
Dell System Track User Guide



February 24, 2011

Dell System Track User Guide - Customer Center v 5.2

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

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

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

Table of Contents

Customer Center Overview	4
Customer Center Highlights.....	4
Reports - Know where it is, who's using it, and what's on it.....	4
Administration - Take Action	4
Data and Device Security - Respond to Suspicious Behavior.....	4
Theft Report - Investigate theft and recover stolen device	5
Getting Started: Five Quick Steps	5
Viewing the Customer Center Home Page	7
Reporting a Theft	7
Using Data Delete	11
Creating a Data Delete Policy.....	11
Requesting Data Delete	13
Disabling Security Administrator Authorization	18
Using Device Freeze	19
Requesting an Authorization Code.....	19
Creating a Custom Device Freeze Message	20
Freezing Devices	21
Unfreezing Devices	22
Managing Device Freeze Messages	24
Tracking Device Freeze Summary Status.....	25

Customer Center Overview

In Customer Center, you can:

- Easily identify devices that have gone missing, regardless of whether they are on or off your network
- Access current asset information for each device in your deployment
- Identify potentially suspicious activities and receive alerts if suspicious activities occur
- Take appropriate security measures for devices that may be at risk
- Report a stolen device and interact with the Theft Recovery team

Customer Center Highlights

Reports - Know where it is, who's using it, and what's on it

- Improve lifecycle management
- Perform accurate audits quickly
- Track expensive hardware like Mobile Broadband Adapters
- Determine location and return dates of leased devices
- Find and return devices that have drifted
- Manage details like call history, device location, unauthorized software, etc.
- Monitor suspect behavior with the Suspicious Devices report. Create conditions and receive an alert if the condition occurs

Administration - Take Action

- Design geofences and manage devices based on their physical location
- Send and receive communication with end users
- Define groups to manage users efficiently
- Build software policies
- Manage your Customer Center account and users

Data and Device Security - Respond to Suspicious Behavior

- Remotely data delete from a device
- Obtain an audit log of the deleted data to prove compliance
- Freeze a device and communicate with the end user to validate status
- Lock a device and post a message to the user with Intel AT technology (if supported on your hardware)
- Set a timer to lock a device with Intel AT if it does not call in

Theft Report - Investigate theft and recover stolen device

- Report a stolen device
- Analyze event details and improve security to avoid future theft

Getting Started: Five Quick Steps

1. Log in

If you bought SystemTrack with the agent pre-installed at the Dell factory (Customer Factory Install, otherwise known as CFI), and need to retrieve your Customer Center username and password, follow these steps.

- Go to <http://content.dell.com/in/en/business/d/services/Dell-SystemTrack-Customer-Center-Portal.aspx> and click "[Customer Center Portal](#)". Then click the link "Activate New Account"
- Enter the **Order Number**, and either a **Phone Number** or **Postal/Zip Code**. If you are not sure of these details, check to see if you received an email containing this information.
- Click the **Submit** button. A prompt to enter your e-mail address will appear.
- Enter your e-mail address. You will receive an e-mail with the login and password.
- Once you have received the e-mail, go to <http://content.dell.com/in/en/business/d/services/Dell-SystemTrack-Customer-Center-Portal.aspx> and click "[Customer Center Portal](#)". Log in using the login and password. You will be prompted to change your password on the first login.
- Change your password

If you bought System Track *without* the agent installed, you should have already received two fulfillment e-mails. One e-mail contains your Customer Center login username and a separate e-mail contains your password. If you did not receive these e-mails, follow these steps.

- Go to <http://content.dell.com/in/en/business/d/services/Dell-SystemTrack-Customer-Center-Portal.aspx> and click "[Customer Center Portal](#)". Then click the "Forgot Password" link. You will receive an e-mail shortly.
- Enter the username and the e-mail address specified for the order. (The username is oftentimes the same as the specified e-mail address).
- Click the **Submit** button. You will receive an e-mail with a login and password.
- Go to <http://content.dell.com/in/en/business/d/services/Dell-SystemTrack-Customer-Center-Portal.aspx> and click "[Customer](#)

[Center Portal](#)". Use the login and password listed on the e-mail. You will be prompted to change your password.

e) Change your password.

2. Download Agent

NOTE Customers who purchased the factory pre-installed product can skip this step.

