<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associating Devices with Device Groups</td>
<td>43</td>
</tr>
<tr>
<td>Adding Devices to a Device Group</td>
<td>43</td>
</tr>
<tr>
<td>Adding Devices to a Device Group Automatically Based on Local IP Addresses</td>
<td>45</td>
</tr>
<tr>
<td>Using Bulk Uploads to Change Device Group Associations</td>
<td>46</td>
</tr>
<tr>
<td>Viewing the Devices in a Device Group</td>
<td>49</td>
</tr>
<tr>
<td>Removing Devices from a Device Group</td>
<td>49</td>
</tr>
<tr>
<td>Deleting Device Groups</td>
<td>49</td>
</tr>
<tr>
<td>Software Policy</td>
<td>50</td>
</tr>
<tr>
<td>Adding Devices to a Device Group Without a Software Policy</td>
<td>51</td>
</tr>
<tr>
<td>Creating a Software Policy</td>
<td>51</td>
</tr>
<tr>
<td>Creating a Software Policy by Copying an Existing One</td>
<td>53</td>
</tr>
<tr>
<td>Viewing a Software Policy</td>
<td>53</td>
</tr>
<tr>
<td>Editing a Software Policy and its Device Group Associations</td>
<td>53</td>
</tr>
<tr>
<td>Deleting a Software Policy</td>
<td>54</td>
</tr>
<tr>
<td>Managing Classic Account Settings</td>
<td>54</td>
</tr>
<tr>
<td>Editing Classic Account Settings</td>
<td>54</td>
</tr>
<tr>
<td>Manually Editing Service Guarantee License Assignment</td>
<td>58</td>
</tr>
<tr>
<td>Managing Event Calling for Your Account</td>
<td>59</td>
</tr>
<tr>
<td>Events That Can Trigger an Event Call</td>
<td>60</td>
</tr>
<tr>
<td>Understanding the Minimum Event Call Period</td>
<td>61</td>
</tr>
<tr>
<td>Turning on Event Calling for Your Account</td>
<td>61</td>
</tr>
<tr>
<td>Editing Event Calling Settings</td>
<td>62</td>
</tr>
<tr>
<td>Turning Off Event Calling</td>
<td>63</td>
</tr>
<tr>
<td>Viewing the List of Devices with Event Calling Turned On</td>
<td>63</td>
</tr>
<tr>
<td>Managing SCCM Status Reporting and Repair for your Account</td>
<td>64</td>
</tr>
<tr>
<td>Managing SCCM Status Reporting for Your Account</td>
<td>64</td>
</tr>
<tr>
<td>Managing SCCM Repair for Your Account</td>
<td>65</td>
</tr>
<tr>
<td>Viewing the List of Devices with SCCM Status Reporting Turned On</td>
<td>66</td>
</tr>
<tr>
<td>Downloading Packages For Your Account</td>
<td>67</td>
</tr>
<tr>
<td>Downloading the Absolute Agent for Android Devices</td>
<td>67</td>
</tr>
<tr>
<td>Upgrading to the Latest Version of the Agent</td>
<td>68</td>
</tr>
<tr>
<td>Testing Your Network for Agent Connectivity</td>
<td>68</td>
</tr>
<tr>
<td>Using the Absolute Manage Suite</td>
<td>69</td>
</tr>
<tr>
<td>Downloading the Absolute Manage Installation Packages</td>
<td>69</td>
</tr>
<tr>
<td>Uploading a Stamped Agent Including Absolute Manage</td>
<td>69</td>
</tr>
<tr>
<td>Downloading the Absolute SIEM Connector</td>
<td>71</td>
</tr>
<tr>
<td>Managing System Notifications</td>
<td>72</td>
</tr>
<tr>
<td>Updating the System Notifications Page</td>
<td>73</td>
</tr>
<tr>
<td>Devices With the Service Guarantee Not Calling</td>
<td>73</td>
</tr>
<tr>
<td>Resolving a Recovery Flag Disparity</td>
<td>73</td>
</tr>
<tr>
<td>Viewing Pending Agent Removal Requests</td>
<td>74</td>
</tr>
<tr>
<td>Managing Your iPads</td>
<td>76</td>
</tr>
<tr>
<td>Importing iPad Serial Numbers into the Absolute Console</td>
<td>76</td>
</tr>
<tr>
<td>Removing iPads from the Absolute Console</td>
<td>77</td>
</tr>
<tr>
<td>Selecting iPads to Remove</td>
<td>77</td>
</tr>
<tr>
<td>Uploading a Device List to Remove iPads</td>
<td>77</td>
</tr>
<tr>
<td>Chapter 3: Generating Reports</td>
<td>Chapter 4: Working with Reports</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Running Reports</td>
<td>Hardware Assets Reports</td>
</tr>
<tr>
<td>Navigating Reports</td>
<td>Opening the Hardware Assets Page</td>
</tr>
<tr>
<td>Expanding and Collapsing the Search Criteria Information</td>
<td>Asset Report</td>
</tr>
<tr>
<td>Using the Choose Feature</td>
<td>Printer Report</td>
</tr>
<tr>
<td>Viewing an Entire Row in a Report Record</td>
<td>Monitor Report</td>
</tr>
<tr>
<td>Moving Between the Pages of a Report</td>
<td>Hardware Configuration and OS Change Report</td>
</tr>
<tr>
<td>Changing the Number of Records That Show in a Report</td>
<td>Hard Disk Space Report</td>
</tr>
<tr>
<td>Changing the Sort Order</td>
<td>Device Readiness Report</td>
</tr>
<tr>
<td>Editing Asset Information</td>
<td>Mobile Broadband Adapter Report</td>
</tr>
<tr>
<td>Device Information on the Device Summary Page</td>
<td>Mobile Device Report</td>
</tr>
<tr>
<td>Hardware Summary Tab</td>
<td>Software Assets Reports</td>
</tr>
<tr>
<td>Software Summary Tab</td>
<td>Opening the Software Assets Page</td>
</tr>
<tr>
<td>Call Tracking Tab</td>
<td>Installed Software Overview Report</td>
</tr>
<tr>
<td>SCCM Status History Tab</td>
<td>Requesting New Software Applications to Include in the Installed Software Overview Report</td>
</tr>
<tr>
<td>Managing Event Calling for a Device</td>
<td>Software Configuration Change Report</td>
</tr>
<tr>
<td>Configuring Event Calling for a Device</td>
<td>Software by Device Report</td>
</tr>
<tr>
<td>Viewing the Call History for a Device</td>
<td>Software License Compliance Overview Report</td>
</tr>
<tr>
<td>Managing SCCM Status Reporting for a Windows Device</td>
<td>Editing License Information</td>
</tr>
<tr>
<td>Managing SCCM Repair for a Windows Device</td>
<td>Viewing a Devices by License Report</td>
</tr>
<tr>
<td>Using the Assigned Username Field</td>
<td>Microsoft Audit Summary Report</td>
</tr>
<tr>
<td>Using the Dormant Devices Field</td>
<td></td>
</tr>
<tr>
<td>Printing Reports</td>
<td></td>
</tr>
<tr>
<td>Saving Report Filters</td>
<td></td>
</tr>
<tr>
<td>Editing Saved Report Filters</td>
<td></td>
</tr>
<tr>
<td>Downloading Reports</td>
<td></td>
</tr>
<tr>
<td>Multi-level Security</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling Geolocation Reporting .......................... 164
Device Location Report ........................................ 165
Device Location History Report .......................... 168
Lease and Inventory Management Reports .................. 171
Lease Completion Report .................................. 171
User-Entered Data ........................................ 173
Generating a User-Entered Data Report .................. 174
Selecting the Data Points You Want to See ............... 175
Account Management Reports .............................. 176
Opening the Account Management Page .................. 176
License Usage Summary Report .......................... 176
Calling Profiles Report .................................... 177
User Audit Report .......................................... 179
User Event Report ........................................ 180
Security Audit Logs Report ................................ 181
My Content .................................................. 183
My Reports .................................................. 183
My Filters .................................................... 183
Editing Saved Report Filters .............................. 184

### Chapter 5: Using Real-Time Technology .............. 185
What is Real-Time Technology? ............................ 185
Minimum System Requirements ........................... 185
Working with RTT ........................................... 186
Viewing Mobile Broadband Adapter Information ........ 187
Editing the Phone Number Override ..................... 187
Viewing the Forced Call Log ............................. 188
Initiating a Forced Call ..................................... 188

### Chapter 6: Using Real-Time Technology over IP ..... 190
Minimum System Requirements ........................... 190
Understanding How RTT-IP Works ......................... 190
Prerequisites of RTT-IP ..................................... 191
Accelerating Operations With RTT-IP ..................... 191
Viewing RTT-IP Status for a Device .................... 191
Enabling RTT-IP ............................................ 192
Enabling RTT-IP for All Devices in Your Account ........ 192
Enabling RTT-IP for an Individual Device ............... 192
Requesting a full agent call using RTT-IP ............... 193
Editing the RTT-IP Ping Period ............................ 193
Editing the RTT-IP Ping Period for All Devices in Your Account .......................... 193
Editing the RTT-IP Ping Period for a Device ............ 194
Viewing RTT-IP Status for All Devices .................. 194
Disabling RTT-IP ............................................ 195
Disabling RTT-IP for All Devices in Your Account ........ 195
Disabling RTT-IP for an Individual Device ............... 196

### Chapter 7: Securing Your Data and Devices ........... 197
Before You Begin ............................................. 197
Security Administration Authorization Agreement ................................................................. 198
  Downloading and Submitting the Authorization Agreement ................................................. 198
  Disabling Security Access for All Authorized Security Users ............................................... 199
  Removing Security Access for One Specific Security Administrator ..................................... 199
  Removing Security Access by Submitting an Absolute Technical Support Case ..................... 200
  Removing Security Access by Suspending the User Account ............................................... 200

Security Authentication Methods ............................................................................................. 201
  Using RSA SecurID Tokens for Security Services ................................................................. 201
  Using RSA SecurID Token Codes .......................................................................................... 202
  Transferring RSA SecurID Tokens ....................................................................................... 202
  Using E-mailed Authorization Codes for Security Services .................................................... 202
  Requesting a Security Authorization Code ......................................................................... 203
  Changing E-mail Addresses for Authorized Security Personnel ........................................... 203
  Changing Your Security Authentication Method .................................................................... 203
  Managing Custom Action Fields ........................................................................................... 203
  Creating Custom Action Fields ............................................................................................ 204
  Editing Custom Action Fields .............................................................................................. 204
  Deleting Custom Action Fields ............................................................................................ 205

Chapter 8: Concluding Intel Anti-Theft Technology Support .................................................. 206
  Troubleshooting Intel AT Disenrollment ............................................................................... 206
  Viewing the Disenrollment Status of Devices ....................................................................... 206
  Unlocking Devices Using a Server Recovery Token .............................................................. 207
  Generating a Server Recovery Token .................................................................................... 207
  Using a Server Recovery Token to Unlock a Locked Device ................................................. 208

Chapter 9: Using Data Delete .................................................................................................. 209
  Minimum System Requirements ............................................................................................. 209
  Deletion Algorithms ............................................................................................................... 209
  Prerequisites for Data Delete ................................................................................................ 210
  Requesting a Data Delete Operation ..................................................................................... 210
  Initiating a Data Delete Request ......................................................................................... 211
  Deletion Logs ........................................................................................................................ 214
  Data Delete Settings ............................................................................................................. 214
  Data Delete Settings for Windows Devices .......................................................................... 214
  Selecting a Data Delete Type Option .................................................................................... 215
  Selecting Data Delete Options .............................................................................................. 217
  Data Delete Settings for Mac Devices .................................................................................... 218
  Data Delete Settings for Mobile Devices .............................................................................. 218
  Deletion Policies .................................................................................................................... 218
  Using Sample Policy File Entries .......................................................................................... 219
  Deleting a Folder Based on a Windows System Variable ...................................................... 219
  Creating a Data Delete Policy ............................................................................................... 220
  Using Data Delete Policy Templates ...................................................................................... 222
  Working with Deletion Policies ............................................................................................ 222
  Tracking Data Delete Status .................................................................................................. 223
  Viewing Data Delete Status .................................................................................................. 223
  Data Delete Details Page ....................................................................................................... 225
  Viewing or Printing an End of Life Data Delete Certificate .................................................. 227
  Removing Details of a Data Delete Operation ........................................................................ 228

Absolute 7.x
Forcing a Data Delete Operation to Complete ................................................................. 229
Clearing Perpetual Data Delete .............................................................. 229
Deleting or Cancelling a Data Delete Request ................................................................. 229
Deleting a Draft Data Delete Request ................................................................. 229
Cancelling a Data Delete Request for a Single Device ......................................................... 230
Cancelling Data Delete Requests for Multiple Devices ............................................................... 230
Deletion Log Files ........................................................................................................ 230
Viewing the Deletion Log File .................................................................................... 232
Viewing the Deletion Log for a Single Device ................................................................ 232
Viewing the Deletion Logs for Multiple Devices ................................................................. 232
Viewing the Deletion Log on a Mobile Device ................................................................. 233

Chapter 10: Using Device Freeze ............................................................................... 234
Minimum System Requirements .................................................................................... 234
Working with Device Freeze Requests ........................................................................ 235
Requesting a Device Freeze ........................................................................................ 236
Cancelling a Device Freeze Request ........................................................................... 239
  Cancelling a Device Freeze Request For a Single Device ........................................... 239
  Cancelling Device Freeze Requests For Multiple Devices ......................................... 239
Removing Device Freeze Request Details ..................................................................... 240
  Removing Details of a Single Device Freeze Request ............................................... 240
  Removing Details of Multiple Device Freeze Requests ............................................. 241
Managing Device Freeze Offline Policies .................................................................... 241
Creating a Device Freeze Offline Policy ....................................................................... 242
Working with Existing Offline Policies ......................................................................... 244
Searching for a Device Freeze Offline Policy .............................................................. 245
Editing a Device Freeze Offline Policy .......................................................................... 245
Designating a Default Offline Policy ............................................................................ 247
Managing Devices Associated with a Device Freeze Offline Policy ................................ 248
  Viewing Devices Associated With an Offline Policy ................................................. 248
  Adding Devices to an Offline Policy ......................................................................... 249
  Removing Devices from an Offline Policy .................................................................. 250
Deleting a Device Freeze Offline Policy ....................................................................... 251
Tracking Device Freeze Status .................................................................................... 251
  Viewing Device Freeze Status ................................................................................... 252
  Viewing Device Freeze Requests .............................................................................. 254
    Viewing Details about a Device Freeze Request .................................................. 255
    Viewing Devices Frozen by an Offline Policy ......................................................... 257
Unfreezing a Frozen Device ....................................................................................... 258
  Unfreezing a Device on Agent Call ........................................................................... 258
    Unfreezing a Single Device on Agent Call ............................................................ 258
    Unfreezing Multiple Devices on Agent Call ............................................................ 259
  Using an Unfreeze Passcode on the Targeted Device ................................................. 259
    Viewing the Unfreeze Passcode ............................................................................. 259
    Unfreezing a Device With a Passcode .................................................................... 260
Managing Custom Device Freeze Messages ................................................................. 261
Creating a Custom Device Freeze Message .................................................................. 261
Including Phone Numbers in Custom Device Freeze Messages ........................................ 262
Editing Existing Custom Device Freeze Messages ......................................................... 263
Deleting Existing Custom Device Freeze Messages .............................................. 263

Chapter 11: Managing Geofences ........................................................................ 265
Geofencing Security .......................................................................................... 265
Authorizing Geolocation Tracking .................................................................. 265
Using Geofence Technology ............................................................................ 266
Understanding Geolocation Maps .................................................................... 267
Map Navigation Tools ...................................................................................... 267
Geofence Tools ................................................................................................. 267
Creating Geofences ......................................................................................... 268
Viewing Geofences ........................................................................................... 269
Editing Geofences ............................................................................................. 270
Deleting Geofences ........................................................................................... 271

Chapter 12: Using Remote File Retrieval ............................................................. 272
Minimum System Requirements ......................................................................... 272
Before You Begin ............................................................................................... 272
Requesting a Remote File Retrieval .................................................................. 273
Viewing the File Retrieval Status ...................................................................... 273
Downloading Retrieved Files ............................................................................ 275
  Downloading Retrieved Files Using Internet Explorer ...................................... 275
  Downloading Retrieved Files Using FireFox or Another Browser .................... 275
Changing the File Retrieval Status ..................................................................... 275
  Cancelling a File Retrieval Request ................................................................ 276
Removing Retrieved Files and Log Files .......................................................... 276

Chapter 13: Using File List ................................................................................... 278
Overview ............................................................................................................ 278
Minimum System Requirements ......................................................................... 279
Retrieving a List of Files on Stolen Devices ....................................................... 279
  Downloading a File List Request ..................................................................... 280
Tracking File List Status ..................................................................................... 280
  Viewing the Status of a File List Request ........................................................ 281
Changing a File List Status ................................................................................ 282
  Cancelling a File List Request ......................................................................... 282
Removing Retrieved Files and Log Files .......................................................... 282

Chapter 14: Absolute for Chromebooks ............................................................... 284
Adding Chromebooks to your Absolute Account ............................................. 284
  Managing Google Account Details in the Absolute Console ......................... 285
    Adding Google Account Details to the Absolute Console ............................ 285
    Editing Google Account Details .................................................................... 286
    Deleting Google Account Details .................................................................. 287
    Deploying the Chromebook extension .......................................................... 287
Working with Chromebooks in the Absolute console ....................................... 288
Removing the Chromebook Extension from a Device ........................................ 289

Chapter 15: Reporting the Theft of a Managed Device ........................................ 290
Investigation Checklist ....................................................................................... 290
Viewing Existing Investigation Reports and Their Report History ........................................... 291
  Viewing the Report History Table ...................................................................................... 293
Creating an Investigation Report .......................................................................................... 293
  Minimum System Requirements ......................................................................................... 294
Understanding the Prepaid Service Guarantee Balance ......................................................... 294
  Viewing the Prepaid Service Guarantee Balance ................................................................. 294
Before You Begin .................................................................................................................. 294
Submitting an Investigation Report ....................................................................................... 295
Editing Existing Investigation Reports .................................................................................... 297
Cloning an Existing Report ................................................................................................... 299
Closing an Open Investigation Report .................................................................................... 299
Managing the Investigation Report Contact List .................................................................... 300
  Adding Contacts to the Investigation Report Contact List .................................................. 300
  Editing Contact Information ............................................................................................... 301
  Viewing and Printing the Investigation Report Contact List .............................................. 302
Disabling Contacts ................................................................................................................ 302
  Activating Disabled Contacts ............................................................................................. 303
Glossary ................................................................................................................................... 304
Index ....................................................................................................................................... 320
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, formerly DDS 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
- Using this Guide
- Conventions Used in this Guide

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.

User Roles

There are five distinct user roles that can be filled by one or more people.

- **Administrators** manage their organization's devices and IT assets, and report device loss or theft. Administrators also create and manage various system communications, such as end user messaging, system notifications, and alerts and suspicious alert events.

- **Security Administrators** exist in those organizations that choose to designate certain Administrators as Security Administrators to manage the device and data security of assets. This user role has more access rights than Administrators.
Security Administrators are authorized to configure, target, and start File Retrieval, Device Freeze, and Data Delete services. Security Administrators use the Absolute console to track and manage devices, both within the organization’s local area network and outside of it.

- **Power Users** have access rights to most features excluding security features. Administrators can restrict Power Users rights to specific Identifiers or Device Groups.
- **Security Power Users** exist in those organizations that choose to designate certain Power Users as Security Power Users to manage the device and data security of assets. This user role has more access rights than Power Users.
  Security Power Users are authorized to configure, target, and start File Retrieval, Device Freeze, and Data Delete services for devices in their assigned Device Group. Security Power Users use the Absolute console to track and manage devices within the organization’s local area network.
- **Guest Users** have limited access to information and reports. These users cannot alter or assign user access rights and cannot alter details on the page. Members of the Guest User group can only browse Investigation Reports they have created and can only view reports they have saved.

Other User Roles
The following user roles, although not defined in the User section of the Absolute console, are important to its overall operation.

- **Signing Officers** assume responsibility for the Security Administrators’ and Security Power Users’ actions. Signing Officers are notified each time a Data Delete request is made.
  Signing Officers are two senior managers in an organization who have signing authority on their company’s behalf.
- **IT Technicians** are usually responsible for installing the agents on devices within their organizations.

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, device groups, and end user messaging.
- "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.
- "Securing Your Data and Devices" describes data and device security services that enable users with security authorization to ensure that managed devices and their data are not compromised in cases of device loss or theft.
- "Concluding Intel Anti-Theft Technology Support" provides information to help you troubleshoot the disenrollment of your managed devices from Intel® AT. The Intel AT service was terminated by Intel in early 2015.
- "Using Data Delete" describes the Data Delete functionality, and the procedures required to start and manage Data Delete operations.
- "Using Device Freeze" describes the Device Freeze functionality, including how to initiate freeze requests and create custom freeze messages.
- "Managing Geofences" describes the Geofencing functionality and the procedures required to manage Geofencing boundaries.
- "Using Remote File Retrieval" describes the Remote File Retrieval functionality.
- "Using File List" describes how to remotely request a File List, which facilitates requesting a Remote File Retrieval.
- "Absolute for Chromebooks" describes how to manage your Chromebook devices in the Absolute console.
- "Reporting the Theft of a Managed Device" describes the procedures used to report the loss or theft of managed devices, as well as how to view and manage Investigation Reports. This chapter also includes a checklist to follow when you submit an Investigation Report and a Service Guarantee Submission form to Absolute.
- "Glossary" provides a list of acronyms, as well as the terms and their definitions used throughout this guide.

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 ctnst.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 Create and Edit 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
- End User Messaging
- Geofences
- Device Groups
- Software Policy
- Managing Classic Account Settings
- Downloading Packages For Your Account
- Managing System Notifications
- Viewing Pending Agent Removal Requests

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 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 129.). 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.
NOTE Alert events can be sent to a Security Information and Event Management (SIEM) application. If you are using a SIEM application and you want the ability to view and analyze Absolute alert events in your SIEM application, along with events from other sources, download the Absolute SIEM Connector to a computer on your network. For more information, see "Download the Absolute SIEM Connector" on page 71.

This section provides information about the following topics and tasks:
- About Predefined Alerts
- Creating New Custom Alerts
- Examples of Alert Conditions
- 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 24.

When the predefined alerts are activated, they perform as described in the following table. See "Activating Alerts" on page 25.

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 26.

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

Predefined Alerts and their Descriptions

<table>
<thead>
<tr>
<th>Predefined (Default) Alerts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Is Newly Installed</td>
<td>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.</td>
</tr>
<tr>
<td>Change in Serial Number</td>
<td>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.</td>
</tr>
<tr>
<td>Device Name Changed</td>
<td>This alert is triggered when a device name change is detected on a managed device. It is set with a Suspicion level of 3.</td>
</tr>
</tbody>
</table>

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.
### Predefined Alerts and their Descriptions (continued)

<table>
<thead>
<tr>
<th>Predefined (Default) Alerts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Rebuild</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>● Operating system product key is changed</td>
</tr>
<tr>
<td></td>
<td>● Device has made a Self Healing Call</td>
</tr>
<tr>
<td>Hard Drive Nearly Full</td>
<td>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%.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Last called 20 days ago</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>In other words, when the device calls in, the alert no longer triggers for that device.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Lease Ending</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Local IP Address Changed</td>
<td>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.</td>
</tr>
<tr>
<td>Major Change</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>● Operating system product key is changed</td>
</tr>
<tr>
<td></td>
<td>● Device name is changed</td>
</tr>
<tr>
<td></td>
<td>● Username is changed</td>
</tr>
<tr>
<td></td>
<td>● Device has made a Self Healing Call</td>
</tr>
</tbody>
</table>
## Predefined Alerts and their Descriptions (continued)

<table>
<thead>
<tr>
<th>Predefined (Default) Alerts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing Software on Required List</td>
<td>This alert is triggered for non-compliance of a Software Policy. Missing Software on a Required List alert triggers for any managed device that is detected without the required software packages installed. If this alert is configured to reset automatically, it is triggered on the same devices each day until corrective action is taken and the device no longer violates this policy.</td>
</tr>
<tr>
<td>Modem Changed</td>
<td>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.</td>
</tr>
<tr>
<td>Network Changed</td>
<td>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.</td>
</tr>
<tr>
<td>New Program File Detected</td>
<td>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.</td>
</tr>
<tr>
<td>Operating System Changed</td>
<td>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.</td>
</tr>
<tr>
<td>Operating System Product Key Changed</td>
<td>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.</td>
</tr>
<tr>
<td>Public IP Address Changed</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Predefined Alerts and their Descriptions (continued)

<table>
<thead>
<tr>
<th>Predefined (Default) Alerts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Healing Call</td>
<td>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.</td>
</tr>
<tr>
<td>Software on Banned List</td>
<td>This alert is triggered for non-compliance of a Software Policy. Software that is defined as banned triggers an alert if it is detected on any device. If this alert is configured to reset automatically, it is triggered on the same devices each day until corrective action is taken to ensure that the device no longer violates this policy.</td>
</tr>
<tr>
<td>Username Changed</td>
<td>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.</td>
</tr>
<tr>
<td>Warranty Ending</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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 Alerts tab, and click Create and Edit Alerts.
2. 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.
3. In the Alert description field enter a detailed description for this alert.
4. 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 129.

**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.
5. 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**.

6. 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.

7. 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.

8. 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.

9. 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.

10. If you do not want to activate the alert at this time, select the Suspend alert scanning option.

11. 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.

Examples of Alert Conditions

The following examples describe some commonly used conditions for alerts:
• Creating a Geofence Alert
• Creating a Security Action Alert
• Creating an Alert Based on Full-Disk Encryption Status Criteria

Creating a Geofence Alert

To set an alert condition to trigger an alert when a device moves outside of its geofence location:

1. On the navigation bar click ☰, click the Alerts tab, and click Create and Edit Alerts.
2. On the Create and Edit Alerts page in the Conditions area, open the Field list and select the value Geofence Location.
3. The Condition area refreshes. Complete the following steps:
   a) Open the Rule list and select one of the following options:
Is Inside: creates an alert whenever a device travels inside a specified Geofence boundary.

Is Outside: creates an alert whenever a device travels outside a specified Geofence boundary.

b) The field next to the Rule field contains the list of Geofences that exist for your account. Open the list and select the appropriate Geofence name.

c) The remaining fields let you specify the time frame after which the alert is triggered. Enter the appropriate number in the for at least field and select Hours, Days, or Weeks to specify the unit of time.

4. Click **Add condition**.

5. Enter the rest of the information that is appropriate to this Geofence alert as described in step 6 through step 11 of the task, “Creating New Custom Alerts” on page 19.

Creating a Security Action Alert

You can create an alert that is triggered when a user initiates an action related to a Data Delete or Device Freeze request.

To trigger an alert when a security action occurs:

1. On the navigation bar click | Alerts | , click the **Alerts** tab, and click **Create and Edit Alerts**.

2. On the Create and Edit Alerts page in the **Conditions** area, open the **Field** list and select **Security Action**.

3. Open the **Rule** list and select one of the following actions:

   - Data Delete Request Cancelled
   - Data Delete Details Removed
   - Data Delete Log File Downloaded
   - Data Delete Requested
   - Device Freeze Details Removed
   - Device Freeze Requested
   - Device Freeze Request Cancelled
   - Unfreeze Requested
   - Unfreeze Request Cancelled

4. Click **Add condition**.

5. Enter the rest of the information that is appropriate to this alert as described in step 6 through step 11 of the task, “Creating New Custom Alerts” on page 19.

Creating an Alert Based on Full-Disk Encryption Status Criteria

You can create alerts based on encryption status strings and conditions set in the filtering area of the Full-Disk Encryption Status Report. For more information about this type of report, see "Full-Disk Encryption Status Report" on page 132. For example, you may want to receive an alert whenever the Encryption Status String changes.
IMPORTANT Currently, the Full-Disk Encryption Status Report only provides information about full-disk encryption products installed on the system or the first physical drive only.

To create an encryption alert:

3. On the Full-Disk Encryption Status Report page, at the and where the Encryption Status String area, set the preferred filtering for the report. For more information, see "Filtering Data to Create a Full-Disk Encryption Status Report" on page 134.
4. Click the Create an alert based on this encryption status criteria link.
5. A warning dialog opens indicating that any unsaved search criteria will be lost if you proceed. To proceed, click OK.
6. On the Create and Edit Alerts page, in the Alert name field, enter an appropriate name for this alert.
7. In the Alert description field, enter an appropriate description for this encryption alert.
8. Open the Suspicion level list and select the appropriate level as described in step 2 of the task, "Creating New Custom Alerts" on page 19.
9. The Conditions table includes the options you provided when you filtered the data on the Full-Disk Encryption Status Report. See "Filtering Data to Create a Full-Disk Encryption Status Report" on page 134.

If needed, you can define more conditions for triggering an encryption alert as follows:

a) Open the Rule list and choose from the following options, if applicable:
   - Begins with
   - Changed
   - Contains
   - Does Not Begin With
   - Does Not Contain
   - Is
   - Is Not

b) Depending upon your selections from the Field and Rule lists, the Criteria field may open. Click Choose to open the Choose dialog and select the appropriate entry from the list. Only those products detected for your account show on the Choose dialog. Select the appropriate one, which is added to your conditions automatically.

c) Click Add condition.
   The page refreshes to show the new condition or conditions you set for this alert in the Condition table.

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

10. Enter the rest of the information that is appropriate to this encryption alert as described in step 6 through step 11 of the task, "Creating New Custom Alerts" on page 19.
If you stop full-disk encryption, when you turn this feature on again you need to reactivate any encryption alerts you created. For more information, see "Reactivating Suspended Alerts" on page 25.

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:

On the navigation bar click [1], click the Alerts tab, and click View and Manage Alerts.

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 [1], click the Alerts tab, and click View and Manage Alerts.
2. On the View and Manage Alerts page, you can search as follows:
At the Search Criteria area open 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 Alerts tab, and click View and Manage Alerts.
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 Alerts tab, and click View and Manage Alerts.
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 2 through step 11 of the task, “Creating New Custom Alerts” on page 19.

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 Alerts tab, and click View and Manage Alerts.
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 and do one of the following:
   - To reset an alert on all devices on which the alert was triggered:
     i) Click the Alerts tab and click View and Manage Alerts.
     ii) On the View and Manage Alerts page select the checkbox for the Active alert you want to reset. You cannot reset a Suspended alert.
     iii) Click Reset. The alert is reset on all devices on which it was triggered.
   - To reset an alert on individual devices:
     i) Click the Alerts tab and 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 .
2. You can suspend alerts in one of the following ways:
   - To create a custom alert in the Suspended state:
     i) Click the Alerts tab and click Create and Edit Alerts.
     ii) Follow the instructions provided in the task, ”Creating New Custom Alerts” on page 19.
     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 the Alerts tab and 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 Alerts tab, and click View and Manage Alerts.
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 Alerts tab, and click Alert Events.
2. 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:
  1. Open 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.
  2. In the **is or contains field**, enter a value.

- To filter your results by the suspicion level, do the following:
  1. 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
  2. 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:
  1. 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.
  2. 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.

3. 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**.
Chapter 2: Setting Up Your Work Environment

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 27.
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 **Download**.
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 92.

End User Messaging

The End User Messaging feature lets Administrators communicate with the end users of managed devices through custom or URL messages. End User Messaging occurs during the agent call to the Monitoring Center. Administrators can also solicit information from end users through end user messaging that populates Custom Device Fields. For more information, the online Help.

Administrators can create any number of end user messages and deploy them to all of their organization’s devices, a specific device group, or a particular device.

There are two types of end user messages:

- Custom messages that can solicit data from end users. See "Creating Custom End User Messages" on page 30.
- URL messages that open the end users’ browser windows to a specified website. See "Creating URL End User Messages" on page 32.

End User Messaging is only available on devices that run the following supported operating systems:

- Windows operating systems with Internet Explorer
- Mac operating systems
This section describes the following tasks:
- Creating End User Messages
- Previewing End User Messages
- Editing End User Messages
- Activating an End User Message
- Suspending an End User Message
- Viewing End User Message Acknowledgements
- Resending End User Messages
- Deleting End User Messages

**IMPORTANT** To perform the tasks in this section, you must log in to the Absolute console as an Administrator.

Creating End User Messages

This section describes the following tasks:
- Creating Custom End User Messages
- Creating URL End User Messages

Creating Custom End User Messages

To create a custom end user message:

1. On the navigation bar click **Data > End User Messaging**. The End User Messaging page shows a list of end user messages.
2. Click **Create new end user message**.
3. On the Create End User Message page at the **Message information** area, in the **Message Name** field enter a descriptive name for the new message. The message name is for your reference only and is not shown to the end user.
4. At the **Message content** area, complete the following information:
   a) In the **Message Type** options, click the **Custom message** option.
   b) In the **Message Title** field enter the title that you want to show on the title bar of the message sent to end users.
   c) In the **Message Text** field you can enter text and URL links, as well as the following standard HTML tags:
      
      `<a>    <b>    <i>    <u>`
      `<font>    `<p>    `<br>`

   d) If you want to include an image with your message, do the following:
      - Enter the **Image URL** for the image you want to show.
      - Open the **Image Display Location** list and select where in the message you want to image to show.
      - In the **Image Hyperlink** field, enter or paste the appropriate hyperlink to the image you want to show.

You are limited to one image per message.
e) If you are soliciting information from your end users, click **Choose fields**, which opens the Custom Fields Dialog. The left column of the dialog shows all **Available Fields**, which you can add to the message. The right column of the dialog provides a list of all currently **Selected Fields**.

From the **Available Fields** list, click the fields you want to include in the message and click > to move them to the **Selected Fields** list. Click >> to move all available fields to the **Selected Fields** list. If you mistakenly move an available field to the **Selected Fields** list, you can select it and click < to move it back to the **Available Fields** list. When finished, click **OK**.

The Fields dialog closes and the Create End User Message page refreshes to show the **Selected Fields** as a list of checkboxes at the **Included Fields** area.

f) Under the **Required** heading, select the checkbox for each field you want to specify as mandatory.

The end user needs to provide information for these mandatory fields to successfully submit a response to the End User Message.

5. At the **Message destination** area in the **Send To** area, indicate the appropriate option that defines the devices that receive the message as follows:

   - Click **All Devices** to send the end user message to all devices, which includes future activations.
   - Click **Specific Device**, click **Choose device**, and then select the device you want to receive the end user message.
   - Click **Specific Group**, click **Choose group**, and then select the **Group Name** you want to receive the end user message. Any device added to or removed from this group is similarly added to or removed from the message. You must define the device group before you can select it. For more information, see "Creating a New Device Group" on page 40.

   **IMPORTANT** When an End User Message is applied to a **Specific Group**, any device added to or removed from that group is similarly associated or disassociated with the end user message.

6. At the **Message display** area in the **Message Display Criteria (Rules)** options, select the option that defines the frequency with which the message is presented to end users from the following available options:

   - **On next call** presents the message to end users on the device’s next call to the Monitoring Center.
   - **On or after** opens a field where you enter the date or you can click the **Calendar** icon to select the appropriate date to send the message.

7. Review the message you have created and then take one of the following options to save the message:

   - Click **Save & activate**. The message is activated and shows on qualifying devices according to the defined Message Display option.
   - Click **Save & suspend** to preview the message. Before activating it, see "Previewing End User Messages" on page 33. No devices receive this message until it is activated. This option is recommended.
The End User Messaging page refreshes the results grid to include the new Custom End User message.

Creating URL End User Messages

A Uniform Resource Locator (URL) message shows any World Wide Web address in the end user’s browser. The Absolute console does not make a record of when the end user acknowledges receipt of a URL message.

To create a URL message:

1. On the navigation bar click ▶️ > Data > End User Messaging.
2. On the End User Messaging page, click Create new end user message.
3. On the Create End User Message page, at the Message information area in the Message Name field, enter a descriptive name for the new message. This message name is for your reference only and is not shown to the user.
4. In the Message content area, do the following:
   a) Click the URL option and type the address including the protocol; for example, http://.
   b) Select one of the following options for delivering your end user message:
      - Attempt to send once indicates that the message is sent only once, on the next agent call.
      - Send repeatedly indicates that the message is sent on all agent calls.
        This frequency is useful when the end user has signed out a device and failed to return it by the due date. When the device is returned, you can suspend or delete the message.
5. At the Message destination area in the Send To area, indicate the appropriate option that defines the devices that receive the message as follows:
   - To send the end user message to all devices, including future activations, click All Devices.
   - To send the end user message to a single device, click Specific Device, click Choose device, and then select the device.
   - To send the end user message to all devices in a device group, click Specific Group, click Choose group, and then select the Group Name you want to receive the end user message. You must define the group before you can select it. For more information, see “Creating a New Device Group” on page 40.

**IMPORTANT** When an End User Message is applied to a Specific Group, any device added to or removed from that group is similarly associated or disassociated with the end user message.

6. At the Message display area in the Message Display Criteria (Rules) options, select the option that defines the frequency with which the web page is presented to end users from the following available options:
   - On next call presents the web page to end users on the device’s next call to the Monitoring Center.
   - On or after opens a field where you enter the date or you can click the Calendar icon to select the appropriate date to send the message.
7. Review the message you have created and save it using one of the following options:
Click **Save & activate** to save the message and activate it immediately.

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

The End User Messaging page refreshes to show the new URL message in the **results** grid, which shows a list of end user messages.

**Previewing End User Messages**

After you create a custom or URL end user message, preview the message before sending it to end users.

To preview an end user message:

1. On the navigation bar click **Data > End User Messaging**.
2. On the End User Messaging page in the **results** grid, click the **Message Name** link for the message you want to preview.
3. On the Create End User Message page, click **Preview in New Window** to open the message in a new window.

**NOTE**  Ensure your browser is configured to allow popups.

Review the message and close the window.

4. Choose from one of the following options:
   - Edit the message. See "[Editing End User Messages](#)" on page 33.
   - Click **Save & activate**. The message shows on qualifying devices on their next agent call.
   - Click **Save & suspend**. No devices receive this message until the message is activated.

**Editing End User Messages**

This section describes the following tasks:

- [Editing a Custom End User Message](#)
- [Editing a URL End User Message](#)

**Editing a Custom End User Message**

To edit an existing custom end user message:

1. On the navigation bar click **Data > End User Messaging**.
2. On the End User Messaging page, in the **results** grid click the **Message Name** or the **Edit** link for the **Active** message you want to edit. (You cannot edit a **Suspended** message.)
3. On the Create End User Message page, make the appropriate changes to the message as follows:
   a) At the **Message information** area in the **Message Name** field, enter the appropriate information.
   b) At the **Message Status** area, click **Suspend** so you can make these changes before the qualifying devices call the Monitoring Center.
c) At the Message content area, select Custom message under Message Type and do the following:
   - Click the Message Title field and enter the updated information.
   - Click the Message Text field and type the appropriate updates.
   - If you want to use a different image, enter the appropriate information in the Image URL field, open the list for Image Display Location and select the correct option, and in the Image Hyperlink field enter the updated information.

d) If you are editing the information you requested from your end users, click Choose fields, which opens the Custom Fields dialog.
   The left column of the dialog shows all Available Fields, which you can add to the message. The right column of the dialog provides a list of all currently Selected Fields.
   Click the fields you want to include in the message and click > to move to the Selected Fields list. Click >> to move all available fields to the Selected Fields list. If you mistakenly move an available field to the Selected Fields list, you can select it and click < to move it back to the Available Fields list. When finished, click OK.
   The Fields dialog closes and the End User Message page refreshes to show the Selected Fields as a list of checkboxes at the Included Fields options location.

e) Select the Required checkbox for each field you want to specify as mandatory.
   The end user needs to provide information for these fields to successfully submit a response to the end user message.

f) Click OK.
   The Fields dialog closes and the End User Message page refreshes to show the Selected Fields as a list of checkboxes at the Included Fields options location.

g) Select the Required checkbox for each field you want to specify as mandatory.
   The end user needs to provide information for these fields to successfully submit a response to the end user message.

4. At the Message destination area in the Send To options, define the end users who receive the message as follows:
   - To send the end user message to all devices, including future activations, click All Devices.
   - To send the end user message to a single device, click Specific Device, click Choose device, and then select the device.
   - To send the end user message to all devices in a device group, click Specific Group, click Choose group, and then select the Group Name you want to receive the end user message. You must define the group before you can select it. For more information, see "Creating a New Device Group" on page 40.

   **IMPORTANT** When an End User Message is applied to a Specific Group, any device added to or removed from that group is similarly associated or disassociated with the end user message.

5. At the Message display location, in the Message Display Criteria (Rules) options, select the option that defines the frequency that the web page is presented to end users from the following available options:
Chapter 2: Setting Up Your Work Environment

- **On next call** presents the web page to end users only once, that is on the device's next call to the Monitoring Center.
- **On or after** opens a calendar dialog where you select the appropriate date to send the message.

Leave the Re-send checkbox unchecked. For more information, see "Resending End User Messages" on page 38.

6. Review the changes you have made to this message. You have the following options to save the message:
   - Click Save & activate to save the message and activate it immediately.
     The End User Messaging page refreshes the results grid with a list of end user messages that includes the message you edited. Notice that the Status has changed to Active.
   - Click Save & suspend to save the message and suspend it. You can activate the message later.
     The End User Messaging page refreshes the results grid with a list of end user messages that includes the message you edited. Notice that the Status is Suspended.

Editing a URL End User Message

To edit an existing URL end user message:
1. On the navigation bar click 🏛 > Data > End User Messaging.
2. On the End User Messaging page, in the grid click the Message Name or the Edit link for the message you want to edit.
3. On the Create End User Message page at the Message information area, make the appropriate changes to the message as follows:
   - a) In the Message Name field, enter the appropriate information.
   - b) At the Message Status location, click Suspend so you can make these changes before the qualifying devices call the Monitoring Center.
4. At the Message content area at the Message Type options, in the URL option field, do the following:
   - a) In the field type the address including the protocol; for example, http://.
   - b) Select one of the following options for delivering your end user message:
     - Attempt to send once indicates that the message is sent only once, on the next agent call.
     - Send repeatedly indicates that the message is sent on all agent calls.
     This frequency is useful when the end user has signed out a device and failed to return it by the due date. When the device is returned, you can suspend or delete the message.
5. At the Message destination location, in the Send To options, define the end users who receive the message as follows:
   - To send the end user message to all devices, including future activations, click All Devices.
   - To send the end user message to a single device, click Specific Device, click Choose device, and then select the device.
To send the end user message to all devices in a device group, click **Specific Group**, click **Choose group**, and then select the **Group Name** you want to receive the end user message. You must define the group before you can select it. For more information, see "Creating a New Device Group" on page 40.

**IMPORTANT** When an End User Message is applied to a **Specific Group**, any device added to or removed from that group is similarly associated or disassociated with the end user message.

6. At the Message display location, in the **Message Display Criteria (Rules)** options, select the option that defines the frequency that the web page is presented to end users from the following available options:

- **On next call** presents the web page to end users on the device’s next call to the Monitoring Center.
- **On or after** opens a calendar dialog where you select the appropriate date to send the message.
- The **Re-send** checkbox lets you resend messages that were already sent and acknowledged. For more information, see "Resending End User Messages" on page 38.

7. Review the changes you have made to this message. You have the following options to save the message:

- Click **Save & activate** to save the message and activate it immediately.
  The End User Messaging page refreshes the **results** grid with a list of end user messages that includes the message you edited. Notice that the **Status** has changed to **Active**.

- Click **Save & suspend** to save the message and suspend it. You can activate the message later.
  The End User Messaging page refreshes the **results** grid with a list of end user messages that includes the message you edited. Notice that the **Status** is **Suspended**.

**Activating an End User Message**

Only activated end user messages are sent to managed devices that meet the message criteria.

To activate existing custom and URL end user messages:

1. On the navigation bar click **Data > End User Messaging**.
2. On the End User Messaging page in the **results** grid, click the **Message Name** or **Edit** link for a **Suspended** message you want to activate.
3. On the Create End User Message page click **Save & activate**.
4. The End User Messaging page refreshes. Look at the **results** grid to see that the message you selected now reads **Active** in the **Status** column.

**Suspending an End User Message**

You can suspend messages that you temporarily do not want to send to end users.

To suspend an end user message:

1. On the navigation bar click **Data > End User Messaging**.
2. On the End User Messaging page in the **results** grid, click the **Message Name** or **Edit** link for an **Active** message that you want to suspend.

3. On the Create End User Message page click **Save & suspend**.

4. The End User Messaging page refreshes. Look at the **results** grid to see the message you selected now reads **Suspended** in the **Status** column.

### Viewing End User Message Acknowledgements

You can see the custom end user messages that were and were not acknowledged by end users. You can also download the details in a report. If you solicited information from end users in a message, you can review the responses. For those devices that did not acknowledge the message, you may want to research why that is the case.

To view end user message acknowledgements:

1. On the navigation bar click \> **Data > End User Messaging**.

2. On the End User Messaging page in the **results** grid, review the **Devices Acknowledged** column. The hyperlinked numbers shown in this column represent the number of devices that have acknowledged the respective end user messages.

   To see which devices have acknowledged the end user message you sent, click the numeric link.

3. On the Devices that have acknowledged End User Message page, you can see the devices that have responded to your message. If you have solicited information from the end user, you can find it here.

   For more information about this device and the device’s user, click the **Identifier**.

   On the Device Summary, you can see who to contact to get further information or possibly to send another message.

4. Click the **Back** link to return to the Devices that have acknowledged End User Message page.

5. To download a report of the devices that have acknowledged the end user message, at the top of the **results** grid click \.

   On the Request Report page, complete the following steps:
   
   a) In the **Report Name** field, enter a name for this report you want to download.

   b) Open the **Report Format** list and select a file format.

   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**.

   When your request is processed, you can retrieve the report file from the My Reports page. For information on retrieving reports, see "[Downloading Reports](#) on page 92.

6. Click the **Back** link to return to the End User Messaging page.

To view end user messages that were not acknowledged by the targeted devices:

1. On the navigation bar click \ > **Data > End User Messaging**.
2. On the End User Messaging page in the **results** grid, review the **Devices Not Acknowledged** column. The hyperlinked numbers shown in this column represent the number of devices that have not acknowledged the respective end user messages.

   To see which devices have not acknowledged the end user message you sent, click the numeric link.

3. On the Devices that have NOT acknowledged End User Message page, you see the devices that have failed to respond. For more information about this device and the device’s user, click the **Identifier**.

   On the Device Summary, you can see who to contact to get further information or possibly to send another message.

4. Click the **Back** link to return to the Devices that have NOT acknowledged End User Message page.

5. To download a report of the devices that have not acknowledged the end user message, at the top of the **results** grid click **↓**.

   On the Request Report page, complete the following steps:
   a) In the **Report Name** field, enter a name for this report you want to download.
   b) In the **Report Format** field, open the list and select a file format.
   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**.

   When your request is processed, you can retrieve the report file from the My Reports page. For information on retrieving reports, see “**Downloading Reports** on page 92.”

6. Click the **Back** link to return to the End User Messaging page.

**Resending End User Messages**

There are times when it is useful to resend a message that was already received and acknowledged by end users. For example, you could edit an existing complex custom message and resend it, instead of taking the time to create a new custom message.

To resend an end user message:

1. On the navigation bar click **Data > End User Messaging**.

2. On the End User Messaging page in the **results** grid, click the **Message Name** or **Edit** link for the message you want to resend.

3. On the Create End User Message page at the Message Display location, select the **Re-send** checkbox.

4. To save this setting, do one of the following:
   - Click **Save & activate** to save the message. This message is shown to qualifying devices according to the defined Message Display option.
   - Click **Save & suspend** to save the message and suspend it. You can activate the message later. No devices receive this message until you activate it.
Deleting End User Messages
You may want to delete end user messages that are no longer required.

To delete end user messages:

1. On the navigation bar click ☰ > Data > End User Messaging.
2. On the End User Messaging page in the results grid, click the Message Name or Edit link for the message you want to delete.
   The End User Message page refreshes with a confirmation indicating the message you selected is deleted.

Geofences
The Geofences feature lets Administrators specify geographical boundaries, based on geolocation tracking data, to help locate managed devices. Geofencing is available to all accounts that have downloaded the Geolocation Authorization Agreement from the Support page in the Absolute console, signed it, and delivered it to Absolute.

Geofence details and tasks are provided in the topic, "Managing Geofences" on page 265.

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 end user messaging.

This section describes the following tasks:
- Creating a New Device Group
- Viewing All Device Groups
- Viewing a Specific 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 ☐️ > Device Groups > Classic Groups.
3. 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 4 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.

4. 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.

5. Click the << Back link to close this page and open the Device Groups page.

**Viewing All Device Groups**

To view all device groups:

1. On the navigation bar click ▲ ▼ > Device Groups > Classic Groups.

On the Device Groups page, look at the results grid, which shows all device groups that belong to your account.

**NOTE** If you are logged in as a Power User or a Guest, you can view only those device groups to which you are assigned.
Viewing a Specific Device Group

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

1. On the navigation bar click ▶️ > Device Groups > Classic Groups.

2. 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.

3. 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.

Editing a Device Group

To edit a device group’s information:

1. Complete the task, "Viewing a Specific Device Group" on page 42.

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. See "Viewing a Specific Device Group" on page 42.
   - 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:
   - 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 43.

You can also remove selected devices from the group. For more information, see "**Removing Devices from a Device Group**" on page 49.

### 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 the 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 Specific Device Group**" on page 42.
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 \[ \text{Import Classic Group <-> IP Mapping} \] 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 \[ \text{Import/Export} \] and click Import/Export on the Administration sidebar.
   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 Administration 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 \( 
   \text{ Groups } \) 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 \( 
   \text{ Groups } \) and click **Import/Export** on the Administration 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 the Devices in a Device Group

To view the devices in a device group:
1. Complete the task, "Viewing a Specific Device Group" on page 42.
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 80.
You can also use the Asset Report to view devices within a group. For more information, see "Asset Report" on page 94.

Removing Devices from a Device Group

To remove any or all devices from a device group:
1. Complete the task, "Viewing All Device Groups" on page 41.
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. See "Viewing a Specific Device Group" on page 42.
   ● 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 All Device Groups" on page 41.
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. For more information about assigning users to device groups,

---

**Software Policy**

Software policies allow Administrators to define their organization’s software rules. A software policy is a list of Banned and Required software titles. Software policies are applied to device groups, after which non-compliant devices are identified using the Software Policy Non-Compliance Report.

A single device may belong to multiple device groups, so it is possible for multiple software policies to apply to a single device. In this scenario, the Software Policy Non-Compliance Report shows any occurrence of non-compliance.

This section describes the following tasks:

- Viewing the List of Software Policies
- Viewing Device Groups Without a Software Policy
- Creating a Software Policy
- Creating a Software Policy by Copying an Existing One
- 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 50.

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 51.

• 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 53.

### Creating a Software Policy

To create a software policy:

1. On the navigation bar click **[Policy Groups]** > **Software Policies** to open the Create and Edit a Software Policy page.

2. In the **Policy Name** field, enter a descriptive name for the policy.

3. In the **Description** field, enter a brief description of the policy.

4. At the right side of the **Policy Groups** field, click **Add Classic Groups** to open the Choose Classic Groups for Software Policy dialog.

5. 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.

6.  **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**.

7.  **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 6.

8.  **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.

Creating a Software Policy by Copying an Existing One

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

1. On the navigation bar click **Edit > 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 53.

Viewing a Software Policy

To view a software policy:

1. Complete the task, "Viewing the List of Software Policies" on page 50.
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 **Edit > 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:
   
   a) In the **Policy Name** field, edit the existing name as appropriate.
   
   b) 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 6 of the task, "Creating a Software Policy" on page 51.

7. Do one of the following:

   a) 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:
- **Open** to show the contents of this software policy in Microsoft Excel.
- **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 53.
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 Classic 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 following features for your devices:

- Full-Disk Encryption data collection
- Event Calling
- SCCM Status and Repair
- Google Maps Wi-Fi Positioning
- RTT-IP

**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:

- Managing Classic Account Settings
- Managing Service Guarantee Licenses
- Managing Event Calling for Your Account
- Managing SCCM Status Reporting and Repair for your Account

**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 57.

**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 58.

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 25.

   For more information about full-disk encryption, see "Full-Disk Encryption Status Report" on page 132.

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 130.

   **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 130.
7. At the **Absolute Customer Service Account Access** area, we recommend that you select the **Allow Absolute customer service staff access to your account** option, if it is not selected by default. From time to time, it may be necessary for an Absolute representative to log in to your account to investigate a problem or correct an issue, and this option enables them to perform these actions.

   Note that when the option is enabled:

   - Absolute customer service staff *can't* perform the following actions on your account:
     - Submit a request for any of the following security actions:
       - Data Delete
       - Device Freeze
     - Submit an Investigation Report
   - All login and logout events performed by Absolute customer service staff are logged for your account. For more information, see *User Event Report* on page 180.

8. 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.

   If you use Data Delete, enable this setting to ensure that when you select the **Include File Date Attributes** option during a Data Delete request, the last file access date and time is included in the Deletion log file. This information helps to determine if a data breach has occurred on a device. For more information about requesting a Data Delete, see *Initiating a Data Delete Request* on page 211.

   **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.

9. To use Google Maps™ Wi-Fi Positioning to find the locations of your managed devices, in the **Google Maps™ Wi-Fi Positioning** area, select the **Use Google Geolocation for Wi-Fi Points** checkbox.

   When you enable this setting:

   - Google Maps Wi-Fi Positioning can be used to find the locations of your managed devices. For more information, see *Understanding Location Technologies* on page 162.
   - The Google Maps™ Wi-Fi Positioning option is available, and selected by default, in the Geofences feature and Geolocation Tracking reports. For more information, see the following topics:
     - "Creating Geofences" on page 268
     - "Geolocation Tracking Reports" on page 161
• The setting is hidden on the Classic Account Settings page.

**NOTE**  This setting is applicable only if Geolocation Tracking is authorized for your account. For more information, see "Authorizing Geolocation Tracking" on page 265.

10. At the **SCCM Status and Repair** area, configure SCCM Status reporting and SCCM Repair for the Windows devices in your account.

**IMPORTANT**  With the release of Absolute 7.2, you can now use the Application Persistence feature to report on and repair SCCM clients installed on your Windows devices. If you have SCCM Report and Repair enabled, we recommend that you disable it and activate the Application Persistence: Microsoft SCCM policy in one or more policy groups. For more information, see About Application Persistence: Microsoft SCCM policies in the online Help.

For more information, see "Managing SCCM Status Reporting and Repair for your Account" on page 64.

11. At the **RTT-IP Setting** area, make any changes to your account-wide RTT-IP settings. For more information about RTT-IP and its various settings see "Using Real-Time Technology over IP" on page 190.

12. 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 59.

**NOTE**  You can also manage Event Calling at the device level. For more information, see "Editing Asset Information" on page 80.

