Absolute User Guide

www.absolute.com

February 2023

ABSOLUTE®

Absolute User Guide, Absolute 7.x—Document Revision 18

Absolute Software Corporation
Suite 1400 Four Bentall Centre
1055 Dunsmuir Street
PO Box 49211
Vancouver, British Columbia
Canada V7X 1K8

Contents

Chapter 1: Introduction

Absolute® brings a fundamentally new approach to cybersecurity by enabling self-healing endpoint security to ensure uncompromised visibility and near real-time remediation of breaches at the source. Our cloud-based platform and embedded Persistence technology puts IT and security professionals in control of devices, data, and applications — whether they are on or off the network — to improve IT asset management, ensure compliance, protect data, and reduce insider threats. Patented Persistence technology is embedded in the firmware of more than 1 billion popular PC and mobile devices from global manufacturers including Acer, Asus, Dell, Fujitsu, HP, Intel, Lenovo, Microsoft, Panasonic, Samsung and Toshiba.

Absolute is an adaptive endpoint security solution. Its technology platform is a client/server architecture that delivers device security, data security, and asset management of endpoints, even if a device is off the network or in the hands of an unauthorized user.

The persistent connection between the secure and patented agent (client) and the Absolute Monitoring Center (server) ensures organizations have protected access to up-to-date information about their entire device inventory. Authorized users can use the built-in tools in the Absolute console to track devices and initiate data and device security operations for the purposes of enforcing compliance policies, identifying at-risk computers, and taking preemptive and reactive measures if a security incident occurs.

About this Guide

This document contains detailed information about various classic tools and functionality available to authorized users.

This section provides information on the following topics:

Audience

This guide provides instructions for system administrators who use the Absolute console to manage their IT assets (devices), to report missing or stolen devices, and to request and monitor data and device security operations. System administrators are assigned to the Security Administrator or Administrator user roles, depending on their organization's specific requirements.

Using this Guide

The *Absolute User Guide* is comprised of the following chapters:

- "Introduction" (this chapter) provides an overview of this document.
- "Setting Up Your Work Environment" describes the features included under the Administration section of the console, including procedures required to set up event alerts, and device groups.
- " Generating Reports" describes the procedures required to generate basic and customized classic reports based on the data collected from your managed devices.
- "Working with Reports" describes the classic reports, and how to run them and view the results.

- "Using Real-Time Technology" describes the Real-Time Technology (RTT) feature and provides tasks that are specific to using it.
- "Using Real-Time Technology over IP" describes the Real-Time Technology over Internet Protocol (RTT-IP) feature and provides tasks that are specific to using it.

Conventions Used in this Guide

The following conventions are used throughout the *Absolute User Guide*:

- Directory names, file names, field names, and UI objects are represented using bold; for example:
  - In Windows 7, the **notepad.exe** file 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 code and commands or statements are shown using the Courier typeface; for example:

  ```
  lanmake ctinst.txt
  ```
- Cross references to other locations within this user guide and hyperlinks are indicated in green text with an underscore; for example: see Conventions Used in this Guide. Clicking a cross reference takes you to that location in the guide.
- Throughout this guide, getting to the appropriate page in the quickest way is represented as follows:

  On the navigation bar click > **Alerts** to open the View and Manage Alerts page.
- The output that is generated by the information you enter in the Search Criteria area is presented in an area referred to as the **results** grid.

Chapter 2: Setting Up Your Work Environment

This chapter provides information on the following topics:

- Alerts
- Device Groups
- Software Policies
- Managing Account Settings
- Managing System Notifications

Alerts

The Alerts feature is used to notify Administrators of notable events regarding managed devices. For example, you may want to know if a device has not connected to the network for an unusually long period of time, potentially indicating a lost device that requires further investigation. In this example, you could use an alert based on the Last Call Time condition.

When you configure alerts for your organization, a managed device triggers an active alert, which then creates an alert event (basically a log file entry) and notifies you by email or pager according to the alert's settings. The e-mail or pager message contains a summary of the conditions that triggered the alert and a link to the Absolute console's home page. After an alert notification is sent, the alert is not triggered again for that device until the alert is reset. You configure the alert to have either a manual reset or an automatic reset after a specified period of time.

The Alerts feature is the foundation of the Suspicious Devices functionality. When you create an alert, you can assign a suspicion level value. A single alert event may seem unremarkable, however when multiple, seemingly insignificant alert events occur within a brief period of time, the activity becomes suspicious. When a device triggers one or more alerts for which you've assigned suspicion level values, these values are consolidated and, if the result exceeds your threshold, the alert events show on the Suspicious Devices Report (see "Suspicious Devices Report" on page 71.). You can use this report to view and manage a list of devices that have a high level of suspicious activity.

There are two types of alerts:

- **Predefined**: Absolute includes preconfigured (default) alerts that, when activated, notify you when certain events occur.
- **Custom**: You can also create user-defined alerts that use a single criterion or multiple criteria. These alerts can target or exclude a single device, or groups of devices.

Alerts have two states:

- **Active**: The alert scans your organization's managed devices for its alert conditions and logs alert events when found.
- **Suspended**: The alert is not scanning for its alert conditions and no alert events are logged. By default, all predefined alerts are in the Suspended state.

This section provides information about the following topics and tasks:

- About Predefined Alerts
- Creating New Custom Alerts
- Alerts
- Managing Alerts

- Managing Triggered Alert Events

About Predefined Alerts

The Absolute console includes numerous predefined alerts, which you can see on the View and Manage Alerts page described in the task, "Viewing Alerts" on page 14.

When the predefined alerts are activated, they perform as described in the following table. See "Activating Alerts" on page 15.

By default, all predefined alerts are configured for manual reset, but you can configure an alert to reset automatically after a specified number of days. See "Resetting Alerts" on page 16.

NOTE If you attempt to delete a predefined alert, it is recreated automatically in a **Suspended** state.

Predefined Alerts and their Descriptions

Predefined (Default) Alerts	Description
Agent Is Newly Installed	This alert is triggered when the agent is installed on a device. This alert should have a reset type of manual and should not be reset from the Alert Events page. Doing so results in alerts getting generated for new devices as they activate, but not re-sending alerts for previously activated devices.
Change in Serial Number	This alert is triggered when a serial number change is detected on a managed device. When this alert is configured to reset automatically, it tests for this condition every x days, where x is the defined frequency. **NOTE** If a managed device makes a call in which a serial number change is detected and then makes no calls for a period of time greater than x, it is possible for the alert to trigger more than once for the same device. When another call is made, however, causing the two most recent Alert Event records to not show a change in serial number, the alert stops triggering.
Device Name Changed	This alert is triggered when a device name change is detected on a managed device. It is set with a Suspicion level of 3.
Device Rebuild	This alert is used to proactively notify the administrator that a device may be stolen. It is set with a Suspicion level of 3 and is triggered when *both* of the following conditions are met: • Operating system product key is changed • Device has made a Self Healing Call
Hard Drive Nearly Full	This alert is triggered when the hard drive free space is less than or equal to 10% of the total hard drive size. This alert matches the results in the Hard Drive Space Available Report, if that report uses the same device group and setting of 10%. If this alert is configured to reset automatically, it tests for this condition every x days and triggers on the same devices each time until the hard drive space is cleaned to more than 10% available.

Predefined Alerts and their Descriptions (continued)

Predefined (Default) Alerts	Description
Last called 20 days ago	The trigger for this alert is the **Last Call Time** condition. If configured to reset automatically, this alert tests the condition every x days and triggers on the same devices each time until they make another call. In other words, when the device calls in, the alert no longer triggers for that device. It is best practice to configure this alert to reset automatically to keep constant track of your devices that fail to call in, even though this configuration may result in a large number of e-mail notifications.
Lease Ending	This alert compares the date in the **Lease End Date** condition to the settings configured for the alert. When the **Lease End Date** is less than or equal to 14 days from the current date, the default setting triggers an alert, which sends an e-mail message with a list of all devices that match this criteria. If this alert is configured to reset automatically, it re-sends the alert every x days, where x is the frequency configured in the alert settings. This alert continues to trigger when the **Lease End Date** has passed unless you reset it.
Local IP Address Changed	This alert is triggered when a Local IP Address change is detected on a managed device. It is set with a Suspicion level of 1.
Major Change	This alert is used to proactively notify the administrator that a device may be stolen. It is set with a highest Suspicion level of 5 and is triggered when *all* of the following conditions are met: ● Operating system product key is changed ● Device name is changed ● Username is changed ● Device has made a Self Healing Call
Modem Changed	This alert is triggered whenever there is a change in modem status between the second-to-last and the last calls made for a specific managed device. This alert does not indicate the date of the second-to-last call, however you can see it on the Call History Report. Because this alert compares the last two call dates for a particular managed device, resetting the alert could result in it getting generated more than once for a single device.
Network Changed	This alert is triggered when both the Local IP Address and the Public IP Address change on a device, which may indicate that the device is no longer on the network. It is set with a Suspicion level of 2.

Predefined Alerts and their Descriptions (continued)

Predefined (Default) Alerts	Description
New Program File Detected	Both new and updated applications trigger this alert. Regardless of the number of new applications installed on a specific managed device, this alert triggers once and does not trigger again until you reset it. If the alert is configured to reset automatically, it tests for the alert condition every x days, where x is the defined frequency. Because the condition is based on comparing the software detected date to the alert modified date, it triggers an alert on the same applications every x days unless the alert itself is changed and saved, thereby changing the modified date of the alert. However, if the alert is configured to reset manually, it only triggers once on a specific managed device until it is reset, even if a new application is installed subsequently.
Operating System Changed	This alert is triggered when an operating system change is detected on a device. This change may be attributed to reimaging of the device, but it may also indicate that the device is stolen. It is set with a Suspicion level of 2.
Operating System Product Key Changed	This alert is triggered when an operating system product key change is detected on a device, which may indicate that the device is stolen and the thief may have reformatted the device. It is set with a Suspicion level of 3.
Public IP Address Changed	This alert is triggered when a Public IP Address change is detected on a managed device. It is set with a Suspicion level of 1.
Self Healing Call	This alert is triggered when a device makes a Self Healing Call. It is used to notify an administrator that the agent on a device has been tampered with or removed from a device. The agent could have been temporarily removed during a normal IT process, but it could also signal a malicious attempt to remove the agent from the device. It is set with a Suspicion level of 3.
Username Changed	This alert is triggered when a username change is detected on a device, which may indicate that the device is being used by another user and it may be stolen. It is set with a Suspicion level of 3.
Warranty Ending	This alert compares the date in the **Warranty End Date** field to the settings configured for the alert. The default setting triggers the alert when the **Warranty End Date** is less than or equal to 14 days from the current date. When triggered, this alert sends an e-mail notification that includes a list of all devices that match the criteria. If this alert is configured to reset automatically, it re-sends the alert every x days, where x is the frequency configured in the alert settings. This alert continues to trigger after the **Warranty End Date** has passed until you reset it.

Creating New Custom Alerts

You can create alerts that meet your organization’s specific needs.

To create a new custom alert:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. On the View and Manage Alerts page click **Create alert ...**.
3. On the Create and Edit Alerts page in the **Alert name** field enter a meaningful name for the alert. This name shows in the **Alert Name** column in the **results** grid of the Alert Events page.
4. In the **Alert description** field enter a detailed description for this alert.
5. In the **Suspicion level** field open the list and select a severity level for suspicious events. Possible values range from **Not Suspicious** to the highest suspicion level of **5**.

   This value is shown on the Suspicious Devices Report, which highlights devices with suspicious activity. See "Suspicious Devices Report" on page 71.

   NOTE When setting suspicion levels, you need to consider the implications of the alert. For example, a lease ending is expected behavior, whereas replacing a hard drive could indicate a stolen device.

6. In the **Conditions** area define the conditions that trigger the alert.

   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 triggered by an agent call and you can only combine them with other conditions that have an asterisk.

   a) Open the **Field** list and select the appropriate value.
   b) Open the **Rule** list and select the appropriate value. This list includes all applicable rules for the field you selected in the **Field** list.
   c) Depending on your selections from the **Field** and **Rule** lists, the **Criteria** field may open.

      Do one of the following to provide the information for the **Criteria** field:

      - Type the appropriate value.
      - Click **Choose** to open a dialog that provides you with a list of all existing criteria. Click the appropriate value from the list. The dialog closes, and refreshes the Create and Edit Alerts page, populating the **Criteria** field with your selection.

   d) Click **Add Condition**. The page refreshes to show the new condition in the **Conditions** table.

      Repeat this step until all appropriate conditions are added.

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

7. In the **Scope** area, indicate which device groups meet the specified criteria and are included in, or excluded from, the alert you are creating.

   - In the **Includes** area, select the device that you want to include in the report as follows:
     - Open the **Devices in the group** list and select the device group to which this alert applies.

> **NOTE** If one or more of the devices in your selected device group were reported as stolen, the Alert does not apply to these devices.

  - Open the **Only where the** list and select the appropriate value. The values include **Any of the fields in this list**, **Identifier**, **Device Name**, **Username**, and **Serial Number**.
  - In the **is or contains** field enter the search criteria. You can also use **Choose** to select a value from the list of all existing criteria.

- In the **Excludes** area, select the devices that you want to exclude from the report:
  - Open the **Devices in the group** list and select the device group to which this alert does not apply.
  - Open the **Only where the** list and select the appropriate value. The values include **Any of the fields in this list**, **Identifier**, **Device Name**, **Username**, and **Serial Number**.
  - In the **is or contains** field enter the search criteria. You can also use **Choose** to select a value from the list of all existing criteria.

8. When a device triggers an alert, the same device cannot trigger the alert again until the alert event is reset for the single device or for all devices. Devices reported as stolen do not trigger an alert.

   At the **Alert Type** area define how the alert is reset for the device that triggered it:

   - To create an alert that you need to reset manually from the Alert Events page, select the **Manual reset** option.
   - To create an alert that resets automatically after a specific number of days, select the **Automatic reset after** option, and then enter a value in the **day(s)** field.

9. At the **Alert Option** area specify whether a single alert e-mail or multiple alert e-mails are sent when this alert is triggered by multiple devices.

   - To send a consolidated single e-mail message that provides details for each device that has triggered the alert, select the **Single e-mail** option.
   - To send an individual e-mail from each device that triggers the alert, select the **Multiple e-mails** option, which may result in a large number of e-mails.

10. At the **Action** area define how the alert is handled when it is triggered.

    Triggered alerts are logged for the Suspicious Devices Report. By default, Administrators are notified by email or pager message when an alert is triggered.

    You can set an alert so that no notifications are sent; for example, when you create an alert with low impact.

    - To send no notification when the alert is triggered select **Log event**.
    - To contact Administrators automatically using e-mail or pager messages when the alert is triggered select **Log event and notify**.
    - To send alert notifications by e-mail, in the **E-mail address** field enter one or more addresses. Separate multiple e-mail addresses with a semicolon.
    - To send alert notifications to an alpha-numeric pager, in the **Pager** field enter the destination pager address. You can enter multiple recipients by separating the addresses with a semicolon.

11. If you do not want to activate the alert at this time, select the **Suspend alert scanning** option.
12. Click **Save**.

    You are returned to the page from which you navigated to the Create and Edit Alerts page and are shown a confirmation message on that page.

Managing Alerts

You manage predefined and custom alerts in the same way, and you can perform the following tasks on both types of alerts:

- Viewing Alerts
- Searching for a Specific Alert
- Activating Alerts
- Editing Alerts
- Reactivating Suspended Alerts
- Resetting Alerts
- Suspending Alerts
- Deleting Alerts

Viewing Alerts

The View and Manage Alerts page shows a table that contains a record for all existing alerts, including the attributes and status for each alert.

NOTE You can apply an alert to a single device or to a device group, whereas *alert events* always apply to a single device.

To view existing alerts:

1. On the navigation bar click , click the **Rules** tab.
2. Click the **Go to the Classic Alerts Page** link at the bottom of the page.

   On the View and Manage Alerts page, the results grid shows all existing alerts, organized in the following columns:

   - **Alert ID** provides the identification number generated for the alert.
   - **Alert Name** is the name for this alert.
   - **Conditions** shows the conditions that are set for this alert.
   - **Scope Include** indicates the specified criteria for devices that trigger this alert.
   - **Scope Exclude** indicates the specified criteria for devices that are excluded from this alert.
   - **Suspicion Level** is the level of suspicion set for this alert. If no value exists a suspicion level was not set.
   - **Status** shows the device's current status.
   - **Type** indicates how the alert is reset after it is triggered, such as **Manual** or **Automatic** reset.

Searching for a Specific Alert

You can use the Search Criteria option to find a specific alert.

To search for a specific alert:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. On the View and Manage Alerts page, you can search as follows:
   - At the **Search Criteria** area open the **the Alert ID is** list and select the appropriate ID number.
   - In the **and the Alert Name contains** field, enter all or part of the alert name that you want to find.
   - Next to **and the Suspicion Level is**:
     i) Open the first list and select one of the following options:
        – **>** greater than
        – **>=** greater than or equal to
        – **=** equal to
        – **<=** less than or equal to
        – **<** less than
     ii) Open the second list and select a value from **0** to **5**.
3. Click **Show results** to regenerate the report using the defined criteria.