- a) On the right-hand side of the home page, click the **Download Packages** link. The Download Packages page opens.
- b) Click the **Windows** link. A File Download dialog opens.
- c) Follow the on-screen instructions to save the ZIP file to your local device.
- d) Double-click the ZIP file containing the Agent installation package, and then extract the contents to a separate folder.
- e) In the folder containing the installation package you extracted, double-click the file **Computrace.exe**.
- f) When prompted, select the desired installation language. The Agent installer displays in the selected language.
- g) On the **Confirm Installation** dialog, click **Next**.

OR

To cancel the installation, click **Cancel**.

3. Verify devices

Go to **Reports > Call History and Loss Control > Activation Reports**. Run the Activation report to verify all activated devices. (You may need to wait approximately 15 minutes after downloading the Agent for the devices to appear. Contact Support at <http://content.dell.com/in/en/business/d/services/Dell-SystemTrack-Customer-Center-Portal.aspx> if devices are missing.)

4. Set up accounts and authorization

Go to **Administration > Users > Create and Edit User**. Determine the users who are authorized to access your Customer Center account. Then go to **Documentation > Service Request Forms > Security Administrators and Geolocation Authorization Form**. Sign the pre-authorization to enable high security functionality such as data delete, device freeze, Intel Anti-Theft, and geotechnology capabilities.

5. Configure your account

Go to **Reports > Hardware Assets > Asset Report**. to view a complete inventory of the devices calling into your Customer Center account. Go to **Administration > Alerts > Create and Edit Alerts** to define conditions and set alerts, so that you will be notified if the condition occurs.

Viewing the Customer Center Home Page

For all Dell System Tracking and Recovery (STR) Enterprise Protection and Dell STR Enterprise Protection and Recovery accounts, the Customer Center Home page displays upon successful log in.

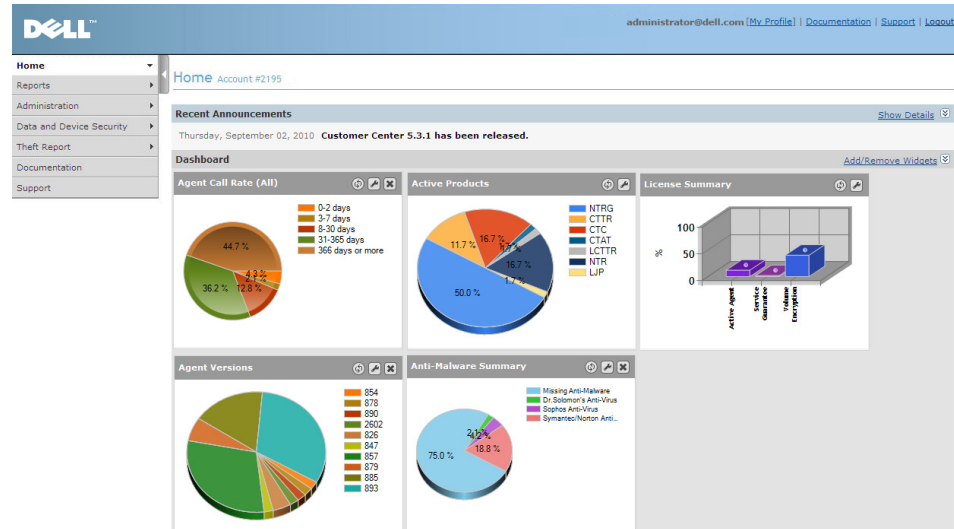


FIGURE 1. Customer Center Home Page

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

- **Recent Announcements** lists any important messages from Global Support that apply to your account or user profile.
- **Account Summary** displays the products you have purchased and the number of licenses you have installed on your devices.

To return to the Home Page from any page in Customer Center:

- On the global navigation bar, click the **Home** link. The Customer Center Home Page opens.

Reporting a Theft

File a theft report to designate a device as stolen.

To file a theft report:

IMPORTANT Required fields are indicated with an asterisk (*).

1. Click the **Theft Report** link on the global navigation bar. The Theft Report page opens.

2. Click the **Create and Edit Theft Report** link on the global navigation bar. The Create and Edit Theft Report page opens.
3. In the **Which Device** section, click the **Choose** button to open the Choose page and select the identifier for the lost or stolen device. If you know the identifier for the stolen device, enter the value in the **Choose Device** text box and enter all other available details in the Make, Model, Serial Number, Asset Number, and Operating System text boxes.

The Create and Edit Theft Report page refreshes to display the selected identifier in the **Choose Device** text box. Depending upon the device selected, some of the information is pre-populated in the theft report.

