specified Geofence boundary.
- **Geofence Name** — Select the Geofence to which the alert pertains.
- **Duration** — Specify the length of time after the specified rules are broken required to trigger the alert. You can specify the length of time in hours, days or weeks.

To set up a functioning Geofence:

1. Create an appropriate Geofence using the Create and Edit Geofences page. See "Creating Geofences" on page 198 for more information.

   NOTE If a Geofence matching your criteria already exists, you do not need to create a new one.

2. Create an alert based on the newly created Geofence using the Create and Edit Alerts page. In the **Field** list, select the value **Location**, and then specify the appropriate rules.

For more information on creating Alerts, see "Creating New Alerts" on page 37.

Editing and Navigating Geofence Maps

The Create and Edit Geofences page shows the Geofence Editor. The Geofence Editor is a map that allows you to add, edit or find Geofences.

All Geofences also show on the appropriate Geolocation Tracking reports for your account. For more information about Geolocation Tracking reports, see "Device Location Report" on page 113 and "Device Location History Report" on page 117.

The following tools and buttons can show on a map showing Geofences:

- — Click the up, down, left or right arrow in the **Pan Tool** to move in the respective direction and show different areas of the map.

- — Click the **Zoom In** tool to view more details about a particular area on the map.

- — Click the **Zoom Out** tool to view a greater area on the map with less detail. Geofences too small to show accurately at a zoom level show on the map as small round markers: ●.

- — Click the **Draw a New Boundary** tool, and then click the map to start drawing a new boundary.

- — Click the **Remove Boundary** tool, and then click a boundary on the map to delete.

- — Click the **Box Zoom** tool, and then click and drag your mouse on the map to define an area to view more closely. Alternatively, hold down the CTRL key, and then click and drag the mouse to use the **Box Zoom** tool.

- — Click the **Find Boundaries and Markers** tool to automatically set the map position and zoom to show all defined boundaries on screen. Clicking the tool repeatedly steps through all the available geofence boundaries and markers on the map.

Creating Geofences

The Create and Edit Geofences page allows you to create a new Geofence and edit existing Geofences.

IMPORTANT The following instructions assume that you have already signed and delivered the Geolocation Tracking Authorization Form to Absolute Software. Also, the first time you access any geolocation page in a login session, a confirmation page prompts you to accept the Terms and Conditions of use.

To create Geofences for devices in your account:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **Create and Edit Geofences** link.
3. Enter a name and description for the new Geofence in the **Geofence Name** and **Geofence Description** boxes.
4. To consider only collected device locations that have a high probability of being accurate in relation to the geofence, select **Only test locations with high Confidence Levels against Geofence boundaries** in the **Applicable Confidence Levels** area.
5. In the **Applicable Location Technologies** area, select the types of location data applicable to the geofence. For more details on location technologies that Customer Center can use, see Chapter 5: "Device Location Report" on page 113.

   IMPORTANT Since IP Georesolution is accurate to the city level at best and varies from the city level to country level, do not enable IP Georesolution for small geofences.

6. Create a boundary using the map and tools in the Geofence Editor. To create a boundary:

   a) In the Geofence Editor, use the navigation tools to show the area on the map where you want to create a boundary. For more information about the navigation tools, see "Editing and Navigating Geofence Maps" on page 197.

   b) Click **Draw a New Boundary** in the panel on the left side of the map, and then to define a boundary click the map at each appropriate point to specify the corners of the boundary polygon.

IMPORTANT Boundary lines cannot cross or intersect at points other than end points. For example, a boundary cannot be shaped like a star polygon. For more information about polygon shapes allowed for creating a boundary, see "Valid Polygon Shapes For Geofences" on page 199.

c) To close the polygon and finish defining the boundary, click the starting point of the polygon.

NOTE To compensate for accuracy limitations of Geolocation technology, create larger boundaries than required.

7. Click **Save**. The new Geofence is created and the View and Manage Geofences page opens with the new Geofence shown in the Geofences table.

Valid Polygon Shapes For Geofences

The Geofence Editor allows the use of simple polygons to create boundaries. A simple polygon is a shape without self-intersecting sides, that is a shape whose sides do not cross. You can, however, define a boundary using more than one simple polygons whose lines cross each other. Figure 1 shows a few polygon shapes that cannot be used to create Geofence boundaries.

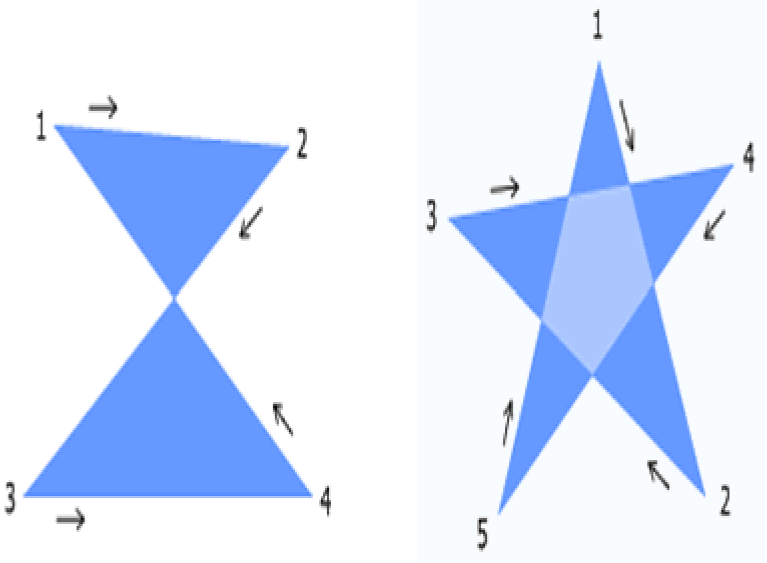

FIGURE 1. Invalid Polygon Shapes For Geofences

Viewing Existing Geofences

The View and Manage Geofences page allows you to view a summary of all Geofences matching specified search criteria.

To view a list of existing Geofences for your account:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the **View and Manage Geofences** link. When prompted, accept the use of the Geolocation Tracking feature. The View and Manage Geofences page opens.
3. In the **Geofence Name** field, enter the complete or a part of the Geofence name that you want to view, and then click **Show Results**. The View and Manage Geofences page refreshes to show a list of all Geofences matching the search criteria in the results grid.
4. Click the **Name** link. The Create and Edit Geofences page for the selected Geofence opens.

Editing Existing Geofences

You can also use the Create and Edit Geofences page to edit existing Geofences. You can perform the following tasks on this page:

- Modify an existing Geofences entry
- Delete an existing Geofences entry

Modifying an Existing Geofences Entry

It is possible to modify the values for an existing Geofence, however Boundaries cannot be modified. To modify a boundary, you must delete it and create a new boundary matching the appropriate criteria using the Geofence Editor.

To modify the values for an existing Geofence:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the View and Manage Geofences link. When prompted, accept the use of the Geolocation Tracking feature. The View and Manage Geofences page opens.
3. In the **Geofence Name** field, enter the complete or a part of the Geofence name that you want to view, and then click **Show Results**.
4. The View and Manage Geofences page refreshes to show a list of all Geofences matching the search criteria in the results grid.
5. Click the **Name** link. The Create and Edit Geofences page for the selected Geofence opens.

6. Edit the appropriate values in the **Geofence Name** and **Geofence Description** boxes.
7. Use the **Geofence Editor** to modify the existing Geofence boundary. For more information about the navigation tools, see "Editing and Navigating Geofence Maps" on page 197.
8. Click **Save**. The Geofence data is updated and the View and Manage Geofences page opens to show the edited values in the results grid.

Deleting an Existing Geofences Entry

To delete an existing Geofences entry:

1. Click the **Administration** link on the global navigation bar. The Administration page opens.
2. Click the View and Manage Geofences link. When prompted, accept the use of the Geolocation Tracking feature. The View and Manage Geofences page opens.
3. In the **Geofence Name** field, enter the complete or a part of the Geofence name that you want to view, and then click **Show Results**.
4. The View and Manage Geofences page refreshes to show a list of all Geofences matching the search criteria in the results grid.
5. Click the **Name** link. The Create and Edit Geofences page for the selected Geofence opens.
6. Click **Delete**. The View and Manage Geofences page opens.

IMPORTANT You cannot delete geofences that have alerts associated.

Chapter 10 Using Device Freeze

The Device Freeze feature allows pre-authorized Customer Center users to target specific devices and show a full screen message restricting users from operating the device. The Device Freeze happens at the operating system (OS) level and when it is in effect it shows a full screen message on the device. When you freeze a device, only the selected message is shown on-screen and no Windows components such as Task Manager are accessible. Windows continues to run in the background and the user is able to switch between Windows by pressing `ALT+TAB` keys to allow saving any open documents or closing any windows open at the time.

The Device Freeze feature is persistent. The frozen state persists on device reboot even when the device is rebooted in safe mode. The freeze simply shows again when the OS reloads. If the user reinstalls the OS, the device freezes again when the Agent self-heals.

Security Administrators can use Customer Center to manage Device Freeze. The following functionality is available in Customer Center:

- Request a Device Freeze
- Unfreeze a frozen device
- Cancel an incomplete Device Freeze request
- Track and monitor Device Freeze request status
- Manage Custom Device Freeze Messages
- Remove details of a completed or canceled Device Freeze request

For Lenovo accounts and devices that are managed under the Lenovo Lost and Found program, the Device Freeze pages allow the following additional functionality:

- Request a Device Freeze and report the device as Lost to Lenovo.
- View the Lenovo Lost and Found status for a managed device.

Minimum System Requirements

Currently, the Device Freeze feature is available for devices that meet the following minimum system requirements:

- **Operating System** — Windows NT, 2000, XP, or Vista
- **Computrace Agent** — Agent Version 8XX series

Requesting a Device Freeze

Security Administrators can launch a Device Freeze request on any device in their account. You need an authorization code to request a Device Freeze. See "Authorization Codes" on page 31 for more information.