Activating Alerts

Predefined and custom alerts show in the **Suspended** state until you activate them.

To activate an alert:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. On the View and Manage Alerts page the list of alerts show in the results grid. Choose the alerts you want to activate in one of the following ways:
   - To activate one or more alerts, review the list of alerts and select the checkbox for each alert you want to activate.
   - To activate all alerts, select the checkbox in the heading row of the column next to **Alert ID**. All checkboxes in that column are now selected.
3. Click **Activate**.

   In the **results** grid the **Status** for the selected alerts is now **Active**.

Editing Alerts

You can edit both predefined and custom alerts.

To edit an alert:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. On the View and Manage Alerts page in the results grid, click the **Alert ID** for the alert you want to edit.

3. On the Create and Edit Alerts page, edit the values as described in step 3 through step 12 of the task, "Creating New Custom Alerts" on page 11.

Reactivating Suspended Alerts

You can reactivate alerts that you suspended; for example, full-disk encryption alerts if you decided to turn off full-disk encryption for a group of devices.

To reactivate suspended alerts:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. On the View and Manage Alerts page in the results grid, find the **Suspended** alert you want to reactivate and select its checkbox.
3. Click **Activate**.

Resetting Alerts

You can configure an alert to reset automatically or on-demand (manually) after the alert is triggered by a device. The device will not trigger the alert again until it is reset. Other devices will still trigger this alert.

To reset an alert:

1. On the navigation bar click , click the **Rules** tab, click the **Go to the Classic Alerts Page** link at the bottom of the page, and then do one of the following:
   - To reset an alert on all devices on which the alert was triggered:
     iii) On the View and Manage Alerts page select the checkbox for the **Active** alert you want to reset. You cannot reset a **Suspended** alert.
     iv) Click **Reset**.
     The alert is reset on all devices on which it was triggered.
   - To reset an alert on individual devices:
     i) Click **Alert Events**.
     ii) On the Alert Events page select the checkbox for the alert you want to reset. You can select multiple alerts.
     iii) Click **Reset**.
     The alert is reset on each associated device , as indicated in the Identifier column. The current date and time show in the **Reset Date** column

   NOTE If the conditions that initially triggered the alert are still present, the alert is triggered again and notification messages resume.

Suspending Alerts

There may be times when you want to suspend alerts. For example, if you are a school district and currently receive alerts from your managed devices when they do not call in every three weeks, you may want to suspend this alert during summer vacation.

To suspend an alert:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. You can suspend alerts in one of the following ways:
   - To create a custom alert in the **Suspended** state:
     i) Click **Create and Edit Alerts**.
     ii) Follow the instructions provided in the task, "Creating New Custom Alerts" on page 11.
     iii) At the bottom of the page, select the **Suspend alert scanning** checkbox.
     iv) Click **Save**. This alert is not scanned until you activate it.
   - To suspend one or more alerts:
     i) Click **View and Manage Alerts**.
     ii) In the results grid select the alerts you want to suspend in one of the following ways:
       - To suspend one or more alerts, review the list of alerts and select the checkbox for each alert you want to suspend.
       - To suspend all alerts, select the checkbox in the heading row of the column next to **Alert ID**. All checkboxes in that column are now selected.

     iii) Click **Suspend**. In the results grid the **Status** for the selected alerts is now **Suspended**.

Deleting Alerts

You can delete alerts that you, or other users, have created. However, if you attempt to delete a predefined alert, it is recreated in a **Suspended** state.

To delete an alert:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. On the View and Manage Alerts page in the results grid, find the alert you want to delete and then do one of the following:
   - Select the checkbox for the alert and click **Delete**.
   - Click the link under the **Alert ID** column and on the Create and Edit Alerts page, click **Delete**.
3. A warning dialog opens indicating that if you delete this alert, you also delete all records (such as alert events) associated with it.

   Click **Continue** to delete this alert.

   NOTE If the alert you deleted was a predefined alert, its status is updated to **Suspended** and it shows at the bottom of the **results** grid with a new **Alert ID**.

Managing Triggered Alert Events

This section provides the following information and tasks:

- Viewing Triggered Alert Events
- Downloading Alert Events

Viewing Triggered Alert Events

The Alert Events page shows a table (results grid) that contains records of the alerts that were triggered for each device.

NOTE By default, seven days of information shows in the results grid. You can change what shows based on the dates set in the **and the Event occurred** area.

To filter and view alert events:

1. On the navigation bar click , click the **Rules** tab, and then click the **Go to the Classic Alerts Page** link at the bottom of the page.
2. Click **Alert Events**.
3. On the Alert Events page, at the **Search Criteria** area, set the preferred filtering and display options using one or more of the following criteria:
   - To filter your results by a specific alert event, do the following:
     i) Open the **the field** list and select one of the following values:
        - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click an **Identifier** shown in the **results** grid to open that device's Device Summary page.
        - **Device Name**: the name assigned to the device in the operating system.
        - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
        - **Alert Id**: the identification number generated for the alert
        - **Alert Name**: the name for the alert.

     ii) In the **is or contains** field, enter a value.
   - To filter your results by the suspicion level, do the following:
     i) Open the list next to **and Suspicion Level** and select one of the following:
        - **<** for a value that is less than
        - **<=** for a value that is less than or equal to
        - **=** for a value that equals
        - **>=** for a value that is greater than or equal to
        - **>** for a value that is greater than

     ii) Open the second list and select a value from **0** to **5**.
   - To filter your results by the date when the alert event was triggered, at the **and the Event occurred** area, do one of the following:
     - Click the **in the last <n> days** option and enter the appropriate number of days in the field. Values from **1** through **365** are supported. A higher value results in a larger report that takes longer to generate.
     - Click the **between** option and enter the start and end dates (dd/mm/yyyy). Alternatively, click the **Calendar** icon next to each date field to open the calendar dialog. Enter the start date in the first date field and the end date in the second.
4. Click **Show results**. The results grid refreshes to show the list of alerts that were triggered and had notifications sent by e-mail. The following data is returned according to your filtering choices:

- **Alert Id** is the identification number generated for the alert
- **Alert Name** is the name for this alert.
- **Identifier** is the unique identifier (electronic serial number) for this device.
- **Username** is the user who was logged in to this device.
- **Device Name** is the name of this device.
- **Reset Date** indicates the date this alert was reset so it continues to trigger the alert.
- **Last Event** indicates the date and time of the last alert event for this device.
- **Suspicion Level** is the level of suspicion set for this alert. No value in this cell indicates that no suspicion level was set.
- **Status** indicates whether the alert is **Active** or **Suspended**.

Downloading Alert Events

The Alert Events page shows a table (results grid) that contains records of the alerts that were triggered for each device.

NOTE By default, seven days of information show in the results grid. You can change what shows based on the dates set in the **and the Event occurred** area.

To download alert events:

1. Complete the task, "Viewing Triggered Alert Events" on page 18.
2. In the results grid, select the appropriate alert events you want to download by doing one of the following:
   - To select one or more alert events, review the list of alert events and select the checkbox for each alert event you want to download.
   - To select all alert events, select the checkbox in the heading row of the column next to **Alert Id**. All checkboxes in that column are now selected.
3. At the top of the results grid click  .
4. On the Request Report: Alert Events page, in the **Report Name** field, enter a name for this report you want to download.
5. Open the **Report Format** list and select a file format.
6. At the **Create E-mail Alert** area, if you want to receive e-mail notification when the file is available, enter your e-mail address in the **Your E-mail Address** field.
7. Click **Continue**.

You will receive an e-mail when your report is generated. You can retrieve the report file from the My Reports page. For information on retrieving reports, see "Downloading Reports" on page 56.

Device Groups

You can organize your managed devices into logical groupings that fit your business model. For example, you can group computers by management levels, security risk assessment (those laptops that contain confidential data), geographical locations (such as building, floor, or room the computers are in), and other criteria.

The Device Groups page has a filter area at the top of the page and a table (results grid) that includes all device groups associated with your account. You can use the Search Criteria filters to locate the device group, or device groups, you want to view.

You can define groups when filtering reports or targeting devices for alerts or other actions.

This section describes the following tasks:

- Creating a New Device Group
- Viewing a Device Group
- Editing a Device Group
- Managing Devices in a Device Group
- Deleting Device Groups

IMPORTANT All tasks, except for the viewing ones, require that you log in to the Absolute console as an Administrator.

Creating a New Device Group

To create a new device group:

1. On the navigation bar, click  to open the Assets > Devices page.
2. On the sidebar, click **Classic Groups**.
3. On the Device Groups page, click **Create new Device Group**.
4. On the Create and Edit Device Group page, at the **Group information** area, do the following:
   a) In the **Group Name** field, enter a name for the new device group. Click the **Check name availability** link to verify that the name you created is not in use.
   b) In the **Group Description** field, enter a description for the device group.
   c) To ensure that only Administrators can change this information, at the **Group information** area, click the **Lock as Read-Only** checkbox. However, for the purposes of this task, unless you are an Administrator or Security Administrator, do not select this checkbox. If this checkbox is activated, you cannot perform step 5 of this task.
   d) Click **Save group information** to save your device group information and to refresh the Create and Edit Device Group page. You see a confirmation line that the device group was created successfully.

   NOTE When first created, device groups do not have any devices associated with them.
5. To add devices to this group, at the **Group Members** area do one of the following:
   - To select the devices you want to add to this device group from a list, click **Add Devices**.
     i) On the Choose Device(s) to add to the group dialog, do one of the following to select the devices:
        - Select the checkbox next to each device you want to add to the group.
        - Select the **Select All** checkbox to select all devices that show on this page of the table.
     ii) Click **Choose device(s)**. The Choose Device(s) to add to the group dialog closes.

On the Create and Edit Device Group page, you see a confirmation line stating the device was added successfully to this group.

Also, the **results** grid refreshes and shows the devices you added, with specific information for each device in the following columns:

- **Identifier**, which is a unique Electronic Serial Number assigned to the agent installed on each device you selected.
- **Department** to which this device belongs. A Departments is a user-created attribute for a device that is included in the filter of many reports.
- **Device Name**, which is the name given to a device.
- **Username**, which is a unique name detected by the agent that identifies a person who is associated with or using a device.
- **Make**, which is the manufacturer of a device.
- **Model Number**, which is the product type of a device.
- **Serial Number**, which is the serial number of the device.
- **Asset Number**, which is an alphanumeric identifier for a device entered by a user.

NOTE You can sort the results in ascending and descending order for each column, except the contents in the **Identifier** column.

iii) Above the **results** grid, in the field next to the **Filter Members** button, you can filter the list shown in the **results** grid by entering one of the following items for a device:

- **Identifier**, which is a unique Electronic Serial Number assigned to the agent installed on each device you selected.
- **Device Name**, which is the name given to a device.
- **Username**, which is a unique name detected by the agent that identifies a person who is associated with or using a device.
- **Serial Number**, which is the serial number of the device.

Click **Filter Members** and the **results** grid refreshes to show a list of devices based on your filter selection.

- To add devices to the group by manually specifying devices in a text file, click **Upload a List of Devices**.

IMPORTANT Lenovo serial numbers with seven characters may be associated with more than one device and may cause errors when you upload a list of devices using a text file. When uploading a list of Lenovo devices, use complete serial numbers or the device **Identifiers**, both of which are unique to each managed device.

i) On the Upload List of Devices for Device Group dialog, under the **Upload List of Serial Numbers or Identifiers** area, in the **File Path** field, click **Browse** and find the location of the file you want to upload.

You can enter a list of devices in a single column, separating each entry with a return (press `Enter`). Do not use any punctuation. Click **Open** to select this file path.

ii) In the **File List Type** area, click one of the following options:

- **Serial Numbers**
- **Identifiers**

iii) Click **Upload File**. Follow the instructions provided on-screen to continue with this procedure.

The devices are added to the device group.

6. Click **Back** to show the Devices sidebar.

Viewing a Device Group

To use filters to locate and view a specific device group:

1. On the navigation bar, click  to open the Assets > Devices page.
2. On the sidebar, click **Classic Groups**.
3. On the Device Groups page, filter your data to show a specific device group using the **Search Criteria** fields as follows:
   - In **the Group Name is or contains** field, enter the name of the device group you want to view.
   - In the **and Group Description is or contains** field, enter several letters that you know are in the device group's description that you want to view.
   - Open the **or the group contains a Device where the field** list and select the appropriate field from the following:
     - **Any Field**
     - **Identifier**
     - **Device Name**
     - **Username**
   - In the **is or contains** field, either use **Choose** or enter the appropriate value for the device group you want to view.
4. Click **Show results** to refresh the **results** grid. If you are logged in as a Power User or a Guest, only those device groups to which you are assigned are included in the results.

   The columns provide the following information:

   - **Device Group Name** is the name of the group.
   - **Count** shows how many devices are in this group,
   - **Description** for this group, which you provided when you created it.
   - **Created By** shows who created this group.
   - **Last Modified** provides the date that this device group was created or when it was edited last.
5. Click **Back** to show the Devices sidebar.

Editing a Device Group

To edit a device group's information:

1. Complete the task, "Viewing a Device Group" on page 22.
2. Open the Create and Edit Device Group page with the details of the device group that you want to edit in one of the following ways:

- Filter the **results** grid to show a particular device group.
- In **results** grid, click the **Device Group Name** link for the device group you want to edit.

3. At the Group information location, you can edit the following details:

   a) In the **Group Name** field, enter a different name for this group. Click the **Check name availability** link to verify that the name you want to use is not already used.

   b) In the **Group Description** field, edit an appropriate description for the group, if you want to change it.

   c) Select or clear the **Lock as Read-Only** checkbox.

   d) Click **Save** to save your changes to the Group information and refresh the Create and Edit Device Group page.

   You see a confirmation line that the device group was updated successfully.

4. If you want to add more devices to this device group, see "Adding Devices to a Device Group" on page 23.

   You can also remove selected devices from the group. For more information, see "Removing Devices from a Device Group" on page 29.

Managing Devices in a Device Group

You can use the Device Group page to manage Device Group memberships, which includes the following tasks:

- Associating Devices with Device Groups
- Viewing Devices in a Device Group
- Removing Devices from a Device Group

Associating Devices with Device Groups

After you have created a device group, you can add devices to it.

NOTE A device can belong to more than one device group.

There are several ways to associate devices with device groups, including:

- Adding Devices to a Device Group
- Adding Devices to a Device Group Automatically Based on Local IP Addresses
- Using Bulk Uploads to Change Device Group Associations

Adding Devices to a Device Group

To add devices to a device group:

1. Complete the task, "Viewing a Device Group" on page 22.
2. In the **results** grid of the Device Groups page, click the **Device Group Name** to which you want to add devices.
3. To add devices to this group, at the **Group Members** area do one of the following:
   - To select the devices you want to add to this device group from a list, click **Add Devices**.

i) On the Choose Device(s) to add to the group dialog, do one of the following to select the devices:
   - Select the checkbox next to each device you want to add to the group.
   - Select the **Select All** checkbox to select all devices that show on this page of the table.

ii) Click **Choose device(s)**. The Choose Device(s) to add to the group dialog closes.

On the Create and Edit Device Group page, you see a confirmation line stating the devices were added successfully to this group.

Also, the **results** grid refreshes and shows the devices you added, with specific information for each device in the following columns:

- **Identifier**, which is a unique Electronic Serial Number assigned to the agent installed on each device you selected.
- **Department** to which this device belongs. A Departments is a user-created attribute for a device that is included in the filter of many reports.
- **Device Name**, which is the name given to a device.
- **Username**, which is a unique name detected by the agent that identifies a person who is associated with or using a device.
- **Make**, which is the manufacturer of a device.
- **Model Number**, which is the product type of a device.
- **Serial Number**, which is the serial number of the device.
- **Asset Number**, which is an alphanumeric identifier for a device entered by a user.

NOTE You can sort the results in ascending and descending order for each column, except the contents in the **Identifier** column.

iii) Above the **results** grid, in the field next to the **Filter Members** button, you can filter the list shown in the **results** grid by entering one of the following items for a device:
   - **Identifier**, which is a unique Electronic Serial Number assigned to the agent installed on each device you selected.
   - **Device Name**, which is the name given to a device.
   - **Username**, which is a unique name detected by the agent that identifies a person who is associated with or using a device.
   - **Serial Number**, which is the serial number of the device.

   Click **Filter Members** and the **results** grid refreshes to show a list of devices based on your filter selection.

- To add devices to the group by manually specifying devices in a text file, click **Upload a List of Devices**.

IMPORTANT Lenovo serial numbers with seven characters may be associated with more than one device and may cause errors when you upload a list of devices using a text file. When uploading a list of Lenovo devices, use complete serial numbers or the device **Identifiers**, both of which are unique to each managed device.

i) On the Upload List of Devices for Device Group dialog, under the **Upload List of Serial Numbers or Identifiers** area, in the **File Path** field, click **Browse** and find the location of the file you want to upload.

You can enter a list of devices in a single column, separating each entry with a return (press `Enter`). Do not use any punctuation. Click **Open** to select this file path.

ii) In the **File List Type** area, click one of the following options:

- **Serial Numbers**
- **Identifiers**

iii) Click **Upload File**. Follow the instructions provided on-screen to continue with this procedure.

The devices are added to the device group.

