Dell Laptop Tracking and Recovery Service

User Quick Guide
# Table of Contents

Theft Reporting ....................................................................................................................................................... 3  
Make a New Theft Report ....................................................................................................................................... 4  
  Provide Theft Report Details – Section 1. Specify the Computer................................................................. 5  
  Provide Theft Report Details – Section 2. Loss Information ........................................................................... 6  
  Provide Theft Report Details – Section 3. Police Report information........................................................... 7  
  Provide Theft Report Details – Section 4. Your contact details. ................................................................. 8  
  Confirm / Submit Report.................................................................................................................................. 9  
Data Delete ............................................................................................................................................................ 11  
  Create Data Delete Policy ................................................................................................................................ 12  
  Disable Pre-Authorization ............................................................................................................................. 14  
  Request Data Delete ................................................................................................................................... 15
Theft Reporting

This is the home page presented upon login to Customer Center. Click either of the areas indicated to enter the Theft Reporting module.

- **Home**
- **Reports**
  View the activity of your Computrace-equipped assets, as well as hardware and software inventory details.
- **Administration**
  Change your password, alter Customer Center settings, and work with Computrace licenses.
- **Theft Reporting**
  Report a lost or stolen computer to our recovery team, and view the status of existing theft reports.
- **Data Delete**
  Remove data from a lost computer.
  Note that a pre-authorization form is required prior to using Data Delete. Click here to download.
- **Documentation**
  View the User’s Guide and other available documentation.

Click here to view, modify, activate or suspend default or custom alerts.

- **Latest PC Agent Version** is 867.
- **Latest Mac OSX Agent Version** is 070.

To download the latest agent for installation or evaluation, click on the “Download Agent” link below and then click on either PC or Mac. If you wish to do a server side upgrade to the latest agent version, please contact us.

Download Agent
### Make a New Theft Report

Click the area indicated to begin a new Theft Report.

#### Theft Report Summary

Report a lost or stolen computer to our recovery team, and view the status of existing theft reports.

<table>
<thead>
<tr>
<th>The group is:</th>
<th>All Computers (0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>and the Report contains keyword</td>
<td></td>
</tr>
<tr>
<td>and the Computer Status is</td>
<td></td>
</tr>
<tr>
<td>✓ Computer Recovered</td>
<td></td>
</tr>
<tr>
<td>✓ Police Reviewing File</td>
<td></td>
</tr>
<tr>
<td>✓ Waiting for Call</td>
<td></td>
</tr>
<tr>
<td>✓ First Call Received</td>
<td></td>
</tr>
<tr>
<td>✓ Waiting for ISP</td>
<td></td>
</tr>
<tr>
<td>✓ Police Locating Computer</td>
<td></td>
</tr>
<tr>
<td>✓ Cold (No Calls)</td>
<td></td>
</tr>
<tr>
<td>✓ Cold (Not Pursue)</td>
<td></td>
</tr>
<tr>
<td>✓ Cold (Out of Jurisdiction)</td>
<td></td>
</tr>
<tr>
<td>✓ Closed (Other than Recovered)</td>
<td></td>
</tr>
</tbody>
</table>

and the Theft Date is between

- [ ] Jan 1 2000
- [ ] Jun 13 2006

and the Guarantee Payment Status is

- [ ] Paid
- [ ] Declined
- [ ] Eligible
- [ ] N/A

OR where the Report ID is

Show Results
Provide Theft Report Details – Section 1. Specify the Computer

Which computer? Click Choose

Make a New Theft Report

Please report any loss, theft, or suspected theft of a Computrace Agent equipped computer as soon as possible. Upon receiving your report, we immediately begin the recovery procedure.

If you are having difficulty reporting your theft, please contact us at 1-800-81-THEFT during standard business hours (Pacific Time) or e-mail recovery@absolute.com

Please Choose Computer:

Please make a separate report for each computer.

Operating System:

Provide Theft Report Details – Section 1.

Select from list. A list of your computers will appear, click on the one that you wish to report.

Choose the Computer by clicking on it.

Note that you can reduce the number of results by entering some data – e.g. the serial number or user name.