When initiated, the Device Freeze operation runs on the next Agent call, even if the user does not log in to the operating system. If a system restart interrupts the Device Freeze operation, the freeze persists on the device on restart and when the operating system loads. When a device is frozen, Security Administrators can either use Customer Center to unfreeze it or generate a Pass Code to allow users to manually unfreeze the device. See "Requesting an Unfreeze Pass Code" on page 209 and "Unfreezing a Frozen Device" on page 210 for more information.

IMPORTANT If you initiate a Device Freeze on a device with an outstanding Data Delete request or initiate a Data Delete Request on a device that has an outstanding Device Freeze request, the Device Freeze request implements after the Data Delete request completes.

Also, you cannot initiate Device Freeze on a stolen device with an open Theft Report. If you choose to implement Device Freeze on a stolen device without a Theft Report, you must unfreeze the device before filing a Theft Report. See your *End User Service Agreement* for more information.

NOTE The following instructions assume you have already signed and delivered the Security Administrator Preauthorization Form to Absolute Software and selected your authentication method. See "Security Administrator Preauthorization Agreement" on page 30 for more information.

To request Device Freeze:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Request Device Freeze** link. The Request Device Freeze page opens.
4. Click **Select Devices** to open the Select Devices dialog box.
5. In the **Device Group** list, select the appropriate Device Group to show a list of devices that you want to freeze.
6. If you want to provide specific details to show devices that meet specific criteria, enter the appropriate information in the **Any Field Includes** field. For example, if you want to show only the devices where the Username field starts with the word "Absolute", enter `Absolute` in the **Any Field Includes** field.

7. Click **Filter**. The Select Devices dialog box refreshes to show a list of devices matching your criteria.
8. Select the appropriate devices by doing one of the following:
   - Select the individual checkboxes for the appropriate devices.
   - To select all the devices shown, select the checkbox in the header. The Select All dialog box opens to ask you whether you want to select all the devices that meet the filter criteria or only the devices shown on the current page. Click **Select All** records or **This Page Only** as appropriate. The Select Devices dialog box opens with the specified devices you have selected.
9. Click **Select Devices**. The Request Device Freeze page opens to show a list of all the devices that you have selected.

   NOTE If you find that the list of selected devices includes devices that were included in error, you can remove these devices from the list. To remove such devices, click the **Remove** link in the last column for the appropriate device. The Request Device Freeze page opens to show the updated list of devices.

10. Select one of the following options:
    - **Generate a different random passcode for each device** to auto-generate and use a different unlock passcode for each of the target devices.
    - **Generate the same random passcode for each device** to auto-generate and use the same unlock passcode for each of the target devices.
    - **Specify a specific 8-digit numeric passcode** for each device to use a previously generated or custom passcode for all the devices.
11. If your target device is running the Windows operating system, you can force the device to reboot when the Device Freeze request is deployed. To force a Windows device to reboot when executing the Device Freeze request, select the **Force Reboot** checkbox.

    By default, devices running Mac operating systems automatically reboot when the Device Freeze request executes. Devices running Windows, however, do not reboot automatically. The user is, thus, able to switch between different application windows and save their work. The Force Reboot option lets you enforce an automatic reboot so that users cannot switch between applications and save their work.
12. Click **Submit**. One of the following options are shown:
    - If the selected device is managed under the Lenovo Lost and Found program, the page shows options that let you report the device as Lost to Lenovo. Follow the instructions available in the section "Device Freeze on Lenovo Devices" on page 205 for more information.

- ○ If the selected device is not a Lenovo device, the Provide Authentication page opens. Continue with step 13 to request the Device Freeze.

13. Enter your Customer Center password and the Authorization Code. See "Authorization Codes" on page 31 for more information.
14. Click **OK**. The Device Freeze request is created and is deployed to the device on the next Agent call.

IMPORTANT After you click **OK** on the Provide Authentication page, the Device Freeze Request cannot be modified. However, it can be canceled, provided the request has not been launched on the target device. See "Canceling a Device Freeze Request" on page 212.

15. If the device is RTT enabled, a dialog box prompting you to force a call to the device using MCIC opens. If necessary, force a call to the device. See "Initiating a Forced Call" on page 67 for more information. When the device receives and processes the SMS message, depending upon the Device Freeze defaults set for the account, the device freezes.

Device Freeze on Lenovo Devices

When you select a device managed under the Lenovo Lost and Found program, the Request Device Freeze page refreshes to show additional options.

IMPORTANT You can only report one or more devices as “Lost” to Lenovo, if all of the devices you are freezing are managed under the Lenovo Lost and Found program. For example, if you are freezing 10 devices, out of which 9 are Lenovo devices and 1 is a Dell device, you cannot report the 9 Lenovo devices as lost and freeze the Dell device at the same time. In such a case, you must create separate Device Freeze requests for the Lenovo and Dell devices.

To complete requesting a Device Freeze for Lenovo Lost and Found devices:

1. On the Request Device Freeze page, select a device managed under the Lenovo Lost and Found program. The page refreshes to show Lenovo specific options.
2. Select one of the following:
   - ○ **Initiate a freeze and report the device as Lost to Lenovo** — flags the device as lost and freezes the device on the next Agent call.
   - ○ **Initiate a freeze on the device** — freezes the device on the next Agent call.
3. Click **Freeze**. The Provide Authentication page opens.
4. Enter your Customer Center password and the Authorization Code. See "Authorization Codes" on page 31 for more information.

5. Click **OK**. The Device Freeze request is created and is deployed to the device on the next Agent call.

   IMPORTANT After you click **OK** on the Provide Authentication page, you cannot modify the Device Freeze Request. However, you can cancel the request, provided the request has not been launched on the target device. See "Canceling a Device Freeze Request" on page 212.

6. If the device is RTT and Intel AT enabled, a dialog box prompting you to force a call to the device using MCIC opens. If necessary, force a call to the device. See "Initiating a Forced Call" on page 67 for more information. After the device receives and processes the SMS message, depending upon the Device Freeze defaults set for the account, the device freezes.

Tracking Device Freeze Status

Customer Center provides near real-time status updates on the progress of Device Freeze requests. The Device Freeze Summary Report page lists all devices that have had Device Freeze requested. For each device listed, the Device Freeze Summary Report page includes the following information:

- **Identifier** — the target device's Identifier
- **Make** — the target device's make
- **Model** — the target device's model
- **Serial #** — the target device's serial number
- **Status** — the current status of the Device Freeze request. Possible values are:
  - `Freeze Requested` — The request has been submitted and is in a transitory state when waiting for an Agent call or when the instruction setup process is running on the target device.
  - `Frozen` — The Device Freeze instructions are sent to the target device and the freeze message shows on the target device.
  - `Unfreeze Requested` — Instructions to unfreeze the frozen device are queued and are sent to the device on the next Agent call. This status is typically set when an unfreeze request is set using Customer Center.
  - `Unfrozen with Agent Call` — The device has been unfrozen by sending an unfreeze request on the next Agent call.
  - `Unfrozen with Passcode` — The end-user has unfrozen the device by entering a Pass Code on the frozen device.

    NOTE Unfreezing via an Agent call is the preferred method for unfreezing a device. If possible, it is recommended that devices be unfrozen by setting the status on Customer Center only.

    - `Request Cancelled` — The Device Freeze request has been canceled.

- **Edit** / **View** link — Depending upon the status of the Device Freeze request, this column shows one of the following two links:
    - **View** — Clicking this link opens the Device Freeze Details page in a read-only state for the selected request. This link shows for Device Freeze requests in an unfrozen or canceled status.
    - **Edit** — Clicking this link opens the Device Freeze Details page in an editable state for the selected request. This link shows for Device Freeze requests in a Freeze Requested status.

Viewing the Device Freeze Request

To view the status and other details for a Device Freeze request:

1. Log in to Customer Center.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. Enter all appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all devices for your account matching the search criteria in the results grid.
5. Click the **Edit** or **View** link for the appropriate device. The Device Freeze Details page opens to show the details for the selected request.

Device Freeze Details for Non-Lenovo Devices

The Device Freeze Details page contains the following detailed information about the Device Freeze request:

- **Current Status** — the current status of the Device Freeze request. Possible values are:
    - `Freeze Requested` — The request has been submitted and is in a transitory state when waiting for an Agent call or when the instruction setup process is running on the target device.
    - `Frozen` — The Device Freeze instructions are sent to the target device and the freeze message is shown on the target device.
    - `Unfreeze Requested` — Instructions to unfreeze the frozen device are queued and are sent to the device on the next Agent call. This status is typically set when an unfreeze request is set using Customer Center.
    - `Unfrozen with Agent Call` — The device has been unfrozen by sending an unfreeze request on the next Agent call.

  - `Unfrozen with Passcode` — The end-user has unfrozen the device by entering a Pass Code on the frozen device.

    NOTE Unfreezing via an Agent call is the preferred method for unfreezing a device. If possible, it is recommended that devices be unfrozen by setting the status on Customer Center only.

  - `Cancelled` — The device freeze request was canceled before being deployed to the target device.

- **Identifier** — the target device's Identifier.
- **Make** — the target device's make and manufacturer name.
- **Model** — the target device's model.
- **Serial #** — the target device's serial number.
- **Asset** — the target device's inventory tracking or asset number as assigned by the network administrator in the organization.
- **Last Call** — the date and time of the device's last Agent call to the Monitoring Center.
- **Status** table — the detailed information about the freeze/unfreeze activity on the target device. The following information is shown:
  - **Step** — the number of status change, used to differentiate updates.
  - **Status** — the status of the Freeze Request.
  - **Date** — the date and time when the change in status occurred.
  - **Username** — the username of the Security Administrator who requested the status change.