Adding Devices to a Device Group Automatically Based on Local IP Addresses

You can assign devices to device groups automatically, based on the devices' local calling IP address. This feature is useful if your network includes multiple subnets, each with a range of local IP addresses.

The following rules apply:

- When a device calls the Monitoring Center and its IP address is within the IP range specified for a device group, it is assigned to the device group associated with that subnet.
- When a device calls in from an IP address that is not part of a range specified in a device group, the device is not assigned to any group.
- When 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.
- When 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 that device group associated with that subnet.

Example

A school district is using the Absolute technology. The following auto-grouping rules are defined for two high schools in the district:

- **Auto-group Lincoln High School**: local IP subnet 172.165.50.*
- **Auto-group Washington High School**:local IP subnet 172.165.60.*

If a teacher's computer calls in with the IP **172.165.50.25**, 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 **123.134.75.13**. There is no auto-group rule for that IP subnet, so the computer stays in the Lincoln High School group.

However, if the teacher then takes the computer to **Washington High School** for a few days, and it calls in from **172.165.60.150**, the computer gets unassigned from the Lincoln High School group and assigned to the Washington High School group. Unlike the teacher's IP address at home, there is an auto-group configured for that IP (Washington High School), so the computer is moved.

To use the auto-grouping feature to add devices to a device group automatically:

1. Create a CSV (comma separated value) file or spreadsheet as follows:
   a) The first row must be the column headings **GroupName** and **IPSubnet**.

b) Subsequent rows should include the “<device group names>” that you want to use, a comma (,) as the separator, and the associated local IPSubnet.

Use the asterisk (*) as a wild card to group devices calling from different local subnets, as shown in the following example:

```
GroupName,IPSubnet
"Device Group Name 1",192.168.*.*
"Device Group Name 2",172.16.*.*
"Device Group Name 3",10.*.*.*
```

c) Choose the appropriate option to save the file to your local device.

2. Upload the CSV file prepared in the preceding step as follows:

a) On the quick access toolbar, click and click **Import Classic Group <-> IP Mapping**.

The on-screen instructions provide both guidance about creating a spreadsheet and a sample file you can view. You created this file in step 1.

b) In the **Name** field, enter an appropriate name for your import. This name is used to track the status of the CSV file import.

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

d) In the **Filename** field, click **Browse** to open the Choose File to Upload dialog and complete the following steps:

i) Browse to the location where you saved the edited CSV file earlier in step 1.

ii) Click the file you want to upload and then click **Open** to select the file.

The Import Groups page opens to show the path to the selected file in the **Filename** field. Click **Upload**.

NOTE CSV file imports are queued and processed in the background. You can track the progress of your import using the Import Group <-> IP Mapping Status page, described next.

3. Verify that the CSV file was imported successfully:

a) On the navigation bar, click  and click **Import/Export** on the Settings sidebar.

a) On the Import/Export sidebar, click **Import Classic Group <-> IP Mapping Status**.

b) On the Import Group <-> IP Mapping Status page in the table, review the import **Status**.

When the import process is complete, the status reads **Ready**. If you entered an e-mail address, notification is sent.

c) 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 that indicate the success of the import line by line.

NOTE For more information, see *Technical Note 050221 – Dynamic Group to IP Subnet Mapping* on the Documentation page.

Using Bulk Uploads to Change Device Group Associations

Manipulating device group associations with large numbers of devices can be an arduous process. To make things easier and quicker, you can extract information from the Absolute console, manipulate it, and then upload the changes back to the Absolute console.

You can associate each device to a maximum of 20 different device groups, as follows:

- Download a CSV file of devices and their current Device Group associations.
- Edit the CSV file to update the device group associations. You can remove any devices whose device group associations are not changing.
- Upload the CSV file to the Absolute console, which updates the device group associations.

To extract, edit, and upload device group associations:

1. On the quick access toolbar, click and click **Export Classic Groups** to open the Export Groups page.
2. Request a download of devices in a current device group, as follows:
   a) At the Search Criteria location, in **The Group is** field, open the list and select the appropriate device group.

   IMPORTANT Ensure the download includes all of the devices that you want to manipulate. After you have extracted the information you cannot add more devices to the exported CSV file. If necessary, downloading the All Devices group ensures you have every managed device in the CSV file.

   b) At the Name and Format location, do the following:
      i) In the **Name** field, enter an appropriate name. This name shows on the Export Group Status page.
      ii) Open the **Format** list and select **CSV** because you can only import a CSV file.
   c) At the **Create E-mail Alert** area, if you want to receive e-mail notification when the file is available, enter your e-mail address in the **Your E-mail Address** field.
   d) Click **Continue**, which refreshes the Export Groups page that provides information about being notified when the report is ready.
3. Retrieve the downloaded CSV file you just requested as follows:
   a) On the navigation bar, click  and click **Import/Export** on the Settings sidebar.
   b) On the Import/Export sidebar, click **Export Classic Group Status** to open the Export Groups Status page.
      If you entered an e-mail address in the preceding step, you can also click the link on the message you received.
   c) When your request is processed, in the table under the **Status** column click the appropriate **Ready** link.
   d) Follow the on-screen instructions to **Open** the CSV file. If prompted, choose the option to **Save** the file to your local device.

IMPORTANT You can open the CSV file with almost any text editing program. However, Absolute 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.

e) Edit the extracted CSV file, as follows:

IMPORTANT Do not alter the format of the CSV file. Doing so causes the data import process to fail.

- The first few columns for each row contain the device's **Identifier**, **Username**, **Device Make**, and **Device Model**.
- Use these columns for identification purposes only. **Do not edit them**.
- Columns named **Group1** through **Group20** contain the group associations that you can edit. Enter precise group names (case-sensitive and accurate spelling) to *associate* the device with a device group. You can *disassociate* a device from a device group by removing the value.
- You can remove rows for devices that you are not editing.
- You cannot add rows for devices in the CSV file.

f) Save the edited CSV file to the preferred location.

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

4. Upload the edited CSV file, as follows:

a) On the quick access toolbar, click and click **Import Classic Groups** to open the Import Groups page.

b) In the **Name** field, enter a name for your import file. This name is used to track the status of the CSV file import.

NOTE CSV file imports are queued and processed in the background. You can track the progress of your import using the **Import Groups Status** page.

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

d) In the **Filename** field, click **Browse** to open the Choose File to Upload dialog and complete the following steps:

i) Browse to the location where you saved the edited CSV file.

ii) Click the file you want to upload and then click **Open** to select it.

The Import Groups page shows the path to the selected file in the **Filename** field.

e) To specify whether to retain or remove existing group membership, select one of the following options:

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

- **Delete Identifier Group Membership If Group Missing From Import** removes a device's existing group associations if they are not included 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. The Import Groups page refreshes to provide information that your file uploaded successfully. The file is queued for processing.

5. Verify that the CSV file was processed successfully:
   a) On the navigation bar, click  and click **Import/Export** on the Settings sidebar.
   b) On the Import/Export sidebar, click **Import Classic Group Status**.
   c) On the Import Groups Status page in the table, review the import **Status**.
   When complete, the status is **Ready**. If you entered an e-mail address, notification is sent.
   d) To verify the success of the import, click the **Ready** link to open a CSV file that reports the processing success or failure by device.
   This file is identical to the CSV file you uploaded, with the addition of two columns indicating the success or failure of the import line by line.

Viewing Devices in a Device Group

To view the devices in a device group:

1. Complete the task, "Viewing a Device Group" on page 22.
2. On the Device Groups page look at the **results** grid, which shows all device groups.
3. To see what devices are in a particular device group, click the appropriate device group name link, which opens the Create and Edit Device Group page.
4. Look at the **results** grid, where you find a list of all devices that you assigned to this device group.
5. If you want to review the details for a particular device, click the **Identifier** link. For more information, see "Editing Asset Information" on page 48.

Removing Devices from a Device Group

To remove any or all devices from a device group:

1. Complete the task, "Viewing a Device Group"
2. On the Device Groups page, use one of the following methods to open the Create and Edit Device Group page with the details of the device group that you want to edit:
   - Filter the **results** grid to show the particular device group that you want to remove.
   - In the **results** grid, click the **Device Group Name** link for the device group that you want to remove.
3. On the Create and Edit Device Group page use one of the following ways to select the device or devices you want to remove:
   - From the **Select All** column, select the checkbox for each device you want to remove from the device group.

- Select the checkbox in the heading row of the **Select All** column to select all devices showing in the **results** grid.

4. Click **Remove Selected Device(s)**.

   The Create and Edit Device Group page refreshes with a confirmation message that provides the **Identifiers** for each device you removed.

Deleting Device Groups

To delete a device group:

1. Complete the task, "Viewing a Device Group"
2. Ensure that no users are assigned to the device group you want to delete.
3. On the Device Groups page in the **results** grid, click the **Device Group Name** link for the device group you want to delete.
4. On the Create and Edit Device Group page, click **Delete this group**.

   A confirmation dialog opens with a warning that all associations to the device group will also be deleted. This means that the group is no longer shown in report filters and any alerts applied to the device group no longer function.
5. Click **Delete this group**.

NOTE If any users are assigned to the device group that you want to delete, a warning message shows and you cannot delete the device group. The message includes the list of assigned users. Before you can delete the device group you need to reassign these users to another device group.

Software Policies

Software policies allow Administrators to define their organization's software rules. A software policy is a list of Banned and Required software titles.

A single device may belong to multiple device groups, so it is possible for multiple software policies to apply to a single device.

This section describes the following tasks:

- Viewing the List of Software Policies
- Viewing Device Groups Without a Software Policy
- Creating a Software Policy
- Copying a Software Policy
- Viewing a Software Policy
- Editing a Software Policy and its Device Group Associations
- Deleting a Software Policy

IMPORTANT All tasks require that you log in to the Absolute console as an Administrator.

Viewing the List of Software Policies

To view the software policies that apply to device groups:

1. On the navigation bar click > **Policy Groups** > **Software Policies**.
2. On the View and Manage Software Policies page, the table shows the following information about your existing software policies:
   - **Policy Name** is the name of the policy.
   - **Created By** is the username for the person who created the policy.
   - **Created At** is the date and time when the policy was originally created.
   - **Last Updated By** is the username of the last person who edited the policy.
   - **Last Updated At** is the date and time stamp when this policy was last edited.
   - **Group Count** indicates the number of device groups to which this policy applies. Click the link to open the Device Groups Added to <Policy Name> Software Policy dialog.
   - The **Edit** link opens the Create and Edit a Software Policy page for each policy.

Viewing Device Groups Without a Software Policy

To view a list of device groups that do not have a software policy:

1. Complete the task, "Viewing the List of Software Policies" on page 31.
2. Click **View groups without a policy**, which opens the Software Policy: Groups Without A Policy dialog.
3. The table shows those device groups that do not have software policies applied to them and the **Number of Devices** this situation affects.
4. Click **Print** to print the list.

You can now assign a software policy to the appropriate device groups as instructed in one of the following locations:

- To create a new software policy and apply it to a device group without a policy, complete the task, "Creating a Software Policy" on page 31.
- To apply an existing software policy to a device group without a policy, complete the task, "Editing a Software Policy and its Device Group Associations" on page 33.

Creating a Software Policy

To create a software policy:

1. On the navigation bar click > **Policy Groups** > **Software Policies**.
2. Click **Create software policy...** to open the Create and Edit a Software Policy page.
3. In the **Policy Name** field, enter a descriptive name for the policy.
4. In the **Description** field, enter a brief description of the policy.
5. At the right side of the **Policy Groups** field, click **Add Classic Groups** to open the Choose Classic Groups for Software Policy dialog.
6. In the **Available** list, select the appropriate device groups, as follows:

NOTE The list includes Classic device groups only. Any device groups created in > **Device Groups** are not listed.

a) To filter the **Available** list, in the **Filter** field enter the criteria that you want to use and click **Show results**.
b) Select the device groups you want to include in the software policy and click **>** to move a single device group to the **Selected** list.
c) Click **>>** to move all available device groups to the **Selected** list.
d) Click **All Devices** to select all device groups.

NOTE If you mistakenly move an available device group to the **Selected** list, you can select the device group and click **<** to move it back to the **Available** list.

e) When finished, click **OK**.
The Create and Edit a Software Policy page refreshes with an updated list of the selected device groups in the **Policy Groups** field based on your selections.

7. Define the **Banned Items** for the software policy as follows:
a) Click the **Banned Items** tab and click **Add**.
On the Choose Software Licenses or Executable Programs dialog, the list shows all available Publisher and Applications by default. You can use the filter to search the database to reduce the list, which makes it easier to find the application you want.
b) To filter the list, do the following:
i) In the **Filter** field enter part or all of a **Publisher** or **Applications** name.
ii) Select the appropriate option to show licenses and/or executables:
- **Show Licenses Only**
- **Show Executable Programs Only**
- **Show Both Licenses and Executable Programs (recommended)**
- **Show Version Independent Licenses/Executables**
- **Show Version Specific Licenses/Executables**

iii) To see only the licenses installed on your organization's devices, click the **Show Only Licenses or Executable Programs Installed On Your Organization's Devices** checkbox.
iv) Click **Filter**.
c) Add one or more applications to the **Banned List**:
i) Under the **Publisher** column, click a specific name to show all applications for that publisher in the **Applications** column.
ii) Select applications to add as follows:
- To select one application, click an **Applications** name and click **>** to move a single application to the **Selected** list.
- To select all applications from a publisher, click **>>** to move all available applications to the **Selected** list.
- To remove an application from the **Selected** list, click the name in that list and then click **<** to move it to the **Applications** list.

- To remove all applications from the **Selected** list, click **<<** to move them all to the **Applications** list.

iii) Click **OK**.

8. Define the **Required Items** for the software policy as follows:
   a) Click the **Required Items** tab and click **Add**, which opens the Choose Software Licenses or Executable Programs dialog.
   b) The process of filtering the list and adding applications to the **Required Items** list is identical to the process described for the **Banned Items** list. For more information, see step 7.
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.

Copying a Software Policy

To create a new software policy by copying an existing one:

1. On the navigation bar click > **Policy Groups** > **Software Policies**.
2. On the sidebar, select the software policy that you to copy.
3. On the Create and Edit a Software Policy page, click **Copy** to create a new software policy.

   The Create and Edit Software Policy page refreshes showing the new policy. The words “Copy of” are appended to the name of the copied software policy.
4. Edit the Software Policy as appropriate. See "Editing a Software Policy and its Device Group Associations" on page 33.

Viewing a Software Policy

To view a software policy:

1. Complete the task, "Viewing the List of Software Policies" on page 31.
2. Find the **Policy Name** of the policy you want to view and click the corresponding **Edit** link.

Editing a Software Policy and its Device Group Associations

To edit an existing software policy and its the associated device groups:

1. On the navigation bar click > **Policy Groups** > **Software Policies**.
2. On the sidebar, select the software policy that you to edit.
3. On the Create and Edit a Software Policy page, edit the Software Policy as follows:
   - In the **Policy Name** field, edit the existing name as appropriate.
   - In the **Policy Description** field, edit the description as appropriate.
4. To add more device groups to this software policy, do the following:

a) In the **Policy Groups** field, you can add this software policy to more groups by clicking **Add**.
b) On the Choose Groups For Software Policy dialog, ensure that the appropriate device groups are moved from the **Available** list to the **Selected** list.
c) Click **OK** to make the changes to the **Policy Groups**.

5. To remove a device group from this software policy, in the **Policy Groups** field, select the appropriate device group and click **Remove**.
6. To add or remove software titles from the **Banned Items** and **Required Items** software lists, perform the instructions provided in step 7 of the task, "Creating a Software Policy" on page 31.
7. Do one of the following:
   - Click **Save & Close** to save your changes, and return to the View and Manage Software Policies page.
   - Click **Save** to save your changes, and remain on the updated Create and Edit a Software Policy page.
   - To export the information for this software policy to a spreadsheet, click **Export to Excel**. Do one of the following:
     - Click **Open** to show the contents of this software policy in Microsoft Excel.
     - Click **Save** to save the spreadsheet and open it later.

Deleting a Software Policy

To delete a software policy:

1. Complete the task, "Viewing a Software Policy" on page 33.
2. Select the appropriate Software Policy and click **Delete**.

IMPORTANT **Exercise caution**. When you click **Delete**, the policy is deleted without prompting you for confirmation.

Managing Account Settings

The Classic Account Settings section is where you configure settings that apply to your entire account and the managed devices within it. For example, you can set your default locale and time zone, edit the automatic assignment of devices under the Service Guarantee, and turn on or turn off the features, such as Event Calling.

NOTE To configure settings for Single Sign-on or Two-Factor Authentication, go to the Administration > Account Settings page. For more information, see the online Help.

This section provides information on the following topics:

NOTE You must log in to the Absolute console as an Administrator to perform these tasks. Power Users and Guests can view existing account settings, but they cannot edit them.

Editing Classic Account Settings

To edit your Classic Account Settings:

1. On the navigation bar click > **Classic Account Settings**.
2. To change the default language and time display formats showing across all pages in the Absolute console select a value from the **Default Language and Locale** list.
3. To show local times across all pages in the Absolute console select a value from the **Default Timezone** list.
4. The **Automatically assign available Service Guarantee Licenses to devices** checkbox is selected by default. It controls whether available Service Guarantee licenses are assigned automatically to *newly activated* devices. To turn off auto-assignment of licenses, clear the checkbox.