13. If the **Chromebooks - Google Account** area is available, and you want to manage your Chromebook devices in the Absolute console, see "Managing Google Account Details in the Absolute Console" on page 285.

14. 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.
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 58.

- **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 58.

- **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 58.

### 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:

- device location
- 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 60.

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:

<table>
<thead>
<tr>
<th>Event Calling turned on?</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>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. If RTT-IP is enabled for the account, the Administrator immediately requests a security operation, such as a Device Freeze. If the device is online, the agent is instructed at the next RTT-IP ping to make a full agent call and the security operation is performed. If the device is off-line, the security operation is performed on the next reboot.</td>
</tr>
<tr>
<td>No</td>
<td>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. If RTT-IP is enabled for the account, the Administrator immediately requests a security operation, such as a Device Freeze. If the device is online, the security operation is performed at the next RTT-IP ping, but RTT-IP alone does not accelerate the initiation of the Alert itself.</td>
</tr>
</tbody>
</table>

For more information about Alerts, see "Alerts" on page 15. For more information about RTT-IP, see "Using Real-Time Technology over IP" on page 190.
This section provides information on the following topics:

- Events That Can Trigger an Event Call
- Understanding the Minimum Event Call Period
- Turning on Event Calling for Your Account
- Editing Event Calling Settings
- Turning Off Event Calling
- Viewing the List of Devices with Event Calling Turned On

**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 80.

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**

<table>
<thead>
<tr>
<th>Change event/Configuration option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Location change                  | A change in the location of a device  
Wi-Fi hotspots are used to identify changes in device location. If the signal strength or availability of the Wi-Fi hotspots stored in a device changes, the device is considered to have changed its location. A location change event is logged only if the current Wi-Fi hotspots indicate that the device moved approximately 200 meters, which is the average range of a Wi-Fi hotspot. |
| 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. |
Description of change events that trigger an event call (continued)

<table>
<thead>
<tr>
<th>Change event/Configuration option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network change</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 61.

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 $^1$ 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 60.

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 $\mathbb{H}$ > **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 86.
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 61.

5. Edit the **Configuration Options** by selecting or clearing each applicable checkbox.

**NOTE** For more information about each option, hover over \(^i\) 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 60.

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 86.

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

1. On the navigation bar click \(\text{ocean icon}\) > **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 \(\text{ocean icon}\) > **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 SCCM Status Reporting and Repair for your Account

**IMPORTANT** With the release of Absolute 7.2, you can now use the Application Persistence feature to report on and repair SCCM clients installed on your Windows devices. If you have SCCM Report and Repair enabled, we recommend that you disable it and activate the Application Persistence: Microsoft SCCM policy in one or more policy groups. For more information, see *About Application Persistence: Microsoft SCCM policies* in the online Help.

If you use Microsoft Service Center 2012 Configuration Manager (SCCM), you can configure the following options on the Classic Account Settings page:

- **Collect SCCM Status on Windows devices**: track the status of the SCCM client installed on the Windows devices in your account. For more information about SCCM and detecting SCCM Status information, see "*About Collecting SCCM Status From Windows Devices*" on page 141.
- **Enable SCCM Repair**: repair any SCCM clients that are not functioning correctly. For more information about this feature, see "*About Repairing SCCM Clients*" on page 141.

This section provides information on the following topics:

- Managing SCCM Status Reporting for Your Account
- Managing SCCM Repair for Your Account
- Viewing the List of Devices with SCCM Status Reporting Turned On

Managing SCCM Status Reporting for Your Account

**IMPORTANT** With the release of Absolute 7.2, you can now use the Application Persistence feature to report on and repair SCCM clients installed on your Windows devices. If SCCM Status Reporting is enabled, we recommend that you disable it and activate the Application Persistence: Microsoft SCCM policy in one or more policy groups. For more information, see *About Application Persistence: Microsoft SCCM policies* in the online Help.

You can track the status of the SCCM client installed on the Windows devices in your account.

When SCCM Status reporting is enabled at the account level:

- The agent is updated on each device on the next agent call. The update includes a script, run every six hours, to detect the status of the device’s SCCM client. The script performs a series of health check tests to determine if the client is present and functioning correctly.
- As new Windows devices are activated, SCCM Status reporting is automatically enabled on those devices.
The most recent SCCM Status information for each Windows device shows in the SCCM Status Report.

A history of SCCM Status changes for each Windows device shows in the SCCM Status History Report, and the SCCM Status History tab of each device’s Device Summary page.

You can use the Alerts feature to trigger an alert notification when a SCCM Status change occurs. For more information about creating Alerts, see "Creating New Custom Alerts" on page 19.

**NOTE** You can also manage SCCM Status reporting for individual devices or groups of devices. For more information, see the following topics:
- "Managing SCCM Status Reporting for a Windows Device" on page 88
- "Managing SCCM Status Reporting and Repair in the SCCM Status Report" on page 145

To disable SCCM Status Reporting for all devices in your account:

1. On the navigation bar click ➕ > Classic Account Settings.
2. Scroll to the SCCM Status and Repair area.
3. Clear the Collect SCCM Status from Windows devices checkbox.
4. Click Save changes.

Managing SCCM Repair for Your Account

**IMPORTANT** With the release of Absolute 7.2, you can now use the Application Persistence feature to report on and repair SCCM clients installed on your Windows devices. If you have SCCM Repair enabled, we recommend that you disable it and activate the Application Persistence: Microsoft SCCM policy in one or more policy groups. For more information, see About Application Persistence: Microsoft SCCM policies in the online Help.

You can use the SCCM Repair feature to repair any SCCM clients that are installed on your managed Windows devices and are not functioning correctly.

This feature works in conjunction with the SCCM Status reporting feature. When SCCM Repair is enabled at the account level:

- The agent is updated on each device on the next agent call. The update includes a script, run every six hours, to detect the status of the device’s SCCM client and automatically repair the client if it is not functioning correctly.
- As new Windows devices are activated, SCCM Repair is automatically enabled on those devices.
- The most recent SCCM Repair information for each Windows device shows in the SCCM Status Report.
- A history of SCCM Repair information for each Windows device shows in the SCCM Status History Report, and the SCCM Status History tab of each device’s Device Summary page.
- You can use the Alerts feature to trigger an alert notification when SCCM Repair occurs on a device. For more information about creating Alerts, see "Creating New Custom Alerts" on page 19.
To disable SCCM Repair for all devices in your account:

1. On the navigation bar click \( \text{Classic Account Settings} \).
2. Scroll to the SCCM Status and Repair area.
3. Clear the Enable SCCM Repair checkbox.
4. Click Save changes.
5. On the Confirm message dialog, review the details of the requested action to confirm that they are correct, and click Continue.

Viewing the List of Devices with SCCM Status Reporting Turned On

To view the list of managed Windows devices that have SCCM Status Reporting turned on:

1. On the navigation bar click \( \text{Classic Account Settings} \).
2. Scroll to the SCCM Status and Repair area.
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
   - **SCCM Status**: the current status of the SCCM client on this device. Possible values are:
     - **Absent**: the SCCM client is not installed on the device.
     - **Needs attention**: One or more health check tests failed and SCCM Repair is not enabled on the device. You may want to enable SCCM Repair for the device.
     - **OK**: all health check tests passed and the SCCM client is functioning correctly.
     - **Repair failed**: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was not repaired. For more details about why the repair failed, click the link.
     - **Repair successful**: SCCM Repair is enabled. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was repaired.

5. Sort the list by clicking a column heading.
6. To view the Device Summary page for a device, click the Identifier link.
7. Click Cancel to close the dialog.
Downloading Packages For Your Account

Depending on the Absolute products your organization has purchased, the Download Packages page may contain the following sections:

- **The Agent for Mobile Operating Systems** section lets you download Android agent installation packages for your account. For more information, see "Downloading the Absolute Agent for Android Devices" on page 67.

**NOTE** To download Windows and Mac agent installation packages, go to Agent Management in the Administration area. For more information, see Downloading the Absolute agent for Windows and Mac devices in the online Help. Agent installation packages are not available for iPads. For information about managing iPads, see "Managing Your iPads" on page 76. To inquire about support for the agent on a Linux-based operating system, such as Ubuntu 16.04 LTS or Debian® 8.x, contact Absolute Technical Support.

- The **Absolute for Chromebooks Extension** section contains details for deploying the Absolute for Chromebooks extension, which lets you to manage your Chromebooks in the Absolute console. This section applies only to customers with Absolute for Chromebooks licenses. For more information, see "Deploying the Chromebook extension" on page 287.

- The **Network Diagnostics** section lets you download a command line utility to check if your network configuration will allow the Absolute agent to contact the Absolute Monitoring Center. For more information, see "Testing Your Network for Agent Connectivity" on page 68.

- The **Absolute Manage** section lets you upload and download Absolute Manage installation packages for your account. For more information, see "Using the Absolute Manage Suite" on page 69.

- The **Absolute SIEM Connector** section lets you download the SIEM Connector installation package. The SIEM Connector uses the syslog protocol to send alert events triggered in the Absolute console to your Security Information and Event Management (SIEM) application. For more information, see "Downloading the Absolute SIEM Connector" on page 71.

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

Downloading the Absolute Agent for Android Devices

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

- **Agent Type**: the platform-specific agent type
- **Agent Version**: the version (build) number of the agent
- **Supported Platforms**: the operating systems that are supported by each agent
- **Last Updated**: the date and time the agent files were created
- **Last Downloaded**: the date and time the agent files were last downloaded
To download Windows and Mac agent installation packages, go to the Agent Management page in the Administration area. For more information, see Downloading the Absolute agent for Windows and Mac devices in the online Help.

To download the stamped agent installation files:

1. On the navigation bar click > Download Packages.
   The Download Packages page opens with a list of all Agent Types and the Agent Versions that are created for your account.

   NOTE To see the most current version of the agent, open the Updated versions of Agents available tooltip. Contact Absolute Technical Support to upgrade to the most current agent version, if required.

2. In the Agent for Mobile Operating Systems section, click the appropriate link in the Agent Type column.
3. Follow the on-screen instructions to complete the download.
   After the agent is installed on a client device, the device is automatically associated with your account.

For more information about installing the agent on Android devices, refer to the Administrator’s Guide for Absolute Agent.

Upgrading to the Latest Version of the Agent

Periodically, Absolute releases a new version of the Absolute agent for Android devices. When a new agent is available, the following steps are taken:

- An announcement is posted in the console.
- New agent packages are automatically created for your account and added to the Download Packages page (assuming the Agent Type applies to your account).
- Your existing managed devices are automatically upgraded to the new agent, as applicable.

Testing Your Network for Agent Connectivity

The Network Diagnostics Tool is a command line utility that you can use to test your network configuration before you install the Absolute agent on your devices. You can also use it to troubleshoot connectivity issues as they arise. The tool determines if your current proxy and firewall settings will allow the Absolute agent to connect to the Absolute Monitoring Center.

To download the Network Diagnostics Tool:

1. On the navigation bar click > Download Packages.
2. On the Download Packages page, in the Network Diagnostics section, click Download Network Diagnostics Tool.
3. Follow the on-screen instructions to download the .zip file that contains the tool (DDSNDT.exe). Depending on your browser and operating system, you may need to click through several dialogs to save the file to a location of your choice.
4. Navigate to the location where you saved the .zip file and extract its contents to a location of your choice. You can copy the files to your hard drive or run them from a USB key or network drive.

For more information about running the Network Diagnostics Tool from the command line, see the NDT Readme.pdf file in the downloaded zip file, or go to the Documentation page and see the Administrator’s Guide for Absolute Agent.

Using the Absolute Manage Suite

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

The Absolute Manage installation packages available in the Absolute Manage section let Administrators extract, download, and use the data collected by agents on managed devices. For accounts including Absolute Manage, the data that was previously available only through classic reports is now available using the Absolute Manage application on the local device.

The Absolute Manage section lets you perform the following functions:

- Downloading the Absolute Manage Installation Packages
- Uploading a Stamped Agent Including Absolute Manage

Downloading the Absolute Manage Installation Packages

To download the Absolute Manage packages for your operating system:

1. On the navigation bar click ➔ > Download Packages.
2. On the Download Packages page, in the Absolute Manage section, click the appropriate link from the following:
   - Download Absolute Manage for Windows Computers
   - Download Absolute Manage for Macintosh Computers
3. Follow the on-screen instructions to complete the download.
4. Install the Absolute Manage application on your device. When prompted, provide the Registration Code and Serial Number available on the Download Packages page.

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

Uploading a Stamped Agent Including Absolute Manage

Devices managed using the Absolute Manage server contain a special agent. You can create a modified agent installation package to reinstall the agent containing Absolute Manage components in the event that the agent on one of your managed devices is removed. The Absolute Manage Persistence area in the Absolute Manage section on the Download Packages page lets you upload modified Windows and Mac agent installation packages for use at a later date.
NOTE Depending on the licenses you own, the Absolute Manage section may not be available, but the Absolute Manage Persistence area may be shown in its own section.

To ensure that the file is uploaded successfully, the agent Installation package must conform to the following requirements:

- The package must be a valid .zip file. Any package extraction errors lead to a validation failure error and the failure of the upload process.
- The installation package can have any name, as long as it is a valid .zip file. The file name changes to a system generated name upon successful upload.
- The package needs to contain the folders and files shown in the following table, depending on the operating system.

### Installation Package details for Windows and Mac operating systems

<table>
<thead>
<tr>
<th>Device Operating System</th>
<th>Installation Package Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>The package must contain the following files:</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\0x0409.ini</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\AgentVersion.exe</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\Data1.cab</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\DefaultDefaults.plist</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\Info.plist</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\instmsiw.exe</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\LANrev Agent.msi</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\LANrevAgentSafeInstaller.exe</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\LANrevAgentUpdater.bat</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\LANrevAgentUpdater.exe</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\LANrevAgentUpdater_Launcher.bat</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\setup.exe</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\Setup.ini</td>
</tr>
</tbody>
</table>

**NOTE** The DefaultDefaults.plist file must contain a ServerList configuration with at least one primary inventory server and an address. For more information, log in to AMRC, open the Absolute Manage Getting Started Guide and see the information under the heading “Deploying the agent using a local installer”. The Info.plist file must contain a CFBundleGetInfoString XML element with appropriate and valid content.
## Installation Package details for Windows and Mac operating systems (continued)

<table>
<thead>
<tr>
<th>Device Operating System</th>
<th>Installation Package Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac</td>
<td>The package must contain the following folders and files:</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\Certificates</td>
</tr>
<tr>
<td></td>
<td>NOTE The Certificates folder must contain three .pem files.</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\Absolute Manage Agent.pkg</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\DefaultDefaults.plist</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\DetermineDeploymentPlatform.sh</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\InstallAgent.sh</td>
</tr>
<tr>
<td></td>
<td>● \Absolute Manage Agent\SpecialSSLUpdater.plist</td>
</tr>
</tbody>
</table>

To upload a changed agent installation package:

1. On the navigation bar click > Download Packages.
2. On the Download Packages page, scroll to the Absolute Manage area.
3. In the Absolute Manage Persistence area, click Browse in the area for the applicable operating system (Windows or Mac).
4. In the File Upload dialog, browse to the location on the local hard disk of your device to find the appropriate agent installation .zip file.
5. Click the file name and click Open to select the file. The Download Packages page refreshes to list the file name in the Filename field in the Absolute Manage Persistence area.
6. Click Upload. The file is uploaded to the Absolute console and the Download Packages page refreshes to show the file in the Filename table for the applicable operating system.

### Downloading the Absolute SIEM Connector

The Absolute SIEM Connector uses the syslog protocol to send alert events triggered in the Absolute console to your Security Information and Event Management (SIEM) application. If you want to view and manage alert events in a SIEM application, download the Absolute SIEM Connector installation package to a computer on your network. For more information about creating alerts, see "Alerts" on page 15.

For more information about the Absolute SIEM Connector, including detailed installation instructions, see the Absolute SIEM Connector Install Guide in the online Help.

To download the Absolute SIEM Connector:

1. On the navigation bar click > Download Packages.
2. On the Download Packages page scroll to the Absolute SIEM Connector area and click the link that shows under Filename.
3. Follow the on-screen instructions to download the installation package, SIEM Connector <version>.msi to your local drive.
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**.

### Viewing Pending Agent Removal Requests

**IMPORTANT** In previous releases, Security Administrators, Administrators, or designated Power Users could remove the Absolute agent from one or more of devices using the self-serve Agent Removal feature to create new agent removal requests and manage existing requests. In the current release, you can still view devices with a pending Agent Removal request, but to remove the agent from your devices, you now need to submit an Unenroll Device request. For more information about submitting these requests, see **Unenrolling devices from your account** in the online Help.

You can view the list of pending Agent Removal Requests for your account. After the agent is removed from a device, the associated request is removed from the Create and View Agent Removal Request page.

**NOTE** You can't use the Absolute console to cancel a pending Agent Removal request. For assistance, contact Absolute **Technical Support**.

To view a pending request for Agent Removal:

1. Log in to the Absolute console as a user who was previously granted permission to create Agent Removal requests.

2. On the navigation bar click **Agent Removal Requests**.

3. On the **View Pending Agent Removal Requests** page, at the **Search Criteria** area, search for one or more requests using the following criteria:

   ● To filter your results by device group, in the **Group** field, open the list and select the appropriate device group.

   ● To filter your results by specific device, in the **Device** 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

     ○ **Make**: the manufacturer of the device

     ○ **Model**: the product type of a device or other hardware

     ○ **Serial Number**: the serial number of the device or other hardware

     ○ **Requested By**: the Username of the user who submitted the request

     ○ **IMEI**: the International Mobile Equipment Identity (IMEI) number of the device, if applicable

     ○ **Subscriber ID**: the unique identifier associated with the subscriber. This identifier is also known as the International Mobile Subscriber Identity (IMSI).
Phone Number: the phone number associated with the mobile 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 change 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.

3. Click Show results. The results grid refreshes to show the following information about each request:

- Identifier: a unique Electronic Serial Number assigned to the agent that is installed on a device
- State: the status of the device’s agent. The value in this column is Disabled for all pending requests.
- 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
- Make: the manufacturer of the device
- Model: the product type of a device or other hardware
- Serial Number: the serial number of the device or other hardware
- 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
- Requested By: the Username of the user who submitted the request
- Requested On: the date and time when the request was submitted
- Last Call: the date and time when the agent installed on a device most recently contacted the Monitoring Center.
- Persistence Status: the current status of the Persistence module on the device. Possible values are:
  - Awaiting Call: the device is set for Agent Removal, but the device has not yet made an agent call. As a result, the Persistence status cannot be confirmed.
  - BIOS/Firmware Active: the Persistence status was Active when the Agent Removal Request was processed on the device.
  - BIOS/Firmware Disabled: the Persistence status was Disabled when the Agent Removal Request was processed on the device. This status is likely to occur if an Agent Removal Request is submitted before the Persistence module is activated on the device.
  - BIOS/Firmware Pending: the Persistence module was in the process of activating when the Agent Removal request was processed on the device.
  - N/A: the device, such as a Mac computer, does not support Persistence.
Pending Removal: the Agent Removal request was processed on the device, but the Persistence status could not be confirmed (in some cases, the Persistence module is not disabled until the operating system is restarted).

**NOTE** The Pending Removal status does not apply to Android devices.

Managing Your iPads

You can import iPad device serial numbers into the Absolute console to initially upload and maintain your asset data.

You are responsible for the following tasks:

- Maintaining your list of active iPad by uploading the serial numbers for new and existing devices you want enrolled
- Disabling the serial numbers of those devices you want to remove from the list of active iPad devices

Organizations can use this manual method to manage iPads, which includes the following tasks:

- Importing iPad Serial Numbers into the Absolute Console
- Removing iPads from the Absolute Console

Importing iPad Serial Numbers into the Absolute Console

Enrolling your iPads requires that you import your list of enrolled devices into the Absolute console.

To import your iPad device data:

1. On the quick access toolbar, click and click **Import Device Data for iPads**.
2. On the Import Device Data for iPads page, click **View a sample file of device data** to open the sample file. Increase the columns to read how to enter this information.
3. Click **Open** and using Microsoft Excel (for example), you can use the template and enter your own data or you can create a new .csv file that contains the **Mobile Device Serial Number**, which is mandatory for each iPad you want to register.

   You can also enter other optional information you want to track with this device, however although it is stored in the database, you cannot view it in the Absolute console.

4. **Save** this file to your hard drive.
5. On the Import Device Data for iPads page, click **Browse** and select the .csv file you created in step 3.
6. Click **Upload File and Import Devices**.

   You see a message that the file upload is complete. If an error occurred during the upload process, you see a message with the number of entries that failed to upload. Click the **View the log file** link to view the errors, then revise your file and upload it again.
Removing iPads from the Absolute Console

When you decide that you no longer want certain iPads enrolled in Absolute for iPads, you can unenroll them and free up licenses for use by other devices. Organizations that are using the Absolute console for iPads only have no security operations available and therefore do not require an authorization code.

You can use one of the following methods to remove iPads:

- Selecting iPads to Remove
- Uploading a Device List to Remove iPads

**IMPORTANT** To perform this task requires that your account was previously set for agent removal and that you log in to the Absolute console as a user with the appropriate role and permissions.

Selecting iPads to Remove

To remove the Absolute for iPad license from an enrolled iPad, log in to the Absolute console, open the help system, and search for the Unenrolling devices from your account task.

For more information or assistance with this task, contact Absolute Technical Support ([www.absolute.com/en/support](http://www.absolute.com/en/support)).

Uploading a Device List to Remove iPads

You may want to unenroll certain devices to free up Absolute for iPad licenses for other devices you want to register.

You need to create a text file with the Identifiers or Serial Numbers of those iPads that you want to remove and upload that text file to the Absolute console to create an agent removal request. Enter the list of devices to remove in a single column, separating each entry with a return (press Enter). Do not use punctuation in this list.

**IMPORTANT** To perform this task requires that you log in to the Absolute console as a Security Administrator with Unenroll Devices permissions.

Currently Upload by CSV is not available. This functionality will be available in a future product release. For urgent requests, contact Absolute Technical Support ([www.absolute.com/en/support](http://www.absolute.com/en/support)).
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 93.

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 93.

**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 ☑ > Custom Reports.
2. On the Reports page, open the report you want by doing one of the following:
   - On the sidebar, click the category that contains the report you want to run and then click that report’s link.
In the work area, click the report you want to run.

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 79.

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 92. For information about preparing reports with results only available for download, see "Working with Reports" on page 93.

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 78.
2. Change the default value by opening the list.
3. Select the appropriate number of records to show in the report from these options:

   ![Number of Records 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 78.
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 78.
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 82.

   **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](#)
- [Managing Event Calling for a Device](#)
- [Managing SCCM Status Reporting for a Windows Device](#)
- [Managing SCCM Repair for a Windows Device](#)
- [Using the Assigned Username Field](#)
- [Using the Dormant Devices Field](#)
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**
- **RTT-IP** for Windows and Mac devices only
  For more information about this section, see "Enabling RTT-IP for an Individual Device" on page 192.
- **Call Settings** for Windows and Mac devices only
  For more information about this section, see "Managing Event Calling for a Device" on page 86.
- **SCCM Status and Repair** for Windows devices only
  For more information about this section, see the following topics:
  - "Managing SCCM Status Reporting for a Windows Device" on page 88
  - "Managing SCCM Repair for a Windows Device" on page 89
- **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 90.
- **Assigned User E-mail Address**, which you can edit
- **Detected Asset Number**
- **Assigned Asset Number**, which you can edit
- **Device Groups** shows the device group 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 42.
- **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**
- **SCCM Status History Tab** (Windows devices only)

---

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. Whatever WMI reports, which is provided by Microsoft or your hardware and/or software vendors, is shown on the Hardware Configuration and OS Change Report. For Microsoft's description of a scenario where this problem may occur, see: [connect.microsoft.com/VisualStudio/feedback/details/623282](http://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. If the agent does not detect the phone number automatically, the device automatically sends an SMS to the Monitoring Center. The reply-to address from the SMS becomes the value for the **Phone Number Override** field. For more information,
- **See hardware details**: provides more information about the device’s hardware.

Click ![ ](image) 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:

- Software By Device Report: a link to this report where you can review all software applications detected by the agent on a managed device. For more information, see "Software by Device Report" on page 112.
- Operating System
- Detected Anti-Malware
- OS Service Pack
- OS Product Key
- 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
If the device is equipped with Geolocation Tracking functionality, the Call Tracking tab also shows the Last known location and the Location Determination Date for the device.

**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 78.

SCCM Status History Tab

**NOTE** This tab applies only if you are using System Center 2012 Configuration Manager and the SCCM Status reporting feature is turned on for this Windows device. For more information about enabling SCCM Status reporting, see the following topics:
- "Managing SCCM Status Reporting and Repair for your Account" on page 64
- "Managing SCCM Status Reporting for a Windows Device" on page 88
- "Managing SCCM Status Reporting and Repair in the SCCM Status Report" on page 145

The SCCM Status History tab shows information about changes to the status of the SCCM client installed on a Windows device. If the device’s agent detects that the status of the SCCM client has changed, a row is added to the results grid. The following information is provided:

- **Issue Count**: the total number of times the device’s SCCM Status has changed from OK to an unhealthy state. The Issue Count is incremented each time one of the following status changes occurs. Possible status changes depend on whether SCCM Repair is enabled.
  - SCCM Repair is enabled:
    - OK to Repair successful
    - OK to Repair failed
    - OK to Absent
    - Repair Failed to Absent
    - Repair successful to Repair successful
    - Repair successful to Repair failed
    - Repair successful to Absent
    - Absent to Repair failed
    - Absent to Repair successful
  - SCCM Repair is disabled:
    - OK to Absent
    - OK to Needs attention
    - Needs attention to Absent
    - Absent to Needs attention
- **Status Date**: the date and time when the status of the SCCM client on the device changed.
• **SCCM Status**: the current status of the SCCM client on this device, reported at the last successful agent call. Possible values are:
  ○ **Absent**: the SCCM client is not installed on the device.
  ○ **Needs attention**: one or more health check tests failed and SCCM Repair is not enabled on the device. You may want to enable SCCM Repair for this device.
  ○ **OK**: all health check tests passed and the SCCM client is functioning correctly.
  ○ **Repair failed**: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was not repaired. For more details about why the repair failed, click the link. If repeated attempts to repair the SCCM client fail, see "Troubleshooting Failed SCCM Repairs" on page 151.
  ○ **Repair successful**: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was repaired.

To view the results of each health check test, click the link. For more information, see "Viewing the Details of a SCCM Status Change" on page 148.

### 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 59.

### Configuring Event Calling for a Managed 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 the **Configuration Options**. For detailed information about the device changes associated with each option, see "Events That Can Trigger an Event Call" on page 60.

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 61.
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 61.
  
  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 60.

3. To sort the information, click the applicable column heading.

4. To close the dialog click Cancel.

Managing SCCM Status Reporting for a Windows Device

IMPORTANT With the release of Absolute 7.2, you can now use the Application Persistence feature to report on and repair SCCM clients installed on your Windows devices. If you have SCCM Status Reporting enabled, we recommend that you disable it and activate the Application Persistence: Microsoft SCCM policy in one or more policy groups. For more information, see About Application Persistence: Microsoft SCCM policies in the online Help.

If you use Microsoft Service Center 2012 Configuration Manager (SCCM), you can track the status of the SCCM client installed on a Windows device by configuring a setting on the device's Device Summary page.

NOTE For more information about SCCM and detecting SCCM Status information, see "About Collecting SCCM Status From Windows Devices" on page 141.
When you enable SCCM Status reporting:

- The agent is updated on the device on the next agent call. The update includes a script, run every six hours, to detect the status of the device’s SCCM client. The script performs a series of health check tests to determine if the client is present and functioning correctly.
- The most recent SCCM Status information for the device shows in the SCCM Status Report.
- A history of SCCM Status changes for the device shows in the SCCM Status History Report and the SCCM Status History tab of the Device Summary page.
- You can use the Alerts feature to trigger an alert notification when a SCCM Status change occurs on the device. For more information about creating Alerts, see "Creating New Custom Alerts" on page 19.

**NOTE**  You can also manage SCCM Status reporting for all Windows devices in your account or for a group of devices. For more information, see the following topics:
- "Managing SCCM Status Reporting for Your Account" on page 64
- "Managing SCCM Status Reporting and Repair in the SCCM Status Report" on page 145

To configure SCCM Status reporting for a Windows device:

1. Navigate to the SCCM Status and Repair area of the Device Summary page.
2. Do one of the following:
   - To turn on SCCM Status reporting, select the Collect SCCM Status for the device checkbox.
   - To turn off SCCM Status reporting, clear the Collect SCCM Status for the device checkbox.

**NOTE**  If SCCM Status reporting is turned on at the account level, you can turn it off for this device by clearing the checkbox.

3. Click Save changes.

**Managing SCCM Repair for a Windows Device**

**IMPORTANT**  With the release of Absolute 7.2, you can now use the Application Persistence feature to report on and repair SCCM clients installed on your Windows devices. If you have SCCM Repair enabled, we recommend that you disable it and activate the Application Persistence: Microsoft SCCM policy in one or more policy groups. For more information, see About Application Persistence: Microsoft SCCM policies in the online Help.

You can use the SCCM Repair feature to repair a SCCM client that is installed on a managed Windows device and is not functioning correctly.

This feature works in conjunction with the SCCM Status reporting feature. When SCCM Repair is enabled:

- The agent is updated on the device on the next agent call. The update includes a script, run every six hours, to detect the status of the device’s SCCM client and automatically repair the client if it is not functioning correctly.
- The most recent SCCM Repair information for the device shows in the SCCM Status Report.
A history of SCCM Repair information for the device shows in the SCCM Status History Report, and the SCCM Status History tab of each device's Device Summary page.

You can use the Alerts feature to trigger an alert notification when SCCM Repair occurs on a device. For more information about creating Alerts, see "Creating New Custom Alerts" on page 19.

For more information about the SCCM Repair feature, see "About Repairing SCCM Clients" on page 141.

**NOTE** You can also manage SCCM Repair for all Windows devices in your account or for a group of devices. For more information, see the following topics:
- "Managing SCCM Repair for Your Account" on page 65
- "Managing SCCM Status Reporting and Repair in the SCCM Status Report" on page 145

To disable SCCM Repair for a Windows device:

1. Navigate to the SCCM Status and Repair area of the Device Summary page.
2. Clear the Turn on SCCM Repair for the device checkbox.
3. Click Save changes.

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.

Setting devices as **Dormant** excludes them from the Missing Devices report and from the agent Call Rate Widgets. For more information, see "Missing Devices Report" on page 155.

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 78.
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 78.
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 > Classic Reports"Running Reports" on page 78.
2. On the Reports page or navigation bar click the My Content link.
3. On the My Content page or navigation bar click the My Filters link. 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 91.
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 78.
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 is 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
- Software requirements
- Software License status
- 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.

**NOTE** After a device is flagged as Stolen, you can view it only in the Asset Report.

This chapter includes the following sections:

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

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 📊.
2. On the Find Devices page, click **Classic Reports > Hardware Assets**.
   The Hardware Assets page shows all of the available reports under this category.

**Asset Report**

The Asset Report shows all managed devices associated with your account, arranged in ascending order by Identifier. You can customize the report to show a subset of devices that meet criteria such as list all devices in a particular department.

For iPad and Chromebook devices, the Asset Report shows a subset of information.

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

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. Whatever WMI reports, which is provided by Microsoft or your hardware and/or software vendors, is shown on the downloaded Asset Report.

To generate an Asset Report:

1. On the Hardware Assets page, click **Asset Report**.
2. On the Asset 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 filter criteria:
     - **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.
     - **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 or other hardware.
     - **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.
     - **E-mail Address**: the e-mail address for the person associated with this device or activity.
     - **Warranty Contract Vendor**: the warranty provider for a 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 results by date:
  i) In the **and when** area, open the list and select one of the following options:
    - **Most recent call** to open a report that shows those devices that made their last call within the date parameters you selected.
    - **Lease Start Date** to open a report that shows those devices whose lease started within the date parameters you selected.
    - **Lease End Date** to open a report that shows those devices whose lease ended within the date parameters you selected.
    - **Service Contract Start Date** to open a report that shows those devices whose service contract started within the date parameters you selected.
    - **Service Contract End Date** to open a report that shows those devices whose service contract ended within the date parameters you selected.
    - **Warranty Start Date** to open a report that shows those devices whose warranty started within the date parameters you selected.
    - **Warranty End Date** to open a report that shows those devices whose warranty ended within the date parameters you selected.
    - **Device Purchase Date** to open a report that shows those devices that were purchased within the date parameters you selected.
    - **[Custom Device Fields]**: if one or more date-based Custom Device Fields have been created for your account you can use them as filter criteria.
  ii) Do one of the following:
    - Click the option for **at any time** to run a report that shows the most recent call regardless of when it took place.
    - 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 wide range of dates takes more time 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 results by agent type and version, at the **and the Agent** area:
  i) In the **Type** field open the list and select the appropriate type of agent as follows:
    - **Any Type** returns a report that shows devices with all agent types.
    - **Android** returns a report that shows only Android devices.
    - **Chromebook** returns a report that shows only Chromebooks.
    - **iOS** returns a report that shows only iPads and iPad minis.
    - **Mac** returns a report that shows only Mac devices.
    - **Windows** returns a report that shows only devices running a Windows operating system.
  ii) In the **and version** field, open the list and select the appropriate agent **Version** for the agent **Type** you selected previously.

For example, if you want to show all devices that have the 898 version of the agent installed on them, in the **type** field, open the list and select **Any Type** and in the **version** field open the list and select **898**.
**NOTE**  SHC (Self-Healing Call) returns a report that shows devices with agents that called in as a result of Persistence. This option appears when a Self Healing Call has occurred.

- To filter results by Department, in the **and the Department** field open the list and select the appropriate department.
- To filter results by the agent status, in the **and the Agent Status is** field open the list and select:
  - **Active** shows only those devices whose agent has called the Monitoring Center.
  - **Inactive** shows only those devices whose agent has not yet called the Monitoring Center.
  - **Disabled** shows only those devices whose agent is either flagged for removal or the agent is removed from the device.
- At the **Display Results** area, select one or both of the following options:
  - **With Custom Device Fields** to see the information that relates to any custom fields you have set.
  - **Include Dormant Devices** to see the information for dormant devices that are included in this report by default. If you do not want to show them, clear this checkbox. For more information about dormant devices, see "Using the Dormant Devices Field" on page 90.

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

- **View Call History** link, which you can click to open this device’s Call History Report. In the filtering area of the Call History Report, the following fields are populated:
  - The **contains the field** area shows the **Identifier** you selected.
  - The **contains or contained** field shows the device whose **View Call History** link you clicked. You can continue to filter according to the information in the task, "Call History Report" on page 153.
- **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 80.
- **E-mail Address**: the e-mail address for the person associated with this device or activity.
- **Last Call**: the date and time when the agent installed on the device most recently contacted the Monitoring Center.
- **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.
- **Operating System**: the software that controls the running of computer programs and may provide various services.
- **Agent Version**: the version number of the Absolute agent that contacts the Monitoring Center.
- **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 this device or other hardware.
- **Model**: the product type of this device or other hardware.
- **Department:** the department to which this device belongs.
- **Agent Status:** the operating condition of the agent on this device, which could be **Active**, **Inactive**, or **Disabled**.
- **Assigned Username:** the Username to which this device is assigned.
- **Incident Date:** if an open Investigation Report exists for this device, the date and time when the incident occurred.

**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 to the printer driver's name. The printer driver data can provide important information for help desk troubleshooting.
       - **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.
       - **Port:** the port under which the printer operates.
       - **Server Name:** the server hosting the printer.
       - **Share Name:** the printer’s network 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 92."

**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 92."

**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 identifies all assets that have had changes to their critical hardware or operating system (OS) during a time period you define. See the **Hardware Description** column for details about what changes were detected on the hardware (such as network cards) and for the operating system.

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. Whatever WMI reports, which is provided by Microsoft or your hardware and/or software vendors, is shown on the Hardware Configuration and OS Change Report.
To generate a Hardware Configuration and OS Change Report:

1. On the Hardware Assets page, click **Hardware Configuration and OS Change Report**.

2. On the Hardware Configuration and OS Change 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 filter criteria:
     - **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 date that the change occurred, at the **and the change occurred 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 the status of the change to the device’s **hardware or operating system**, at the **Status** area, select one of the following options:
     - **All**: returns a report that shows the hardware and operating system that is installed, removed or reconfigured on a device.
     - **Changed**: returns a report that shows the hardware or operating system that was reconfigured on a device.
     - **Removed**: returns a report that shows the hardware or operating system that was uninstalled from a device.
     - **New**: returns a report that shows the hardware or operating system that was replaced on a device.

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 80."
- **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.
- **Hardware Description**: the hardware or operating system that was changed.
- **Date Detected**: the date and time when the change was detected.
- **Previous**: the previous hardware or operating system description.
- **New**: the current hardware or operating system description.
- **Status**: indicates whether a detected difference involves New, Removed or Changed hardware or software.

**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 80.
- **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:
Device  RAM  CPU
Identifier  In  Open
HD  Operating
Model  CPU  Click  To  Absolute
Make  >=  To  Absolute
5:  Chapter
4:  Working
with
Reports

5. 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 80.
- **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.
- **Operating System**: software that controls the running of computer programs and may provide various services.
- **CPU Name**: the manufacturer of the Central Processing Unit.
- **CPU Speed**: the processing speed of the Central Processing Unit.
- **RAM size**: the amount of Random Access Memory (RAM) on the device.
- **HD Size**: the amount of data storage on the device in megabytes (MBs).
- **HD Free Space**: the amount of available storage space on the hard disk in megabytes (MBs).
- **Make**: the manufacturer of a device or other hardware.
- **Model**: the product type of a device or other hardware.
Mobile Broadband Adapter Report

**IMPORTANT** Before using Real Time Technology (RTT) features including Mobile Broadband Adapter asset tracking and Monitoring Center Initiated Calling, you need to activate these features for your account or individual Identifiers within your account. Contact Absolute Technical Support to activate these features.

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 80.

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 80.
- **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. If a phone number for a device is not automatically detected, the device sends a Short Message Service (SMS), also known as a text message, to the Monitoring Center.

The Reply-to address in the text message becomes the value in the **Phone Number Override** field. You can also specify an override number on the Device Summary Page. When sending text messages to a device, the value in the **Phone Number Override** field takes precedence over the value in the **Detected Phone Number** field.

**[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 shows a list of smartphone and tablet devices in an account. A smartphone is a mobile phone that offers advanced capabilities, often with computer-like functionality, and provides a good computer-mobile handset convergence.

Smartphones that support more than one network technology are shown multiple times in the report. In such cases, the **Phone Number**, **Equipment Id**, and **Subscriber Id** columns have different values for each network technology detected.
To generate a Mobile Device Report:

1. On the Hardware Assets page, click **Mobile Device Report**.
2. On the **Mobile Device 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.
     - **Make**: the manufacturer of a device or other hardware.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
     - **Model**: the product type of a device or other hardware.
     - **Operating System**: software that controls the operation and applications of the mobile device, and may provide various services.
     - **Phone Number**: the phone number associated with the mobile device.
     - **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.
     - **MAC Address**: one or more Media Access Control (MAC) addresses detected on the smartphone, most commonly Wi-Fi MAC addresses. Some platforms may also have an Ethernet MAC address and other Custom Device Fields.

   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 operating system, in the **and the Operating System is** area, open the list and select the appropriate operating system as follows:
     - **Android** returns a report that shows only devices running an Android operating system.
     - **iOS** returns a report that shows only iPads and iPad minis.
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 80."
   - **Last Call Time** link that shows the date and time when the device most recently contacted the Monitoring Center. Clicking on this link opens the Call History Report. For more information, see "**Call History Report** on page 153.
   - **User Name**: the unique name that identifies the person who is associated with this mobile device.
• **E-Mail Address:** the e-mail address for the person associated with this mobile device.
• **Make:** the manufacturer of the mobile device.
• **Model:** the product type of a device or other hardware.
• **Operating System:** the software that controls the operation and applications of the mobile device, and may provide various services.
• **Phone Number:** the phone number associated with the device.
• **Equipment Id:** the identification number unique to a smartphone. The **Equipment Id** is 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.
• **MAC Address:** indicates that one or more Media Access Control (MAC) addresses were detected on the smartphone, most commonly Wi-Fi MAC addresses. Some platforms may also have an Ethernet MAC address.

### Software Assets Reports

The ability of the agent to identify installed applications automatically is hindered by the fact that software developers do not adhere to published standards for identifying their products. Generally, application developers embed identifying information into the actual code of their products. Unfortunately, the information is not embedded the same way from one company to another or, in some cases, from one product to another from the same company.

To address the issue caused by differences in embedded information, Absolute maintains a database that distinguishes applications by how their identifying information is recorded within the application. As the database develops, the ability of the agent to identify specific applications increases.

This section provides information about and related tasks for the following reports:

- Installed Software Overview Report
- Software Configuration Change Report
- Software by Device Report
- Software License Compliance Overview Report
- Microsoft Audit Summary Report
- Software Policy Non-Compliance Report
- Installed Programs by Device Report
- Installed Programs by Account Report

### Opening the Software Assets Page

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

To open the Software Assets page:

1. On the navigation bar, click 📊.
2. On the Find Devices page, click Custom Reports > Software Assets.
The Software Assets page shows all of the available reports.

Installed Software Overview Report

The Installed Software Overview Report shows detected software applications on tracked devices. You can use the report for software inventory and license management, as well as to identify essential or non-essential software applications. For information about making more applications available from this report, see "Requesting New Software Applications to Include in the Installed Software Overview Report" on page 110.

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

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

To monitor and review software licensing details, see "Software License Compliance Overview Report" on page 114.

To generate an Installed Software Overview Report:

2. On the Installed Software Overview 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 a Department, in the and the Department is field, open the list and select the appropriate department.
   - To filter your results by a software publisher such as Microsoft or Adobe, at the and the Publisher contains area:
     i) Enter all or part of the name of the software publisher.
     ii) Click Choose and select the appropriate publisher.
   - To filter your results by a specific application name such as Microsoft Word or Adobe Photoshop, at the and the Application Name contains area:
     i) Enter all or part of the application name.
     ii) Click Choose and select the appropriate application.
   - To filter your results by a specific program name such as Microsoft Office or Adobe Creative Suite, at the and the Program Name contains area:
     i) Enter all or part of the program name.
     ii) Click Choose and select the appropriate program.
3. Click Show results. The results grid refreshes to show the following data returned according to your filtering choices.
**IMPORTANT**  In the results grid, blank content for Publisher, Application, Program, or Version fields indicates vendors have not provided that information with their software programs.

- **Publisher**: the organization that created the software application.
- **Application Name**: the name of the application on the device and its function if available.
- **Program Name**: the title associated with one or more related applications. In practice, many publishers mutually exchange Program Name and Application Name values.
- **Version**: a number that distinguishes releases of the same software application sold separately, as detected by the agent and reported in the Absolute console.
- **Devices Installed On Count**: the number of devices that have this application or program installed.

4. To view the list of devices that a particular application or program is installed on, click **List Devices**.

   The Installed Software Overview Details report shows information about the **Software Package** and the following information about each device:

   - **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 80.
   - **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.
   - **Serial Number**: the serial number of this device.
   - **Asset Number**: the identification number associated with a device in the Absolute console.
   - **Department**: the department to which this device belongs.
   - **Operating System**: the software that controls the running of computer programs and may provide various services.

**Requesting New Software Applications to Include in the Installed Software Overview Report**

Absolute invites its customers to request specific applications they want added to the database of detected software applications, also referred to as software mapping.

To request that a specific application is mapped and included in the Installed Software Overview Report, send your software mapping request to Absolute Technical Support

Include the following information in your request to Technical Support:

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

**IMPORTANT**  Absolute does not guarantee that it will implement all software mapping requests.
Software Configuration Change Report

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

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

To generate an Installed Software Configuration Change Report:

1. On the Software Assets page, click **Software Configuration Change Report**.
2. On the **Software Configuration Change 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:
     - **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.
     - 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 a Department, in the **and the Department is field** open the list and select the appropriate department.
   - To filter your results by a software publisher, at the **and the Publisher contains** area:
     - Enter all or part of the name of the software publisher.
     - Click **Choose** and select the appropriate publisher.
   - To filter your results by a specific application, at the **and the Application Name contains** area:
     - Enter all or part of the name of the application.
     - Click **Choose** and select the appropriate application.
   - To filter your results by a specific program, at the **and the Program Name contains** area:
     - Enter all or part of the name of the application.
     - Click **Choose** and select the appropriate program.
   - To filter your results by the date the agent detected a change, at the **and the change occurred 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 the status of the change to the device’s software configuration, select one of the following options:
  - **All**: returns a report that shows all the software that was installed, removed or reconfigured on a device.
  - **Changed**: returns a report that shows the software that was reconfigured on a device.
  - **New**: returns a report that shows the software that was installed on a device.
  - **Removed**: returns a report that shows the software that was uninstalled from a device.

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

- **Identifier** link, which you click to open this device’s Device Summary page. For more information, see "Editing Asset Information" on page 80.
- **Username**: the unique name that identifies the person who is associated with this device.
- **Publisher**: a company or organization selling applications that is detected by the agent and reported in the Absolute console.
- **Application Name**: the name of the application on the device and its function if available. In practice, many publishers mutually exchange Application Name and Program Name values.
- **Program Name**: the title associated with one or more related applications. In practice, many publishers mutually exchange Program Name and Application Name values.
- **Previous Version**: the previous version number of a program installation.
- **New Version**: the current version number of a program installation.
- **Change Detected On Date**: the date when the agent detected a change that was made to the device’s software configuration.
- **Status**: indicates whether a detected difference involves **New**, **Removed**, or **Changed** software.

**IMPORTANT** In the **results** grid, blank content for **Publisher**, **Application**, **Program**, or **Version** fields indicates vendors have not provided that information with their software programs.

Software by Device Report

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

To generate a Software by Device Report:

1. On the Software Assets page, click **Software By Device Report**.
2. On the Software By Device 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:
     - **Any of the fields in this list**: selects all the values in the list.
1. Identify: a unique Electronic Serial Number assigned to the agent that is installed on a device.
2. Username: the unique name detected by the agent that identifies the person who is associated with this device.
3. Device Name: the name assigned to the device in the operating system.
4. IMEI: the International Mobile Equipment Identity (IMEI) number of the device, if applicable
5. 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 a Department, in the and the Department is field open the list and select the appropriate department.
- To filter your results by software, in the and the field area open the list and select one of the following values:
  - Publisher: the organization creating a software application.
  - Version: a number that distinguishes releases of the same software application sold separately, as detected by the agent and reported in the Absolute console.
  - Program: an executable file on a device that is detected by the agent and reported in the Absolute console.

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. 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 80.
- Device Name: the name assigned to this device in the operating system.
- 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.
- Serial Number: the serial number of this device.
- 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
- 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.
- Version: a number that distinguishes releases of the same software application sold separately, as detected by the agent, and is reported in the Absolute console.
- Program Name: the title associated with one or more related applications. In practice, many publishers mutually exchange Program Name and Application Name values.
Operating System: software that controls the running of computer programs and may provide various services.

IMPORTANT In the results grid, blank content for Publisher, Application, Program, or Version fields indicates vendors have not provided that information with their software programs.

Software License Compliance Overview Report

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

To generate a Software License Compliance Overview Report:

2. On the Software License Compliance Overview 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.
     Select one of the following options:
     - Show Version-Specific Licenses returns a report that shows the License Name as well as the version number.
     - Show Version-Independent Licenses returns a report that shows only the License Name.

   - To filter your results by software publisher, at the and the Publisher area:
     i) Enter all or part of the publisher’s name.
     ii) Click Choose to open the list and select the appropriate publisher.

   - To filter your results by software license, in the and the License Name contains area:
     i) Enter all or part of the publisher’s name or click Choose to open the list and select the appropriate publisher.
     ii) Select one of the following options:
     - Show all licenses
     - Show only licenses that are purchased or installed
     - Show only licenses installed on Agent-equipped Device

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

   - Publisher: a company or organization selling applications that is detected by the agent and reported in the Absolute console.
   - License Name: the known Identifier of an installed application. Click a license name to open the Edit License page. For more information, see “Editing License Information” on page 115.
   - Purchased: the number of owned licenses for an application.
   - Installed on non-Agent Equipped Devices: the number of installations of an application on devices that do not have the agent installed.
• **Installed in This Group:** the number of license installations of an application in a Group. Click a value to open the Devices by License Report. For more information, see "Viewing a Devices by License Report" on page 115.

• **Installed in Other Groups:** the number of application licenses that are installed on devices in a Device Group that are not included in this report.

• **Available Violations:** the number of available application licenses to be installed on devices. A negative value in this column indicates that your organization has exceeded its number of purchased licenses.

**IMPORTANT** In the results grid, blank content for Publisher, Application, Program, or Version fields indicates vendors have not provided that information with their software programs.

### Editing License Information

The Edit License page shows the number of licenses that have been purchased, installed, and are available to your organization. You can access the Edit License page by generating the Software License Compliance Overview Report. See "Software License Compliance Overview Report" on page 114.

To edit the licensing information for a specific license:

1. Generate the Software License Compliance Overview Report by completing the task, "Software License Compliance Overview Report" on page 114.

2. In the results grid under the License Name column, click the name of the license you want to update.

3. In the Licenses Purchased field, edit the number of licenses purchased by your organization.

4. In the Licenses installed on non-Agent equipped devices field, edit the number of devices on which the software license is installed.

5. Save your edits by doing one of the following:
   - Click Save to save your changes and refresh the Edit License page with the new values.
   - Click Save & close to save your changes and return to the Software License Compliance Overview Report.

### Viewing a Devices by License Report

The Devices by License Report provides a list of all devices on which a specific application is installed. You can only access this report through a link in the Software License Compliance Overview Report.

To view the Devices by License Report:


2. In the results grid, click a value in the Installed In This Group column.

3. On the Devices by License 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. In the is or contains field, click Choose and select a value from the list.

● To filter your results by a Department, in the and the Department is field, open the list and select the appropriate department.

4. 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 80.
  ○ **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.
  ○ **Serial Number**: the serial number of this device.
  ○ **Asset Number**: the identification number associated with a device in the Absolute console.
  ○ **Product Id**: a unique identifier for an application.
  ○ **Operating System**: software that controls the running of computer programs and may provide various services.

Microsoft Audit Summary Report

The Microsoft Audit Summary Report is a downloaded CSV (Comma Separated Value) or XML (eXtensible Markup Language) file that provides a list of all Microsoft licenses shown in the Software License Overview Report. Use the Microsoft Audit Summary file to track your organization's compliance with Microsoft's licensing requirements. This file adheres to the layout and content of one of the Microsoft Audit Summary templates published by Microsoft.

To generate a Microsoft Audit Summary Report:

1. Do one of the following:
   ○ On the Software Assets page, click Microsoft Audit Summary Report.
   ○ On Software License Compliance Overview Report page, click Download Microsoft audit summary.

2. On the Microsoft Audit Summary Report page, at the Name and Format location, in the Name field enter a unique name for the 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.

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 92.

The Microsoft Audit Summary Report includes license information in the following fields:

- **Name**: the license name.
- **# of Installs**: the total number of detected instances of the application, and the manually entered value for any instances of the application installed on non-agent equipped devices.
- **# of Licenses**: the number of licenses purchased.
- **# Available**: the number of available licenses for the application (negative numbers indicate non-compliance).

**IMPORTANT** In the results grid, blank content for Publisher, Application, Program, or Version fields indicates vendors have not provided that information with their software programs.

Software Policy Non-Compliance Report

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

**IMPORTANT** To use the Software Policy Non-Compliance Report, you must first define and apply a software policy. For information on how to define and apply a software policy, see "Software Policy" on page 50.

To generate a Software Policy Non-Compliance Report:


2. On the Software Policy Non-compliance 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 is field, open the list and select the appropriate department.
   - To filter your results by Policy, in the and the field area:
     i) Open the list and select one of the following values:
        - **Policy Name**: the name of a defined Software Policy. See "Software Policy" on page 50.
        - **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.
• **Publisher**: the organization creating a software application.
   Depending on what value you selected from the preceding list, you may want to further define this field using the is or contains field by clicking Choose.

ii) Select one of the following options:
• **Has Software On The Banned List**
• **Missing Software On The Required List**

• To filter your results by date, in the and the Device called between area, do one of the following:
  o 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.
  o 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 return a report that shows software that does not have a license defined in the Absolute console, select the Show Unlicensed Software/Executables checkbox.

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 80.
• **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.
• **Software Policy ID**: the unique identifier assigned to a Software Policy in the Absolute console. See “Software Policy” on page 50.
• **Publisher**: the organization creating a software application.
• **License Name**: the known identifier of an installed application.
• **Policy Name**: the name of a defined Software Policy. See “Software Policy” on page 50.
• **Last Trace Call Date**: when the agent installed on a device most recently contacted the Monitoring Center.
• **Status**: indicates whether a detected software is Banned or Missing.

**IMPORTANT** In the results grid, blank content for Publisher, Application, Program, or Version fields indicates vendors have not provided that information with their software programs.

### Installed Programs by Device Report

The Installed Programs by Device Report provides a list of all correctly installed Windows software programs for each managed device in the Device Group you specify.

To generate an Installed Programs by Device Report:

1. On the Software Assets page, click **Installed Programs By Device Report**.
2. On the Installed Programs By Device 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. In the is or contains field, 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 Program, in the and the field area, open the list and select one of the following values:
  - Any Program Identifier: filters results by a program Name, Publisher, or Version.
  - Name: the title associated with one or more related applications.
  - Publisher: the organization creating a software application.
  - Version: a number that distinguishes releases of the same program.

On the Choose dialog, select the appropriate value to further define this field.

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 80.
- Program Name: the title associated with one or more related applications.
- Version: a number that distinguishes releases of the same software application sold separately, is detected by the agent, and is reported in the Absolute console.
- Publisher: a company or organization selling applications that is detected by the agent and reported in the Absolute console.
- Device Name: the name assigned to this device in the operating system.
- Department: the Department to which the device belongs.
- 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.
- Operating System: software that controls the running of computer programs and may provide various services.
IMPORTANT In the results grid, blank content for Publisher, Application, Program, or Version fields indicates vendors have not provided that information with their software programs.

Installed Programs by Account Report

The Installed Programs by Account Report shows a list of all correctly installed Windows applications installed on one or more managed devices that are associated with an account.

To generate an Installed Programs by Account Report:

2. On the Installed Programs by Account 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 is 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:
     - Name: the title associated with one or more related applications.
     - Publisher: the organization creating a software application.
     - Version: a number that distinguishes releases of the same software application.
   - 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 column heading, in the group by area select one of the following options:
     - Name, Publisher and Version returns a report that shows the Program Name, Version, Publisher, and Quantity.
     - Name and Publisher returns a report that shows only the Program Name, Publisher, and Quantity.
3. Click Show results. The results grid refreshes to show the following data returned according to your filtering choices.
   - Name: the title associated with one or more related applications. In practice, many publishers mutually exchange Program Name and Application Name values.
   - Version: a number that distinguishes releases of the same software application sold separately, is detected by the agent, and is reported in the Absolute console.
   - Publisher: a company or organization selling applications that is detected by the agent and reported in the Absolute console.
   - Quantity: the number of applications installed on devices in your account. Click the value to open the Installed Programs By Device Report – Details page.