In addition to this information, the Device Freeze Details page contains the following buttons allowing Security Administrators to perform additional tasks:

- **Get Unfreeze Pass Code** — Clicking this button allows Security Administrators to request a Pass Code to unfreeze a device manually. See "Requesting an Unfreeze Pass Code" on page 209 and "Using an unfreeze code on the target device" on page 212 for more information.
- **Unfreeze Device** — Clicking this button allows Security Administrators to submit a request to unfreeze a frozen device on the next Agent call. See "Using Customer Center to Unfreeze on Agent Call" on page 210 for more information.
- **Cancel Request** — Clicking this button allows Security Administrators to cancel a Device Freeze request before the device is frozen. See "Canceling a Device Freeze Request" on page 212 for more information.
- **Remove Details** — Clicking this button allows Security Administrators to remove the details of a Device Freeze Request. See "Removing Device Freeze Request Details" on page 214 for more information.

Device Freeze Details for Lenovo Devices

For all Lenovo Lost and Found devices, the Device Freeze Details page shows the following information:

- **Identifier** — the target device’s Identifier.
- **Make** — the target device’s make and manufacturer name.
- **Model** — the target device’s model.
- **Serial #** — the target device’s serial number.
- **Asset** — the target device’s inventory tracking or asset number as assigned by the network administrator in the organization.
- **Freeze Status** — the status of the Freeze Request.
- **Lenovo EL+F Status** — the current status under the Lenovo Lost and Found program. Possible values are:
    - **Lost** — reported as Lost to Lenovo.
    - **Found** — reported as Found to Lenovo.
    - **Received** — all devices returned to Lenovo.
- **Unfreeze Passcode** — the passcode used to unfreeze devices by entry on the frozen device.

Requesting an Unfreeze Pass Code

In some circumstances, it is not feasible to wait for the next Agent call to unfreeze a device. In such cases, it is possible to unfreeze a device by entering a Pass Code on the frozen device. Security Administrators can submit a request to generate a Pass Code from the Device Freeze Details page in Customer Center. The Pass Code is randomly generated in Customer Center and is shown only once to the Security Administrator who requested it.

To request an unfreeze Pass Code:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. Enter all appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all devices for your account containing a Device Freeze request in the results grid.
5. Click the **Edit** link for the appropriate device. The Device Freeze Details page opens to show the details for the selected request.
6. Click **Unfreeze**. The Provide Authentication page opens.

7. Enter your Customer Center password and the Authorization Code. See "Authorization Codes" on page 31 for more information.
8. Click **OK**. The Device Freeze Details page opens to show the Pass Code and instructions on how to use it to unfreeze a device. See "Using an unfreeze code on the target device" on page 212 for more information.

Unfreezing a Frozen Device

Devices frozen using the Device Freeze feature can be unfrozen and made operational in the following two ways:

- Using Customer Center to Unfreeze on Agent Call
- Using an unfreeze code on the target device

Using Customer Center to Unfreeze on Agent Call

Security Administrators can unfreeze a device using the Device Freeze Details page on Customer Center. When the unfreeze request is set on Customer Center, the device is unfrozen on the next Agent call to the Monitoring Center. The Agents on frozen devices call into the Monitoring Center every 15 minutes.

You can unfreeze a single device or multiple devices at the same time. See Unfreezing a Single Device on Agent Call and Unfreezing Multiple Devices on Agent Call.

Unfreezing a Single Device on Agent Call

To unfreeze a single device using Customer Center:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. Enter all appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all devices for your account matching your search criteria in the results grid
5. For the appropriate device, click the **Edit** link to open the Device Freeze Details page.
6. Click **Unfreeze**. The device is unfrozen on the next Agent call. The following scenarios are possible:
    - If the device is RTT and Intel AT enabled, a dialog box prompting you to force a call to the device using MCIC opens. If necessary, force a call to the device. See "Initiating a Forced Call" on page 67 for more information. After the device receives and

processes the SMS message, depending upon the Device Freeze defaults set for the account, the device unfreezes.

OR

- If the device does not support RTT and the new Intel AT features, the device is unfrozen on the next Agent call.

Unfreezing Multiple Devices on Agent Call

To unfreeze multiple devices at the same time using Customer Center:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. For Device Freeze Status, select the **Frozen** checkbox.
5. Enter all other appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all frozen devices for your account matching your search criteria in the results grid.
6. Select the checkbox in the left-hand column of the top row to open the Select All dialog box.
7. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Device Freeze Summary Report results grid.
   - **This Page Only** — selects the devices that show on the current page of the Device Freeze Summary Report results grid only.

   The Device Freeze Summary Report page opens to show the checkboxes for the selected devices checked.
8. Click **Edit Selected Devices** to open the Edit Selected Devices page.
9. In the **Action** list for the **Frozen** row, select **Unfreeze**.
10. Click **Submit**. The device is unfrozen on the next Agent call. The following scenarios are possible:
    - If any devices are RTT and Intel AT enabled, a dialog box prompting you to force a call to these device using MCIC opens. If necessary, force a call to the selected devices. See "Initiating a Forced Call" on page 67 for more information. After the device receives and processes the SMS message, depending upon the Device Freeze defaults set for the account, the device unfreezes.

    OR

    - If a device does not support RTT and the new Intel AT features, the device is unfrozen on the next Agent call.

Using an unfreeze code on the target device

Frozen devices call the Monitoring Center every 15 minutes. In case the device is unable to make Agent calls, it is possible to unfreeze it manually.

NOTE Unfreezing via an Agent call is the preferred method for unfreezing a device. If possible, it is recommended that devices be unfrozen by setting the status on Customer Center only.

To unfreeze a device manually:

1. The user contacts their organization's Customer Support or the Security Administrator for their account to initiate a manual unfreeze request.
2. The Security Administrator generates an Unfreeze Pass Code using Customer Center and provides it to the user with detailed instructions on unfreezing the device. For more information on requesting an unfreeze passcode, see "Requesting an Unfreeze Pass Code" on page 209.
3. The user unfreezes the device as follows:

   IMPORTANT The frozen device does not show any supporting fields to facilitate code entry. Pressing the `Esc` key allows the user to enter the Pass Code and unfreeze the device.

   a) On the frozen device, press the `Esc` button on the keyboard.

   b) Enter the Pass Code provided using the number keys in the upper row.

      IMPORTANT If you enter the Pass Code using the numeric keypad, the Device does not unfreeze.

The device is immediately unfrozen.

Canceling a Device Freeze Request

Before a Theft Report can be filed for a device, all outstanding freeze requests need to be completed or canceled. If any outstanding Device Freeze requests exist, they need to be canceled and the device unfrozen before the device can be flagged as **Stolen** and a theft report filed for it. A Device Freeze request can only be canceled before it has been deployed on the target device.

NOTE Device Freeze requests can only be canceled if the status is **Freeze Requested**. When a device is frozen, initiate an unfreeze request to return the device to operational status. See "Unfreezing a Frozen Device" on page 210 for more information.

You can cancel the Device Freeze request for a single device or for multiple devices at the same time. See Canceling a Device Freeze Request For a Single Device and Canceling Device Freeze Requests For Multiple Devices.

Canceling a Device Freeze Request For a Single Device

To cancel a Device Freeze request for a single device:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. Enter all appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all devices for your account containing a Device Freeze request in the results grid.
5. Click the **Edit** link for the appropriate request. The Device Freeze Details page opens to show the details for the selected request.
6. Click **Cancel Request**. The Device Freeze request is canceled.

Canceling Device Freeze Requests For Multiple Devices

To cancel the Device Freeze requests for multiple devices at the same time:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. For Device Freeze Status, select the **Frozen** checkbox.
5. Enter all other appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all devices for your account matching your search criteria in the results grid.

6. Select the checkbox in the left-hand column of the top row to open the Select All dialog box.
7. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Device Freeze Summary Report results grid.
   - **This Page Only** — selects the devices that show on the current page of the Device Freeze Summary Report results grid only.

   The Device Freeze Summary Report page opens to show the checkboxes for the selected devices checked.
8. Click **Edit Selected Devices** to open the Edit Selected Devices page.
9. In the **Action** list for the **Freeze Requested** row, select **Cancel Request**.
10. Click **Submit**. The Device Freeze requests for all the selected devices are canceled.

Removing Device Freeze Request Details

In certain circumstances, you may no longer need to save the details of a particular Device Freeze Request in Customer Center. Some examples are when a Device Freeze Request was canceled, completed, or the device recovered successfully. You can remove the details of such a Device Freeze request from Customer Center.

IMPORTANT Exercise caution in removing the details of a Device Freeze request. After you remove the details of a request operation, you cannot restore these details.

You can remove the details of the Device Freeze request for a single device or for multiple devices at the same time. See Removing Details of a Single Device Freeze Request and Removing Details of a Single Device Freeze Request.

Removing Details of a Single Device Freeze Request

To remove details of a Device Freeze request:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. Enter all appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all

devices for your account containing a Device Freeze request in the results grid.

5. Click the **View** or **Edit** link for the appropriate request. The Device Freeze Details page opens to show the details for the selected request.
6. Click **Remove Details**. The Confirm Removal of Device Freeze Details page opens.
7. Click **OK**. The Device Freeze Request details are deleted from Customer Center.

Removing Details of Multiple Device Freeze Requests

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. For Device Freeze Status, select the **Unfreeze Requested**, **Unfrozen With Agent Call**, **Request Cancelled**, and **Unfrozen With Passcode** checkboxes.
5. Enter all other appropriate criteria on this page, and then click **Show Results**. The Device Freeze Summary Report page refreshes to show a list of all devices for your account containing a Device Freeze request in the results grid.
6. Select the checkbox in the left-hand column of the top row to open the Select All dialog box.
7. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Device Freeze Summary Report results grid.
   - **This Page Only** — selects the devices that show on the current page of the Device Freeze Summary Report results grid only.