Filter

Press Ctrl+F to find a record in this window.

<table>
<thead>
<tr>
<th>ESN</th>
<th>Computer Name</th>
<th>User Name</th>
<th>Assigned User Name</th>
<th>Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>XYZ</td>
<td></td>
<td></td>
<td></td>
<td>123</td>
</tr>
</tbody>
</table>
Provide Theft Report Details – Section 2. Loss Information

How was the computer lost?

- Select the Day, Month and Year that the computer was lost
- Enter the Victim’s Name
- Enter the Address of the Theft
- Enter the nearest city or town where the loss occurred
- Select the State/Province where the loss occurred
- Select the Country where the loss occurred
- Select if the Power Cord was Stolen (Yes, No, Unknown)
- In the large text box, enter details of the Theft including the last known location of the computer and how it was stolen.

2. How was the computer lost?

<table>
<thead>
<tr>
<th><em>Date:</em></th>
<th>Day</th>
<th>Month</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2008</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><em>Victim’s Name:</em></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><em>Address of Theft:</em></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><em>City of Theft:</em></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><em>State/Province of Theft:</em></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><em>Country of Theft:</em></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><em>Was Power Cord Stolen?</em></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Unknown</th>
</tr>
</thead>
</table>

*Details of Theft:
Include the last known location of the computer and how it was stolen.
Provide Theft Report Details – Section 3. Police Report information

Left column
- Select whether you have reported this to the police (Yes, No)
- Enter the name of the police agency to which the loss was reported
- Enter the main phone number for the police agency

Right column
- Enter the District/Division/Precinct Number (if available)
- Enter the Police File Number
- Enter the name and/or badge number of the Investigating Officer (if available)

Note: A police report must be filed. At a minimum, the Agency, Agency Phone Number and Police File Number provided before we can elicit police assistance in the recovery process.

### 3. Have you filed a police theft report?
A police report must be filed before we can elicit police assistance in the recovery process.

<table>
<thead>
<tr>
<th>Reported?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

**Agency**

The name of the police agency to which the loss was reported.

**Agency Phone Number**

The main phone number for the police agency.

**District/Division/Precinct Number**

**Police File Number**

**Investigating Officer**

If possible, please provide a name and/or badge #.
Provide Theft Report Details – Section 4. Your contact details
• Enter your First Name and Your Last Name
• Enter your Job Title
• Enter the name of your Company
• Enter your Phone Number
• Enter your Email address

Note: We can only accept a report from an authorized contact person in your organization.

Select the first push button at the bottom to Send This Report

4. Who are you?
We can only accept a report from an authorized contact person in your organization.

*First Name: __________________________  *Last Name: __________________________
*Job Title: __________________________
Company: __________________________

*Phone Number
(________) ________

Email: __________________________

• Mandatory information is designated by an asterisk (*).
• While not all information is mandatory, some is critical to the success of the recovery procedure, such as a police file number, the date of the loss, and the ESN of the computer.
• Should you have anything further to report after making this report, please see Theft Report Summary.
• A Theft Recovery Officer may contact you to request further information.
• For your records, you will receive a copy of the information you have submitted in this report by email.
• You will receive updates as the recovery proceeds.

Send This Report  Cancel
Confirm / Submit Report
- Verify all sections of the Report.
- Select the first push button at the bottom of the page “Edit This Report” to make changes.
- Select the first push button at the bottom of the page “This Report is Correct” to submit the report.

Confirm This Report
Please check to make sure this information is correct.

1. Which computer?

<table>
<thead>
<tr>
<th>ESN:</th>
<th>4Q285K05CA</th>
<th>Make:</th>
<th>Dell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model:</td>
<td>Latitude</td>
<td>Serial Number:</td>
<td>PARENT ESN</td>
</tr>
<tr>
<td>Asset Number:</td>
<td></td>
<td>Operating System:</td>
<td>unknown</td>
</tr>
</tbody>
</table>