IMPORTANT In the results grid, blank content for Publisher, Application, Program, or Version fields indicates vendors have not provided that information with their software programs.
Installed Programs by Device Report – Details

With the Installed Programs by Account Report open, clicking a value link in the Quantity column in the results grid opens the Installed Programs By Device Report – Details page. This page shows data with the same Search Criteria you used for the Installed Programs by Account Report, but for the specific program only.

The Installed Programs By Device Report – Details page provides the following information for the selected program:

- In the Details of Installed Program area:
  - Name: the title associated with one or more related applications. In practice, many publishers mutually exchange Program Name and Application Name values.
  - Publisher: a company or organization selling applications that is detected by the agent and reported in the Absolute console.
  - Version: a number that distinguishes releases of the same software application sold separately, is detected by the agent, and is reported in the Absolute console.

- In the results grid:
  - 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 80.
  - Name: the title associated with one or more related applications.
  - Version: a number that distinguishes releases of the same software application sold separately, is detected by the agent, and is reported in the Absolute console.
  - Publisher: a company or organization selling applications that is detected by the agent and reported in the Absolute console.
  - Device Name: the name assigned to the device in the operating system.
  - Department: the Department to which the device belongs.
  - 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.
  - Operating System: software that controls the running of computer programs and may provide various services.

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
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 🗃️.
   The Security page opens showing all of the available reports.

Operating System Updates Report
The Operating System Updates Report shows the installed operating system for each managed device.
For devices that are running the Windows operating system, the report also shows details about each service pack and hotfix installed on the device. You can also filter the report to show Windows devices that include, or are missing, a specific hotfix.

**IMPORTANT** You must log in as a Security Administrator to open the Operating System Updates Report.

To generate an Operating System Updates Report:
2. On the Operating System Updates 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 is field, open the list and select the appropriate department.
   - To filter your results by Operating System, in the and the Operating System is or contains field, enter the name of the operating system.
3. To generate a report based on the service pack and hotfix level of your Windows devices, do the following:
   a) To filter your results by service pack, in the and the latest Service Pack installed is or contains field, enter the name of the service pack.
   b) To filter your results by hotfix, at the and display devices area:
      i) Open the list and select one of the following options:
         - with hotfix returns a report that shows only devices where a hotfix was installed.
         - without hotfix returns a report that shows only devices where a hotfix was not installed.
      ii) In the hotfix is or contains field, enter all or part of the file name for the hotfix.
c) To include service pack and hotfix information in the report, select the **Include hotfix details** checkbox.

4. 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 80.
   - **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.
   - **Operating System**: the installed version of the software that controls the running of computer programs and may provide various services.
   - **Service Pack**: the service pack level of the device (applies to devices running the Windows operating system only).

   **NOTE** This column shows only if the **Include hotfix details** checkbox is selected.

   - **Windows Hotfix**: provides a link to the Microsoft Knowledge Base article that describes the software changes included in the hotfix (applies to devices running the Windows operating system only).

### 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 80.
- **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 \( \times \) height in units of pixels such as 1024 \( \times \) 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:


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 80.
- **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 identifies devices that have anti-malware software installed. You can use the report to identify devices that use an older version of anti-malware software or have outdated virus definition files.

For the complete list of anti-malware applications detected by the Absolute agent, see Detected full-disk encryption products in the online Help.

**NOTE**  If the targeted device contains an anti-malware program that does not show in the list, the agent may not detect the presence or absence of the program accurately.

To export a report that provides statistical information about the anti-virus products detected on your devices, see "Security Posture Report" on page 151.

To generate an Anti-Malware Report:

**IMPORTANT** You must log in as a Security Administrator to open the Anti-Malware Report.

2. On the Anti-Malware 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 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 what 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 Department, in the **and the Department** field, open the list and select the appropriate department.

To filter your results by Version, in the **and the Anti-Malware application version is less than** field, enter the appropriate value.

To filter your results by Vendor, in the **and the Application Vendor contains** field, enter the name of the vendor.

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 80.
- **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 to which this device belongs.
- **Anti-Malware Software**: the name of the Anti-Malware application.
- **Version**: a unique name or number assigned to an identified and documented body of software.
- **Definition Date (Text)**: the date and time of the Virus Definition.
- **Definition**: the search string used by anti-malware software to detect a computer virus.
- **Detected Date**: the date and time when the data was detected on the device.
- **Last Call**: the date and time when the last agent call was made on the device.

**Missing Anti-Malware Report**

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

For the complete list of anti-malware applications detected by the Absolute agent, see **Detected full-disk encryption products** in the online Help.

**NOTE** If the targeted device contains an anti-malware program that does not show in the list, the agent may not detect the presence or absence of the program accurately.
To generate a Missing Anti-Malware Report:

**IMPORTANT** You must log in as a Security Administrator to open the Missing Anti-Malware Report.

2. On the Missing Anti-Malware 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 **Department** field open the list and select the appropriate department.
   - To filter your results by specific device, in the **Device Name** 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.
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 80."
   - **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 to which this device belongs.
   - **Assigned Username**: the username entered or edited by a user.
   - **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.
   - **Last Call**: the date and time when the last agent call was made from the device.

**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 80.
   - **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 15.

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 80.
   - **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 Suspicous** 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 the how often authentication failed, authentication types, or the 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 19.

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:
  - 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.
  - 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 80.
- **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**

Full-Disk Encryption (FDE) is a software or hardware solution that secures, or encrypts, the entire content of a physical drive.

The agent detects FDE hardware (self-encrypting drives) and software full-disk encryption products that are installed on the hard drives of your organization’s managed Windows and Mac devices. Each encryption vendor uses specific encryption status strings in their products.

**IMPORTANT** Currently, the Full-Disk Encryption Status Report provides information about full-disk encryption products installed on the system or the first physical drive only.

Using the filtering available in the Full-Disk Encryption Status Report, you can search your account’s tracked devices to detect those devices that have full-disk encryption enabled, and return the results based on your filter in the Full-Disk Encryption Status Report – Products Detected. You can save the filters used to create specific versions of the Full-Disk Encryption Status Report – Products Detected to your My Filters location in the My Content area.

You can also create a report of those tracked devices that do not have hardware or software full-disk encryption enabled. The Full-Disk Encryption Status Report – Products Not Detected includes an SED Capable column that indicates a device has a self-encrypting drive (SED) that is capable of FDE, but that may not be enabled or supported by Absolute. This capability provides you with an opportunity to remediate that situation.

From either Full-Disk Encryption Status Report, you can create alerts to notify you when the conditions you provide in the filtering details are met. Creating an alert from this report populates the conditions on the Create and Edit Alerts page with those shown on the report. For more information on creating these types of alerts, see "Creating an Alert Based on Full-Disk Encryption Status Criteria" on page 22.

**NOTE** To export a report that provides statistical information about the Full-Disk Encryption products installed on your devices, see "Security Posture Report" on page 151.

This section provides information about the following topics and tasks:
- **Turning On Full-Disk Encryption Data Collection for Your Account**
- **Filtering Data to Create a Full-Disk Encryption Status Report**
- **Identifying Devices That Have Full-Disk Encryption Products Installed**
- **Identifying Devices With No Installed Full-Disk Encryption Products**
- **Viewing Changes to a Device’s Encryption Status Strings**
Full-Disk Encryption Software Products and Self-Encrypting Drives Detected

**IMPORTANT** Currently, the Full-Disk Encryption Status Report only provides information about full-disk encryption products installed on the system or the first physical drive only.

Absolute collects FDE data from the vendors of FDE software products and self-encrypting drives and returns the data in the following reports:

- Full-Disk Encryption Status Report – Products Detected
- Full-Disk Encryption Status Report – Products Not Detected

For the complete list of full-disk encryption products detected by the Absolute agent, see *Detected full-disk encryption products* in the online Help.

Turning On Full-Disk Encryption Data Collection for Your Account

By default, the collection of full-disk encryption data is turned off. You can collect full-disk encryption data on your managed Windows and Mac devices by turning it on in the Full-Disk Encryption Status Report (if you are a first-time user), or by using the Classic Account Settings page. Currently, the Full-Disk Encryption Status Report only provides information about full-disk encryption products installed on the system or the first physical drive only.

**NOTE** The time it takes for full-disk encryption data collection to start or stop is dependent on how often a device makes agent calls.

**IMPORTANT** You must log in as a Security Administrator to open the Full-Disk Encryption Status Report.

To turn on full-disk encryption data collection from the Full-Disk Encryption Status Report:

1. On the Security page, click **Full-Disk Encryption Status Report**.
2. When first-time users open the Full-Disk Encryption Status Report, a **Start Data Collection** button shows. Click **Start Data Collection** to begin collecting full-disk encryption data the next time this device makes an agent call.
   
   The Full-Disk Encryption Status Report refreshes with a confirmation message that data collection was enabled and that it may take some time before the collected data is available from this report.

To turn on the collection of full-disk encryption data from devices using the Classic Account Settings page:

**IMPORTANT** You must log in as an Administrator to open the Classic Account Settings page.

1. On the Security page, click ⬇️, and then click **Account > Classic Account Settings**.
2. At the **Full-Disk Encryption Status** area, select the **Collect full disk encryption data from devices** checkbox.
You can turn off data collection for full-disk encryption products on your devices. For more information, see "Turning Off Full-Disk Encryption Data Collection for Your Account" on page 140.

Filtering Data to Create a Full-Disk Encryption Status Report

The **Search Criteria** area on the Full-Disk Encryption Report provides similar functionality as most other reports (see "Generating Reports" on page 78.), with several exceptions that are particular to it.

**IMPORTANT** You must log in as a Security Administrator to filter data to create a Full-Disk Encryption Status Report.

To filter data to create a Full-Disk Encryption Status Report:

1. On the Security page, click **Full-Disk Encryption Status Report**.
2. On the Full-Disk Encryption Status 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 full-disk encryption products detected or not, at the **Full-Disk Encryption product is** location, select one of the following options:
     - Click **detected** to return a report that shows devices where FDE is detected. For more information, see "Identifying Devices That Have Full-Disk Encryption Products Installed" on page 136.
     - Click **not detected** to return a report that shows those devices on which no FDE products are detected. Selecting this option adds an **SED Capable** column to the results grid. For more information, see "Identifying Devices With No Installed Full-Disk Encryption Products" on page 137.
   - 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:
     - **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 given to a device.
     - **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
     - **Product Name**: the name of the full-disk encryption software.
     - **Version**: the version number of the detected full-disk encryption product (or program).
     - **Drive Description**: the collected encryption data to show only those devices with the detected attributes matching this drive description of the hard drive.
     - **Drive Serial Number**: the collected encryption data for devices where this drive serial number is detected on the hard drives of your account’s devices.
   - Depending on the values you selected from the 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 Last Agent 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 results in a larger report and takes 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 self-encrypted drive, in the and the device has a Self-Encrypting Drive field, select one of the following options:
  - Any: shows devices with software or hardware encryption.
  - Yes (SED capable): shows devices with a self-encrypting drive.
  - No: shows devices without a self-encrypting drive.
  - Not Detected: shows devices that do not have a self-encrypted drive detected.

- To filter results by the encryption status string used by a particular vendor, which is encrypted on a device, in the and where the Encryption Status String area, do the following:
  1. In the Select a rule field, open the list and select the appropriate rule.
  2. Enter the conditions based on the Encryption Status Strings from vendors. For more information, see "Viewing Changes to a Device’s Encryption Status Strings" on page 138.
  3. When you have entered up to five conditions specific to the vendors’ encryption status strings, click Add Condition.
     If you enter more than five conditions, the Add Condition button is inaccessible until you only have five conditions. Also the conditions allow and arguments only. You cannot enter an or argument.

If you do not add any conditions, all Encryption Status Strings show in the report.

**NOTE** You can Create an alert based on this encryption status criteria by clicking this link. If you want to save the filter information you have entered, you need to save it before creating a full-disk encryption alert. For those instructions and to add more conditions, see "Creating an Alert Based on Full-Disk Encryption Status Criteria" on page 22.

- At The status has changed since the last Agent call area, select the checkbox to see those devices whose full-disk encryption status changed between the last two agent calls.
  For alerts, if there’s a change in status between the Last Agent Call and the Next Agent Call, the alert is triggered.

- If BitLocker is your primary full-disk encryption product, clear the Show non-encrypted Microsoft BitLocker detections as not detected checkbox.
  In the absence of an installed full-disk encryption product, Absolute detects Microsoft BitLocker on most Windows platforms because the drivers are present even if the feature is not enabled.

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

**IMPORTANT** Currently, the Full-Disk Encryption Status Report only provides information about full-disk encryption products installed on the system or the first physical drive only.
• **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 80.

• **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.

• **Product Name**: the name of the detected encryption program.

• **Version**: the version number of the detected encryption product (or program).

• **Encryption Status String**: the detected string from the encryption vendor, which could be truncated due to length. Open the tooltip to see the entire string, which you can copy if necessary.

• **Algorithm**: the detected algorithm used by the encryption program, if available.

• **Drive Description**: the detected description for this device’s hard drive.

• **Drive Serial Number**: the detected serial number for the encryption drive on this device.

• **SED Capable**: indicates that an SED capable drive was detected on this device, however encryption may not be managed with SED management software.

• **Detected Date**: the date and time when the data was detected on the device.

• **Last Call**: the date and time when the agent last made a call on this device.

• **Last Reboot**: the date and time when the device was last started up.

• **Application Started**: the date and time when the application was started last.

• **The History** link opens the Encryption History Report that shows the 10 most recent changes to the Encryption Status String for this device. For more information, see "Viewing a Device’s Full-Disk Encryption History" on page 139.

For information about each report, see the following topics:

- "Identifying Devices That Have Full-Disk Encryption Products Installed" on page 136
- "Identifying Devices With No Installed Full-Disk Encryption Products" on page 137

**Identifying Devices That Have Full-Disk Encryption Products Installed**

**IMPORTANT** Currently, the Full-Disk Encryption Status Report provides information about full-disk encryption products installed on the system or the first physical drive only. You must log in as a Security Administrator to complete this task.

To run a report that shows the devices in your account that have full-disk encryption software installed on the hard drive that contains the operating system or that have an SED:

1. On the Security page, click **Full-Disk Encryption Status Report**.

2. On the Full-Disk Encryption Status Report in the Search Criteria section, at the Full-Disk Encryption product is area, click the detected option.

3. Enter all appropriate filtering criteria as described in the task, "Filtering Data to Create a Full-Disk Encryption Status Report" on page 134.

4. Look at the results grid to see the FDE software that was detected.
NOTE If nothing shows in a column, that information was not provided by the vendor and, therefore, could not be detected by the agent.

- **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 80.
- **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.
- **Product Name**: the name of the detected full-disk encryption product.
- **Version**: the version number of the detected encryption product (or program).
- **Encryption Status String**: the detected string from the full-disk encryption vendor, which could be truncated due to length. Open the tooltip to see the entire string, which you can copy if necessary.

NOTE Messages are provided about whether the drive is encrypted or not, or if there are any errors.

- **Algorithm**: the detected algorithm used by the encryption program, if available.
- **Drive Description**: the detected description for this device’s hard drive.
- **Drive Serial Number**: the detected serial number for the encrypted drive on this device.
- **SED Capable**: indicates that a drive capable of self-encryption was detected on this device, however full-disk encryption may not be managed with SED management software.
- **Detected Date**: the date and time when the data was detected on the device.
- **Last Call**: the date and time when the last agent call was made on this device.
- **Last Reboot**: the date and time when this device was last started up.
- **Application Started**: the date and time when the application was started last.
- **The History link opens the Encryption History Report that shows the 10 most recent changes to the Encryption Status String for this device. For more information, see "Viewing a Device’s Full-Disk Encryption History" on page 139.**

The Last Reboot and Application Start information is important in theft scenarios when you see that these dates are greater than the Incident Date. This means that the thief is logged into the device past the pre-boot authentication and the full-disk encryption product’s startup. Such cases indicate that the thief may have access to the device and that the theft could be an internal theft. The Encryption History Report is also useful in this type of theft scenario because it shows the last 10 changes to the device. See "Viewing a Device’s Full-Disk Encryption History" on page 139.

**Identifying Devices With No Installed Full-Disk Encryption Products**

Running a report that shows the devices in your account where the agent did not detect any full-disk encryption software products installed on the hard drive (that contains the operating system) lets you know if there are hard drives on which you can install a hardware encryption product. This report also lets you know if any SEDs are detected. If so, perhaps the SEDs are not managed by SED management software. You can also see what type of drive is detected by looking at the Drive Description and Drive Serial Number information.
IMPORTANT You must log in as a Security Administrator to open the Full-Disk Encryption Status Report.

To run a report that shows the devices in your account where the agent did not detect any full-disk encryption products installed on the hard drive:

2. On the Full-Disk Encryption Status Report, in the Search Criteria area, at the Full-Disk Encryption product is area, click the not detected option.
3. Enter all appropriate filtering criteria as described in the task, "Filtering Data to Create a Full-Disk Encryption Status Report" on page 134.

NOTE When you want to show devices where The Full-Disk Encryption product is not detected, the Encryption Status String filtering option is not available.

4. Look at the results grid, which shows the following information specific to what was detected.

NOTE If nothing shows in a column, that information was not provided by the vendor and, therefore, could not be detected by the agent.

- **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 80.
- **Device Name**: the name given to a device
- **Username**: the unique name detected by the agent to identify a person who is using a device.
- **Status**: is not available in this mode because there is no FDE software product installed.
- **Drive Description**: the detected description for this device’s hard drive.
- **Drive Serial Number**: the detected serial number for the encryption drive on this device.
- **SED Capable**: indicates that an SED capable drive was detected on this device, however encryption may not be managed with SED management software.
- **Detected Date**: the date and time when the data was detected on the device.
- **Last Call**: the date and time when the last agent call was made on this device.
- **History** link opens the Encryption History Report that shows the 10 most recent changes to the Encryption Status String for this device. For more information, see "Viewing a Device’s Full-Disk Encryption History" on page 139.

Viewing Changes to a Device’s Encryption Status Strings

Changes in a device’s Encryption Status Strings could indicate any of the following potential situations:

- a user has installed a different encryption product
- an encrypted drive that you were not tracking is now getting tracked
- there were other changes
- an encrypted drive was removed from the device
Setting an alert for these situations lets you know when they happen, without you having to determine these changes from analyzing the Full-Disk Encryption Status Report on your own. For more information, see "Creating an Alert Based on Full-Disk Encryption Status Criteria" on page 22.

**IMPORTANT** You must log in as a Security Administrator to open the perform this task.

To view changes to a device’s full-disk Encryption Status String:

1. On the Security page, click **Full Disk Encryption Status Report**.

2. On the Full-Disk Encryption Status Report page, at the **Full-Disk Encryption product** is area, click **detected**.

3. At the **Search Criteria** area, enter the appropriate filtering data as instructed in the task, "Filtering Data to Create a Full-Disk Encryption Status Report" on page 134.

4. At the **and where the Encryption Status String** area, do the following:
   a) Open the list, click **Contains**, and type **System disk**.
   b) Click **Add Condition**.
   c) Click **Show results**. The results grid refreshes to show all devices that contain **system disk** under the full-disk **Encryption Status String** column.

Viewing a Device's Full-Disk Encryption History

You can see the last 10 changes to a device’s full-disk Encryption Status String by opening the full-disk Encryption History Report.

**IMPORTANT** You must log in as a Security Administrator to perform the following task.

To view a device’s full-disk Encryption History Report:

1. On the Security page, click **Full Disk Encryption Status Report**.

2. On the Full-Disk Encryption Status Report page, at the **Search Criteria** area, enter the appropriate filtering data as instructed in the task, "Filtering Data to Create a Full-Disk Encryption Status Report" on page 134.

3. Click **Show results** and on the refreshed results grid find the appropriate device, scroll to the far right side of the grid, and click the **History** link for that device.

4. The full-disk Encryption History Report for the selected device opens and shows you the following information:

**IMPORTANT** Currently, the Full-Disk Encryption Status Report provides information about full-disk encryption products installed on the system or the first physical drive only.

- **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 80.
- **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.
- **Product Name**: the name of the detected full-disk encryption program.
Chapter 4: Working with Reports

- **Version**: the version number of the detected encryption product (or program).
- **Encryption Type**: indicates whether the device’s detected full-disk encryption is software or hardware.
- **Encryption Status String**: the detected string from the encryption vendor, which could be truncated due to length. Open the tooltip to see the entire string, which you can copy if necessary.
- **Algorithm**: the detected algorithm used by the encryption program, if available.
- **Drive Description**: the detected description for this device’s hard drive.
- **Drive Serial Number**: the detected serial number for the encryption drive on this device.
- **Detected Date**: the date and time when the data was detected on the device.
- **Last Call**: the date and time when the last agent call was made on this device.
- **Last Reboot**: the date and time when this device was last started up.
- **Application Started**: the date and time when the application was started last.
- **Action Date**: the date and time when an entry was added to the full-disk Encryption History Report for this device.

5. Click **<<Back** to return to the Full-Disk Encryption Status Report.

### Turning Off Full-Disk Encryption Data Collection for Your Account

You can turn off the collection of data for full-disk encryption for your account. This setting is found on the Classic Account Settings page at the **Full Disk Encryption Status** area. For more information, see "Editing Classic Account Settings" on page 54.

### SCCM Status Reports

SCCM Status reports show current and historical information about the status of the SCCM client installed on your managed Windows devices.

SCCM Status reports are applicable only if you are using System Center 2012 Configuration Manager, and the SCCM Status feature is turned on in the Absolute console. This feature can be turned on at the account level, the device level, or in this report. For more information, see the following topics:

- "Managing SCCM Status Reporting and Repair for your Account" on page 64
- "Managing SCCM Status Reporting for a Windows Device" on page 88
- "Managing SCCM Status Reporting and Repair in the SCCM Status Report" on page 145

This section includes the following topics:

- About Collecting SCCM Status From Windows Devices
- About Repairing SCCM Clients
- Working with the SCCM Status Report
- Working with the SCCM Status History Report
- Viewing the Details of a SCCM Status Change

**NOTE** To export a report that provides statistical information about the status of the SCCM clients installed on your Windows devices, see "Security Posture Report" on page 151.
About Collecting SCCM Status From Windows Devices

Microsoft System Center Configuration Manager (SCCM) is a system management software product that lets IT administrators manage their Windows devices by performing tasks remotely, such as:

- Deploying operating systems, software applications, and software updates
- Monitoring and reconciling compliance settings
- Monitoring hardware and software inventory

**NOTE** The SCCM Status feature supports System Center 2012 Configuration Manager only.

If your organization uses SCCM to manage its Windows devices, a small software application, the SCCM client, is installed on each Windows device to allow the device to connect to the SCCM server and be managed remotely. From time to time, the SCCM client may stop functioning correctly causing the device to lose contact with the SCCM server.

When the SCCM Status reporting feature is turned on, the agent detects the status of a device's SCCM client by running a script on the device every six hours. The script performs a series of health check tests to determine if the client is present and functioning correctly. You can view the results of these tests, and the device's SCCM Status, in the following reports:

- SCCM Status Report
- SCCM Status History Report

For more information about the components of the SCCM client that are tested, see "Viewing the Details of a SCCM Status Change" on page 148.

**NOTE** You can use the Alerts feature to trigger an alert notification when a device's SCCM Status changes. For more information about creating Alerts, see "Creating New Custom Alerts" on page 19.

About Repairing SCCM Clients

If the SCCM Status reporting feature is enabled, you can also enable the SCCM Repair feature. This feature initiates the repair of SCCM clients if they are not functioning correctly.

For more information about enabling SCCM Repair, see the following topics:

- "Managing SCCM Repair for Your Account" on page 65
- "Managing SCCM Repair for a Windows Device" on page 89
- "Managing SCCM Status Reporting and Repair in the SCCM Status Report" on page 145

When you enable the SCCM Repair feature, the agent runs a script every six hours to check the status of the SCCM client. The script performs a series of health check tests to determine if the client is present and functioning correctly. If any health check tests fail, an attempt is made to fix the problem. If the fixes are successful, the SCCM Status is updated to Repair successful on the next agent call. If any fixes fail, the status is updated to Repair failed on the next agent call, but the agent continues to attempt to fix the problem.

For more information about the components of the SCCM client that are tested and potentially fixed, see "Viewing the Details of a SCCM Status Change" on page 148.

**NOTE** If the SCCM client is absent from a device, SCCM Repair does not install the client.
You can view the results of each SCCM Repair on the following reports and pages:

- SCCM Status Report
- SCCM Status History Report
- SCCM Status History tab

**NOTE** You can use the Alerts feature to trigger an alert notification when SCCM Repair occurs on a device. For more information about creating Alerts, see "Creating New Custom Alerts" on page 19.

Working with the SCCM Status Report

The SCCM Status Report shows information about the current status of the SCCM client installed on your managed Windows devices. You can use this report to see if the client is missing or not functioning correctly on any of your Windows devices. You can also enable or disable SCCM Status reporting and Repair in the SCCM Status Report.

This section includes the following topics:

- Viewing the SCCM Status Report
- Managing SCCM Status Reporting and Repair in the SCCM Status Report

**Viewing the SCCM Status Report**

**NOTE** After the SCCM Status reporting feature is turned on, a device needs to make two successful agent calls before its initial SCCM Status is available in the report.

To view the SCCM Status of one or more Windows devices:

1. On the Security page, click **SCCM Status Report**.
2. On the SCCM Status Report page, at the **Search Criteria** area, enter the appropriate filtering data:
   - To filter your results by Device Group, in the **Group is** field, open the list and select the appropriate device group.
   - To find a 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 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 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 SCCM Status, click the **and the SCCM status is** field and select one of the following values:
     - **Absent**: the SCCM client is not installed on the device.
     - **Needs attention**: one or more health check tests failed and SCCM Repair is currently not enabled on the device
     - **OK**: all health check tests passed and the SCCM client is functioning correctly.
Repair failed: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client failed to be repaired.

Repair successful: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was repaired.

- To filter your results by date, in the **and the last call in occurred** area do one of the following:
  - To not limit the report based on the date of the last call, select **at any time**. This option may result in a very large report that takes longer to generate.
  - To limit the report to devices that have called within a specific number of days, 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 results in a larger report that takes longer to generate.
  - To limit the report to devices that have called during a specific data range, 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 SCCM configuration, in the **and SCCM Settings are** area clear one or more of the following checkboxes:
  - Repair enabled
  - Repair disabled
  - Reporting enabled
  - Reporting disabled

3. Click **Show results**.

The results grid refreshes and shows the following information:

- **SCCM Reporting**: shows an indicator of whether SCCM Status reporting is **currently** enabled for the device.
- **SCCM Repair**: shows an indicator of whether SCCM Repair is **currently** enabled for the device.
- **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 80.
- **Device Name**: the name given to a device.
- **SCCM Status**: the status of the SCCM client on this device, reported at the last successful agent call. Possible values are:
  - **Absent**: the SCCM client is not installed on the device.
  - **Needs attention**: one or more health check tests failed and SCCM Repair is not enabled on the device. You may want to enable SCCM Repair for this device.
  - **OK**: all health check tests passed and the SCCM client is functioning correctly.
  - **Repair failed**: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was not repaired. For more details about why the repair failed, click the link.
NOTE If repeated attempts to repair the SCCM client fail, see “Troubleshooting Failed SCCM Repairs” on page 151.

- **Repair successful**: SCCM Repair is enabled. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was repaired.

To view the results of each health check test, click the link to open the SCCM Status Details dialog. If SCCM Repair is enabled, any applicable repair results also show. For more information, see “Viewing the Details of a SCCM Status Change” on page 148.

- **Status Date**: the date and time of the agent call when the SCCM Status was reported
- **Issue Count**: the total number of times the device’s SCCM Status has changed from OK to an unhealthy state. The Issue Count is incremented each time one of the following status changes occurs

NOTE Possible status changes depend on whether SCCM Repair is enabled.

<table>
<thead>
<tr>
<th>SCCM Repair</th>
<th>Status changes that increment Issue Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>• OK to Repair successful</td>
</tr>
<tr>
<td></td>
<td>• OK to Repair failed</td>
</tr>
<tr>
<td></td>
<td>• OK to Absent</td>
</tr>
<tr>
<td></td>
<td>• Repair failed to Absent</td>
</tr>
<tr>
<td></td>
<td>• Repair successful to Repair successful</td>
</tr>
<tr>
<td></td>
<td>• Repair successful to Repair failed</td>
</tr>
<tr>
<td></td>
<td>• Repair successful to Absent</td>
</tr>
<tr>
<td></td>
<td>• Absent to Repair failed</td>
</tr>
<tr>
<td></td>
<td>• Absent to Repair successful</td>
</tr>
<tr>
<td>Disabled</td>
<td>• OK to Absent</td>
</tr>
<tr>
<td></td>
<td>• OK to Needs attention</td>
</tr>
<tr>
<td></td>
<td>• Needs attention to Absent</td>
</tr>
<tr>
<td></td>
<td>• Absent to Needs attention</td>
</tr>
</tbody>
</table>

Click the linked numeral to open the SCCM Status History Report page and view the device's status history.

- **Username**: the unique name detected by the agent that identifies the person who is associated with this device
- **Serial Number**: the serial number of the device
- **Make**: the manufacturer of a device
- **Model**: the product type of a device
- **Operating System**: software that controls the operation and applications of the device, and may provide various services
Managing SCCM Status Reporting and Repair in the SCCM Status Report

**IMPORTANT** With the release of Absolute 7.2, you can now use the Application Persistence feature to report on and repair SCCM clients installed on your Windows devices. If you have SCCM Status Reporting and Repair enabled, we recommend that you disable it and activate the Application Persistence: Microsoft SCCM policy in one or more policy groups. For more information, see *About Application Persistence: Microsoft SCCM policies* in the online Help.

You can manage SCCM Status reporting or SCCM Repair for one or more Windows devices that show in the SCCM Status report.

**NOTE** To disable SCCM Status reporting and SCCM Repair for all devices in your account, see "Managing SCCM Status Reporting and Repair for your Account" on page 64.

**IMPORTANT** You must log in as an Administrator or Power User to perform these SCCM tasks.

To manage SCCM Status reporting and Repair for one or more Windows devices:

1. On the Security page, click **SCCM Status Report**.
2. On the SCCM Status Report page, at the **Search Criteria** area, enter the appropriate filtering data to generate the desired list of devices in the results grid. For more information, see "Viewing the SCCM Status Report" on page 142.
3. Click **Show results**.
4. In the results grid, select the devices that you want to update by doing one of the following:

**NOTE** Each device's **SCCM Reporting** indicator shows whether SCCM Status reporting is currently enabled or disabled. Similarly, each device's **SCCM Repair** indicator shows whether SCCM Repair is currently enabled or disabled. If you want to enable these features on some devices and disable other devices, you need to perform two separate tasks.

- To select individual devices, select the checkbox for each device.
- To select all devices shown on this page, select the checkbox in the header.
- To select all devices in the results, hover your mouse over the down arrow in the header. Click the **Select All <n> Records** (where <n> is the number of records) to select all of the devices that meet the filter criteria you set earlier.

5. To manage SCCM Status reporting for the selected devices, select **Disable SCCM Reporting** from the list.
6. To manage SCCM Repair for the selected devices, select **Disable SCCM Repair** from the list.
7. Click **Save changes**.
8. If the Confirm dialog shows, review the details of the requested action to confirm that they are correct and click **Continue**.

On the SCCM Status Report page, the applicable SCCM indicators are refreshed to show their new status.
Working with the SCCM Status History Report

The SCCM Status History Report shows information about changes to the status of the SCCM client installed on your managed Windows devices. You can use this report to see if a device's SCCM client is repeatedly experiencing issues that prevent it from functioning correctly.

**NOTE** After the SCCM Status feature is turned on, a device needs to make two successful agent calls before its initial SCCM Status is available in the report.

To view the SCCM status of one or more Windows devices:

1. On the Security page, click **SCCM Status History Report**.
2. On the SCCM Status History Report page, at the **Search Criteria** area, enter the appropriate filtering data:
   - To filter your results by Device Group, in the **Group** field, open the list and select the appropriate device group.
   - To find a 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 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 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 SCCM Status, click the **and the SCCM status** field and select one of the following values:
     - **Absent**: the SCCM client is not installed on the device.
     - **Needs attention**: one or more health check tests failed and SCCM Repair is currently not enabled on the device
     - **OK**: all health check tests passed and the SCCM client is functioning correctly.
     - **Repair failed**: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was not repaired.
     - **Repair successful**: SCCM Repair is enabled. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was repaired.

   - To filter your results by date, in the **and the last call in 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 results in a larger report and takes 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 and shows the following information:

- **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 80.
- **Device Name**: the name given to a device.
- **SCCM Status**: the status of the SCCM client on this device, reported at the last successful agent call. Possible values are:
  - **Absent**: the SCCM client is not installed on the device.
  - **Needs attention**: one or more health check tests failed and SCCM Repair is not enabled on the device. You may want to enable SCCM Repair for this device.
  - **OK**: all health check tests passed and the SCCM client is functioning correctly.
  - **Repair failed**: SCCM Repair is enabled on the device. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was not repaired. For more details about why the repair failed, click the link.

**NOTE** If repeated attempts to repair the SCCM client fail, see "Troubleshooting Failed SCCM Repairs" on page 151.

- **Repair successful**: SCCM Repair is enabled. An attempt was made to repair the SCCM client because it was not functioning correctly. The client was repaired.

To view the results of each health check test, click the link to open the SCCM Status Details dialog. If SCCM Repair is enabled, any applicable repair results also show. For more information, see "Viewing the Details of a SCCM Status Change" on page 148.

**NOTE** Each row in the SCCM Status History Report corresponds to a SCCM Status change. A SCCM Status change is logged if the details of a test result change between agent calls (date and time changes are excluded). This means that it is possible for the SCCM Status History Report for a device to include consecutive entries with the same SCCM Status.

For example, a device with SCCM Repair enabled shows on the report with a status of **Needs attention** because two health check tests failed. At the next agent call, the script is run again and three health check tests fail. Although the SCCM Status for the device remains set to **Needs attention**, a status change is logged because the results of the health check tests changed. Similarly, if a SCCM attribute changes when a device’s status is **OK**, a status change is logged, but the status remains set to **OK**.

- **Status Change Date**: the date and time when the SCCM Status change occurred
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device
- **Serial Number**: the serial number of the device
- **Make**: the manufacturer of a device
- **Model**: the product type of a device
- **Operating System**: software that controls the operation and applications of the device, and may provide various services
Viewing the Details of a SCCM Status Change

From the SCCM Status report, you can view the individual test results that led to a device’s SCCM Status change.

To view the details of a SCCM Status change:

1. Open the SCCM Status Report or the SCCM Status History Report and enter the appropriate search criteria to generate the report. For more information, see the following topics:
   - “Viewing the SCCM Status Report” on page 142
   - “Working with the SCCM Status History Report” on page 146

2. In the results grid, click the applicable link in the SCCM Status column. You can view test results for all SCCM statuses.

The SCCM Status Details dialog opens to show the following information:

<table>
<thead>
<tr>
<th>Section</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Status</td>
<td>SCCMStatus</td>
<td>The status of the SCCM client, as determined by the health check tests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are <strong>Absent</strong>, <strong>Needs attention</strong> and <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>StatusChangeDate</td>
<td>The date and time when the test results were collected and the device’s SCCM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status changed</td>
</tr>
<tr>
<td></td>
<td>RepairResult</td>
<td>The overall status of an attempt to repair the SCCM client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are <strong>Repairs succeeded</strong>, <strong>At least one repair failed</strong> and</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>N/A</strong></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td>Applies only if SCCM Repair is enabled for the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If repeated attempts to repair the SCCM client fail, see</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Troubleshooting Failed SCCM Repairs&quot; on page 151.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td><strong>N/A</strong> indicates that a repair was not attempted because</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all health check tests passed.</td>
</tr>
</tbody>
</table>

<p>| Client Information | CCMInstallPath       | The directory where the Microsoft Configuration Client Manager (CCM) is     |
|                   |                      | installed                                                                  |
|                   |                      | CCM is a component of SCCM and is used to install the SCCM client.          |
|                   | AssignedSite         | The primary SCCM site that the device is assigned to                        |
|                   | ManagementPoint      | The site system role that provides policy and service location information   |
|                   |                      | to the SCCM client and receives configuration data from the client         |
|                   | SCCMClientVersion    | The version number of the installed SCCM client                            |
|                   | Domain               | The current domain of the computer                                         |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Information</td>
<td>DriveLetter</td>
<td>The drive where the cache folder is stored</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>The temporary download location for software, applications, and software updates that are deployed to the SCCM client. The default location is %windir%\ccmcache.</td>
</tr>
<tr>
<td></td>
<td>TotalSize</td>
<td>The maximum size (MB) of the cache folder. The default value is 5120 MB.</td>
</tr>
<tr>
<td></td>
<td>FreeSize</td>
<td>The unused space (MB) in the cache folder</td>
</tr>
<tr>
<td>Inventory Scans</td>
<td>LastHWScan</td>
<td>The date and time of the last scan by the SCCM client of installed hardware</td>
</tr>
<tr>
<td></td>
<td>LastSoftwareScan</td>
<td>The date and time of the last scan by the SCCM client of installed software</td>
</tr>
<tr>
<td>Section</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tests</td>
<td>Test Description</td>
<td>The SCCM component that was tested and the purpose of the test.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following components are tested:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Windows Management Instrumentation (WMI)</em>: an infrastructure that is critical for the operation of the SCCM client. The test checks that it can connect to the WMI and make a simple query.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Admin share</em>: used to deploy the SCCM software remotely by allowing administrative remote access to the disk volume over the network. The test checks that this share is present and enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Local CCM Path</em>: the test checks the path to the CCM component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>CCM Service Status</em>: the test checks that the CCM component is running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Services</em>: the test checks that the SCCM client service and its dependent services are running. The following services are checked: <code>winmgmt</code>, <code>lanmanserver</code>, <code>rpcss</code>, <code>bits</code>, and <code>ccmexec</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Registry</em>: the test checks the registry to ensure that DCOM is enabled. DCOM is a protocol that allows for remote client connections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Client version</em>: the test checks the version number of the installed SCCM client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Client variables</em>: the test checks that it can retrieve the SCCM client variables.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Assigned site</em>: the test check for the primary SCCM site.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Hardware inventory</em>: the test checks for the last hardware inventory date and time. The test fails if a hardware scan has never been run, or the value cannot be retrieved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>Software inventory</em>: the test checks for the last software inventory date and time. The test fails if a software scan has never been run, or a value cannot be retrieved.</td>
</tr>
<tr>
<td></td>
<td>TestStatus</td>
<td>The result of the test. Possible values are <strong>Pass</strong> and <strong>Fail</strong>.</td>
</tr>
<tr>
<td></td>
<td>TestResultsDetails</td>
<td>A brief description of the test result</td>
</tr>
<tr>
<td>Tests</td>
<td>RepairResults</td>
<td>The result of an attempt to repair a particular component of the SCCM client.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td>Applies only if SCCM Repair is enabled for the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are <strong>Repair succeeded</strong>, <strong>Repair failed</strong>, and <strong>N/A</strong> (repair not attempted because the health check test passed).</td>
</tr>
</tbody>
</table>

3. To close the dialog, click **Close**.
Troubleshooting Failed SCCM Repairs

When SCCM Repair is enabled on a device, and the SCCM client is not functioning correctly, the device's agent attempts to repair the SCCM client at six hour intervals.

You may find that repeated attempts to repair the client are unsuccessful. If this is the case, Absolute recommends that you perform the following steps to troubleshoot the issue with the device's SCCM client:

1. Review the details of each of the device's failed repair attempts. In particular, review the information provided in the TestResultDetails attribute for each failed HealthCheck test. For more information, see "Viewing the Details of a SCCM Status Change " on page 148.

2. If one or more services failed to be repaired, contact the user and ask them to restart the device. Some services, specifically lanmanserver and ccmexec, require a device reboot after the service is repaired.

3. If the SCCM client is not repaired after step 2 is completed, refer to System Center 2012 Configuration Manager documentation, or search the articles and posts available from Microsoft TechNet Support at https://technet.microsoft.com/en-us/ms772425.

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
- SCCM status (for Windows devices only)
- Anti-virus definition status
- Last agent call statistics
- Device counts for Device Freeze, Data Delete, and Investigation Reports

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:

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 92.

   **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**
- **Device Drift History Report**
- **Activation Report**
- **Geolocation Tracking Reports**
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 🔄.
2. On the Find Devices page, click **Classic Reports > 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, Missing Devices, and Device Drift History reports may contain caller identification information. The caller identification information usually shows as a link. Clicking the link opens the Extended IP Call Information page, 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.
o **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:**
  - Open the list and select one of the following options:
    - **Public IP**
    - **Local IP**
  - 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 80.
- **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 153.

**Missing Devices Report**

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

Periodically review the Identifiers assigned to devices in your organization. Check for any devices that have not contacted the Monitoring Center for an unusually long period of time, such as 45 days. Lack of contact from a device may indicate that the agent is missing, or that an event has occurred preventing the agent from contacting the Monitoring Center. Dormant devices are excluded from the report automatically. You may also need to adjust the **Most Recent Call Filter** value to ensure that results grid contains results. See "About Extended IP Call Information" on page 153.

To generate a Missing Devices Report

1. **On** the Call History and Loss Control page, click **Missing Devices Report**.
2. On the **Missing 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 is** field, open the list and select the appropriate department.
   - To filter your results by agent call, in the **and the most recent Call is more than** field, enter a value for the number of 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 80.
   - **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.
   - **Serial Number**: the serial number of the device or other hardware.
   - **Asset Number**: the identification number associated with a device in the Absolute console.
- **Make**: the manufacturer of the device.
- **Model**: the product type of a device or other hardware.
- The **Call History** link opens the Call History Report that shows all communications this device. For more information, see "Call History Report" on page 153.

### Device Drift by Device Name Report

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

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

This section provides information about the Device Drift History Report, which you can open from this report.

To generate a Device Drift by Device Name Report:

1. On the Call History and Loss Control page, click **Device Drift by Device Name Report**.
2. On the Device Drift by Device Name 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 a specific device, at the **and the field** area, open the list and select **Device Name**.
   - Click **Choose** to open the list and select the appropriate device.
   - 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, at the **and the change occurred 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 80.
   - **Device Name**: the name assigned to this device in the operating system.
   - **Serial Number**: the serial number of this device.
   - **Asset Number**: the identification number associated with a device in the Absolute console.
   - **Full Windows Device name**: The fully qualified domain name (FQDN) of a device, including the device name, domain name, and all higher-level domains.
Chapter 4: Working with Reports

- The **Device History** link opens the Device Drift History Report that shows all changes for a specific **Identifier** to the **Username, Device Name, Call Time, Local Ip (Address), Caller Id, Domain, and Workgroup** values.

  In the **Caller Id** column click an IP address to view more detailed caller ID information. For more information, see "About Extended IP Call Information" on page 153.

**Device Drift History Report**

The Device Drift History Report is a sub-report available from the **Device Drift by Device Name** and **Device Drift by Username** reports.

The Device Drift History Report shows all changes for a specific **Identifier** to the **Username, Device Name, Call Time, Local Ip (Address), Caller Id, Domain, and Workgroup** values.

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

To view the Device Drift History Report, in the **results** grid for the Device Drift by Device Name or Device Drift by Username reports, click the **Device History** link.

To view more detailed caller ID information, click an IP address in the **Caller Id** column. For more information, see "About Extended IP Call Information" on page 153.

**Device Drift by Username Report**

The Device Drift by Username Report identifies devices that have had a change in the **Username** within a specified date range. You can specify filter criteria pertaining to current or previous Usernames.

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

From the Device Drift by Username Report, you can also open the Device Drift History Report.

To generate a Device Drift by Username Report:

1. On the Call History and Loss Control page, click **Device Drift by Username Report**.
2. On the Device Drift by Username 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 **Username**.
   - Click **Choose** to open the list and select the appropriate device.
   - 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**, at the **and the change occurred 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.
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 80.
- **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.
- **Full Windows Device name**: the fully qualified domain name (FQDN) of a device, including the device name, domain name and all higher-level domains.
- The **Device History** link opens the Device Drift History Report that shows all changes for a specific **Identifier** to the **Username**, **Device Name**, **Call Time**, **Local Ip (Address)**, **Caller Id**, **Domain**, and **Workgroup** values.
- In the **Caller Id** column click an IP address to view more detailed caller ID information. See "About Extended IP Call Information" on page 153.

**Activation Report**

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

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

To generate an Activation report:

1. On the Call History and Loss Control page, click **Activation Report**.
2. On the Activation 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, at 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.
     - **Assigned Username**: The username assigned to a device by a system administrator on the View and Edit Custom Device Fields page.
     - **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.

Device Name: the name assigned to this device in the operating system.

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.

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 Department, in the and the Department is field, open the list and select the appropriate department.

To return a report that shows devices that have been recently activated, select the Show Most Recent Activations checkbox. Selecting this option will turn the Persistence Status filter off.

- To filter your results by date, at the and the Activation Date area, do one of the following:
  - In the in the last \(<n>\) days field, select the option and enter the number of days you want to include in the report. For example, enter a value of "500" to include all activations that occurred over the past 500 days.

  **NOTE** Entering a higher value in this field may result in a larger report and may take longer to generate results.

  - In the between field, select 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 results by agent type and version, at the and the Agent area:
  - In the Type field open the list and select the appropriate type of agent as follows:
    - Any Type returns a report that shows devices with all agent types.
    - Android returns a report that shows only Android devices.
    - Chromebook returns a report that shows only Chromebooks and Chrome devices.
    - iOS returns a report that shows only iPads and iPad minis.
    - Mac returns a report that shows only Mac devices.
    - Windows returns a report that shows only devices running a Windows operating system.
  - In the and version field, open the list and select the appropriate agent version for the agent Type you selected previously.

  For example, if you want to show all devices that have the 898 version of the agent installed on them, in the type field, open the list and select Any Type and in the and version field open the list and select 898.

**IMPORTANT** SHC (Self-Healing Call) returns a report that shows devices with agents that called in from Persistence. This option shows when a Self Healing Call has occurred.
To filter your results by the condition of the Persistence Technology, at the **Persistence Status** area, select one of the following values:
- **All**: returns results for all devices regardless of their Persistence state.
- **BIOS/Firmware Active**: returns results for devices with activated firmware-based Persistence modules. Firmware Persistence is **Active** and is providing application agent health checks when the devices are restarted.
- **BIOS/Firmware Pending**: returns results for devices with firmware-based Persistence modules that are in the process of activating. Additional automatic agent calls may be required before this device transitions to **Active** status.
- **N/A**: describes devices that have no Persistence whatsoever; for example, a Mac computer.

**NOTE** Before you can detect BIOS/Firmware Persistence on an activated device, you need to reboot the device once after it is activated and have it make at least two agent calls.

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 80.
- **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.
- **Assigned Username**: the username assigned to a device by a system administrator on the View and Edit Custom Device Fields page.
- **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.
- **Activation Date/Time**: the date and time the device completed its first call to the Monitoring Center.
- **Last Call Date/Time**: when the agent installed on a device most recently contacted the Monitoring Center.
- **Version**: the version number of the Absolute agent that contacts the Monitoring Center.
- **Persistence Status**: how the agent is automatically restored when necessary.
- **System BIOS/Firmware Version**: the unique name and number assigned to the Basic Input/Output System (BIOS) of a device.
- **System BIOS/Firmware Date**: the date and time the Basic Input/Output System (BIOS) installed on the device was released.
- **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.
Geolocation Tracking Reports

Geolocation Tracking reports include the Device Location Report and the Device Location History Report. These reports can be used to monitor the locations of your managed devices using any or all of the supported location technologies.

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

This section provides information on the following topics:

- Geolocation System Requirements
- Understanding Location Technologies
- Enabling Geolocation Reporting
- Device Location Report
- Device Location History Report

**NOTE** Depending on the product your organization purchased, the Geolocation Tracking feature may not be available.

Geolocation System Requirements

You must install a supported version of the agent on devices that you want to be tracked using geolocation.

The Geolocation Tracking feature supports the following platforms, hardware, and software on devices:

**NOTE** The Geolocation Tracking feature is not supported on devices running a Linux-based operating system.

- For Windows devices:
  - Operating Systems: for more information about the requirements for Windows devices, open the Absolute console’s help system and search for supported platforms for managed devices.
  - Current version of the agent. See "Downloading the Absolute Agent for Android Devices" on page 67.
  - If you want locations using GPS, you need a supported GPS receiver from the following list:

    **IMPORTANT** Most GPS receivers available for Windows devices are supported. The following list is not exhaustive. Location data is not collected from a tether, using a Bluetooth wireless, USB, or serial connection, for example, to a device that has a GPS receiver. Ensure that you install the driver for the GPS receiver and that the wireless switch is enabled.

    - Qualcomm UNDP-1 (Gobi 1000) mobile broadband adapters
    - Qualcomm 9202 mobile broadband adapter
    - Ericsson F3507g and F3607gw mobile broadband adapters
    - HP un2400 & un2420 mobile broadband adapters
    - Dell 5600 mobile broadband adapter
If you want locations using Wi-Fi, the device must have a built-in Wi-Fi network adapter that is enabled.

- For Mac devices:
  - Operating Systems: for more information about the requirements for Mac devices, open the Absolute console's help system and search for supported platforms for managed devices.
  - Mac agent version 914 or higher. See "Downloading the Absolute Agent for Android Devices" on page 67.
  - If you want locations using Wi-Fi, the device must have a built-in Wi-Fi network adapter that is enabled.

**NOTE** Core Location is **not** supported at this time.

- For Android devices:
  - Operating Systems: for more information about the requirements for Android devices, open the Absolute console's help system and search for supported platforms for managed devices.
  - If you want locations using GPS, the device must have a built-in GPS/A-GPS receiver that is enabled.
  - If you want locations using Wi-Fi positioning, the device must have a built-in Wi-Fi network adapter that is enabled.
  - If you want locations using Cell Tower/Network location technology, the device must support this feature, which needs to be enabled.

- For Chromebooks:
  - Operating Systems: for more information about the requirements for Chromebooks, open the Absolute console's help system and search for supported platforms for managed devices.

**NOTE** Chromebooks support API and IP Georesolution location technologies only.

### Understanding Location Technologies

This section provides information on the following topics:

- Types of Location Technologies
- Limitations of Global Positioning Systems (GPS)
- Limitations of Wi-Fi Positioning
- Collecting Location Data
Types of Location Technologies

In order of accuracy and reliability, location information can be collected using any of the following technologies:

<table>
<thead>
<tr>
<th>Location Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Maps™ Wi-Fi Positioning</td>
<td>Google Maps Wi-Fi Positioning determines a device's location by comparing Wi-Fi hotspots detected by the device with Google's extensive database of known hotspots and their locations. The device does not need to be connected to a Wi-Fi hotspot for the hotspot to be detected. This technology is most effective in urban areas where Wi-Fi hotspots are plentiful. It works with Windows and Mac devices, and Android mobile devices. To use Google Maps Wi-Fi Positioning, a setting needs to be enabled in your account. For information about enabling this setting, see &quot;Editing Classic Account Settings&quot; on page 54. NOTE If a managed device is in a country where Google Maps is prohibited, Google Maps Wi-Fi Positioning cannot be used to resolve the device’s location.</td>
</tr>
<tr>
<td>Global Positioning System (GPS)</td>
<td>Global Positioning System (GPS) technology determines a device's location using built-in sensors to capture satellite signals that indicate the device's location. GPS is most effective when the device is outdoors. This technology works with Windows devices and Android mobile devices that are equipped with a supported GPS receiver.</td>
</tr>
<tr>
<td>Other Location Technologies</td>
<td>Includes the following technologies:</td>
</tr>
<tr>
<td></td>
<td>● API, such as the Microsoft Windows Sensor and Location API and the Geolocation API, use a variety of methods to identify device locations. This technology works with Windows and Chromebook devices.</td>
</tr>
<tr>
<td></td>
<td>● Cell, identifies device locations using Cell Tower/Network location technology. This information is typically determined using triangulation techniques that are based on known locations of 2G, 3G, and 4G base stations and/or known locations of Wi-Fi networks. These known locations are maintained by the device manufacturer or by the mobile network operator. This technology works with Android mobile devices.</td>
</tr>
<tr>
<td>Absolute Wi-Fi Positioning</td>
<td>Absolute Wi-Fi Positioning determines a device's location by comparing Wi-Fi hotspots detected by the device with Absolute's database of known hotspots and their locations. The device does not need to be connected to the Wi-Fi hotspot for the hotspot to be detected. This technology is most effective in urban areas where Wi-Fi hotspots are plentiful. It works with Windows and Mac devices, and Android mobile devices.</td>
</tr>
<tr>
<td>IP Georesolution</td>
<td>IP Georesolution uses a database of IP addresses and their locations to determine a device's location. This technology is typically accurate at the country level, but device locations within a region or city are less reliable. This technology works with Windows, Mac, Android, and Chromebook devices.</td>
</tr>
</tbody>
</table>

Limitations of Global Positioning Systems (GPS)

GPS receivers are designed to receive a signal from satellites reliably when outside with an unobstructed view of the sky. Therefore, GPS receivers are unlikely to work well when surrounded by high-rise buildings or inside metal-framed or concrete buildings. GPS receivers may work inside non-metal framed buildings or near a window.
The accuracy of the location reported by a GPS depends on environmental issues such as how many satellites are in view, potential reflection of satellite signals from nearby objects, or atmospheric effects. In ideal conditions, the GPS available typically reports locations within 10 m of actual location. When conditions are less favorable, error may increase to 100 m or more. GPS coordinates are unlikely to be exact.

Limitations of Wi-Fi Positioning

Wi-Fi positioning is a correlational tracking method based on the known GPS location of Wi-Fi hotspots detected near a device. The measured strength of the Wi-Fi signal helps to determine the device’s proximity to a given hotspot. Typically, Wi-Fi positioning provides a location accurate to within a few city blocks.

Collecting Location Data

For all location technologies, except Google Maps Wi-Fi Positioning and IP Georesolution, location data is collected hourly and uploaded to the Absolute console each time a device calls the Monitoring Center (usually once a day). For Google Maps Wi-Fi Positioning and IP Georesolution, locations are collected every time the device calls the Monitoring Center.

**NOTE** If you want to upload location data every time a device changes its location, you can enable Event Calling for your managed Windows and Mac devices. For more information, see "Managing Event Calling for Your Account" on page 59.

End users of a device can disable the location technology; for example, users can disable GPS or Wi-Fi for all applications. To collect location information, at least one of the supported location technologies must be enabled on the device.