   The Device Freeze Summary Report page opens to show the checkboxes for the selected devices checked.
8. Click **Edit Selected Devices** to open the Edit Selected Devices page.
9. In the **Action** list for the **Freeze Requested** row, select **Cancel Request**.
10. Click **Submit**. The Device Freeze Request details for all the selected devices are deleted from Customer Center.

Managing Custom Device Freeze Messages

Security Administrators can create and edit custom Device Freeze messages using a combination of plain text and HTML formatting. Custom messages help you ensure that the appropriate information is available to the users of a frozen device. Such messages may include support contact information and/or other information that is necessary for users when calling Technical Support to restore functionality for frozen devices.

Creating a Custom Device Freeze Message

To create a custom Device Freeze message:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Create Device Freeze Message** link. The Create Device Freeze Message page opens.

   NOTE Alternatively, you can also click **Add** on the Device Freeze Messaging page to go to the Create Device Freeze Message page.

4. In the **Message Name** field, type a meaningful title for the new Device Freeze message. The title shows as an option in the **Select a message** list on the Request Device Freeze page.
5. In the Message Text field, type the text you want to show on frozen devices. You can use plain text or a combination of text with the following HTML formatting tags:
   - <b> — render as bold
   - <i> — italicize text
   - <u> — add underline
   - <font> — specify font to show a selection of text
   - <p> — define a paragraph with default spacing before and after text
   - <br> — add a line break without default spacing
6. Click **Save**. Customer Center saves the new message and refreshes the Create Device Freeze Message page to show a confirmation message.

Editing Existing Custom Device Freeze Messages

To edit existing Device Freeze messages:

1. Log in to Customer Center as a Security Administrator.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Messaging** link. The Device Freeze Messaging page opens to show a list of all messages available for your account.
4. Click the **Message Name** or the **Edit** link for the message you want to edit. The Create Device Freeze Message page opens.
5. Edit the message as appropriate.
6. Click **Save**. Customer Center saves the change and refreshes the Create Device Freeze Message page to show a confirmation message.

Deleting Existing Custom Device Freeze Messages

To delete existing Device Freeze messages:

1. Open the Create Device Freeze Message page for the appropriate message. See step 1 to 4 in "Editing Existing Custom Device Freeze Messages" on page 216 for more information on opening the Create Device Freeze message page.
2. Click **Delete**. Customer Center deletes the message and refreshes the Create Device Freeze Message page to show a confirmation message.

Chapter 11 Managing Encryption

Customer Center offers a new Encryption feature letting authorized administrators create and maintain encrypted volumes on devices in an account. The Encryption tool is primarily intended to provide an easy-to-use encryption tool and comfort customers about the protection of the data saved in the encrypted volume. The Encryption area in Customer Center provides the following functionality:

- Specifying Encryption Defaults For Your Account
- Creating an Encrypted Volume on a Device
- Managing Devices Equipped With Volume Encryption

What is Volume Encryption?

Volume encryption denotes a type of secure storage where a specific amount of data storage space on the hard disk is encrypted. The Volume Encryption feature is incorporated into the existing Customer Center, and offers the following advantages over traditional Full Disk Encryption (FDE) solutions:

- **Automatic and Remote Deployment** — Unlike most encryption solutions, the Volume Encryption feature does not require any manual configuration by the administrator on each specific device. The creation and maintenance of encrypted volumes is managed using the Customer Center interface, and deployed to the target device using the Agent.
- **Low Processor Cycles** — Volume encryption does not use significant CPU cycles. Unlike full disk encryption (FDE) solutions, volume encryption is easy to deploy and maintain. Full disk encryption involves adding overhead to the general use of a device, with all file transactions requiring encryption and decryption. Volume encryption adds no overhead when accessing applications and other files not requiring encryption.
- **Device Management** — The Manage Devices Equipped With Encryption page allows administrators to search for and manage devices with encrypted volumes. See "Managing Devices Equipped With Volume Encryption" on page 224 for more information.

Minimum System Requirements

Currently, the Volume Encryption feature is available for devices that meet the following minimum system requirements:

- **Operating System** — Windows XP, Vista, 2003, or 7
- **File System** — NTFS

- **Computrace Agent** — Agent Version 8XX series

IMPORTANT The Volume Encryption feature is not available on Windows Mobile, Macintosh, or BlackBerry devices; or for file systems other than NTFS such as FAT32.

Specifying Encryption Defaults For Your Account

Administrators can use the Set Encryption Defaults page to define volume encryption settings for supported devices in your account. You can specify the following options using the Set Encryption Defaults page:

- **Group** — the device group for which you are specifying the settings
- **Default Volume Size (MB)** — the default data storage capacity for the encrypted volume, specified in megabytes (MBs). The encrypted volume can use up to 90 percent of the total free space on the hard drive.
- **Default Volume Label** — the default drive name associated with the encrypted volume, such as Sales Reports or HR files.

NOTE We recommend that you use a generic yet meaningful name, that may not work as a clue denoting encyrption on the device, such as “My files”. Names such as such as Encrypted or Confidential are not advisable.

- **Default Drive Letter** — the letter associated with the drive created on the device, such as *H:*, *G:*, or *X:*. Possible values can be any drive letters between *F:* and *Z:*.

IMPORTANT If the default drive letter specified on the Set Encryption Defaults page is already mapped to an existing drive, the creation of the encrypted volume fails.

- **Automatically create encrypted volumes for this group** — settings associated with all the devices targeted for Volume Encryption. For devices that do not currently contain encryption, an encrypted volume is automatically created depending upon the defaults specified.

Using the Set Encryption Defaults page

To specify encryption defaults for your account:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Set Encryption Defaults** link. The Set Encryption Defaults page opens.

4. Specify the appropriate settings for the following:

   IMPORTANT All values on the Set Encryption Defaults page are mandatory.

   - Group
   - Default Volume Size (MB)
   - Default Volume Label
   - Default Drive Letter

5. If you want to automatically apply these default encryption settings to all the devices in the selected device group, select the **Automatically create encrypted volumes for this Group** checkbox.

   When you select the **Automatically create encrypted volumes for this Group** checkbox, the specified settings are automatically applied to all devices in the device group. For devices without an existing encrypted volume, a new encrypted volume based on the defaults you have specified is created. For devices with an existing encrypted volume, the encryption settings do not change. You can manually apply these encryption settings to such devices using the Device Details page. For more information about editing the values for a single device see "Modifying the Encrypted Volume On a Single Device" on page 225. For more information about editing the values for multiple devices see "Modifying the Encrypted Volumes for Multiple Devices" on page 229.

6. Click **Save**. A dialog box opens to inform you that specified default settings are applied to all devices in the group.

7. Click **Continue**. The dialog box closes and the Set Encryption Defaults page shows with a message confirming that Customer Center has saved the default settings.

Creating an Encrypted Volume on a Device

After you specify encryption defaults for a device group, adding new devices to the group automatically creates a new encrypted volume on the device. For devices already existing in the device group, you need to create the encrypted volume using the Device Details page. The Device Details Page for devices without an existing encrypted volume lists the following fields:

- **Identifier** — the unique identifying number associated with the device.
- **Make** — the name of the manufacturer of the device.
- **Model** — the model number, if available, of the device.
- **Serial** — the hardware identification number associated with the device.
- **Volume Letter** — the drive letter to be assigned to the encrypted volume on the device, as specified on the Set Encryption Defaults page.
- **Volume Size (MB)** — the data storage capacity to be made available on the encrypted volume, as specified on the Set Encryption Defaults page.

- **Volume Label** — the descriptive name to be associated with the encrypted volume, as specified on the Set Encryption Defaults page.
- **Volume State** — the read-only value lists the current volume encryption state, that is **No encryption**. The drop-down list next to the Volume State field lists the possible encryption states you can assign to the device. The only possible value for devices without encryption is **Create Encrypted Volume**.

You can create encrypted volumes on a single device or multiple devices. For more information see the sections on Creating an Encrypted Volume on a Single Device and Creating Encrypted Volumes on Multiple Devices.

Creating an Encrypted Volume on a Single Device

To create an encrypted volume on a single device:

IMPORTANT Before creating an encrypted volume on a device, ensure that you have set account-wide encryption defaults using the Set Encryption Defaults page. You cannot create an encrypted volume on a device with an open Theft Report.

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Manage Devices Equipped With Encryption** link. The Manage Devices Equipped With Encryption page opens.
4. In the **State** area, clear all checkboxes except the **No Encryption** checkbox.

   NOTE If available, you can directly enter the appropriate value in the **Identifier** field, and then click **Show Results**.

5. Specify all the other appropriate filter criteria.
6. Click **Show Results**. The Manage Devices Equipped With Encryption page refreshes to show devices matching specified filter criteria in the results grid.
7. For the appropriate device, click the **Edit** link showing in the last column in the results grid. The Device Details page opens.
8. Modify the appropriate values for the Volume Letter, Volume Size (MB), and the Volume Label fields.
9. In the **Volume State** list, select **Create Encrypted Volume**.
10. Click **Save**. The Manage Devices Equipped page opens showing a confirmation message that the request was successfully created. On

the next Agent call, a new encrypted volume is created on the specified device.

IMPORTANT Currently, using the Switch User functionality in Windows leaves the encrypted volume accessible to the new user. To ensure security of your encrypted data, log off the device before allowing another user to log in.

Creating Encrypted Volumes on Multiple Devices

To create encrypted volumes on multiple devices without encryption:

IMPORTANT Before creating an encrypted volume on a device, ensure that you have set account-wide encryption defaults using the Set Encryption Defaults page. You cannot create an encrypted volume on devices with an open Theft Report.