2. How was the computer lost?

<table>
<thead>
<tr>
<th>Date:</th>
<th>June 10, 2008</th>
<th>Details of Theft:</th>
<th>Theft report 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victim’s Name:</td>
<td>Tony Cameron</td>
<td>City of Theft:</td>
<td>Vancouver</td>
</tr>
<tr>
<td>Address of Theft:</td>
<td>1234 Main Street</td>
<td>State Province of Theft:</td>
<td>British Columbia</td>
</tr>
<tr>
<td>Country of Theft:</td>
<td>Canada</td>
<td>Was Power Cord Stolen?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

3. Have you filed a police theft report?

<table>
<thead>
<tr>
<th>Reported?</th>
<th>No</th>
<th>District/Division/Precinct Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency:</td>
<td>Vancouver Police Department</td>
<td>Police File Number:</td>
</tr>
<tr>
<td>Agency Phone Number:</td>
<td>(804) 355-1212</td>
<td>Investigating Officer:</td>
</tr>
</tbody>
</table>

4. Who are you?

<table>
<thead>
<tr>
<th>First Name:</th>
<th>Artes</th>
<th>Company:</th>
<th>Dell Pro Support Test Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name:</td>
<td>Manlig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job Title:</td>
<td>Manager, IT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Upon making this report, you will receive a copy of the report by e-mail.
The e-mail message also contains additional information regarding recovery process.
Theft Report Confirmation

Your Theft Report has been sent to the Recovery Team. You will receive a copy of the report by e-mail. The e-mail message also contains additional information regarding the recovery process.

Thank you.

This report's file number is: 24406. Please use this number to track the progress of the recovery.

- A Theft Recovery Officer may be in contact with you regarding this file.
- You will receive updates as the recovery proceeds.
- Should you have anything further to report on this file, you can update it at Theft Report Summary.
Data Delete

This is the home page presented upon login to Customer Center. Click the area indicated to enter the Data Delete module.

- **Reports**
  View the activity of your Computrace-equipped assets, as well as hardware and software inventory details.

- **Administration**
  Change your password, alter Customer Center settings, and work with Computrace licenses.

- **Theft Reporting**
  Report a lost or stolen computer to our recovery team, and view the status of existing theft reports.

- **Data Delete**
  Remove data from a lost computer.
  Note that a pre-authorization form is required prior to using Data Delete. Click [here](#) to download.

- **Documentation**
  View the User's Guide and other available documentation.

**Click Here** to view, modify, activate or suspend default or custom alerts.

Latest PC Agent Version is 857.
Latest Mac OSX Agent Version is 870.

To download the latest agent for installation or evaluation, click on the "Download Agent" link below and then click on either PC or Mac. If you wish to do a server side upgrade to the latest agent version, please [contact us](#).

[Download Agent](#)
Create Data Delete Policy

Select the highlighted area to create a Data Delete Policy.

1. Enter a **Policy Name** and **Description** for the policy in the appropriate text boxes.

2. Define all files and directories to be deleted. Customer Center includes a number of predefined file and directory entries. Additionally, Data Delete administrators can define their own unique file and folder entries. A single Deletion Policy may include any combination of predefined and user-defined entries. Follow the instructions below to add either type of entry to the policy.

   a. To add predefined entries — Highlight the desired selection in the **Add Common Files/Directories** list and click the **Add >>** button to move your selection into the **Chosen Files/Directories** table on the right side of the page. Repeat this process to add additional predefined entries to the policy.

   b. To define and add unique entries — Enter an entry for each file or folder to be deleted into the text box provided, following the standard Windows file path convention. The * wildcard is supported. Click the **Add >>** button to move each entry into the **Chosen Files/Directories** table on the right side of the page. Repeat this process to define all desired entries. To remove any entries from the **Chosen Files/Directories** table click the **<< Remove** button in the middle of the page.

   When specifying a folder, be sure to include the trailing backslash after the folder name (e.g. c:\temp\). All files in the main folder and all files and subfolders are deleted. The root directory is retained, empty.

3. Once you have defined all desired descriptions, click the appropriate button at the bottom of the page:

   - To save the policy — click the **Save** button.
- To delete the policy — click the **Delete** button.