Enabling Geolocation Reporting

By default, the Device Location and the Device Location History reports are not enabled for your account. You must submit a Geolocation Authorization Agreement before the reports are enabled.

**NOTE** Location data is collected for devices equipped with the Geolocation Tracking feature only. For a list of the hardware and software required to collect geolocation information from a device, see "Geolocation System Requirements" on page 161.

**IMPORTANT** You must log in to the Absolute console as an Administrator to perform the next task.

To enable Geolocation reporting:

1. On the navigation bar, click ．
2. The Help and Support page opens with the Documentation page showing.
3. Under the Service Request Forms area, click the Security Administrator and Geolocation Tracking Authorization Form link.
4. Complete and return the form to the Absolute Technical Support fax number shown on the form. Technical Support notifies you when the Geolocation Reporting feature is enabled for your account.
Device Location Report

The Device Location Report shows the most recent geographic locations, also called geolocations, of devices based on the best location technology available on a device when reporting a location.

To generate a Device Location Report:

1. On the Call History and Loss Control page, click **Device Location Report**. The Geolocation Tracking page opens.
2. On the Geolocation Tracking page, click **Accept** to accept the terms and conditions of the Service Agreement.
3. On the Device Location 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 a specific device, at 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.
     - **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.
     - **Assigned Username**: the username assigned to a device by a system administrator.
     - **Warranty Contract Vendor**: the warranty provider for a 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 when the** 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 results by agent type and version, at the **and the Agent** area:
     - **i)** In the **Type** field open the list and select the appropriate type of agent as follows:
       - **Any Type** returns a report that shows devices with all agent types.
       - **Android** returns a report that shows only Android devices.
       - **Mac** returns a report that shows only Mac devices.
       - **Windows** returns a report that shows only devices running a Windows operating system.
○ **Chromebook** returns a report that shows only Chromebooks and Chrome devices.

ii) In the **and version** field, open the list and select the appropriate agent **Version** for the agent **Type** you selected previously.

For example, if you want to show all devices that have the 898 version of the agent installed on them, in the **type** field, open the list and select **Any Type** and in the **version** field open the list and select **898**.

**NOTE** **SHC** (Self Healing Call) returns a report that shows devices with agents that called in from Persistance. This option appears when a Self Healing Call has occurred.

- 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 the agent status, in the **and Status is** field, open the list and select one of the following options:
  - **All** shows those specified devices where the operating condition of the agent is Active, Inactive, or Disabled.
  - **Active** shows only those devices whose agent has called the Monitoring Center.
  - **Inactive** shows only those devices whose agent has not yet called the Monitoring Center.
  - **Disabled** shows only those devices whose agent is either flagged for removal or removed from the device.

- To filter your results by Location, at the **and the Location area** 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 of the following options:
  - **Google Maps™ Wi-Fi Positioning**
    
    If this option is grayed out, this location technology is not available because the **Use Google Geolocation for Wi-Fi Points** setting is not enabled in your account. For information about enabling this setting, see "Editing Classic Account Settings" on page 54.

    If this option is not shown, Google Maps and its location technology are prohibited in your country (determined by the IP address of your computer).

    - **GPS**
    - **Other Location Technologies**
    - **Absolute Wi-Fi Positioning**
    - **IP Georesolution**

    For more information about each location technology, see "Types of Location Technologies" on page 163.

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

   In the **results** grid, devices equipped with Geolocation Tracking show as icons on the map. All existing Geofence boundaries for your account also show.
You can navigate the map using the following tools:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pan</td>
<td>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.</td>
</tr>
<tr>
<td>Zoom</td>
<td>Use the Zoom tool to zoom in or out of specific areas of the map.</td>
</tr>
<tr>
<td></td>
<td>● To zoom in, click ( \uparrow ) repeatedly, or move the slider towards the button. You can also zoom in by double-clicking the map or moving your mouse scroll wheel.</td>
</tr>
<tr>
<td></td>
<td>● To zoom out, click ( \downarrow ) repeatedly, or move the slider towards the button. You can zoom out by moving your mouse scroll wheel.</td>
</tr>
</tbody>
</table>
| 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 geolocation map in the Device Location Report is a Google Map. If Google Maps are prohibited in your country (determined by the IP address of your computer), an ESRI® map shows instead. For more information about working with ESRI maps, go to [www.esri.com](http://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 are 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 Geolocation

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

5. Click an icon to open a dialog containing a Zoom In link to view the location, as well as the following details about devices that the icon represents:

- **Identifier** is the unique identifying number associated with the device.
- **Device Name** is the name assigned to this device in the operating system.
- **Username** is the unique name detected by the agent that identifies the person who is associated with this device.
- **Make** is the name of the device manufacturer as captured by the agent.
- **Model** is the model number of the device as captured by the agent.
- **Location** is a link that lets you zoom in to the last known location of the device.
- **Location Time** is the date and time of the last known location of the device. Clicking the History link opens the Device Location History Report for the device.
- **Location Technology** is the technology used to determine the location of the device.

6. The results grid below the map provides full location details for each device. Click a link in the Last Known Location (Latitude, Longitude) column to view a device’s location on the map.

For more information about using geotechnology, see "Managing Geofences" on page 265.

**Device Location History Report**

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

The Device Location History Report tracks the location of a single device over time, using the best location technology available when the device reported a location. For a list of available location technologies organized in order of accuracy and reliability, see "Types of Location Technologies" on page 163.
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.

For more information about using geotechnology, see "Managing Geofences" on page 265.

**IMPORTANT** You must log in to the Absolute console as an Administrator or Power User to perform the next task.

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**
       - If this option is grayed out, this location technology is not available because the **Use Google Geolocation for Wi-Fi Points** setting is not enabled in your account. For information about enabling this setting, see "Editing Classic Account Settings" on page 54. If this option is not shown, Google Maps and its location technology are prohibited in your country (determined by the IP address of your computer).
       - **GPS**
       - **Other Location Technologies**
       - **Absolute Wi-Fi Positioning**
       - **IP Georesolution**
   - For more information about each location technology, see "Types of Location Technologies" on page 163.
• 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:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pan</td>
<td>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.</td>
</tr>
<tr>
<td>Zoom</td>
<td>Use the Zoom tool to zoom in or out of specific areas of the map.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• To zoom out, click ™ repeatedly, or move the slider towards the button. You can zoom out by moving your mouse scroll wheel.</td>
</tr>
<tr>
<td>Map</td>
<td>Satellite picker</td>
</tr>
<tr>
<td></td>
<td>• To show a street map, click <strong>Map</strong>. This is the default option.</td>
</tr>
<tr>
<td></td>
<td>• To show a street map with terrain and vegetation information, click <strong>Map</strong> and select <strong>Terrain</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To show a map of satellite images click <strong>Satellite</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To show a map of satellite images with place names, click <strong>Satellite</strong> and select <strong>Labels</strong>.</td>
</tr>
<tr>
<td>Go to Address</td>
<td>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 <strong>Enter</strong>. For greater accuracy provide a street address as well as city and state names.</td>
</tr>
<tr>
<td>Find Boundaries and Markers</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 ☑ > Classic Reports > Lease and Inventory Management > 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 leased goods.
     - **Lease Vendor**: the provider of leased 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 80.
   - **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 ☐ > Classic Reports > Lease and Inventory Management > 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 80.
- 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:

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 ☰.
2. On the Find Devices page, click Classic Reports > 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:

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 92.
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 **Department** field, open the list and select the appropriate department.
   - To filter your results by specific device, in the **Device** 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 92."

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 enables Absolute administrators to download a CSV (Comma Separated Value) or XML (eXtensible Markup Language) file that identifies all users that are added or modified. The User Audit Report does not show data on-screen.

To generate a User Audit Report:

2. On the User Audit 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 92.

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 configured to do so, you receive an e-mail notification.

The User Audit Report file includes the following fields:

- Changed By User Id: the Username of the person who made the change.
- Changed By User First/Last Name: the name of the person who made the change.
- Type: the nature of the change. Possible values are Insert (new user created), Edit, Delete, or Reactivate.
- Date/Time Of Change: the date and time when the change was made.
- New User Id: the new or changed username or login ID.
- New Email: the new or changed e-mail address associated with the user.
- New User Type: the modified value of the user access rights such as ADMIN or POWER.
- New First/Last Name: the new or changed first and last name associated with this user.
- New Computer Group: the modified value of the device group.
- Old User Id: the old username or login ID associated with the user.
- Old Email: the old e-mail addresses associated with this user.
- Old User Type: the access rights associated with the old user such as ADMIN or POWER.
- Old First/Last Name: the first and last name associated with the old user account.
- Old Computer Group: the device group to which the old user account belongs.
User Event Report

The User Event Report enables Administrators to view a log of users who were suspended from the Absolute console or changed their password. The system records the event, the date and time of the occurrence, as well as the username and name of the individual.

The following types of user events are logged:

<table>
<thead>
<tr>
<th>User Reactivated From Temporary Lockout State</th>
<th>User Logged In/ Password Validated</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Suspended Permanently Due To Failed Logins</td>
<td>User Login Failed/Password Validation Failed</td>
</tr>
<tr>
<td>User Suspended Temporarily Due To Failed Logins</td>
<td>Password Changed</td>
</tr>
<tr>
<td>User Suspended Permanently Due To Inactivity</td>
<td>Password Reset</td>
</tr>
<tr>
<td>User Suspended Manually Permanently</td>
<td>Password Question Changed</td>
</tr>
<tr>
<td>User Suspended Manually Until Date</td>
<td>User Logged Out</td>
</tr>
<tr>
<td>User Manually Unlocked</td>
<td>Login Rejected from Unauthorized IP Address</td>
</tr>
<tr>
<td>Absolute Customer Service Login</td>
<td>Absolute Customer Service Logout</td>
</tr>
</tbody>
</table>

To generate a User Event Report:

1. On the Account Management page, click **User Event Report**.
2. On the User Event Report at the **Search Criteria** area, filter the events you want returned as follows:
   a) In the **Username contains** field, enter all or part of the Username associated with the device.
   b) In the **and the Event Detail contains** field, enter a **user event type**.
   c) At the **and the 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 results in a larger report, which takes longer to generate.
      - In the **between** field, click the option and enter the dates (mm/dd/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**, which refreshes the **results** grid to show the following user event details based on your filtering choices.
   - **For Username**: the Username associated with the user event
   - **Date and Time**: the date and time the user event occurred
   - **Event Details**: the **user event type** that was logged
   - **Changed by Username**: the Username of the Administrator who changed a password

**NOTE** When the event is triggered due to inactivity or failed login attempts, the column shows **System**.

- **Changed by First Name**: the first name of the Administrator who changed the password
- **Changed by Last Name**: the last name of the Administrator who changed the password
• **Public IP Address**: The public IP address of the device used to log in to the Absolute console

## 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 and Device Freeze requests:

- Device Freeze Requested
- Device Freeze Request Cancelled
- Device Freeze Details Removed
- Scheduled Freeze Pending
- Device Freeze Scheduled
- Unfreeze Requested
- Data Delete Requested
- Data Delete Request Cancelled
- Data Delete Log File Downloaded
- Data Delete Details Removed
- Unfreeze Request Cancelled

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 "Creating a Security Action Alert" on page 22.

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

- **Freeze Message**: a link to the Freeze message associated with a Device Freeze request, if applicable
  Click **View Message** to view the message text.

- **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 214.

- **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 🔄 > **My Content** > **My Reports**.
2. 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 ⬤ > My Content > My Filters.
2. 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 ⬤ > My Content > My Filters.
2. On the My Filters page, click the appropriate Filter name in the table.
3. 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.
4. If necessary, save the modified filters as a new saved filter. For more information, see "Saving Report Filters" on page 91.

NOTE The original saved report remains unchanged.
Chapter 5: Using Real-Time Technology

The optional Real-Time Technology (RTT) feature provides real-time communications with supported devices, which is enabled using a web application that sends and receives communication.

If your device is equipped with a supported mobile broadband adapter and meets the minimum system requirements, you can use the RTT feature to do the following:

- Manage the mobile broadband-enabled equipment in your asset base.
- Force an agent call from a device using SMS messages. If the managed device has an Internet connection, it contacts the Monitoring Center to receive instructions and take immediate action.

What is Real-Time Technology?

Real-Time Technology (RTT) lets you better track your mobile broadband-enabled devices. Additionally, RTT leverages mobile broadband and SMS messaging, also known as text messaging, to dramatically increase the performance of the Absolute Asset Tracking and Recovery features.

RTT encompasses the following features:

- **Mobile Broadband Adapter Tracking (MBAT):** MBAT permits Absolute customers to view a list of mobile broadband adapters and their attributes including equipment, subscriber, and network information in the Absolute console. MBAT is a unique feature letting customers track and manage devices using mobile broadband adapters and data plans in their asset base.

- **Monitoring Center-initiated Calling (MCIC):** MCIC lets customers remotely initiate an agent call using the Absolute console. Monitoring Center-initiated calling, under specific circumstances, enables a drastic reduction in the time required to initiate action on the targeted device. For example, MCIC can be used to initiate Data Delete and Freeze operations on the targeted device within minutes of submitting a request in the Absolute console. MCIC also enables near-real-time geolocation updates and tracking for the asset. In the absence of MCIC, each of these operations will only start at the next scheduled agent call. Under some circumstances, MCIC also permits communications with computers that do not have an active IP connection.

Minimum System Requirements

Currently, RTT and MCIC technology is not available for Mac devices.

To use the RTT feature, you need to meet the following minimum system requirements:

- **Operating System:** The targeted device must be running a supported version of one of the following operating systems:
  - Windows
  - Android

  For details, open the Absolute console help system and search for supported platforms for managed devices.

- **Agent:** The targeted device must have an active agent installed and must regularly call in to the Absolute Monitoring Center. For information about the most current agent versions, see "Downloading the Absolute Agent for Android Devices" on page 67.
• **Broadband Adapter**: The mobile broadband adapter installed on the targeted device must be supported for RTT. For a complete list of the supported mobile broadband adapters, see the Administrator's Guide for Absolute Agent.
• **Valid Data Subscription with SMS Support**: The targeted device must have a valid mobile data subscription that supports SMS messaging.

**IMPORTANT** Before using RTT, ensure that the targeted device has an active agent regularly calling in to the Absolute Monitoring Center. Additionally, you should be able to establish a data connection and send and receive SMS messages using the "watcher application" provided with your mobile broadband adapter. For more information, refer to the instructions provided with your mobile broadband adapter or the device.

**Working with RTT**

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

- powered on
- associated with an active SMS service
- in the network coverage area

For more information about searching for devices in your account with mobile broadband adapters, see "Mobile Broadband Adapter Report" on page 105.

For more information about the MCIC features such as SMS messages, see the following topics:

- "Viewing the Forced Call Log" on page 188
- "Initiating a Forced Call" on page 188

To take advantage of RTT functionality, your devices need to meet the following requirements:

- The RTT feature, including Mobile Broadband Adapter asset tracking and Monitoring Center Initiated Calling, is enabled for your account or the device. To activate these features, contact Absolute Technical Support.
- The device meets the system requirements. See "Minimum System Requirements" on page 185.
- The agent is installed and the device is regularly calling the Monitoring Center
- The device has a supported mobile broadband adapter with an active data plan that has Short Message Service (SMS) support. For more information, see the Administrator's Guide for Absolute Agent.

**IMPORTANT** Only Security Administrators can change RTT settings in the Absolute console. Administrators, Security Power Users, Power Users, and Guest Users can only view and filter the list of RTT devices. For more information,

This section includes the following tasks:

- Viewing Mobile Broadband Adapter Information
- Editing the Phone Number Override
- Viewing the Forced Call Log
- Initiating a Forced Call
Viewing Mobile Broadband Adapter Information

To view the mobile broadband adapter details for an RTT-enabled device:


2. On the Mobile Broadband Adapter Report page, use the filter to limit your search and click Show results.

3. In the results grid, click the Identifier link for the device that you want to view.

4. On the Device Summary page, you see the details for the selected device.
   
   This page opens with the contents of the Hardware Summary tab showing. If you are using the RTT feature, partway down the page you see the Mobile Broadband Adapters area.

5. Click the Details link for the appropriate device.
   
   The Mobile Broadband Adapter Details dialog opens, which provides the following details for the device:

   - **Time Attributes Collected**: the date and time when information about the mobile broadband adapter installed on the device was collected.
   - **Manufacturer**: the name of the manufacturer of the mobile broadband adapter.
   - **Model**: the model number, if available, of the mobile broadband adapter.
   - **Equipment ID**: the identification number unique to the mobile broadband adapter; usually available on the bottom of the notebook or on the removable mobile broadband adapter. For EVDO adapters, the Electronic Serial Number (ESN) and/or the Mobile Equipment ID (MEID) may be reported. For UMTS networks, the International Mobile Equipment Identifier (IMEI) is reported.
   - **Subscriber ID**: the unique number associated with the subscriber; stored in the adapter, the Subscriber Identity Module (SIM) card, or equivalent.
   - **Network**: the mobile service provider associated with the mobile device.
   - **Service Status**: the last reported status of the availability of the associated network.
   - **Detected Phone Number**: the phone number associated with the mobile broadband adapter, as reported by the device.
   - **Phone Number Override**: the alternative or override phone number associated with the mobile device or broadband adapter. If the agent does not detect the phone number automatically, the device automatically sends an SMS to the Monitoring Center. The reply-to address from the SMS becomes the value for the Phone Number Override field. You can edit the phone number using the Edit Phone Number Override dialog. See "Editing the Phone Number Override" on page 187.

6. On the Mobile Broadband Adapter Details dialog, click Close to return to the Device Summary page.

Editing the Phone Number Override

The Edit Phone Number Override dialog allows you to enter a new phone number to use instead of the detected phone number when sending SMS text messages to the adapter. SMS text messages are used to contact devices as part of the MCIC feature.
To set an override phone number:

1. Open the Device Summary page for the device on which you want to attempt a forced call by completing step 1 through step 5 of the task, "Viewing Mobile Broadband Adapter Information" on page 187.
   
   For more information about the Device Summary page, see "Editing Asset Information" on page 80.

2. On the Hardware Summary tab in the Mobile Broadband Adapters area, for the appropriate adapter, click the Edit link under the Phone Number Override column.

3. On the Edit Phone Number Override dialog, type the new phone number including country and area codes in the Phone Number Override field. The phone number should follow the format: +16045556789, without spaces, parentheses, periods, or hyphens.

4. Click Set Override.
   
   The Edit Phone Number dialog closes and the Device Summary page refreshes to show the new phone number override value in the Phone Number Override column.

Viewing the Forced Call Log

On the Device Summary page, the Forced Call Log tab shows detailed information about events associated with all forced calls attempted on a device. The Forced Call Log shows information about SMS messages sent to and received from the device. The following information is available:

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

Initiating a Forced Call

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

**IMPORTANT** The following task requires that you log in to the Absolute console as an Administrator.

To force a call from a device:


2. On the Mobile Broadband Adapter Report page, use the filter to limit your search and click Show results.

3. In the results grid, click the Identifier link to open the Device Summary page for the device.

4. Follow the appropriate steps below to force a call to the device:
   - For Windows devices:
i) On the **Hardware Summary** tab in the **Mobile Broadband Adapters** area, in the row for the appropriate adapter, click **Attempt forced call**.

ii) On the Attempt Forced Call dialog, click **Attempt call**.

iii) The Forced Call Status dialog opens, where you see the success or failure of your request.
   - The Monitoring Center sends an SMS to the adapter, requesting an immediate call from the agent. If the device is on and the mobile broadband adapter is within network coverage, the agent initiates a call to the Monitoring Center.
   - The message is queued if the mobile broadband adapter cannot receive it.
   - If the agent does not have an Internet connection, the agent will contact as soon as it is back online.

iv) Click **Close**, which returns you to the Device Summary page for the device.

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

You can view the status of the forced call request on the **Forced Call Log** tab. For more information, see "**Viewing the Forced Call Log** on page 188.

You can also force calls using MCIC as part of Data Delete and Device Freeze requests.
Chapter 6: Using Real-Time Technology over IP

Real-Time Technology over IP (RTT-IP) reduces the time it takes for an account Administrator to invoke remote operations such as Data Delete on managed Windows and Mac devices. Using RTT-IP can significantly reduce the window of opportunity for data loss or for unauthorized access to systems.

The RTT-IP feature is not turned on by default, and an Administrator must manually enable it for your account.

This chapter provides information on the following topics:

- Minimum System Requirements
- Understanding How RTT-IP Works
- Accelerating Operations With RTT-IP
- Enabling RTT-IP
- Requesting a full agent call using RTT-IP
- Editing the RTT-IP Ping Period for a Device
- Viewing RTT-IP Status for All Devices
- Disabling RTT-IP

**IMPORTANT** To perform the tasks in this chapter, you need to log in to the Absolute console as a Security Administrator.

Minimum System Requirements

RTT-IP works on devices with Internet access that are running a supported version of the Windows or Mac operating system.

Understanding How RTT-IP Works

Normally, when you request a security operation, such as Data Delete or Device Freeze, on your devices, you need to wait until the next scheduled agent call for the operation to occur. By default, devices are scheduled to make an agent call once every 24.5 hours. Therefore, you could wait up to this length of time for the security operation to take effect on your device.

RTT-IP reduces this wait time in time-critical situations. The Ping Period, which is independent of the agent call period, is configurable. The RTT-IP feature is not turned on by default, and an Administrator must manually enable it for your account. To accommodate a shorter time delay, the Windows or Mac agent on RTT-IP enabled devices makes a lightweight ping, sending 24 bytes of data, not including HTTP header bandwidth. This ping is sent to an RTT-IP server at a specified interval using a separate channel than regular agent calls. Enabling RTT-IP will increase the load on your network infrastructure including any DNS servers, firewalls, and proxies. You need to coordinate with your network administrator before enabling or modifying your RTT-IP settings. In particular, enabling RTT-IP for a large number of devices with a high Ping Period may have an adverse impact on your network. For more information about the additional network infrastructure load, see the Technical Note *TN130222 – RTT Over IP Network Infrastructure Load* available on the Documentation page.
When you enable the RTT-IP feature for your account, you can select the Ping Period that is appropriate for your organization. In the Absolute console, the fastest Ping Period that you can set for devices in your account is one ping every 15 minutes. If you want to purchase faster Ping Periods of 1 to 15 minutes, contact Absolute Technical Support.

The RTT-IP feature is implemented in such a way that when you request a security operation, the agent is instructed automatically on the device’s next ping to make a full agent call and, thereby, initiate the specific security operation you requested.

You can force a call when you want to test the feature and validate that it is working on a device.

Prerequisites of RTT-IP

Customers who want to use RTT-IP need to ensure their devices meet the minimum system requirements. For more information, see "Minimum System Requirements" on page 190.

Accelerating Operations With RTT-IP

For accounts that are set up for RTT-IP, the RTT-IP feature interacts with security operations and, therefore, requires users who are familiar with Absolute, preferably network administrators or IT staff members in your organization.

The RTT-IP feature is implemented in such a way that when you request a security operation, the agent is instructed automatically on the device’s next ping to make a full agent call and, thereby, initiate the specific security operation you requested.

This capability works with the following security operations:

- Data Delete requests
- Freeze and Remove Freeze requests
- Remote File List requests
- Remote File Retrieval requests
- Investigation Report submissions

Viewing RTT-IP Status for a Device

On a device’s Device Summary page, the RTT-IP area shows the following information:

- RTT-IP status of the device: If RTT-IP is turned on, the check box is selected.
- The Ping Period for the device: When you turn on the RTT-IP feature for your account, you have to select a default Ping Period. Unless you have specified a different Ping Period for this device, the value in this field matches the account defaults.
- The Last Ping Time for the device: Indicates the last time the device pinged the RTT-IP server.

For more information about a device’s Device Summary page, see "Editing Asset Information" on page 80.

Your organization may choose to group all devices that are enabled for RTT-IP together, in which case you can follow the instructions provided in the task, "Enabling RTT-IP for All Devices in Your Account" on page 192.
Enabling RTT-IP

There are several ways to enable RTT-IP for your organization’s devices:

- Enabling RTT-IP for All Devices in Your Account
- Enabling RTT-IP for an Individual Device

Enabling RTT-IP for All Devices in Your Account

When you use the Classic Account Settings page to enable RTT-IP, you set a default value that enables this feature for all devices in your account.

To enable RTT-IP for all devices in your account:

1. On the navigation bar click  > Classic Account Settings.
2. Scroll down to the RTT-IP Setting area, open the Current Ping Period list, and select the appropriate value.

**IMPORTANT** Enabling RTT-IP increases the load on your network infrastructure including any DNS servers, firewalls and proxies. Please coordinate with your network administrator before enabling or changing your RTT-IP settings. In particular, enabling RTT-IP for a large number of devices with a high Ping Period may have an adverse impact on your network.

Initially, set this interval for a faster period or whatever is appropriate for your organization. The fastest Ping Period you can select is one ping every 15 minutes. If you want to purchase faster Ping Periods of 1 to 15 minutes, contact Absolute Technical Support.

3. Click Save changes.
4. On the Apply changes to dialog, ensure that the All devices checkbox is selected and click Continue.

For all existing devices in the account, RTT-IP is enabled on the next scheduled agent call from the device. When new devices are activated on the account, RTT-IP is enabled and the Ping Period is applied.

Enabling RTT-IP for an Individual Device

You can enable RTT-IP for individual devices in your account using the Device Summary page.

To enable RTT-IP for an individual device:

2. On the Asset Report page, do the following:
   a) In the Search Criteria area, at the Group is field open the list and select All Devices.
   b) Click Show results and in the results grid locate the device on which you want to enable RTT-IP.
   c) Click the device’s Identifier link.
3. On the Device Summary, select the Turn on the RTT-IP feature for this Identifier checkbox to enable RTT-IP for this device.
4. Set the RTT-IP Ping Period for this device.
**IMPORTANT** Enabling RTT-IP will increase the load on your network infrastructure including any DNS servers, firewalls and proxies. Please coordinate with your network administrator before enabling or modifying your RTT-IP settings. In particular, enabling RTT-IP for a large number of devices with a high Ping Period may have an adverse impact on your network.

Initially, set this interval for a faster period or whatever is appropriate for your organization. The fastest Ping Period you can select is one ping every 15 minutes. If you want to purchase faster Ping Periods of 1 to 15 minutes, contact Absolute Technical Support.

5. Click **Save changes**.

**Requesting a full agent call using RTT-IP**

To perform a full scan of a device to collect up-to-date device information, you can request that the device make a full agent call to the Monitoring Center during its next RTT-IP ping period.

To request a full agent call using RTT-IP:

1. On the navigation bar click ☰️ > **Custom Reports > Hardware Assets > Asset Report**.
2. Open the Asset Report and in the **Search Criteria** area, at the **Group is** field, open the list and select **RTT-IP**.
3. Click **Show results**. In the **results** grid you see all devices in that group.
4. Click the **Identifier** link for the device you want to have call in.
5. On the Device Summary page at the **RTT-IP** area, click **Request Full Inventory Call**.
6. On the Forced Call Status confirmation dialog, you are notified that your request is submitted. If the device is currently online, it will call during the next ping period. If it is offline, a call is initiated when the device comes online.

    On the dialog click **Close**.

7. If you want to determine when the next ping is scheduled to occur:
   a) In the RTT-IP area, make note of the setting for **Ping Period**.
   b) Open the Asset Report again and check the device’s **Last Call** column to see when the last call was made.

**Editing the RTT-IP Ping Period**

There are two ways to edit the RTT-IP Ping Period for your organization’s devices:

- **Editing the RTT-IP Ping Period for All Devices in Your Account**
- **Editing the RTT-IP Ping Period for a Device**

**Editing the RTT-IP Ping Period for All Devices in Your Account**

If the current Ping Period set at the account level is not satisfactory you can change it. The new Ping Period can be applied to all devices in your account, or select groups of devices.

To edit the RTT-IP Ping Period at the account level:

1. On the navigation bar click ☰️ > **Classic Account Settings**.
2. Scroll down to the RTT-IP Setting area, open the Current Ping Period list, and select the appropriate value.

3. Click Save changes.

4. On the Apply changes to dialog, do one of the following:
   - To apply the Ping Period to all existing and newly activated devices for the account, ensure that the All devices checkbox is selected.
   - To apply the changes to specific devices, clear the All devices checkbox and select one or more of the following options:
     - Make the Ping Period for new RTT-IP capable devices: when new devices are activated for the account, RTT-IP is enabled and the selected Ping Period is applied.
     - Turn on the RTT-IP feature for all devices where RTT-IP is turned off: enables RTT-IP and applies the selected Ping Period to existing devices.
     - Change the devices with a RTT-IP Ping Period of <current value> to <new value>: applies the selected Ping Period to devices that are RTT-IP enabled and their current Ping Period matches the <current value>.
     - Change the devices that do not have a RTT-IP Ping Period of <current value> to <new value>: applies the selected Ping Period to devices that are RTT-IP enabled and their current Ping Period does not match the <current value>.

5. Click Continue.

   The new Ping Period is applied when the agent on each device makes the next scheduled agent call to the Monitoring Center.

Editing the RTT-IP Ping Period for a Device

The default setting for the Ping Period for devices is 30 minutes. You can change that period based on your organization’s requirements.

To edit the Ping Period for an individual device:


2. On the Asset Report page, do the following:
   a) In the Search Criteria area, at the Group is field open the list and select All Devices.
   b) Click Show results and in the results grid locate the device on which you want to enable RTT-IP.
   c) Click the device’s Identifier link.

3. On the Device Summary page, in the Change RTT-IP Ping Period list, select the appropriate value.

4. Click Save changes. The device receives the new Ping Period when the agent on the device makes the next scheduled agent call to the Monitoring Center. Agent calls to the Monitoring Center occur once every 24.5 hours.

Viewing RTT-IP Status for All Devices

If RTT-IP is enabled for your account, you can view the RTT-IP status of all devices in a results grid.
To view the RTT-IP status for all devices:

1. On the navigation bar click Classic Account Settings.
2. Scroll to the RTT-IP Setting area and under RTT-IP Status click the View link.

**NOTE** The View link is available only if a Ping Period has been set.

In the Devices that have the RTT-IP feature turned on window, the following information is shown for each device:

- **Identifier**: the identifier associated with the device. Click this link to open the Device Summary page for the device.
- **Username**: the unique name detected by the agent that identifies the person who is associated with this device.
- **Operating System**: the software that controls the running of computer programs and services on the device.
- **Agent Version**: the version number of the agent installed on the device.
- **Ping Period**: the time period between pings by the device to the RTT-IP server.
- **Last Ping Time (UTC)**: the last time the device pinged the RTT-IP server.

3. To navigate, filter, and sort the results, do the following:
   - To change the number of records shown on each page of the results grid, click the Per Page field and select an option from the list. The following options are available:
     - 10
     - 20
     - 50
     - 100
     - 500
     - 1000
   - To go to another page in the results, click the applicable page link (<First, <Prev, <page #>, Next>, or Last>).
   - To filter the results, enter a value for Identifier, Username, Operating System, Agent Version, or Ping Period in the field, and click Filter.

**NOTE** If you enter only a portion of the value, the filtered results include all records that satisfy the filter criteria. For example, if you type "win" to filter by the Windows operating system, all results that contain "win", such as Username "Winston", are included in the filtered results.

- By default, the results are sorted by Identifier. To sort the results by another criterion, click the applicable column heading.

4. When you are finished reviewing the information, close the window.

**Disabling RTT-IP**

There are two ways to disable RTT-IP for your organization’s devices:

- **Disabling RTT-IP for All Devices in Your Account**
● **Disabling RTT-IP for an Individual Device**

**Disabling RTT-IP for All Devices in Your Account**

When you use the Classic Account Settings page to edit RTT-IP settings, you set a default value for this feature for all devices in your account.

To disable RTT-IP for all devices in your account:

1. On the navigation bar click ✎ > **Classic Account Settings**.
2. Scroll down to the **RTT-IP Setting** area, open the **Current Ping Period** list, scroll down to the end of the list, and click **Turn off RTT-IP**.
3. Click **Save changes**.

**Disabling RTT-IP for an Individual Device**

You can disable RTT-IP for individual devices in your account using the Device Summary page.

To disable RTT-IP for an individual Device:

1. On the navigation bar click ✎ > **Classic Reports** > **Hardware Assets** > **Asset Report**.
2. On the Asset Report page, do the following:
   a) In the **Search Criteria** area, at the **Group is** field open the list and click **All Devices**.
   b) Click **Show results** and in the **results** grid locate the device on which you want to disable RTT-IP.
   c) Click the device’s **Identifier** link.
3. On the Device Summary page, clear the **Turn on the RTT-IP feature for this Identifier** checkbox to disable RTT-IP for this device.
4. Click **Save changes**.
Chapter 7: Securing Your Data and Devices

The following security operations are available, which enable Security Administrators and Security Power Users to ensure that managed devices, and the data they contain, are not compromised in cases of device loss or theft:

- Data Delete (see "Using Data Delete" on page 209.)
- Device Freeze (see "Using Device Freeze" on page 234.)
- Intel® Anti-theft Technology (AT) (see "Concluding Intel Anti-Theft Technology Support" on page 206.)

**NOTE** Only Security Administrators can perform Intel Anti-theft Technology security operations.

- File List (see "Using File List" on page 278.)
- Remote File Retrieval (see "Using Remote File Retrieval" on page 272.)

To access these security operations, authorized Security Administrators and Security Power Users are required to use an emailed authorization code or a code from an RSA SecurID® token. Your organization indicates which authentication method you want to use when you sign the Security Administration Authorization Agreement.

**NOTE** Security Power Users can perform security operations on only those devices that are in the Device Group to which the Security Power User is assigned.

This chapter includes information on the following tasks:

- Before You Begin
- Security Administration Authorization Agreement
- Security Authentication Methods
- Managing Custom Action Fields

**Before You Begin**

Due to the potentially destructive nature of some security features, the following security checks are implemented to ensure that the security operations are initiated only by authorized individuals and that the security operations only run on correctly targeted devices.

Make sure that you have met the following prerequisites:

- Absolute must have a signed authorization agreement on file for your company. For more information, see "Security Administration Authorization Agreement" on page 198. This agreement is a prerequisite to your organization getting an account. Your account indicates the security operations that are available to your organization.
- To run security operations, such as Data Delete, you need to ensure that all of the following prerequisites are in place:
  - A Username and associated Password that provide security authorization privileges. For more information,
  - A unique authorization code generated from your RSA SecurID® token or received in an e-mail message, whichever authentication method is applicable.
Each security operation must be substantiated using an authorization code available only to the Security Administrator or Security Power User who is requesting the security service. For more information, see "Security Authentication Methods" on page 201.

- The devices that are targeted with the security service must have an activated agent with a unique Identifier. For more information, see "Downloading the Absolute Agent for Android Devices" on page 67.

**NOTE** Any Absolute employee, irrespective of their access rights, is unable to start a security operation for devices in your account.

### Security Administration Authorization Agreement

Before you can use the security operations available in the Absolute console, Absolute must have a signed authorization agreement on file for your company. The authorization agreement identifies the personnel in your company who are authorized to perform security operations and specifies the type of authentication method used by your company.

This section provides the following tasks:

- Downloading and Submitting the Authorization Agreement
- Disabling Security Access for All Authorized Security Users
- Removing Security Access for One Specific Security Administrator

### Downloading and Submitting the Authorization Agreement

To download a blank copy of the authorization agreement and submit it when it is completed:

1. On the navigation bar, click ☰ to open the Help and Support page.
2. Click **Support**.
3. Scroll down to the **Service Request Forms** area and click the **Security Administration Authorization Agreement** link.
   
4. Fill in the forms to complete the document, print it, sign it, scan it, and attach it to a new support case.
5. To attach the document to a new Support case, do the following:
   a) Click the **Support** tab to open the Support features on the sidebar.
   b) Under the Technical Support heading, click the **Submit a Support Case** link.
   c) In the **Severity** field, open the list and select one of the following options:
      - **1 – Critical** indicates that critical business processes are severely impacted over a large number of users.
      - **2 – Urgent** indicates that business is impacted over a large number of users, however critical business processes are not affected.
      - **3 – Standard** indicates that business is moderately impacted, efficiency is hampered, however users can still perform their work.
      - **4 – Low** indicates that business is not impacted significantly, although the issue is annoying. This level of severity may also indicate a request for an enhancement.
d) In the Classification field, open the list and click Security Admin & Geolocation Authorization Form.
e) In the Problem Title field, enter a name; for example, Security Administrator Authorization.
f) In the Problem Description field, enter a description; for example, type: Submitting our Security Administration Authorization Agreement.
g) To add an attachment to your support case, click Add Attachment and browse to the location of the scanned version of your completed and signed form, and click Open to attach it.
h) Click Submit.
The form is sent to Absolute Technical Support, where the particulars for your account are processed. When this procedure is complete, you receive a confirmation e-mail message.

IMPORTANT All of the tasks that follow require that you log in to the Absolute console as a Security Administrator.

Disabling Security Access for All Authorized Security Users
If you believe that the integrity of your security operations was compromised for any reason, you can disable the security access authorization, which suspends security access for all authorized personnel.

WARNING! Exercise caution. Disabling security access authorization suspends all Security Administrators and Security Power Users, preventing those users from requesting new security operations. All pending security operation requests are processed as usual.

To enable access to features that require security authorization again, you must contact Absolute Technical Support.

To disable all Security Administrator’s security access to the Absolute console:
1. On the navigation bar click the > Disable Pre-Authorization.

IMPORTANT Careful: There is no confirmation dialog for this action.

2. On the Disable Preauthorization page click Disable.

IMPORTANT To enable Security Authorization again, you must contact Absolute Technical Support. To do so, click the Support link and follow the on-screen instructions.

Removing Security Access for One Specific Security Administrator

NOTE The instructions for this task apply to both Security Administrators and Security Power Users. For the purpose of explanation only, the information in this section refers to the Security Administrator only.

Depending on your situation, there are two ways to remove security access for a specific Security Administrator, both of which are described in this section as follows:

● Removing Security Access by Submitting an Absolute Technical Support Case
Removing Security Access by Suspending the User Account

Removing Security Access by Submitting an Absolute Technical Support Case

If a particular Security Administrator leaves your organization, or moves to another role within it, you can instruct Absolute Technical Support by submitting a support case or you can suspend the user account for that user while you notify Technical Support of the change and create security authorization for a new security administrator.

To remove security access for an existing Security Administrator by submitting a Technical Support case:

1. On the navigation bar click ☰ > Support and on the sidebar under the Technical Support heading click the Submit a Support Case link.
2. On the Contact Customer Support page do the following:
   a) A Severity of 3 - Standard is appropriate for this type of request.
   b) In the Classification field, open the list and select Account Administration.
   c) In the Subject field, provide appropriate text for this case; for example, Removing <username>'s Security Access.
   d) In the Description field, clearly instruct Technical Support as to what you want; for example, Remove security access for <username> as this person's user role has changed. We are submitting a new Security Administration Authorization Agreement to indicate the new Security Administrator.
   e) Click Submit.
      On the confirmation page, you see your support case number. You may want to make a note of it as you need it if you contact Technical Support. Click OK, close this window, and open the Absolute console window.
      When Technical Support reviews your support case and takes action, this user's security access is revoked and security operations are no longer within this users capability.
3. On the navigation bar click ☰ > Support and under the Service Request Forms area, click the Security Administration Authorization Agreement link.
   Follow the instructions on this form to indicate who your Security Administrators are (include both the new and existing users), complete this form in its entirety, including having the Signing Officers sign off, and submit this agreement to Absolute Technical Support.

Removing Security Access by Suspending the User Account

Suspending the user's account prevents that user from logging any new requests for security operations, but it does not impact any pending requests. For example, if Security Administrator A has an open Data Delete request and has their user account suspended, the Data Delete request runs as specified on the next agent call. For those organizations that want to limit this user's access immediately, use the following instructions.

To remove security access for an existing Security Administrator by suspending this user's rights:

1. Click ☰ > User Management > Users to see the list of all users.
2. Find the security administrator you want to suspend in the list and click the corresponding link to open the Edit User page for this person.

3. Click User Status and Suspension Settings and under the User Status area, click the Temporarily suspended until option, click the calendar and select a date at least four days in the future.

**NOTE** During the time interval you select, this particular user cannot log in to the Absolute console.

4. Click Save.

5. Complete the task, Downloading and Submitting the Authorization Agreement

   Follow the instructions on the form to indicate who your Security Administrators are (include both the new and existing users), complete this form in its entirety, including having the Signing Officers sign off, and submit this agreement to Absolute Technical Support.

   **NOTE** It could take some time for this form to take effect. If this user needs access to the Absolute console immediately, contact Absolute Technical Support for assistance.

6. Depending on your specific situation, do one of the following:
   
   - If this user is leaving your organization, follow the instructions in the task,
   - If this user is staying with your organization, follow the instructions in the task,

Security Authentication Methods

Absolute uses either RSA SecurID® tokens or unique e-mailed security authorization codes to substantiate requested security operations. If you purchased Absolute directly from Absolute Software Corporation, you select your Security Authentication method when you complete your Security Administration Authorization Agreement. If you purchased Absolute from a reseller, you can specify your authentication method when you register your account at [https://registration.absolute.com](https://registration.absolute.com).

This section provides information on the following topics:

- Using RSA SecurID Tokens for Security Services
- Using E-mailed Authorization Codes for Security Services
- Changing Your Security Authentication Method

Using RSA SecurID Tokens for Security Services

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

If you are using RSA SecurID tokens as the authentication method, the Security Administrator or Security Power User enters the code from his or her RSA SecurID token to validate each security operation.

RSA is the security division of EMC2®. However, all RSA SecurID tokens must be purchased directly from Absolute.
When Absolute receives your signed authorization agreement, we send the RSA SecurID® tokens to authorized Security Administrators and Security Power Users by mail.

The following information and tasks are provided in this section:

- **Using RSA SecurID Token Codes**
- **Transferring RSA SecurID Tokens**

**Using RSA SecurID Token Codes**

Accounts using RSA SecurID tokens do not need to request a security authorization code. The token constantly generates security authorization codes. When the Security Administrator or Security Power User requests a security operation, the code shown on the token is entered into the appropriate field on the required page, based on the requested operation.

A SecurID Token Code is required to access security operations for those organizations that select the RSA SecurID tokens method of security authentication. When you request a security operation, for example, a Data Delete or Remote File Retrieval, the Provide Authentication page opens. The Security Administrator or Security Power User then enters his or her Absolute console password and the SecurID Token Code that currently shows on the RSA SecurID token.

**Transferring RSA SecurID Tokens**

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

To transfer an RSA SecurID Token:

1. On the navigation bar click the link, which opens the Help and Support page with the Documentation tab's content showing.
2. Scroll down to the Service Request Forms area and click the RSA SecurID Token Transfer Form link to open the token transfer agreement in a new window as a PDF file.
3. Print the agreement.
4. Fill in the form and return it by courier or fax to Absolute, using the mailing address or fax number provided on the agreement.

**Using E-mailed Authorization Codes for Security Services**

For organizations that select E-mailed Authorization Codes when they sign the Absolute Security Administration Authorization Agreement, a Security Administrator or Security Power User must request a unique authorization code in the Absolute console before using security services.

A security authorization code is a globally unique identifier (GUID) that is required to substantiate each security operation. An e-mail message that includes the security authorization code is sent to the e-mail account on file for this user.

The following conditions apply to the security authorization code:

- It is valid for two (2) hours from the time it is issued to the appropriate recipient.
- Only the user who requests the security authorization code can use it.
- The security authorization code can be used only once.
This section provides the following information for those accounts that opted to have security authorization codes sent to specific Security Administrator and Security Power User e-mail addresses:

- **Requesting a Security Authorization Code**
- **Changing E-mail Addresses for Authorized Security Personnel**

**Requesting a Security Authorization Code**

If your company uses e-mailed authorization codes to substantiate security operations, you must request a security authorization code before initiating any action in the Data and Device Security section. When you receive your security authorization code, you use it to validate the requested security service.

**IMPORTANT** To perform the following task you need to log in to the Absolute console as a Security Administrator or Security Power User.

To request a security authorization code be provided in an e-mail message:

1. On the quick access toolbar, click ![Authorization Code](image) and click **Authorization Code**.
   A confirmation message indicates that an authorization code is generated and the security authorization code is sent in an e-mail message to the e-mail account on file for the Security Administrator or Security Power User who requested it.
3. From the e-mail message, copy the security authentication code to use where appropriate.

**Changing E-mail Addresses for Authorized Security Personnel**

Security Administrators and Security Power Users can change their e-mail addresses. When doing so, it is important to know that those users are temporarily suspended from performing security operations for the next 72 hours. For more information,

**Changing Your Security Authentication Method**

You cannot change your authentication method using the Absolute console. To change your security authentication method, contact Absolute Technical Support at www.absolute.com/support.

**Managing Custom Action Fields**

Security Administrators can create up to five custom fields to show on the Request Data Delete page and another five fields to show on the Request Device Freeze page.

Depending on the needs of your organization, users can use these fields to record additional information about a security operation request. For example, you can create a **Reason** field to show on the Device Freeze Request page to allow users to explain why the Device Freeze request is required.

All information entered in the custom fields is retained with the request. For Data Delete requests, you can view this information on the Data Delete Summary Report and the Data Delete Details page. For Device Freeze requests, it shows on the Device Freeze Summary Report and the Device Freeze Details page.

This section describes the following tasks:

- **Creating Custom Action Fields**
Creating Custom Action Fields

To create a new custom field to show on the Request Data Delete page or the Request Device Freeze page:

1. On the navigation bar, click ✪ > Custom Action Fields.
2. On the Manage Custom Action Fields page, do one of the following:
   a) To create a custom field for the Request Data Delete page, click Create Custom Action Field for Data Delete.
   b) To create a custom field for the Request Device Freeze page, click Create Custom Action Field for Device Freeze.

   NOTE  You can create up to five fields for each type of request. If the Create button is inaccessible, you need to delete a field before you can add a new one.

3. On the Create Custom Action Field page, in the Field Label field, enter a name for the new field.
4. Select one of the following Field Type options:
   - Text (50 character maximum): the field accepts plain text up to 50 characters in length.
   - Date: the field accepts date values in the form m/d/yyyy. A Calendar picker is also available for this field.
   - Drop-down list: the field contains a list of options.

   If you selected the Drop-down list option, enter the list options in the Drop-down List Values field. Use commas to separate the list options.

   NOTE  You don't need to type the double quotes. When you click outside the text field, the double quotes are added to each option.

5. If the user is not required to complete the custom field, in the Field Option area clear the Required field checkbox.
6. Click Save.

   The new field shows in the Custom Action Fields section of the applicable Request page.

Editing Custom Action Fields

To edit a Custom Action Field:

1. On the navigation bar, click ✪ > Custom Action Fields.
2. On the Manage Custom Action Fields page, click the Edit link that is associated with the custom field you want to change.
3. On the Edit Custom Action Field page, in the Field Label field, change the name as appropriate.
NOTE   The Field Type options are not available for edit. If you want to change this information, you need to Delete the custom field and create a new one with the appropriate information. For more information, see "Deleting Custom Action Fields" on page 205.

4. If this field is a Drop-down list, in the Drop-down List Values field add or remove list options as appropriate. Use commas to separate the list options.

NOTE   You don’t need to type the double quotes. When you click outside the text field, the double quotes are added to each option.

5. Select or clear the Required field checkbox as appropriate.
6. Click Save changes.

Deleting Custom Action Fields
You can delete a Custom Action Field that is no longer required.

IMPORTANT   When you delete a custom field, all of the information that users have entered in that field, in all existing requests, is also deleted.

To delete a Custom Action Field:
1. On the navigation bar, click > Custom Action Fields.
2. On the Manage Custom Action Fields page, click the Edit link that is associated with the custom field you want to delete.
3. On the Edit Custom Action Field page, click Delete.
4. On the confirmation dialog, click Continue.
   The Manage Custom Action Fields page refreshes and the field is deleted.
Chapter 8: Concluding Intel Anti-Theft Technology Support

With the termination of Intel® Anti-Theft Technology (Intel AT) in early 2015, Absolute has concluded its support of Intel AT. All Intel AT equipped devices should now be disenrolled from the service in the Absolute console.


You can continue to protect your managed Windows devices in the Absolute console as follows:
- Freeze devices. For more information, see *Freezing devices* in the online Help.
- Establish device lock options and timer period settings similar to what was available with Intel AT using a Conditional Freeze request. For more information, see *Freezing offline devices* in the online Help.

Troubleshooting Intel AT Disenrollment

If any of your Intel AT equipped devices are still active (Current State is set to Intel AT On), it is likely that these devices have not called the Monitoring Center for some time. To resolve this issue you may need to unlock the device using a server recovery token. In some cases, you may also need to install updated Intel AT drivers if the drivers are missing or out-of-date.

Intel AT equipped devices come pre-installed with Intel AT drivers, such as:
- Host Embedded Controller Interface (HECI) driver
- Active Management Technology (AMT) driver
- Management Engine Interface (MEI) driver

This section provides information on the following topics:
- *Viewing the Disenrollment Status of Devices*
- *Unlocking Devices Using a Server Recovery Token*

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

Viewing the Disenrollment Status of Devices

To view the status of your Intel AT equipped devices:

1. On the navigation bar, click > **Intel® Anti-Theft Technology** > **Manage Devices Equipped with Intel® Anti-Theft Technology**.

   The Intel® Anti-Theft Technology disenrollment status area shows the following information:

   - **Total Devices** enrolled in Intel AT.
   - **Intel AT Off Devices** indicates the number of devices that have been disenrolled from Intel AT. You don't need to do anything with these devices.
   - **Intel AT On Devices** indicates the number of devices that have Intel AT turned on.
2. If any devices still have Intel AT turned on, click the View link next to Intel AT On Devices. The results grid provides details for each device. Look at the Last Call column to see when each device last called in to the Monitoring Center.

3. If the Current State column for a device shows Locked, you may be able to unlock the device using a server recovery token. For more information, . After the device is unlocked, it is disenrolled from Intel AT on the next agent call.

4. If there are any Intel AT errors that are preventing the device from being disenrolled, a warning icon ! shows in the Current State column. Hover over the icon to view details about the error.
   - For the list of error code definitions, refer to the following InTelligence Knowledge Base article: KB-1076. If the error is related to missing or out-of-date Intel AT drivers, also refer to the following InTelligence Knowledge Base article: KB-1183.
   - If you require further assistance, contact Technical Support.

Unlocking Devices Using a Server Recovery Token

System Administrators can use a server recovery token to unlock a device that is locked using Intel AT. This section includes the following tasks:
- Generating a Server Recovery Token
- Using a Server Recovery Token to Unlock a Locked Device

Generating a Server Recovery Token

To generate a server recovery token for your locked device:

1. On the navigation bar, click ✿ > Intel® Anti-Theft Technology > Manage Devices Equipped with Intel® Anti-Theft Technology.

2. On the Manage Devices Equipped with Intel® Anti-Theft Technology page, search for the appropriate Intel AT locked device.

3. In the results grid, click in the Identifier column of the appropriate device.

4. On the menu, click Generate server recovery token.


NOTE The Platform Recovery ID is shown on the locked device.

6. Click Generate server recovery token.
   If your account uses authentication, the Provide Authentication page opens.
   a) Enter your Password.
   b) Enter your SecurID Token Code or Authorization Code.
   c) Click OK.
   The Generate Server Recovery Token page refreshes to show the server recovery token.

7. Record the code for the server recovery token.
Using a Server Recovery Token to Unlock a Locked Device

To unlock a locked device using a server recovery token:

1. Turn on the locked device.
2. On the Intel AT Recovery page, specify the Server Token option (depending on the device, you are instructed to type 2 or press F2).
3. Type the reactivation server recovery token using the number row on the keyboard (not the numeric keypad).
4. Press Enter to reboot your device.
   The device is disenrolled from Intel AT (Intel AT state set to Off) on the next agent call.

**IMPORTANT** If the device fails to disenroll, the Intel AT drivers on the device may be missing or out-of-date. For more information about installing new drivers, refer to the following InTelligence Knowledge Base article: KB-1183.

If you need further troubleshooting assistance, contact Absolute Technical Support.
Chapter 9: Using Data Delete

Data Delete lets authorized Security Administrators and Security Power Users delete some or all of the hard drive data on a remote device. Security Power Users can perform a Data Delete operation on only those devices that belong to the Device Group to which these users are assigned.

**NOTE** Depending on the product your organization purchased, Data Delete may not be available.

This chapter includes the following sections:

- Minimum System Requirements
- Deletion Algorithms
- Prerequisites for Data Delete
- Requesting a Data Delete Operation
- Deletion Policies
- Tracking Data Delete Status
- Deleting or Cancelling a Data Delete Request
- Deletion Log Files

**IMPORTANT** All tasks in this chapter require that you log in to the Absolute console as a Security Administrator or Security Power User.

Minimum System Requirements

Data Delete is available for devices that meet the following minimum system requirements:

- **Operating Systems**: The targeted device must have one of the supported operating systems installed. For more information, open the Absolute console’s help system and search for supported platforms for managed devices

  **NOTE** Data Delete is not supported on devices running the Chrome OS operating system.

- **Agent**: The targeted device must have an active agent installed and regularly calling in to the Absolute Monitoring Center. For information about the most current agent versions, see "Downloading the Absolute Agent for Android Devices" on page 67.

Deletion Algorithms

The Data Delete service uses different deletion algorithms for different types of devices and operating systems. The algorithm used on Windows computers far exceeds the recommendations documented by the United States National Institute of Standards and Technology. For further details, see *NIST Special Publication 800-88: Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology*, referenced at: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

On all operating systems, you cannot recover data after it is deleted, even using forensic software and data remanence analysis tools.
Prerequisites for Data Delete

Data Delete may not be available for all devices in your account depending on other security operations in progress, such as Remote File Retrieval. The devices on which you want to start a Data Delete operation must be clear of any conflicts with other security operations.

Before you request a Data Delete operation for a device, if applicable, do the following:

1. Unfreeze the device if it is frozen. If you initiate Data Delete on a machine with a Freeze request in the Freeze Requested state, the Data Delete request implements before the Freeze request. The Freeze request status changes to Pending until the Data Delete Request is complete.

   **NOTE** If you request a Device End of Life Data Delete operation for a Windows device, or an All Files - Security Data Delete operation for a Mac device, and the device has an outstanding Freeze request, the Freeze request is cancelled automatically.

2. Cancel any outstanding Remote File Retrieval request or wait for the request to complete before requesting a Data Delete operation. For more information, see "Cancelling a File Retrieval Request" on page 276.

3. Ensure that any associated Investigation Report is closed because you cannot run a Data Delete request on a device that has an open Investigation Report. Before you run a Data Delete operation, contact Absolute Technical Support to close any open Investigation Reports that are associated with the device.

4. Ensure that the Security Administrator or Security Power User who requests the Data Delete operation has not recently changed his or her e-mail address. Although e-mail addresses can be changed, doing so temporarily suspends those users from performing security operations for the next 72 hours.