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Manage Devices Equipped With Encryption** link. The Manage Devices Equipped With Encryption page opens.
4. In the **State** area, clear all checkboxes except the **No Encryption** checkbox.

   NOTE If available, you can directly enter the appropriate value in the **Identifier** field, and then click **Show Results**.

5. Specify all the other appropriate filter criteria.
6. Click **Show Results**. The Manage Devices Equipped With Encryption page refreshes to show devices matching specified filter criteria in the results grid.
7. Select the checkbox in the left-hand column of the top row to open the Select All dialog box.
8. Click the appropriate button from the following:
   - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped With Encryption report page.
   - **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped With Encryption report page only.

The Manage Device Equipped With Encryption report page opens to show the checkboxes for the selected devices checked.

9. Click **Edit Selected Devices** to open the Edit Selected Devices page.
10. In the **Action** list for the **No Encryption** row, select **Create Encrypted Volume**.
11. Click **Submit**. The Manage Devices Equipped page opens showing a confirmation message that the request was successfully created. On the next Agent call, a new encrypted volume is created on the specified devices.

IMPORTANT Currently, using the Switch User functionality in Windows leaves the encrypted volume accessible to the new user. To ensure security of your encrypted data, log off the device before allowing another user to log in.

Managing Devices Equipped With Volume Encryption

The Managing Devices Equipped With Volume Encryption area provides access to the following functionality:

- Generating a Report Listing Devices Supporting Encryption.
- Modifying the Encrypted Volume On a Single Device.

Generating a Report Listing Devices Supporting Encryption

The Manage Devices Equipped With Encryption page provides filter criteria that allow you to generate a list of devices in your account equipped with encryption and at various stages of the encryption process. By default, the report shows results for all devices in your encryption group.

Additionally, you can filter the Manage Devices Equipped With Encryption report by a number of different criteria:

- **Group** — shows only devices belonging to a specific Device Group
- **Field** — includes devices that match a specific value in certain data fields. The fields available for the filter are any user-defined fields and the following: **Any Field, Identifier**, **Make**, **Model**, **Serial#**, **Device Name**, and **Username**. For more information about Managing User-defined Fields see "Viewing and Editing User-defined Fields Data" on page 45.
- **Volume Size** — shows devices containing an encrypted volume matching a specific size in MBs
- **Volume Label** — shows devices containing an encrypted volume with a volume name matching specific criteria

- **Drive Letter** — shows devices where the encrypted volume is mapped to a specific drive letter, such as “H:” or “J:”.
- **State** — shows devices in a particular state of encryption. Possible values include:
  - **No Encryption** — devices without any encrypted volumes.
  - **Creating Encrypted Volume** — devices with an outstanding request to create a new encrypted volume
  - **Volume Encrypted** — devices with an existing encrypted volume
  - **Locking Encrypted Volume** — devices where the contents of the encrypted volume are being locked
  - **Locked Encrypted Volume** — devices with a locked encrypted volume
  - **Unlocking Encrypted Volume** — devices where the contents of the encrypted volume are being unlocked
  - **Show only devices for which an error occurred** — devices where the encryption process generated an error message

    NOTE To view the error message, point to ⚠. A small dialog box opens to show the details of the error message.

  - **Removing Encrypted Volume** — devices with an outstanding request to remove the existing encrypted volume

To generate the report:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Manage Devices Equipped With Encryption** link. The Manage Devices Equipped With Encryption page opens.
4. Specify the appropriate filter criteria.
5. Click **Show Results**. The Manage Devices Equipped With Encryption page refreshes to show devices matching specified filter criteria in the results grid.

Modifying the Encrypted Volume On a Single Device

For an account with encryption defaults specified using the Set Encryption Defaults page, any new devices added to the account automatically creates a new encrypted volume on the device matching the settings specified. You can use the Device Details page to edit the encryption details for devices with an encrypted volume. The information listed on the Device Details page is the same as the information listed on the Device Details page for devices without an encrypted volume, with one difference — value of the volume state field.

Depending upon the encryption state on the device, various options are available in the **Volume State** drop-down list. Refer to the following table for details.

Table 1. Options Available In The Volume State List

#	Current State	Options Available
1.	Creating Encrypted Volume	Cancel
2.	Volume Encrypted	Remove Encryption, Lock Encrypted Volume
3.	Locking Encrypted Volume	Cancel
4.	Locked Encrypted Volume	Unlock Encrypted Volume
5.	Unlocking Encrypted Volume	Cancel
6.	Removing Encrypted Volume	Cancel

You can use the Modify Encryption Settings functionality for the following:

- Removing Volume Encryption
- Locking an Encrypted Volume
- Unlocking an Encrypted Volume

For information on modifying the encrypted volumes for multiple devices see "Modifying the Encrypted Volumes for Multiple Devices" on page 229.

Removing Volume Encryption

IMPORTANT Removing the encrypted volume deletes the files stored in the volume. If necessary, copy critical data to another volume or location on your hard drive before removing the encrypted volume.

To remove the encrypted volume on a device:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Manage Devices Equipped With Encryption** link. The Manage Devices Equipped With Encryption page opens.
4. Specify appropriate search criteria.
5. In the **State** area, select the **Encrypted** Volume checkbox.

NOTE If available, you can directly enter the appropriate value in the **Identifier** field, and then click **Show Results**.

6. Click **Show Results**. The Manage Devices Equipped With Encryption page refreshes to show devices matching specified filter criteria in the results grid.
7. For the appropriate device, click the **Edit** link showing in the last column in the results grid. The Device Details page opens.
8. In the **Volume State** list, select the **Remove Encrypted Volume** option.
9. Click **Save**.
10. If your account uses authentication, the Request Authentication page opens.

    NOTE By default, authentication is turned on for all accounts. To disable or modify authentication for your account, contact Absolute Software Customer Support.

11. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
12. Click **OK**. The Manage Devices Equipped page opens to show a confirmation message that the request to modify encryption details was successfully created. On the next Agent call, the volume encryption settings on the specified device are modified.

Locking an Encrypted Volume

When a device containing an encrypted volume is stolen and a Theft Report for the device is opened, you can submit a request in Customer Center to lock the contents of the encrypted volume on the device. Locking the encrypted volume secures the stored data and ensures that the thief is unable to gain access to confidential information even if the password is compromised. See *Reporting a Theft* in the *Customer Center User's Guide* available on the Customer Center Documentation page for information on creating a Theft Report for stolen devices.

To lock an encrypted volume:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Manage Devices Equipped With Encryption** link. The Manage Devices Equipped With Encryption page opens.
4. Specify appropriate search criteria.
5. In the **State** area, select the **Volume Encrypted** checkbox.

    NOTE If available, you can directly enter the appropriate value in the **Identifier** field, and then click **Show Results**.

6. Click **Show Results**. The Manage Devices Equipped With Encryption page refreshes to show devices matching specified filter criteria in the results grid.
7. For the appropriate device, click the **Edit** link showing in the last column in the results grid. The Device Details page opens.
8. In the **Volume State** list, select the **Lock Encrypted Volume** option.
9. Click **Save**.
10. If your account uses authentication, the Request Authentication page opens.

NOTE By default, authentication is turned on for all accounts. To disable or modify authentication for your account, contact Absolute Software Customer Support.

11. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
12. Click **OK**. The Manage Devices Equipped page opens to show a confirmation message that the request to modify encryption details was successfully created. On the next Agent call, the volume encryption settings on the specified device are modified.

Unlocking an Encrypted Volume

To unlock a locked encrypted volume:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Manage Devices Equipped With Encryption** link. The Manage Devices Equipped With Encryption page opens.
4. Specify appropriate search criteria.
5. In the **State** area, select the **Volume Encrypted** checkbox.

NOTE If available, you can directly enter the appropriate value in the **Identifier** field, and then click **Show Results**.

6. Click **Show Results**. The Manage Devices Equipped With Encryption page refreshes to show devices matching specified filter criteria in the results grid.
7. For the appropriate device, click the **Edit** link showing in the last column in the results grid. The Device Details page opens.
8. In the **Volume State** list, select the **Unlock Encrypted Volume** option.
9. Click **Save**.

10. If your account uses authentication, the Request Authentication page opens.

    NOTE By default, authentication is turned on for all accounts. To disable or modify authentication for your account, contact Absolute Software Customer Support.

11. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code.
12. Click **OK**. The Manage Devices Equipped page opens to show a confirmation message that the request to modify encryption details was successfully created. On the next Agent call, the volume encryption settings on the specified device are modified.

Modifying the Encrypted Volumes for Multiple Devices

You can also use the Edit Selected Devices button on the Manage Devices Equipped With Encryption page to modify the encrypted volumes on multiple devices. To modify encrypted volumes on multiple devices:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. In the **Encryption** area, click the **Manage Devices Equipped With Encryption** link. The Manage Devices Equipped With Encryption page opens.
4. Specify appropriate filter criteria.
5. Click **Show Results**. The Manage Devices Equipped With Encryption page refreshes to show devices matching specified filter criteria in the results grid.
6. Select the checkbox in the left-hand column of the top row to open the Select All dialog box.
7. Click the appropriate button from the following:
    - **Select All Records** — selects all the devices that match your filter criteria. These devices show up on different pages of the Manage Devices Equipped With Encryption report page.
    - **This Page Only** — selects the devices that show on the current page of the Manage Devices Equipped With Encryption report page only.

    The Manage Device Equipped With Encryption report page opens to show the checkboxes for the selected devices checked.
8. Click **Edit Selected Devices** to open the Edit Selected Devices page.
9. For the appropriate rows, edit the value in the **Action** list.