The screenshot shows the '1. Which device?' section of a web form. At the top are two buttons: 'Send this Report' and 'Cancel'. Below them is a note: '* Indicates required fields'. The section title is '1. Which device?'. A instruction reads: 'Click "Choose" to select the device that has been stolen or enter the device details in the fields provided.' There is a 'Choose Device:' label followed by a text input field and a 'Choose' button. Below this is a link: 'If you cannot find the stolen Device's Identifier in the "Choose" list, please contact [Support](#)'. A section titled 'Or enter device details manually:' contains several fields: 'Make:', 'Model:', 'Serial Number:', 'Asset Number:', and 'Operating System:'. Each has a corresponding text input field. A note below the 'Serial Number' field says: 'Please confirm the serial number is correct and that Agent was installed on the laptop.' Another note below the 'Asset Number' field says: 'The asset number may or may not be assigned by your organization.' At the bottom, a disclaimer states: 'Theft reporting and recovery services are only available with certain products, to see which products are eligible for these services refer to your [Service Agreement](#).'

FIGURE 2. Create Theft Report — Which device section

4. In the **How was the device lost** section, enter the following information about the theft:
 - o Date of theft
 - o Name of the victim or the user who had possession of the device prior to loss
 - o Location where the theft or loss occurred
 - o Power cord status, whether the cord was stolen with the device

NOTE The greater the accuracy and detail of the information you provide, the greater the likelihood that the police are able to help facilitate a recovery.

2. How was the device lost?

Date and Time of Theft: *

Timezone: *
 (GMT-12:00) International Date Line West

Address of Theft: *

Victim's Name: *

City of Theft: *

Nearest city or town to where the loss occurred.

Country of Theft: *

Was Power Cord Stolen? *
☐ Yes
☐ No
☒ Unknown

State/Province of Theft: *

Details of Theft: *
 Include the last known location of the device and how it was stolen.

FIGURE 3. Create Theft Report — How was the device lost section

5. In the **Have you filed a report with the police** section, enter the following information about the police or law enforcement agency where a report was filed:
 - o Agency name
 - o Location and contact details
 - o Police file number
 - o Name of the investigating officer

3. Have you filed a report with the police?

A police report must be filed before we can elicit police assistance in the recovery process.

Reported?:
☐ Yes
☒ No

Agency:

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

District/Division/Precinct Number:

E.g. Southwest Division or 122nd Precinct

Investigating Officer:

If possible, please provide a name and/or badge #.

Country Code: **Agency Phone:** **Ext:**

The main phone number for the police agency.

Police File Number:

FIGURE 4. Create Theft Report — Have you filed a report with the police section

6. In the **Who are you** section, enter the following information about you (or the person filing the theft report):
 - o Name
 - o Designation and organization
 - o Contact details including e-mail address and phone number

The screenshot shows a web form titled "4. Who are you?". Below the title is a note: "We can only accept a report from an authorized contact person in your organization." The form contains several input fields: "First Name: *" with the value "Administrator", "Last Name: *" with the value "Dell", "Company:" with the value "Test Account EVAL20090906", "Job Title: *" (empty), "E-mail:" with the value "administrator@dell.com", "Country Code: *" with the value "1", "Phone Number: *" (empty), and "Ext:" (empty). Below these fields is a paragraph of text: "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 e-mail. You will receive updates as the recovery proceeds." At the bottom of the form are two buttons: "Send this Report" and "Cancel".

FIGURE 5. Create Theft Report — Who are you section

7. Click the **Send this Report** button. The Report Validation page opens.
8. Review your information to make sure that the report is correct, and then click the **This report is correct** button.

NOTE If you need to make further changes, click the **Edit this report** button. The Create and Edit Theft Report page opens. Make the necessary changes and click the **Send this Report** button.

The confirmation page opens, listing the file number of the theft report. From the confirmation page, you can:

- o Click the **File number** link to open the report you have just completed.
- o Click the **Reports Made** link to go to the list of theft reports for your organization.
- o Click the **Make another report** button to create a new report.

Using Data Delete

Data Delete allows pre-authorized Customer Center users to delete some or all of the hard drive data on a remote device. The proper workflow to use Data Delete effectively is as follows:

1. [Creating a Data Delete Policy](#)
2. [Requesting Data Delete](#)

NOTE Prior to using Data Delete features, you need to download, complete, and return the Security Administrator and Geolocation Authorization Form. The form is available in SystemTrack Customer Center, on the Documentation page. Once your pre-authorization agreement has been processed, you will be granted access to the advanced data protection features on SystemTrack's Customer Center Web site ("Customer Center"), and receive notification by e-mail.