5. If you are requesting a Device End of Life - Data Delete operation, disable all data and device security options on the targeted device before you continue. Failure to do so may result in multiple reboots of the targeted device. If these preconditions are not met after five reboots and five successful agent calls to the Monitoring Center, the Data Delete request does not start and the status changes to Failed.

**WARNING!** You cannot submit an Device End of Life - Data Delete request for those devices with Full-Disk Encryption (FDE). Submitting an Device End of Life - Data Delete request for devices with FDE can cause your device to stop functioning. To submit a Data Delete request in such cases, in the Reason field select Other or decrypt the device before you proceed with this type of Data Delete request. Also note that for a Device End of Life - Data Delete request to complete successfully, the device must be connected to the Internet through a LAN connection. If a device is using a wireless connection, its Data Delete request remains pending.

Requesting a Data Delete Operation

The following instructions presume that you have already signed and delivered your Absolute Security Administration Authorization Agreement to Absolute, and that you have selected your Security Authentication method. See "Securing Your Data and Devices" on page 197.
IMPORTANT  You cannot edit a Data Delete request. However, you can cancel a request if that request has not yet started on the targeted device. For more information, see “Deleting or Cancelling a Data Delete Request” on page 229. You can also delete a request if the request is saved as a draft.

This section provides information about the following topics:

- Initiating a Data Delete Request
- Deletion Logs
- Data Delete Settings

Initiating a Data Delete Request

To initiate a Data Delete request:

1. On the navigation bar, click > Data Delete > Request Data Delete, which opens the Request Data Delete page.

   NOTE  You could also open the Request Data Delete page by clicking Data Delete Summary Report on the sidebar and on the Data Delete Summary Report page, click New request.

2. Ensure that you have met all prerequisites. See “Prerequisites for Data Delete” on page 210.

3. If your Security Authentication Method is Emailed Authorization Codes and you have not requested and received an authorization code for this operation, on the Request Data Delete page at the Request Authorization Code area, click Request Code.

   A confirmation message indicates that an authorization code is requested and sent to your-email address. Check your email for the message. You will need to enter the code in step 12 of this task.

4. At the Data Delete Request Name and Reason area, do the following:

   a) In the Request Name field, enter an appropriate name for your Data Delete request.

   b) In the Reason field, open the list and select a reason from the following choices:

   - For devices that are lost, but not stolen, click Missing.
   - If you want to perform a Data Delete for other reasons, such as preparing devices for reassignment, click Other.
   - For devices that are nearing the end of their lease, retiring, or being taken out of commission for any other reason, select End of Lease / Life. A Device End of Life Data Delete request requires the device to reboot twice before the Data Delete request is complete. To ensure that the Data Delete request completes successfully, disable the device in the Absolute console before you reinstall the operating system or reuse the device.
**IMPORTANT** You cannot submit an Device End of Life Data Delete request for devices with Full-Disk Encryption (FDE). Submitting an Device End of Life Data Delete request for devices with FDE can cause your device to stop functioning. To submit a Data Delete request in such cases, in the **Reason** field select **Other** or decrypt the device before you proceed with this type of Data Delete request. Also note that for an Device End of Life Data Delete request to complete successfully, the device must be connected to the Internet via an Ethernet connection. If a device is using a wireless connection, its Data Delete request remains pending.

5. At the **Select Devices** area, select one or more devices by doing the following:
   a) Click **Select Devices** to open the Select Devices dialog.
   b) In the **where Group is** field, open the list and select the appropriate Device Group.

   **NOTE** If you are logged in as a Security Power User, you can select only the Device Group to which you are assigned.

c) In the **Please select a field** field, open the list and select a filter criterion.

d) If you want to show devices that meet specific criteria, enter the appropriate information in the remaining two fields. For example, you may want to show only those devices where the **Username** field begins with the letters **Admin**.

   Alternatively, to show all devices in the selected Device Group, leave these two fields blank.

e) By default, the list of devices in the **results** grid is limited to only those devices that are eligible for Data Delete. If you want to show all devices that match the criteria you specified, clear the **Show eligible devices only** checkbox.

f) Click **Filter**. The Select Devices dialog refreshes to show a list of devices matching your criteria.

g) In the list of devices, select the checkboxes next to the **Identifier** for the devices on which you want to run the Data Delete request.

h) Click **Continue**, which closes the Select Devices dialog and returns you to the Request Data Delete page.

   Under the **Select Devices** area, you see the devices you selected.

6. At the **Data Delete Settings** area, depending on the types of devices you have selected, the appropriate tabs on the Data Delete Settings section are enabled, as follows:

   - **PC <device count>** tab
     i) At the **Select Data Delete Type** location, select one of the following options:
        o **Custom Policy**
        o **All Files**
        o **Lost or Stolen Device - Delete all Files and OS**
        o **Device End of Life - Delete all Files, Sector Wipe, and OS**
        o **Firmware Drive Wipe**

        For more information about these options, see "Data Delete Settings for Windows Devices" on page 214.

     ii) At the **Select Data Delete Options** location do the following, if applicable:
         o Open the **Number of Data Overwrites** list and select one of the options.
Select the **Perpetual Deletion** checkbox to have Data Delete re-initialize on the targeted device on the next agent call after the deletion cycle is complete.

Select the **Include File Date Attributes** checkbox to include file date attributes in the Deletion log file.

Select the **Ignore hard drive serial number check** checkbox to let Data Delete override the Hard Disk Serial Number (HDSN) check.

For more information about these options, see "Selecting Data Delete Options" on page 217.

- **Mac <device count>** tab

  Select one of the following **Select Data Delete Type** options:

  - **All Files**
  - **All Files – Security**

  For more information about these options, see "Data Delete Settings for Mac Devices" on page 218.

- **Mobile Devices <device count>** tab

  Select one or more of the following options:

  - **Delete Emails**
  - **Delete Contacts**
  - **Delete Phone Logs**
  - **Delete Files in Removable Storage**
  - **Delete Files in Non-removable Storage**

  For more information about these options, see "Data Delete Settings for Mobile Devices" on page 218.

7. **If the Data Delete request applies to one or more RTT enabled devices, the Force a call to MCIC-enabled devices checkbox is selected by default at the Monitoring Center Initiated Calling (MCIC) area.**

   For more information, see "Initiating a Forced Call" on page 188.

   After the targeted device receives and processes the SMS message, depending on the Data Delete settings specified for the account, the Data Delete request runs.

8. **In the Data Delete Comment area, type the appropriate comments for this Data Delete request in the field.**

9. **If the Custom Action Fields area shows, complete the fields, as required, to add additional information about this Data Delete request.**

   **NOTE** For more information about adding, editing, and removing Custom Action Fields, see "Managing Custom Action Fields" on page 203.

10. **Under Data Delete Agreement in the Data Delete Validation area, read the agreement carefully. Select the checkbox under the agreement to indicate you have read and accept the terms of the agreement, and that you consent to the installation of additional software components on the selected device to enable the Data Delete operation.**

11. **Click Continue to refresh the Request Data Delete page, which shows the Data Delete information specific to this request.**
12. Review the information and when satisfied that it is accurate, click **Submit Data Delete Request**, which refreshes the Request Data Delete page again to show the **Provide Authentication** area. Do one of the following:

   ● If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
   
   ● If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.

13. Click **OK**.

   When initiated, the Data Delete operation runs on the next agent call, even if the user does not log in to the device.

   When the Data Delete process has begun, it cannot be stopped. If the Data Delete operation is interrupted by a system restart, Data Delete restarts only when the operating system Login screen opens.

   **IMPORTANT** In some cases, if the hard drive serial number option is not selected, the Data Delete operation may fail because the agent believes that the targeted device is different from the selected device. If the Data Delete operation fails in such cases, a notification email is sent to the Security Administrator or Security Power User who requested the Data Delete operation.

**Deletion Logs**

When a Data Delete operation completes, you can view a log file from within the Absolute console. This log file shows the name of the Data Delete Request and a list of all of the files that were deleted. You can review this log file to confirm that all sensitive data was removed, which helps organizations comply with regulations for security operations. For more information, see "**Deletion Log Files** on page 230."

**IMPORTANT** If you use a Data Delete policy file that specifies **no boot without log file** (Windows devices only), no log file is available for viewing.

**Data Delete Settings**

Depending on the devices you selected for your Data Delete Request, the options on the appropriate tab for each type of device are enabled. The following three tabs are available in the **Data Delete Settings** section:

   ● The **PC** tab lets you specify options for Windows devices. For more information, see "**Data Delete Settings for Windows Devices** on page 214."

   ● The **Mac** tab lets you select options for Mac devices. For more information, "**Data Delete Settings for Mac Devices** on page 218."

   ● The **Mobile Devices** tab lets you specify the options for Mobile devices. For more information, see "**Data Delete Settings for Mobile Devices** on page 218."

**Data Delete Settings for Windows Devices**

The PC tab is where you specify detailed settings for your Windows-based devices. This section provides the following two tasks:

   ● **Selecting a Data Delete Type Option**

   ● **Selecting Data Delete Options**
Depending on your needs and the configuration of your device, some or all of the Data Delete types and options may apply to your Data Delete request.

Selecting a Data Delete Type Option

**IMPORTANT** Exercise caution when using wildcards. For example, typing ".s*" deletes all of your system drivers, whereas typing ".d*" deletes all of your dlls, which makes it impossible to restore your system.

Select one of the following Data Delete Type options:

- **Custom Policy** is a previously created and saved policy that lets you delete specific files and folders. The operating system is not removed. The device continues to contact the Absolute Monitoring Center. Specify the custom Data Delete policy using one of the following methods:
  - Select **Custom Policy** and then select an existing policy from the **Select Custom Policy name** list.
  - Create a new policy to meet your specific needs. Select **Custom Policy** and then click the **Create a Policy** link. The Create and Edit Data Delete Policies page opens. For instructions on creating a deletion policy, see "Creating a Data Delete Policy" on page 220.

- **All Files** deletes all non-OS data files and user profiles from the device; the operating system is not deleted. This option also securely removes all previously deleted files, including recoverable files.

  Although the operating system remains intact, all user profiles are deleted from the device, which prevents users from logging in. If you want to let users log in to the device, use the **Custom Policy** option.

  When you select **All Files**, the Windows folder and the root folder (usually C:\) are not deleted. All other files and folders are deleted. In addition, Data Delete searches for and deletes any files in the Windows folder and the root with the following extensions:

  - .ACCDB .ACCDE .ACCDT .bak .bmp .csv .doc
  - .docm .docx .dot .dotm .dotx .gif .htm .html
  - .jpeg .jpg .mdb .msg .ost .pdf .potm
  - .potx .ppam .ppsm .ppsx .ppt .pptm .pptx .pst
  - .rtf .tif .tiff .txt .vsd .xlam .xls .xslb
  - .xsm .xls .xlsm .xlsx .xml .zip

- **Lost or Stolen Device - Delete all Files and OS** deletes all data files and user profiles from the device. This option also securely removes all previously deleted files, including recoverable files. After the Deletion log file is uploaded to the server, any remaining operating system files are deleted. The device stops contacting the Monitoring Center. After the Data Delete process is complete, the device can no longer boot into Windows unless it is reformatted and Windows is reloaded.
IMPORTANT We recommend using the Lost or Stolen Device - Delete all Files and OS option when a device is reported missing, lost, or stolen and you want to make the device unusable by deleting all files. For best results, we recommend that you create a custom deletion policy that emulates Lost or Stolen Device - Delete all Files and OS but keeps intact all files required to complete the Data Delete process. For instructions on creating a deletion policy, see "Creating a Data Delete Policy" on page 220.

- **Device End of Life - Delete all Files, Sector Wipe, and OS** performs a sector-by-sector wipe of the device, which removes data from all internal drives and external USB connected drives. The operating system is also removed and the device stops contacting the Monitoring Center. Performing a Device End of Life Data Delete disables the Persistence technology on the device. This option downloads a proprietary Linux kernel that contains predefined Ethernet drivers. A Linux Tiny Core OS is also loaded, which initiates the data wipe from the Linux OS to perform a sector by sector wipe of all data including the Windows OS until all data, on the device and any connected USB drives, is deleted.

  If there is an outstanding Freeze request on a device, that request is cancelled when you submit a Device End of Life Data Delete request.

IMPORTANT We recommend using the Device End of Life - Delete all Files, Sector Wipe, and OS option for End-of-Lease or End-of-Life scenarios only. This option is not stealthy and should not be used for devices that are reported missing, lost, or stolen.

When the operation is complete, you can view the End of Life Data Delete Certificate. See "Viewing or Printing an End of Life Data Delete Certificate" on page 227.

NOTE
- If you want to reassign the Absolute product license to another device, remove the agent from the device that you are retiring. Removing the agent disables the device Identifier and makes the license available for assignment to another device. For information on how to remove the agent from a device, see Unenrolling devices from your account in the online Help.
- An Ethernet connection is required. This option is not available over Wi-Fi, Mobile Broadband, or other network connections.
- This option is not supported on hard drives protected with Full-Disk Encryption (FDE). Decrypt the device before submitting the Data Delete request.
- This option is not supported on devices with Unified Extensible Firmware Interface (UEFI) Trusted Boot Implementations, such as Secure Boot and Measured Boot implementations.
- This option is not supported on Small Computer System Interface (SCSI) hard drives.

- **Firmware Drive Wipe**, also known as Panasonic BIOS wipe, is available only for selected Panasonic devices. Select this option to delete all data from all internal hard drives. When the wipe completes, the operating system and all data on the device are removed and the device cannot call the Monitoring Center. For more information on service centers, visit Panasonic’s Support site at: panasonic.net/support. The Firmware Drive Wipe is not stealthy.

NOTE Drive wipe and sector wipe are not supported on hard drives protected with BitLocker Drive Encryption and encrypted Self Encrypting Drives.
Selecting Data Delete Options

Select one or more of the following options:

- **Number of Data Overwrites** lets you specify the number of times to overwrite the specified data with random or garbage data to make the original data impossible to recover. The overwrite process is called a “data wipe”. Possible values for this setting are:
  - **1**: wipe the data once. The process is the fastest and offers the lowest level of security. This is the default setting for the **Device End of Life - Delete all Files, Sector Wipe, and OS** Data Delete type.
  - **3**: wipe the data three times. The process is slower than the process for one data wipe and offers a higher level of security.
  - **7**: wipe the data seven times. The process is the slowest and offers the highest level of security. This is the default setting for all Data Delete types except **Device End of Life - Delete all Files, Sector Wipe, and OS**.

- **Perpetual Deletion** re-initializes the Data Delete on the targeted device if the agent on the device makes a call to the Monitoring Center after the deletion cycle is complete. The Perpetual Deletion option is disabled if you have selected more than one device for your Data Delete Request.

**IMPORTANT** Selecting a Data Delete against a device for which there is an open Investigation Report results in the closure of that Investigation Report, as Perpetual Deletion removes and/or prevents collection of forensic evidence required to recover the device.

- **Include File Date Attributes** option includes the **Created**, **Modified**, and **Accessed** dates in the Deletion log file.
  By default, only the **Created** and **Modified** dates appear in the log file. To include **Accessed** dates, you need to also enable the following setting in Classic Account Settings: **Enable last file access date and time stamps (Windows devices only)**. For more information, see “**Editing Classic Account Settings**” on page 54.

**IMPORTANT** Including file date attributes increases the size of the Deletion log file. If the log file is large and the target machine has a low-bandwidth Internet connection, Data Delete completion may be delayed while the client device repeatedly attempts to upload the log file to the Absolute console.

- **Ignore hard drive serial number check** option lets you specify whether Data Delete should override the Hard Disk Serial Number (HDSN) check and continue even when the HDSN is unknown or changes during the lifecycle of the request.

**IMPORTANT** Use the **Ignore hard drive serial number check** feature with care. A Data Delete operation deletes data on the targeted device. Overriding the HDSN check before performing a Data Delete operation may delete data created or owned by any post-loss possessors of the device or on an unrelated hard drive.

If no hard drive serial number is detected for the targeted device, the **Ignore hard drive serial number check** option is selected by default. To continue, do not change the default value.
Data Delete Settings for Mac Devices

Select one of the following options:

- The **All Files** option deletes all non-OS data files, including all files used by Apple apps and third-party apps, and files on connected USB drives. The operating system is not deleted. User profiles are retained so the user is able to log in to the device after the Date Delete operation is completed.

- The **All Files - Security** option deletes the same content as the All Files option and deletes the OS files on devices running macOS 10.9 or 10.10 only.

If there is an outstanding Freeze request on a device, that request is cancelled when you submit an All Files - Security Data Delete request.

**NOTE** For devices running macOS 10.11 or higher, Absolute’s Data Delete feature cannot delete OS files or potentially other applications deemed by Apple as essential to their OS working properly. From a data security perspective, every Mac user has the same version of those Apple-provided apps, therefore no sensitive data will remain within these apps. Third-party apps that are installed by users or distributed through the Mac App Store can be deleted using the Data Delete feature.

Data Delete Settings for Mobile Devices

Select one or more of the following options:

- **Delete Emails** deletes all email messages downloaded to your mobile device and all the email accounts set up on your device. Two items to note are:
  - Your email messages are not deleted from your mailbox on your email provider’s server. You can retrieve these messages from a different device using your email provider’s website.
  - Your email account with the email provider is not deleted.

- **Delete Contacts** deletes all contact phone numbers and other information from your mobile device.

- **Delete Phone Logs** deletes information about all phone calls made or received from your mobile device.

- **Delete Files in Removable Storage** removes all data and files stored in any data storage media you have inserted in your mobile device. Some examples of removable data storage media are SD cards or other digital storage cards.

- **Delete Files in Non-removable Storage** removes all data and files stored on your mobile device.

Deletion Policies

In addition to the predefined Data Delete options of *all files except the operating system* and *all files including the operating system*, Security Administrators and Security Power Users can customize Data Delete by creating deletion policies to delete specific sets of files and folders.

A deletion policy is a user-created list of file and folder locations. When Data Delete is invoked, all files on the targeted device in the specified locations are deleted.

This section provides information about the following topics:

- [Using Sample Policy File Entries](#)
Using Sample Policy File Entries

There are some useful policy file entries that you can use to create a deletion policy:

- **no boot with log file**: Use this entry as the last entry in a policy file, only appearing after the process deletes all other specific files. When you select this entry, Data Delete always uploads the log file of what was deleted before starting the sector wipe.

- **no boot without log file**: Use this entry as the last entry in a policy file, only appearing after the process deletes all other specific files. When you select this entry, Data Delete starts the sector wipe immediately after all specified files are deleted. The agent does not upload a log file to the Monitoring Center or make it available on the Absolute console.

- **DELETE**: Append this entry to a registry path to delete any key (or subkeys) from the Windows registry. For example, the following policy file deletes all existing subkeys under Run:
  
  ```plaintext
  DELETE_HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
  \Run
  ```

- **NO_DELETE**: Append this entry to a file or folder path to prevent the deletion of certain files or folders during a Data Delete operation that would normally delete a wide range of files. For example, C:\Project_Documents\NO_DELETE ensures that a Data Delete operation does not delete the Project_Documents folder. Many encryption products use a certain set of files to boot the device. When a Data Delete operation forces a reboot to delete locked files, the device does not reboot successfully if the files needed by the encryption software were already deleted. This situation prevents the Data Delete operation from terminating, and the user does not receive a confirmation of the operation in the Absolute console.

- **do not force reboot**: Use this entry to prevent a reboot when a Data Delete operation encounters locked files. This entry is useful when you are creating a policy file on devices with encryption software installed, and forcing a reboot could cause the device to hang because some files that the encryption software require to boot the machine were already deleted. You can use the **do not force reboot** entry in tandem with the **NO_DELETE** option to create a policy file that performs a successful Data Delete operation on devices with encryption software installed.

Deleting a Folder Based on a Windows System Variable

You can delete a folder based on a Windows system variable by specifying the variable name in a policy file. The variable name must be delimited with the % character. For example, specifying %windir% deletes everything in the Windows installation folder, regardless of the physical location of the installation folder; for example, C or D drive. Data Delete deletes all files within the folder and all its subfolders as specified by the system variable.
NOTE Data Delete works on system variables only. The Data Delete operation has no access to current user variables. In addition, when a new system variable is created, the variable definition is not loaded to memory until the device is rebooted. Therefore, the Data Delete operation is not able to access system variables created within a given session until the device is rebooted.

Creating a Data Delete Policy

To create a Data Delete Policy:

1. On the navigation bar, click **Data Delete > Create and Edit Data Delete Policies.**
2. On the Create and Edit Data Delete Policies page, enter a name for your deletion policy in the **Policy Name** text box.

NOTE Data Delete Policies must have unique names.

3. Enter a brief description for your deletion policy in the **Description** text box.
4. Define all files and directories to be deleted. A number of predefined file and directory entries are included by default. Additionally, you can define your own unique file and folder entries. A single deletion policy may include any combination of predefined and user-defined entries.

IMPORTANT You can also use policy templates to create a Data Delete Policy. For more information, see "Using Data Delete Policy Templates" on page 222.

5. To add predefined entries:
   a) Click **Pre-defined Data Deletes** to expand the section.
   b) Select the appropriate checkboxes for the file types that you want to delete.
6. To define and add unique entries:
   a) If not already expanded, click **Custom Data Deletes.**
   b) In the provided field, type an entry for each file or folder to be deleted. Use the standard Windows file path convention and follow these guidelines:
      ● The * wildcard is supported, however we recommend that you exercise caution when using them.
      ● When specifying a folder, be sure to include the trailing backslash after the folder name; for example, c:\temp\. All files in the main folder, and all files and subfolders are deleted. The empty root directory is retained.
      ● To delete a folder, include a trailing backslash in the path, for example: c:\folder\.
      ● To delete a file, do not include a trailing backslash in the path, for example: c:\folder\xyz.doc

The following table provides further examples.

<table>
<thead>
<tr>
<th>To delete...</th>
<th>type this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a folder on C drive</td>
<td>c:\folder\</td>
</tr>
<tr>
<td>a specific folder on all drives</td>
<td>*:\folder</td>
</tr>
<tr>
<td>a specific file type in a specific folder on C drive</td>
<td>c:\folder*.abc</td>
</tr>
</tbody>
</table>
To delete...

<table>
<thead>
<tr>
<th>Type this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a specific file in a specific folder on C drive</td>
</tr>
<tr>
<td>a specific variable in the registry</td>
</tr>
<tr>
<td>all files for a specific file type</td>
</tr>
</tbody>
</table>

7. To specify registry key entries or specific file types:
   a) Click **Registry Data Deletes** to expand the section.
   b) To delete a registry key and all subkeys under the key:
      i) In the **Registry Delete Type and Key Entry Value** list, select **Delete key at**.
      ii) In the **Registry Delete Type and Key Entry Value** field, enter the key in an appropriate registry key format. For example, to delete the key and all subkeys add:
           HKEY_LOCAL_MACHINE\SOFTWARE\MyKey
      iii) Click **Add** to add the entry.
   c) Repeat step b to add all the keys and subkeys you want to delete.
   d) To delete a file found under a specific registry key:
      i) In the **Registry Delete Type and Key Entry Value** list, select **Delete FILE found at**.
      ii) In the **Registry Delete Type and Key Entry Value** field, enter the key containing the physical path to the file you want to delete. For example, to delete the file C:\Program Files\app_name.exe, which is found under the MyApp software key, add:
           HKEY_LOCAL_MACHINE\SOFTWARE\MyApp
      iii) Click **Add** to add the entry.
   e) Repeat step d to add all files for a registry key that you want to delete.

8. To retain the data in specific folders, or for specific files and files types: specific files and folders:
   a) Click **Excluded files or folders** to expand the section.
   b) Add the list of files and folders you want to exclude from the Data Delete operation in the same format that you used for the Custom Data Delete.
   c) If you want to force a Data Delete operation on files or folders in the excluded files and folders list that you specified in the preceding step, click **To force a Data Delete operation on files or folders located in the above list**.
   d) Add the list of files and folders in the provided field.

**NOTE** For more information about the format of the commands used, see "Creating a Data Delete Policy" on page 220.

9. To specify other options:
   a) If not already expanded, click **Options**.
   b) If you want to perform additional deletions, select **Perform additional deletions**.
   c) Select one of the following options:
      - **Wipe recoverable files**: This option securely erases any previously deleted files that are recoverable.
      - **Erase free space**: This option securely erases any data that is left in the used disk space.
d) If you want to make the targeted device unbootable, select **Make the target device unbootable**.

e) Select one of the following options:
   - **Immediately after the Data Delete operation is complete**: This option does not provide any log file.
   - **After the log file is uploaded**: This option stops the device from booting into the operating system after the Deletion log file is uploaded.

f) If you do not want to force a reboot of the device that has open or locked files or full-disk encryption enabled, select the **Do not force reboot if the target device has locked files or full disk encryption enabled**. In such cases, the Data Delete operation pauses until the device is rebooted.

10. When you have defined all appropriate descriptions, click **Save**.

### Using Data Delete Policy Templates

Policy templates are provided that contain sample text and examples for selected Data Delete scenarios. You can use policy templates to create Data Delete policies much faster by copying and pasting the appropriate text.

The following sample Data Delete scenarios are available:

- I have CheckPoint Full Disk Encryption.
- I want to delete sensitive files first, and then disable the Cisco VPN on the device.
- After the Windows user profile folders and files are deleted, I just need to make the device unbootable as fast as possible.

To use Data Delete Policy templates:

1. In the Create and Edit Data Delete Policies page, click **View Policy Templates**. The Policy Templates windows shows.

   **NOTE** You can resize and move the window.

2. Click the appropriate scenario to expand.
3. Copy and paste the sample text to each appropriate field in the corresponding section.
4. In the **Options** section on the Create and Edit Data Delete Policies page, select the same options you see in the **Example**.
5. Click **Close**.

### Working with Deletion Policies

Security Administrators and Security Power Users can manage existing deletion policies in the following ways:

- View the settings of a deletion policy
- Edit the settings of a deletion policy
- Create a copy of a deletion policy
- Delete a deletion policy
NOTE You can edit or delete a deletion policy without impacting any active Data Delete requests that are using the deletion policy. All active requests are processed as usual using the deletion policy configurations that were in place when the request was created.

To edit, copy, or delete a deletion policy:

1. On the navigation bar, click 🈴 > Data Delete > View and Manage Data Delete Policies. The View Data Delete Policies page opens showing all currently defined Deletion Policies.

2. Click the view link of the deletion policy you want to modify. The Create and Edit Data Delete Policies page opens to show the current configuration of the selected deletion policy.

3. Do one of the following:
   - To edit the existing settings for this deletion policy, make your changes and click Save. For details, see "Creating a Data Delete Policy" on page 220.
   - To create a copy of this deletion policy, which you can then edit, click Copy. The new deletion policy is added to View Data Delete Policies page with the name "Copy of <deletion policy name>."
   - To delete this deletion policy, click Delete and on the confirmation dialog click OK. The deletion policy is deleted.

Tracking Data Delete Status

You can view real-time status updates on the progress of Data Delete requests. Additionally, upon successful completion of a Data Delete operation, a Deletion Log is created that shows all files and folders that were deleted.

NOTE To view an audit log of completed security actions related to Data Delete requests, see "Security Audit Logs Report" on page 181. To export a report that provides statistics on the Data Delete requests submitted for your account, see "Security Posture Report" on page 151.

Viewing Data Delete Status

To view the status of a Data Delete request:


2. On the Data Delete Summary Report page at the Search Criteria area, set the preferred filtering and display options for the results 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.

   **NOTE** If you are logged in as a Security Power User, you can select only the Device Group to which you are assigned.

   - To filter results by a specific Identifier, Make, Model, or Serial Number, or custom field (if applicable), in the and the field open the list and select the value type. In the is or contains field enter the value to search for or use the Choose feature. For more information on the Choose feature, see "Editing Asset Information" on page 80.
● To filter by request name, in the **and the Request Name is or contains** field, enter all or part of the complete name of the Data Delete request.

● To filter by Status, in the **and the Data Delete Status is** area, select one or more checkboxes from these possible values:
  ○ **Requested**: The request was submitted and is in a transitory state while the Data Delete instructions are set up. Data Delete requests stay in this state briefly.
  ○ **Launched**: The Data Delete instructions were sent to the targeted device, and that device has called in and received the Data Delete request instructions.
  ○ **Triggered**: For the Panasonic BIOS wipe only, this state is similar to Launched, but it is a final state. Panasonic BIOS wipe does not return a **Fail** or **Done** state for Data Delete requests.
  ○ **Canceled**: The Data Delete request was cancelled.
  ○ **Cleared**: The targeted device was recovered before the Data Delete operation started. The Absolute Investigations team has cancelled the request.
  ○ **Set, Awaiting Call**: The Monitoring Center is configured to send the Data Delete instructions to the targeted device on its next call.
  ○ **Completed, Attempting to Upload Log File (If Applicable)**: Data Delete has completed on the targeted device, however the agent is unable to send the log file to the Monitoring Center. If specified for your account or the device, the agent continues to initiate calls to the Monitoring Center until the log file is uploaded to it.
  ○ **Completed, Log File Uploaded**: Data Delete has completed on the targeted device and the agent has sent a log file with details of the Data Delete operation to the Monitoring Center.
  ○ **Failed**: The Data Delete request failed to run on the targeted device. Contact [Absolute Technical Support](https://www.absolute.com/technical-support).
  ○ **Processing**: The Data Delete request is being created. Data Delete requests go through the Processing state before they enter the Requested state.

● To filter by Data Delete options, in the **and the Data Delete Type is** area, select one or more checkboxes from the following possible choices:
  ○ **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](https://www.absolute.com/technical-support)” on page 214.

● To filter by reason, in the **and the Data Delete Reason is** area, select one or more checkboxes from the following possible choices:
  ○ **Missing** indicates the device is lost or misplaced.
  ○ **End of Lease / Life** indicates the device is at the end of its functional lease or life.
  ○ **Other** represents all other reasons for the Data Delete request.

3. Click **Show results** to regenerate the report using specified criteria.
The Data Delete Summary Report shows all devices that have had Data Delete requested. For each device listed, the Data Delete Summary Report includes the following information:

- **Identifier**: the targeted device’s Identifier.
- **Request ID**: the identifier assigned to the Data Delete request by the system.
- **Request Name**: the name of the Data Delete request.
- **Make**: the targeted device’s make.
- **Model**: the targeted device’s model.
- **Serial Number**: the targeted device’s serial number.
- **Requested On**: the date and time when the Data Delete was requested.
- **Status**: the current status of the Data Delete request. Possible values include:
  - Custom
- **Type**: the Data Delete policy and options that were set for this request.
- **Reason**: the reason for the Data Delete request.

**NOTE** If Custom Action Fields are associated with the Data Delete request, a column for each custom field shows on the far right of the report. For more information, see "Managing Custom Action Fields" on page 203.

You can perform the following additional tasks on the generated report, if desired:

- To download the report, click . For more information, see "Downloading Reports" on page 92.
- To print the current page of the report, click . For more information, see "Printing Reports" on page 90.
- To save the filters you used to generate the report, click . For more information, see "Saving Report Filters" on page 91.

**Data Delete Details Page**

The Data Delete Details page shows the setup information for each Data Delete request. This page also provides a link to the Deletion Log file after the Data Delete operation has completed. See "Deletion Log Files" on page 230.

To open the Data Delete Details page:

1. Complete the steps in the task, "Viewing Data Delete Status" on page 223.
2. On the Data Delete Summary Report page, click the **view** link for the appropriate device. The Data Delete Details page opens showing the following information:

   - **Request ID**: the identifier assigned to the Data Delete request by the system.
   - **Identifier**: the targeted device’s Identifier.
   - **Make**: the targeted device’s make.
   - **Model**: the targeted device’s model.
   - **Serial Number**: the targeted device’s serial number.
   - **Asset Number**: the asset number of the targeted device.
   - **Last Call**: the date and time (including the timezone) of the targeted device’s last call to the Monitoring Center.
Chapter 9: Using Data Delete

- **Reason for Data Delete Request**: the reason specified for initiating the Data Delete operation on this device, which could include one of the following:
  - **Missing** means the device is lost, but not stolen.
  - **End of Lease / Life** means the device is nearing the end of its lease, is going to be retired, or is going to be taken out of commission.

**IMPORTANT** For a Device End of Life - Data Delete request to complete successfully, the device must be connected to the Internet through a LAN connection. If a device is using a wireless connection, its Data Delete request remains pending.

- **Other** means this device is being prepared for reassignment or removed for some reason other than those provided.

- **Perpetual Deletion**: shows a Yes or No value, depending on whether perpetual deletion was applied.

- **Ignore hard drive serial number check**: specify whether Data Delete should override the Hard Disk Serial Number (HDSN) check and continue even when the HDSN is unknown or changes during the request’s lifecycle.

**IMPORTANT** Use the Ignore hard drive serial number check option with caution. Overriding the HDSN check before you perform a Data Delete operation may delete data created or owned by any post-loss possessors of the device or on an unrelated hard drive.

- **Number of Data Overwrites**: shows the number of data wipes selected. Possible values are 1, 3, or 7.

- **Data Delete type**: shows the delete options configured for the request, with the following possible values:
  - **Custom Policy**: the operation deletes specific files and folders.
  - **All Files**: the operation deletes all files except the Operating System.
  - **Lost or Stolen Device - Delete all Files and OS**: the operation deletes all files, including the Operating System, and, upon completion of the first Data Delete operation, wipes the connected hard drives. The Data Delete request is prompted by a security breach and a need to remove sensitive data from a device.
  - **Device End of Life - Delete all Files, Sector Wipe & OS**: the operation deletes all files including the Operating System and wipes the hard drive after the request is complete. The Data Delete request is prompted by the need to retire the device because of end of lease or life requirements.

**IMPORTANT** For a Device End of Life - Data Delete request to complete successfully, the device must be connected to the Internet through a LAN connection. If a device is using a wireless connection, its Data Delete request remains pending.

- **Firmware Drive Wipe**: also known as the Panasonic BIOS Wipe, this type of Data Delete is supported on the BIOS level for specific Panasonic devices.

- **Mobile Device**: the operation runs on the mobile device and deletes all e-mail messages, e-mail accounts, contacts, phone logs, and any other type of data saved on the device.

- **Set for deletion**: shows the directory for the information you want to delete.
- **Include File Date Attributes in the Data Delete log**: indicates whether the file date attributes are included in the Deletion log file. For more information, see "Deletion Log Files" on page 230.
- **Agreement**: indicates whether the I Accept the agreement checkbox was selected when the request was prepared.
- **Requestor Username**: shows the name of the Security Administrator or Security Power User who submitted the request.
- **Data Delete Comment**: shows the comment made by the Security Administrator or Security Power User who submitted the request.
- **[Custom Action Fields]**: shows the value for each custom field, if one or more Custom Action Fields are associated with the Data Delete request. For more information, see "Managing Custom Action Fields" on page 203.
- **Data Delete Status table**: shows information on the status of the delete request and includes the date and time when each status was achieved. This table includes:
  - the progressive steps that form the Data Delete operations performed on the device
  - the **Status** of each Data Delete operation
  - the **Date** in the dd/mm/yyyy hh:mm:ss AM or PM format
  - the **User** who requested this operation
  - any **Details**

### Viewing or Printing an End of Life Data Delete Certificate

For devices that are at the end of their lifecycle or are nearing the end of a lease period, you can request a Data Delete to remove sensitive information from such devices. In such cases, if the Data Delete type is **Device End of Life - Delete all Files, Sector Wipe, & OS**, Security Administrators and Security Power Users can view and print an End of Life (EOL) Data Delete Certificate for compliance purposes. Such certificates are useful in proving that the device that was retired or taken out of circulation does not contain sensitive information.

The following information is available in the certificate:
- **Information about the Data Delete Request and the device**, including:
  - **Request Name**: the name of the Data Delete request
  - **Identifier**: the device’s Identifier
  - **Make**: the name of the device manufacturer
  - **Model**: the model name and number of the device
  - **Serial Number**: the device’s serial identification number
  - **Asset Tag**: any specific tag added to the device
  - **Device Name**: name of the device
  - **Data Delete Type**: type of the Data Delete request, that is All Files, Sector Wipe & OS
  - **Started**: date and time when the Data Delete request started running on the device
  - **Finished**: date and time when the Data Delete request completed
  - **Data Delete Launched By**: e-mail address or username of the Security Administrator or Security Power User who requested the Data Delete operation

- **Information about the hard drive where the Data Delete operation happened**, including:
  - **Drive**: the number of the drive in the device
Model: the model number of the drive
Serial Number: the serial number of the drive
Interface Type: the type of drive, for example, whether it is a disk drive or a solid state drive
Sector Size: the size of individual sectors on the drive
Total Sectors: the total number of individual sectors on the drive
Reallocated Sectors: the number of sectors that were reallocated due to the Data Delete operation
SMART Drive Status: information about whether the drive contains Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T)
Size: the total size of the drive
Data Delete Speed (MB/sec): the speed in MegaBytes (MB) per second at which the Data Delete operation was run
Data Delete Duration (mm:ss): the total duration in minutes that it took for the Data Delete operation to run
Status: the status of the drive, whether the information was wiped or otherwise

Information about the certifying authority including:
- Name and signature of the Data Security Operator, commonly also the Security Administrator
- Name and signature of the supervisor of the Data Security Operator

To view or print an End of Life Data Delete Certificate:

1. On the Data Delete Summary Report, click the view link of the Data Delete operation for which you want to view or print the End of Life Data Delete certificate.
2. On the Data Delete Details page, click View Certificate (PDF) to open the certificate file.

**NOTE** If your browser’s security is set to prompt you before opening or downloading files, click Open or Save As to open or save the PDF file.

3. Print the certificate PDF using the appropriate printer attached to your device.

Removing Details of a Data Delete Operation

In certain circumstances, you may no longer need to save the details of a particular Data Delete Request. Some examples are when a Data Delete Request was cancelled, completed, or the device recovered successfully. You can remove the details of such a Data Delete operation from the Absolute console.

**IMPORTANT** Exercise caution in removing the details of a Data Delete operation, because after you remove the details of a Data Delete operation, you cannot restore the details.

To remove details of a Data Delete operation:

1. On the Data Delete Summary Report page, click the view link of the Data Delete operation for which you want to remove details.
NOTE If you have not done so already, it is strongly recommended that you download the log file first, before you remove these Data Delete details.

2. On the Data Delete Details page, click **Remove Details**.
3. A confirmation message opens. Click **OK** to remove the details of the Data Delete operation and the log file.

Forcing a Data Delete Operation to Complete

You cannot start a second Data Delete operation on a specific device when an existing process is already underway.

If a Data Delete operation fails to complete, you can force it to complete, which sets the status of the Data Delete operation in the database to **Complete**, and lets you start a new Data Delete operation. Doing this does not affect any processes currently running on any devices, and does not stop any Data Delete operations that are currently in progress.

After you have forced a Data Delete operation to complete, you are not able to undo the status change.

To force a Data Delete operation to complete:

1. On the Data Delete Summary Report page, click the **view** link of the Data Delete operation you want to force to completion.
2. On the Data Delete Details page, click **Complete Request**.
3. On the confirmation message, click **OK** to complete the Data Delete operation.

Clearing Perpetual Data Delete

If a Data Delete request was submitted with the **Perpetual Deletion** option, you can stop the Perpetual Data Delete on a targeted device.

**IMPORTANT** Perpetual Data Delete can be stopped only after the initial deletion cycle has completed.

To clear Perpetual Data Delete:

1. On the Data Delete Summary Report page, click the **view** link of the Data Delete operation that was requested with the Perpetual Deletion option.
2. Click **Clear Perpetual Data Delete Flag**.
3. On the confirmation message, click **OK** to clear Perpetual Data Delete for the Data Delete request.

Deleting or Cancelling a Data Delete Request

Before Data Delete is started on the targeted device, you can delete or cancel a Data Delete request, depending on its status. If the Data Delete request’s status is **Draft**, it can be deleted. If the Data Delete status is **Requested** or **Set Awaiting Call**, the request cannot be deleted, but you can cancel it.

The following tasks are included in this section:

- Deleting a Draft Data Delete Request
- Cancelling a Data Delete Request for a Single Device
Cancelling Data Delete Requests for Multiple Devices

Deleting a Draft Data Delete Request

To delete a draft Data Delete request:

1. On the Data Delete Summary Report page, click the view link for the draft Data Delete operation.
2. Review the details of the draft to ensure it is the one you want to delete.
3. Scroll to the bottom of the page and click Delete.
4. On the confirmation message, click OK to confirm the delete operation.

Cancelling a Data Delete Request for a Single Device

To cancel a Data Delete request with a status of either Requested or Set, Awaiting Call:

1. On the Data Delete Summary page, click the view link for the appropriate Data Delete operation.
2. Review the details of the request to ensure this is the one you want to cancel.
3. Click Cancel Request to cancel the Data Delete request.
4. On the confirmation message, click OK to confirm the cancellation.

Cancelling Data Delete Requests for Multiple Devices

To cancel multiple Data Delete requests with a status of either Requested or Set, Awaiting Call:

1. On the Data Delete Summary page in the results grid, do one of the following:
   - To cancel one or more Data Delete operations, select the checkbox next to each Data Delete operation you want to cancel.
   - To cancel all Data Delete operations on the current page, select the checkbox next to Identifier in the top row of the results grid.
2. Click Edit Requests for Selected Devices. The Edit Selected Devices dialog opens.
3. In the Action column of the Requested and Set, Awaiting Call rows, open the list and select Cancel Request.
4. Click Submit. The Data Delete requests for all selected devices are cancelled.

Deletion Log Files

When a Data Delete request is complete, a Deletion Log file is uploaded and made available on the Data Delete Details page. A Deletion Log file provides details on what was deleted from the targeted device.

**NOTE** Dates and times in a log file are expressed in the Coordinated Universal Time (UTC) format.

Deletion Log Files include the following information about the Data Delete operation:

- **Completion Date**: the date and time when the delete request completed on the targeted device.
- **Data Delete Type**: indicates the deletion type. Possible values are:
Chapter 9: Using Data Delete

- All Files Except OS
- All Files Including OS
- Specific Files/Directories (Windows devices only)

- **Data Delete Reason**: indicates why the Data Delete request was run. Possible values are:
  - Missing
  - End of Life / Lease
  - Other

- **Identifier**: the Identifier of the targeted device.
- **Model**: the targeted device’s model.
- **Make**: the targeted device’s make.
- **Serial Number**: the targeted device’s serial number.
- **Asset Tag**: the targeted device’s asset tag, which is an optional user-defined tracking number.
- **Device Name**: the targeted device’s network name.
- **Started**: the date and time when Data Delete began running on the targeted device.
- **Deleted File List**: the full path of all deleted files.
- **Finished**: the date and time when the Data Delete process was completed.
- **Data Overwrites**: the number of data wipes performed.
- **File List**: a list of all files deleted in the operation.

If the **Include File Date Attributes** option was selected when the Date Delete was requested, the file date attributes (Created, Modified, and Accessed) for each file are listed in tab-delimited format.

**NOTE** For Windows devices, the **Accessed** date shows only if the following setting is enabled in Classic Account Settings: Enable last file access date and time stamps (Windows devices only). For more information, see "Editing Classic Account Settings" on page 54. For Mac devices, no setting is required. Last file access dates and times are always logged and included in the Deletion log file.

**IMPORTANT** In a post-theft scenario, the **Accessed** date for a file may be later than the Incident Date. The Accessed date is not necessarily indicative of a file which was compromised post-theft. Undetected malware, antivirus and spyware scans, automated backup and other similar applications may all trigger an **Accessed** date change, indicating when the file was last accessed. As a result, this value should be considered useful for determining whether a file has definitively not been accessed, but not the converse.

- **e-mail Accounts**: for Android phones only: a list of all e-mail accounts deleted from the mobile device during the Data Delete operation.
- **Recoverable Files Deletion Start Date** applies to **All Files** and **All Files - Security** options only: the date and time when the Data Delete operation started wiping the recoverable files.
- **Recoverable Files Deletion End Date** applies to **All Files** and **All Files - Security** options only: indicates the date and time when the Data Delete Operation finished wiping the recoverable files.
Viewing the Deletion Log File

When the Data Delete request is complete, the status updates to Completed, Log File Uploaded and the Deletion Log becomes available, letting you download and view the results of the Data Delete operation.

The following tasks are included in this section:
- Viewing the Deletion Log for a Single Device
- Viewing the Deletion Logs for Multiple Devices
- Viewing the Deletion Log on a Mobile Device

Viewing the Deletion Log for a Single Device

To download and view the Deletion Log file:

1. On the Data Delete Summary Report page, click the view link for the appropriate Data Delete operation.
2. On the Data Delete Details page, click View deletion log.
3. The File Download dialog opens, where you take one of the following actions:
   - Click Open to open the log file.
   - Click Save to save the file to your local device.

   The log file is in text (.txt) format and can be viewed using any text file editor.

Viewing the Deletion Logs for Multiple Devices

To download a .ZIP file containing the log files for multiple Data Delete operations:

1. On the Data Delete Summary page in the results grid, do one of the following:
   - To view the log file for one or more completed Data Delete operations, select the checkbox next to each Data Delete operation.
   - To view the log files for all completed Data Delete operations on the current page, select the checkbox next to Identifier in the top row of the results grid.
2. Click Download Log Files for Selected Devices.
3. If the Download Log File(s) for Selected Devices dialog opens, click Download.

   NOTE   This dialog is shown only if you selected one or more Data Delete operations that do not have a status of Completed, Log File Uploaded.

4. The File Download dialog opens, where you take one of the following actions:
   - Click Open to extract the .ZIP file and view the individual log files.
   - Click Save to save the .ZIP file to your local device.

   The individual log files are in text (.txt) format and can be viewed using any text file editor.
Viewing the Deletion Log on a Mobile Device

To download and view the log file on a mobile device:

1. On the Data Delete Summary Report page, click the view link for the appropriate Data Delete operation.
2. On the Data Delete Details page, click View deletion log.
3. In the File Download dialog, click Save to save the file to your local device.
4. Save the log file with an .xml file extension.
   You can view the log file using any XML viewer or a web browser.
Chapter 10: Using Device Freeze

The Device Freeze feature lets Security Administrators and Security Power Users target specific devices and show a full screen message restricting users from operating the device.

NOTE Depending on the configuration of your account, the Device Freeze functionality described in this chapter may not be available.

The Device Freeze operation happens at the operating system (OS) level and, when it is in effect, a full screen message shows on the device. When you freeze a device, only the selected message is shown on-screen and no Windows components (such as Task Manager) are accessible. Windows continues to run in the background and the user is able to switch between Windows by pressing Alt+Tab keys to save any open documents or close any windows open at the time.

The Device Freeze feature is persistent. The frozen state persists on device reboot even when the device is rebooted in safe mode. The freeze shows again when the OS reloads. If a user reinstalls the OS, the device freezes again when the agent self-heals.

Security Administrators and Security Power Users can manage Device Freeze operations in the following ways:

- Submit Device Freeze requests
- Create and manage Device Freeze offline policies
- Track the Device Freeze status of devices
- Unfreeze a frozen device

NOTE Security Power Users can perform Device Freeze operations on only those devices that belong to the Device Group to which they are assigned.

This chapter includes the following sections:

- Minimum System Requirements
- Working with Device Freeze Requests
- Managing Device Freeze Offline Policies
- Tracking Device Freeze Status
- Unfreezing a Frozen Device
- Managing Custom Device Freeze Messages

Minimum System Requirements

Currently, the Device Freeze feature is available for devices that meet the following minimum system requirements:

- **Operating systems**: the targeted device must be running a supported version (open the Absolute console’s help system and search for supported platforms for managed devices) of one of the following operating systems:
  - Windows
  - macOS
  - Android
– Chrome OS (installed on Chromebooks only)

**NOTE**  Device Freeze offline policies are supported on Windows devices only.

- **Agent**: For Windows, Mac, and Android devices, the targeted device must have an agent status of Active, meaning that the agent is installed and regularly calling in to the Absolute Monitoring Center.

- **Chromebook extension**: The Chromebook extension must be activated on the targeted device, meaning that the extension is deployed and regularly calling in to the Absolute Monitoring Center.

---

### Working with Device Freeze Requests

Authorized security personnel can submit a Device Freeze request, which is associated with a Device Freeze message, on any device in their account. The device can be set to freeze on the next agent call, or on a specific date in the future. You need an authorization code to request a Device Freeze. For more information, see "Requesting a Security Authorization Code" on page 203.

When initiated, the Device Freeze operation runs on the next agent call, even if the user does not log in to the operating system. If a system restart interrupts the Device Freeze operation, the freeze persists on the device on restart and when the operating system loads. When a device is frozen, you can either use the Absolute console to unfreeze it or generate a passcode to let users manually unfreeze the device. For more information, see the following topics:

- "Viewing the Unfreeze Passcode" on page 259
- "Unfreezing a Frozen Device" on page 258

**IMPORTANT**  If you initiate a Device Freeze on a device with an outstanding Data Delete request or initiate a Data Delete Request on a device that has an outstanding Device Freeze request, the Device Freeze request is initiated after the Data Delete request is completed. However, you can't submit a Device Freeze request for the following devices:

- Windows devices with an outstanding Device End of Life - Data Delete request
- Mac devices with an outstanding All Files - Security Data Delete request
- Devices with an open Investigation Report

This section provides information on the following topics:

- Requesting a Device Freeze
- Cancelling a Device Freeze Request
- Removing Device Freeze Request Details

**NOTE**  You can create Alerts to notify you when these security actions are initiated. For more information, see "Creating New Custom Alerts" on page 19.
Requesting a Device Freeze

**NOTE** The following instructions presume you have already signed and delivered the Security Administration Authorization Agreement to Absolute and that you have selected your Security Authentication Method. For more information, see "Security Administration Authorization Agreement" on page 198.

To request a Device Freeze:

1. On the navigation bar click > Device Freeze > Request Device Freeze to open the Request Device Freeze page.


   A confirmation message indicates that an authorization code is requested and sent to your-email address. Check your e-mail for the message.

3. In the Request Name field, enter an appropriate name for your Device Freeze request. This value does not need to be unique.

4. Click Select devices.

5. On the Select devices dialog, select one or more devices by doing the following:

   a) In the Where Group is field, open the list and select the appropriate Device Group.

      **NOTE** If you are logged in as a Security Power User, you can select only the device group to which you are assigned.

   b) In the Please select a field field, open the list and select one of the following filter criterion:

      ○ **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 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

   c) If you want to show devices that meet specific criteria, enter the appropriate information in the remaining two fields. For example, you may want to show only those devices where the Username field begins with the letters Admin.

   Alternatively, to show all devices in the selected Device Group, leave these two fields blank.

   d) Click Filter. The Select devices dialog refreshes to show a list of devices that match your criteria.

   e) Select the appropriate devices by doing one of the following:
● To select individual devices, select the checkbox for each device.
● To select all devices shown on this page, select the checkbox in the header.
● To select all devices in this device group, hover your mouse over the down arrow in the checkbox in the header. Click the Select All <n> Records (where <n> is the number of records) to select all of the devices that meet the filter criteria you set earlier.

f) With the appropriate devices selected, click Select devices. The Request Device Freeze page refreshes with a list of all selected devices.

NOTE If you find that the list of selected devices includes devices that were included in error, you can remove these devices from the list. To remove such devices, click the Remove link in the last column for the appropriate device. The Request Device Freeze page refreshes to show the updated list of devices.

6. In the Select a message field, open the list and select the message you want to associate with this Device Freeze request. A preview of the message shows in the Preview of the message field.

7. In the Schedule Freeze Date area, click the field and select one of the following options to specify when you want the freeze to occur:
   ● To freeze the selected devices the next time they successfully connect to the Absolute Monitoring Center, select On next agent call.
   ● To schedule the selected devices to be frozen on a future date:
     i) Select On or after date.
     ii) In the date field, enter a date in the defined date format, or click the Calendar icon and select a date. Any future date within one year of the current date is supported.

NOTE Each device will be frozen on its first successful connection to the Absolute Monitoring Center on or after the selected date.

8. In the Select a Passcode Option area, do the following:
   a) Click the Select code length field and select the length of the passcode. The options are 4 digits and 8 digits.

NOTE If you are freezing one or more Android devices, select 4 digits.

b) Select one of the following options for generating the unfreeze passcode:
   ● Generate a different random passcode for each device to auto-generate and use a different unlock passcode for each of the targeted devices.
   ● Generate the same random passcode for each device to auto-generate and use the same unlock passcode for each of the targeted devices.
   ● Specify a numeric passcode of the selected length for each device to enter a custom passcode to use for all devices in this request. Enter the passcode in the field, ensuring that the length of the passcode matches the option you selected in step a.

For more information about the unfreeze passcode, see "Viewing the Unfreeze Passcode" on page 259.
9. If the **Custom Action Fields** area shows, complete the fields, as required, to add additional information about this Device Freeze request.

**NOTE** For more information about adding, editing, and removing Custom Action Fields, see "Managing Custom Action Fields" on page 203.

10. At the **Email Notification** area, do the following:

a) If you want to receive a notification when the Device Freeze status of any of the devices changes, select the **Send me status updates for each device** checkbox.

b) To send status update notifications to other users, in the field type the e-mail address of each contact, separated by a semicolon.

**NOTE** If the request applies to multiple devices, you may receive numerous email messages.

11. The **Force reboot before freezing device (Windows Devices Only)** checkbox is selected by default. This setting forces the device to reboot when the Device Freeze request is deployed, which prevents the current user from switching between applications and saving their work. It also enables the Device Freeze message to show on the device before a user attempts to log in to the operating system.

If your targeted device is running the Windows operating system, ensure that you leave this checkbox selected.

**NOTE** Devices running Mac operating systems automatically reboot when the Device Freeze request runs, regardless of whether this checkbox is selected or not.

12. At the **Consent to Install Software** area, select the checkbox to indicate that you consent to the installation of additional software components on the selected devices for the purpose of processing the Device Freeze.

13. Click **Submit**, to refresh the Request Device Freeze page and show the **Provide Authentication** area, where you do one of the following:

- If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
- If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.

For more information, see "Security Authentication Methods" on page 201.

14. Click **OK**.

The Device Freeze request is created.

**IMPORTANT** After you click **OK** on the Provide Authentication page, you cannot change the Device Freeze Request. However, you can cancel the request, provided it has was not started on the targeted device. See "Managing Custom Device Freeze Messages" on page 261.

15. If the request is not scheduled to occur at a future date and the device is RTT enabled, a dialog opens prompting you to force a call to the device using MCIC. If necessary, force a call to the device. For more information, see "Initiating a Forced Call" on page 188.
When the device receives and processes the SMS message, depending upon the Device Freeze defaults set for the account, the device freezes.

Depending on the option you selected in the Schedule Freeze Date area, one of the following scenarios applies:

- If you selected **On next agent call**, the request has a status of Freeze Requested and the device is frozen on the next successful agent call.
- If you selected **On or after date**, the request has a status of Scheduled Freeze Pending and the device will be frozen on the first successful agent call that occurs on or after the selected date.