10. Click **Submit**. The Manage Devices Equipped page opens showing a confirmation message that the encrypted volume on the selected devices was successfully modified. On the next Agent call, the modified settings are applied to the devices.

IMPORTANT Currently, using the Switch User functionality in Windows leaves the encrypted volume accessible to the new user. To ensure security of your encrypted data, log off the device before allowing another user to log in.

Chapter 12 *Using Remote File Retrieval*

The Remote File Retrieval feature allows Security Administrators to remotely retrieve files that may contain important information from the devices in your account.

Security Administrators use file paths to specify the files to retrieve. File paths can be obtained by using the File List feature. See Using File List for more information.

Minimum System Requirements

Remote File Retrieval is available for devices that meet the following system requirements:

- **Operating System** — Windows NT, 2000, XP, Vista, or 7
- **Computrace Agent** — Agent Version 8XX series

Remote File Retrieval on Stolen Devices

Remote File Retrieval is available for stolen devices. However, you can only retrieve the files that were created before the device's date of theft.

Requesting a Remote File Retrieval

To request a Remote File Retrieval:

1. Log in to Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Remote File Retrieval** link. The Remote File Retrieval page opens.
4. Click the **Request File Retrieval** link. The Request Remote File Retrieval page opens.
5. In the **Request Name** field, type a meaningful name for the new request.
6. Use the **Choose** feature to specify the target device for the Remote File Retrieval operation. To select a device using the Choose feature:

a) Click **Choose**. The Choose dialog box opens to show a list of all devices in your account.

b) Click the **Identifier** of the appropriate device. The Choose dialog box closes and the Request File Retrieval page refreshes.

IMPORTANT You cannot choose a device that already has an outstanding Data Delete request. You must either cancel the outstanding Data Delete request or wait for the request to complete. See Cancelling a Data Delete Request for more information.

7. In the **File Path to Retrieve** field, specify the path of the file you want to retrieve. If you are unsure of the file path for the target file, you can request a list of files available on the target device. For more information see "Requesting a File List" on page 237.

IMPORTANT There are no restrictions on the size of the file you want to retrieve. However, for files larger than 1 GB in size, the chances of successful file retrieval diminish.

8. Click **Enter**. The path is added to the list below.
9. Repeat step 8 to add multiple paths to the list.

IMPORTANT You can add up to 20 files to the list.

NOTE To remove a path from the list, click **Remove** next to the path you want to remove.

10. Read the **Legal Notice** carefully and select the **I agree** checkbox to indicate that you have read the notice and agree to the terms.
11. Click **Submit**. The Remote File Retrieval request is created and is deployed to the device on the next Agent call.

Tracking Remote File Retrieval Status

Customer Center provides near real-time status updates on the progress of Remote File Retrieval requests. The File Retrieval Summary Report page lists all devices for which Remote File Retrieval has been requested. For each device listed, the File Retrieval Summary report page includes the following information:

- **Identifier** — the target device’s Identifier
- **Request Name** — the name of the Remote File Retrieval request
- **Status** — the current status of the File Retrieval request. Possible values are:

- `Requested` — The request has been submitted and is in a transitory state when waiting for an Agent call or when the instruction setup process is running on the target device.
- `Retrieving` — The File Retrieval operation is in progress to retrieve the requested file.
- `Ready` — The File Retrieval operation has finished retrieving the requested file. The file is ready for download.

  IMPORTANT Retrieved files are available for download for 30 days before being automatically deleted from the servers.

- `Canceled` — The File Retrieval request has been canceled. For more information about canceling a File Retrieval request see "Canceling a File Retrieval Request" on page 235.
- `Failed` — The File Retrieval request failed to execute on the target device.
- `Purged` — The retrieved file has been deleted from the servers.

- **Action** — the action you can perform on the request.
- **File Name** — the name of the retrieved file
- **File Size** — the file size of the retrieved file
- **Device Name** — the device's network name as captured by the Agent
- **Username** — the device's username as captured by the Agent
- **Make** — the target device's make
- **Model** — the target device's model
- **Requested On** — the date of the request
- **Requested By** — the name of the Security Administrator who submitted the request

Viewing the File Retrieval Status

1. Log in to Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Remote File Retrieval** link. The Remote File Retrieval page opens.
4. Click the **File Retrieval Summary Report** link on the global navigation bar or the Remote File Retrieval page. The File Retrieval Summary Report page opens.

5. Specify the appropriate filtering options, and then click **Show Results**. The Remote File Retrieval page refreshes to show a list of all File Retrieval requests that match your filtering criteria. If a File Retrieval operation has successfully finished, the status of the request becomes **Ready** and the file is ready for download.

Downloading Retrieved Files

After you have successfully created a File Retrieval request, the request runs on the target device on the next Agent call. When the retrieval is complete, you can download the retrieved files to your local device.

To download a file:

1. Use the File Retrieval Summary report to search for the appropriate request. If the file is available for download, the Status column shows Ready.
2. For the file you want to download, click the file name link.
3. Enter your Customer Center Password and your RSA SecurID® Token validation code or Security Authorization Code. See "Security Authentication Methods" on page 31 for more information.
4. Follow the on-screen instructions to save the file to a location of your choosing.

Known Issue

When you use Internet Explorer to download the retrieved file to your local device, you may be prompted to enter a second Security Authorization code before Customer Center lets you download the retrieved file. To work around this issue, do the following:

1. On the **Security** tab of the the Internet Options dialog, add the Customer Center domain (**cc.absolute.com**) as a trusted site.
2. For all trusted sites, click Custom Level, and in the Security Settings - Trusted Sites Zone dialog box, enable the “Automatic prompting for Downloads” option.

If you do not want to make these changes to Internet Explorer’s security settings, you can use FireFox to download the retrieved file to your local device.

Changing the File Retrieval Status

Depending upon the current File Retrieval status, you can either:

- Cancel a File Retrieval request; or
- Remove the files retrieved and the log files generated during the retrieval process

Table 1 lists possible File Retrieval statuses and the actions you can perform for each of them.

Table 1. Available Actions

Status	Action
Requested	`Cancel`
Retrieving	
Ready	`Remove`
Canceled	
Failed	
Purged	

Canceling a File Retrieval Request

If the status of the File Retrieval process is set to Requested or Retrieving, you can cancel the request and stop the file retrieval. To cancel a File Retrieval request:

1. Log in to Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Remote File Retrieval** link. The Remote File Retrieval page opens.
4. Click the **File Retrieval Summary Report** link on the global navigation bar or the Remote File Retrieval page. The File Retrieval Summary Report page opens.
5. Search for the appropriate File Retrieval request. If the File Retrieval request has not yet run or is in the process of running, the **Status** column shows Requested or Retrieving.
6. In the **Action** column of the File Retrieval request you want to cancel, click the **Cancel** link.
7. When prompted if you want to cancel the request, click **OK** to confirm. The File Retrieval Summary Report page refreshes to show Canceled in the **Status** Column next to the Remote File Retrieval request you canceled.

Removing Retrieved Files and Log Files

When you run a File Retrieval request, a directory log file is also generated. This log file provides a list of all files and their retrieval status. When a File Retrieval request is successful, the files that you had requested are available in Customer

Center. You can choose to download these files to a folder on your local device. After the File Retrieval request is complete or if you have canceled a File Retrieval request, you may need to delete the downloaded files and/or the directory log file. To remove downloaded files and/or the directory log file:

1. Log in to Customer Center as an administrator with Security administration privileges.

   NOTE If you are not logged in as a Security Administrator, all options on Data and Device Security pages are unavailable.

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Remote File Retrieval** link. The Remote File Retrieval page opens.
4. Click the **File Retrieval Summary Report** link on the global navigation bar or the Remote File Retrieval page. The File Retrieval Summary Report page opens.
5. Search for the appropriate File Retrieval request.
   - If the File Retrieval request has successfully run and the files are available for download, the **Status** column shows Ready and the **Action** column shows Remove.
   - If the File Retrieval request has not run or was canceled, the **Status** column shows Failed or Canceled and the **Action** column shows Remove.
6. In the **Action** column of the appropriate File Retrieval request, click the **Remove** link.
7. When prompted if you want to remove the retrieved files and the log files, click **OK** to confirm. The File Retrieval Summary Report page refreshes without any details about the File Retrieval request you just removed.

Chapter 13 *Using File List*

The File List feature allows Customer Center administrators to remotely retrieve a list of files from a device. The full paths of files can be used to make Remote File Retrieval requests.

IMPORTANT Only Security Administrators can make File List requests. See Using Remote File Retrieval for more information.

Minimum System Requirements

File List is available for devices that meet the following system requirements:

- **Operating System** — Windows NT, 2000, XP, Vista, or 7
- **Computrace Agent** — Agent Version 8XX series

Listing Files on Stolen Devices

File List is available for stolen devices. However, you can only retrieve a list of files that were created before the submission date of the theft report for a device.

Requesting a File List

You can use the Request File List page to send a request to retrieve a list of files with specific file extensions available in a specific location on the target device. For ease of use, Customer Center contains a variety of pre-defined file extensions that need to be retrieved. If the file extension you want is not listed on the Request File List page, you can also specify the file extension. Table 1 lists the pre-defined file types that are available to you on the Request File List page.