- To copy the policy — click the **Copy** button. The **View Data Delete Policies** page will open with the new copy of the policy named **Copy of %original policy name%**. This feature is useful if you wish to create a Deletion Policy which is similar to the currently displayed one. First copy the original and then click the appropriate View link and make any desired changes.

---

**Create / Edit Data Delete Policy**

To utilize the Data Delete service, you must fill out and sign a Data Delete pre-authorization agreement and send to Absolute. Click **Here** to download the agreement.

**Policy Name:**

**Description:**

---

**Add Common Deletion Functions**

Directory deletes will delete all files and sub-folders for all Computer users (when applicable).

```
Add "My Documents Directory"
Add "Desktop"
Add "Application Data Directory"
Add "Internet Explorer Cookies Directory"
Add "Internet Explorer Favorites Directory"
Add "Internet Explorer History Directory"
Add "Internet Explorer Temporary Files Directory"
Add "Windows Temporary Files Directory"
Add "All MSWord documents (*.doc)"
Add "All Adobe Acrobat documents (*.pdf)"
Add "All MS Excel documents (*.xls)"
Add "All MS Powerpoint documents (*.ppt)"
Add "All MS Visio documents (*.vdx)"
Add "All MS Access documents (*.mdb)"
Add "All MS Project documents (*.mpp)"
```

**Selected Common Deletion Functions**

Files/Directories will usually be deleted in the specified order. However, explicit items will be deleted before wildcards for efficiency purposes.

---

**Add Custom**

Create custom data deletes. Wildcards (*) are allowed. Note that file deletions are applied recursively.

Examples:

- `c:\folder`  
- `c:\folder\abc`  
- `c:\folder\file.abc`  
- `file.abc`

To delete a folder, ensure the path contains a trailing backslash - i.e. `c:\folder\`

To delete a file, ensure the path does not have a trailing backslash - i.e. `c:\file.abc`
Disable Pre-Authorization

Select the highlighted area to disable Data Delete Pre-Authorization.

Data Delete

Select the first button to Disable Data Delete Authorization.

Disabling the Pre-Authorization Agreement will make it impossible for any new Requests to be created, as well all existing active Requests will be Cancelled. The Agreement may only be re-enabled by calling the Recovery department during business hours (see the Contact Us menu item).
Request Data Delete
Select the highlighted area to Request a Data Delete transaction.

Data Delete

A. Specify the Reason — Select the reason for the Data Delete request from the Reason drop-down list. Possible values are Stolen/Lost, End of Lease, Retiring and Other.

B. Choose Computer — This section identifies the computer that will be the target of the Data Delete operation.
   - Click the Choose button to display a list of all computers in your account.
   - Click the ESN of the desired computer. The Choose window will close and the Request Data Delete page will update, listing details of the selected computer.

C. Select Data Delete Options — This section specifies which Data Delete options to run on the targeted computer.

D. Perpetual Deletion — Perpetual Deletion allows Data Delete to re-initialize on the targeted computer should it make a call to the Monitoring Center after the deletion cycle has completed. To use this feature, check the Perpetual Deletion check-box. On Windows Mobile devices, Perpetual Deletion is not dependent on a call to the Monitoring Center. Once Perpetual Deletion has been initialized on a Windows Mobile device, it will restart automatically every twelve (12) hours.

Perpetual Deletion is not recommended in the case of a stolen computer as repeated Data Delete cycles will likely delete the thief’s data and/or make the thief aware of remote activity on the computer, which may reduce the chances of recovery.
E. **Select Data Delete Type** — select one of the three options below:

- **All Files Except O/S** — Select this option to delete all files on the computer with the exception of the operating system. Once the delete operation is completed, a results log is sent to the Monitoring Center.
- **All Files Including O/S** — Select this option to delete all files on the target computer, including its operating system. This Data Delete operation is executed in two phases; in phase one all user files are deleted and a results log is sent to the Monitoring Center; in phase two the operating system files are deleted. No results log is created during phase two as the operating system has been destroyed, and it is not possible to upload the log file.
- **Specific Files/Directories** — Select this option to delete specific files, file types and directories. This option is only available for PCs and Windows Mobile devices. To use this feature, you must select a Deletion Policy from the drop-down list. Once the delete operation is completed, a results log is sent to the Monitoring Center.