### Cancelling a Device Freeze Request

You cannot file an Investigation Report for a stolen device until all outstanding freeze requests are completed or cancelled.

If the stolen device is frozen, you need to unfreeze it before you can submit an Investigation Report. To submit an unfreeze request to return the frozen device to an operational state, follow the task, "Unfreezing a Frozen Device" on page 258.

**IMPORTANT** You can cancel a Device Freeze request before it is deployed on the targeted device; therefore the Device Freeze request must have a status of **Freeze Requested, Scheduled Freeze Pending, or Freeze Scheduled.**

You can cancel the Device Freeze request for a single device or for multiple devices:

- [Cancelling a Device Freeze Request For a Single Device](#)
- [Cancelling Device Freeze Requests For Multiple Devices](#)

### Cancelling a Device Freeze Request For a Single Device

To cancel a Device Freeze request for a single device:

1. On the navigation bar click ✖️ > **Device Freeze** > **Device Freeze Summary Report**.
2. On the Device Freeze Summary Report page at the Search Criteria area, enter all appropriate criteria and click **Show results**.
   The Device Freeze Summary Report refreshes and the results grid shows a list of all devices for your account that contain a Device Freeze request.
3. At the far right side of the grid click the **Edit** or **View** link for the appropriate device.
4. The Device Freeze Details page opens to show the details for the selected request. Click **Cancel Request**. The Device Freeze request is cancelled.

### Cancelling Device Freeze Requests For Multiple Devices

To cancel the Device Freeze requests for multiple devices at the same time:

1. On the navigation bar click ✖️ > **Device Freeze** > **Device Freeze Summary Report**.
2. On the Device Freeze Summary Report page at the and the Device Freeze Status is area, select the **Frozen** checkbox and clear all other checkboxes.
3. Enter all other appropriate criteria and click **Show results**.
The Device Freeze Summary Report refreshes and the **results** grid shows a list of all devices for your account that match your search criteria.

4. Select the devices in one of the following ways:
   - **This Page Only**: in the leftmost column of the top row of the **results** grid select the checkbox to select only those devices that show on the current page of the Device Freeze Summary Report **results** grid.
   - **Select All Records**: hover your mouse over the list button in the leftmost column of the top row of the **results** grid and click the **Select All <n> Records** link, where <n> is the total number of devices that match your filter criteria. These devices show up on different pages of the Device Freeze Summary Report **results** grid.

The Device Freeze Summary Report refreshes to show the checkboxes for the selected devices checked.

5. Click **Edit selected devices** to open the Edit Selected Devices dialog.

6. In the **Action** column of the **Freeze Requested** row, open the list and select **Cancel Request**.

7. Click **Submit**. The Device Freeze requests for all selected devices are cancelled.

Removing Device Freeze Request Details

In certain circumstances, you may no longer need to save the details of a particular Device Freeze Request. Some examples include when a Device Freeze Request is cancelled or completed, or when the device is recovered successfully.

**WARNING!** Exercise caution when removing the details of a Device Freeze Request because when removed, you cannot restore these details.

You can remove the details of the Device Freeze Request for a single device or for multiple devices:

- Removing Details of a Single Device Freeze Request
- Removing Details of Multiple Device Freeze Requests

Removing Details of a Single Device Freeze Request

To remove details of a single Device Freeze Request:

1. On the navigation bar click **Device Freeze > Device Freeze Summary Report**.

2. On the Device Freeze Summary Report page enter all appropriate criteria and click **Show results**.

   The Device Freeze Summary Report refreshes and the **results** grid shows a list of all devices for your account that contain a Device Freeze request.

3. Click the **View** or **Edit** link for the appropriate request. The Device Freeze Details page opens to show the details for the selected request.

4. Click **Remove Details**. The Confirm Removal of Device Freeze Details page opens.

5. Click **OK**. The Device Freeze Request details are deleted from the Absolute console.
Removing Details of Multiple Device Freeze Requests

To remove details of multiple Device Freeze Requests:

1. On the navigation bar click  > Device Freeze > Device Freeze Summary Report.
2. On the Device Freeze Summary Report page at the and the Device Freeze Status is area, select the Unfrozen With Agent Call, Request Cancelled, and Unfrozen With Passcode checkboxes. Clear all other checkboxes.
3. Enter all other appropriate criteria on this page, and then click Show results.

The Device Freeze Summary Report refreshes and the results grid shows a list of all devices for your account that match each selected Device Freeze Status.

4. Select the devices in one of the following ways:
   - **This Page Only**: in the leftmost column of the top row of the results grid and select the checkbox to select only those devices that show on the current page of the Device Freeze Summary Report results grid.
   - **Select All Records** by hovering your mouse over the list button in the leftmost column of the top row of the results grid and clicking the Select All <n> Records link, where <n> is the total number of devices that match your filter criteria. These devices show up on different pages of the Device Freeze Summary Report results grid.

The Device Freeze Summary Report refreshes to show the selected devices.

5. Click Edit selected devices to open the Edit Selected Devices dialog.
6. In the Action list for each Device Status, select Remove Details.
7. Click Submit. The Device Freeze Request details for all selected devices are deleted from the Absolute console.

Managing Device Freeze Offline Policies

Authorized security personnel can create a Device Freeze offline policy to freeze devices that have not contacted the Monitoring Center for a specified number of days. Offline policies ensure that your managed devices are protected even when a device is powered off or a network connection is not available.

Depending on the needs of your organization, you may want to create one offline policy and apply it to all of your managed devices, or create multiple offline policies, with different settings, and assign groups of devices to each of them. You can also designate an offline policy as the default policy to apply automatically to newly activated devices.

A new offline policy is activated on its associated devices on the next agent call. The policy’s Timer then begins to count down on each device. You can set the Timer Period to any value between 4 days and 365 days, and it is reset after each successful agent call. If a device does not call the Monitoring Center before the Timer Period elapses, the device is frozen and an email notification is sent to the Security Administrator or Security Power User who created the offline policy.

Devices that are frozen by an offline policy are included on the Device Freeze Summary Report. You can view these devices and unfreeze them as required.

**NOTE** Device Freeze offline policies are supported on Windows devices only.
This section provides information on the following topics:

- Creating a Device Freeze Offline Policy
- Working with Existing Offline Policies
- Searching for a Device Freeze Offline Policy
- Editing a Device Freeze Offline Policy
- Designating a Default Offline Policy
- Managing Devices Associated with a Device Freeze Offline Policy
- Deleting a Device Freeze Offline Policy

Creating a Device Freeze Offline Policy

To create a Device Freeze offline policy and assign devices to it:

1. On the navigation bar click \ Device Freeze > Create a Device Freeze Offline Policy.\n

   A confirmation message indicates that an authorization code is requested and sent to your-email address. Check your e-mail for the message.

3. Under Policy information, enter the following information:
   a) Type a name in the Policy Name field and click the Check name availability link to verify that the name you typed is not in use.
   b) Enter a Policy Description.
   c) In the Timer Period field type the number of days that must elapse before a device associated with this policy is frozen. Values between 4 days and 365 days are supported.

4. Click the Freeze Message field and select the message you want to show on a device when it is frozen. The message text shows in the Preview of the message field.

   If the appropriate message does not exist, click the Create Message link to create a new one. For more information, see "Creating a Custom Device Freeze Message" on page 261.

5. Under Timer Action, select one of the following options:
   - Freeze immediately: After the Timer Period elapses, a forced restart occurs on the device to freeze it immediately.
   - Freeze on next restart: After the Timer Period elapses, the device is frozen the next time it is started. This is the default option.

6. In the Passcode Options area, select one of the following options:
   - Generate a different random passcode for each device to auto-generate and use a different unlock passcode for each of the targeted devices.
   - Generate the same random passcode for each device to auto-generate and use the same unlock passcode for each of the targeted devices.
   - Specify an 8-digit passcode for each device to use a previously generated or custom passcode. Click the field and enter (or copy and paste) the passcode to use on each device. For more information, see "Viewing the Unfreeze Passcode" on page 259.
7. If you want to assign this Device Freeze offline policy to each newly activated device, select the checkbox next to **Default policy for newly activated devices**.

If this option is disabled, another offline policy is already set as the default. To set this policy as the default, you need to remove this designation from the other policy and then set the option here. For more information, see "Designating a Default Offline Policy" on page 247.

8. Click **Save Policy** and in the Provide Authentication dialog, do one of the following:

- If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
- If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.

9. Click **OK**. A message confirms that the offline policy is created.

10. Do one of the following, depending on whether you want to associate devices with the offline policy:

- If you do not want to add devices at this time, click **Back**. The Manage Device Freeze Policies page opens. The status of the offline policy is set to Inactive until the policy is assigned to one or more devices. For more information about adding devices to an existing offline policy, see "Adding Devices to an Offline Policy" on page 249.

- If you want to add devices to the offline policy, do the following:
  i) If your Security Authentication Method is E-mailed Authorization Codes, you need to request a second authorization code to add devices to the new offline policy. Under Policy Members, at the Request Authorization Code area, click **Request Code**. A confirmation message indicates that an authorization code is requested and sent to your email address. Check your e-mail for the message.
  ii) Click **Add Devices**. A dialog opens.
  iii) On the **Choose devices to add to this policy** dialog, open the where Group is list and select the appropriate Device Group.

  **NOTE** If you are logged in as a Security Power User, you can select only the Device Group to which you are assigned.

  iv) In the **Please select a field** field, open the list and select a filter criterion.

  v) If you want to show devices that meet specific criteria, enter the appropriate information in the remaining two fields. For example, you may want to show only those devices where the **Username** field begins with the letters **Admin**. Alternatively, to show all devices in the selected Device Group, leave these remaining two fields blank.

  vi) By default, the list of devices in the **results** grid is limited to only those devices that are eligible for assignment to an offline policy. If you want to show all devices that match the criteria you specified, clear the **Show eligible devices only** checkbox.

  **NOTE** A device may be associated with only one offline policy.

  vii) Click **Filter**. The **Choose devices to add to this policy** dialog refreshes to show a list of devices matching your criteria.
viii) Select the devices that you want to add:
   ○ To select individual devices, select the checkbox next to each device you want to add.
   ○ To select all devices on this page of the table, select the Select All checkbox.

   **NOTE** You can change the number of records shown per page. For more information, see "Changing the Number of Records That Show in a Report" on page 80.

ix) Select the checkbox to indicate that you consent to the installation of additional software components on the selected devices to enable the Device Freeze offline policy.

x) Click Choose device(s) and in the Provide Authentication dialog, do one of the following:
   ○ If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
   ○ If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.

xi) Click **OK**.

The dialog closes and the results grid on the Manage Device Freeze Policies page refreshes to show the devices you added.

The policy is applied to the added devices on the next successful agent call. In the interim, each device's status is set to Assignment Pending.

Going forward, if a device fails to call the Monitoring Center before the Timer Period elapses, the device is frozen and an email notification is sent to the Security Administrator or Security Power User who created the offline policy.

**Working with Existing Offline Policies**

You can use the Manage Device Freeze Offline Policies page to create new offline policies, view and edit existing offline policies, and manage the devices associated with an offline policy.

To view the list of existing Device Freeze offline policies, and perform actions on them:

1. On the navigation bar click ** ↳ Device Freeze > Manage Device Freeze Offline Policies**.

The Manage Device Freeze Offline Policies page opens to show the list of existing policies. The following information shows in the table for each policy:
   - **Policy Name**: the name assigned to the policy.
   - **Device Count**: the number of devices associated with the policy.
   - **Description**: a description of the policy.
   - **Created By**: the username of the user who created the policy.
   - **Last Modified**: the date and time when the policy was last updated.
   - **Status**: the current status of the offline policy. Possible values are Active and Inactive.

   **NOTE** A status of Inactive indicates that the offline policy is deleted, but one or more of its associated devices have not yet called the Monitoring Center to receive the update. After all devices make an agent call, the policy is removed from the system. For more information, see "Deleting a Device Freeze Offline Policy" on page 251.
• **Default Policy:** you can set only one policy as the Default Policy. A value of Yes indicates that the policy is designated as the default policy to be assigned to all newly activated devices.

From the Manage Device Freeze Offline Policies page you can perform the following tasks if you are logged in as a Security Administrator or Security Power User:

• To search for an offline policy, enter **Search Criteria** and click **Show results**. For more information, see "Searching for a Device Freeze Offline Policy" on page 245.

• To open an offline policy for editing, in the **results** grid click the **Policy Name** link. For more information, see "Editing a Device Freeze Offline Policy" on page 245.

• To add or remove devices, in the **results** grid click the **Policy Name** link. For more information, see "Managing Devices Associated with a Device Freeze Offline Policy" on page 248.

• To create a new offline policy, click **New policy**. The Create and Edit Device Freeze Offline Policy page opens. For more information, see "Creating a Device Freeze Offline Policy" on page 242.

• To download the list of policies, click **Download**. For more information, see "Downloading Reports" on page 92.

• To print the current page of the list of policies, click **Print**. For more information, see "Printing Reports" on page 90.

• To save the filters you used to generate the list of policies, click **Save**. For more information, see "Saving Report Filters" on page 91.

**Searching for a Device Freeze Offline Policy**

To search for a Device Freeze offline policy:

1. On the navigation bar click **Device Freeze > Manage Device Freeze Offline Policies**.

2. On the Manage Device Freeze Offline Policies page, search for the policy that you want to view using any of the **Search Criteria** fields as follows:
   
   • In the **Policy Name is or contains** field, enter the name of the offline policy.
   
   • In the **and Policy Description is or contains** field, enter several letters that you know are in the offline policy description.
   
   • Click the field next to **or the policy contains a device where the field**, select the appropriate field from the list, and then in the **is or contains** field, either use **Choose** or enter the appropriate value for the offline policy you want to view.

3. Click **Show results**. The **results** grid refreshes to show the results of the search.

**Editing a Device Freeze Offline Policy**

You can change the settings for an offline policy at any time. If you make changes to the Timer Period, Freeze Message, or Timer Action settings, your changes are effective on the offline policy’s devices after the next agent call.
NOTE To change the devices associated with an offline policy, see "Managing Devices Associated with a Device Freeze Offline Policy" on page 248.

To edit a Device Freeze offline policy:

1. On the Manage Device Freeze Offline Policies page, search for the policy that you want to edit. See "Searching for a Device Freeze Offline Policy" on page 245.

2. In the results grid, click the Policy Name for the policy you want to edit. The Edit a Device Freeze Offline Policy page opens.

   A confirmation message indicates that an authorization code is requested and sent to your-email address. Check your e-mail for the message.

4. Under Policy information, edit the following information, as required:
   a) Edit the name in the Policy Name field and click the Check name availability link to verify that the name you typed is not in use.
   b) Edit the Policy Description.
   c) In the Timer Period field edit the number of days that must elapse before a device is frozen. Values between 4 days and 365 days are supported.

5. Click the Freeze Message field and select the message you want to show on a device when it is frozen. The message text shows in the Preview of the message field.
   If the appropriate message does not exist, click the Create Message link to create a new one. For more information, see "Creating a Custom Device Freeze Message" on page 261.

6. Under Timer Action, select one of the following options:
   ● Freeze immediately: After the Timer Period elapses, a forced restart occurs on the device to freeze the device immediately.
   ● Freeze on next restart: After the Timer Period elapses, the device is frozen the next time it is started. This is the default option.

7. A passcode is used to unfreeze a frozen device. In the Passcode Options area, select one of the following options:
   ● Generate a different random passcode for each device to auto-generate and use a different unlock passcode for each device.
   ● Generate the same random passcode for each device to auto-generate and use the same unlock passcode for each device.
   ● Specify an 8-digit passcode for each device to use a previously generated or custom passcode. Click the field and enter (or copy and paste) the passcode to use on each device. For more information, see "Viewing the Unfreeze Passcode" on page 259.

8. If you want to assign this offline policy to each newly activated device, select the checkbox next to Default policy for newly activated devices.
NOTE If this option is disabled, another Device Freeze offline policy is already set as the default policy. To set the policy you are editing as the default, you need to remove this designation from the other policy and then set the option here. For more information, see “Designating a Default Offline Policy” on page 247.

9. Click **Save Policy** and in the Provide Authentication dialog, do one of the following:
   - If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
   - If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.

10. Click **OK**. A message confirms that the policy is edited.
    The offline policy is updated on each device on the next agent call. In the interim, the device's status is set to Update Pending.

    **NOTE** If a device is frozen, the policy on that device is updated after the device is unfrozen.

### Designating a Default Offline Policy

You can designate an offline policy as the default policy to be assigned to all newly activated devices. You can set only one policy as the default policy.

To designate a policy as the default policy:

1. On the navigation bar click ↵ > **Device Freeze** > **Manage Device Freeze Offline Policies**.
   The Manage Device Freeze Offline Policies page opens to show the list of existing policies.

2. In the **results** grid, review the values in the **Default Policy** column to determine if a policy is already set as the Default Policy (column value is set to **Yes**).

3. Do one of the following:
   - If no policies are set as the default policy, go to step 4.
   - If an offline policy is set as the default policy and you want to designate another policy as the default, do the following:
     i) Click the **Policy Name** link of the policy that is currently set as the default policy. The Edit a Device Freeze Offline Policy page opens.
     ii) If your Security Authentication Method is E-mailed Authorization Codes, at the Request Authorization Code area, click **Request Code**.
        A confirmation message indicates that an authorization code is requested and sent to your email address. Check your e-mail for the message.
     iii) Clear the checkbox next to **Default policy for newly activated devices**.
     iv) Click **Save Policy** and in the Provide Authentication dialog, do one of the following:
        - If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
        - If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.
     v) Click **OK**.
4. Click the **Policy Name** link of the policy that you want to set as the default policy. The Edit a Device Freeze Offline Policy page opens.

5. If your Security Authentication Method is E-mailed Authorization Codes, at the Request Authorization Code area, click **Request Code**.
   A confirmation message indicates that an authorization code is requested and sent to your-email address. Check your e-mail for the message.

6. Select the checkbox next to **Default policy for newly activated devices**.

7. Click **Save Policy** and in the Provide Authentication dialog, do one of the following:
   - If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
   - If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.

8. Click **OK**.
   As new devices are activated, the offline policy is applied on each device. Going forward, if a device fails to call the Monitoring Center before the offline policy’s Timer Period elapses, the device is frozen automatically and an email notification is sent to the Security Administrator or Security Power User who created the offline policy.

**Managing Devices Associated with a Device Freeze Offline Policy**

You can view details about an offline policy’s devices. You can also add devices to an existing offline policy or remove devices.

**NOTE** You can associate a device with only one offline policy.

This section describes the following tasks:

- Viewing Devices Associated With an Offline Policy
- Adding Devices to an Offline Policy
- Removing Devices from an Offline Policy

**Viewing Devices Associated With an Offline Policy**

To view the devices associated with a Device Freeze offline policy:

1. On the Manage Device Freeze Offline Policies page, search for the offline policy that you want to view. For more information, see "Searching for a Device Freeze Offline Policy" on page 245.
2. In the **results** grid, click the appropriate **Policy Name** link to open the policy.
3. Scroll to the Policy Members area. The **results** grid shows the devices associated with this policy.
4. Review the list of devices and their associated device details. A device may have any of the following statuses:
   - **Assignment Pending**: the policy is assigned to the device in the Absolute console, but the device has not yet called the Monitoring Center. After a successful agent call, the offline policy is activated on the device and the device’s status is updated to Assigned.
   - **Assigned**: the offline policy is deployed to the device and the Timer is running.
1.  **Update Pending**: the offline policy was edited, but the device has not yet called the Monitoring Center. After a successful agent call, the offline policy is updated on the device and the status is updated to Assigned.

2.  **Removal Pending**: the device was removed from an offline policy, but the device has not yet called the Monitoring Center. After a successful agent call, the device is removed from the offline policy’s list of associated devices on the Manage Device Freeze Offline Policies page.

5.  To find a specific device, type an Identifier, Device Name, Username, or Serial Number in the text field and click **Filter Members**.

6.  To sort the list by specific information, such as Username, click the appropriate column header. To reverse the sort order, click the column header again.

### Adding Devices to an Offline Policy

You can add devices to an existing offline policy at any time. The policy is activated on the device at the next agent call.

**NOTE**  You can associate a device with only one offline policy.

To add devices to a Device Freeze offline policy:

1.  On the Manage Device Freeze Offline Policies page, search for the offline policy that you want to add devices to. See “Searching for a Device Freeze Offline Policy” on page 245.

2.  In the **results** grid, click the appropriate **Policy Name** link to open the offline policy.

3.  If your Security Authentication Method is E-mailed Authorization Codes, under Policy Members, at the Request Authorization Code area, click **Request Code**.

   A confirmation message indicates that an authorization code is requested and sent to your-email address. Check your e-mail for the message.

4.  The **results** grid shows the devices currently associated with this offline policy. Click **Add Devices**.

5.  On the **Choose devices to add to this policy** dialog, open the **where Group is** list and select the appropriate Device Group.

   **NOTE**  If you are logged in as a Security Power User, you can select only the Device Group to which you are assigned.

6.  In the **Please select a field** field, open the list and select a filter criterion.

7.  If you want to show devices that meet specific criteria, enter the appropriate information in the remaining two fields. For example, you may want to show only those devices where the **Username** field begins with the letters **Admin**.

   Alternatively, to show all devices in the selected Device Group, leave these two fields blank.

8.  By default, the list of devices in the **results** grid is limited to only those devices that are eligible for assignment to an offline policy. If you want to show all devices that match the criteria you specified, clear the **Show eligible devices only** checkbox.
9. Click **Filter**. The **Choose devices to add to this policy** dialog refreshes to show a list of devices matching your criteria.

10. Select the devices that you want to add:

   - To select individual devices, select the checkbox next to each device you want to add.
   - To select all devices on this page of the table, select the **Select All** checkbox.

   **NOTE** You can change the number of records shown per page. See "Changing the Number of Records That Show in a Report" on page 80.

11. Select the checkbox to indicate that you consent to the installation of additional software components on the selected devices to enable the Device Freeze offline policy.

12. Click **Choose devices** and in the Provide Authentication dialog, do one of the following:

   - If your Security Authentication Method is E-mailed Authorization Codes, enter your **Password** and **Authorization Code**.
   - If your Security Authentication Method is RSA SecurID tokens, enter your **Password** and **SecurID Token Code**.

13. Click **OK**.

   The dialog closes and the **results** grid refreshes to show the devices you added. The offline policy is assigned to each device on the next successful agent call. In the interim, the device’s status is set to Assignment Pending.

   Going forward, if a device fails to call the Monitoring Center before the offline policy’s Timer Period elapses, the device is frozen and an email notification is sent to the Security Administrator or Security Power User who created the offline policy.

**Removing Devices from an Offline Policy**

You may need to remove devices from an existing offline policy. For example, you cannot submit an Investigation Report on a device until the device is removed from its offline policy.

**NOTE** If a device’s status is Frozen By Policy, or a change to this status is imminent, you cannot remove the device from the offline policy.

To remove devices from a Device Freeze offline policy:

1. On the Manage Device Freeze Offline Policies page, search for the policy from which you want to remove devices. See "Searching for a Device Freeze Offline Policy" on page 245.

2. In the **results** grid, click the appropriate **Policy Name** link to open the offline policy.

3. Scroll to the Policy Members area. The **results** grid shows the devices associated with this offline policy.

4. Select the devices that you want to remove:

   - To select individual devices, select the checkbox next to each device you want to add.
   - To select all devices on this page of the table, select the **Select All** checkbox.

   **NOTE** You can change the number of records shown per page. See "Changing the Number of Records That Show in a Report" on page 80.
5. Click **Remove Selected Devices**.
   A message confirms that the selected devices are removed from the offline policy, but the offline policy is not removed from the device until the next successful agent call. In the interim, the device's status is set to Removal Pending.

**NOTE** Devices that are removed from an offline policy are not frozen if they are offline for a period of time. To ensure that your managed devices are protected at all times, add these removed devices to another offline policy.

Deleting a Device Freeze Offline Policy

If a Device Freeze offline policy is no longer required you can delete it.

When you delete an offline policy the policy’s status is set to Inactive while it waits for its devices to call the Monitoring Center and receive the update to the policy. After the policy is removed from all of its devices, the policy is deleted from the system.

**NOTE** The devices that were associated with a deleted policy are not frozen if they are offline for a period of time. To ensure that these devices are protected at all times, add these devices to another offline policy. For more information, see "Adding Devices to an Offline Policy" on page 249.

To delete a Device Freeze offline policy:

1. On the Manage Device Freeze Offline Policies page, search for the offline policy that you want to delete. See "Searching for a Device Freeze Offline Policy" on page 245.
2. In the results grid, click the appropriate **Policy Name** link to open the offline policy.
3. Click **Delete Policy**.
4. On the confirmation message click **Delete Policy**.

On the Manage Device Freeze Offline Policies page, the offline policy’s status is changed to Inactive and each device’s policy status is changed to Removal Pending.

On the next successful agent call the offline policy is removed from each device. After the offline policy is removed from all of the policy’s devices, the policy is deleted from the system.

**IMPORTANT** The policy cannot be removed from devices with a status of Frozen By Policy. You need to unfreeze these devices before the policy can be deleted. For more information about unfreezing frozen devices, see "Unfreezing a Frozen Device" on page 258.

Tracking Device Freeze Status

You can view near real-time status updates on the progress of Device Freeze requests and Device Freeze offline policies. The Device Freeze Summary Report shows all devices that have had a Device Freeze requested or are associated with an offline policy. You can filter this report by Device Freeze status to view specific devices.

**NOTE** To view an audit log of completed security actions related to Device Freeze requests, see "Security Audit Logs Report" on page 181. To export a report that provides statistics on Device Freeze requests submitted for your account, see "Security Posture Report" on page 151.
This section provides information on the following topics:

- Viewing Device Freeze Status
- Viewing Device Freeze Requests
- Viewing Devices Frozen by an Offline Policy

### Viewing Device Freeze Status

To view the status of all Device Freeze requests:

1. On the navigation bar click **Viewing** > **Device Freeze** > **Device Freeze Summary Report**.
2. On the Device Freeze Summary Report page at the **Search Criteria** area, set the preferred filtering and display options for the results 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.
   - If you are logged in as a Security Power User, you can select only the Device Group to which you are assigned.
   - To filter results by a specific Identifier, IMEI, Subscriber ID, Phone Number, Make, Model, Serial Number, or custom field (if applicable), in the **field** open the list and select the value type.
   - In the **is or contains** field enter the value to search for or use the **Choose** feature. For more information on the **Choose** feature, see "Editing Asset Information" on page 80.
   - To filter results by request name or policy name, in the **Request Name/Policy Name is or contains** field enter all or part of the name.
   - To filter results by the date the Device Freeze was requested, at the **Requested Date** area, do one of the following:
     - **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.
     - **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 by status, in the **Device Freeze Status is** area, select one or more checkboxes from these possible values:
     - **Freeze Requested**: the request was submitted and is in a transitory state when waiting for an agent call or when the instruction setup process is running on the targeted device.
     - **Frozen By Request**: the Device Freeze instructions were sent to the targeted device and the freeze message shows on the targeted device.
     - **Unfreeze Requested**: instructions to unfreeze the frozen device are queued and are sent to the device on the next agent call. This status is typically set when an unfreeze request is set using the Absolute console.
     - **Frozen By Policy**: the device was frozen by a Device Freeze offline policy because it did not make contact with the Monitoring Center before the policy’s Timer Period elapsed. The freeze message shows on the targeted device.
Chapter 10: Using Device Freeze

- **Unfrozen with Agent Call**: the device was unfrozen by sending an unfreeze request on the next agent call.
- **Request Cancelled**: the Device Freeze request was cancelled.
- **Unfrozen with Passcode**: the end user has unfrozen the device by entering a Passcode on the frozen device.
- **Pending**:
  - For Device Freeze requests, the request is pending because a Data Delete operation is being processed on the device. The device is frozen after the Data Delete operation is completed.
  - For offline policies, the policy is pending because a Device Freeze request was submitted on the device. After the request is processed, the status is changed to Policy Assigned.
- **Policy Assigned**: a Device Freeze offline policy is assigned to the device. If the device does not make contact with the Monitoring Center before the policy’s Timer Period elapses, the device is frozen.
- **Processing**: the Device Freeze request was sent to the device and is in progress.
- **Scheduled Freeze Pending**: the submitted Device Freeze request is scheduled to occur on or after a future date. When the scheduled date is reached, the status changes to Freeze Scheduled.
- **Freeze Scheduled**: the current date equals or exceeds the date on which the device is scheduled to be frozen. After the device makes a successful call to the Monitoring Center, the device is frozen.
- **Frozen by Scheduled Freeze**: the device was frozen by a Device Freeze request that was scheduled to occur on or after a specified date.

3. Click **Show results** to regenerate the report using the specified criteria.

The Device Freeze Summary Report shows all devices that have a Device Freeze requested. For each device listed, the Device Freeze Summary Report includes the following information:

- **Identifier**: the targeted device’s Identifier
- **Request ID**: the identifier assigned to the Device Freeze request by the system.
- **Request Name/Policy Name**: the name assigned to this Device Freeze request, or the name of the Device Freeze offline policy assigned to the device
- **Make**: the targeted device’s make
- **Model**: the targeted device’s model
- **Serial Number**: the targeted device’s serial number
- **IMEI**: the International Mobile Equipment Identity (IMEI) number of the device, if applicable
- **Subscriber ID**: the unique identifier associated with the subscriber at the time the Device Freeze was requested. This identifier is also known as the International Mobile Subscriber Identity (IMSI).
- **Phone Number**: the phone number associated with the mobile device, at the time the Device Freeze was requested
- **Requested on**: the date and time when the Device Freeze request was submitted
- **Requested By**: the username of the Security Administrator or Security Power User who submitted the request
• **Timer Period (days):** the duration of the Timer Period in number of days. Possible values are between 4 and 365 days. This column applies to only those devices that are associated with a Device Freeze offline policy.

• **Timer Action:** the action to perform if the Timer Period elapses on a device. This column applies to only those devices that are associated with a Device Freeze offline policy.

• **Status:** the current status of the device’s Device Freeze request or Device Freeze offline policy.

• **Scheduled for:** the date when a Device Freeze request is set to be processed. The device is frozen on the first successful agent call on or after this date.

| NOTE | The **Scheduled for** column applies only to Device Freeze requests that are scheduled to occur on or after a future date. See step 7 in "Requesting a Device Freeze" on page 236. |

• **Passcode:** the passcode used to unfreeze a device manually. For more information, see "Using an Unfreeze Passcode on the Targeted Device" on page 259.

| NOTE | If Custom Action Fields are associated with the Device Freeze request, a column for each custom field shows on the far right of the report. For more information, see "Managing Custom Action Fields" on page 203. |

You can perform the following additional tasks on the generated report, if desired:

• To download the report, click ✉️. For more information, see "Downloading Reports" on page 92.

| NOTE | Depending on your account, the Download icon may not be available. |

• To print the current page of the report, click Ⓟ. For more information, see "Printing Reports" on page 90.

• To save the filters you used to generate the report, click 🖼️. For more information, see "Saving Report Filters" on page 91.

**Viewing Device Freeze Requests**

To view the status and other details for a Device Freeze request:

1. On the navigation bar click ✉️ > **Device Freeze** > **Device Freeze Summary Report**.

2. On the Device Freeze Summary Report page enter all appropriate criteria to generate the report. See "Viewing Device Freeze Status" on page 252.

   The Device Freeze Summary Report refreshes and the **results** grid shows a list of all devices for your account that contain a Device Freeze request.

3. Do one of the following, depending on the status of the Device Freeze request:

   • If the status of the Device Freeze request is **Policy Assigned, Unfrozen With Agent Call, Unfrozen With Passcode,** or **Request Cancelled,** click the **View** link to open the Device Freeze Details page in a read-only state for the selected request.
If the status of the Device Freeze request is one of the following, click the Edit or View link to open the Device Freeze Details page in an editable state for the selected request:

- Freeze Requested
- Scheduled Freeze Pending
- Freeze Scheduled
- Frozen By Request
- Frozen By Policy
- Frozen By Scheduled Freeze
- Unfreeze Requested
- Pending

If the status of the Device Freeze request is Processing and you want to cancel the request, click Cancel.

Viewing Details about a Device Freeze Request

The Device Freeze Details page contains the following detailed information about the Device Freeze request:

- Current Status: the current status of the Device Freeze request. Possible values are:
  - Freeze Requested: the request was submitted and is in a transitory state when waiting for an agent call or when the instruction setup process is running on the targeted device.
  - Frozen By Request: the Device Freeze instructions are sent to the targeted device and the freeze message is shown on the targeted device.
  - Frozen By Policy: the device was frozen by a Device Freeze offline policy because it did not make contact with the Monitoring Center before the policy’s Timer Period elapsed. The freeze message shows on the targeted device.
  - Unfreeze Requested: instructions to unfreeze the frozen device are queued and are sent to the device on the next agent call. This status is typically set when an unfreeze request is set using the Absolute console.
  - Unfrozen with Agent Call: the device was unfrozen by sending an unfreeze request on the next agent call.
  - Unfrozen with Passcode: the end user has unfrozen the device by entering a Pass Code on the frozen device
  - Pending: the Device Freeze request is pending because a Data Delete operation is being processed on the device. The device is frozen after the Data Delete operation is completed.
  - Policy Assigned: a Device Freeze offline policy is assigned to the device. If the device does not make contact with the Monitoring Center before the policy’s Timer Period elapses, the device is frozen.
  - Processing: the Device Freeze request was sent to the device and is in progress. This status is used for Device Freeze requests for more than one device.
  - Request Cancelled: the Device Freeze request was cancelled before being deployed to the targeted device.
  - Scheduled Freeze Pending: A scheduled Device Freeze request was submitted for the device. The Device Freeze is scheduled to occur on or after a future date. When the scheduled date is reached, the status changes to Freeze Scheduled.
Chapter 10: Using Device Freeze

- **Freeze Scheduled**: A scheduled Device Freeze was submitted for the device. The current date equals or exceeds the date on which the device is scheduled to freeze. The device will be frozen after it makes a successful call to the Monitoring Center.
- **Frozen by Scheduled Freeze**: the device was frozen by a Device Freeze request that was scheduled to occur on or after a specified date.

- **Scheduled for**: the date when the Device Freeze request is set to be processed. The device is frozen on the first successful agent call on or after this date.

**NOTE** The Scheduled for field applies only to Device Freeze requests that are scheduled to occur on or after a future date. See step 7 in "Requesting a Device Freeze" on page 236.

- **Identifier**: the targeted device’s Identifier
- **IMEI**: the International Mobile Equipment Identity number of the device, if applicable
- **Subscriber ID**: the unique identifier associated with the subscriber at the time the Device Freeze was requested. This identifier is also known as the International Mobile Subscriber Identity (IMSI).
- **Phone Number**: the phone number associated with the mobile device, at the time the Device Freeze was requested
- **Make**: the targeted device’s make and manufacturer name
- **Model**: the targeted device’s model
- **Serial**: the targeted device’s serial number
- **Asset**: the targeted device’s inventory tracking or asset number as assigned by the network administrator in the organization
- **Last Call**: the date and time of the device’s last agent call to the Monitoring Center
- **Unfreeze Passcode**: the passcode used to unfreeze a device manually. For more information, see "Using an Unfreeze Passcode on the Targeted Device" on page 259.
- **[Custom Action Fields]**: shows the value for each custom field, if one or more Custom Action Fields are associated with the Device Freeze Delete request. For more information, see "Managing Custom Action Fields" on page 203.
- **Status table**: the detailed information about the freeze/unfreeze activity on the targeted device. The following information is shown:
  - **Step**: the sequential number of the status change
  - **Status**: the status of the Freeze Request
  - **Date**: the date and time when the change in status occurred
  - **Username**: the username of the Security Administrator or Security Power User who requested the status change

In addition to this information, the Device Freeze Details page contains the following buttons letting you perform additional tasks, such as:

- **Unfreeze device**: click to unfreeze a frozen device on the next agent call. For more information, see "Unfreezing a Device on Agent Call" on page 258.
- **Cancel request**: click to cancel a Device Freeze request before the device is frozen. For more information, see "Managing Custom Device Freeze Messages" on page 261.
- **Remove details**: click to remove the details of a Device Freeze Request. For more information, see "Removing Device Freeze Request Details" on page 240.
Viewing Devices Frozen by an Offline Policy

When an offline policy is assigned to a device, and the device fails to contact the Monitoring Center for the number of days specified in the offline policy’s Timer Period, the device is frozen. Administrators receive a daily email notification listing the devices that were frozen by an offline policy during the past 24 hours.

**NOTE** After an e-mail notification is sent for a device no further e-mails are sent, regardless of how many days the device remains frozen.

In the Device Freeze Summary report, you can view a list of all devices that are currently frozen by an offline policy and determine which ones you want to unfreeze, and which require further action.

To view devices that are frozen by an offline policy:

1. On the navigation bar click ☰ > Device Freeze > Device Freeze Summary Report.
2. In the Search Criteria location, clear all checkboxes in the and the Device Freeze Status is area except Frozen By Policy.
3. Click Show results. The results grid refreshes to show only those devices that are frozen because they have not contacted the Monitoring Center for the number of days specified in their policy’s Timer Period.
4. To sort the results by Policy Name, Timer Period, or Timer Action, click the appropriate column header.
5. To view details about the frozen device, click the Edit or View link. The Device Freeze Details page opens and shows the following information:
   - **Current Status**: shows Frozen By Policy, which is the current status of the frozen device
   - **Identifier**: the device’s Identifier
   - **IMEI**: not applicable to Windows devices
   - **Subscriber ID**: the unique identifier associated with the subscriber at the time the Device Freeze was requested. This identifier is also known as the International Mobile Subscriber Identity (IMSI)
   - **Phone Number**: not applicable to Windows devices
   - **Make**: the device’s make and manufacturer name
   - **Model**: the device’s model
   - **Serial**: the device’s serial number
   - **Asset**: the device’s inventory tracking or asset number as assigned by the network administrator in the organization
   - **Last Call**: the date and time of the device’s last agent call to the Monitoring Center.
   - **Unfreeze Passcode**: the passcode used to unfreeze a device manually. For more information, see "Using an Unfreeze Passcode on the Targeted Device" on page 259.
   - **Status** table: the detailed information about the freeze/unfreeze activity on the targeted device. The following information is shown:
     - **Step**: the sequence number of the status change
     - **Status**: the status of the device’s offline policy
     - **Date**: the date and time when the change in status occurred
Chapter 10: Using Device Freeze

- **Username:** the username of the Security Administrator or Security Power User who requested the status change

In addition to this information, the Device Freeze Details page includes an **Unfreeze device** button to unfreeze a frozen device on the next agent call. For more information, see "Unfreezing a Device on Agent Call" on page 258.

Unfreezing a Frozen Device

Devices can be frozen by a Device Freeze request or a Device Freeze offline policy. Authorized security personnel can unfreeze a device and make it operational in the following two ways:

- [Unfreezing a Device on Agent Call](#)
- [Using an Unfreeze Passcode on the Targeted Device](#)

**IMPORTANT** Unfreezing a device forces its operating system to restart.

**NOTE** You can create an Alert to notify you when a device is unfrozen. For more information, see "Creating New Custom Alerts" on page 19.

Unfreezing a Device on Agent Call

Authorized security personnel can unfreeze a device from the Device Freeze Details page. When the Unfreeze request is set, the targeted device is unfrozen on the next agent call to the Monitoring Center. When a device is frozen, the agent calls the Monitoring Center every 9 minutes.

This section provides instructions for the following tasks:

- [Unfreezing a Single Device on Agent Call](#)
- [Unfreezing Multiple Devices on Agent Call](#)

**NOTE** When an Android device with no screen lock protection (PIN or password) is frozen, its lock screen PIN is automatically set to 1234. When you unfreeze the device one of two scenarios applies, depending on the type of Android device:

- If the device **supports Persistence Technology**, and is running Android 7 or higher, the user receives a notification that they need to enter **1234** to unlock the device. The user can then go to Settings to remove or reset the PIN.
- For all other devices, the PIN is cleared when the device is unfrozen.

Unfreezing a Single Device on Agent Call

To unfreeze a single targeted device using the Absolute console:

1. On the navigation bar click **>` Device Freeze > Device Freeze Summary Report**.
2. On the Device Freeze Summary Report page enter all appropriate criteria and click **Show results**. The Device Freeze Summary Report refreshes to show a list of all devices for your account matching your search criteria in the **results** grid.

**NOTE** Security Power Users can unfreeze only those devices that belong to the Device Group to which they are assigned.
3. For the appropriate device, click the Edit or View link.
4. On the Device Freeze Details page click Unfreeze device. The device is unfrozen on the next agent call.

Unfreezing Multiple Devices on Agent Call

To unfreeze multiple targeted devices at the same time using the Absolute console:

1. On the navigation bar click  > Device Freeze > Device Freeze Summary Report.
2. On the Device Freeze Summary Report page at the and the Device Freeze Status is area, select the Frozen checkbox.
3. Enter all other appropriate criteria on this page and click Show results. The Device Freeze Summary Report refreshes to show a list of all frozen devices for your account matching your search criteria in the results grid.
4. Do one of the following:
   ● To select all devices on the current page of the results grid, select the checkbox in the header of the leftmost column. All devices on the page are selected.
   ● To select all devices in the results grid, hover your mouse over the checkbox in the header of the leftmost column and click Select All <n> Records. All devices in the report are selected.
5. Click Edit selected devices.
6. On the Edit Selected Devices page, in the Action list for the Frozen row, click the field and select Unfreeze.
7. Click Submit. The device is unfrozen on the next agent call.

Using an Unfreeze Passcode on the Targeted Device

Most frozen devices call in to the Monitoring Center every 9 minutes. In cases where the device is unable to make agent calls, it is possible to unfreeze the device manually.

This section provides information on the following topics:
   ● Viewing the Unfreeze Passcode
   ● Unfreezing a Device With a Passcode

Viewing the Unfreeze Passcode

In some circumstances, it is not feasible to wait for the next agent call to unfreeze a device. In such cases, it is possible to unfreeze a device by entering a passcode on the frozen device. The passcode is generated when the Device Freeze request is created and is shown on the Device Freeze Details page.

To view the unfreeze Passcode associated with a Device Freeze request:

1. On the navigation bar click  > Device Freeze > Device Freeze > Device Freeze Summary Report.
2. On the Device Freeze Summary Report page enter all appropriate criteria and click Show results.
The Device Freeze Summary Report refreshes and the results grid shows a list of all devices for your account that contain a Device Freeze request.

3. Click the Edit or View link for the appropriate device. The Device Freeze Details page opens to show the details for the selected request.

4. Record the Unfreeze Passcode.

The next step is to enter the passcode on the frozen device. For more information, see "Using an Unfreeze Passcode on the Targeted Device" on page 259.

Unfreezing a Device With a Passcode

To unfreeze a device manually:

1. The user contacts their organization’s Customer Support, or a Security Administrator or Security Power User for their account, to initiate a manual unfreeze request.

2. The Security Administrator or Security Power User provides the passcode to the user with detailed instructions about unfreezing the device. For more information on finding a device’s Unfreeze Passcode, see “Viewing the Unfreeze Passcode” on page 259.

3. The user unfreezes the device as follows:
   - For Windows devices:
     i) On the frozen device (which does not show any supporting fields to facilitate code entry) press the Esc key on the keyboard.
     ii) Enter the Passcode using the number keys in the upper row of the keyboard. If you enter the Passcode using the numeric keypad, the frozen device does not unfreeze. The device is immediately unfrozen.
   - For Mac devices:
     i) On the frozen device (which does not show any supporting fields to facilitate code entry) press the Esc key on the keyboard.
     ii) Enter the Passcode using the number keys in the upper row of the keyboard. If you enter the Passcode using the numeric keypad, the frozen device does not unfreeze.
     iii) Press the return key on the keyboard. The device is immediately unfrozen.
   - For Android devices:
     i) Power on the frozen device.
     ii) If the full screen Device Freeze message shows, click Unfreeze Device at the bottom of the message.
     iii) In the Enter Unfreeze Code field, enter the device’s Unfreeze Passcode you recorded in step 4 of the section, Viewing the Unfreeze Passcode. The device is immediately unfrozen.
     iv) Do one of the following:
        o If a PIN or password was set on the device before it was frozen, unlock the device as you normally would.
        o If there was no PIN or password set on the device before it was frozen, a notification message may show indicating that the device’s screen lock PIN is now set to 1234. Click OK and enter 1234 to unlock the device. To remove or reset the PIN, go to Settings.
Managing Custom Device Freeze Messages

Authorized security personnel can create and edit custom Device Freeze messages using a combination of plain text and HTML formatting. Custom messages help you ensure that the appropriate information is available to the users of a frozen device. Such messages typically state that the device has been frozen and may include instructions and contact information to help an authorized user restore functionality to their frozen device.

This section provides instructions for the following tasks:

- Creating a Custom Device Freeze Message
- Including Phone Numbers in Custom Device Freeze Messages
- Editing Existing Custom Device Freeze Messages
- Deleting Existing Custom Device Freeze Messages

Creating a Custom Device Freeze Message

**NOTE** If you intend to include a contact phone number in a Device Freeze message that shows on Android devices, also see "Including Phone Numbers in Custom Device Freeze Messages " on page 262.

To create a custom Device Freeze message:

1. On the navigation bar click &amp;gt; Device Freeze &gt; Device Freeze &gt; Create Device Freeze Message.

   **NOTE** Alternatively, you can also click New message on the Manage Device Freeze Messages page to open the Create Device Freeze Message page.

2. On the Create Device Freeze Message page in the Message Name field, type an appropriate title for the new Device Freeze message. The title shows as an option in the Select a message list on the Request Device Freeze page.

3. In the Message Text field, type the text you want to show on frozen devices. You can use plain text or a combination of text and the following HTML formatting tags:

<table>
<thead>
<tr>
<th>HTML tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;body&gt;</code>, including <code>&lt;body bgcolor&gt;</code></td>
<td>Apply a style, such as a background color, to your entire message</td>
</tr>
<tr>
<td><code>&lt;img src&gt;</code></td>
<td>Insert an image</td>
</tr>
<tr>
<td><code>&lt;b&gt;</code></td>
<td>Bold text</td>
</tr>
<tr>
<td><code>&lt;i&gt;</code></td>
<td>Italicize text</td>
</tr>
<tr>
<td><code>&lt;u&gt;</code></td>
<td>Underline text</td>
</tr>
<tr>
<td><code>&lt;font face=&quot;font_family&quot;/&gt;</code></td>
<td>Specify the font to apply to text</td>
</tr>
<tr>
<td><code>&lt;p&gt;</code></td>
<td>Define a paragraph with default spacing before and after text</td>
</tr>
<tr>
<td><code>&lt;p align&gt;</code></td>
<td>Set the alignment for a paragraph</td>
</tr>
<tr>
<td><code>&lt;center&gt;</code></td>
<td>Center a paragraph</td>
</tr>
<tr>
<td><code>&lt;br&gt;</code></td>
<td>Add a line break without default spacing</td>
</tr>
</tbody>
</table>
You can also include the following device attributes in your message:

<table>
<thead>
<tr>
<th>Device attribute</th>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMEI</td>
<td>[%IMEI%]</td>
<td>Insert an Android device's IMEI. When you preview the message, the variable is replaced by a sample value.</td>
</tr>
<tr>
<td>IMSI</td>
<td>[%IMSI%]</td>
<td>Insert an Android device's IMSI (also known as Subscriber ID). When you preview the message, the variable is replaced by a sample value.</td>
</tr>
<tr>
<td>Detected Phone Number</td>
<td>[%Detected Phone Number%]</td>
<td>Insert an Android device's Detected Phone Number. When you preview the message, the variable is replaced by a sample value.</td>
</tr>
<tr>
<td>Detected Serial Number</td>
<td>[%Detected Serial Number%]</td>
<td>Insert the target device's Detected Serial Number. When you preview the message, the variable is replaced by a sample value.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>[%Serial Number%]</td>
<td>Insert the target device's Serial Number. When you preview the message, the variable is replaced by a sample value.</td>
</tr>
<tr>
<td>Any Fixed Field</td>
<td>[%CDF:&lt;Fixed Field Name&gt;%]</td>
<td>Insert the target device's value for the specified Fixed Field.</td>
</tr>
<tr>
<td>Any Custom Device Field</td>
<td>[%CDF:&lt;Custom Device Field Name&gt;%]</td>
<td>Insert the target device's value for the specified Custom Device Field.</td>
</tr>
</tbody>
</table>

4. Click **Save**. The new message is saved and the Create Device Freeze Message page refreshes to show a confirmation message.

**Including Phone Numbers in Custom Device Freeze Messages**

*NOTE* This section applies only to Android devices running the Absoluteagent version 3219 or higher.

You can include a contact phone number in a Device Freeze message that allows the user of a frozen Android device to tap the hyperlinked phone number and place a call directly to that number. This feature is intended to allow users to use their frozen Android device to call for assistance, even though their device is otherwise unusable.

To include a phone number in a custom Device Freeze message:
1. On the navigation bar click > Device Freeze > Create Device Freeze Message.

2. On the Create Device Freeze Message page in the Message Name field, type an appropriate title for the new Device Freeze message.

3. In the Message Text field, type the text you want to show on frozen Android devices, including a contact phone number. Only international phone numbers are supported, in the following format: 

   +<country code> <phone number>

   For example, +33 509 758 351 or +1 555-1234

   The phone number must contain a minimum of eight (8) digits, not including the leading plus sign (+). It can include spaces ( ) or hyphens (-) for readability.

   Alternatively, you can create a Custom Device Field that includes the contact phone number and then include the field in the Device Freeze message. The phone number format requirements described above also apply. For more information about creating a Custom Device Field, see the online Help.

   **NOTE** Only those phone numbers that adhere to the defined format requirements will be hyperlinked and tappable on an Android device.

4. Click Save. The new message is saved and the Create Device Freeze Message page refreshes to show a confirmation message.

**Editing Existing Custom Device Freeze Messages**

To edit existing Device Freeze messages:

1. On the navigation bar click > Device Freeze > Manage Device Freeze Messages.

   The Manage Device Freeze Messages page opens to show a list of all messages available for your account.

2. Click the Message Name or the Edit link for the message you want to edit.

3. On the Create Device Freeze Message page at the Message Text field, edit the message as appropriate.

4. Click Save.

   The change is saved and the Create Device Freeze Message page refreshes to show a confirmation message.

**Deleting Existing Custom Device Freeze Messages**

To delete existing Device Freeze messages:

1. On the navigation bar click > Device Freeze > Manage Device Freeze Messages.

   The Manage Device Freeze Messages page opens to show a list of all messages available for your account.
2. Click the **Message Name** or the **Edit** link for the message you want to delete.

3. Click **Delete**. The message is deleted and the Create Device Freeze Message page refreshes to show a confirmation message.
Chapter 11: Managing Geofences

Administrators can use the Geofences feature to specify boundaries based on Geolocation Tracking data to track monitored devices.

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

The Geolocation Tracking and Geofences features let your organization determine the physical location of a specific computing device, more precisely and immediately, as of the most recent agent call to the Monitoring Center. It is also assumed that the device is properly equipped with a positioning device approved for use with these features.

An Administrator can specify boundaries using the Geofences Editor and track the movement of devices through these locations. Whenever a device crosses a boundary set using the Geofences feature, alerts are triggered and, depending upon the settings specified for the account, result in e-mail notifications to administrators and/or other events on the Absolute console. Geofencing is available to all accounts authorized for the Geolocation Tracking feature. Further, Geofencing is supported for all agents (devices) in that account for which Geolocation Tracking data is available.

For information about geolocation system requirements, see "Understanding Location Technologies" on page 162.

This chapter includes the following sections:

- Geofencing Security
- Using Geofence Technology
- Understanding Geolocation Maps
- Creating Geofences
- Viewing Geofences
- Editing Geofences
- Deleting Geofences

Geofencing Security

Due to the sensitive nature of the Geolocation Tracking and Geofencing features, several security checks are implemented to ensure the service is only initiated by authorized individuals and that it only runs on correctly targeted devices:

- Absolute must have a signed authorization agreement on file for your company.
- The device must have an activated agent with a unique Identifier and valid Geolocation Tracking data to be assigned to a Geofence area.

Authorizing Geolocation Tracking

Absolute must have a signed authorization agreement for your company on file before you can use the Geolocation Tracking and Geofences features.
The Geolocation Authorization Agreement provides several forms to gather specific information for your organization.

- Complete the Security Administration and Geolocation Authorization Form to specify the Security Administrators for your account who are authorized to use the advanced security operations included in your Absolute product and to track and monitor devices.
- Complete the Geolocation Tracking Activation section to indicate whether or not your organization is going to use Geolocation and, if so, will you enable all devices or only specific devices to use this feature.
- Complete the Authorization and Signatures section to specify the Signing Officers in your company who agree to your organization’s use of the advanced security operations according to the terms of this agreement.

To download a blank copy of the authorization agreement follow the instructions in the task, "Downloading and Submitting the Authorization Agreement" on page 198.

Using Geofence Technology

Geofences are used primarily as building blocks of security policies based on the location of devices. Geofences, in combination with Geolocation Tracking, can be used to pinpoint the location of a device and consequently ensure that the security of these devices is not breached. For example, a Geofence specifying the entire state of New York as a secure zone and an accompanying alert in the Absolute console are created for Account A. When one of the devices in Account A travels outside New York state, all administrators for that account are alerted through an automated notification e-mail. Depending upon the location and the secure status of the device, the Administrator can then choose to implement other security measures, such as performing a Data Delete or requesting a Device Freeze.

To use Geofences effectively, you first create a Geofence and then create an alert that links to the Geofence. When you create an alert for a Geofence, you need to specify the rules for triggering the alert based on the following options:

- **Location:**
  - **Outside:** Create an alert when a device travels outside a specified Geofence boundary.
  - **Inside:** Create an alert when a device travels inside a specified Geofence boundary.

- **Geofence Name:** The Geofence to which the alert pertains.

- **Duration:** The length of time after the specified rules are broken required to trigger the alert. You can specify the length of time in hours, days or weeks.

To set up a functioning Geofence:

1. Create an appropriate Geofence using the Create and Edit Geofences page. For more information, see "Creating Geofences" on page 268.

   **NOTE** If a Geofence matching your criteria already exists, you do not need to create a new one.

2. Create an alert based on the newly created Geofence using the Create and Edit Alerts page. In the **Field** list, select the value **Location**, and then specify the appropriate rules.

   For more information on creating Alerts, see "Creating New Custom Alerts" on page 19.
Understanding Geolocation Maps

Geolocation maps show on any geolocation pages within the Absolute console. These pages include:

- The **Create and Edit Geofences** page, which includes the Geofence Editor. You can use the Geofence Editor to add, edit, and find Geofences on a map.
- **Geolocation Tracking reports**, which provide location information about your devices. The Geofences created for your account show on Geolocation Tracking reports. For more information, see "Geolocation Tracking Reports" on page 161.