Table 1. Pre-defined File Types and File Extensions

File Type	File Extensions
Microsoft Word Files	*.doc, *.dot, *.docx, *.docm, *.dotx, *.dotm
Microsoft Excel Files	*.xls, *.xlt, *.xlsx, *.xlsm, *.xltx, *.xltm, *.xlsb, *.xlam
Microsoft Powerpoint Files	*.ppt, *.pot, *.pps, *.pptx, *.pptm, *.potx, *.potm, *.ppam, *.ppsx, *.ppsm

Table 1. Pre-defined File Types and File Extensions

File Type	File Extensions
Microsoft Access Files	*.mar, *.maq, *.mdb, *.accdb, *.accde, *.accdt, *.accd
Microsoft Project Files	*.mpp*. *.mpt*. *.mpx, *.mpd
Microsoft Visio Files	*.vsd, *.vss, *.vst, *.vdx, *.vsx, *.vtx
Microsoft Outlook Files	*.pst, *.ost, *.wab
Microsoft Outlook Express Files	*.dbx
Adobe Files	*.pdf,*.pm3, *.pm4, *.pm5, *.pm6, *.psd
Autocad Files	*.dwg, *.dxf
Certificate Files	*.crt, *.pfx
Comma-Separated Value Files	*.csv
Compressed Archive Files	*.zip, *.rar, *.7z, *.tar
Corel Draw Files	*.cdt
Data Files	*.dat
Eudora Email Files	*.mbx, *.toc
Extensible Markup Language Files	*.xml, *.xps
Hyper Text Markup Language Files	*.html, *.htm
Image Files	*.bmp, *.gif, *.jpg, *.jpeg, *.tif, *.tiff, *.pcx
Initialization/Configuration Files	*.ini, *.cfg
Log Files	*.log
Lotus 1-2-3 Spreadsheet Files	*.wk*
Message Files	*.msg
Microsoft Office (& others) Backup Files	*.bak
Microsoft Windows Address Books Files	*.wab
Microsoft SQL Server Master Database Files	*.mdf
Microsoft SQL Server Transaction Log Files	*.ldf
Office Base Files	*.sdb, *.odb
Open Office Calc Files	*.sdc, *.sxc, *.ods, *.ots
Open Office Draw Files	*.sda, *.sxd, *.odg, *.otg
Open Office Impress Files	*.sdd, *.sxi, *.odp, *.otp
Open Office Math Files	*.smf, *.sxm, *.odf

Table 1. Pre-defined File Types and File Extensions

File Type	File Extensions
Open Office Schedule Files	*.sds
Open Office Writer Files	*.sdw, *.sxw, *.odt, *.ott
Paintshop Pro Files	*.psp, *.ps
Remote Desktop Protocol Files	*.rdp
Rich-Text Files	*.rtf
Sound Files	*.mp3, *.wav, *.ogg, *.aif, *.cda, *.rm, *.ram, *.mid, *.m4p
Temporary Files	*.tmp
Text Files	*.txt
Transact-SQL Query Files	*.sql
Video Files	*.mov, *.avi, *.mpg, *.mpeg, *.mp4, *.rm, *.ram
Windows Live Messenger Contact Lists	*.ctt
WordPerfect Documents	*.wkb, *.wpd

To request a File List:

1. Log in to Customer Center as an administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **File List** link. The File List page opens.
4. Click the **Request File List** link. The Request File List page opens.
5. In the **Request Name** field, type a meaningful name for the new request.
6. Use the **Choose** feature to specify the target device for the File List operation. To select a device using the Choose feature:
    a) Click **Choose**. The Choose dialog box opens to show a list of all devices in your account.

    b) Click the **Identifier** of the appropriate device. The Choose dialog box closes and the Request File List page refreshes.
7. In the **Selected Volume to Scan** pane, choose the volume from where you want to retrieve the file list.

    NOTE If the **Selected Volume to Scan** pane does not list the volume where your files are available, select the volume you want in the **Other** list.

8. Select the checkboxes for the specific file types you want to retrieve.

   NOTE To specify file types that are not listed, select the **Other** checkbox located at the bottom of the list, and then type the appropriate file extensions, separated by commas (,).

9. Click **Submit**. The File List request is created.

Tracking File List Status

Customer Center provides near real-time status updates on the progress of File List requests. The File List Summary Report page lists all devices that have had File List requested. For each device listed, the File List Summary Report page includes the following information:

- **Identifier** — the target device's Identifier
- **Request Name** — the name of the File List request
- **Status** — the current status of the File List request. Possible values are:
  - `Requested` — The request has been submitted and is in a transitory state when waiting for an Agent call or when the instruction setup process is running on the target device.
  - `Retrieving` — The File List operation is in progress to retrieve the list from the requested device.
  - `Ready` — The File List operation has finished. The list is ready for download.
  - `Canceled` — The File List request has been canceled.
  - `Failed` — The File List request failed to execute on the target device.

- **Action** — the action you can perform on the request. You can perform the following actions depending on the status of the request:

Table 2. Available Actions

Status	Action
Requested	`Cancel`
Retrieving	
Ready	`Remove`
Canceled	
Failed	

- **Device Name** — the device's network name as captured by the Agent
- **Username** — the device's username as captured by the Agent
- **Make** — the target device's make
- **Model** — the target device's model
- **Requested On** — the date of the request
- **Requested By** — the name of the administrator who submitted the request

To view the status of a File List request:

1. Log in to Customer Center as an administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **File List** link. The File List page opens.
4. Click the **File List Summary Report** link. The File List Summary Report page opens.
5. Enter all appropriate criteria on this page, and then click **Show Results**. The File List Summary Report page refreshes to show a list of all requests for your account matching the search criteria in the results grid.

If a File List operation has successfully finished, the status of the request becomes **Ready** and the list is ready for download.

To download a list:

1. In the File List Summary report, click the request name.
2. Follow the on-screen instructions to save the list to your machine.

Appendix A User Access Rights

The following three different User Access Rights groups are available in Customer Center:

- Administrator
- Power User
- Guest

The following table outlines the different access rights and the functions the three user groups can perform.

	Administrator	Power User	Guest
Reports Area			
Can view Geolocation Tracking reports	Yes	Yes	No
Can view all other reports	Yes	Yes	Yes
Can view all Identifiers in Account	Yes	No - can be restricted	No - can be restricted
Can create/view all Saved Reports	Yes	Yes	No - can only view those created by self
Functions available in Device Summary report	View and edit	View and edit	View only
Theft Reporting Area			
Can create Theft Reports	Yes	Yes - only for visible Identifiers	Yes - only for visible Identifiers
Can browse all Theft Reports	Yes	Yes - only for visible Identifiers	No - can only view those created by self

	Administrator	Power User	Guest
Administration Area			
Can access Users section (Create Users and grants Access Rights)	Yes	Yes - can only assign rights to visible Identifiers	No - access is read only
Can access Groups section (Create device group)	Yes	Yes - only for visible Identifiers	Yes - only for visible Identifiers
Can access Settings section	Yes	Access is read only except for changing their password	Access is read only except for changing their password
Can access Alerts section	Yes	Yes - only for visible Identifiers	Yes - only for visible Identifiers
Can access Data section	Yes	Yes - only for visible Identifiers	Yes - only for visible Identifiers
Can add, rename, and delete User-defined Fields	Yes	No	No

Appendix B Theft and Service Guarantee Submission Checklist

Stage	Action Required	Description	□
Device Handling	Handle the device in a reasonably secure manner.	Ensure that the device was not left unattended or in a location that is not secure.	□
Theft Report	Report to the appropriate law enforcement agency, and then submit a theft report.	Contact the law enforcement within 7 days of detecting the theft and no later than 14 days after the actual theft.	□
Service Guarantee Submission	Submit the completed Service Guarantee Submission form including all receipts for the device and all complete or professional licenses associated with the device.	Ensure that the form is submitted no later than 30 days after receipt. Receipts for both the original purchase price of the device and the licenses associated with the device must be provided when submitting the Service Guarantee Submission form.	□
	Confirm receipt of form by Absolute.	Contact Absolute Software to confirm receipt of the Service Guarantee Submission form in case you do not receive confirmation of receipt via e-mail.	□

Appendix C Installing and Activating the Intel Anti-Theft Technology Feature

This appendix describes the procedure to install, activate, and troubleshoot possible issues with Intel Anti-Theft Technology (Intel AT) equipped devices.

Best Practices

To install and activate Intel AT on devices:

1. Check the device manufacturer's (OEM) Web site to confirm that the hardware on the target devices is capable of supporting Intel AT.
   For example — In the case of Lenovo devices, refer to the following link for supported hardware: http://shop.lenovo.com/SEUILibrary/controller/e/web/LenovoPortal/en_US/special-offers.workflow:ShowPromo?LandingPage=/All/US/Sitelets/Software/Anti-Theft-Protection.

2. Log in to the Absolute Software Customer Center Web site and confirm that the client has placed an order to add the Intel AT software license for the account. To confirm that the account has the required Intel AT software license:

   ○ Log in to the Absolute Customer Center Web site at: https://cc.absolute.com/default.aspx.

   ○ Check that the Intel Anti-theft Technology option is visible under the Data and Device Security menu.

3. If required, update the BIOS to the latest version available for your device. Refer to the hardware manufacturer's (OEM) Web site for more information.
   For example — In the case of Lenovo devices, download the latest BIOS updates from the following link: http://www-307.ibm.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=MIGR-70945.

4. If required, install the latest version of Intel Management Engine. Refer to the hardware manufacturer's (OEM) Web site for more information.
   For example (Lenovo Devices Only) —

   ○ For **Intel Core i3**, **Intel Core i5**, **Intel Core i7**, and **Intel Core i7 Extreme processors**, download the Intel Management Engine from the following link: http://www-307.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-71137.

     NOTE If the Intel Management Engine installation process does not work as intended, refer to the following potential work around: http://www-307.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-73723.

   ○ For **Intel Centrino 2** and **Intel Centrino 2 vPro** processors, download the Intel Management Engine from the following link:

http://www-307.ibm.com/pc/support/site.wss/WIN7-BETA.html#mei.

5. Confirm that the Intel Management engine installation was successful. *For example* — On Windows devices, to confirm installation of the Intel Management Engine:

    a) Open **Device Manager**.

    b) Open the **System Devices Section**.

    c) Confirm that the **Intel Management Engine Interface** shows in the **System Devices** section.