   For more information about Absolute products with a Service Guarantee, see "Managing Service Guarantee Licenses" on page 36.

   NOTE Auto-assignment of licenses applies to new devices only. If a Service Guarantee license becomes available and an *existing* device is unlicensed, the license is not automatically assigned to the device. To assign a license to an existing device, see "Manually Editing Service Guarantee License Assignment" on page 37.

5. At the **Full Disk Encryption Status** area, do one of the following:
   - To turn on full-disk encryption data collection from the devices in your account, select the **Collect full disk encryption data from devices** checkbox.

     NOTE Full-disk encryption data collection is supported for Windows and Mac devices only. When data collection is turned on, the collection process starts when the device makes its next agent call. Therefore, depending on the agent's call frequency, the Full-Disk Encryption Status Report may be updated within a timeframe from several minutes up to 24 hours.

   - To stop collecting data about full-disk encryption from your devices, clear the **Collect full disk encryption data from devices** checkbox. This action does not delete any current or historical data, however encryption alerts are suspended automatically.
   - If you want to turn on full-disk encryption data collection again, enable this setting and manually activate the encryption alerts. For more information, see "Reactivating Suspended Alerts" on page 16.

   For more information about full-disk encryption, see "Full-Disk Encryption Status Report" on page 74.

6. At the **Absolute Secure Drive** area, do one of the following:

- To turn on data collection, select the **Collect Absolute Secure Drive Failed Login data from devices** checkbox. For more information, see "Absolute Secure Drive Authentication Failures Report" on page 73.

  NOTE By default, data collection for Absolute Secure Drive Failed Logins is turned on for all accounts.

- To turn off data collection, clear the **Collect Absolute Secure Drive Failed Login data from devices** checkbox. The data collected before turning off this option is not deleted and continues to show on the Absolute Secure Drive Authentication Failures Report. For more information, see "Absolute Secure Drive Authentication Failures Report" on page 73.

7. If you want your managed Windows devices to log the date and time when a file was last accessed, in the **Last Access Time Stamp** area, select the checkbox next to **Enable last file access date and time stamps (Windows devices only)**.

   NOTE For Mac devices, no setting is required. Last file access dates and times are always logged and included in the Deletion log file.

   NOTE On supported Windows devices, the following registry key controls the logging of file access time stamps:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate`
   By default, this registry key is set to "1". When you enable the **Last Access Time Stamp** setting, the registry key is set to "0" (zero), which may slow performance slightly on some Windows devices.

8. The RTT-IP feature has been retired. Ignore the **RTT-IP Setting** area.
9. At the **Call Settings** area, configure whether an agent call is made when specific events occur on the account's managed devices. For more information, see "Managing Event Calling for Your Account" on page 38.

   NOTE You can also manage Event Calling at the device level. For more information, see "Editing Asset Information" on page 48.

10. Click **Save changes**.

Managing Service Guarantee Licenses

When a device that is assigned a Service Guarantee license is stolen and Absolute is unable to recover the device, or start a Data Delete operation, you may be eligible for a service guarantee payout on that device. To be eligible for this payout, the devices in your account must be correctly flagged as being Service Guarantee-applicable before a theft incident occurs.

One of the following scenarios is applicable:

- **Your account includes Absolute products with the Service Guarantee and you have licenses available**: By default, if your account includes Absolute products with the Service Guarantee, and you have additional licenses available, a Service Guarantee license is automatically assigned to each new device making the device eligible for Service Guarantee payouts.

IMPORTANT If you turn auto-assignment of Service Guarantee licenses off, you must manually assign the service guarantee license to applicable devices in your account. For more information on manually assigning a service guarantee license, see "Manually Editing Service Guarantee License Assignment" on page 37.

- **Your account includes Absolute products with the Service Guarantee and you do not have licenses available**: If your account contains more devices than licenses, automatic assignment of licenses to devices is disabled until you either add more licenses to your account or manually remove the Service Guarantee license from some devices.

  For example, if you have 1000 licenses, and 1250 devices contacting our Monitoring Center, then 250 devices are neither assigned licenses, nor are they eligible for the service guarantee.

  For more information on manually removing the Service Guarantee license from devices, see "Manually Editing Service Guarantee License Assignment" on page 37.

- **Your account contains products both with and without the Service Guarantee**: If your account contains a mix of Absolute products, where some products include the Service Guarantee and others don't, the Service Guarantee licenses for your account may be assigned incorrectly.

  To address such an issue, you must edit the Service Guarantee license assignment manually. For more information, see "Manually Editing Service Guarantee License Assignment" on page 37.

Manually Editing Service Guarantee License Assignment

You can either assign or remove the Service Guarantee License for each device individually or use device groups to make the change.

- **Editing the value for a single device**: If you want to assign or remove the Service Guarantee license for a single device, you can do so from the View or Edit Custom Device Fields page for the device.
  - To assign the Service Guarantee license to a device, open the View or Edit Custom Device Fields page, open the **Has Service Guarantee** list, and click **Yes**.
  - To remove the Service Guarantee license for a device, open the View or Edit Custom Device Fields page, open the **Has Service Guarantee** list, and click **No**.

  For more information, see the online Help.

- **Editing the value for a group of devices**: The quickest way to manually assign or remove Service Guarantee licenses from devices is to create a device group and change the **Has Service Guarantee** value.

  To change the Service Guarantee License assignment for a group of devices:

  a) Create a device group containing the devices for which you want to assign or remove Service Guarantee licenses. For example, if you want to assign the Service Guarantee to all the employees working in the Sales department, create a device group containing the devices of all the Sales employees.

  b) Open the View and Edit Custom Device Fields page for the device group you have just created in step a, open the **Has Service Guarantee** list, and click **Yes** to assign or **No** to remove the Service Guarantee licenses, whichever is appropriate. For information on changing a Custom Device Field for a device group, see the online Help.

Managing Event Calling for Your Account

Depending on the product your organization purchased, this feature may not be available for your account.

You can turn on Event Calling for all active Windows and Mac devices within an account. Event Calling lets these managed devices make an agent call when a significant change event occurs on a device. A change to any of the following device attributes can trigger an event call:

- hardware configuration
- installed software
- network information (Public IP)
- logged in user

For more information about the change events that trigger an event call, see "Events That Can Trigger an Event Call" on page 39.

Event calls supplement the scheduled calls that occur automatically from each managed device every 24.5 hours. However, when an event call occurs it resets the regular call schedule. Typically, when Event Calling is turned on, device information in the Absolute console is more up-to-date, which means that Alerts are triggered on a more timely basis and your reports are more accurate.

For example, a Windows device makes a scheduled agent call to the Monitoring Center at 9:00 a.m. At 10:30 a.m. the device's Public IP changes, which is considered a rule violation based on the settings made by the Administrator.

One of the following outcomes may occur, depending on whether Event Calling is turned on:

Event Calling turned on?	Outcome
Yes	An event call is triggered immediately, which updates the device's Public IP address in the Absolute console. If a Public IP related Alert was created, the event call triggers an Alert to notify the Administrator that a rule violation has occurred.
No	The next scheduled agent call occurs at 9:30 a.m. the following day (23 hours after the Public IP change event). The device's Public IP address is updated in the Absolute console. If a Public IP related Alert was created, the agent call triggers an Alert to notify the Administrator that a rule violation has occurred, but by then, the device has been off the network for 23 hours.
For more information about Alerts, see "Alerts" on page 8.	

This section provides information on the following topics:

NOTE By default, Event Calling is turned off for all devices. You can turn on Event Calling for all active Windows and Mac devices within an account, or for individual managed devices. For more information about turning on Event Calling for an individual device, see "Editing Asset Information" on page 48.

Events That Can Trigger an Event Call

An event call is triggered when a change event (change in a device attribute) occurs on the device. The following table describes the change events that can be configured to trigger an event call.

Description of change events that trigger an event call

Change event/ Configuration option	Description
Hardware change	A change to the memory, CPU, or hard drive on a device Adding or removing the following devices does not trigger a hardware change: • Printers • Firewire devices • Thunderbolt devices • Bluetooth devices **NOTE** To detect a hardware change, the device needs to be restarted. The device's hardware inventory is compared before and after the restart. If the inventories do not match, a hardware change event is logged and an event call is triggered.
Software change	A change to the inventory of installed software applications, or changes to the operating system of the device
Logged in user change	A change of the user of the device The username of the currently logged in user is compared to the username associated with the previous session. If they do not match, a user change event is logged and an event call is triggered. On Windows devices, a user change event is also logged when the Switch User feature is used.
Network change	A change to the Public IP Address of a device When a managed device's local IP address changes, the device's public IP address is checked to determine if it has also changed. If so, a network change event is logged and an event call is triggered.

Understanding the Minimum Event Call Period

When you configure Event Calling, you need to specify a Minimum Event Call Period, which controls the minimum amount of time that must elapse between event calls from a device. This setting lets you determine how frequently a device calls the Monitoring Center when multiple change events occur on a device in rapid succession.

The purpose of the Minimum Event Call Period setting is to reduce the flow of unnecessary traffic to your network gateways. We recommend that you experiment with the various settings to determine the optimal setting for your organization.

Possible values are:

- 15 minutes
- 20 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 2 hours
- 3 hours
- 4 hours
- 6 hours

Example

Event Calling is activated on a device and the Minimum Event Call Period is set to **2 hours**.

The next day, two software changes occur on the device 10 minutes apart. The first software change triggers an event call immediately, but the second call must wait for the Minimum Event Call Period to expire.

A network change then occurs on the device 20 minutes after the second software change. No event call is made because the Minimum Event Call Period has not yet expired.

The Minimum Event Call Period expires two hours after the first event call. A new event call is triggered from the device to send the details of the second software change and the network change to the Monitoring Center.

Turning on Event Calling for Your Account

By default, Event Calling is turned off at the account level. To turn on Event Calling for all devices in your account:

1. On the navigation bar click  > **Classic Account Settings**.
2. Scroll to the **Call Settings** area.
3. Click the field and select one of the following options:
   - **Set call settings for all capable devices**: Turn on Event Calling for all existing and newly activated Windows and Mac devices. As new Windows and Mac devices are activated, turn on Event Calling and apply the specified call settings.
   - **Set call settings for new devices**: As new Windows and Mac devices are activated, turn on Event Calling and apply the specified call settings.
   - **Turn on event calling for all devices where event calling is turned off**: Turn on Event Calling for existing Windows and Mac devices only.
4. In the **Minimum Event Call Period** list select the minimum amount of time that must elapse between agent calls from a device. Possible values range from 15 minutes to 6 hours. For more information, see "Understanding the Minimum Event Call Period" on page 39.
5. All **Configuration Options** are selected by default. To exclude one or more **Configuration Options**, clear each applicable checkbox.

   NOTE For more information about each option, hover over ⓘ next to **Configuration Options**. For detailed information about the device changes associated with each option, see "Events That Can Trigger an Event Call" on page 39.

6. Click **Save changes**. Event Calling is activated on each device on the next scheduled agent call.

NOTE If you selected a call setting option that applies to newly activated devices, the **Minimum Event Call Period** and **Configuration Options** that will be applied to those devices show under **Current default call settings for new devices**.

Editing Event Calling Settings

If Event Calling is turned on at the account level, you can edit the **Minimum Event Call Period** and **Configuration Options** at any time.

To edit the call settings for devices associated with the account:

1. On the navigation bar click  > **Classic Account Settings**.
2. Scroll to the **Call Settings** area.
3. Click the field and select one of the following options:
   - **Set call settings for all capable devices**: Update the call settings for all existing and newly activated Windows and Mac devices.
   - **Set call settings for new devices**: Update the call settings for newly activated Windows and Mac devices only.
   - **Change call settings for all devices where event calling is turned on**: Update the call settings for all existing Windows and Mac devices that currently have Event Calling turned on. If Event Calling was turned off for one or more devices at the device level, those devices are left unchanged.
   - **Turn on event calling for all devices where event calling is turned off**: Turn on Event Calling for the following Windows and Mac devices:
     - Devices with Event Calling turned off at the device level
     - Newly activated devices without Event Calling turned on

     NOTE This option is available only if Event Calling is turned on at the account level, but it is turned off for some devices. For more information about managing Event Calling at the device level, see "Configuring Event Calling for a Device" on page 53.
4. Edit the **Minimum Event Call Period**. Possible values range from 15 minutes to 6 hours. For more information, see "Understanding the Minimum Event Call Period" on page 39.
5. Edit the **Configuration Options** by selecting or clearing each applicable checkbox.

   NOTE For more information about each option, hover over ⓘ next to **Configuration Options**. For detailed information about the device changes associated with each option, see "Events That Can Trigger an Event Call" on page 39.
6. Click **Save changes**. The updated call settings are activated on each device on the next scheduled agent call.

Turning Off Event Calling

If Event Calling is turned on at the account level, you can turn it off for all devices in the account.

NOTE To turn off Event Calling for individual devices, see "Configuring Event Calling for a Device" on page 53.

To turn off Event Calling for all devices in the account:

1. On the navigation bar click > **Classic Account Settings**.
2. Scroll to the **Call Settings** area.
3. Click the field and select **Turn off event calling**.
4. Click **Save changes**. Event Calling is turned off on each device on the next scheduled agent call.

Viewing the List of Devices with Event Calling Turned On

To view the list of managed devices that have Event Calling turned on:

1. On the navigation bar, click > **Classic Account Settings**.
2. Scroll to the **Call Settings** area.
3. Under **Devices with event calling turned on**, click **View**. A dialog opens.
4. Filter the list of devices using any of the following criteria:
   - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device
   - **Username**: the unique name detected by the agent that identifies the person who is associated with this device
   - **Device Name**: the name assigned to the device in the operating system
   - **Serial Number**: the serial number of the device or other hardware
   - **Event Call Settings**: the Configuration Options enabled when Event Calling was turned on
   - **Minimum Event Call Period**: the time period selected when Event Calling was turned on
   - **Last Call Reason**: the reason for the last agent call from the device. Possible values are **Scheduled** or **Event | <type of change>**.

   NOTE The results cannot be filtered by the **Last Call Time**, which is the date and time of the last agent call from the device.

5. Sort the list by clicking a column heading.

   NOTE You cannot sort on the **Event Call Settings** or **Last Call Reason** columns.

6. To view the Device Summary page for a device, click the **Identifier** link.
7. Click **Cancel** to close the dialog.

Managing System Notifications

The System Notifications page lets Administrators configure a list of recipients for system notification messages. System notifications are auto-generated messages warning users 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 Administrators on your recipient list. You are limited to 20 recipients per notification.

IMPORTANT All tasks in this section require that you log in to the Absolute console as an Administrator.

This section describes the following tasks:

- Updating the System Notifications Page
- Devices With the Service Guarantee Not Calling
- Resolving a Recovery Flag Disparity

Updating the System Notifications Page

To update the System Notifications page:

1. On the navigation bar click > **System Notifications**.
2. On the System Notifications page click the appropriate tab and edit the list of e-mail addresses.
3. 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. On the navigation bar click > **System Notifications**.
2. On the System Notifications page click the **Devices With The Service Guarantee Not Calling** tab and do one of the following:
   - 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**.

Resolving a 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.

To resolve a recovery flag disparity:

1. On the navigation bar click > **System Notifications**.
2. On the System Notifications page, click the **Recovery Flag Disparity** tab and do one of the following:
   - 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.

- 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.
- To disable the system notification, remove all e-mail addresses from the recipient list.

3. Click **Save**.

Chapter 3: Generating Reports

This chapter describes how to generate reports based on the data the agent collects from managed devices. You can customize and filter reports to focus on key areas of interest. For specific details about each report, see "Working with Reports" on page 58.

You can open the report you want, set the appropriate filter criteria, and generate the report results. You can also download report results in CSV or XML formats. For the following reports, the results are available in CSV or XML format only:

- Printer Report
- Monitor Report
- Microsoft Audit Summary Report
- License Usage Summary Report
- Calling Profiles Report
- User Audit Report

When you create a custom report, you can save the report's filter criteria. You can retrieve saved reports on subsequent visits to the Absolute console and regenerate the report to show updated results.

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

Several tasks are common to most reports, including:

- Running Reports
- Navigating Reports
- Editing Asset Information
- Printing Reports
- Saving Report Filters
- Editing Saved Report Filters
- Downloading Reports
- Multi-level Security

Running Reports

For an overview of each report, see "Working with Reports" on page 58.

NOTE Depending on the user role to which you are assigned, you see only those reports that are designated as appropriate to that user role.

To run and view a report in the Absolute console:

1. On the navigation bar, click  to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. If necessary, click **Accept** to agree to the terms and conditions of running the report.

4. In the **Search Criteria** location, specify how to filter the report's results.

   NOTE When first opened, some reports return results that are based on default filter criteria. For information about using the Choose feature, see "Using the Choose Feature" on page 47.

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

   NOTE For information about downloading CSV or XML output for reports that show on screen, see "Downloading Reports" on page 56. For information about preparing reports with results only available for download, see "Working with Reports" on page 58.

   If your session times out while you are viewing a report, a time-out warning message opens with instructions about how to continue.