Creating a Data Delete Policy

To create a Data Delete Policy:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.

NOTE If you are not logged in as a Security Administrator, Customer Center displays an error when you open any Data and Device Security page.

3. Click the **Data Delete** link. The Data Delete home page opens.
4. Click the **Create and Edit Data Delete Policies** link. The Create and Edit Data Delete Policies page opens.
5. Enter a name for your Data Delete policy in the **Policy Name** text box.

NOTE Data Delete policies must have unique names.

6. Enter a brief description for your policy in the **Description** text box.
7. Define all files and directories to be deleted. Use either the predefined file and directory entries or define your own unique file and folder entries. A single policy may include any combination of predefined and user-defined entries.
8. To add predefined entries:
 - a) Click the **predefined Data Deletes** tab.
 - b) Select the desired files and directories in the **Available Data Delete Functions** list, and then click the **Add** button. The

selected items move to the **Selected Data Deletes** list on the right.

- c) Repeat this process to add additional predefined entries to the policy.
 - d) To remove any entries from the **Selected Data Deletes** table, click the desired entry in the Selected Data Deletes table, and then click the **Remove** button.
9. To define and add unique entries:
- a) Click the **Custom Data Deletes** tab.
 - b) Create an entry for each file or folder to be deleted into the text box provided, following the standard Windows file path convention. When specifying a folder, 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.
- NOTE** The * wildcard is supported. When specifying a folder, be sure to include the trailing backslash after the folder name (e.g.— c:\temp\). All files in the main folder and all files and subfolders are deleted. The root directory is retained, empty.
- c) Click the **Add** button to move each entry into the **Selected Data Deletes** list on the right.
 - d) Repeat this process to define all desired entries.
 - e) To remove any entries from the Selected Data Deletes table click the **Remove** button.
10. Once you have defined all desired descriptions, click the appropriate button at the bottom of the page:
- o **To save the policy** — click the **Save** button.
 - o **To delete the policy** — click the **Delete** button.
 - o **To copy the policy** — click the **Copy** button. Copy the original and then click the appropriate View link to make any desired changes. The **View Data Delete Policies** page opens with the new copy of the policy named **Copy of %original policy name%**. This feature is useful if you 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.

Requesting Data Delete

NOTE The following instructions assume you have already signed and delivered the Security Administrator Pre-Authorization form and selected your Authorization Method.

To initiate data delete:

1. Log in to Customer Center as a Security Administrator.

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

2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Data Delete** link. The Data Delete page opens.
4. Click the **Request Data Delete** link. The Request Data Delete page opens. All fields except the Identifier field and Choose button are greyed out.
5. Use the **Choose** feature to specify the target device for the Data Delete operation. To select a device using the Choose feature:
 - Click the **Choose** button. The Choose dialog opens to display a list of all devices in your account.
 - Click the **Identifier** of the desired device. The Choose dialog closes and the Request Data Delete page refreshes listing details of the selected device.

IMPORTANT If you initiate Data Delete on a machine with a Device Freeze request in the **Freeze Requested** state, the Data Delete request implements before the Device Freeze request. The Device Freeze request status changes to **Pending** until the Data Delete Request is complete. However, you cannot request Data Delete on a device that is already frozen. You must unfreeze the device before requesting Data Delete.

6. In the **Reason for Data Delete Request** list, select one of the following values and then continue to step step 7:
 - **Stolen** — for stolen devices. For stolen devices, a Theft Report is mandatory. If a Theft Report is not available for the specified device, a warning message appears prompting you to create a Theft Report before continuing. Selecting **Stolen** as the reason displays the Date of Theft as a read-only value based on information available in the Theft Report.
 - **Missing** — for devices that are lost but not stolen. Selecting **Missing** as the reason displays a field allowing you to

enter a Date of Loss for the device. Enter a Date of Loss to continue.

- **Other** — for devices that are nearing the end of their lease, retiring, or are being taken out of commission for any other reason.

Request Data Delete

Request a data delete by providing information that will help with the recovery of your device.

Warning – In a theft scenario, using Data Delete may decrease the chance of device recovery, as it may alert the thief and encourage the disposal of the device. To reduce the chance of alerting the thief, choose "Custom Policy", a Data Delete type which allows you to select specific files to delete.