6. If available on the devices, access the BIOS and confirm that the AT module is **enabled**. Refer to the User Guide provided by the hardware manufacturer for the procedure to confirm whether the AT module is enabled on your device.

    For example — On Lenovo devices, to confirm that the AT module is enabled:

    a) In the BIOS, navigate to the **Security** area, then the **Anti-theft** area, and then the **AT Module** page.

    b) In the options listed, select **Enabled**, and then press ENTER on your keyboard.

    NOTE There are three options available: Disabled, Enabled, and Permanently Disabled.

    c) Save changes.

    d) Restart the device.

7. If the Agent is not already installed, install the Agent by running the **Computrace.msi** installer on the device. After the Agent is installed on the machine, connect to the Internet and force two test calls using the Agent Management (ctmweb.exe) utility.

    NOTE The ctmweb.exe file is available in the installation folder containing the Agent installation package you extracted when installing the Agent. By default, the out-of-the-box password for the Agent Management utility is password. Refer to the Forcing a Test Call section in the Agent Install Guide for more information.

8. Wait at least five minutes.

9. Log into the Absolute Customer Center Web site at: https://cc.absolute.com/default.aspx.

10. In the Customer Center left navigation menu, click **Data and Device Security**, then click **Intel Anti-theft Protection**, and then click **Manage AT Equipped Computers**.

11. Search for the devices from which you made a test call. Confirm that the devices are shown in the list of AT equipped devices and the AT State is shown as **Active**.

12. If the devices you have just attempted to activate do not show on the list of **Active** AT devices:

    a) Log out of the Customer Center Web site.

    b) Delete the cached information from your browser.

    c) Close all and restart all Web browsers.

    d) Log in to the Customer Center Web site and search for the devices again.

    e) If the devices still do not show as **Active**, contact Absolute Software Global Support for troubleshooting. Please visit us at http://www.absolute.com/support and follow the instructions on the page to contact technical support in your region.

Appendix D Intel Anti-theft Technology Error Codes

Error Code	Error Description
General Platform Errors	
0	Platform version check failed.
1	Intel AT is enabled, but is currently Inactive.
2	Intel AT is enabled and Active.
3	Intel AT is not supported on the device due to limitations of the Chipset, CPU, or the BIOS.
5	Intel AT is not allowed on this machine because it is turned off in BIOS or the device does not support Intel AT.
8192	The Intel Management Engine Interface Driver is not present.
8193	The Intel Management Engine Interface Driver is not present.
8194	The command to the Intel Management Engine Interface Driver failed because of incorrect driver version.
8192	Windows Management Instrumentation COM failed.
12290	Windows Management Instrumentation failed to create an instance.
12291	Windows Management Instrumentation failed to read the SMBIOS. It needs to read the SMBIOS to see if Intel AT is capable. Check WMI on the machine.
12292	Windows Management Instrumentation failed to create a proxy. Check WMI on the machine.
12293	Windows Management Instrumentation failed to read the SMBIOS and confirm if the device is Intel AT capable.
16358, 16386, 16389, 16390, 16391, 16392	The Intel AT firmware generated an error when reading the platform information. The main cause of error could be incorrect firmware.
16387	The device chipset does not comply with the hardware required for Intel AT to function.
16388	The Intel AT version could not be determined.
Intel Enrollment Error	
1	Intel AT enrollment process failed due to a time out error.
2	The Intel AT enrollment type requested is not authorized and enrollment failed.
3, 5, 8, 9, 16	There was an error communicating with the Intel Permit Server, please try again.
4	Intel Permit Server returns a enrollment in progress error if the client requests enrollment when a previous request is already in progress.

Error Code	Error Description
6	An enrollment error occurred due to one or more of the following: • Invalid license key • Null Intel Permit Server name • Invalid Intel Permit Server name • Invalid port number
7	Intel Permit Server returns a enrollment not in progress error if an enrollment message is received when enrollment is not in progress.
10	Client cannot enroll in Intel AT, because the platform does not support it. Check your BIOS to see if it supports Intel AT.
11	Client cannot enroll in Intel AT, because it is not available on the platform. Check your Management Engine firmware to see if it supports Intel AT.
12	Intel Management Engine Interface Driver returned a communication error.
13	The Intel permit server failed the enrollment process.
14	The client returns an error because of an attempted Agent call from a client that is not enrolled and in inactive state.
15	The construction of the next message to the client failed.
16	Error due to passing a null pointer for a msgIn or msgOut for function.
17	Received a continue Agent Call message when the Agent call is not in progress.
18	The Agent Call is in progress
19	Error due to a mismatch in the client ID in the received message and the ID of the originating device.
20, 21, 22, 23, 24, 25, 26, 27	Failed to communicate with the local firmware on the machine, please try again.
28	Last response from Management Engine has decryption failure
29	Last response from Management Engine has invalid signature
30	Client is not in the correct state to perform operation.
31	The enroll recovery must be completed before another enrollment operation can take place.
32	The operation failed because the specified version was not as expected
33	The enrollment operation failed because the communication with the permit server timed out.
34	The enrollment operation failed because of a network-related error during communication with the permit server.
35	The SDK API call failed because the SDK was not properly initialized.
40	NULL or invalid Client ID supplied to client WWAN registration.
41	WWAN setup failed on client.
42	Client was unable to dynamically load a DLL.
43	Client attempt to unregister with WWAN interface failed because client had not registered.

Error Code	Error Description
47	Server encountered a problem calculating a Server Recovery Token (SRTK).
49	Client received an invalid SMS message
50	Client attempt to access an SMS message failed because no SMS messages were available.
51	Client attempt to access an SMS message failed because the message was intended for another recipient.
52	Server did not retry 3G lock due to exceeding number of send messages.
53	An error occurred when reading the SMS message.
54	The expected 3G module is not available.
55	The attempt to send the SMS message failed.

Glossary of Terms

Term	Description
Activation	An event when a device contacts the Absolute Monitoring Center for the first time through the Internet to obtain an unique Identifier.
Agent	A small software client which resides in the BIOS firmware of a device. It is either embedded at the factory or manually installed by a user.
Agent Call	A secure connection established between the Agent and the Absolute Monitoring Center through which device authentication or inventory data is sent.
Alert	A small software client which resides in the BIOS firmware of a device. It is either embedded at the factory or manually installed by a user.
Alert Event	A record of an alert that was triggered in Customer Center.
Application	The smallest unit of software installed on a device that is detected by the Agent and reported in Customer Center.
Asset Number	An alphanumeric identifier for a device which is entered by a Customer Center user.
Assigned	Entered and/or edited by a Customer Center user.
Authorization	A permission held by a Customer Center user to perform security operations, such as Data Delete or Device Freeze, after a signed pre-authorization agreement is received and filed by Absolute Software.
Authorization Code	A globally unique identifier which is e-mailed to a Security Administrator in response to a request made in Customer Center. The code is represented as a 32 character hexadecimal character string.
CTMWeb Application	Also known as CTMWeb.exe or Agent Management Utility, an application which allows a user to verify and manage the Agent's installation on a device.
Customer Center	A Web-based user interface which enables corporate customers to centrally manage all assets within the account.
Data Delete	A remote data deletion function that enables an authorized user to delete sensitive data on target devices in case of theft or loss. The function can also be performed at the end of life or lease of a device.
Data Delete Policy	A file created to enable users to specify files and/or file types to be deleted on target devices on the Windows platform. The file can also be used to delete registry key entries and/or files from registry key entries.
Department	A user-created attribute for a device which is included in the filter of many Customer Center reports.
Device	A piece of electronic communication hardware on which the Agent can be installed, such as Windows computers, Macintosh computers, or mobile handsets.
Device Freeze	A function managed in Customer Center which enables an authorized user to specify the devices to show a full screen message restricting device users from operating the device.

Term	Description
Detected	Identified by the Agent during the call to the Monitoring Center.
End User Messaging	A function managed in Customer Center which enables a user to specify the devices to show a message during the Agent call to the Monitoring Center. The content and rules for messages are customizable, and messages can also be used for data input from device users.
Export (Data/Group)	A function in Customer Center which enables users to download files containing information on device data or device groups in multiple formats.
Geofences	A function in Customer Center which enables users to specify boundaries of areas on a map and track devices based on Geolocation Tracking data.
Group	A logical collection of devices in Customer Center based on criteria such as geographical areas or departments. The group can be used to filter reports and target specific devices for many Customer Center functions.
Identifier	A unique Electronic Serial Number assigned to the Agent installed on a device.
Import (Data/Group)	A function in Customer Center which enables users to upload files containing information on device data or device groups in multiple formats.
Monitoring Center	A server with which the Agent makes a secure connection to send device authentication and inventory data.
Recovery	A service performed by the Absolute Theft Recovery Team to pinpoint the physical location of a stolen device and return it to the owner in collaboration with local police agencies.
Program	An executable file on a device that is detected by the Agent and reported in Customer Center.
Publisher	A company or organization selling applications that is detected by the Agent and reported in Customer Center.
Software Policy	A list of software requirements which consists of Banned, Required, and Approved software titles. A policy is applied to Device Groups to identify non-compliant devices.
Theft Report	A report available in Customer Center which is filled out and sent online by users to notify Absolute Software of a theft or loss of a device.
User-defined Field	An attribute for a device that can be created and edited by a Customer Center user. A type of a field can be, Date, Drop-down list or Text. Values for the fields are maintained by input from users.
Username	A unique name detected by the Agent to identify a person on a device.

Term	Description
Version	A number distinguishing releases of the same software application sold separately that is detected by the Agent and reported in Customer Center.
Volume Encryption	A function managed in Customer Center which enables an authorized user to specify the amount of data storage space on the hard disk that can be encrypted.

Index