Navigating Reports

To navigate the reports, there are some common features, which are noted next:

- Expanding and Collapsing the Search Criteria Information
- Using the Choose Feature
- Viewing an Entire Row in a Report Record
- Moving Between the Pages of a Report
- Changing the Number of Records That Show in a Report
- Changing the Sort Order

Expanding and Collapsing the Search Criteria Information

The Search Criteria can expand or collapse. Depending on whether the Search Criteria section is expanded or collapsed, these buttons show the upward arrows or downward arrows.

Using the Choose Feature

Many areas of the Absolute console require that you 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 opens with a list of all available and valid values for the data field.
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.

Viewing an Entire Row in a Report Record

Columns in a report's results grid are presented in a horizontal format, with columns and rows. Drag the scroll bar at the bottom of the page to the right to see the entire row of a report record.

Moving Between the Pages of a Report

You can move to various locations in a report, as follows:

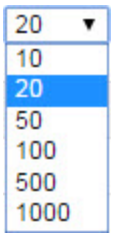
- to the first page by clicking **<<First** or the link for page number **1**
- to a previous page by clicking **<Prev**
- to a specific page by clicking the **link** for the page number you want
- to the next page by clicking **Next>**
- to the last page by clicking **Last>>**

Changing the Number of Records That Show in a Report

The default number of records shown in each report depends upon the report. For example, when you open a report you may see 20 ▼ above and below the results grid at its right side.

To change the number of records that show in a report:

1. Log in to the Absolute console and open the appropriate report. See "Running Reports" on page 46.
2. Change the default value by opening the list.
3. Select the appropriate number of records to show in the report from these options:



Changing the Sort Order

Initially most reports are sorted by **Identifier**, however, you can sort using any column heading.

To sort a report by any other criteria:

1. Log in to the Absolute console and open the appropriate report. See "Running Reports" on page 46.
2. In the **results** grid click the column heading by which you want to sort the report.

Editing Asset Information

Each device on which the agent is installed is given a unique Identifier by the Monitoring Center. Click an Identifier to open the Device Summary page where you can update the information associated with a particular device. For example, if an Identifier is transferred to a new device, you can change the device information attached to that Identifier.

To edit the information associated with a device:

1. Log in to the Absolute console and open the appropriate report following the task "Running Reports" on page 46.

2. In any report, click the **Identifier** you want to edit, which opens the Device Summary page.

   The Device Summary page provides information about the device.

   Some information on this page is editable and some is read-only. For more information about working with the information on the Device Summary page, see "Device Information on the Device Summary Page" on page 50.

   NOTE Depending on the type of device, some values on the Device Summary are not populated. For example, if the Identifier is associated with an Android device, only the subset of the hardware and software information relevant to an Android device is shown. For details about the specific information detected for each supported operating system, go to the Documentation page and see *Absolute Products and Services—Data Points Collected*.

3. If you changed any device information, click **Save Changes**. The Device Summary page updates to confirm that your changes are saved.
4. To regenerate the report and view any changes you made, click the **Back** link.

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

This section provides information on the following topics:

Device Information on the Device Summary Page

This page opens when you click an Identifier that shows on any of the Classic Reports. The Device Summary page provides the following information about the device:

- **Identifier**, which is a unique identifier for this device
- **Make**
- **Model**
- **Serial Number**[1]
- **RTT-IP** (feature is retired)
- **Call Settings** for Windows and Mac devices only
  For more information about this section, see "Managing Event Calling for a Device" on page 53.
- **Device Name**
- **Full Windows Device Name** for Windows devices only
- **Windows Domain** for Windows devices only
- **Workgroup** for Windows devices only
- **Department**, which you can edit
- **Detected Username**
- **Assigned Username**, which you can edit. For more information, see "Using the Assigned Username Field" on page 54.
- **Assigned User E-mail Address**, which you can edit
- **Detected Asset Number**
- **Assigned Asset Number**, which you can edit
- **Device Groups** shows the device groups to which this managed device belongs.
  To edit a device group, click the applicable device group link. For more information, see "Editing a Device Group" on page 22.
- **View and Edit Custom Device Field Data** link opens the View and Edit Custom Device Field page, where you can enter values for the device's custom fields

IMPORTANT You can edit values in the **Department**, **Assigned Username**, **Assigned User E-mail Address**, and **Assigned Asset Number** fields. If you edit any of these fields, click **Save Changes**.

More information about the device is available on the following tabs:

- Hardware Summary Tab
- Software Summary Tab
- Call Tracking Tab

[1] When detecting hard drive serial numbers, the agent queries the disk controller first. If that fails, then the agent uses Microsoft's Windows Management Interface (WMI) to get the hard disk serial numbers. For Microsoft's description of a scenario where this problem may occur, see: connect.microsoft.com/VisualStudio/feedback/details/623282

Hardware Summary Tab

The **Hardware Summary** tab provides information about the following identification points:

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.

- **Detected Make**
- **Detected Model**
- **Detected Serial** number values shown 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 provided in the Asset Summary section.
- **CPU**
- **RAM**
- **Disk Drive Information** shows detected information about the installed hard drives on the device, which includes:
  - **Physical Drives**: the name of the detected hard **Drive** partition and the **Serial Number** for each
  - **Volumes**: the name of the detected hard drive partition
    - **Type**: the type of hard drive
    - **Filesystem**: 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 Network Radios**: This area is shown if any radios are detected on a mobile device. The following information is available:
  - **Radio Type**: the mobile network radio available on the device. Possible values are:
    - **GSM** (Global System for Mobile Communication)
    - **CDMA** (Code Division Multiple Access)
  - **Equipment ID**: the identification number unique to the mobile device.
  - **Subscriber ID**: also known as International Mobile Subscriber Identity (IMSI), the unique identifier associated with the subscriber
  - **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.
- **See hardware details**: provides more information about the device's hardware.
  Click to open the list to view the following detected information:
  - **Local IP**
  - **Public IP**
  - **Network Card 1 Description**
  - **Network Card 1 MAC Address**
  - **Network Card 1 IP**
  - **Network Card 2 Description**
  - **Network Card 2 MAC Address**
  - **Network Card 2 IP**

- **Number Of CPUs**
- **System BIOS/Firmware Date**
- **System BIOS/Firmware Version**
- **Video Device Description**
- **Video Display Color Depth**
- **Video Display Resolution**

NOTE The Printer Driver report provides a list of all printer drivers installed on the device. To download this report click the **Download Printer Report** link. This report is identical to the Printer Report, with the exception that these results are limited to printer drivers installed on this device.

Software Summary Tab

The Software Summary tab provides information about the following identification points:

- **Operating System**
- **Detected Anti-Malware**
- **OS Service Pack**
- **See installed Microsoft Hotfixes**: a table that shows the following information about installed packages:
  - **Application**
  - **Package Name**
  - **Hotfix Number**
  - **Details**
  - **Installed By** name
  - **Installed On** date

Call Tracking Tab

The Call Tracking tab provides information about the operation of the agent, including:

- **Call History Report**: a link to this report. To view **Extended IP Call Information** details, click the link under the **Public IP Address** column in the **results** grid of the report.
- **Agent first installed on (first call)**: date and time of the first agent call to the Monitoring Center
- **Agent version**: agent version and number
- **Agent last called on**: date and time of the last agent call to the Monitoring Center
- **Agent last called from**: IP address from which the agent last called
- **Agent next call expected on**: date and time for the next agent call to the Monitoring Center
- **Asset tracking data last collected on**: date and time the Asset tracking data was last collected

NOTE To view the Call History Report for this Identifier, go to the Call History Report. 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 "Running Reports" on page 46.

Managing Event Calling for a Device

Depending on the product your organization purchased, this feature may not be available.

You can use the Call Settings area of the Device Summary page to configure Event Calling for the device. Event Calling is independent of and in addition to the standard scheduled agent calls that occur automatically from each managed device.

NOTE Event Calling can be turned on at the account or device level. For more information about Event Calling, and instructions for turning it on at the account level, see "Managing Event Calling for Your Account" on page 38.

Configuring Event Calling for a Device

To configure Event Calling for a managed device:

1. Navigate to the **Call Settings** area of the Device Summary page.

   NOTE For more information about each option, hover over ⓘ next to **Configuration Options.** For detailed information about the device changes associated with each option, see "Events That Can Trigger an Event Call" on page 39.

2. Do one of the following:

   - To turn on Event Calling:
     i) Select the **Turn on event calling for the device** checkbox.

     NOTE Event Calling is activated when the device makes its next scheduled agent call. The **Scheduled Call** field shows the current scheduled call frequency for the device.

     ii) In the **Minimum Event Call Period** list select the minimum amount of time that must elapse between agent calls from a device. Possible values range from 15 minutes to 6 hours.

     For more information, see "Understanding the Minimum Event Call Period" on page 39.

     iii) All **Configuration Options** are selected by default. To exclude one or more **Configuration Options**, clear each applicable checkbox.
   - To edit the existing call settings for a device that has Event Calling turned on:
     i) Edit the **Minimum Event Call Period**. Possible values range from fifteen minutes to six hours. For more information, see "Understanding the Minimum Event Call Period" on page 39.
     ii) Edit the **Configuration Options** by selecting or clearing each applicable checkbox.
   - To turn off Event Calling, clear the **Turn on event calling for the device** checkbox.

3. Click **Save changes**.

   Event Calling is configured on the device on the next scheduled agent call.

Viewing the Call History for a Device

You can view details about the agent calls made from a Windows or Mac device over the past 365 days.

To view a device's call history:

1. Navigate to the **Call Settings** area of the Device Summary page.

   The **Last Call Reason** field shows the details of the most recent agent call from the device. Possible values are:

   - **Scheduled**
   - **Event | <type of change>**

   For example: **Event | Software removed, Software installed, Logged in user changed**

2. Click **View Call History** to open the Call History dialog.

   The following information about each agent call is provided:

   - **Call Time**: the date and time of the call
   - **Reason**: the type of agent call

     For event calls, the type of change is provided. Possible values are:

     - **Location changed**
     - **Hardware changed**
     - **Software installed**
     - **Software removed**
     - **Logged in user changed**
     - **Public IP changed**

     For more information about these changes, see "Events That Can Trigger an Event Call" on page 39.

3. To sort the information, click the applicable column heading.
4. To close the dialog click **Cancel**.

Using the Assigned Username Field

The Assigned Username field on the Device Summary page is a static, editable field that lets Administrators identify to whom a device was assigned originally. This 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.

For more information about setting the **Assigned Username** field, see the online Help.

NOTE The **Assigned Username** field is appended to all report downloads that include an **Identifier** or **Username**, regardless of whether or not the **Assigned Username** field is included in the actual report.

Using the Dormant Devices Field

The **Dormant** field helps administrators distinguish those devices that are truly missing from those devices that are located in places without access to an Internet connection, such as storage facilities.

The **Dormant** field is a static, editable field that administrators can use to identify devices that are not expected to contact the Monitoring Center. For more information about how to set values for Custom Device Fields, see the online Help.

Printing Reports

You can print reports in whole or in part. Each page of a report includes a **Print** icon, such as  .

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

To generate a version of the current page of a report for printing, which is optimized for creating a hard copy:

1. Log in to the Absolute console and open the appropriate report. See "Running Reports" on page 46.
2. Open any report page and click  .
3. The current page is downloaded into a Microsoft Excel spreadsheet and you can print the report page using Excel.

Saving Report Filters

Most reports allow you to edit the data shown. You can save custom reports using the **Save Report Filter** feature.

NOTE Saved reports define the criteria for a report, not the existing data. The actual data, which meets the criteria, changes with time, thereby changing the content of the saved report.

To save a report filter:

1. Log in to the Absolute console and open the appropriate report. See "Running Reports" on page 46.
2. On any report page click  .
3. In the Save Report Filter dialog, enter a name (up to 48 characters in length) for the saved report.
4. Click **OK**, which refreshes the dialog to show that the report was saved successfully.
5. Click **Close** to exit the dialog.

   The saved report is available under **My Filters** in the **My Content** section.

Editing Saved Report Filters

To edit a saved report filter:

1. On the navigation bar, click to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. Under My Content click **My Filters**. The My Filters page opens to show a list of saved filters.
4. Click the appropriate **Filter** name to select it. The report page opens, showing the filters that you have saved. For more information, see "Saving Report Filters" on page 55.
5. Edit the existing filters, as required, and do one of the following:
   - To update the existing report filter, click **Show results**. The changes are saved to the report filter.
   - To create a new saved report filter:
     i) In the report header click .
     ii) In the Save Report Filter dialog, enter a name (up to 48 characters in length) for the report and click **OK**.

     A new saved report filter is created, and the original saved report filter remains unchanged.

Downloading Reports

Users can download any full or partial report. Requests for report downloads are queued and processed offline. When processed, report downloads are available from the My Reports page. You can download report data in a Comma Separated Values (CSV) or an eXtensible Markup Language (XML) format.

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

To download a report:

1. Log in to the Absolute console and open the appropriate report following the task, "Running Reports" on page 46.
2. On any report page, define any appropriate filters.
3. Click **Show results**.
4. When the report shows, click .
5. Enter a name for the report in the **Report Name** field.
6. In the **Report Format** list select a value (**CSV** or **XML**).

   Remember, if you plan to upload the report, you can only do so with a CSV file.
7. If you want to receive e-mail notification when the download is available, enter your e-mail address in the **Create Email Alert** field.
8. Click **Continue** to queue the download.

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

To retrieve a report that was processed:

1. On the navigation bar, click the **My Content** > **My Reports** link.
2. On the My Reports page, in the **Status** column click the **Ready** link.
3. Follow the instructions that are provided on screen to download the file.

NOTE While your file request is being processed, the **Status** column shows **Queued** and the report is not available. When processing in complete, the **Status** column shows the **Ready** link and, if configured to do so, you receive an e-mail notification.

Multi-level Security

Multi-level security features let an authorized user grant different access rights and privileges on reports to specific users or groups of users. There are five different user access levels: Security Administrator, Administrator, Security Power User, Power User, and Guest.

Chapter 4: Working with Reports

Reports help you track and manage your assets, allowing you to review many information types, such as:

- Lease deadlines
- Hardware requirements
- Necessary upgrades

The reports in the Absolute console vary widely in scope. Some reports are broad and include a summary of numerous assets, and others focus and specify precise details pertaining to a single device. Each report is described in this chapter.

This chapter includes the following sections:

Hardware Assets Reports

The reports that show under the Hardware Assets page are determined by the product your organization purchased and may include the following:

- Asset Report
- Printer Report
- Monitor Report
- Hardware Configuration and OS Change Report
- Hard Disk Space Report
- Device Readiness Report
- Mobile Broadband Adapter Report
- Mobile Device Report

Opening the Hardware Assets Page

Complete the following task to open any of the Hardware Assets reports included in this classification.

To open the Hardware Assets page:

1. On the navigation bar, click  to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.

3. Click **Hardware Assets**.

   The Hardware Assets page shows all of the available reports under this category.

Asset Report

The Asset Report has been retired. To view your devices, go to the Assets area and view the All Devices page. For more information, see *Working with your active devices* in the online Help.

Printer Report

The Printer Report does not show data on-screen. Instead, the Printer Report lets users download a Comma Separated Value CSV) or eXtensible Markup Language (XML) file that identifies installed printer drivers, printer ports, and devices by printer.

To generate a Printer Report:

1. On the Hardware Assets page, click **Printer Report**.
2. On the Printer Report page, at the **Search Criteria** area, set the preferred display options for the report using one or more of the following criteria:
   - In the **Display** field, select one of the following options:
     - **Printer Drivers** returns a CSV or XML 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 or XML 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 under which the printer operates.
       – **Attribute**: indicates whether the printer is installed locally or is installed on a network as a shared printer.
     - **Printer Ports** returns a CSV or XML file that organizes printer driver data according to their port.

       Printer Port CSV or XML 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** returns a CSV or XML file that lists all devices with installed printer drivers.

When the report criteria is set to this value, the page refreshes to include **the Group is** field. To filter your results by Device Group, open the list and select the appropriate device group.

Devices by Printer CSV or XML 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 name assigned to this device in the operating system.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Department**: the department the device belongs to.

- In **the Group is** field, open the list to show all Device Groups in your account and select **All Devices** or the appropriate **Device Group name**.

3. At the **Name and Format** area, in the **Name** field enter a unique name for your report.
4. In the **Format** field, open the list and select one of the following options:
   - **CSV**: a plain text file with comma separated columns that is opened with software included in your operating system. Recommended for SQL queries and uploading large data files.
   - **XML**: a Unicode language file that is opened with an XML editor such as Microsoft Excel or OpenOffice. Recommended for filtering and formatting data.
5. At the Create E-mail Alert location, in the **Your E-mail address** field enter your e-mail address if you want to receive an e-mail notification when the report is processed.
6. Click **Continue** to queue the download.
7. When your request is processed, you can retrieve the CSV or XML file of the report from the **My Reports** page. For more information, see "Downloading Reports" on page 56.

Monitor Report

The Monitor Report does not show data on-screen. Instead, the Monitor Report enables users to download a CSV (Comma Separated Value) or XML (eXtensible Markup Language) file that identifies the installed monitor drivers.