Note – If Data Delete is launched on a device, the conditions of your Service Guarantee may be affected. For further details, please refer to the Service Agreement.

FIGURE 6. Request Data Delete — Device Selection and Reason for Data Delete Request

7. In the **Data Delete Policy** section, select the desired Data Delete policy that should drive the Data Delete operation and then continue to step 8. Possible values are:

- **All Files Except OS** deletes all files on the device, with the exception of the operating system. Once the delete operation is completed, a results log is sent to the Monitoring Center.

NOTE When you select the All Files Except OS option, Windows folder and the root folder (usually C:\) are not deleted. All other files and folders are deleted. In addition, Data Delete searches for and deletes any files in the Windows folder and the root with the following extensions: ".doc", ".xls", ".ppt", ".pdf", ".mdb", ".vsd", ".mpp", ".txt", ".pst", ".ost", ".msg", ".csv", ".xml", ".htm", ".html", ".gif", ".jpg", ".jpeg", ".tif", ".tiff", ".zip", ".rtf", ".bak", ".dot", ".bmp"

- **All Files Including OS** deletes all files on the target device, including the operating system. The Data Delete operation is executed in two phases. In phase one, all user files are deleted, and a results log is sent to the Monitoring Center. In phase two, all system files excluding the Windows directory and the system root are deleted. No results log is created during phase two, as the operating system is destroyed, and it is not possible to upload the log file. All special settings and/or software components such as Antivirus software, encryption software, or special proxy settings are deleted in phase two, which might, occasionally result in a premature reboot or an incomplete Data Delete. For best results, it is recommended that you create a custom deletion policy that emulates "All Files Including OS" that

keeps files necessary for completing the Data Delete process intact.

- o **Custom Policy** allows you to specify a customized Data Delete policy. Specify the custom Data Delete policy using one of the following methods and then continue to step 8. one of the following methods:
 - Select the desired value in the list appearing next to the **Custom Policy** option button.
 - Create a new policy to meet your specific needs. Click the **Create a Policy** link. The Create and Edit Data Delete Policies page opens.

2. Data Delete Policy: *

☐ All Files Except OS ⓘ

☐ All Files Including OS ⓘ

☐ Custom Policy ⓘ

FIGURE 7. Request Data Delete — Data Delete Policy

8. In the **Data Delete Options** section, select the desired option in the **Number of Data Overwrites** list. The Data Overwrite feature deletes the specified data and overwrites it with random or garbage data to make the original data impossible to recover. The overwrite process is called a “data wipe”. Possible data wipe values are:
 - o **1 Data Overwrite** wipes the data once. The process is the fastest and offers the lowest level of security.
 - o **3 Data Overwrites** wipes the data three times. The process is slower than the process for 1 data wipe and offers a higher level of security.
 - o **7 Data Overwrites** is the default value for the **Number of Data Overwrites** list. The process is the slowest and offers the highest level of security.

3. Data Delete Options:

Number of Data Overwrites: ⓘ

7

☐ Perpetual Deletion ⓘ

☐ Include File Date Attributes ⓘ

FIGURE 8. Request Data Delete — Data Delete options

9. If desired, select the **Perpetual Deletion** option. Perpetual Deletion allows Data Delete to re-initialize on the targeted device should the

Agent on the device make a call to the Monitoring Center after the deletion cycle has completed.

IMPORTANT Perpetual Deletion is not recommended in the case of a stolen device. Repeated Data Delete cycles may delete the thief's data and/or make the thief aware of the device's remote activity that can reduce the chances of recovery.

NOTE **Perpetual Deletion** is only supported on Windows computers and Windows Mobile devices. On Windows Mobile devices, Perpetual Deletion is not dependent on a call to the Monitoring Center. Once Perpetual Deletion is initialized on a Windows Mobile device, deletion restarts automatically every twelve (12) hours.

10. If desired, select the **Include File Date Attributes in the Data Delete Log** option to specify Data Delete Attributes. Selecting this option includes the Created, Modified, and Accessed dates in the Data Delete log file.

By default, the **Created** and **Modified** dates appear in the log file for Windows Vista devices, and the **Created**, **Modified**, and **Accessed** dates appear for Windows XP devices.

NOTE File Date Attribute reporting is only supported on Windows computers.

IMPORTANT Including file date attributes increases the size of the data delete log file. If the log file is large and the target machine has a low-bandwidth Internet connection, data delete completion may be delayed while the client device repeatedly attempts to upload the log file to Customer Center.