F. **File Date Attributes** — this section is used to specify whether to include the Created, Modified and Accessed dates in the Data Delete log file.

- Click the **Include File Date Attributes in the Data Delete Log** check box. By default, the **Created** and **Modified** dates will appear in the log file for Windows Vista computers, and the **Created**, **Modified** and **Accessed** dates will appear for Windows XP computers.

G. **Data Delete Authorization** — This section is used to authenticate the individual requesting the Data Delete operation.

- Read the Data Delete Authorization Agreement carefully.
- Check the **I Accept the agreement** check box to indicate you have read the agreement and accept the terms.
- Check the **I Confirm the Computer Selected** check box to indicate you have verified the ESN listed in the Choose Computer section is the ESN assigned to the intended target computer.
- Enter your name, telephone number and e-mail address in the spaces provided. These values should match those on the Pre-Authorization Form.

H. Click the appropriate button at the bottom of the page:

- To save your draft and initiate the Data Delete operation as specified:
  - Click the **Set Data Delete** button. The Confirm Data Delete Request page opens.
  - Review the information, and then click the **Submit** button. The Request Authentication screen will open.
  - Enter your Customer Center password and the Data Delete Authorization Code.
  - Click the **OK** button.
- To save your draft, without launching the delete operation:
  - Click the **Save Draft** button. The Request Authentication screen will open.
  - Enter your Customer Center password and your Data Delete Authorization Code.
  - Click the **OK** button.
- To cancel the delete request, click the **Delete** button.
- To close the Request Data Delete page without saving or submitting the request, click the **Close** button. You will be returned to the Data Delete Summary page.
Request Data Delete

Warning - In a theft scenario, Data Delete reduces the chance of computer recovery as it may alert the thief and cause them to dispose of the computer. Choosing the “Specific Files/Directories” data delete type may reduce the chance of alerting the thief due to the selective nature of the deletion.

Note also that Data Delete, if launched post-theft, also invalidates the recovery guarantee (if applicable).

To utilize the Data Delete service, you must fill out and sign a Data Delete pre-authorization agreement and send to Absolute. Click Here to download the agreement.

Reason: 

Choose Computer

ESN:
Make:
Model:
Serial No:
Asset No:

Last Call:

Select Data Delete Options

Perpetual Deletion: ☐

Data Delete Types

☐ All Files Except O/S
☐ All Files Including O/S (PC and Mac Only)
☐ Specific Files/Directories (PC and Windows Mobile Only)
File Data Attributes

- Include File Data Attributes in the Data Delete Log

Warning: Selecting this option will result in the inclusion of the Created, Modified and Last-Accessed date in the log file. Including this data may conceivably double the size of the data delete log file, if the log is large and the target machine has a low-bandwidth internet connection, data delete completion may be delayed while the client repeatedly attempts to upload this file. If speed of Data Delete completion is important, this option should be skipped.

Data Delete Authorization

THE BELOW IS SUBJECT TO THE TERMS AND CONDITIONS OF THE ABSOLUTE SOFTWARE SERVICE AGREEMENT

The "Data Delete Operation" means an operation authorized by the Corporation to have Absolute Software perform a Data Delete Operation on your behalf. Absolute Software will only allow the setup a Data Delete operation if:

a) A Data Delete Pre-Authorization form has previously been completed in full, sent to Absolute Software and acknowledged.

b) The RSA Security token entered after you save this request matches that on Absolute Software’s records.

c) The password entered after you save this request matches the password for the user currently logged in.

d) The user currently logged into Absolute Software’s Customer Center is an authorized Data Delete administrator.

e) The user currently logged into Absolute Software’s Customer Center has administrator level access.

By proceeding, on behalf of the Corporation, you hereby provide permission for Absolute Software to perform a Data Delete Operation on your behalf.

Accept the agreement: [ ] I Accept the agreement

Confirm the Computer Selected: [ ] I Confirm the Computer Selected

Your Name: [ ]

Your Phone No: [ ]

Your Email: [ ]