To generate a Monitor Report:

1. On the Hardware Assets page, click **Monitor Report**.
2. On the Monitor Report page, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter results by Device Group, open **the Group is** list and select the appropriate device group.
   - To filter your results by specific device, open the **and the field** list and select one of the following values:

- **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Device Name**: the name assigned to the device in the operating system.
- **Serial Number**: the serial number of the device or other hardware.
- **Asset Number**: the identification number associated with a device in the Absolute console.
- **Department**: the department to which this device belongs.
- **Make**: the manufacturer of a device or other hardware.
- **Model**: the product type of a device or other hardware.
- **Monitor manufacturer:** the manufacturer of the device's monitor.
- **Monitor type**: the monitor configuration such as Default or Plug and Play.
- **Monitor refresh frequency**: the number of times in a second that a monitor draws the data. Increasing the refresh rate decreases flickering and reduces eye strain.
- **Video device description**: the name of the device's video card.
- **Video display resolution**: the number of distinct pixels that can be displayed by the monitor quoted as width × height, with the units in pixels such as 1024 × 768.
- **Video display color depth**: the number of bits used to indicate the color of a single pixel in a bitmap image or video such as 1-bit monochrome or 8-bit grayscale.

Depending on the value you selected from the preceding list, you may want to further define this field. In the **is or contains** field, click **Choose** and select a value from the list.

3. At the **Name and Format** area, in the **Name** field enter a unique name for your report.
4. In the **Format** field, open the list and select one of the following options:
   - **CSV**: a plain text file with comma separated columns that is opened with software included in your operating system. Recommended for SQL queries and uploading large data files.
   - **XML**: a Unicode language file that is opened with an XML editor such as Microsoft Excel or OpenOffice. Recommended for filtering and formatting data.
5. At the **Create E-mail Alert** location, in the **Your E-mail address** field enter your e-mail address if you want to receive an e-mail notification when the report is processed.
6. Click **Continue** to queue the download.
7. When your request is processed, you can retrieve the CSV or XML file of the report from the **My Reports** page. For more information, see "Downloading Reports" on page 56.

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

Hardware Configuration and OS Change Report

The Hardware Configuration and OS Change Report has been retired. To view devices with changes to their critical hardware or operating system (OS) during a particular time period, go to the History area and view the Events page. For more information, see *Monitoring events* in the online Help.

Hard Disk Space Report

The Hard Disk Space Report shows total, used, and available hard disk space on each disk volume detected on tracked devices. The data collected using this report lets you track devices that may not be able to accept software upgrades or that are running out of available hard disk space.

To generate a Hard Disk Space Report:

1. On the Hardware Assets page, click **Hard Disk Space Report**.
2. On the Hard Disk Space Report page, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values:
     - **Any of the fields in this list**: selects all the values in the list.
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
     - **Device Name**: the name assigned to the device in the operating system.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
     - **[Custom Device Fields]**: if one or more Custom Device Fields have been created for your account you can use them as filter criteria.

     Depending on the criteria you selected from the preceding list, enter a value in the field or click **Choose** and select a value from the list.
   - To filter your results by Department, in the **and the Department** field, open the list and select the appropriate department.
   - To filter your results by the amount of available hard disk space on the device, at the **and any Volume has less than** area, do one of the following:
     - Open the list and select a value for available hard disk space.
     - At the bottom of the Search Criteria pane, select the **Display hard drive size and space available for all selected devices** checkbox to show all devices with less than 100% of available hard disk space.
3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices. Some of the columns in the report may not be visible on your screen. To view all the columns in the report, use the arrow key on your keyboard to scroll to the right.
   - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
   - **Device Name**: the name assigned to this device in the operating system.
   - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
   - **E-mail Address**: the e-mail address for the person associated with this device or activity.

- **Threshold Value (MB)**: the minimum amount of available hard disk space required by the operating system to function before affecting the performance of your device. If the value in the Volume Free Space column is less than the Threshold Value, your device may run the risk of shutting down.
- **Volume**: a partition of storage space on the hard disk identified by a letter such as `A:\` or `B:\`.
- **Volume Label**: the descriptive name assigned to a volume on the hard disk such as Local Disk or Public.
- **Volume Size (MB)**: the storage capacity of the volume in megabytes (MBs).
- **Volume Free Space (MB)**: the amount of available space in the volume in megabytes (MBs).
- **Volume Used Space (MB)**: the amount of storage space used on the volume in megabytes (MBs).
- **Hard Disk Size (MB)**: the amount of data storage on the device in megabytes (MBs).
- **Hard Disk Free Space (MB)**: the amount of available storage space on the hard disk in megabytes (MBs).
- **Hard Disk Used Space (MB)**: the amount of available storage space used on the hard disk in megabytes (MBs).

Device Readiness Report

Depending on your needs, you can generate a Device Readiness Report to show the list of devices that meets, or fails to meet, a set of operating system and hardware requirements.

For example, you can generate a Device Readiness Report to do the following:

- Locate devices that can (or cannot) support a particular software or operating system rollout.
- Find devices that are ready for retirement.
- Identify hardware components that require an upgrade.

To generate a Device Readiness Report:

1. On the Hardware Assets page, click **Device Readiness Report**.
2. On the Device Readiness Report page, at the **Search Criteria** area, set the preferred filters for the report using one or more of the following criteria:
   - To filter results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by Department, in the **and the Department** field, open the list and select the appropriate department.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values:
     - **Make**: the manufacturer of a device or other hardware.
     - **Model**: the product type of a device or other hardware.
     - **[Custom Device Fields]**: if one or more Custom Device Fields have been created for your account you can use them as filter criteria.

     Depending on the criteria you selected from the preceding list, enter a value in the field or click **Choose** and select a value from the list.

3. To filter the results based on system requirements, select one of the following options:
   - **Any**: shows devices that meet *any* of the system requirements you enter.
   - **All of the following conditions are true**: shows devices that meet *all* of the system requirements you enter.
4. To set the system requirements to apply to the report, do one or more of the following:
   - To narrow your results by operating system, select the **O/S** checkbox.
     i) Open the list and select one of the following:
        - **Is** shows devices that have the selected operating system.
        - **Is Not** excludes devices that have the selected operating system.

     ii) Click **Choose**. On the Choose O/S dialog, select an operating system in the Available Fields pane and click **>** to add it to the Selected Fields pane. To add all fields, click **>>**.

     iii) To remove a field, select the field in the Selected Fields pane, and then click **<**. To remove all fields, click **<<**.
   - To narrow your results by a specific processor type, select the **CPU** checkbox.
     i) Open the list and select one of the following:
        - **Is** shows devices that have the CPU you selected.
        - **Is Not** excludes devices that have the CPU you selected.

     ii) Click **Choose**. On the Choose CPU dialog, select a CPU in the Available Fields pane and click **>** to add it to the Selected Fields pane. To add all fields, click **>>**.

     iii) To remove a field, select the field in the Selected Fields pane, and then click **<**. To remove all fields, click **<<**.
   - To filter your results by a specific processor speed, at the **Max detected CPU** area:
     i) Open the list and select one of the following options:
        - **<**: for a value that is less than
        - **<=**: for a value that is less than or equal to
        - **=**: for a value that equals
        - **>=**: for a value that is greater than or equal to
        - **>**: for a value that is greater than

     ii) In the **MHz** field, enter a value for the processor speed. The default value is 300 MHz.
   - To filter your results by a specific memory size, at the **RAM** area:
     i) Open the list and select one of the following options:
        - **<**: for a value that is less than
        - **<=**: for a value that is less than or equal to
        - **=**: for a value that equals
        - **>=**: for a value that is greater than or equal to
        - **>**: for a value that is greater than

     ii) In the **MB** field, enter a value for the RAM size. The default value is 128 MB.
   - To filter your results by a hard disk size, at the **HD size** area:
     i) Open the list and select one of the following options:
        - **<**: for a value that is less than

- **<=**: for a value that is less than or equal to
- **=**: for a value that equals
- **>=**: for a value that is greater than or equal to
- **>**: for a value that is greater than

ii) In the **MB** field, enter a value for the size of the device's hard disk. The default value is 2000 MB.

- To filter results by the amount of free space on the hard disk, at the **HD free space** area:

i) Open the list and select one of the following options:

- **<**: for a value that is less than
- **<=**: for a value that is less than or equal to
- **=**: for a value that equals
- **>=**: for a value that is greater than or equal to
- **>**: for a value that is greater than

ii) In the **MB** field, enter a value for the amount of free space on the device's hard disk. The default value is 1500 MB.

5. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.

Mobile Broadband Adapter Report

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. For more information, see "Editing Asset Information" on page 48.

To generate a Mobile Broadband Adapter Report:

1. On the Hardware Assets page, click **Mobile Broadband Adapter Report**.
2. On the **Mobile Broadband Adapter Report page**, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values:
     - **Any of the fields in this list**: selects all the values in the list.
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
     - **Mobile Broadband Adapter Manufacturer**: the name of the manufacturer of the mobile broadband adapter.
     - **Mobile Broadband Adapter Model**: the model number, if available, of the mobile broadband adapter.
     - **Mobile Broadband Adapter Equipment ID**: the adapter's identification number.

- **Mobile Broadband Adapter Subscriber ID**: the unique number associated with the subscriber, stored in the adapter, the Subscriber Identity Module (SIM) card, or equivalent.
- **Mobile Broadband Adapter Network**: the mobile service provider associated with the mobile broadband adapter.
- **Either Phone Number**: the Detected Phone Number or the Phone Number Override associated with the device.
- **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 provided by an Administrator when a phone number is not automatically detected.

Depending on the value you selected from the preceding list, enter a value in the field or click **Choose** and select a value from the list.

- To filter your results by Department, in the **and the Department** field, open the list and select the appropriate department.

3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.
   - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
   - **Device Username**: the unique name detected by the agent that identifies the person who is associated with this device.
   - **Device Name**: the name assigned to this device in the operating system.
   - **Device Make**: the manufacturer of the mobile device.
   - **Device Model**: the product type of the mobile device.
   - **Adapter Last Detected**: the date and time when the adapter installed on the device most recently contacted the Monitoring Center.
   - **Adapter Manufacturer**: the name of the company that made the mobile broadband adapter.
   - **Adapter Model**: the product type of a mobile broadband network adapter.
   - **Equipment ID**: the identification number unique to a smartphone. The equipment ID is typically found on a printed label on the battery. For CDMA smartphones, the Electronic Serial Number (ESN) or the Mobile Equipment ID (MEID) are reported. For GSM and UMTS smartphones, the International Mobile Equipment Identifier (IMEI) is reported.
   - **Subscriber ID**: the unique number associated with the smartphone network service subscriber. The number is retrieved from the Smartphone hardware, the Subscriber Identity Module (SIM) card, or an equivalent.
   - **Network**: the mobile service provider associated with a mobile broadband adapter.
   - **Detected Phone Number**: the phone number associated with a mobile broadband adapter, as reported by the device.
   - **Phone Number Override**: the alternative phone number associated with a mobile device or broadband adapter.

[Custom Device Fields]: if one or more Custom Device Fields have been created for your account you can use them as filter criteria.

Mobile Device Report

The Mobile Device Report has been retired. To view your smartphone and tablet devices, go to the Assets area and filter the All Devices page by platform type. For more information, see *Working with your active devices* in the online Help.

Software Assets Reports

All Software Assets reports have been retired.

To view information about the applications installed on your devices:

- Review the reports in the Applications report category on the Reports page. For more information, see *Getting started with Application reports* in the console Help.
- Go to the Applications page in the Assets area. For more information, see *Viewing installed applications* in the console Help.

Security Reports

The reports that show under the Security Reports page are determined by the Absolute product your organization purchased and may include the following:

- Operating System Updates Report
- Internet Browsing Configuration Report
- Unauthorized Software Report
- Anti-Malware Report
- Missing Anti-Malware Report
- Modem Addition Report
- Suspicious Devices Report
- Absolute Secure Drive Authentication Failures Report
- Full-Disk Encryption Status Report
- SCCM Status Reports
- Security Posture Report

Opening the Security Page

Complete the following task to open any of the Security reports included in this classification.

To open the Security page:

1. On the navigation bar, click to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. Click **Security**.

   The Security page opens showing all of the available reports.

Operating System Updates Report

The Operating System Updates Report has been retired. To view operating system information for a device, go to the Reports area and view the Operating Systems report. For more information, see *Operating Systems report* in the online Help.

Internet Browsing Configuration Report

The Internet Browsing Configuration Report identifies the browser type and version on a device, as well as the monitor resolution settings for all monitored devices. You can use the report to identify devices that use an older version of a browser.

IMPORTANT You must log in as a Security Administrator to open the Internet Browsing Configuration Report.

To generate an Internet Browsing Configuration Report:

1. On the Security page, click **Internet Browsing Configuration Report**.
2. On the Internet Browsing Configuration Report page, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values:
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
     - **Device Name**: the name assigned to the device in the operating system.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.

     Depending on the value you selected from the preceding list, you may want to further define this field using the **is or contains** field by clicking **Choose**.
   - To filter your results by Browser, in the **and the Browser Name is or contains** field, enter all or part of the name of the browser.
   - To filter your results by Browser Version, in the **and the Browser Version number is or contains** field, enter the browser's version number.
3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.
   - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
   - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
   - **Device Name**: the name assigned to this device in the operating system.
   - **Browser Name**: the name of the program used to access the Internet and view web pages on a device.

- **Browser Version**: a number that distinguishes releases of the Internet browser as detected by the agent, and reported in the Absolute console.
- **Display Resolution**: the number of pixels that can be displayed on a device monitor quoted as width × height in units of pixels such as 1024 × 768.
- **Color Depth**: the number of distinct colors that can be represented by a piece of hardware or software.

Unauthorized Software Report

The Unauthorized Software Report lets users search for devices that contain unauthorized software applications.

IMPORTANT You must log in as a Security Administrator to open the Unauthorized Software Report.

To generate an Unauthorized Software Report:

1. On the Security page, click **Unauthorized Software Report**.
2. On the Unauthorized Software Report page, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by Department, in the **and the Department** field, open the list and select the appropriate department.
   - To filter your results by a Program, in the **and the field** area, open the list and select one of the following values.
     - **Publisher**: the organization creating a software application.
     - **Program**: an executable file on a device that is detected by the agent and reported in the Absolute console.
     - **Application**: the smallest unit of software installed on a device that is detected by the agent and reported in the Absolute console.
     - **Version**: a number that distinguishes releases of the same software application.
   - To filter results by a keyword, in the **contains any of the words** field, enter the keywords.
   - To filter results by a specific keyword, in the **contains all of the words** field, enter specific keywords.
   - To filter results by a specific phrase, in the **and contains exactly the phrase** field, enter the exact phrase.
   - To filter results excluding keywords, in the **and does not contain the words** field, enter the keywords.
3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.
   - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
   - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
   - **Device Name**: the name assigned to this device in the operating system.

- **Department**: the department to which this device belongs.
- **Publisher**: the organization creating a software application.
- **Application Name**: the title of an executable file. In practice, many publishers mutually exchange Application Name and Program Name values.
- **Program Name**: the name of an executable file on a device that is detected by the agent and reported in the Absolute console.
- **Version**: a unique name or number assigned to an identified and documented body of software.
- **Date First Detected**: the date and time identified by the agent during the call to the Monitoring Center.

Anti-Malware Report

The Anti-Malware Report has been retired. To view information about the anti-malware applications installed on your devices, go to the Reports area and under **Security**, open the Anti-Malware report. For more information, see *Anti-Malware report* in the online Help.

Missing Anti-Malware Report

The Missing Anti-Malware Report has been retired. To configure a report that shows the devices without an anti-malware application installed, go to the Reports area and under **Security**, open the Anti-Malware report. For more information, see *Anti-Malware report* in the online Help.

Modem Addition Report

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

IMPORTANT You must log in as a Security Administrator to open the Modem Addition Report.

To generate a Modem Addition Report:

1. On the Security page, click **Modem Addition Report**.
2. On the Modem Addition Report page, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by Department, in the **and the Department** field, open the list and select the appropriate department.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values:
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a Device.
     - **Device Name**: the name assigned to this device in the operating system.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.

Depending on the value you selected from the preceding list, you may want to further define this field. In the **is or contains** field, click **Choose** and select a value from the list.

- To filter your results by date, at the **and a Modem was installed or re-configured between** area, do one of the following:
  - In the **in the last <n> days** field, click the option and enter the appropriate number of days. Any value from **1** through **365** is appropriate. A higher value in this field will result in a larger report and will take longer to generate results.
  - In the **between** field, click the option and enter the dates (dd/mm/yyyy) or click the **Calendar** icon to open the calendar dialog. Enter the dates in chronological order, with the earliest date entered first and the later date entered second.

3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.

- **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Device Name**: the name assigned to this device in the operating system.
- **Detected Date**: the date and time when the data was detected on the device.
- **Current Model Name**: the product type of a device or other hardware detected by the agent.
- **Current Port**: the port under which the modem operates as detected by the agent.
- **Previous Model Name**: the product type of a device or other hardware previously detected by the agent.
- **Previous Port**: the port under which the modem operates as previously detected by the agent.

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 to specify events that trigger suspicious alert notifications. For more information about creating and managing alerts, see "Alerts" on page 8.

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.

Another example is to use the Major Change alert to notify Administrators immediately when a device is detected that has the **Device Name**, **Username**, and **Operating System Product Key** changed simultaneously, with the agent subsequently making a self-healing call.