11. In the Data Delete Validation section, if desired, select the **Ignore hard drive serial number check** box. Selecting the box allows Data Delete to override the Hard Disk Serial Number (HDSN) check and continue even when the Hard Disk serial number is unknown or changes during the lifecycle of the request.

IMPORTANT Use the Ignore HDSN check feature with care. A Data Delete operation deletes data on the target device. Overriding the HDSN check before performing a Data Delete operation may delete data created or owned by any post-loss possessors of the device.

NOTE If no hard drive serial number is detected for the target device, the **Ignore hard drive serial number check** box is selected by default. To continue, do not change the default value.

4. Data Delete Validation:

Drive Serial Number Check: ⓘ

☒ Ignore hard drive serial number check.

Data Delete Agreement:

THE BELOW IS SUBJECT TO THE TERMS AND CONDITIONS OF THE ABSOLUTE SOFTWARE SERVICE AGREEMENT AND A WRITTEN AND SIGNED DATA DELETE PRE-AUTHORIZATION AGREEMENT BETWEEN THE PARTIES, IF ANY (THE "WRITTEN AGREEMENT"). TO THE EXTENT OF ANY INCONSISTENCY BETWEEN THE SERVICE AGREEMENT AND THE BELOW TERMS AND CONDITIONS, THE TERMS AND CONDITIONS OF THE SERVICE AGREEMENT SHALL PREVAIL.

The "Data Delete Operation" means an operation authorized by the Corporation to have Absolute Software Corporation ("Absolute Software") attempt to remove all data and software, including the operating system if requested, from a personal device. For the Data Delete operation to be launched, the Computrace agent on the targeted device must make a call to Absolute's monitoring center after the Data Delete has been set up. Even if a call occurs, Absolute Software cannot guarantee the Data Delete Operation will be successful, nor will Absolute Software necessarily be able to verify that the Data Delete Operation has been completed. Further, as Absolute Software will not be able to back up the data or software as part of the Data Delete Operation, the data and software on the personal device will be lost to you following the completion of the Data Delete Operation. Please note Absolute Software will not

☐ I accept the agreement

Set Data Delete Save Draft Delete Draft Cancel

FIGURE 9. Request Data Delete - Data Delete Validation

12. Read the Data Delete Authorization Agreement carefully and select the **I accept the agreement** box to indicate you have read the agreement and accept the terms.
13. Click the **Set Data Delete** button. The Confirm Data Delete Request page opens.
14. Review the information, and then click the **Submit** button. The Request Authentication page opens.
15. Enter your Customer Center password and the RSA SecurID® Token Code or Security Authorization Code.
16. Click the **OK** button.

IMPORTANT Once you have clicked the **OK** button on the Request Authorization page, the Delete Request cannot be modified. However, it can be canceled, provided the request has not been launched on the target device.

NOTE To save your draft without launching the data delete operation, click the **Save Draft** button. Type your Customer Center Password and RSA SecurID® Token validation code or Security Authorization Code, and then click **OK**. To cancel the data delete request, click the **Cancel** button.

IMPORTANT Only draft requests can be deleted. Submitted requests can be canceled from the Data Delete Details page, provided the request has not been launched on the target device. Once a delete request is launched, it cannot be canceled, nor can the request be edited.

17. If the device is RTT and Intel AT enabled, a dialog box prompting you to force a call to the device using MCIC opens. If desired, force a call to the device. Once the device receives and processes the SMS message, depending upon the Data Delete settings specified for the account, the data delete request runs. See step 18 for more details on the data delete operation.
18. Once initiated, the Data Delete operation runs on the next Agent call, even if the user does not log in to the OS. Once the Data Delete process has begun, it cannot be stopped. If the Data Delete operation is interrupted by a system restart, Data Delete restarts only when the Windows or OS Login Screen appears.

IMPORTANT In some cases, if the hard drive serial number option is not selected, the Data Delete operation may fail because the Agent believes that the target device is different from the desired device. If the Data Delete operation fails in such cases, Customer Center sends a notification e-mail to the Security Administrator who requested the Data Delete operation.

Disabling Security Administrator Authorization

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

To disable your Security Administrator authorization:

1. Log in to Customer Center as a Security Administrator.

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

2. Click the **Administration** link on the global navigation bar. The Administration page opens.
3. In the Account section, click the **Disable Pre-Authorization** link. The Disable Pre-Authorization page opens.
4. Click the **Disable** button. A confirmation dialog displays.
5. Click the **OK** button to confirm the request.