**NOTE** The Geofence Editor and Geolocation Tracking reports use Google Maps™. If Google Maps are prohibited in your country (determined by the IP address of your computer), ESRI® maps are used instead. For more information about working with ESRI maps, go to [www.esri.com](http://www.esri.com).

Map Navigation Tools

The following Google Map navigation tools are available:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pan</td>
<td>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.</td>
</tr>
<tr>
<td>Zoom</td>
<td>Use the Zoom tool to zoom in or out of specific areas of the map.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• To zoom out, click - repeatedly, or move the slider towards the button. You can zoom out by moving your mouse scroll wheel.</td>
</tr>
<tr>
<td>Map</td>
<td>Satellite picker</td>
</tr>
<tr>
<td></td>
<td>• To show a street map, click Map. This is the default option.</td>
</tr>
<tr>
<td></td>
<td>• To show a street map with terrain and vegetation information, click Map and select Terrain.</td>
</tr>
<tr>
<td></td>
<td>• To show a map of satellite images click Satellite.</td>
</tr>
<tr>
<td></td>
<td>• To show a map of satellite images with place names, click Satellite and select Labels.</td>
</tr>
</tbody>
</table>

Geofence Tools

The following controls are available to add, edit, and find Geofences:

<table>
<thead>
<tr>
<th>Geofence tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to Address</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Creating Geofences

You can use the Create and Edit Geofences page to define the boundaries of a new Geofence.

A Geofence can include a single boundary polygon that covers one area, or you can draw multiple polygons to include several areas in a single Geofence.

**IMPORTANT** The following instructions presume that you have already downloaded the Geolocation Authorization Agreement from the Support page in the Absolute console, signed it, and delivered it to Absolute. For more information, see "Downloading and Submitting the Authorization Agreement" on page 198. Also, the first time you access any geolocation page in a session, a confirmation page prompts you to accept the Terms and Conditions of use.

To create a Geofence for devices in your account:

1. On the quick access toolbar, click 🗺️ and click Geofence.

2. On the Geolocation Tracking page, read the information and if you agree click Accept the use of the Geolocation Tracking feature.

3. On the Create and Edit Geofences page, in the **Geofence Name** and **Geofence Description** fields, enter a name and description for the new Geofence.

4. To consider only collected device locations that have a high probability of being accurate in relation to the Geofence, select Only test locations with high Confidence Levels against Geofence boundaries in the Applicable Confidence Levels area.

5. In the **Applicable Location Technologies** area, select the location technologies that you want to apply to the Geofence. For more information on location technologies, see "Understanding Location Technologies" on page 162.
If the Google Maps™ Wi-Fi Positioning option is grayed out, this location technology is not enabled for the devices in your account. To enable this technology for all new and existing Geofences, see "Editing Classic Account Settings" on page 54.

**IMPORTANT** IP Georesolution is accurate to the city level at best and varies from the city level to country level. Therefore, do not enable IP Georesolution for small Geofences.

6. Create a boundary polygon using the map and tools in the Geofence Editor, as follows:
   a) Use the map navigation tools to show the area on the map where you want to create a boundary. For more information about using the navigation tools, see "Map Navigation Tools" on page 267.
   b) Click 🗺.
   c) Click the location on the map where you want to start the polygon.
   d) Click the location on the map where you want to create the first corner. The first side of the polygon is added to the map.
   e) Use the method described in step d to create each side of the polygon, except the final side.
   f) To complete the polygon, double-click the end point of the last side you created. The polygon is closed.

**IMPORTANT** The lines of a boundary polygon cannot cross or intersect, except at the end points. To compensate for accuracy limitations of location technology, draw a slightly larger boundary polygon than is required.

7. Repeat step 6 for each boundary polygon that you want to include in this Geofence.

8. Click Save.
   The View and Manage Geofences page opens with the new Geofence shown in the Geofences table. Geofences that are too small to show accurately at a particular zoom level show on the map as small round markers.

**Viewing Geofences**

The View and Manage Geofences page lets you view a summary of all Geofences matching specified search criteria.

To view a list of existing Geofences for your account:

1. View the Geofences created for your account by doing one of the following:
   - On the quick access toolbar, click 🌍 and click Geofences.
     When prompted, accept the use of the Geolocation Tracking feature.
     On the Create and Edit Geofences page, click Cancel, which opens the View and Manage Geofences page where you see a table of all of the Geofences for your account.
   - On the navigation bar click 🗺 and click Geofences.
     The sidebar provides a list of each Geofence created for your account.
2. On the View and Manage Geofences page, in the Geofence Name field, enter all of or part of the Geofence name that you want to view, and click Show results.

   The View and Manage Geofences page refreshes to show a list of all Geofences matching the search criteria in the results grid.

3. Click the Name link, which opens the Create and Edit Geofences page for the selected Geofence.

### Editing Geofences

You can edit a Geofence’s properties and settings. You can also use the Geofence Editor to move, reshape, and delete boundary polygons for an existing Geofence.

To edit an existing Geofence:

1. Open the Geofence that you want to edit by doing one of the following:
   - From the View and Manage Geofences page, click the name of the Geofence you want to edit.
   - From the list of Geofences presented on the sidebar, click the Geofence you want to edit.

   For more information, see "Viewing Geofences" on page 269.

2. On the Create and Edit Geofences page (that shows a Delete option), edit the values in the Geofence Name and Geofence Description fields, if required.

3. Update the selections in the Applicable Confidence Levels area and the Applicable Location Technologies area, if required.

4. To change the size or shape of a boundary polygon:
   a) Click .
   b) Click the polygon you want to edit. Handles show at the corners of the polygon and on the center points of each line.
   c) Click a handle and drag it to its new location. To undo a change click .
   d) Repeat step c until the polygon is the required size and shape.

5. To move a boundary polygon:
   a) Click .
   b) Click the polygon you want to edit. Handles show at the corners of the polygon and on the center points of each line.
   c) Click anywhere in the polygon and drag it to its new location.

6. To remove a boundary polygon:
   a) Click .
   b) Click the polygon you want to remove.

7. Click Save. The Geofence data is updated and the View and Manage Geofences page opens to show the edited values in the results grid.
Deleting Geofences

**IMPORTANT** You cannot delete Geofences that are associated with one or more alerts.

To delete a Geofence:

1. Open the Geofence that you want to delete. For more information, see "Viewing Geofences" on page 269.

2. On the Create and Edit Geofences page click **Delete**. The View and Manage Geofences page opens and the Geofence is deleted from the **results** grid.
Chapter 12: Using Remote File Retrieval

The Remote File Retrieval feature allows Security Administrators and Security Power Users to remotely retrieve files that may contain important information from the Windows devices in your account.

This chapter provides information on the following topics:
- Minimum System Requirements
- Before You Begin
- Requesting a Remote File Retrieval
- Viewing the File Retrieval Status
- Downloading Retrieved Files
- Changing the File Retrieval Status

IMPORTANT All tasks in this chapter require that you log in to the Absolute console as a Security Administrator or Security Power User.

Minimum System Requirements

Remote File Retrieval is available for devices that meet the following system requirements:
- Windows operating system: The targeted device must have one of the supported Windows Operating Systems installed. For more information, open the Absolute console's help system and search for supported platforms for managed devices.
- Current version of the Absolute agent for Windows devices.

NOTE The Remote File Retrieval feature is supported on Windows devices only.

Before You Begin

These are some important considerations to make before you request a Remote File Retrieval, such as:
- Stolen Devices: You can only retrieve the files that were created before the Incident Date recorded on the devices Investigation Report.
- File Paths: You need file paths using the File List feature to specify the files to retrieve. For more information, see "Using File List" on page 278.
- File Size: You can make Remote File Retrieval requests for files under 2 GB in size. However, for files larger than 1 GB in size, the chances of successful file retrieval diminish.
- Outstanding Data Delete Requests: You cannot choose a device that already has an outstanding Data Delete request. You must either cancel that outstanding request or wait for it to complete. For more information, see "Deleting or Cancelling a Data Delete Request" on page 229.
- Number of Files: You can retrieve up to 20 files per request.
- Accessibility of Retrieved Files: You can access and download the retrieved files for 30 days after the files are retrieved. After 30 days, the files are no longer available.
Requesting a Remote File Retrieval

To request a Remote File Retrieval:

1. On the quick access toolbar, click [ ] and click Request File Retrieval.
2. On the Request File Retrieval page in the Request Name field, type an appropriate name for the new request.
3. In the Select a Device area, click Choose to open the list and select the appropriate device.
   Click the appropriate device Identifier to select it. The Choose dialog closes and the Request File Retrieval page refreshes to show the selected device.
4. In the File Path to Retrieve field, specify the path of the file you want to retrieve.
5. Click Add. The path is added to the File Path list.
   Repeat to add multiple paths to the list.

   **NOTE** To remove a path from the list, click Remove next to the path you want to remove.

6. Read the Legal Notice carefully and select the I agree checkbox to indicate that you have read the notice and agree to the terms, and have the authority to take this action.
7. Click Submit.
   The Remote File Retrieval request is created and is deployed to the device on its next agent call.

Viewing the File Retrieval Status

You can view near real-time status updates on the progress of Remote File Retrieval requests. The File Retrieval Summary Report provides a list of all devices for which you made the requests.

To view the File Retrieval status:

2. On the File Retrieval Summary 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 results by Device Group, in the Group is field open the list and select the appropriate Device Group.

   **NOTE** If you are logged in as a Security Power User, you can select only the Device Group to which you are assigned.

   - To filter 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 name of an individual who is associated with a particular device.
     - **Make:** The manufacturer of a device or other hardware.
     - **Model:** The product type of a device or other hardware.
● To filter results by the File Retrieval status, in the and the Retrieval Status is area, select one or more of the following values:
  ○ **Requested**: The request was submitted and is in a transitory state when waiting for an agent call or when the targeted device is preparing for the File Retrieval operation.
  ○ **Retrieving**: The File Retrieval operation is in progress to retrieve the requested file.
  ○ **Ready**: The File Retrieval operation has finished retrieving the requested file. The file is ready for download.
  ○ **Cancelled**: The File Retrieval request was cancelled. For more information about cancelling a File Retrieval request, see "Cancelling a File Retrieval Request" on page 276.
  ○ **Failed**: The File Retrieval request failed to run on the targeted device.
  ○ **Purged**: The retrieved file was deleted from the servers.

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. Clicking an Identifier shown in the results grid opens the Device Summary page. For more information, see "Editing Asset Information" on page 80.
   
   ● **Request Name**: The name of the Remote File Retrieval request
   
   ● **Status**: The current status of the File Retrieval request, which includes the following possible values:
     ○ **Requested**: The request was submitted and is in a transitory state when waiting for an agent call or when the targeted device is preparing for the File Retrieval operation.
     ○ **Retrieving**: The File Retrieval operation is in progress to retrieve the requested file.
     ○ **Ready**: The File Retrieval operation has finished retrieving the requested file. The file is ready for download.
     ○ **Cancelled**: The File Retrieval request was cancelled. For more information, see "Cancelling a File Retrieval Request" on page 276.
     ○ **Failed**: The File Retrieval request failed to run on the targeted device.
     ○ **Purged**: The retrieved file was deleted from the servers.

   ● **Action**: The action you can perform on the request
   
   ● **File Name**: The name of the retrieved file
   
   ● **File Size**: The file size of the retrieved file
   
   ● **Device Name**: The 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
   
   ● **Make**: The manufacturer of the device
   
   ● **Model**: The product type of a device or other hardware
   
   ● **Requested On**: The date of the request
   
   ● **Requested By**: The name of the Security Administrator or Security Power User who submitted the request
Downloading Retrieved Files

After you have successfully created a File Retrieval request, the request runs on the targeted device on the next agent call. When the retrieval is complete, you can download the retrieved files to your local device.

You can select one of the following methods to download retrieved files depending on the browser you use:

- Downloading Retrieved Files Using Internet Explorer
- Downloading Retrieved Files Using FireFox or Another Browser

Downloading Retrieved Files Using Internet Explorer

To download a file using Internet Explorer:

1. On the Security tab of the Internet Options dialog, add the Absolute console domain (cc.absolute.com) as a trusted site.
2. For all trusted sites, click Custom Level, and in the Security Settings - Trusted Sites Zone dialog, enable the Automatic prompting for Downloads option.
3. Use the File Retrieval Summary report to search for the appropriate request. If the file is available for download, the Status column shows Ready.
4. In the File Name column, click the file name link.
5. Enter your Password and your SecurID Token Code or Authorization Code. For more information, see "Security Authentication Methods" on page 201.
6. Follow the on-screen instructions to save the file to your local drive.

Downloading Retrieved Files Using FireFox or Another Browser

To download a file using a browser other than Internet Explorer:

1. Use the File Retrieval Summary report to search for the appropriate request. If the file is available for download, the Status column shows Ready.
2. In the File Name column, click the file name link.
3. Enter your Password and your SecurID Token Code or Authorization Code. For more information, see "Security Authentication Methods" on page 201.
4. Follow the on-screen instructions to save the file to your local drive.

Changing the File Retrieval Status

Depending on the current File Retrieval status, you can do one of the following:

- Cancelling a File Retrieval Request
- Removing Retrieved Files and Log Files
The following table provides a list of possible File Retrieval states and the actions that you can perform for each of them.

### Available File Retrieval States and Actions

<table>
<thead>
<tr>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested</td>
<td>Cancel</td>
</tr>
<tr>
<td>Retrieving</td>
<td></td>
</tr>
<tr>
<td>Ready</td>
<td>Remove</td>
</tr>
<tr>
<td>Cancelled</td>
<td></td>
</tr>
<tr>
<td>Failed</td>
<td></td>
</tr>
<tr>
<td>Purged</td>
<td></td>
</tr>
</tbody>
</table>

### Cancelling a File Retrieval Request

If the status of the File Retrieval process is set to **Requested** or **Retrieving**, you can cancel the request and stop the file retrieval.

To cancel a File Retrieval request:

1. On the navigation bar click > **File Retrieval Summary Report**.
2. On the File Retrieval Summary Report in the **and the Request Name is or contains** field, enter the request name to search the appropriate File Retrieval request.
   
   If the File Retrieval request has not yet run, or it is running currently, the **Status** column shows **Requested** or **Retrieving**.
3. In the **Action** column of the File Retrieval request you want to cancel, click the **Cancel** link.
4. To cancel the request, click **OK** when prompted.

   The File Retrieval Summary Report refreshes to show **Cancelled** in the **Status** column next to the Remote File Retrieval request you cancelled.

### Removing Retrieved Files and Log Files

When you run a File Retrieval request, a directory log file is also generated. This log file provides a list of all files and their retrieval status.

When a File Retrieval request is successful, the files that you requested are available in the Absolute console. You can download these files to a folder on your local device. After the File Retrieval request is complete or if you have cancelled a File Retrieval request, you may want to delete the downloaded files and the directory log file.

To remove downloaded files and the directory log file:

1. On the navigation bar click > **File Retrieval Summary Report**.
2. On the File Retrieval Summary Report page search for the appropriate File Retrieval request.
● If the File Retrieval request is complete and the files are available for download, the **Status** column shows **Ready** and the **Action** column shows **Remove**.

● If the File Retrieval request is not complete or was cancelled, the **Status** column shows **Failed** or **Cancelled** and the **Action** column shows **Remove**.

3. In the **Action** column of the appropriate File Retrieval request, click the **Remove** link.

4. When prompted, if you want to remove the retrieved files and the log files, click **OK** to confirm. The File Retrieval Summary Report refreshes without any details about the File Retrieval request you just removed.
Chapter 13: Using File List

The File List feature lets Security Administrators, Administrators, and Security Power Users retrieve a list of files from a device remotely. You can use the full file paths to make Remote File Retrieval requests.

This following tasks are included in this section:

- **Overview**
- **Minimum System Requirements**
- **Retrieving a List of Files on Stolen Devices**
- **Tracking File List Status**

**IMPORTANT** All tasks in this chapter require that you log in to the Absolute console as a Security Administrator or Security Power User.

Overview

You can use the Request File List page to send a request to retrieve a list of files with specific file extensions available in a specific location on a targeted device.

For ease of use, the Request File feature contains a variety of predefined file extensions that you can retrieve. If you do not see the file extension you want on the Request File List page, you can also specify the file extension using the Other checkbox.

The following table provides a list of the predefined file types that are available to you on the Request File List page.

### Predefined File Types and File Extensions

<table>
<thead>
<tr>
<th>File Types</th>
<th>File Extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Word files</td>
<td>*.doc, *.dot</td>
</tr>
<tr>
<td>Microsoft Excel files</td>
<td>*.xls, *.xlt, *.xlam</td>
</tr>
<tr>
<td>Microsoft PowerPoint files</td>
<td>*.ppt, *.pot, *.pps, *.ppam</td>
</tr>
<tr>
<td>Microsoft Project files</td>
<td><em>.mpp</em>, <em>.mpt</em>, *.mpx, *.mpd</td>
</tr>
<tr>
<td>Adobe files</td>
<td>*.pdf, *.pm3, *.pm4, *.pm5, *.pm6, *.psd</td>
</tr>
<tr>
<td>Autocad files</td>
<td>*.dwg, *.dx</td>
</tr>
<tr>
<td>Corel Draw files</td>
<td>*.cdt</td>
</tr>
<tr>
<td>Eudora Email files</td>
<td>*.mbx, *.toc</td>
</tr>
<tr>
<td>HTML files</td>
<td>*.htm</td>
</tr>
<tr>
<td>Lotus 1-2-3 Spreadsheet files</td>
<td><em>.wk</em></td>
</tr>
<tr>
<td>Microsoft Office (and other) Backup files</td>
<td>*.bak</td>
</tr>
<tr>
<td>Microsoft Outlook files</td>
<td>*.pst, *.ost, *.wab</td>
</tr>
</tbody>
</table>
### Predefined File Types and File Extensions (continued)

<table>
<thead>
<tr>
<th>File Types</th>
<th>File Extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Outlook Express files</td>
<td>*.dbx</td>
</tr>
<tr>
<td>Open Office Writer files</td>
<td>*.sdw, *.sxw, *.odt, *.ott</td>
</tr>
<tr>
<td>Open Office Calc files</td>
<td>*.sdc, *.sxc, *.ods, *.ots</td>
</tr>
<tr>
<td>Open Office Impress files</td>
<td>*.sdd, *.sxi, *.odp, *.otp</td>
</tr>
<tr>
<td>Open Office Draw files</td>
<td>*.sda, *.sxd, *.odg, *.otg</td>
</tr>
<tr>
<td>Office Base files</td>
<td>*.sdb, *.odb</td>
</tr>
<tr>
<td>Open Office Math files</td>
<td>*.smf, *.sxm, *.odf</td>
</tr>
<tr>
<td>Open Office Schedule files</td>
<td>*.sds</td>
</tr>
<tr>
<td>Paintshop Pro files</td>
<td>*.psp, *.ps</td>
</tr>
<tr>
<td>Rich-Text files</td>
<td>*.rtf</td>
</tr>
<tr>
<td>Text Files</td>
<td>*.txt</td>
</tr>
<tr>
<td>WordPerfect documents</td>
<td>*.wkb, *.wpd</td>
</tr>
</tbody>
</table>

### Minimum System Requirements

File List is available for devices that meet the following system requirements:

- Windows operating systems: The targeted device must have one of the supported Windows Operating Systems installed. For more information, open the Absolute console's help system and search for supported platforms for managed devices.
- Current version of the Absolute agent for Windows devices.

**NOTE** The File List feature only works on Windows devices with .NET Framework 2.0 or higher installed.

### Retrieving a List of Files on Stolen Devices

You can use the File List feature to provide a list of the files on a stolen device. However, you can only retrieve a list of files that were created before the reported Incident Date.

To request a File List:

1. On the navigation bar click ⚙ > **File List Summary Report**.
2. On the File List Summary Report page click **Request a new file list**.
3. On the Request File List page in the **Request Name** field, type an appropriate name for the new request.
4. In the **Select a Device** area, click **Choose** to open the list and select the appropriate device. Click the appropriate device **Identifier** to select it. The Choose dialog closes and the Request File Retrieval page refreshes to show the selected device.
5. In the **Select a Volume to Scan** area, open the list and select the volume from where you want to retrieve the file list.

**NOTE** If you do not see the volume where your files are available, select the volume you want in the **Other** list.

6. Retrieve the list of files you want in one of the following ways:
   - **Select the checkboxes for the specific file types you want to retrieve.**
   - **Specify a file type that is not included in the list of predefined file types list by selecting the **Other** checkbox located at the end of the list, and entering the appropriate file extension. For multiple entries, separate your choices using commas, such as `.mov`, `.avi`.

7. Click **Submit** to create the File List request.

### Downloading a File List Request

To download a File List:

1. On the quick access toolbar, click [1] and click **File List Summary Report**.
2. On the File List Summary Report page click **Show results** and from the table under the **Request Name** column, click the link for the request’s name you want to download.
3. Open the downloaded file and follow the on-screen instructions to save the .txt file to your device.

### Tracking File List Status

You can view near real-time status updates on the progress of File List requests. The File List Summary Report provides a list of all devices for which you made the requests.

For each device in the list, the File List Summary Report includes the following information:

- **Identifier**: A unique Electronic Serial Number assigned to the agent that is installed on a device. Click the link to open the device’s Device Summary page. For more information, see "*[Editing Asset Information]* on page 80."

- **Request Name**: the name of the File List request

- **Status**: the current status of the File List request. Possible values include:
  - **Requested**: The request was submitted and is in a transitory state while waiting for an agent call or while the instruction setup process is running on the targeted device.
  - **Retrieving**: The File List operation is in progress to retrieve the list from the requested device.
  - **Ready**: The File List operation has finished and the list is ready for download.
  - **Cancelled**: The File List request was cancelled.
  - **Failed**: The File List request failed to run on the targeted device.
• **Action**: the action you can perform on the request, which includes the following actions depending on the request's status:

<table>
<thead>
<tr>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested</td>
<td>Cancel</td>
</tr>
<tr>
<td>Retrieving</td>
<td></td>
</tr>
<tr>
<td>Ready</td>
<td>Remove</td>
</tr>
<tr>
<td>Cancelled</td>
<td></td>
</tr>
<tr>
<td>Failed</td>
<td></td>
</tr>
</tbody>
</table>

• **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

• **Make**: The manufacturer of the device

• **Model**: The product type of a device or other hardware

• **Requested On**: the date of the request

• **Requested By**: the name of the administrator who submitted the request

Viewing the Status of a File List Request

To view the status of a File List request:

2. On the File List Summary 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.

   **NOTE**  If you are logged in as a Security Power User, you can select only the Device Group to which you are assigned.

   • To filter 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. Click the link to open the device's Device Summary page. For more information, see "[Editing Asset Information]" on page 80.
     - **Device Name**: The name assigned to the device in the operating system
     - **Username**: The name of an individual who is associated with a particular device
     - **Make**: The manufacturer of a device or other hardware
     - **Model**: The product type of a device or other hardware
     - **File Name**: The name of the retrieved file

   • To filter results by the File Retrieval status, in the **and the Retrieval Status is** area, select one or more of the following values:
     - **Requested**: The request was submitted and is in a transitory state while waiting for an agent call or while the instruction setup process is running on the targeted device.
○ **Retrieving**: The File List operation is in progress to retrieve the list from the requested device.
○ **Ready**: The File List operation has finished and the list is ready for download.
○ **Cancelled**: The File List request was cancelled.
○ **Failed**: The File List request failed to run on the targeted device.

### Changing a File List Status

Depending on the current File List status, you can do one of the following:

- Cancelling a File List Request
- Removing Retrieved Files and Log Files

For a list of possible File List states and the actions you can perform for each of them, see "Tracking File List Status" on page 280.

### Cancelling a File List Request

If the status of the File List process is set to **Requested** or **Retrieving**, you can cancel the request and stop the file list retrieval.

To cancel a File List request:

1. On the navigation bar click **File List Summary Report**.
2. On the File List Summary Report page, click **Show results** and in the table search for the appropriate File List request.
   
   If the File List request has not yet run or is currently running, the **Status** column shows Requested or Retrieving.
3. In the **Action** column of the File List request you want to cancel, click the **Cancel** link.
4. When prompted, if you want to cancel the request, click **OK** to confirm.
   
   The File List Summary Report refreshes to show **Cancelled** in the **Status** column next to the File List request you cancelled.

### Removing Retrieved Files and Log Files

When you run a File List request, a directory log file is also generated. This log file provides a list of all file lists and their retrieval status.

When a File List request is successful, the file list that you requested is available in the Absolute console. You can download these file lists to a folder on your local device. After the File List request is complete or if you have cancelled a File List request, you may need to delete the downloaded files and the directory log file.

To remove downloaded files and/or the directory log file:

1. On the navigation bar click **File List Summary Report**.
2. On the File List Summary Report page click **Show results** and in the table search for the appropriate File List request.
If the File List request was run successfully and the list is available for download, the **Status** column shows **Ready** and the **Action** column shows **Remove**.

If the File List request did not run or was cancelled, the **Status** column shows **Failed** or **Cancelled**, and the **Action** column shows **Remove**.

3. In the **Action** column of the appropriate File List request, click the **Remove** link.

4. When prompted, if you want to remove the retrieved file list and the log files, click **OK** to confirm.

   The File List Summary Report refreshes without any details about the File List request you just removed.
Chapter 14: Absolute for Chromebooks

The Absolute for Chromebooks service lets you safeguard your Chromebooks in cases of loss or theft. This service provides the following two important components:

- **Absolute Safe Schools Program**
  
  You can implement best practices within schools throughout your school district or within your organization to ensure devices are handled responsibly. This program focuses on teaching students and end-users how to avoid becoming targets for criminals by using best practices and safe actions.

  The combination of a formal process for reporting lost and stolen devices, identity tags on managed devices, and ongoing user awareness and education can result in a decrease in overall loss and theft.


- **Theft Investigation Services**

  When a security incident is reported, the Absolute Investigations team initiates rapid response service, begins an investigation to gather information and evidence for law enforcement agencies, and prepares court-ready investigative reports and other case critical work.

  Depending on your organization’s specific agreement with Absolute, the Incident Investigation program may include a Service Guarantee in the event the team is unable to recover a stolen Chromebook. For more information, see "[Understanding the Prepaid Service Guarantee Balance](http://www.absolute.com/en/resources/datasheets/safe-schools) on page 294.

This chapter includes the following sections:

- [Adding Chromebooks to your Absolute Account](#)
- [Working with Chromebooks in the Absolute console](#)
- [Removing the Chromebook Extension from a Device](#)

**IMPORTANT** To perform the tasks in this chapter requires that you log in to the Absolute console as an Administrator.

**Adding Chromebooks to your Absolute Account**

Chromebooks run the Chrome OS operating system, which is a lightweight Linux-based operating system that is integrated with the Chrome browser and designed to primarily run web applications. User data is stored in the “cloud” rather than on the device’s hard drive.

Due to the unique nature of the Chrome operating system, the Absolute agent can’t be installed on a Chromebook. Instead, you manage your Chromebooks in Absolute by deploying the Chromebook extension to each device. The extension is a small software program that enables Chromebooks to secure a connection with the Absolute Monitoring Center and allows you to manage these devices in the Absolute console.

To add Chromebooks to your Absolute account, you need to do the following:

1. Enable the Google Synchronization Service by updating your Classic Account Settings in the Absolute console. For more information, see "[Adding Google Account Details to the Absolute Console](http://www.absolute.com/en/resources/datasheets/safe-schools) on page 285."
After the Google Synchronization Service is enabled it retrieves information about each Chromebook from your Google account and populates the Absolute console with this data. This process also assigns a unique Identifier to each Chromebook and allows for deployment of the Chromebook extension.

In the Asset Report, and the Call Tracking tab for each Chromebook, the sync from the Google account shows as a call, with an Agent Version of 2200.

2. Deploy the Chromebook extension to each device using the Google Admin console. For more information about deploying the Chromebook extension to your Chromebooks, see "Deploying the Chromebook extension" on page 287.

After the Chromebook extension is deployed on a new Chromebook, the extension is activated with its first secure call to the Absolute Monitoring Center. The extension then makes regularly scheduled calls to the Monitoring Center on a daily basis. During these calls, the latest device data is sent to the Monitoring Center and instructions for any pending security operations, such as Device Freeze, are sent to the device.

In the Asset Report, and the Call Tracking tab for each Chromebook, a call by the Chromebook extension shows as Agent Version 24xx.

**NOTE** In the Absolute console, references to attributes of the "agent" also refer to the corresponding attributes of the Chromebook extension, if the feature supports Chromebooks. For example, the version of the Chromebook extension installed on a Chromebook shows in the **Agent Version** column of Absolute reports.

Managing Google Account Details in the Absolute Console

This section provides information on the following topics:

- Adding Google Account Details to the Absolute Console
- Editing Google Account Details
- Deleting Google Account Details

Adding Google Account Details to the Absolute Console

For your Chromebooks that are currently managed in your Google account to be visible in the Absolute console, you need to add your Google account name to your Absolute account. This process enables the Google Synchronization Service to retrieve initial device information from your Google account and show it in the Absolute console.

To add Google account details to your Absolute account:

1. Before you begin this task ensure that you are assigned a Google Admin role with the following minimum set of administrator privileges:
   - **Organization Units**, including **Create**, **Read**, **Update**, and **Delete** privileges
   - **Users**, including **Read** privileges only
   - **Services > Chrome OS**, including **Manage Device**, **Manage User Settings**, and **Manage Device Settings** privileges

   These privileges are assigned by default to the Super Administrator role, or you can create a User Created role and assign these privileges to it. For more information about Google Admin roles and privileges, refer to Google’s Admin console Help.
2. On the navigation bar click \( \triangleright \) **Classic Account Settings**.

3. Scroll to the **Chromebooks - Google Account** area and in the **Account Name** field enter the email address you use to log in to your organization's Google account.

4. Click **Add**.

5. If you are not already signed in to your Google account, the Google Signin page opens. Sign in using the appropriate credentials.

6. The Google Request for Permission page opens to let you authorize the synchronization service. This service synchronizes the device information in the Absolute console with the information maintained in the Google Admin console. Click **Accept**.

7. In the Select Organizational Units dialog, select each Google organizational unit that contains the Chromebooks you want added to your Absolute account. To select all organizational units, select the checkbox next to the organization.

   If you have not purchased Absolute for Chromebooks licenses for all Chromebooks in your fleet, ensure that the Chromebooks you want added to the Absolute console are in their own organizational units (directly under the organization) and you select only those units. By doing so, you ensure that only available licenses are consumed.

   **IMPORTANT** You must select at least one Google organizational unit.

8. Click **Continue** to save your changes and close the dialog.

   The Google Synchronization Service then adds all Chromebooks associated with the selected Google organization units to the Absolute console. When this process is complete, the **Last Sync Time** column is populated with the date and time.

   Adding Chromebooks to your Absolute account is a two-step process. You have completed the first step. To go to the next step, see "Deploying the Chromebook extension" on page 287.

**Editing Google Account Details**

You can add additional Chromebooks to your Absolute account by editing the Chromebooks - Google Account setting. You can also remove Chromebooks.

To edit your Google account details:

1. On the navigation bar click \( \triangleright \) **Classic Account Settings**.

2. Scroll to the **Chromebooks - Google Account** area and next to Google account name click **Edit**.

3. In the Select Organizational Units dialog, select each Google organizational unit that contains the Chromebooks you want to add to your Absolute account. To select all organizational units, select the checkbox next to the organization. To remove Chromebooks from your account, clear each checkbox next to the applicable organizational units.

4. If you cleared any checkboxes, a warning message shows. Click **Yes** to continue.
WARNING! Clearing the checkbox of a previously selected organizational unit (OU) automatically sets that OU's Chromebooks to Disabled, which frees up Absolute for Chromebooks licenses. See "Viewing Pending Agent Removal Requests" on page 74.

5. Click Continue to save your changes and close the dialog.

The Google Synchronization Service then updates the list of Chromebooks associated with your Absolute account in the Absolute console. When this process is complete, the Last Sync Time column is populated with the date and time.

6. Adding Chromebooks to your Absolute account is a two-step process. If you selected new organization units in step 3, you have completed the first step. To go to the next step, see "Deploying the Chromebook extension" on page 287.

Deleting Google Account Details

If a Google account was added in error, or the account is not required anymore, you can delete it from the Classic Account Settings page.

WARNING! Use caution when deleting an existing Google account from Classic Account Settings. This action has the following effect on Chromebooks in the Absolute console:
- Device information is no longer synchronized between the Google account and the Absolute console.
- If you add new devices to the Google account, the devices are not added to your Absolute account.
- The Agent Status of all existing Chromebooks in your Absolute account remains set to Active and the devices continue to connect to the Absolute Monitoring Center. To disable these devices, see "Removing the Chromebook Extension from a Device" on page 289.

To delete a Google account:

1. On the navigation bar click ↗️ > Classic Account Settings.
2. Scroll to the Chromebooks - Google Account area, locate the Google account that you want to delete and click its Delete link in the rightmost column.
3. On the confirmation message click OK.

Deploying the Chromebook extension

You can manage your Chromebooks in Absolute by deploying the Chromebook extension to each device using the Google Admin console. For more information about the extension, see "Adding Chromebooks to your Absolute Account" on page 284.

To deploy the Chromebook extension to your Chromebooks:

1. On the navigation bar click ↗️ > Download Packages.
2. On the Download Packages page, in the Absolute for Chromebooks section, click Copy to clipboard in the Extension ID column to copy the identifier. In the next step, you will use the Extension ID to find the extension in the Chrome Web Store.
3. Sign in to the Google Admin console at admin.google.com using your domain's Google account and complete the steps required to configure the applicable organizational units and deploy the extension to your Chromebooks.
For more information, go to the Documentation page and see "Installing and Managing the Absolute for Chromebooks Extension" in the Administrator's Guide for Absolute Agent.

Working with Chromebooks in the Absolute console

The Chromebook extension collects data from each Chromebook, including operating system information, geolocation information, and details about installed hardware and software. For details about the specific information detected by the extension and made available in the Absolute console, see Absolute Products and Services—Data Points Collected in the online Help.

**NOTE** The Chromebook extension is unable to collect a device's Asset ID. This data is always synced directly from your Google Account to the Absolute console. Asset ID shows in the Asset Number field. You can view this field on a device's Custom Fields page in Device Details. We recommend that you don't edit the values in this field.

The Chromebook extension enables Chromebook support for the following Absolute reports, features, and functionality:

- **Hardware Asset reports**, including:
  - Asset Report
  - Monitor Report
  - Device Readiness Report
  See "Hardware Assets Reports" on page 93.

- **Software Asset reports**, including:
  - Software Overview Report
  - Software Configuration Change Report
  - Software By Device Report
  See "Software Assets Reports" on page 108.

- **Security reports**, including:
  - Operating System Updates Report
  - Suspicious Devices Report
  See "Security Reports" on page 121.

- **Call History and Loss Control reports**, including:
  - Call History Report
  - Activation Report
  - Device Location Report
  - Device Location History Report
  See "Call History and Loss Control Reports" on page 152.

- **Alerts**
  See "Alerts" on page 15.

- **Geofences**
  See "Managing Geofences" on page 265.

- **Device Freeze**
See Freezing devices in the online Help.

- Investigation Reports
  See "Reporting the Theft of a Managed Device" on page 290.

Removing the Chromebook Extension from a Device

To remove the Chromebook extension from a device you need to complete the following tasks:

- Submit an Unenroll Device request to set the device to Disabled in the Absolute console.
- Remove the extension from the device using the Google Admin console. For more information, see the Administrator's Guide for Absolute Agent.
Chapter 15: Reporting the Theft of a Managed Device

When you determine that one of your managed devices is stolen, and after you have filed a report with your local authorities, you can use the Investigations area to report the loss or theft to the Absolute Investigations team.

**NOTE** Depending on the Absolute products your organization purchased, Investigation Reports and the services of the Absolute Investigations team may not be available.


This chapter includes the following information and tasks:

- Investigation Checklist
- Viewing Existing Investigation Reports and Their Report History
- Creating an Investigation Report
- Editing Existing Investigation Reports
- Cloning an Existing Report
- Closing an Open Investigation Report
- Managing the Investigation Report Contact List

**Investigation Checklist**

The following checklist provides best practice guidelines for reporting the loss or theft of a device and for completing the Investigation Report.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Action Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Handling</strong></td>
<td>Handle the device in a reasonably safe and secure manner.</td>
<td>Ensure that the device is not left unattended or in a location that is not secure.</td>
</tr>
<tr>
<td><strong>Investigation Report</strong></td>
<td>According to our Service Agreement, the Incident Date is the date you discovered the theft. Report the theft of a device to the appropriate law enforcement agency, and then submit an Investigation Report to Absolute. See &quot;Creating an Investigation Report&quot; on page 293.</td>
<td>Contact the appropriate law enforcement agency and Absolute within 14 days of detecting the theft. At this point, a theft file is opened at Absolute [Technical Support](<a href="http://Absolute">http://Absolute</a> Technical Support). If you fail to notify Absolute of the theft within 14 days, you are not eligible for the Service Guarantee. When Technical Support receives your Investigation Report, you are sent an e-mail acknowledging receipt from a Service Guarantee contact the next day.</td>
</tr>
<tr>
<td>Stage</td>
<td>Action Required</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Service Guarantee Submissions</td>
<td>You have 30 days from receipt within which to submit the completed Service Guarantee Submission form.</td>
<td>Thirty days from the date that your theft file was opened at Absolute, a Service Guarantee Submission form is sent to you for completion and submission.</td>
</tr>
<tr>
<td></td>
<td>Ensure that you include all receipts for both the original purchase price of the device and for any professional licenses that are associated with the device.</td>
<td>Absolute's Service Guarantee Administrator reimburses for the loss of the device based on the receipts provided.</td>
</tr>
<tr>
<td></td>
<td>Appendix B of the Service Agreement sets out the default values that Absolute applies for Service Guarantee Submissions.</td>
<td>If you do not return the completed Service Guarantee Submission Form within the 30 day timeframe, Absolute will apply the default value of the device as per the Service Agreement and reimburse accordingly. For details about these values, visit our Service Agreement at <a href="http://www.absolute.com/company/legal/agreements/computrace-agreement">www.absolute.com/company/legal/agreements/computrace-agreement</a>.</td>
</tr>
</tbody>
</table>

**Viewing Existing Investigation Reports and Their Report History**

To view existing Investigation Reports, and their Report History:

1. On the navigation bar click **Investigations > Investigations Summary.**

**NOTE** If no thefts are recorded, the Investigations Summary page shows a No records found message.

2. On the Investigations Summary page at the Search Criteria location you can filter the Investigation Reports that are shown in the results grid, as follows:

   - To view the Report History for multiple Investigation Reports:
     
     i)   In the **In the Group** field, open the list and select the device group that has the Investigation Report you want to view.
     
     ii)  In the **and the report contains keyword** field, enter the appropriate keyword.
     
     iii) In the **and the incident date is between** field, select one of the following options:

     o   Click the **at any time** option to show Investigation Reports for any date.
     
     o   Click the **in the last x days** option and enter the appropriate number of days since the incident occurred. The results grid shows results for this timeframe.
     
     o   Click the **between** option and click in the first field to enter the starting date (dd/mm/yyyy) or click the calendar and click the appropriate starting date.
     
     o   Do the same for the second field, which is the ending date; for example, between 12/06/2012 and 18/06/2012.
     
     iv)  In the **and the status is** area, select each status that you want to include in the report:

**NOTE** Status definitions are provided at: www.absolute.com/en/support/theft_report_definitions.aspx
To include Active Investigation Reports, select the **Active** checkbox and select each checkbox that applies to the list you want to show, as follows:
- Under Investigation: Researching
- Under Review: First Contact Received
- Awaiting Customer: Device Connecting Internally
- Awaiting Customer: Require Information

To include Monitoring Investigation Reports, select the **Monitoring** checkbox and select each checkbox that applies to the list you want to show, as follows:
- Awaiting Device Movement
- Awaiting 1st Contact
- Awaiting Further Device Contact
- Police Unable to Pursue
- Pending New Leads

To include Closed Investigation Reports, select the **Closed** checkbox and select each checkbox that applies to the list you want to show, as follows:
- Recovered
- Police Recovered
- Customer Requested Closure
- Perpetual Delete Deployed by Customer
- Software not Installed
- Retrieved–Not Stolen
- Cancelled
- Incomplete Report
- No Contact from Device
- Other

v) In the **and the Guarantee Payment Status is** area, select each of the following checkboxes, as appropriate:
- Paid
- Eligible
- Declined
- N/A (not applicable)

- To view the Report History of a single Investigation Report, in the **or the Report ID is** field, open the list and select the appropriate Investigation Report Identifier.

3. Click **Show results** to populate the **results** grid with the choices you made in the Search Criteria location.

You can see the following information about each Investigation Report associated with your account:
- **Report ID** is a unique identification number assigned to the report.
- **Identifier**
- **Incident Date**
- **Date Reported**
Chapter 15: Reporting the Theft of a Managed Device

- Recovered Date
- Location
- City, State, and Country
- Make, Model, and Serial
- Device Status: the device’s Investigation Report status.
- Guarantee Status
- Action: View or Clone this Investigation Report.

4. In the results grid under the Report ID column, click a link to open the Create and Edit Investigation Report where you see that report’s history.

Viewing the Report History Table

At the bottom of the Investigations Summary page, you see the results grid that includes the Report ID, Identifier, Date Reported, Date Updated, Make, Model, and Serial number for the missing or stolen device.

When you click a link under the Report ID column, the Create and Edit Investigation Report opens for that report. From this page you can edit the report’s information.

The Report History table shows a record of all edits made to an original Investigation Report number, appended with a hyphen and a number each time an edit is made to the report, such as 84544-1. This table tracks the number of times you edit an Investigation Report and provides the details of each recorded change. Under the Report History table, you have several options, as follows:

- Click the make a new report link to create a new Investigation Report.
- Click the reports made link to view the list of all Investigation Reports for your organization.

Creating an Investigation Report

When a device is stolen, you need to file a report with the appropriate authorities. To recover the reported device, the Absolute Investigations team uses the details provided on the police file, which you enter in the Investigation Report, and the information that is gathered by the agent on the stolen device.

If the stolen device is eligible for a Service Guarantee payout, Absolute contacts you when you become eligible to receive the payout. For details about eligibility requirements, click the Service Agreement link on any page to see the Service Guarantee document that applies to your account.

In some cases, your account may contain a Prepaid Service Guarantee Balance, which is described next. This prepaid balance impacts your eligibility for the amount of Service Guarantee payout.

This section includes the following information:

- Minimum System Requirements
- Understanding the Prepaid Service Guarantee Balance
- Before You Begin
- Submitting an Investigation Report
Minimum System Requirements

You can submit an Investigation Report for devices that meet the following system requirements:

- **Operating system:** The targeted device must be running a supported version (open the Absolute console help system and search for supported platforms for managed devices) of one of the following operating systems:
  - Windows
  - macOS
  - Android
  - Chrome OS (installed on Chromebooks only)

- **Agent:** For Windows, Mac, and Android devices, the targeted device must have an agent status of Active, meaning that the agent is installed and regularly calling in to the Absolute Monitoring Center.

- **Chromebook Extension:** The Absolute for Chromebook extension must be activated on the targeted device, meaning that the extension is deployed and regularly calling in to the Absolute Monitoring Center.

Understanding the Prepaid Service Guarantee Balance

If one of your devices from a previous Investigation Report was recovered within 30 days after you received the Service Guarantee payout, the amount of the Service Guarantee payout that you received is considered to be a Prepaid Service Guarantee balance for your account.

In such cases, instead of you refunding the amount of the payout back to Absolute, the Prepaid Service Guarantee balance is applied to any future Service Guarantee payments that you may receive.

For example, let’s use a scenario where you received $500 toward a Service Guarantee payout for Device 1. And let’s presume that Device 1 was recovered 10 days after you received the payout. Some time later, you lose another device, Device 2, which is worth $900 and which is eligible for a Service Guarantee payout. When you receive the payout for Device 2, you will receive $400, as your account has a $500 Prepaid Service Guarantee balance and you have already received $500 out of the $900 value of Device 2.

For more information, click the **Service Agreement** link on any page to see the Service Guarantee document that applies to your account.

Viewing the Prepaid Service Guarantee Balance

Your Prepaid Service Guarantee balance shows when you file a new Investigation Report.

If you want to know your Prepaid Service Guarantee balance without filing a new Investigation Report, contact Absolute **Technical Support**.

Before You Begin

Before you can submit an Investigation Report, you need to meet the following prerequisites:

- The device is not frozen. If the device is frozen, you must unfreeze it before continuing.
- The device is not assigned to a Device Freeze offline policy. If the device is assigned to an offline policy, you must remove it from the offline policy before continuing. For more information, see "Removing Devices from an Offline Policy" on page 250.
• If you would like to run a Data Delete request on the device, create and launch a Data Delete request on the device before you file an Investigation Report. For information on how to run a Data Delete request, see "Requesting a Data Delete Operation" on page 210.

Submitting an Investigation Report

To create an Investigation Report for an agent equipped device:

1. On the navigation bar click ➕ > Investigations > Investigations Summary.
2. On the Investigations Summary page, scroll down and click Create new report.
3. On the Create and Edit Investigation Report page at the Which device? area, do one of the following to select the appropriate device:
   - Click Choose to open the Choose the Identifier dialog where you click the appropriate record from a list of all detected devices to select it. For more information on the Choose feature, see "Editing Asset Information" on page 80.
   - The Choose the Identifier dialog closes and the Create and Edit Investigation Report refreshes to populate the Make, Model, Serial Number, Asset Number, and Operating System fields.
   - Enter the appropriate values in the Make, Model, Serial Number, Asset Number, and Operating System fields.
4. At the What are the incident details? area, do the following:

   **NOTE** The greater the accuracy and detail of the information you provide, the greater the likelihood that the Investigations team are able to facilitate a recovery. Required fields are indicated with an asterisk (*).

   • In the Date and Time of Incident fields, enter the date (dd/mm/yyyy format) in the first field or open the calendar and select the appropriate date. In the second field, enter the time in the hh:mm format.
   • In the Timezone field, open the list and select the appropriate timezone.
   • In the Address where Incident Occurred fields, enter the full address where the theft occurred.
   • In the Victim’s Name field, enter the victim’s full name.
   • In the City where Incident Occurred field, enter the city or town where the theft occurred.
   • In the Country where Incident Occurred field, open the list and select the appropriate country where the theft occurred.
   • In the State/Province where Incident Occurred field, enter the appropriate state or province in which the theft occurred.
   • In the Was Power Cord Taken? options, click the appropriate response from Yes, No, and Unknown.
   • In the Details of Incident field, enter the details about the last known location of the device and the circumstances of the incident.
5. At the Have you filed a report with the police? area, enter the following information using the police report you filed when you reported the incident to the authorities.
   • In the Agency field, enter the police agency with which you filed the police report.
6. Select the checkbox to acknowledge that you have filed a police report and provided accurate information with respect to that police report.

7. In the Who are you? section, edit the following information for the authorized contact person in your organization:

   - In the First Name field, enter the contact person’s first name.
   - In the Last Name field, enter the contact person’s last name.
   - In the Company field, enter your organization’s name.
   - In the Job Title field, enter this contact person’s job title.
   - In the E-mail field, enter this contact person’s e-mail address.
   - In the Country Code field, enter the country code for this contact person’s phone number.
   - In the Phone Number and Ext field, enter the phone number for the contact person at your organization.

8. In the What is your Investigation Report Contact List? section, confirm the contact list for this Investigation Report.

    Investigation Report notifications are sent to the individuals listed in the default Investigation Report Contact List. To view the list, click Investigation Report Contact List.

    **NOTE** The Investigation Report Contact List is managed by authorized users only. To request an update to the contact list, contact an administrator with Security Administrator privileges.

    If you want to also send notifications to one or more other individuals:

    a) Select For this investigation only, identify anyone you would like updated beyond the users in the Contact List.
    b) In the field, type the e-mail address of each contact, separated by a semicolon.

9. At the Consent to Install Software area, select the checkbox to indicate that you consent to the installation of additional software components on the selected device to assist with the investigation and recovery of the device.

10. When you finish entering information in the report, click Send this report.

    The Create and Edit Investigation Report page refreshes with the information you entered and is presented again for you to verify that the report is correct.

    **NOTE** If you need to make further changes, click Edit this report. The Create and Edit Investigation Report page opens where you make the necessary changes and click Send this report.
11. When you are satisfied that the information in the report is accurate, click **This report is correct**.

12. A confirmation page opens with information about the Investigation Report you just created and shows the report’s **file number**.

   From this confirmation page, you can do the following:
   
   - Click the **file number** link to open the report you have just created.
   - Click the **Investigations Summary** link to open that page. Look at the **results** grid for the list of Investigation Reports for your organization and you can find your new report at the top of the list.
   - Click **Create another report** to create a new Investigation Report.

In the Absolute console, the device is flagged as Stolen. While the Absolute Investigations team completes its investigation, you can view the device on the Investigations Summary page and the Asset Report. For more information, see the following topics:
- "**Viewing Existing Investigation Reports and Their Report History**" on page 291
- "**Asset Report**" on page 94

**Editing Existing Investigation Reports**

To edit the information in an existing Investigation Report:

1. On the navigation bar click **> Investigations > Investigations Summary**.

2. On the Investigations Summary page in the results grid, click the **Report ID** link for the appropriate report.

   A read-only version of the Create and Edit Investigation Report page for the selected report opens.

3. To edit the report, click **Update**.

   The Create and Edit Investigation Report page for the selected report opens. At the **Which device?** area, the fields are populated with information that you cannot change.

4. Edit the information you need to change, as follows:

   a) In the **What are the incident details?** section, edit the following information:
      
      - In the **Date and Time of Incident** field, enter the new **date** (in the dd/mm/yyyy format) or open the calendar and select the appropriate date. In **time** field, enter the time in the hh:mm format.
      - In the **Timezone** field, open the list and select the appropriate timezone.
      - In the **Address where Incident Occurred** field, enter the address on the lines provided.
      - In the **Victim’s Name** field, enter the name of the victim.
      - In the **City where Incident Occurred** field, enter the nearest city or town to where the theft occurred.
      - In the **Country where Incident Occurred** field, open the list and select the appropriate country where the theft occurred.
      - In the **State/Province where Incident Occurred** field, enter the appropriate state or province in which the theft occurred.
      - At the **Was Power Cord Taken?** options, click one of the following:
• Yes
• No
• Unknown

- In the **Details of Incident** field, enter the last known location of the device and the circumstances surrounding the incident.

b) In the **Have you filed a report with the police?** section, edit the following information from the police report you filed:

- In the **Agency** field, enter the agency where you filed the police report.
- In the **Country Code** field, enter the country code for the phone number.
- In the **Agency Phone** field, enter the phone number for the police department where you filed the police report.
- In the **Ext** field, enter the phone extension if appropriate.
- In the **District/Division/Precinct Number** field, enter the appropriate information.
- In the **Police File Number** field, enter the appropriate information.
- In the **Investigating Officer** field, enter the appropriate information.

c) In the **Who are you?** section, edit the following information for the authorized contact person in your organization:

- In the **First Name** field, enter the contact person’s first name.
- In the **Last Name** field, enter the contact person’s last name.
- In the **Company** field, enter your organization’s name.
- In the **Job Title** field, enter this contact person’s job title.
- In the **E-mail address** field, enter this contact person’s e-mail address.
- In the **Country Code** field, enter the country code for this contact person’s phone number.
- In the **Phone Number** field, enter the phone number for the contact person at your organization.
- In the **Ext** field, enter the phone extension if appropriate.

d) In the **What is your Investigation Report Contact List?** section, edit the contact information for this Investigation Report.

Investigation Report notifications are automatically sent to the individuals listed in the default Investigation Report Contact List. To view the list, click **Investigation Report Contact List**.

**NOTE**  The Investigation Report Contact List is managed by authorized users only. To request an update to the contact list, contact an administrator with Security Administrator privileges.

If you want to also send notifications to one or more other individuals:

i) **Select** **For this investigation only, identify anyone you would like updated beyond the users in the Contact List.**

ii) In the field, type the e-mail address of each contact, separated by a semicolon.

5. When you are satisfied that you have made all of the required changes, click **Save**.

A confirmation page opens to indicate that the report was updated and a copy of the updated report is sent to you by e-mail.
Cloning an Existing Report

When multiple devices are stolen at the same time and from the same location, you can create one Investigation Report with all of the details, and then clone that Investigation Report for every other device that was stolen.

Each time you clone an Investigation Report, a new **Report ID** is automatically assigned to each clone.

To clone an existing Investigation Report:

1. **Create an Investigation Report for one of the missing or stolen devices by completing the task, “Submitting an Investigation Report” on page 295.**
   Now you can clone this Investigation Report for the remaining devices that were stolen at the same time, and from the same location.

2. **With the Investigations Summary page open from step 1, in the results grid search for that Investigation Report and, under the last column, click the **Clone** link.**
   The Create and Edit Investigation Report page opens. Notice that most of the fields are populated with information from the selected report, except the device information.

3. **In the **Which device?** area at the **Choose Device** field, click **Choose**.**
   The Choose the Identifier page opens. For more information on the **Choose** feature, see "Editing Asset Information" on page 80.

4. **Select one of the multiple devices that was stolen by clicking the appropriate record.**
   You are returned to the Create and Edit Investigation Report page. The rest of the fields in the **Which device?** area of the Investigation Report are populated with information that is specific to the device you selected.

5. **Click **Save**.**
   The Create and Edit Investigation Report page opens, showing all of the information that is specific to this Investigation Report. At the top of the page at the **Report ID** area, you see the Investigation Report number for the report that you just created.

6. **At the bottom of this page, you see a **Report History** table (with no contents yet).**
   Below the Report History table, there are some links where you can take the following actions:
   - **Click the make a new report link to create a new Investigation Report.**
   - **Click the reports made link to view the list of all Investigation Reports for your organization.**

7. **If you want to edit the report, click **Update** and edit the appropriate fields in this report summary as described in the task, “Editing Existing Investigation Reports” on page 297.”

8. **Repeat step 2 through step 6 until you have cloned the Investigation Report Summary for all devices stolen at the same time from the same location.”

Closing an Open Investigation Report

You cannot close an Investigation Report using the Absolute console.

To close an Investigation Report for a device that is reported as stolen, contact Absolute **Technical Support.”**
Managing the Investigation Report Contact List

The Investigation Report Contact List contains contact information for the individuals within your organization who receive Investigation Report notifications. When users submit an Investigation Report, they can click a link on the Create and Edit Investigation Report page to view the contact list. See "Submitting an Investigation Report" on page 295.

Only Security Administrators are authorized to manage the Investigation Report Contact List. They can add new contacts to the list, edit contact information, and update the Contact Status of a contact.

Possible values for Contact Status are:

- **Active**: the contact receives Investigation Report notifications via the contact information recorded in the Investigation Report Contact List.
- **Disabled**: the contact’s information is stored but the individual does not receive Investigation Report notifications.