IMPORTANT You must log in as a Security Administrator to open the Suspicious Devices Report.

To generate a Suspicious Devices Report:

1. On the Security page, click **Suspicious Devices Report**.
2. On the Suspicious Devices Report, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by Department, in the **and the Department** field open the list and select the appropriate department.
   - To filter your results by specific device, in the **and the field** area open the list and select one of the following values:
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
     - **Device Name**: the name given to a device.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.

     Depending on the value you selected from the preceding list, you may want to further define this field. In the **is or contains** field, click **Choose** and select a value from the list.
   - To filter your results by date, in the **and the suspicious event occurred** area, do one of the following:
     - In the **in the last <n> days** field, click the option and enter the appropriate number of days. Any value from **1** through **365** is appropriate. A higher value in this field will result in a larger report and will take longer to generate results.
     - In the **between** field, click the option and enter the dates (dd/mm/yyyy) or click the **Calendar** icon to open the calendar dialog. Enter the dates in chronological order, with the earliest date entered first and the later date entered second.
   - To filter your results by Suspicion Level, in the **and the Suspicion level is** area:
     i) Open the list and select a value for **Greater than**, **Equal to**, or **Less than**.
     ii) Open the list and select the appropriate **Suspicion Level**.
3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.
   - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
   - **Asset Number**: the identification number associated with a device in the Absolute console.
   - **IMEI**: the International Mobile Equipment Identity (IMEI) number of the device, if applicable
   - **Subscriber ID**: also known as International Mobile Subscriber Identity (IMSI), the unique identifier associated with the subscriber
   - **Phone Number**: the phone number associated with the mobile device, if applicable
   - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
   - **Device Name**: the name given to a device.
   - **Make**: the manufacturer of a device or other hardware.
   - **Model**: the product type of a device or other hardware.

- **Suspicion Level**: the severity level of a suspicious event. Possible values range from **Not Suspicious** to a suspicion level of **5**.
- **Suspicious Events**: click the value to open the Alert Events page to view the Alert Name and description.

Absolute Secure Drive Authentication Failures Report

The Absolute Secure Drive Authentication Failures Report shows a list of those devices that Absolute Secure Drive failed to authenticate based on the options you set.

You can filter this report based on how often authentication failed, or the authentication or failure types available.

You can also set an alert to notify you about failed Absolute Secure Device login attempts by selecting the **Absolute Secure Drive failed login** condition on the Create and Edit Alerts page. For more information, see "Creating New Custom Alerts" on page 11.

To generate an Absolute Secure Drive authentication failures Report:

1. On the Security page, click **Absolute Secure Drive Report**.
2. On the Absolute Secure Drive Authentication Failures Report, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by specific device, in the **and the field** area open the list and select one of the following values:
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
     - **Device Name**: the name given to a device.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.

     Depending on the value you selected from the preceding list, you may want to further define this field. In the **is or contains** field, click **Choose** and select a value from the list.
   - To filter your results by date, in the **and when unsuccessful authentication attempts occurred** area, do one of the following:
     - In the **or more times** field, enter the appropriate number of failed login attempts you want to see in your report.
     - Select one of the following options:
       – In the **in the last <n> days** field, click the option and enter the appropriate number of days. Any value from **1** through **365** is appropriate. A higher value in this field will result in a larger report and will take longer to generate results.
       – In the **between** field, click the option and enter the dates (dd/mm/yyyy) or click the **Calendar** icon to open the calendar dialog. Enter the dates in chronological order, with the earliest date entered first and the later date entered second.
   - To filter your results by authentication failure type, in the **and the failure type is** area:
     i) Open the **Authentication Types** list and select one of the following values:

- **All Authentication Types** where the authentication component is one or more of the following values.
- **Master Password** where the password entered is authenticated against a current password.
- **Fingerprint** where input from the fingerprint scanner is authenticated against the current value.
- **RFID** where input from an RFID device is authenticated against the current value.
- **SmartCard** where input from a chip card or an integrated circuit card (ICC) is authenticated against the current value.

ii) Open the **Failure Types** list and select one of the following values:

- **All Failure Types** where the failure is one or more of the following values.
- **Authentication Failed** where the password or login authentication did not match the current value.
- **Component Failure** where the authentication component, such as RFID or fingerprint recognition device, failed.
- **Unknown User** where the username is unknown or does not match the current value.
- **Too Many Attempts** where the username or component attempted to login more than a specified number of times with incorrect credentials.

3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.

- **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
- **Device Name**: the name given to a device.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Number of Failed Logins**: the number of Absolute Secure Drive login attempts that failed to authenticate.
- **Call Time**: when the device contacted the Monitoring Center.
- **Logged Date (UTC)**: the date and time when the authentication failures were logged.
- **Attempted Username**: the username that was used when the authentication failure occurred.
- **Type of Failed Login**: the type of authentication failure, which is a mix of the **Authentication Type** and **Failure Type** fields, for example, **Master Password: Failed** or **Master Password: Unknown User**.
- **Encryption Status**: the status of encryption available on the device. Click the **View Encryption Status** link to open the Full-Disk Encryption Status Report.

Full-Disk Encryption Status Report

The Full-Disk Encryption Status Report has been retired. To view the encryption status of your devices, go to the Reports area and under **Security**, open the Full-Disk Encryption Status report. For more information, see *Full-Disk Encryption Status report* in the online Help.

SCCM Status Reports

The SCCM Status Report has been retired. To view the status of SCCM on your devices, enable the Application Resilience policy and review the Application Resilience reports. For more information, see *Getting started with Application Resilience policies* in the online Help.

Security Posture Report

You can use the Security Posture Report to assess the overall security status of your devices. The report contains the following information for the devices in your account, in a summarized format:

- Domains
- Windows product keys (for Windows devices only)
- Full-disk encryption status, if applicable
- Anti-virus definition status
- Last agent call statistics

The report consists of two components:

- An Excel template, which you download to your workstation from the Security Posture Report page. This template contains a set of macros that processes the raw report data into a format that supports easy analysis.

  NOTE The Security Posture Report template supports Microsoft Excel 2013 and 2010 only.

- A CSV file of exported report data, which you export using the Security Posture Report page and then download from the My Reports page.

You can then generate the report by importing the CSV file into the Excel template. Details about customizing the template and importing the CSV file are provided on the *Getting Started* sheet of the Excel template.

IMPORTANT You must log in as an Administrator to open the Security Posture Report.

To generate a Security Posture Report:

1. On the Security page, click **Security Posture Report**.
2. On the Security Posture Report page, do one of the following:
   - If this is your first time exporting a Security Posture Report you need to download the report's Excel template. Click **Download Template** and follow your browser's prompts to save the template to your workstation.
   - If you have downloaded the Security Posture Report template before, you most likely modified the template variables to suit the needs of your organization, so you'll want to use that template. Go to step 3.
3. In the field under **Export Report Data**, type a unique file name for the CSV file you are about to export. Record the filename so you can locate the file on the My Reports page after the export is processed.

4. You will receive an email notification when the export process is complete. To send an email notification to other users, add their email addresses to the email address field. Use a semicolon (;) to separate email addresses.
5. Click **Export Data** to queue the export.
6. In the Data export in progress dialog click **Close**.
7. After you receive the notification email stating that your request is processed, go to the **My Reports** page and download the CSV file. For more information, see "Downloading Reports" on page 56.

   NOTE While your file request is being processed, the **Status** column on the My Reports page shows **In Queue** and the report is not available. When processed, the **Status** column shows the **Ready** link and, if configured to do so, you receive an email notification.

8. On your workstation, navigate to the Excel template that you downloaded and open it in Excel 2013 or 2010.

   For detailed instructions about customizing the template, importing the CSV file of report data, and viewing the report results, see the template's *Getting Started* sheet.

Call History and Loss Control Reports

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

The following information and reports are included in this section:

- About Extended IP Call Information
- Call History Report
- Missing Devices Report
- Device Drift by Device Name Report
- Device Drift by Username Report
- Activation Report
- Device Location History Report

Opening the Call History and Loss Control Page

Complete the following task to open any of the Call History and Loss Control reports included in this classification.

To open the Call History and Loss Control page:

1. On the navigation bar, click  to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. Click **Call History and Loss Control**.

   The Call History and Loss Control page shows all of the available reports.

About Extended IP Call Information

Call 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, which provides details about the location or origin of an IP address or telephone number. The information is useful when locating devices that are outside of a corporate network.

The Extended IP Call Information page lists the following information:

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

Call History Report

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

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 it takes longer to generate results.

To generate a Call History Report:

1. On the Call History and Loss Control page, click **Call History Report**.
2. On the Call History Report, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following filter criteria.
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
     - **Assigned Username**: the username assigned to a device by a system administrator on the View and Edit Custom Device Fields page.
     - **Serial Number**: the serial number of the device or other hardware.
     - **Asset Number**: the identification number associated with a device in the Absolute console.
     - **IMEI**: the International Mobile Equipment Identity (IMEI) number of the device, if applicable
     - **Subscriber ID**: also known as International Mobile Subscriber Identity (IMSI), the unique identifier associated with the subscriber
     - **Phone Number**: the phone number associated with the mobile device, if applicable

- **[Custom Device Fields]**: if one or more Custom Device Fields have been created for your account you can use them as filter criteria.

Depending on the criteria you selected from the preceding list, enter a value in the field, click **Choose** and select a value from the list, or use the Date Picker to specify a date or date range.

- To filter your results by Department, in the **and the Department is** field, open the list and select the appropriate department.
- To filter your results by date, in the **and the call occurred** area, do one of the following:
  - In the **in the last <n> days** field, click the option and enter the appropriate number of days. Any value from **1** through **365** is appropriate. A higher value in this field will result in a larger report and will take longer to generate results.
  - In the **between** field, click the option and enter the dates (dd/mm/yyyy) or click the **Calendar** icon to open the calendar dialog. Enter the dates in chronological order, with the earliest date entered first and the later date entered second.
- To filter your results by a specific IP address, in the **and IP address for** location:
  i) Open the list and select one of the following options:
    - **Public IP**
    - **Local IP**
  ii) Enter a valid IP address.

3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.

NOTE The background color of each column header indicates the applicability of the information. Current information has a lighter background whereas information that applied at the time of the agent call has a slightly darker background.

- **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
- **Serial Number**: the serial number of the device or other hardware.
- **Asset Number**: the identification number associated with a device in the Absolute console.
- **IMEI**: the International Mobile Equipment Identity (IMEI) number of the device, if applicable
- **Subscriber ID**: also known as International Mobile Subscriber Identity (IMSI), the unique identifier associated with the subscriber
- **Phone Number**: the phone number associated with the mobile device, if applicable
- **Make**: the manufacturer of the device.
- **Model**: the product type of a device or other hardware.
- **Device Name**: the name assigned to this device in the operating system.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Call Time**: when the device contacted the Monitoring Center.
- **Location (Latitude & Longitude)**: the position of the device on the surface of the earth expressed in latitude and longitude.

- **Local IP Address**: the IP address assigned to a device on the Local Area Network (LAN) when calling the Monitoring Center.
- **Public IP Address**: the IP address used to communicate with the Internet. For modem calls, caller ID information is reported instead. Click the **Public IP Address** link to open the Extended IP Call Information page. See "About Extended IP Call Information" on page 77.

Missing Devices Report

The Missing Devices Report has been retired. To view your devices that haven't called in to the Absolute Monitoring Center for 30 days or more, go to the Reports area and view the Dark Devices report. For more information, see *Dark Devices report* in the online Help.

Device Drift by Device Name Report

The Device Drift by Device Name Report has been retired. To view the devices with device name that changed within a specific time period, go to the History area and view the Events page. For more information, see *Monitoring events* in the online Help.

Device Drift by Username Report

The Device Drift by Username Report has been retired. To view the devices with a username that changed within a specific time period, go to the History area and view the Events page. For more information, see *Monitoring events* in the online Help.

Activation Report

The Activation Report has been retired. To view your devices that have completed a first check-in to the Absolute Monitoring Center, go to the Reports area and view the Activation report. For more information, see *Activation report* in the online Help.

Device Location History Report

NOTE If your account was migrated from Classic to ABS 7 Geolocation, the Device Location History Report will be available for one year after your migration date. The report will then be retired.

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.

The position of a device over time is represented as a set of icons on a map. The color of the icon indicates the timeframe of the information. The most recent locations are red, while locations reported in the past fade from red to white as they grow older. Clicking an icon opens a dialog that shows details about the devices that the icon represents.

Information in the results grid that shows below the map represents latitude and longitude coordinates, measured in decimal degrees.

NOTE You must log in to the Absolute console as an Administrator or Power User to perform the next task. Also note that 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 generate a Device Location History Report:

1. On the Call History and Loss Control page, click **Device Location History Report**.
2. On the Device Location History Report, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device, in **the Device is** field, click **Choose** to open the list and select the appropriate device.
   - To filter your results by date, at the **and a Location was determined between** area, do one of the following:
     - In the **in the last <n> days** field, click the option and enter the appropriate number of days. Any value from **1** through **365** is appropriate. A higher value in this field will result in a larger report and will take longer to generate results.
     - In the **between** field, click the option and enter the dates (dd/mm/yyyy) or click the calendar icon to open the calendar dialog. Enter the dates in chronological order, with the earliest date entered first and the later date entered second.
   - To filter your results by Location, at the **and the Confidence is** area, select one or both of the following options:
     - **Only show locations with high Confidence Levels**
     - **Only show a maximum of 500 locations**
   - To filter your results by location technology, at the **and the Location was obtained via** area, select one or more of the following options:
     - **Google Maps™ Wi-Fi Positioning**
     - **GPS**
     - **Other Location Technologies**
     - **Absolute Wi-Fi Positioning**
     - **IP Georesolution**
   - Click the **and show location** field and select one of the following options to indicate the scope of the location data to include in the report:
     - **between calls (all intermediate known locations)**
     - **at last call (last known location at last call)**

     NOTE If you selected only the Google Maps™ Wi-Fi Positioning option in the preceding step, the **at last call** option is selected by default and cannot be changed. This location technology collects location data at agent calls only.
3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.

   In the **results** grid, the device's locations show as icons on the map. All existing Geofence boundaries for your account also show.

   You can navigate the map using the following tools:

Tool	Description
Pan 	Use the Pan tool to move to a specific area of the map. Click one or more of the arrows until the desired area is in view. This tool is typically used in conjunction with the Zoom tool.
Zoom 	Use the Zoom tool to zoom in or out of specific areas of the map. • To zoom in, click + repeatedly, or move the slider towards the button. You can also zoom in by double-clicking the map or moving your mouse scroll wheel. • To zoom out, click − repeatedly, or move the slider towards the button. You can zoom out by moving your mouse scroll wheel.
Map | Satellite picker	Use the Map | Satellite tool to select a map type. To select a map type, perform one of the following actions: • To show a street map, click **Map**. This is the default option. • To show a street map with terrain and vegetation information, click **Map** and select **Terrain**. • To show a map of satellite images click **Satellite**. • To show a map of satellite images with place names, click **Satellite** and select **Labels**.
Go to Address 	Use the Go to Address tool to view a specific location on the map. To find a location, click the icon, enter the address of the location in the provided field, and press `Enter`. For greater accuracy provide a street address as well as city and state names.
Find Boundaries and Markers 	If multiple boundaries show on a map, use the Find Boundaries and Markers tool to view the boundaries individually. Click the icon repeatedly to step through each Geofence boundary and marker on the map.

NOTE The Device Location History Report uses Google Maps. If Google Maps are prohibited in your country (determined by the IP address of your computer), ESRI® maps show instead. For more information about working with ESRI maps, go to www.esri.com.

Each type of location technology shows a specific icon on the map:

 Google Maps Wi-Fi Positioning

NOTE If a device is located in a country where Google Maps is prohibited, this technology cannot be used to resolve the device's location.

 GPS

 Computers using other location technologies, such as API

 Mobile devices using other location technologies, such as CELL

 Absolute Wi-Fi Positioning

 IP Georesolution

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

4. Click an icon to open a dialog containing a **Zoom In** link to view the icon location, as well as the following details:
   - **Location Time**: the date and time of the last known location of the device.
   - **Location**: a link letting you zoom in to the last known location of the device.
   - **Location Technology**: the technology used to determine the location of the device.
5. The **results** grid below the map provides full details about the device's locations. Click a link in the **Location (Latitude, Longitude)** column to view a particular location on the map.

Lease and Inventory Management Reports

This section provides information on the following reports:

- Lease Completion Report
- User-Entered Data

Lease Completion Report

The Lease Completion Report identifies all assets that have leases expiring in a given time period. The Lease Completion Report does not show fields with null values.

By default, the Lease Completion Report's output includes devices that have a lease expiring within the next 30 days. You can change the range of dates to include in the results grid.

NOTE For detailed instructions on entering new lease information or updating information on existing leases, see *Editing Device Field data* in the online Help.

To generate a Lease Completion Report:

1. On the navigation bar, click to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
1. Under Lease and Inventory Management click **Lease Completion Report**.
2. On the Lease Completion Report, at the **Search Criteria** area. set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values:
     - **Asset Number**: the identification number associated with a device in the Absolute console.
     - **Assigned Username**: the username assigned to a device by a system administrator.
     - **Cost Center/Code**: a unique identifier for a unit for which costs are accumulated or computed.
     - **Device Name**: the name assigned to the device in the operating system.
     - **IP Address**: a unique number identifying a device on the Internet.