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

Using Device Freeze

The Device Freeze feature allows pre-authorized Customer Center users to target specific devices and display a full screen message restricting users from operating the device. The proper workflow to use Device Freeze effectively is as follows:

1. [Requesting an Authorization Code](#)
2. [Creating a Custom Device Freeze Message](#)
3. [Freezing Devices](#)

Requesting an Authorization Code

You must request an authorization code before initiating any action in the data and device security section. Once you receive your authorization code by e-mail, you use it to validate your security operation.

To request an Authorization Code:

1. Log in to Customer Center as a Security Administrator.

NOTE If you do not log in as a Security Administrator, Customer Center displays an error when you open any Data and Device Security page.

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

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

Creating a Custom Device Freeze Message

To create a custom Device Freeze message:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Create Device Freeze Message** link. The Create Device Freeze Message page opens.

NOTE Alternatively, you can also click the **Add** button on the Device Freeze Messaging page to go to the Create Device Freeze Message page.

4. In the **Message Name** field, type a meaningful title for the new Device Freeze message. The title displays as an option in the **Select a message** list on the Request Device Freeze page.
5. In the Message Text field, type the text you want to display on frozen devices. You can use plain text or a combination of text with the following HTML formatting tags:
 - `<b>` — Render as bold
 - `<i>` — Italicize text
 - `<u>` — Add underline
 - `<font>` — Specify font to display a selection of text
 - `<p>` — Define a paragraph with default spacing before and after text
 - `<br>` — Add a line break without default spacing
6. Click the **Save** button. Customer Center saves the new message and refreshes the Create Device Freeze Message page to display a confirmation message.

See [“Managing Device Freeze Messages” on page 24](#) for more information about working with Custom Device Freeze messages.

Freezing Devices

Security Administrators can launch a Device Freeze request on any device in their account. You need an authorization code to request a Device Freeze. See [“Requesting an Authorization Code” on page 19](#) for more information.

IMPORTANT If you initiate a Device Freeze on a device with an outstanding Data Delete request or initiate a Data Delete Request on a device that has an outstanding Device Freeze request, the Device Freeze request implements after the Data Delete request completes.

Also, you cannot initiate Device Freeze on a stolen device with an open Theft Report. If you choose to implement Device Freeze on a stolen device without a Theft Report, you must unfreeze the device before filing a Theft Report. See your *End User Service Agreement* for more information.

Request Device Freeze

Request a Freeze for a device in your account.

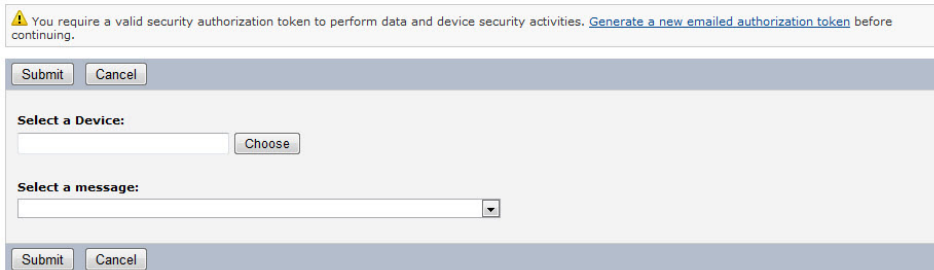


FIGURE 10. Request Device Freeze Page

To request Device Freeze:

NOTE The following instructions assume you have already signed and delivered the Security Administrator Pre-Authorization Form.

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the Create **Request Device Freeze** link. The Request Device Freeze page opens.
4. Specify the device to freeze in the **Identifier** box. To specify the device:
 - a) Click the **Choose** button to display a list of all devices in your account. The **Choose** dialog opens.
 - b) Click the **Identifier** of the desired device. The **Choose** dialog closes and the Device Freeze Details page opens to allow you to select a message for display on freeze.

5. In the **Message** drop-down list, select the desired message for display on the frozen device.
6. Click the **Freeze** button. The Provide Authentication page opens.
7. Enter your Customer Center password and the Authorization Code. See [“Requesting an Authorization Code” on page 19](#) for more information.
8. Click the **OK** button. The Device Freeze request is created and deployed to the device on the next Agent call.

IMPORTANT Once you click the **OK** button on the Provide Authentication page, the Device Freeze Request cannot be modified. However, it can be canceled, provided the request has not been launched on the target device.