**NOTE** When you first access the Investigation Report Contact List it may be prepopulated with contact information collected from previously submitted Investigation Reports. If some of these contacts are no longer applicable, you can disable their contact record.

Contacts cannot be deleted. If you need to prevent a former contact from receiving Investigation Report notifications, disable the contact in the Investigation Report Contact List. See "Disabling Contacts" on page 302.

This section provides information on the following topics:

- Adding Contacts to the Investigation Report Contact List
- Editing Contact Information
- Viewing and Printing the Investigation Report Contact List
- Disabling Contacts
- Activating Disabled Contacts

**IMPORTANT** To perform the tasks in this section requires you log in to the Absolute console as a Security Administrator.

Adding Contacts to the Investigation Report Contact List

To add a new contact to the Investigation Report Contact List:

1. On the navigation bar click **> Investigations > Investigations Contact List**.
2. On the Investigation Report Contact List page, click **New Contact**.
3. On the Create and Edit Investigation Report Contact Details page in the **General Information** section, enter the following information about the individual:
   - **First Name**
   - **Last Name**
   - **Title**: the individual’s title within your organization
   - **Language**: select the preferred language of the individual from the list

**NOTE** **First Name** and **Last Name** are required fields.
4. If your account includes Absolute products with the Service Guarantee, you need to designate one contact in your organization as the **Service Guarantee Contact**. If this applies to this individual, select the checkbox.

**NOTE** If this option is disabled, another contact has already been specified as the **Service Guarantee Contact**.

5. In the **Contact** section, enter the following information about the individual:

- **E-mail Address** (required field)
- **Phone and Ext**
- **Fax**
- **Cell**
- **Pager**

6. If you want to add additional information, enter a comment in the **Note** field.

7. Click **Save**.

On the Investigation Report Contact List page, the new contact is added to the list and the **Contact Status** is set to **Active**.

**Editing Contact Information**

If the contact information for an individual has changed, you can update that information in the Investigation Report Contact List.

To edit a contact’s contact information:

1. On the navigation bar click **> Investigations > Investigations Contact List**.

2. On the Investigation Report Contact List page, in the **Search Criteria** area, do the following:

   a) Use one or more of the following criteria to find the contact you want to edit:
      - **contact name**: search using all or part of the name of the contact
      - **e-mail address**: search using all or part of the e-mail address of the contact
      - **phone**: search using all or part of the contact’s phone number, if recorded in the Absolute console

   b) To include disabled contacts in the search results, select the **Include Disabled Contacts** checkbox.

   c) Click **Show results**. The search results show in the **results** grid.

3. Click the **Contact Name** link of the contact you want to edit.

4. On the Create and Edit Investigation Report Contact Details page, edit the contact information for the individual.

5. Select or clear **Service Guarantee Contact** as applicable. For more information, see step 4 of the task, "**Adding Contacts to the Investigation Report Contact List**" on page 300.

6. If applicable, edit the content in the **Note** field.

7. Do one of the following:
To save the edits and set the Contact Status of the contact to Active, click **Save & Activate**.
To save the edits and set the Contact Status of the contact to Disabled, click **Save & Disable**.

**Viewing and Printing the Investigation Report Contact List**

To view the Investigation Report Contact List and save it to a CSV file for printing:

1. On the navigation bar click **Investigations > Investigations Contact List**.

   By default on the Investigation Report Contact List only Active contacts show in the contact list. The following information about each contact is presented in columns in the results grid:

   - **Contact Name**
   - **Phone**
   - **E-mail Address**
   - **Service Guarantee Contact**
   - **Note**
   - **Contact Status**

2. To search for a contact, in the **Search Criteria** area do the following:
   a) Use one or more of the following criteria to find the contact:
      - **contact name**: search using all or part of the name of the contact
      - **e-mail address**: search using all or part of the e-mail address of the contact
      - **phone**: search using all or part of the contact’s phone number, if recorded in the Absolute console
   b) To include disabled contacts in the search results, select the **Include Disabled Contacts** checkbox.
   c) Click **Show results**. The search results show in the results grid.

3. The list is sorted by contact creation date in descending order; the most recently added contact is at the top of the list. To sort the list by one of the columns, click the column header.

4. To send an e-mail to a contact, click the contact’s **E-mail Address**. A new message dialog opens.

5. To print the current page of the contact list:
   a) Click **Print**. If your browser’s security is set to prompt you before opening or downloading files, click **Open** to open the CSV file.
      
      The content is exported to a CSV file, which you can view in a spreadsheet application, such as Microsoft® Excel.
   b) Print the file.

**Disabling Contacts**

You can change the Contact Status of a contact from Active to Disabled. Disabled contacts do not receive Investigation Report notifications.
NOTE To ensure that contact information for closed Investigation Reports is retained, you cannot delete a contact.

To disable a contact:

1. On the navigation bar click [ ] > Investigations > Investigations Contact List.
2. On the Investigation Report Contact List page, in the Search Criteria area, do the following:
   a) Use one or more of the following criteria to find the contacts you want to disable:
      - **contact name**: search using all or part of the name of the contact
      - **e-mail address**: search using all or part of the e-mail address of the contact
      - **phone**: search using all or part of the contact’s phone number, if recorded in the Absolute console
   b) Click **Show results**. The search results show in the results grid.
3. In the results grid, select the checkbox next to each contact you want to disable. To select all contacts on the current page of the results grid, select the checkbox next to **Contact Name** in the header.
4. Click **Disable**. The Contact Status is set to **Disabled**.

NOTE By default, Disabled contacts are not visible in the Investigation Report Contact List. To view and edit them, select the **Include Disabled Contacts** checkbox in the Search Criteria area and perform a search.

Activating Disabled Contacts

You can change the Contact Status of a contact from Disabled to Active. Only Active contacts receive Investigation Report notifications.

To activate a disabled contact:

1. On the navigation bar click [ ] > Investigations > Investigations Contact List.
2. On the Investigation Report Contact List page in the Search Criteria area, do the following:
   a) Use one or more of the following criteria to find the contacts you want to activate:
      - **contact name**: search using all or part of the name of the contact
      - **e-mail address**: search using all or part of the e-mail address of the contact
      - **phone**: search using all or part of the contact’s phone number, if recorded in the Absolute console
   b) Select the **Include Disabled Contacts** checkbox.
   c) Click **Show results**. The search results show in the results grid.
3. Select the check box next to each contact you want to activate. To select all contacts on the current page of the results grid, select the checkbox next to **Contact Name** in the header.
4. Click **Activate**. The Contact Status for all selected contacts is set to **Active**.
A

Absolute console
Formerly Absolute DDS console, and before that Customer Center. A web-based user interface which enables corporate customers to centrally manage all assets within their account.

Absolute for Chromebooks extension
A small account-specific software program that enables a Chromebook to secure a connection with the Absolute Monitoring Center through which device authentication and inventory data is sent.

Absolute Monitoring Center
The Monitoring Center where devices call for self-healing.

Absolute Persistence
See Persistence Technology.

Activation Date
An event when a device contacts the Absolute Monitoring Center for the first time through the Internet to obtain the managed device’s unique Identifier.

Adapter Equipment ID
An Identifier, which is unique to each broadband adapter. For EVDO adapters, the Identifier and/or the Mobile Equipment ID (MEID) may be reported. For UMTS networks, the International Mobile Equipment Identifier (IMEI) is reported.

Adapter Last Detected Date
When information about a network adapter was last collected.

Adapter Manufacturer
The maker of a mobile broadband network adapter.

Adapter Model
The product type of a mobile broadband network adapter.

Adapter Network
The mobile service provider associated with a mobile broadband adapter.

Agent
A small software client that resides in the BIOS firmware of a device. It is either embedded at the factory or manually installed by a user.
Agent Call
A secure connection established between the agent and the Monitoring Center through which device authentication or inventory data is sent.

Agent Status
The operating condition of an agent. Possible values are Active (indicates that the agent has called the Monitoring Center), Inactive (indicates that the agent has not yet called the Monitoring Center), and Disabled (indicates that the agent is either flagged for removal or removed from the device).

Agent Version
The version number of the agent that contacts the Monitoring Center.

Alert
An alert is a pager or e-mail message that notifies users when specific, user-definable conditions are met.

Alert Event
A record of an alert that was triggered in the Absolute console.

Anti-Malware Software
Anti-virus software that detects, blocks, and removes malicious software from a device.

Anti-Malware Software Vendor
The provider of an anti-virus application that detects, blocks, and removes malware software from a device.

Anti-Malware Software Version
The unique name or number assigned to a particular release of Anti-Malware software.

Application
The smallest unit of software installed on a device that is detected by the agent and reported in the Absolute console.

Application Name
The title of an executable. In practice, many publishers mutually exchange Application Name and Program Name values. See also Program.

ARIN Who IS Info
Information related to the registrant or assignee of a Proxy IP Address.

ASD
Absolute Secure Drive (ASD) supports the new OPAL SEDs, providing our customers with a method to control this encryption technology within their organizations. ASD lets IT administrators configure and set up each SED, and thereby administer users, authentication methods, policies, and system maintenance throughout a managed device’s life-cycle.
Asset Number
An alphanumeric identifier for a device, which is entered in the Absolute console by a user.

Assigned
Entered and/or edited by a user; for example, Assigned Username.

Assigned E-mail Address
The e-mail address of the individual responsible for the device.

Assigned Username
The username assigned to a device by an Administrator.

Authentication
A way to establish the credibility of a user. Security operations are authenticated using either RSA SecurID tokens or unique e-mailed security authorization codes. The authentication method is specified on the Security Administration Authorization Agreement. See Authorization.

Authorization
A permission held by a user. When a signed Absolute Security Administration Authorization Agreement is received and filed by Absolute, designated Security Administrators and Security Power Users can perform security operations, such as Data Delete or Device Freeze, by requesting security authorization. The authentication method, which is either sending e-mail messages with an authorization code or purchasing RSA SecurID tokens and using the randomly generated authorization codes, is selected when completing the agreement.

Authorization Code
A globally unique identifier that is e-mailed to a Security Administrator in response to a request made in the Absolute console. The code is represented as a 32 character hexadecimal character string. This authorization code also refers to the randomly generated codes generated by an RSA SecurID token.

Available Violations
The number of purchased licenses for an application that are available for installation on devices. A negative value in this column indicates that your organization has exceeded its number of purchased licenses.

B

Banned Items List
The list of software applications that your organization has deemed are banned (not allowed) in its Software Policy. You can view this list on the Software Policy Non-Compliance Report.

Browser Name
The name of a software application used to navigate the Internet.

Browser Version Number
The unique name or number assigned to a particular release of a web browser.
C

Call Time
When a device contacted the Monitoring Center.

Caller ID
A telephone company service describing the origin of an incoming call, including the phone number. See also Public IP Address.

Change Status
Indicates whether a detected difference involves New, Removed, or Changed hardware or software.

Chrome device
A personal computer running the Chrome OS operating system. Chrome devices include Chromebooks (laptop computers) and Chromeboxes (desktop computers).

Code Division Multiple Access (CDMA)
CDMA is a channel access method used by various radio communication technologies.

Confidence Level
The estimated accuracy of a Location. Possible values are High and Low.

Cost Center/Code
A unique identifier for a unit for which costs are accumulated or computed.

CPU Name
The known identification of the microprocessor in a device.

CPU Speed
The rate at which a microprocessor computes.

CTM Web Application
Also known as CTMWeb.exe or Agent Management Utility, an application that lets users verify and manage the agent’s installation on a device.

Current port
The port to which a modem currently installed in a device is connected.

Custom Action Field
An attribute of a Data Delete or Device Freeze request that a user can create and edit. The field can be set to contain a date, a list option, or text. Values for the fields are maintained by input from users.
**Custom Device Field**
An attribute for a device that a user can create and edit. The field can be set to contain a date, a list option, or text. Values for the fields are maintained by input from users.

**Data Delete**
A remote data deletion function that enables an authorized user to delete sensitive data on targeted devices in case of theft or loss. The function can also be performed at a device’s end-of-life or end-of-lease.

**Data Delete Policy**
A user-definable file created to enable users to specify files and/or file types to be deleted on targeted devices on the Windows platform. The file can also be used to delete registry key entries and/or files from registry key entries.

**Data Wipe**
The Data Overwrite feature deletes the specified data and overwrites it with random, or garbage, data to make the original data impossible to recover. The overwrite process is called a data wipe.

**Date Change Detected**
When a difference was detected.

**Date Stolen**
The date and time stamp when it was noticed that a device was missing.

**Department**
A user-created attribute for a device that is included in the filter of many reports.

**Detected**
Identified by the agent during a call to the Monitoring Center.

**Detected Phone Number**
The phone number associated with a mobile broadband adapter, as reported by the device.

**Device**
A piece of electronic communication hardware on which the agent can be installed, such as Windows computers, Macintosh computers, or mobile handsets.

**Device Freeze**
A function managed in the Absolute console which enables an authorized user to specify the devices to show a full screen message restricting device users from operating the device.
Device Group
A way to organize managed devices into various groupings based on areas of commonality. 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 where the devices are located), and other criteria.

Device Name
The name given to a device.

Dormant Devices
Administrators may assign this status to devices that do not call in to the Monitoring Center on a regular basis.

Drive Description
Indicates the detected description for this device’s hard drive; for example, on the Full-Disk Encryption Status Report.

Drive Letter
The alphabetical identifier for a physical or logical disk drive or partition.

Drive Serial Number
Indicates the detected serial number; for example, for the full-disk encryption drive detected on a device.

Encryption Status
The current or last known status of full-disk encryption for devices.

Encryption Status String
Each encryption vendor uses specific encryption status strings in their products. The Full-Disk Encryption Status Report shows the detected string from the full-disk encryption vendor, which could be truncated due to length.

Encryption Type
Found on the Full-Disk Encryption Status Report, indicates whether the device’s detected full-disk encryption is Software or Hardware.

End User Messaging (EUM)
A function managed in the Absolute console that enables a user to specify the devices on which to show a message during the agent call to the Monitoring Center. The content and rules for messages are customizable, and messages can also be used for data input from device users.
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) and/or the Mobile Equipment ID (MEID) are reported. For GSM and UMTS smartphones, the International Mobile Equipment Identifier (IMEI) is reported.

Event Calling
A feature that enables Windows and Mac devices to make an agent call when a specific event, such as a change in installed software, occurs on a device.

Event Details
A description of an activity related to user administration in the Absolute console.

Executable File
A computer file that contains a program that is ready to be run or carried out.

Export (Data/Group)
A function in the Absolute console that enables users to download files, which contain information on device data or device groups, in multiple formats.

F

First Call Date
When the agent on a device first called in to the Monitoring Center.

FQDN
Fully Qualified Domain Name (FQDN) of a device, which includes the device name, domain name, and all higher-level domains. This value shows on the Device Drift by Device report under the Full Windows Device Name column.

Full-Disk Encryption (FDE)
A software or hardware solution that secures, or encrypts, the entire contents of a physical drive. FDE prevents unauthorized access to data storage. The agent detects FDE Hardware (self-encrypting drives) and Software encryption programs that are installed on the hard drives of your organization’s tracked devices.

Full Windows Device Name
The Fully Qualified Domain Name (FQDN) of a device, including the device name, domain name, and all higher-level domains.

G

Geofences
A function in the Absolute console that lets users specify boundaries of areas on a map and track devices based on Geolocation Tracking data.
**Global System for Mobile Communications (GSM)**
GSM is a standard set developed by the European Telecommunications Standards Institute that describes technologies for second generation digital cellular networks.

**Group**
See Device Group.

**GUID**
Globally Unique IDentifier.

**H**

**Hard Drive Free Space**
The amount of storage currently available on a hard disk.

**Hard Drive Serial Number (HDSN)**
The manufacturer’s serial number associated with the hard drive installed on a device. 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. Whatever WMI reports, which is provided by Microsoft or your hardware and/or software vendors, is shown on the Hardware Configuration and OS Change Report.

**Hard Drive Size**
The maximum capacity of a hard disk.

**Hard Drive Space Threshold**
The minimum amount of storage on a hard disk that needs to be unavailable for a device to show in the results grid.

**Hard Drive Total Free Space**
The amount of storage currently available on all hard disks installed in a device.

**Hard Drive Total Size**
The maximum capacity of all hard disks installed in a device.

**Hard Drive Total Used Space**
The amount of storage currently unavailable on all hard disks installed in a device.

**Hard Drive Used Space**
The amount of storage currently unavailable on a hard disk.

**Hardware Asset**
A traditional device, such as a laptop or desktop computer, or a mobile device, such as a smartphone or tablet.

**Hardware Description**
The type of hardware that changed.
**Hardware Profile**  
The collection of Identification Points that define a device.

**Has Service Guarantee**  
Indicates whether a payment may be issued if attempts to run a guaranteed service fails.

---

**Identification Points**  
The inventory items designated to identify and return self-healing devices to the Monitoring Center. Also referred to as data points.

**Identifier**  
A unique Electronic Serial Number assigned to the agent installed on a device.

**IMEI**  
International Mobile Equipment Identity. See Equipment ID.

**Import (Data/Group)**  
A function in the Absolute console that enables users to upload files in multiple formats, which contain information on device data or device groups.

**Install Source**  
The full directory path to the folder containing the installation files for a program.

**Installation Directory**  
The full directory path to the primary folder where a program is installed.

**Inventory Record**  
When the agent makes its first activation call, the Monitoring Center creates a record (in a database) of the details about this device’s Identification Points, based on the device’s Hardware Profile settings, which you configure.

**Investigation Report**  
A report available in the Absolute console that is filled out and sent online by users to notify Absolute of a theft or loss of a device.

**IP Address**  
A unique number identifying a computer on the Internet. See also Local IP Address and Public IP Address. In the Absolute console, enter IP addresses in the format [1-255],[0-255],[0-255],[0-255]. You can use the asterisk (*) wildcard character. For example, to search for all IP addresses in the range 127.10,[0-255],[0-255], type 127.10.*.*
L

Last Agent Call
The date and timestamp that indicates when the device last made an agent call.

Last Call
The date and timestamp when the agent installed on a device most recently contacted the Monitoring Center. If available, clicking the Last Call Date or Last Call Time links open the Call History page for the device.

Last Call Date
The date and timestamp when the agent installed on a device most recently contacted the Monitoring Center. If available, clicking the Last Call Date or Last Call Time links open the Call History page for the device.

Last Call Time
The date and timestamp when the agent installed on a device most recently contacted the Monitoring Center. If available, clicking the Last Call Date or Last Call Time links open the Call History page for the device.

Last Reboot
The date and timestamp when this device was last restarted.

Latest Service Pack
The most recent collection of updates, fixes and/or enhancements to a software program delivered in the form of a single installable package.

License Name
The known identifier of an installed application.

Licenses Available
The difference between the number of installations of an application and the number of Licenses Purchased.

Licenses Purchased
The number of owned licenses for an application.

Local IP Address
The IP address assigned to a device on the Local Area Network (LAN) when calling the Monitoring Center. See also IP Address and Public IP Address.

Local IP RDNS
The domain name associated with a Local IP Address. See also Proxy IP RDNS.

Location
The position of a device on the surface of the earth expressed in latitude and longitude.
**Location Technology**
A technology, such as GPS or Wi-Fi Positioning, used to determine the location of a device.

**Location Time**
The timestamp that indicates when the position of a device was recorded.

**MAC Address**
For laptops and computing devices with mobile broadband adapters, the Media Access Control (MAC) address is the hardware address that uniquely identifies each node of a network, such as Ethernet, or the mobile broadband adapter used to complete a call to the Monitoring Center. For smartphones, it is the MAC address detected on the smartphone, most commonly the Wi-Fi MAC address. Some platforms may also have an Ethernet MAC address.

**Make**
The manufacturer of a device or other hardware.

**MEID**
Mobile Equipment Identifier. See Equipment ID.

**Mobile Broadband Adapter Tracking (MBAT)**
This service permits Absolute customers to view a list of mobile broadband adapters and their attributes including equipment, subscriber, and network information in the Absolute console.

**Model**
The product type of a device or other hardware.

**Monitor Refresh Frequency**
The scanning rate of a display.

**Monitoring Center**
A server with which the agent makes a secure connection to send device authentication and inventory data (also called Identification Points). See also Absolute Monitoring Center.

**Monitoring Center-initiated Calling (MCIC)**
A feature that lets customers remotely initiate an agent call using the Absolute console. Monitoring Center-initiated calling, under specific circumstances, enables a drastic reduction in the time required to initiate action on the targeted device.

**Operating System**
Software that controls the running of computer programs and may provide various services.
Organizational unit
A Google account term that has relevance for managed Chrome devices. An organizational unit allows services and features to be made available to one or more users through the configuration of policies.

Persistence Status
The status of the Absolute Persistence module on a managed device. Possible values are: BIOS/Firmware Active, BIOS/Firmware Pending, and N/A. A device’s Persistence Status is indicated on the Activation Report.

Persistence technology
Includes BIOS and Firmware persistence. Activated during the agent’s first call to a Monitoring Center. Checks for the status of the agent and initiates self-healing to restore the agent if it is missing, tampered with, or damaged.

Program
An executable file on a device that is detected by the agent and reported in the Absolute console. See also Application Name.

Proxy IP RDNS
Results of performing a Reverse Domain Name System (RDNS) lookup on a Proxy IP Address.

Public IP Address
The IP address used to communicate with the Internet. For modem calls, caller ID information is reported instead. See also IP Address, Local IP Address, and Caller ID.

Publisher
A company or organization selling applications that is detected by the agent and reported in the Absolute console.

RAM Size
The amount of dynamically accessible memory in a device.

Required Item List
The list of software applications that your organization has deemed are required (must be installed on all devices) in its Software Policy. You can view this list on the Software Policy Non-Compliance Report.

Results grid
The table that is populated underneath the search or filter criteria location on a Absolute console page and which is based on the specified filtering criteria. Also called a report table.
RTT
Real-Time Technology (RTT) is a feature that lets you track your mobile broadband-enabled devices. Additionally, this feature leverages mobile broadband and SMS (text) messaging to increase the speed to run security operations on devices in your account.

RTT-IP
Real Time Technology over Internet Protocol (RTT-IP) lets you initiate security operations on your managed Windows and Mac devices without waiting for the next scheduled agent call. RTT-IP can be enabled at the account level or the device level. See also Monitoring Center-initiated Calling (MCIC).

S

SCCM client
A small software application installed on each Windows device to allow the device to connect to the SCCM server and be managed remotely. Also see "System Center Configuration Manager (SCCM)".

SCCM Repair
A feature that works in conjunction with SCCM Status reporting. If the SCCM client installed on a Windows device is not functioning correctly, SCCM Repair attempts to repair the client. Also see "SCCM Status" and "System Center Configuration Manager (SCCM)".

SCCM Status
The status of the SCCM client installed on a Windows device. The agent can be configured to detect a device's SCCM Status. Also see "System Center Configuration Manager (SCCM)".

Security Administrator
A user role that exists in those organizations that choose to designate certain Administrators as Security Administrators to manage the device and data security of assets. This user role has more access rights than Administrators. Security Administrators have the authority to configure, target, and start File Retrieval, Device Freeze, and Data Delete services. Security Administrators use the Absolute console to track and manage devices, both within the organization's local area network and outside of it.

Security Power User
A user role that exists in those organizations that choose to designate certain Power Users as Security Power Users to manage the device and data security of assets. This user role has more access rights than Power Users. Security Power Users have the authority to configure, target, and start File Retrieval, Device Freeze, and Data Delete services for devices in their assigned Device Group. Security Power Users use the Absolute console to track and manage devices within the organization's local area network.

Self-Encrypting Drive (SED)
A type of drive that is capable of FDE and can be detected by the agent, but may not be enabled or may not be supported by Absolute.
Self-Healing Call (SHC)
When agent modules are corrupted or tampered with, or when attempts are made to remove the agent from a device, the technology rebuilds (self-heals) itself.

Serial Number
The serial number of the device or other hardware.

Service Guarantee
For Premium accounts, the End User Service Agreement provides remuneration in the event that the Absolute Investigations and Recovery Services team is unable to recover a stolen managed device.

Service Pack
A collection of updates, fixes and/or enhancements to a software program delivered in the form of a single installable package.

SIEM
Security Information and Event Management (SIEM) applications collect logged events from multiple software programs and store them in a central repository for consolidated reporting and analysis. You can enable Absolute alert events to be viewed in a SIEM application.

SMS
Short Message Service (cellular phone text messaging).

Software Policy
A list of software requirements that consists of Banned and Required software titles. A Software Policy is applied to Device Groups to identify non-compliant devices.

Software Status
The type of compliance status of a software installation with a Software Policy. The possible values include Banned and Required.

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.

Suspicion Level
The importance level or grade that defines the severity of a suspicious event.

Suspicious event
An event that triggered one or more alert notifications based on alerts defined for the account.

System BIOS Date
When the Basic Input/Output System (BIOS) installed in a device was released.
**System BIOS Version**
The unique name or number assigned to the Basic Input/Output System (BIOS) of a device.

**System Center Configuration Manager (SCCM)**
Microsoft System Center Configuration Manager (SCCM) is a system management software product that lets IT administrators manage their Windows devices by performing tasks remotely.

**Threshold Value (MB)**
For hard disks, the minimum preferred amount of available storage (expressed in MB) on a device’s logical drive to show in reports.

**Username**
A unique name detected by the agent to identify a person who is associated with or using a device.

**Version**
A number that distinguishes releases of the same software application, sold separately, that is detected by the agent and reported in the Absolute console. See also Agent Version.

**Video Display Color Depth**
The number of bits used to represent color on a monitor.

**Video Display Resolution**
The number of distinct horizontal and vertical pixels showing on a monitor.

**Volume**
A single accessible storage area with a single file system that is resident on a single partition of a hard disk.

**Volume Label**
The descriptive name assigned to a volume on a hard disk, such as Local Disk or Public.

**Wi-Fi**
A technology that allows electronic devices to connect to the Internet or communicate with one another wirelessly within a particular area over radio waves.
**Wi-Fi hotspot**

A private or public location where Internet access is available via a WLAN (wireless local area network).
Index

A

Absolute for Chromebooks
  adding Google account details to the Absolute console 285
  Chromebook Extension about 284
deploying 287
described 284
  Google Synchronization Service 285
Absolute for iPads
  removing iPads enrolled 77
Absolute Manage suite 69
Absolute Secure Drive
  turning data collection for your account off 55
on 55
Absolute Secure Drive Authentication Failures Report 130
Absolute Security Administration Authorization Agreement
  Authorized Signatory and Signing Officer form 266
described 266
  for performing security operations 198
  geolocation tracking activation, described 266
Absolute SIEM Connector
  downloading 71
  sending alerts using 16
Account Management reports 176
Account section, described 54
acknowledged end user message 37
activating
  an end user message 36
  custom alerts 25
  encryption alerts manually when you turn
    Full-Disk Encryption data collection on again 55
  predefined alerts 25
Activation Report 158
Active alert state 15
adding
  applications to the
    Banned Items list in a software policy 52
    Required Items list in a software policy 52
devices to a
  Device Freeze offline policy 249
device group 43
device group automatically using the
  auto-grouping feature 45
multiple devices to a device group by import-
...
suspending
alert scanning 26
alerts 26
suspicious activity on devices, described 15
triggering an alert, described 15
types
custom 15
viewing
alerts 24
triggered alert events 27
Anti-Malware Report 125
API and other sampling technologies 163
Asset Report
described 94
viewing a complete overview for specific
devices that have the Agent 94
WMI reporting hard disk serial numbers
based on Microsoft or vendor’s inform-
ation 94
Asset Summary information 81
Assigned Username field
described 90
assigning
device groups automatically 45
associating devices with device groups,
described 43
attempting a forced call 188
audience for this guide 12
Authorized Signatory and Signing Officer
form 266
authorizing a security service using an
RSA SecurID Token code 202
authorizing security personnel using an
e-mailed authorization code 203
auto-grouping feature used to add devices to a
device group automatically 45
automatic assignment of available Service Guar-
antee Licenses for your account
turning off 55

B
Banned Items, adding them to the software
policy 52

C
Call History and Loss Control reports 152
Call History Report 153
Calling Profiles Report 177
cancelling
Data Delete request for
a single device 230
multiple devices at the same time 230
Device Freeze request for
a single device 239
multiple devices at the same time 239
cell tower/network location technology 163
cellular technology used to maintain network con-
nectivity 185
Change in Serial Number predefined alert 16
changing
an e-mail address for security personnel 203
the number of records shown in a report 80
choose feature, described 79
Chromebook Extension
about 284
deploying 287
role of Google Synchronization Service 285
Chromebooks
Chromebook extension
about 284
deploying 287
Classic Account Settings page
adding Google account details 285
editing
automatic assignment of available Ser-
vice Guarantee Licenses 54
off 55
described 54
RTT-IP settings for your account 57
enabling last file access dates and times 56
Event Calling
ingiting Call Settings 62
turning
Absolute Customer Service access
off 56
on 56
Absolute Secure Drive data collection
off 55
on 55
Event Calling for your account
off 63
on 61
Full-Disk Encryption data collection
off 55
on 55
Google Maps Wi-Fi Positioning
on 56
SCCM Repair on 65
SCCM Status reporting on 64
cloning an existing Investigation Report 299
consequences of disabling the preauthorization
agreement 199
Contact list. See Investigation Report Contact
List
conventions used in this guide 14
copying
a software policy 53
creating
custom
Device Freeze messages 261
custom action fields 204
custom alerts 19
Data Delete

- enabling last file access dates and times 56
- managing custom action fields 204
- minimum system requirements 209
- prerequisites to a request 210
- request
  - cancelling for a single device 230
  - multiple devices at the same time 230
- requesting 211
- viewing status 223

Data Delete Details page 225

- defining
  - devices associated to device groups automatically 45
  - manually 47

- deleting
  - custom action fields 205
  - custom alerts 27
  - custom Device Freeze messages 263
  - Device Freeze offline policy 251
  - device group 49
  - end user messages 39
  - geofences 271
  - software policy 54

- deletion policies
  - editing one 223
  - file entries you can use described 219
  - no boot with log file 219

- detecting
  - devices with Full-Disk Encryption products 55
  - devices without Full-Disk Encryption products 55
  - full-disk encryption software products and self-encrypting drives 133

- Device Drift by Device Name Report 156
- Device Drift by Username Report 157
- Device Drift History Report 157
- viewing more detailed caller ID information 157

Device Freeze

- described 234
- editing Device Freeze messages 263
- forcing a reboot on Windows devices 238
- managing custom action fields 204
- minimum system requirements 234

- offline policy
  - about 241
  - adding devices to 249
  - creating 242
  - deleting offline policies 251
  - designating a default policy 247
  - editing 246
  - removing devices from 250
  - viewing 244
  - viewing devices 248

D

- data and device security administration
  - changing the e-mail address for security personnel 203
  - described 197
  - disabling your Security Administrator authorization agreement 199
  - providing an RSA SecurID Token code 202
  - requesting an e-mailed security authorization code 203
Device Location History Report 168
Device Location Report 165
Device Readiness Report 102
Device Rebuild predefined alert 17
Device Summary page
Asset Summary information 81
Call Tracking information 84
configuring Event Calling for a device 86
described 81
Forced Call log 188
Hardware Details information 83
Hardware Summary information 83
SCCM Status history information 85
Software Details information 84
turning on SCCM Repair 89
turning on SCCM Status reporting 88
viewing call history 88
device groups 88
adding devices to a
device group automatically using the auto-grouping feature 45
single device group 43
multiple devices to a device group by importing CSV files 47
associating devices with a device group 43
creating Investigation Report for multiple stolen devices 299
data and device security administration,
described 197
deleting
device groups 49
downloading data delete log file 232
log file for a single device 232
mobile devices 233
multiple devices 232
editing
details for a single device with a mobile broadband adapter 187
details for a specific device 81
Identifier’s asset information 80
information for a device group 42
filtering to find a specific device group 42
finding devices that are ready for retirement 102
identifying hardware components that need an upgrade 102
importing a CSV file for IP mapping to a device group 46
locating those that cannot support a particular software or operating system rollout 102
removing devices from device groups 49
setting up dormant devices 90

Device Freeze Summary Report 251
device groups adding devices to a group 43
devices to a group automatically using the auto-grouping feature 45
multiple devices to a device group by importing CSV files 47
Asset Summary information 81
assigning devices automatically 45
associating a device with a device group 43
creating 40
defining what devices are assigned to which device group manually 47
deleting
device groups 49
described 39
editing information for a device group 42
filtering to find a specific device group 42
Hardware Details information 83
Hardware Summary information 83
importing
a CSV file for IP mapping 46
an edited CSV file 48
removing
a device group from a software policy 53
devices associated with a device group 49
viewing
all device groups 41
device groups without a software policy 51
devices associated with a device group 49
software policies applied to device groups 50
specific device group 42
Device History Report
viewing 157

request
canceling for a single device 239
multiple devices at the same time 239
detailed information 255
removing its details and the consequences 240
states 255
tracking the status 251
unfreeze passcode for Device Freeze operation 259
viewing the status 254
requesting 236
scheduling for future date 236
unfreezing
a frozen device using an unfreeze passcode 260
a single device on an Agent call 258
multiple devices on an Agent call 259

Device Freeze Summary Report 251
device groups adding
devices to a group 43
devices to a group automatically using the auto-grouping feature 45
multiple devices to a device group by importing CSV files 47
Asset Summary information 81
assigning devices automatically 45
associating a device with a device group 43
creating 40
defining what devices are assigned to which device group manually 47
deleting
device groups 49
described 39
editing information for a device group 42
filtering to find a specific device group 42
Hardware Details information 83
Hardware Summary information 83
importing
a CSV file for IP mapping 46
an edited CSV file 48
removing
a device group from a software policy 53
devices associated with a device group 49
viewing
all device groups 41
device groups without a software policy 51
devices associated with a device group 49
software policies applied to device groups 50
specific device group 42
Device History Report
viewing 157
turning
  data collection for Absolute Secure Drive
    off 55
    on 55
  Event Calling for a device
    off 86
    on 86
  Event Calling for your account
    off 63
    on 61
  Full-Disk Encryption data collection
    off 55
    on 55
unfreeze before requesting a Data
  Delete 210
unfreezing a frozen device using an unfreeze
  passcode 260
viewing
  a list of mobile broadband adapters
    installed and operational on man-
    aged devices 105
  all device groups 41
  details for a single device with a mobile
    broadband adapter 187
details for a specific device 81
log file for
  a single device 232
  mobile devices 233
  multiple devices 232
managed devices that have Event Calling
  turned on 63
managed devices with SCCM Status
  reporting turned on 66
memberships in a device group 49
specific device group 42
total, used, and available disk space for
  each device 101
with Full-Disk Encryption cannot submit an
  End of Lease/Life Data Delete
  request 210
Devices by License Report 115
disabling
  consequences to 199
  RTT-IP 195
  Security Administrator authorization 199
dormant devices
  described 90
Download Packages page
  Absolute Manage Persistence section 69
  Absolute Manage section 69
  Agent section 67
downloading
  a CSV or XML file that identifies installed
    monitor drivers 98
a CSV or XML file that identifies installed
    printer drivers 97
  Absolute Manage installation packages 69
  Absolute SIEM Connector 71
and submitting the Absolute Security Admin-
  istration Authorization Agreement 198
data delete log file 232
File List request 280
reports, described 92
retrieved files 275
the Agent 67
the log file for
  a single device 232
  mobile devices 233
  multiple devices 232
triggered alert events 29

E

e-mailed
  security authorization codes for security oper-
  ation 203
  security authorization codes for security per-
  sonnel 203
editing
  alerts
    custom 25
    predefined 25
  asset information for a device 80
  assignment of Service Guarantee licenses
    manually for a
    group of devices 58
    single device 58
  Classic Account Settings 54
custom
    Device Freeze messages 263
    end user messages 33
custom action fields 204
deletion policies 223
details for a single device with a mobile
  broadband adapter 187
details for a specific device 81
device group’s information 42
existing geofences 270
information for an existing Investigation
  Report 297
license information using the Software
  License Compliance Overview
  Report 115
  RTT-IP settings 57
  saved report filters 91, 184
  software policy 53
  URL end user messages 35
enabling
  geolocation reporting 164
  Security Administrator authorization
    again 199
Encryption History Report 139
Encryption Status Report
turning on full-disk encryption data
  collection 133
End of Lease/Life Data Delete request described 210
problems for devices with Full-Disk Encryption 210
end user messages, see End User Messaging
End User Messaging activating a message 36
creating custom messages 30
URL messages 32
deleting end user messages 39
described 29
editing custom messages 33
URL messages 35
minimum system requirements 29
previewing 33
resending a message 38
suspending a message 36
types custom messages 29
URL messages described 29
viewing a list of end user messages 30
end user messages that were acknowledged 37
were not acknowledged 37
ensuring security operations are conducted safely 197
error codes for Intel AT 207
ESRI map, when used in the Absolute console 267
Event Calling described 59
device changes that trigger a call 60
for a device turn it off 86
turn it on 86
viewing call history 88
for your account editing Call Settings 62
turn it off 63
turn it on 61
viewing managed devices that have Event Calling turned on 63
Minimum Event Call Period 61
exporting a software policy to an Excel spreadsheet 54
Extended IP Call Information page, described 153

F
file entries for deletion policies 219
File List 278
downloading a request 280
minimum system requirements 278
requesting 278
requesting one for stolen devices 279
tracking the status 280
File Retrieval cancelling request 276
changing status 275
downloading files 275
minimum system requirements 272
removing log files 276
requesting 273
filtering a report’s results 79
alert events by date alert event was triggered 28
specific alert event 28
suspicion level 28
data to create a Full-Disk Encryption Status report 134
existing Investigation Reports 291
to locate specific device groups 42
finding devices that are ready for retirement 102
devices with self-encrypting drives capable of full-disk encryption 132
Forced Call log, described 188
Forced Call request status 189
forcing a call on devices with mobile broadband adapters 188
a reboot on Windows devices when the Device Freeze request completes 238
freezing devices Device Freeze offline policy 242
Device Freeze request 236
full-disk encryption described 132
filtering data to create a Full-Disk Encryption Status report 134
finding SEDs capable of full-disk encryption 132
identifying devices that have an SED installed 136
have full-disk encryption products installed 136
have no full-disk encryption products installed 138
reactivating a suspended alert 26
software products and self-encrypting drives detected 133
status-based alert 22
turning it on in Classic Account Settings 133
Encryption Status Report 133
viewing a device’s full-disk Encryption History report 139
changes to a device’s full-disk encryption status string 139
when to decrypt a device 210
Full-Disk Encryption Status Report 132
creating a full-disk encryption alert 23
turning detection of FDE products for your account off 55
on 55

G

gathering
 asset data from iPads 76
generating a server recovery token to unlock a locked Intel AT device 207
Geofence Editor, described 267
Geofence Tracking reports, described 267
geofences
 creating 268
 deleting 271
 editing 270
 example of a Geofence Location alert 21
 explained 265
 Geofence Editor, described 267
 security checks 265
 using the technology 266
 viewing a list of them 269

ger

global
 Authorization form 164
 collecting location information 164
 enabling reporting 164
 limitations of
 GPS 163
 Wi-Fi positioning 164
 system requirements 161
 Tracking Activation form 266
 tracking reports, described 267
 tracking, described 265
types of location technologies, described 163
Global Positioning Systems. See GPS.
Google Maps
 using in prohibited country 267
 using navigation tools
 in Geofences 267
 in reports 167
 Wi-Fi Positioning
 definition 163
 enabling 56
Google Synchronization Service
 about 285
 enabling 285
GPS
 described 163
 limitations 163
Guest User user role, described 13

H

Hard Disk Space Report 101
Hard Drive is Nearly Full predefined alert 17
Hardware Configuration and OS Change Report 99
Hardware Details information 83
Hardware Summary information 83

I

identifier, editing asset information 80
identifying
 devices that
 have an SED installed 136
 have full-disk encryption products installed 136
 have hardware or operating system changes 99
 have no full-disk encryption products installed 138
devices that do not meet specified minimum requirements for hardware or operating system 102
hardware components that need an upgrade 102
importing
 a CSV file for IP mapping 46
 an edited CSV file for device groups 48
iPad data into the Absolute console 76
initiating a forced call on devices with mobile broadband adapters 188
Installed Programs by Account Report 120
Installed Programs by Device Report 118
Installed Programs by Device Report, details 121
Installed Software Overview Report 109
Intel AT
 concluding the service 206
 generating a server recovery token to unlock a locked device 207
 link to troubleshooting table 207
 other ways to protect your devices 206
 troubleshooting disenrollment 206
 unlocking locked devices using a server recovery token 208
Internet Browsing Configuration Report 123
Investigation Report
 adding additional contacts 296
 cloning 299
 closing 299
 contact list, managing 300
 creating
 stolen devices 295
editing the information on the Investigations
Summary page 297
filtering 291
status definitions 291
viewing 291
history 293
report history table 293
Investigation Report Contact List
about 300
activating Disabled contacts 303
adding contacts 300
Contact Status
about 300
changing status of a contact 302-303
disabling Active contacts 302
editing contact information 301
printing the contact list 302
viewing the contact list 302
IP georesolution 163
iPads
gathering asset data 76
importing data into the Absolute console 76
meeting your Service Guarantee 76
prerequisites for
removing iPad devices enrolled 77
removing iPads enrolled 77

L
Last called 20 days ago predefined alert 17
Lease Completion Report 171
Lease Ending predefined alert 17
License Usage Summary Report 176
licenses
editing information using the Software
License Compliance Overview
Report 115
limitations of
GPS technology 163
Wi-Fi positioning 164
Local IP Address Changed predefined alert 17
locating devices
outside your corporate network 153
that cannot support a particular software or
operating system rollout 102
location technologies
Absolute Wi-Fi Positioning 163
API and other sampling technologies 163
cell tower/network 163
Google Maps Wi-Fi Positioning 163
GPS 163
IP georesolution 163
Other Location Technologies 163
log files
downloading 232
for a single device
downloading 232
viewing 232
for mobile devices
downloading 233
viewing 233
for multiple devices
downloading 232
viewing 232

M
Major Change predefined alert 17
managing
custom alerts 24
custom Device Freeze messages 261
predefined alerts 24
tiggered alert events 27
manually
defining what devices are assigned to which
device groups 47
editing the assignment of Service Guarantee
licenses for a group of devices 58
editing the assignment of Service Guarantee
licenses for a single device 58
Microsoft Audit Summary Report 116
Minimum Event Call Period 61
minimum system requirements needed for
Data Delete 209
Device Freeze security operation 234
End User Messaging 29
File List 278
File Retrieval 272
RTT 185
RTT-IP 190
Missing Anti-Malware Report 126
Missing Devices Report
described 155
Missing Software on Required List predefined
alert 18
Mobile Broadband Adapter Details page, view-
ing for RTT-enabled devices 187
Mobile Broadband Adapter Report 105
Mobile Device Report 106
Mobile Theft Management service
for Chrome devices 284
Modem Addition Report 127
Modem Changed predefined alert 18
monitor drivers, downloading a CSV or XML file
that identifies installed monitor drivers on
devices 98
Monitor Report 98
moving
between pages in a report 80
My Content 183
described 183
My Filters 183
My Reports 183
My Filters 183
My Reports 183
N
Network Changed predefined alert 18
Network Diagnostics Tool 68
New Program File Detected predefined alert 18
no boot with log file deletion policy entry 219

O
offline policy. See Device Freeze opening
  Data Delete Details page 225
  Device Summary page 81
  Reports page 78
  Software Policy page 50
Operating System Changed predefined alert 18
Operating System Updates Report 122
OS Product Key Changed predefined alert 18

P
passcode
  used to
    unfreeze a frozen device 260
policies
  Device Freeze offline policy. See Device Freeze 241
  software policy described 50
Power User user role, described 13
predefined alerts
  activating them 25
  Agent is Newly Installed 16
  Change in Serial Number 16
described 16
  Device Name Changed 16
  Device Rebuild 17
  editing them 25
  Hard Drive is Nearly Full 17
  inability to delete them 16
  Last called 20 days ago 17
  Lease Ending 17
  list of default alerts 16
  Local IP Address Changed 17
  Major Change 17
  managing them 24
  Missing Software on Required List 18
  Modem Changed 18
  Network Changed 18
  New Program File Detected 18
  Operating System Changed 18
  OS Product Key Changed 18
  Public IP Address Changed 18
  resetting them 26
  searching for 24
  Self Healing Call 19
  Software on Banned List 19
  suspending alert scanning 26
  suspending them 26
  Username Changed 19
  viewing them 24
  Warranty Ending 19
prepaid Service Guarantee balance 294
Prepaid Service Guarantee balance
  viewing 294
prerequisites for
  Data Delete requests 210
  removing iPads enrolled 77
  previewing end user messages 33
printer drivers
  downloading a CSV or XML file that identifies
    installed printer drivers on devices 97
Printer Report 97
printing
  reports 90
  the current page of a report 91
providing RSA SecurID Token codes for security
  services 202
Public IP Address Changed predefined alerts 18

R
reactivating a suspended alert 26
Real-Time Technology. See RTT.
Remote File Retrieval 272
removing
  Device Freeze Request details and the con-
dsequences 240
  device from
    Device Freeze offline policy 250
device group from a software policy 53
devices from
  device groups 49
  from enrolled iPads 77
Reports
Account Management
  Calling Profiles report 177
  License Usage Summary report 176
  Security Audit Logs report 181
  User Audit report 179
  User Event report 180
Call History and Loss Control
  Activation report 158
  Call History report 153
described 152
  Device Drift by Device Name report 156
  Device Drift by Username report 157
  Device Drift History report 157
  Device Location History report 168
  Device Location report 165
Extended IP Call Information page, loc-
cating devices outside your cor-
porate network 153
  Missing Devices report 155
changing the number of records shown 80
editing saved reports 91
Encryption Status Report, turning on full-disk
encryption data collection 133
filtering
a report's results 79
Investigation Reports 291
finding devices that are ready for
retirement 102
Hardware Assets
Asset report 94
Device Readiness report 102
Hard Disk Space report 101
Hardware Configuration and OS Change
report 99
Mobile Broadband Adapter report 105
Mobile Device report 106
Monitor report 98
Printer report 97
identifying
devices that do not meet specified min-
imum requirements for hardware
or operating system 102
hardware components that need an
upgrade 102
Lease and Inventory Management
Lease Completion report 171
User-entered Data report 174
lease management, described 171
locating devices that cannot support a par-
ticular software or operating system
rollout 102
loss control, computer drift history 158
moving between pages 80
MyContent
My Filters 183
My Reports 183
printing
reports 90
the current page of a report 91
saving 91
Security
Absolute Secure Drive Authentication Fail-
ures report 130
Anti-Malware report 125
Encryption History report 139
Full-Disk Encryption Status report 132
Internet Browsing Configuration
report 123
Missing Anti-Malware report 126
Modem Addition report 127
Operating System Updates report 122
SCCM Status History Report 146
SCCM Status Report 142
Security Posture Report 151
Suspicious Devices report 129
Unauthorized Software report 124
Software Assets
Devices by License report 115
Installed Programs by Account report 120
Installed Programs by Device report 118
Installed Programs by Device report,
details 121
Installed Software Overview report 109
Microsoft Audit Summary report 116
Software by Device report 112
Software Configuration Change
report 111
Software License Compliance Overview
report 114
Software Policy Non-Compliance
report 117
viewing
complete overview for specific devices
that have the Agent installed 94
details about mobile devices (Smart
Phones, Tablets) 106
entire row in a report record 80
list of mobile broadband adapters
installed and operational on man-
aged devices 105
total, used, and available disk space for
each device 101
Reports page, opening it 78
request 203
requesting
a Data Delete operation 211
a Device Freeze 236
a File List 278
a File Retrieval 273
an unfreeze passcode for a Device Freeze
security operation 259
e-mailed security authorization code for
security personnel 203
File List on a stolen device 279
Required Items list, adding to the software
policy 52
resending messages to end users 38
resetting
custom alerts 26
predefined alerts 26
RSA SecurID
Token codes
for security services 202
providing one 202
transferring tokens 202
RTT
minimum system requirements 185
setting an override phone number 188
using cellular technology to maintain network
connectivity 185
viewing the Forced Call log 188
RTT-IP
benefits of 191
described 190
disabling 195
editing the settings for your account 57
enabling
for a specific device 192
for all devices in your account 192
minimum system requirements 190
overview 190
Ping Period
definition 191
ingedit for
a single device 194
all devices in your account 193
requesting a full agent call 193
viewing status for a device 191
viewing status of all devices 194
running a report 78

S

saving
report filters 184
your reports and filter criteria 183
SCCM Repair
feature overview 141
History tab for a device 85
reports for
SCCM Status History Report 146
SCCM Status Report 142
troubleshooting failed repairs 151
turning on feature
at the account level 65
at the device level 89
from the SCCM Status Report 145
viewing repair result details 148
SCCM Status
feature overview 141
History tab for a device 85
reports for
SCCM Status History Report 146
SCCM Status Report 142
troubleshooting failed repairs 151
turning on feature
at the account level 64
at the device level 88
from the SCCM Status Report 145
viewing devices with the feature turned on 66
viewing test result details 148
SCCM Status Reports 140
scheduled
Device Freeze, requesting for future
date 236
searching for
custom alerts 24
predefined alerts 24
security actions
alerts for 22
Security Audit Logs Report 181
Security Administration Authorization Agree-
ment, described 198
Security Administrators
authorization agreement 266
data and device security administration,
described 197
disabling authorization for 199
enabling authorization again 199
managing the Investigation Report Contact
List 300
providing an RSA SecurID Token code 202
requesting a security authorization code sent
by e-mail 203
user role, described 12
Security Audit Logs Report 181
security authentication methods
described 201
disabling the security administrator author-
ization 199
requesting an e-mailed security authorization
code 203
RSA SecurID tokens 201
security authorization code
described 202
requesting one using e-mail 203
security checks for geofences 265
security checks for security operations 197
Security Posture Report 151
Security Power Users
authorization agreement 266
data and device security administration,
described 197
providing an RSA SecurID Token code 202
requesting a security authorization code sent
by e-mail 203
user role, described 13
SEDs, finding those capable of full-disk encryp-
tion 132
Self Healing Call predefined alert 19
server recovery token
generating one to unlock a locked Intel AT
device 207
using to unlock a locked Intel AT device 208
Service Guarantee license
described 57
editing the assignment manually for a
group of devices 58
single device 58
payout eligibility 57
setting
override phone number 188
settings
for your account
turn it off 63
turning
data collection for devices with Absolute
Secure Drive
off 55
on 55
encryption data collection for devices with Full-Disk Encryption

off 55
on 55

SIEM Connector
downloading 71
sending alerts using 16
Signing Officer user role 13
smart phones, viewing their details 106
Software by Device Report 112
Software Configuration Change Report 111
Software License Compliance Overview Report 114
Software on Banned List predefined alert 19
software policy
adding
applications to the Banned Items list 52
Required Items list 52
copying 53
creating 51
deleting 54
described 50
editing 53
exporting to an Excel spreadsheet 54
removing a device group 53
viewing 50
a software policy 53
device groups without a software policy 51
Software Policy Non-Compliance Report 117
Software Policy page, opening it 50
states for Device Freeze requests 255
statuses defined for Investigation Reports 291
stolen devices
cloning an Investigation Report for multiple devices 299
requesting a
Data Delete operation 211
Device Freeze 236
File List 279
File Retrieval 273
submitting an Investigation Report 293
Suspected alert state 15
suspending
alert scanning 26
alerts 26
an end user message 36
suspicious activity on devices, described 15
Suspicious Devices Report 129
system requirements
minimum required for
Data Delete 209
Device Freeze 234
End User Messaging 29
File List 278
File Retrieval 272
RTT 185
RTT-IP 190

T
tables, viewing details about mobile devices 106
tracking
Device Freeze request status 251
File List status 280
transferring RSA SecurID tokens 202
triggered alert events
managing them 27
viewing them 27
triggered alerts, downloading them 29
triggering an alert 15
troubleshooting Intel AT error codes 207
turning
automatic assignment of available Service Guarantee Licenses for your account
off 55
data collection for Absolute Secure Drive
off 55
on 55
encryption data collection for Full-Disk Encryption products
off 55
on 55
Event Calling for your account
off 63
on 61
turning on
full-disk encryption data collection in
Classic Account Settings 133
Encryption Status Report 133
types of user events 180
typographical representations for conventions used in this guide 14

U
unacknowledged end user message 37
Unauthorized Software Report 124
unfreezing
a frozen device using an unfreeze passcode 260
a single device on an Agent call 258
multiple devices on an Agent call 259
the device before requesting a Data Delete on the same device 210
unfreezing a Device Freeze request
getting an unfreeze passcode 259
unlocking locked Intel AT devices using a server recovery token 208
upgrading the agent 68
URL end user messages
activating them 36
creating 32
deleting them 39
described 29
editing 35
previewing them 33
suspending them 36
viewing a list of them 30
user-defined alerts, described 15
User-entered Data Report 174
User Audit Report 179
User Event Report 180
user events, types 180
User Guide, overview of what’s included 13
user roles
   Administrators 12
   Guest Users 13
   Power Users 13
   Security Administrators 12
   Security Power Users 13
   Signing Officers 13
Username Changed predefined alert 19
using
   choose feature 79
Data Delete; Data Delete
described 209
Device Freeze 234
e-mailed authorization codes to authorize
   security personnel 203
File List 278
geofence technology 266
Remote File Retrieval 272
RSA SecurID Token codes to authorize a
   security service 202
RTT 185
RTT-IP feature 190
this guide 13

V
viewing
   acknowledged end user message 37
alerts
   custom 24
   predefined 24
all device groups 41
call history for a device 88
changes to a device’s full-disk encryption
   status 139
complete overview for specific devices that
   have the Agent 94
detailed caller ID information 157
detailed information about Device Freeze
   requests 255
details about mobile devices, including smart
   phones and tablets 106
details for
   a device with a mobile broadband
   adapter 187
   a specific device 81
Device Drift History Report 157
Device Freeze request 254
Device Freeze request status 254
device groups without a software policy 51
devices
   in a device group 49
   entire row in a report record 80
   existing Investigation Reports 291
   Forced Call log 188
   Forced Call request status 189
   Investigation Report history 293
list of
   detected applications on a managed
   device 109
   end user messages 30
   existing geofences 269
   mobile broadband adapters installed and
   operational on managed
   devices 105
   software policies 50
list of managed devices that have Event
   Calling turned on 63
list of managed devices with SCCM Status
   reporting turned on 66
log file for
   a single device 232
   mobile devices 233
   multiple devices 232
Mobile Broadband Adapter Details page 187
Prepaid Service Guarantee balance 294
Report History table for Investigation
   Reports 293
Reports page 78
software policy 53
specific device group 42
total, used, and available disk space for each
   device 101
triggered alert events 27
unacknowledged end user messages 37
viewing call history for a device 88

W
Warranty Ending predefined alert 19
Wi-Fi positioning
   limitations 164
Windows devices, forcing a reboot after Device
   Freeze completes 238
WMI, reporting hard disk serial numbers based
   on Microsoft or vendor’s information 94