- **Lease Number**: a unique identifier assigned to a lease.
- **Lease Responsibility**: a party accountable for let goods.
- **Lease Vendor**: the provider of let goods. 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.
- **Purchase Order Reference**: a unique identifier associated with an authorization to buy goods or services.
- **Serial**: the serial number of this device.
- **Service Contract**: a provision of support and maintenance of goods.
- **User Phone/Extension**: the complete telephone number of an individual associated with a device.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Warranty Contract Vendor**: the warranty provider for a device.
- **Physical/Actual Location**: where the device resides.
- Any Custom Device Fields that you may have set are listed here and you can use them to filter your report.

Depending on the value you selected from the preceding list, you may want to further define this field. In the is or contains field, click **Choose** and select a value from the list.

- To filter your results by date, at the **and Lease End date is** area, do one of the following:
  - In the **in the last <n> days** field, click the option and enter the appropriate number of days. Any value from **1** through **365** is appropriate. A higher value in this field will result in a larger report and will take longer to generate results.
  - In the **between** field, click the option and enter the dates (dd/mm/yyyy) or click the **Calendar** icon to open the calendar dialog. Enter the dates in chronological order, with the earliest date entered first and the later date entered second.
- To filter your results by dates in a customer agreement, at the **and when the** area:

  i) Open the list and select one of the following options:
  - **Lease End Date**
  - **Lease Start Date**
  - **Service Contract End Date**
  - **Service Contract Start Date**
  - **Warranty End Date**
  - **Warranty Start Date**
  - **Device Purchase Date**

  ii) In the **is** field, select one of the following options:
  - **Before**
  - **On or after**
  - **On**

  iii) Enter the date (dd/mm/yyyy) or click the **Calendar** icon to select it.

  By default, the Lease Completion Report's output includes devices that have a lease expiring within the next 30 days.

3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.
   - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
   - **Field Name**: the custom device field used to filter the report in step 2.
   - **Field Value**: the value of the custom device field used to filter the report in step 2.
   - **Department**: the department to which this device belongs
   - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
   - **Make**: the manufacturer of a device or other hardware.
   - **Model**: the product type of a device or other hardware.
   - **Serial Number**: the serial number of this device.
   - **Asset Number**: the identification number associated with a device in the Absolute console.

User-Entered Data

The User-Entered Data Report lets you view all manually-entered data associated with your tracked devices, including all data stored in Custom Device Fields and data points that the agent is unable to capture automatically.

NOTE For more information about Custom Device Fields, see the online Help.

This section provides the following tasks:

- Generating a User-Entered Data Report
- Selecting the Data Points You Want to See

Generating a User-Entered Data Report

To generate a User-Entered Data Report:

1. On the navigation bar, click  to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
1. Under Lease and Inventory Management click **User-Entered Data Report**.
2. On the User-Entered Data Report, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values:
     - **Asset Number**: the identification number associated with a device in the Absolute console.
     - **Assigned Username**: the username assigned to a device by a system administrator.
     - **Cost Center/Code**: a unique identifier for a unit for which costs are accumulated or computed.

- **Device Name**: the name assigned to the device in the operating system.
- **Device Purchase Date**: the date the device was purchased.
- **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a Device.
- **Installation Date**: the date and time of first agent call to the Monitoring Center.
- **Lease Number**: a unique identifier assigned to a lease.
- **Lease Responsibility**: a party accountable for let goods.
- **Lease Vendor**: the provider of let goods. 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.
- **Purchase Order Reference**: a unique identifier associated with an authorization to buy goods or services.
- **Serial**: the serial number of this device.
- **Service Contract End Date**: when a provision of support and maintenance of goods ends.
- **Service Contract Start Date**: when a provision of support and maintenance of goods begins.
- **Service Contract Vendor**: the name of the provider of support and maintenance of goods.
- **User Phone/Extension**: the complete telephone number of an individual associated with a device.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Warranty Contract Vendor**: the warranty provider for a device.
- **Physical/Actual Location**: the physical location of the device.
- Any Custom Device Field that you may have set are listed here and you can use them to filter your report.

Depending on the value you selected from the preceding list, you may want to further define this field. In the **is or contains** field, click **Choose** and select a value from the list.

- To filter your results by date, at the **and when** area:
  i) Open the list and select one of the following options:
     - **Device Purchase Date**
     - **Installation Date**
     - **Lease End Date**
     - **Lease Start Date**
     - **Service Contract End Date**
     - **Service Contract Start Date**
     - **Warranty End Date**
     - **Warranty Start Date**

  ii) Do one of the following:
     - In the **in the last <n> days** field, click the option and enter the appropriate number of days. Any value from **1** through **365** is appropriate. A higher value in this field will result in a larger report and will take longer to generate results.

    - In the **between** field, click the option and enter the dates (dd/mm/yyyy) or click the **Calendar** icon to open the calendar dialog. Enter the dates in chronological order, with the earliest date entered first and the later date entered second.
- To filter your results by department, in the **and the Department** field, open the list and select the appropriate department.

3. Click **Show results**. The **results** grid refreshes to show the following data returned according to your filtering choices.
    - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open this device's Device Summary page. For more information, see "Editing Asset Information" on page 48.
    - **Asset Number**: the identification number associated with a device in the Absolute console.
    - **Device Name**: the name assigned to this device in the operating system.
    - **IP Address**: a unique number identifying a device on the Internet.

Selecting the Data Points You Want to See

To select which data points show in the results grid:

1. Complete the task, "Generating a User-Entered Data Report" on page 84.
2. In the **results** grid, click **Choose Columns**.
3. On the Custom Fields dialog, 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 **>>**.

   To remove a field from the **results** grid, select the field in the Selected Fields pane, and then click **<**. To remove all fields, click **<<**.
4. Repeat step 3 as needed to prepare the **results** grid format.
5. Click **OK** to return to the User-entered Data report page.

Account Management Reports

You can use Account Management reports to monitor and track agent licenses belonging to your organization, and to help resolve licensing issues.

NOTE Guest Users cannot access the Account Management Reports area and, therefore, cannot see any of the reports contained therein.

This section provides information on the following reports:

- License Usage Summary Report
- Calling Profiles Report
- User Audit Report
- User Event Report
- Security Audit Logs Report

Opening the Account Management Page

Complete the following task to open any of the Account Management reports included in this classification.

To open the Account Management page:

1. On the navigation bar, click to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. Click **Account Management**.

   The Account Management page shows all of the available reports.

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. On the Account Management page, click **License Usage Summary Report**.
2. On the License Usage Summary Report, in the **Name** field, enter a unique name for your report.
3. In the **Format** field, open the list and select one of the following options:
   - **CSV**: a plain text file with comma separated columns that is opened with software included in your operating system. Recommended for SQL queries and uploading large data files.
   - **XML**: a Unicode language file that is opened with an XML editor such as Microsoft Excel or OpenOffice. Recommended for filtering and formatting data.
4. At the Create E-mail Alert location, in the **Your E-mail address** field, enter your e-mail address if you want to receive an e-mail notification when the report is processed.
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. For more information, see "Downloading Reports" on page 56.

   The downloaded License Usage Summary shows the total number of licenses for each product. It also shows the following data:

   - **Total Installed**: combined total of all 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 total number of Service Guarantee licenses that have called the Monitoring Center in the last 30 days as a percentage.

Calling Profiles Report

The Calling Profiles Report provides detailed information on the calling patterns of each active device.

To download the Calling Profiles Report:

1. On the Account Management page, click **Calling Profiles Report** link.
2. On the Calling Profiles Report, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by Department, in the **and the Department** field, open the list and select the appropriate department.
   - To filter your results by specific device, in the **and the field** area, open the list and select one of the following values.
     - **Any of the fields in this list**: selects all the values in the list.
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device.
     - **Device Name**: the name assigned to the device in the operating system.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
     - **Serial Number**: the serial number of this device.
     - **Asset Number**: the identification number associated with a device in the Absolute console.
     - **Make**: the manufacturer of a device or other hardware.
     - **Model**: the product type of a device or other hardware.
     - **Assigned Username**: the username assigned to a device by a system administrator.

     Depending on the value you selected from the preceding list, you may want to further define this field. In the **is or contains** field, click **Choose** and select a value from the list.
3. At the **Name and Format** area, in the **Name** field, enter a unique name for your report.
4. In the **Format** field, open the list and select one of the following options:
   - **CSV**: a plain text file with comma separated columns that is opened with software included in your operating system. Recommended for SQL queries and uploading large data files.
   - **XML:** a Unicode language file that is opened with an XML editor such as Microsoft Excel or OpenOffice. Recommended for filtering and formatting data.
5. At the Create E-mail Alert location, in the **Your E-mail address** field enter your e-mail address if you want to receive an e-mail notification when the report is processed.
6. Click **Continue** to queue the download.

7. When your request is processed, retrieve the CSV or XML file of the report from the **My Reports** page. For more information, see "Downloading Reports" on page 56.

   The downloaded Calling Profiles includes the following data for each active device:

   - **ESN**: the device's Electronic Serial Number.
   - **Device Make**: the manufacturer of a device or other hardware.
   - **Device Model**: the product type of a device or other hardware.
   - **Department:**: the department to which this device belongs.
   - **Last Host Name**: the name of the server the agent called from.
   - **Last Username**: the unique name detected by the agent that identifies the person who is associated with this device at the last agent call.
   - **Serial Number**: the serial number for this device.
   - **Asset Number**: the identification number associated with a device in the Absolute console
   - **Activation Date**: the date the agent first contacted the Monitoring Center from a device.
   - **Last Caller ID**: the IP address for the origin of the incoming call by the agent to the Monitoring Center.
   - **Local IP**: the IP address assigned to a device on the Local Area Network (LAN) when calling the Monitoring Center.
   - **Agent Version Number**: the version number of the Absolute agent that contacts the Monitoring Center.
   - **First Call**: the date and time of the first agent call to the Monitoring Center.
   - **Last Call**: the date and time of the most recent agent call to the Monitoring Center.
   - **Second to Last Call**: the date and time of the second to last agent call to the Monitoring Center.
   - **Third Last Call**: the date and time of the third last agent call to the Monitoring Center.
   - **Fourth Last Call**: the date and time of the fourth last agent call to the Monitoring Center.
   - **Fifth Last Call**: the date and time of the fifth last agent call to the Monitoring Center.
   - **Calls 0-30 Days**: the number of agent calls to the Monitoring Center in the last 30 days.
   - **Calls 31-60 Days**: the number of agent calls to the Monitoring Center in the last 31-60 days.
   - **Calls 61-90 Days**: the number of agent calls to the Monitoring Center in the last 61-90 days.
   - **Calls Over 90 Days**: the number of agent calls to the Monitoring Center more than 90 days.
   - **All Calls**: the total number of agent calls to the Monitoring Center.

User Audit Report

The User Audit Report has been retired. To view changes to user accounts, go to the History area and view the Events page. For more information, see *Monitoring events* in the online Help.

User Event Report

The User Event Report has been retired. To view changes to user accounts, go to the History area and view the Events page. For more information, see *Monitoring events* in the online Help.

Security Audit Logs Report

Security Administrators can use the Security Audit Logs Report to view details about the following completed security actions related to Data Delete requests:

- Data Delete Request Cancelled
- Data Delete Log File Downloaded
- Data Delete Details Removed

The report includes all logged information that is typically used for audit purposes, such as the username of the user who initiated the security action, the date and time of the security action, and the device Identifier.

NOTE You can create an Alert to notify you when a particular security action occurs. For more information, see "Alerts" on page 8.

IMPORTANT You need to log in to the Absolute console as a Security Administrator to perform the next task.

To generate a Security Audit Logs Report:

1. On the Account Management page, click **Security Audit Logs Report**.
2. On the Security Audit Logs Report page, at the **Search Criteria** area, set the preferred filtering and display options for the report using one or more of the following criteria:
   - To filter your results by Device Group, in **the Group is** field, open the list and select the appropriate device group.
   - To filter your results by device, in the **and the field** area, open the list and select one of the following values.
     - **Any of the fields in this list**: selects all the values in the list
     - **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device
     - **Device Name**: the name assigned to the device in the operating system
     - **Username**: the unique name detected by the agent that identifies the person who is associated with the device
     - **Make**: the manufacturer of a device or other hardware
     - **Model**: the product type of a device or other hardware
     - **Serial Number**: the serial number of the device
     - **Requested By**: the username of the Security Administrator or Security Power User who submitted the request
     - **Data Delete Policy**: the name of the Data Delete policy associated with the request, if applicable
     - **IMEI**: the International Mobile Equipment Identity (IMEI) number of the device, if applicable

     Depending on the value you selected from the preceding list, you may want to further define this field. In the **is or contains** field, click **Choose** and select a value from the list.
   - To filter your results by date, in the **and the Security Action occurred** area do one of the following:

- Select the **in the last <n> days** option and enter a number of days in the field. Values between **1** and **365** are supported.
- Select the **between** option and enter the applicable dates (dd/mm/yyyy) in the two fields. Enter the dates in chronological order (earliest date in the first field and the later date in the second field). Alternatively, click the **Calendar** icons to open the calendar dialog.

- To filter your results by the security action associated with the Data Delete request, click the **and the Security Action is** field and select an option.

3. Click **Show results**. The results grid refreshes to show the following information based on your defined search criteria:

- **Date and Time**: the date and time when the security action was completed
- **Request ID**: the identifier assigned to the Data Delete request by the system
- **Identifier**: a unique Electronic Serial Number assigned to the agent that is installed on a device
- **Requested By**: the username of the Security Administrator or Security Power User who submitted the request
- **Security Action**: the security action associated with the logged event

  Possible values are:

  - Data Delete Request Cancelled
  - Data Delete Log File Downloaded
  - Data Delete Details Removed

- **Data Delete Type**: the setting associated with a Data Delete request, if applicable

  Possible values are:

  - Custom Policy
  - All Files
  - Lost or Stolen Device - Delete all Files and OS
  - Device End of Life - Delete all Files, Sector Wipe, and OS
  - Firmware Drive Wipe
  - Mobile Device

  For more information about these options, see "Data Delete Settings" on page 1.

- **Data Delete Policy**: the name of the Data Delete policy associated with the request, if applicable
- **Username**:the unique name detected by the agent that identifies the person who is associated with this device
- **Device Name**: the name assigned to the device in the operating system
- **Serial Number**: the serial number of this device
- **IMEI**: the International Mobile Equipment Identity number of the device, if applicable
- **Make**: the manufacturer of a device or other hardware
- **Model**: the product type of a device or other hardware

My Content

The My Content reporting area is where you store your saved reports and filter criteria. The reports provided in the **My Content** area include:

- My Reports
- My Filters

My Reports

All reports can be downloaded as a Comma Separated Value (CSV) or eXtensible Markup Language (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.

The My Reports page shows all requested report downloads and includes the following information for each report:

- **Report Requested On**: shows the date and time when the CSV or XML file was requested.
- **Report Name**: shows the name assigned to the CSV or XML request.
- **Report Type**: indicates the report type; for example, **Group Import**.
- **File Size**: shows the size of the report file you requested.
- **Status**: indicates the status of the request, which can have the possible values of **In Queue**, **Ready**, and **Error**.

To view the My Reports page and download a processed report:

1. On the navigation bar, click to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. Under My Content, click **My Reports**.
4. On the My Reports page, in the row containing the appropriate report in the **Status** column, click the **Ready** link and follow the on-screen instructions to download the report.

> **NOTE** When your file request is being processed, the **Status** column shows **In Queue** and the report is not available. When processed, the **Status** column shows the **Ready** link and, if requested, you receive an e-mail notification.

My Filters

The My Filters page shows all saved report filters. Saved filters define the criteria for a report, not the report's output contained in the results grid. Data that meets this criteria may change with time, so the report output can change as well.

To use a saved report filter:

1. On the navigation bar, click to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. Under My Content, click **My Filters**.
4. On the My Filters page, click the appropriate **Filter** name in the table.

The report is regenerated based on the saved filter criteria.

Editing Saved Report Filters

To edit a saved report filter:

1. On the navigation bar, click  to open the Reports page.
2. Near the bottom of the page, click **Go to Classic Reports Page**.
3. Under My Content, click **My Filters**.
4. On the My Filters page, click the appropriate **Filter** name in the table.
5. The report is regenerated based on the saved filter criteria.

   Edit the existing filters and click **Show results**. The report regenerates and shows on the page.
6. If necessary, save the modified filters as a new saved filter. For more information, see "Saving Report Filters" on page 55.

NOTE The original saved report remains unchanged.

Chapter 5: Using Real-Time Technology

The Real-Time Technology (RTT) service provided real-time communications using SMS messaging for devices with a supported mobile broadband adapter.

The RTT feature has been retired and is no longer available.

Chapter 6: Using Real-Time Technology over IP

Real-Time Technology over IP (RTT-IP) reduced the time it took for an account Administrator to invoke remote operations such as Data Delete on managed Windows and Mac devices.

The RTT-IP feature has been retired and is no longer available.

Index

A

B

C

D

M

N

O

P

R

S

T

U

V

W