Unfreezing Devices

Devices frozen using the Device Freeze feature can be unfrozen and made operational in the following two ways:

- Using Customer Center to unfreeze on Agent call
- Using an unfreeze code on the target device

Using Customer Center to unfreeze on Agent call

Security Administrators can unfreeze a device using the Device Freeze Details page on Customer Center. Once the unfreeze request is set on Customer Center, the device is unfrozen on the next Agent call to the Monitoring Center. Agents on frozen devices call into the Monitoring Center every 15 minutes.

To unfreeze devices using Customer Center:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. Enter all desired criteria on this page, and then click the **Show Results** button. The Device Freeze Summary Report page refreshes to display a list of all devices for your account containing a Device Freeze request in the results grid.
5. Click the **Unfreeze** button. The device is unfrozen on the next Agent call.

Using an unfreeze code on the target device

Frozen devices call the Monitoring Center every 15 minutes. If a device is unable to make Agent calls, you can unfreeze the device manually.

NOTE Unfreezing via an Agent call is the preferred method for unfreezing a device. If possible, unfreeze devices by setting the status on Customer Center only.

To unfreeze a device manually:

1. The user contacts their organization's Customer Support or the Security Administrator for their account to initiate a manual unfreeze request.
2. The Security Administrator generates an Unfreeze Pass Code using Customer Center and provides the Pass Code to the user with detailed instructions on unfreezing the device. To request an unfreeze Pass Code:
 - a) Log in to Customer Center as a Security Administrator.
 - b) Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
 - c) Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
 - d) Enter all desired criteria on this page, and then click the **Show Results** button. The Device Freeze Summary Report page refreshes to display a list of all devices for your account containing a Device Freeze request in the results grid.
 - e) Click the **Edit** link for the desired device. The Device Freeze Details page opens to display the details for the selected request.
 - f) Click the **Unfreeze** button. The Provide Authentication page opens.
 - g) Enter your Customer Center password and the Authorization Code. See ["Requesting an Authorization Code" on page 19](#) for more information.
 - h) Click the **OK** button. The Device Freeze Details page opens to display the Pass Code and instructions on how to use the Pass Code to unfreeze a device.

3. The user unfreezes the device as follows:

IMPORTANT The frozen device does not display any supporting fields to facilitate code entry. Pressing the **ESC** key allows the user to enter the Pass Code and unfreeze the device.

- a) On the frozen device, press the **ESC** button.

- b) Enter the Pass Code provided using the number keys in the upper row of the keyboard. The device is immediately unfrozen.

IMPORTANT If you enter the Pass Code using the numeric keypad, the device does not unfreeze.

Managing Device Freeze Messages

Security Administrators can create and edit custom Device Freeze messages using a combination of plain text and HTML formatting. Custom messages help you ensure that the appropriate information is available to the users of a frozen device. Such messages may include support contact information and/or other information that is necessary for users when calling Technical Support to restore functionality for frozen devices.

Editing Existing Custom Device Freeze Messages

To edit existing Device Freeze messages:

1. Log in to Customer Center as a Security Administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Messaging** link. The Device Freeze Messaging page opens to display a list of all messages available for your account.
4. Click the **Message Name** or the **Edit** link for the message you want to edit. The Create Device Freeze Message page opens.
5. Edit the message as desired.
6. Click the **Save** button. Customer Center saves the change and refreshes the Create Device Freeze Message page to display a confirmation message.

Deleting Existing Custom Device Freeze Messages

To delete existing Device Freeze messages:

1. Open the Create Device Freeze Message page for the desired message. See steps 1 to 4 above in the [Editing Existing Custom Device Freeze Messages](#) section for more information on opening the Create Device Freeze message page.
2. Click the **Delete** button. Customer Center deletes the message and refreshes the Create Device Freeze Message page to display a confirmation message.

Tracking Device Freeze Summary Status

To view the status and other details for a Device Freeze request:

1. Log in to Customer Center as an administrator.
2. Click the **Data and Device Security** link on the global navigation bar. The Data and Device Security page opens.
3. Click the **Device Freeze Summary Report** link. The Device Freeze Summary Report page opens.
4. Enter all desired criteria on this page, and then click the **Show Results** button. The Device Freeze Summary Report page refreshes to display a list of all devices for your account matching the search criteria in the results grid.
5. Click the **Edit** or **View** link for the desired device. The Device Freeze Details page opens to display the details for the selected request.